Guia do usuário

AWS Security Hub

AWS Security Hub : Guia do usuário

Table of Contents

O que são o Security Hub e o Security Hub CSPM?

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

AWS O Security Hub e o AWS Security Hub CSPM protegem seu ambiente de nuvem. Serviços da AWS Os serviços se complementam. Quando usados juntos, eles fornecem informações valiosas sobre a postura de segurança do seu AWS ambiente.

O Security Hub CSPM fornece uma visão abrangente de sua postura de segurança e ajuda você a avaliar seu ambiente de nuvem em relação aos padrões e melhores práticas do setor de segurança. O Security Hub fornece uma experiência unificada que ajuda você a priorizar e responder a problemas críticos de segurança. As descobertas do CSPM do Security Hub são encaminhadas automaticamente para o Security Hub, onde são correlacionadas com as descobertas de outros serviços de segurança, como o Amazon Inspector, para gerar exposições. Isso ajuda você a identificar os riscos mais críticos em seu ambiente. O Security Hub também fornece recursos automatizados de fluxo de trabalho, que ajudam você a incorporar as descobertas do CSPM do Security Hub em seus fluxos de trabalho operacionais.

Como prática recomendada, recomendamos ativar os dois serviços. Você pode habilitar o CSPM do Security Hub sem habilitar o Security Hub se seu foco principal for identificar configurações incorretas e avaliar sua postura de segurança. No entanto, se você habilitar o Security Hub sem habilitar o CSPM do Security Hub, o Security Hub não poderá usar as descobertas do CSPM do Security Hub para fornecer informações sobre riscos e exposições em seu ambiente. AWS Para obter a melhor experiência possível, recomendamos não apenas ativar o Security Hub e o CSPM do Security Hub, mas também ativar esses outros serviços de segurança: Amazon GuardDuty, AmazonInspector e Amazon Macie.

O que é o AWS Security Hub?

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

AWS O Security Hub é uma solução unificada de segurança em nuvem que prioriza seus problemas críticos de segurança e ajuda você a responder em grande escala. O Security Hub detecta problemas de segurança correlacionando e enriquecendo automaticamente sinais de segurança de várias fontes, como gerenciamento de postura, gerenciamento de vulnerabilidades (Amazon Inspector), dados confidenciais (Macie) e detecção de ameaças (). GuardDuty Isso permite que as equipes de segurança priorizem os riscos ativos em seus ambientes de nuvem por meio de análises automatizadas e insights contextuais. Por meio de visualizações intuitivas, o Security Hub transforma sinais de segurança complexos em insights acionáveis, o que permite que você tome decisões informadas sobre sua segurança rapidamente. O Security Hub também inclui fluxos de trabalho de resposta automatizados para ajudá-lo a corrigir riscos, melhorar a produtividade da equipe e minimizar interrupções operacionais.

Atributos

Solução de segurança unificada

Obtenha visibilidade mais ampla em seu ambiente de nuvem por meio do gerenciamento centralizado em uma solução unificada de segurança na nuvem.

Insights de segurança acionáveis

Obtenha insights de segurança acionáveis por meio de análises avançadas para aprender sobre os riscos de segurança associados ao seu ambiente.

Tempos de resposta reduzidos

Simplifique os tempos de resposta com fluxos de trabalho automatizados e um sistema de emissão de bilhetes integrado.

Descobertas de exposição

O Security Hub correlaciona as descobertas das verificações de controle CSPM do Security Hub, do Amazon Inspector e outras Serviços da AWS para detectar exposições associadas aos recursos. AWS

As descobertas são formatadas no Open Cybersecurity Schema Framework (OCSF)

O Security Hub gera descobertas no OCSF e recebe descobertas no OCSF do Security Hub CSPM e outros: Serviços da AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Painel

O console do Security Hub fornece uma visão abrangente de suas exposições, ameaças, cobertura de segurança e recursos, bem como uma visualização interativa chamada gráfico do caminho do ataque, que mostra como invasores em potencial podem acessar e assumir o controle dos recursos associados a uma descoberta de exposição.

Integrações com produtos de terceiros

Você pode aprimorar sua postura de segurança com as integrações do Security Hub. Por exemplo, se você usa Jira Cloud ouServiceNow ITSM, você pode usar esse recurso para criar tickets a partir de descobertas.

Integrações

O Security Hub se integra com o seguinte Serviços da AWS.

- AWS CSPM do Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

Regiões da AWS suportado para pré-visualização pública

O Security Hub oferece suporte ao seguinte Regiões da AWS para esta versão prévia pública.

- Ásia-Pacífico (Tóquio)
- Ásia-Pacífico (Seul)
- Asia Pacific (Osaka)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Canadá (Central)
- Europa (Frankfurt)
- Europa (Estocolmo)
- Europa (Irlanda)
- Oeste dos EUA (Norte da Califórnia)
- Oeste dos EUA (Oregon)
- Europa (Londres)
- Europa (Paris)
- América do Sul (São Paulo)
- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)

Os itens a seguir são opcionais Regiões da AWS, que exigem que você os habilite antes de poder acessá-los.

- Africa (Cape Town)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Jacarta)
- Europa (Milão)
- Oriente Médio (Bahrein)

Para obter informações sobre eles Regiões da AWS, consulte Status de aceitação no Guia do Regiões da AWS usuário das zonas de disponibilidade.

Acessibilidade

O Security Hub está disponível na Regiões da AWS lista acima. Você pode ativar o Security Hub para contas individuais ou contas em sua organização. Você pode acessar o Security Hub por meio do seguinte:

Console do Security Hub

O console do Security Hub é uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. Nesse console, você pode acessar sua conta, dados e recursos.

API do Security Hub

A API do Security Hub oferece acesso programático à sua conta, dados e recursos. Você pode enviar solicitações HTTPS diretamente para o Security Hub.

AWS CLI

Com o AWS CLI, você pode executar comandos na linha de comando do sistema para realizar tarefas e criar scripts que executem tarefas. Em alguns casos, o AWS CLI pode ser mais útil do que o console do Security Hub.

AWS SDKs

AWS SDKsconsistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação (C++, Go, Java, .NET e Python). Eles fornecem acesso programático ao Security Hub e outros Serviços da AWS no seu idioma preferido e podem ajudá-lo a gerenciar tarefas como gerenciar erros, assinar solicitações e repetir solicitações.

Preços

Não há custo para usar o Security Hub. O Security Hub é gratuito durante esta prévia pública.

Introdução ao Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Os tópicos desta seção descrevem como começar a usar o Security Hub.

Habilitar o Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Você pode ativar o Security Hub para qualquer um Conta da AWS. Os procedimentos neste tópico descrevem como habilitar o Security Hub a partir de uma conta de gerenciamento da AWS organização, uma conta de administrador delegado e uma conta independente.

> **Note**
>
> Depois de habilitar o Security Hub, as exposições em seu ambiente são analisadas imediatamente. No entanto, você pode esperar até 6 horas para receber uma descoberta de exposição para um recurso.

Habilitar o Security Hub para uma organização

O procedimento nesta seção descreve como habilitar o Security Hub para a conta de gerenciamento AWS da organização. O procedimento pressupõe que você tenha definido um administrador delegado para o CSPM do Security Hub e inclui uma etapa em que você pode definir um administrador delegado para sua organização no Security Hub. Para obter mais informações sobre como configurar um administrador delegado no Security Hub, consulte Configurando uma conta de administrador delegado no Security Hub.

Se você decidir definir um administrador delegado para o Security Hub durante a habilitação, precisará criar uma política de recursos no AWS Organizations console permitindo que o administrador delegado execute ações em nome da sua organização. Você pode usar o exemplo de política de recursos a seguir para a conta de administrador delegado.

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

```
      "Principal": {
        "AWS": "arn:aws:iam::delegated-administrator-account-id:root"
      },
      "Action": [
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations:DetachPolicy",
        "organizations:DeletePolicy",
        "organizations:UpdatePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType"
      ],
      "Resource": "*"
    }
  ]
}
```

Se você não definir um administrador delegado, poderá definir um administrador delegado posteriormente. Para obter mais informações, consulte Configurando uma conta de administrador delegado no Security Hub. O tópico inclui um procedimento que descreve como definir um administrador delegado para sua organização na página Geral no console do Security Hub.

O procedimento a seguir descreve como definir uma conta de administrador delegado para sua organização no Security Hub.

Para habilitar o Security Hub para uma conta de gerenciamento AWS da organização

1. Faça login na sua AWS conta com as credenciais da conta de gerenciamento da AWS organização. Abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. Na página inicial do Security Hub, selecione Security Hub. Escolha Começar.
3. (Opcional) Para Conta de administrador delegado, defina um administrador delegado com base nas opções fornecidas. Como prática recomendada, recomendamos usar o mesmo administrador delegado em todos os serviços de segurança para uma governança consistente. Para obter mais informações sobre como configurar uma conta de administrador delegado, consulte Configurando uma conta de administrador delegado no Security Hub.

4. (Opcional) Em Ativação da conta, selecione a caixa para ativar o Security Hub para sua AWS conta.
5. Escolha Copiar e anexar para abrir as configurações da organização. No console Organizations, selecione Delegate em Delegated administrator for AWS Organizations e cole a política de recursos. Escolha Criar política.
6. Acesse o console do Security Hub. Selecione Configurar.

Quando você ativa o Security Hub, uma função vinculada ao serviço chamada AWSServiceRoleForSecurityHubV2 é criada na sua conta e um gravador vinculado ao serviço é adicionado à sua conta. Um gravador vinculado a serviços é um tipo de AWS Config gravador gerenciado por um AWS serviço que pode registrar dados de configuração em recursos específicos do serviço. Com um gravador vinculado ao serviço, o Security Hub permite uma abordagem orientada por eventos para obter os itens de configuração de recursos necessários para a cobertura da análise de exposição. Um gravador vinculado ao serviço é configurado por Conta da AWS e. Região da AWS

> **Note**
>
> Se você definir um administrador delegado, o administrador delegado poderá criar e aplicar uma política que permita habilitar e desabilitar contas de membros do Security Hub. Para obter mais informações, consulte Criação de uma política como administrador delegado para gerenciar contas de membros.

Habilitar o Security Hub para o administrador delegado

Se a conta de gerenciamento AWS da organização definir um administrador delegado para sua organização, o administrador delegado deverá habilitar o Security Hub para sua conta. O procedimento a seguir deve ser concluído pelo administrador delegado, mas somente se o administrador delegado não tiver habilitado o Security Hub para sua conta. Para obter informações sobre como configurar um administrador delegado, consulte Configurando uma conta de administrador delegado no Security Hub.

Para habilitar o Security Hub para uma conta de administrador delegado

1. Entre na sua AWS conta com suas credenciais de administrador delegado e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/ v2/home.

2. Na página inicial do Security Hub, selecione Security Hub e escolha Começar.
3. Escolha Habilitar.
4. (Opcional) Para Tags, determine se deseja adicionar um par de valores-chave à configuração da conta.
5. Escolha Ir para o Security Hub.

Quando você ativa o Security Hub, uma função vinculada ao serviço chamada AWSServiceRoleForSecurityHubV2 é criada na sua conta e um gravador vinculado ao serviço é adicionado à sua conta. Um gravador vinculado a serviços é um tipo de AWS Config gravador gerenciado por um AWS serviço que pode registrar dados de configuração em recursos específicos do serviço. Com um gravador vinculado ao serviço, o Security Hub permite uma abordagem orientada por eventos para obter os itens de configuração de recursos necessários para a cobertura da análise de exposição. Um gravador vinculado ao serviço é configurado por Conta da AWS e. Região da AWS

> **Note**
>
> Como administrador delegado de uma organização, você pode criar e aplicar uma política que permite habilitar e desabilitar contas de membros para o Security Hub. Para obter mais informações, consulte Criação de uma política como administrador delegado para gerenciar contas de membros.

Ativar o Security Hub para uma conta independente

O procedimento a seguir descreve como habilitar o Security Hub para uma conta autônoma. Há dois tipos de contas autônomas que podem ativar o Security Hub: uma que Conta da AWS não está dentro de uma organização e uma Conta da AWS está dentro de uma organização. Um Conta da AWS interior de uma AWS organização pode ser aquele Conta da AWS em que um administrador delegado anexa uma AWS Organizations política ao. Conta da AWS Para obter mais informações, consulte as políticas do Security Hub no Guia AWS Organizations do Usuário.

Para habilitar o Security Hub para uma conta independente

1. Entre na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. Na página inicial do Security Hub, selecione Security Hub e escolha Começar.

3. Escolha Habilitar.

Quando você ativa o Security Hub, uma função vinculada ao serviço chamada AWSServiceRoleForSecurityHubV2 é criada na sua conta e um gravador vinculado ao serviço é adicionado à sua conta. Um gravador vinculado a serviços é um tipo de AWS Config gravador gerenciado por um AWS serviço que pode registrar dados de configuração em recursos específicos do serviço. Com um gravador vinculado ao serviço, o Security Hub permite uma abordagem orientada por eventos para obter os itens de configuração de recursos necessários para a cobertura da análise de exposição. Um gravador vinculado ao serviço é configurado por Conta da AWS e. Região da AWS

Configurando uma conta de administrador delegado no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Na conta de gerenciamento AWS da organização, você pode definir um administrador delegado para sua organização. Como prática recomendada, recomendamos usar o mesmo administrador delegado em todos os serviços de segurança para uma governança consistente. Os procedimentos desta seção descrevem como definir um administrador delegado para sua organização de duas maneiras. A primeira maneira é usar uma conta de gerenciamento AWS da organização que não tenha definido um administrador delegado no CSPM do Security Hub. A segunda forma é usar uma conta de gerenciamento AWS da organização que habilitou o Security Hub, mas ignorou a configuração de um administrador delegado durante a habilitação.

Considerações

Você pode encontrar um cenário em que deseja definir um administrador delegado para o Security Hub que seja diferente do administrador delegado para o Security Hub CSPM. Se você tiver um administrador delegado configurado no Security Hub CSPM, considere o seguinte:

- Se a conta de gerenciamento AWS da organização estiver definida como administrador delegado do CSPM do Security Hub, você não poderá definir essa conta como administrador delegado do Security Hub. No entanto, você pode designar outro Conta da AWS na organização como administrador delegado do Security Hub. Para uma governança consistente em todos os serviços

de segurança, recomendamos usar a mesma conta (exceto a conta de gerenciamento da AWS organização) do administrador delegado do Security Hub CSPM e do Security Hub.

- Se uma conta diferente da conta de gerenciamento da AWS organização for definida como administrador delegado do CSPM do Security Hub, essa conta se tornará automaticamente o administrador delegado no Security Hub. Nesse cenário, o Security Hub só permite que esse específico Conta da AWS sirva como administrador delegado.

> **Note**
>
> Se você estiver usando uma conta diferente da conta de gerenciamento da organização como administrador delegado do CSPM do Security Hub, removê-la por meio do console CSPM do Security Hub ou da API AWS Organizations também a removerá do Security Hub. Da mesma forma, se você remover o administrador delegado do Security Hub por meio do console do Security Hub ou da API AWS Organizations, ele será removido do CSPM do Security Hub. Quando o administrador delegado for removido do CSPM do Security Hub, a Configuração Central desativará automaticamente.

O procedimento a seguir pressupõe que você não tenha definido um administrador delegado para o CSPM do Security Hub e esteja configurando um administrador delegado para o Security Hub.

Para definir um administrador delegado no Security Hub

1. Entre na sua AWS conta com as credenciais da conta de gerenciamento da organização e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. Na página inicial do Security Hub, selecione Security Hub e escolha Começar.
3. Em Administrador delegado, escolha Configurar. Na janela pop-up, insira o Conta da AWS número de 12 dígitos do Conta da AWS que você deseja ou escolha uma conta sugerida (se você usa administradores delegados em outros serviços de segurança) para definir como administrador delegado da sua organização. Escolha Salvar.
4. (Opcional) Para habilitação da conta, selecione a caixa para habilitar o Security Hub para sua. Conta da AWS
5. Escolha Copiar e anexar para abrir as configurações da organização. No console Organizations, selecione Delegate em Delegated administrator for AWS Organizations e cole a política de recursos. Escolha Criar política.
6. Acesse o console do Security Hub. Selecione Configurar.

> **Note**
>
> Depois de definir o administrador delegado, essa conta deve habilitar o Security Hub e configurar políticas para receber descobertas de sua conta membro.

O procedimento a seguir pressupõe que você habilitou o Security Hub, mas ignorou a configuração de um administrador delegado durante a habilitação. Você pode definir um administrador delegado no console do Security Hub na página Geral.

Para definir um administrador delegado no console do Security Hub a partir da página Geral

1. Entre na sua AWS conta com as credenciais da conta de gerenciamento da organização e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. No painel de navegação, escolha Geral.
3. Em Administrador delegado, escolha Configurar. Na janela pop-up, insira o Conta da AWS número de 12 dígitos do Conta da AWS que você deseja definir como administrador delegado da sua organização. Ou escolha uma sugestão Conta da AWS se você definir um administrador delegado em outros serviços AWS de segurança. Escolha Salvar.

Depois de concluir esse procedimento, você precisará copiar a declaração de política de delegação do Security Hub e anexá-la ao administrador delegado para obter a AWS Organizations política, para que o administrador delegado do Security Hub possa executar ações no Security Hub. Sem essa declaração de política, o administrador delegado não pode configurar o Security Hub para sua organização. Para obter mais informações, consulte Anexando a declaração de política de delegação para o Security Hub.

Anexando a declaração de política de delegação para o Security Hub

Na conta de gerenciamento da organização, você deve copiar a declaração de política de delegação do Security Hub e anexá-la ao administrador delegado para obter a AWS Organizations política, para que o administrador delegado do Security Hub possa realizar ações no Security Hub. Sem essa declaração de política, o administrador delegado não pode configurar o Security Hub para sua organização. Você pode copiar essa política da página Geral no console do Security Hub. Ao fazer isso, você é direcionado para a página Configurações no AWS Organizations console, onde pode editar a AWS Organizations política do administrador delegado. Este tópico descreve como copiar a política no Security Hub. Para obter informações sobre como atualizar a política do administrador

delegado, consulte Atualizar uma AWS Organizations política de delegação baseada em recursos AWS Organizations no Guia do AWS Organizations Usuário.

Para anexar a declaração de política de delegação para o Security Hub

1. Entre na sua AWS conta com as credenciais da conta de gerenciamento da organização e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. No painel de navegação, escolha Geral.
3. Na declaração de política de delegação para o Security Hub, escolha Copiar e anexar. Você será direcionado para a página Configurações, na AWS Organizations qual poderá editar a AWS Organizations política do administrador delegado para incluir a declaração da política de delegação. Se você quiser ver a declaração de política antes de copiá-la, escolha Detalhes da política.

> **Note**
>
> Se você definir um administrador delegado, o administrador delegado poderá criar e aplicar uma política que permita habilitar e desabilitar contas de membros. O procedimento no tópico a seguir descreve como definir essa política.

Criação de uma política como administrador delegado para gerenciar contas de membros

Como administrador delegado de uma organização, você pode criar e aplicar uma política que permite ativar e desativar contas de membros. Você pode acessar todas as suas políticas configuradas na tela Configurações do console do Security Hub. O procedimento a seguir descreve como criar essa política.

> **Note**
>
> A etapa 6. é uma etapa opcional na qual você pode descrever como essa política interage com as políticas principais. Para obter informações sobre herança de políticas, consulte Entendendo a herança de políticas de gerenciamento no Guia do usuário.AWS Organizations

Para criar uma política que permita ativar e desativar contas de membros

1. Faça login usando suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, escolha Configurações e, em seguida, selecione Configurações.
3. Selecione Criar política.
4. Em Detalhes, insira um nome para a política e determine se deseja inserir uma descrição opcional para a política.
5. Em Regiões, escolha Ativar todas as regiões, Desativar todas as regiões ou Especificar regiões. Se você escolher Ativar todas as regiões, poderá determinar se deseja ativar automaticamente novas regiões. Se você escolher Desativar todas as regiões, poderá determinar se deseja desativar automaticamente novas regiões. Se você escolher Especificar regiões, deverá escolher quais regiões deseja ativar e desativar.
6. (Opcional) Para configurações avançadas, consulte as orientações do AWS Organizations.
7. (Opcional) Para Tags, determine se deseja adicionar um par de valores-chave à política. É possível adicionar até 50 tags.
8. Escolha Próximo.
9. Revise suas alterações e escolha Aplicar. Suas contas de destino são configuradas com base na política. Para ver a política efetiva no nível da conta, você pode revisar a guia Organização na página Configurações, onde você pode escolher uma conta.

Removendo a conta de administrador delegado no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Você pode remover a conta de administrador delegado no console do Security Hub a qualquer momento. No entanto, essa ação não só remove o administrador delegado do Security Hub, mas também o CSPM do Security Hub. Recomendamos realizar essa ação somente quando você tiver confirmado essa operação com sua conta de segurança.

> **Note**
>
> Se você estiver usando uma conta diferente da conta de gerenciamento da organização como administrador delegado do CSPM do Security Hub, removê-la por meio do console do CSPM ou da AWS Organizations API também a removerá do Security Hub.
> Da mesma forma, se você remover o administrador delegado do Security Hub por meio do console ou da AWS Organizations API do Security Hub, ele também será removido do CSPM do Security Hub. Quando o administrador delegado for removido do CSPM, a Configuração Central desativará automaticamente.

Para remover a conta de administrador delegado

1. Faça login na sua AWS conta com as credenciais da conta de gerenciamento da organização e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home?região = us-east-1.
2. No painel de navegação, escolha Geral.
3. Em Administrador delegado, escolha Remover administrador delegado. Na janela pop-up, insira confirmar e escolha Remover.

Recomendações do Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Os seguintes serviços de segurança AWS enviam descobertas para o Security Hub no formato OCSF. Depois de habilitar o Security Hub, recomendamos habilitá-los Serviços da AWS para segurança adicional.

CSPM do Security Hub

Ao habilitar o Security Hub CSPM, você obtém uma visão abrangente do seu estado de segurança em. AWS Isso ajuda você a avaliar seu ambiente em relação aos padrões e às melhores práticas do setor de segurança. Embora você possa começar a usar o Security Hub sem habilitar o CSPM do

Security Hub, recomendamos habilitar o CSPM do Security Hub porque o Security Hub correlaciona os sinais de segurança do CSPM do Security Hub para melhorar seu gerenciamento de postura.

Se você habilitar o CSPM do Security Hub, também recomendamos ativar o padrão AWS Foundational Security Best Practices para sua conta. Esse padrão consiste em um conjunto de controles que detectam quando seus recursos Contas da AWS e recursos se desviam das melhores práticas de segurança. Quando você ativa o padrão AWS Foundational Security Best Practices para sua conta, o AWS Security Hub CSPM ativa automaticamente todos os seus controles, incluindo controles para os seguintes tipos de recursos:

- Controles de conta
- Controles do DynamoDB
- EC2 Controles da Amazon
- Controles do IAM
- AWS Lambda controles
- Controles do Amazon RDS
- Controles do Amazon S3

Você pode desativar qualquer um dos controles dessa lista. No entanto, se você desabilitar qualquer um desses controles, não poderá receber descobertas de exposição dos recursos suportados. Para obter informações sobre controles que se aplicam ao padrão AWS Foundational Security Best Practices, consulte o padrão AWS Foundational Security Best Practices v1.0.0 (FSBP).

GuardDuty

Ao habilitar GuardDuty, você pode visualizar todas as suas descobertas sobre ameaças e cobertura de segurança no painel do console do Security Hub. Se você habilitar GuardDuty, começará GuardDuty automaticamente a enviar dados para o Security Hub no formato OCSF.

Amazon Inspector

Ao habilitar o Amazon Inspector, você pode visualizar todas as suas exposições e descobertas de cobertura de segurança no painel do console do Security Hub. Se você habilitar o Amazon Inspector, o Amazon Inspector começará automaticamente a enviar dados para o Security Hub no formato OCSF.

Recomendamos ativar o escaneamento da Amazon e o EC2 escaneamento padrão Lambda. Quando você ativa o EC2 escaneamento da Amazon, o Amazon Inspector verifica as instâncias da

EC2 Amazon em sua conta em busca de vulnerabilidades de pacotes e problemas de acessibilidade de rede. Quando você ativa o escaneamento padrão do Lambda, o Amazon Inspector verifica as funções do Lambda em busca de vulnerabilidades de software nas dependências do pacote. Para obter mais informações, consulte Ativar um tipo de escaneamento no Guia do usuário do Amazon Inspector.

Macie

Ao habilitar o Macie, você pode detectar exposições adicionais para seus buckets do Amazon S3. Recomendamos configurar a descoberta automática de dados confidenciais, para que o Macie possa avaliar seu inventário de buckets do Amazon S3 diariamente.

Conceitos do Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Os termos e conceitos a seguir ajudarão você a entender como gerenciar as descobertas de exposição.

Exposição

Um possível cenário de segurança em sua conta que pode ser devido a vulnerabilidades, recursos exploráveis ou configurações incorretas.

Constatação de exposição

Um tipo de descoberta que descreve uma exposição presente em seu ambiente. Uma descoberta de exposição inclui características e sinais. Um sinal pode incluir um ou mais tipos de características de exposição. O Security Hub gera uma descoberta de exposição quando sinais das descobertas de controle do CSPM do Security Hub ou de outros Serviços da AWS, como o Amazon Inspector, indicam a presença de uma exposição. Um recurso pode ter no máximo uma descoberta de exposição. O Security Hub gera uma descoberta de exposição quando um recurso é exposto. Se um recurso não tiver nenhuma característica de exposição ou tiver características insuficientes, o Security Hub não gerará uma descoberta de exposição para esse recurso.

Sinal

Uma descoberta que contribui para uma descoberta de exposição. Um sinal pode ser chamado de descoberta contributiva. Um sinal pode se originar no Security Hub, CSPM, ou outro AWS Config Serviços da AWS, como o Amazon Inspector.

Traço

Um desvio de segurança que resulta em uma descoberta de exposição. Os tipos de características incluem configuração incorreta, acessibilidade, dados confidenciais e vulnerabilidade. Uma característica está associada a um sinal e um sinal pode conter várias características. Por exemplo, um controle CSPM do Security Hub indica que uma política gerenciada pelo cliente permite o controle de acesso administrativo. Esse sinal contém uma característica de configuração incorreta.

Descobertas do OCSF no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Todas as descobertas no Security Hub são formatadas no Open Cybersecurity Schema Framework (OCSF). O Security Hub considera `activity_name != Close` as descobertas com descobertas ativas. As descobertas ativas são excluídas automaticamente se não forem atualizadas em 90 dias. O Security Hub considera as descobertas com `Activity_name = Close` descobertas fechadas. As descobertas fechadas são excluídas automaticamente se não forem atualizadas em 14 dias. O Security Hub determina quando uma descoberta é atualizada usando o valor mais recente da descobertamodified_time_dt. Ao final do período de retenção de uma descoberta, o Security Hub exclui permanentemente a descoberta. Os provedores de busca podem alterar o valor do `finding.info.modified_time_dt` campo ao atualizarem uma descoberta. Para obter informações sobre outros `Activity_name` valores, consulte Detecção de vulnerabilidades no esquema OCSF.

Descobertas de cobertura no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

As descobertas de cobertura do Security Hub fornecem visibilidade sobre quais recursos de AWS segurança estão habilitados e onde pode haver lacunas na cobertura em uma conta independente ou em todo o AWS ambiente de uma organização. A ativação de recursos de segurança adicionais aprimorará os recursos de detecção do Security Hub. As descobertas de cobertura avaliam quais GuardDuty recursos de CSPM do Amazon Inspector, Macie e Security Hub estão habilitados para uma conta. Essas descobertas aparecem como um widget no painel do Security Hub com a capacidade de detalhar visualizações mais detalhadas por recurso de segurança específico. Para o administrador delegado, esse widget mostra o detalhamento da cobertura em todas as contas habilitadas para o Security Hub.

Limitações

- Para contas de membros, as informações de cobertura são agregadas em todas as contas vinculadas Regiões da AWS, mas somente para essa conta de membro.
- As informações de cobertura não são mostradas para contas não integradas ao Security Hub
- A cobertura indica apenas se um AWS service (Serviço da AWS) está ativado, não se recursos específicos em um AWS serviço estão habilitados.

Resultados da cobertura do Security Hub CSPM

As descobertas da cobertura do CSPM do Security Hub avaliam se um padrão de segurança qualificado de gerenciamento de postura está habilitado em uma conta. A ativação de qualquer padrão CSPM do Security Hub se qualificará, com exceção dos padrões de marcação AWS Control Tower de recursos.

Pode levar até 24 horas para detectar padrões habilitados por padrão ao ativar o CSPM do Security Hub.

Conclusões de cobertura para GuardDuty

GuardDuty os resultados de cobertura avaliam se GuardDuty está habilitado e quais GuardDuty recursos estão habilitados em um Conta da AWS:

- Proteção contra malware para a Amazon EC2 — verifica as EC2 instâncias da Amazon em busca de possíveis malwares
- Proteção do Amazon EKS — monitora os registros de auditoria do Kubernetes em busca de ameaças nos clusters do Amazon EKS
- Proteção Lambda — analisa as invocações da função Lambda em busca de possíveis ameaças
- Proteção do Amazon S3 — analisa eventos de dados em busca de possíveis ameaças aos buckets do Amazon S3
- Proteção do Amazon RDS — monitora ameaças aos bancos de dados do Amazon RDS
- Monitoramento do tempo de execução — Fornece monitoramento em tempo real do comportamento do tempo de execução nas EC2 instâncias da Amazon

Pode levar até 24 horas para que as atualizações da GuardDuty cobertura sejam refletidas em todas as contas dos membros de uma organização.

Descobertas de cobertura do Amazon Inspector

As descobertas de cobertura do Amazon Inspector avaliam se o Amazon Inspector está ativado e quais recursos estão habilitados em uma conta:

- Amazon EC2 Scanning — Verifica as EC2 instâncias da Amazon em busca de vulnerabilidades
- Amazon ECR Scanning — digitaliza imagens de contêineres no Amazon ECR em busca de vulnerabilidades
- Escaneamento padrão do Lambda — verifica as funções do Lambda em busca de vulnerabilidades
- Digitalização de código Lambda — verifica as funções do código Lambda em busca de vulnerabilidades de código
- Segurança de código do Amazon Inspector — verifica o código-fonte de aplicativos primários, dependências de aplicativos de terceiros e a infraestrutura como código em busca de vulnerabilidades

Conclusões da cobertura de Macie

As descobertas de cobertura do Macie são avaliações que indicam se o Macie está habilitado para cruzar. Contas da AWS

Pode levar até 24 horas para que as atualizações da descoberta automatizada de dados confidenciais do Macie sejam refletidas em todas as contas dos membros de uma organização.

Descobertas de exposição no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub correlaciona descobertas das verificações de controle CSPM do Security Hub e outras Serviços da AWS, como o Amazon Inspector, para detectar exposições associadas aos recursos. AWS Uma descoberta de exposição é um tipo de descoberta que descreve uma possível exposição em seu ambiente devido a vulnerabilidades, recursos exploráveis ou configurações incorretas. Ao priorizar e resolver suas exposições mais críticas, você pode evitar possíveis ataques contra seu ambiente. Você pode acessar suas descobertas de exposição no console do Security Hub e programaticamente com as operações do Security Hub CSPM e da API do Security Hub.

Tipos de recursos compatíveis para descobertas de exposição no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub gera descobertas de exposição para os seguintes tipos de AWS recursos:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`

- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`

O Security Hub gera uma descoberta de exposição por recurso. Se um recurso não tiver nenhuma característica de exposição ou tiver características insuficientes, o Security Hub não gerará uma descoberta de exposição para esse recurso.

Tipos de características compatíveis no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub gera uma descoberta de exposição quando as descobertas do controle CSPM do AWS Security Hub e as descobertas geradas por outros suportados Serviços da AWS, como o Amazon Inspector, contêm características de exposição de um recurso. A tabela a seguir fornece informações sobre os tipos de características compatíveis.

Tipo de característica	Descrição	Origem	Recursos afetados
Configuração incorreta	Indica um recurso mal configurado.	Descobertas do controle CSPM do Security Hub.	Todos os tipos de recursos.
Acessibilidade	Indica caminhos de rede abertos para um recurso.	Descobertas do controle CSPM do Security Hub e descobertas de acessibilidade da rede do Amazon Inspector.	EC2 Instâncias da Amazon

Tipo de característica	Descrição	Origem	Recursos afetados
Dados sigilosos	Indica que um recurso contém dados confidenciais.	Descobertas de dados confidenciais da Macie.	Buckets do Amazon S3
Vulnerabilidades	Indica que um recurso está exposto a vulnerabilidades e exposição comuns (CVEs).	Descobertas de vulnerabilidade do pacote Amazon Inspector.	EC2 Instâncias da Amazon, serviços do Amazon ECS, clusters do Amazon EKS e funções Lambda

Cada característica pode ser associada a vários títulos que fornecem detalhes sobre a exposição que afeta o recurso. Por exemplo, você pode ver um título de exploração disponível para a característica de vulnerabilidade nos detalhes de uma descoberta de EC2 exposição.

Gerando resultados de exposição

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub gera resultados de exposição a cada 6 horas. Durante cada período de 6 horas, o Security Hub considera as características de exposição disponíveis para um recurso. Ele produz no máximo uma descoberta de exposição por ID de recurso. A exclusividade de uma descoberta é determinada por ID Região da AWS, tipo e conta. Isso significa que você pode ter dois recursos com a mesma ID, mas os recursos seriam de tipos diferentes. Essa descoberta de exposição agrega todas as características de exposição aplicáveis que se aplicam ao recurso.

Se um recurso não tiver nenhuma característica de exposição ou tiver características insuficientes, o Security Hub não gerará uma descoberta de exposição para esse recurso. O Security Hub não publica descobertas de exposição para tipos de recursos que não suportam descobertas de exposição. Quando um recurso tem um número significativo e uma combinação de características,

o Security Hub gera uma descoberta de exposição. O número e a combinação de características também determinam o nível de severidade da descoberta de exposição.

Descoberta da exposição da amostra

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub normaliza as descobertas de exposição no Open Cybersecurity Schema Framework (OCSF).

Exemplo de esquema OCSF

No exemplo de esquema OCSF a seguir, o `related_events` parâmetro contém detalhes exclusivos da descoberta de exposição, como descobertas contribuintes. As descobertas que contribuem são as características e sinais associados a uma descoberta de exposição. Uma única descoberta contributiva pode incluir uma ou mais características. O `observables` parâmetro identifica o recurso associado à descoberta contribuinte. Isso pode ser diferente do `resources` parâmetro, que identifica o recurso associado à descoberta da exposição.

```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
```

```
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
                            "Exploit Available",
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
```

```
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title":  "Lambda function policies should prohibit public access",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
```

```
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "VeepLambdaRule3"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
VeepLambdaRule3/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
```

```
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
    "severity": "Critical",
    "severity_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
    }
}
```

Determinar o nível de severidade de uma constatação de exposição

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O Security Hub atribui a cada exposição encontrando uma severidade padrão de`CRITICAL`,`HIGH`,`MEDIUM`, ou`LOW`. Os resultados de exposição com uma severidade de `INFORMATIONAL` não foram publicados. O Security Hub usa vários fatores para determinar o nível de severidade padrão de uma descoberta de exposição:

- Consciência — Até que ponto a exposição não é teórica, mas tem explorações automatizadas ou disponíveis publicamente. Isso se aplica às descobertas de exposição para EC2 instâncias e funções Lambda.
- Facilidade de descoberta — se ferramentas automatizadas, como varredura de portas ou pesquisa na Internet, estão disponíveis para descobrir o recurso em risco.
- Facilidade de exploração — A facilidade com que um agente de ameaça pode explorar a exposição. Por exemplo, se existirem caminhos de rede abertos ou metadados mal configurados, um agente de ameaça poderá explorar mais facilmente a exposição.

- Probabilidade de exploração — A probabilidade de a exposição ser explorada nos próximos 30 dias. Esse fator corresponde ao Exploit Protection Scoring System (EPSS) e se aplica às descobertas de exposição para instâncias da Amazon EC2 e funções Lambda.
- Impacto — O dano se a exploração for realizada. Por exemplo, uma exposição pode levar à perda de responsabilidade, perda de disponibilidade, perda de confidencialidade devido à exposição de dados ou perda de integridade devido à corrupção de dados.

Analisando os resultados da exposição

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Você pode revisar todas as suas descobertas de exposição no console do AWS Security Hub e com a API. A página Exposições no console do Security Hub mostra todas as descobertas de exposição ativa. Os resultados da exposição são listados por severidade decrescente. Você pode filtrar suas descobertas de exposição adicionando e removendo filtros com a barra de pesquisa Adicionar filtro. Você pode agrupar suas descobertas de exposição com o menu suspenso Grupo por. Você também pode filtrar suas descobertas de exposição com o menu Filtros rápidos.

Detalhes dos resultados de exposição

Você pode ver muitos detalhes de uma descoberta de exposição. No console do Security Hub, esses detalhes são divididos entre as guias. A guia Visão geral fornece um instantâneo da descoberta de exposição. A guia Características lista as características e sinais associados a uma descoberta de exposição. A guia Recursos fornece detalhes sobre o recurso e as tags de recursos associadas a uma descoberta de exposição. A lista a seguir fornece descrições dos detalhes da descoberta de exposição.

- Título da descoberta — O título da descoberta da exposição.
- Nível de severidade — O nível de severidade da descoberta de exposição. O Security Hub usa o número e a combinação de características de um recurso para determinar o nível de severidade de uma descoberta de exposição. O nível de severidade pode ser `CRITICAL`,`HIGH`,`MEDIUM`, ou`LOW`. O Security Hub não publica descobertas de exposição com uma severidade de`INFORMATIONAL`. Você pode atualizar o `Severity` por meio do console do Security Hub ou com a operação BatchUpdateFindingsV2da API.

- Descrição — A descrição da descoberta de exposição.
- Tipo — O nome do tipo de descoberta de exposição. Por exemplo, o nome pode ser parecido `Exposure/Potential Impact/Resource Hijacking` com.
- Conta — O ID do Conta da AWS local em que a descoberta de exposição foi gerada.
- Idade — Indica há quanto tempo a descoberta de exposição está ativa.
- Hora de criação — Um carimbo de data/hora que indica quando a descoberta de exposição foi criada.
- Hora modificada — Uma data e hora que indica quando a descoberta da exposição foi atualizada pela última vez.
- Região — Região da AWS Onde a descoberta de exposição foi gerada.
- Nome do produto — O nome do produto que gerou a descoberta de exposição.
- Nome da empresa — O nome da empresa que gerou a descoberta de exposição.
- Nome da atividade — O nome da atividade.
- Status — O status dessa descoberta de exposição.
- ID de busca — Um identificador exclusivo associado à descoberta de exposição.
- Caminho de ataque potencial (somente console) — Uma visualização interativa mostra como possíveis invasores podem acessar e assumir o controle dos recursos associados a uma descoberta de exposição. Para obter mais informações, consulte Visualizando exposições no Security Hub com o gráfico do caminho de ataque potencial.
- Traços — Identifica os tipos e títulos de características associados à descoberta de exposição. No console do Security Hub, você pode visualizar características por tipo de característica ou sinal. Isso ajuda você a analisar as descobertas contribuintes no contexto da exposição relacionada.
- Recursos — Identifica o recurso associado à descoberta de exposição.

Analisando os detalhes das descobertas de exposição

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Este tópico descreve como analisar detalhes sobre descobertas de exposição no console do Security Hub e com a API.

Analisando detalhes de uma descoberta de exposição no console do Security Hub

Para ver detalhes de uma descoberta de exposição no console do Security Hub

1. Faça login usando suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, escolha Exposições.
3. Escolha uma descoberta de exposição da qual você deseja ver os detalhes.

Analisando detalhes de uma descoberta de exposição com a API

Você pode revisar os resultados da exposição com a `GetFindingsV2`API ou com AWS CLI o. Você pode filtrar os resultados com o `FindingProviderFieldsTypes` parâmetro e fornecer um valor de filtro de `Exposure/EC2` se quiser retornar apenas as descobertas de exposição para EC2 instâncias. Você pode filtrar por outros campos para restringir os resultados.

Exemplo de comando

Veja a seguir um AWS CLI exemplo que recupera as 10 descobertas de exposição geradas mais recentemente em sua conta. 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-v2 \
                    --max-results '10' \
                    --filter '{"CompositeFilters": [{"StringFilters":
 [{"FieldName":"finding_info.title","Filter":
 {"Value":"GuardDuty","Comparison":"PREFIX"}} ]}]}'
```

Remediando os resultados da exposição

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Os tópicos desta seção descrevem os riscos de remediação para diferentes Serviços da AWS.

O `Remediation` campo do formato OCSF contém dois campos: e. `remediation` `references`

```
"Remediation": {
```

```
      "Recommendation": {
       "remediation":{"desc":"String",
       "references":["string array"]}
      }
},
```

> **Note**
>
> A orientação de remediação fornecida nas seções a seguir pode exigir consultas adicionais em outros AWS recursos.

Correção de exposições para tabelas do DynamoDB

AWS O Security Hub pode gerar descobertas de exposição para tabelas do DynamoDB.

No console do Security Hub, a tabela do DynamoDB envolvida em uma descoberta de exposição e suas informações de identificação estão listadas na seção Recursos dos detalhes da descoberta. Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a reduzir o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

Características de configuração incorreta no DynamoDB

A seguir, descrevemos as características de configuração incorreta e as etapas de correção das tabelas do DynamoDB.

A tabela do DynamoDB tem a recuperação desativada point-in-time

Habilitar a recuperação do DynamoDB point-in-time

A recuperação do point-in-time DynamoDB fornece backups automáticos contínuos para os dados da tabela do DynamoDB. Para obter informações sobre como restaurar uma tabela do DynamoDB em um determinado momento, consulte Restauração de uma tabela do DynamoDB em um ponto no tempo no Guia do usuário do Amazon DynamoDB.

A tabela do DynamoDB não é coberta por um plano de backup

AWS O Backup fornece um serviço centralizado para configurar, gerenciar e automatizar backups em vários AWS serviços, incluindo o DynamoDB. Sem um plano de backup, sua tabela não tem backups programados e automatizados com períodos de retenção personalizáveis, criando riscos de segurança significativos. Um invasor pode corromper ou excluir os dados da tabela de forma maliciosa. Sem backups adequados, você pode não ter nenhuma opção de recuperação além da janela de Point-in-Time recuperação (se ativada), o que pode resultar em perda permanente de dados. Seguindo as melhores práticas de proteção de dados, recomendamos cobrir suas tabelas do DynamoDB com um plano de backup.

Criar um plano de backup

Antes de criar um plano de backup, determine a frequência de backup e os períodos de retenção adequados para seus dados. Para obter informações sobre como criar um plano de backup, consulte Atribuir recursos a um plano de backup no Guia do usuário do Amazon DynamoDB.

A tabela do DynamoDB tem a proteção contra exclusão desativada

A proteção contra exclusão impede a exclusão acidental de tabelas do DynamoDB. Quando a proteção contra exclusão está desativada, as tabelas do DynamoDB ficam vulneráveis à exclusão

não intencional por meio de ações do console, chamadas de API, comandos da CLI ou processos automatizados. Isso pode expor seu AWS ambiente à perda de dados, pois uma entidade não autorizada com acesso ao seu AWS ambiente pode excluir tabelas intencionalmente, resultando em interrupção do serviço e perda permanente de dados. Seguindo as melhores práticas de proteção de dados, recomendamos ativar a proteção de dados para tabelas do DynamoDB.

Habilitar proteção contra exclusão

Se você gerencia várias tabelas, considere usar AWS CloudFormation para atualizar as propriedades da tabela em massa. Você pode modificar seus AWS CloudFormation modelos para incluir `DeletionProtectionEnabled` propriedades e atualizar suas pilhas. Depois de concluir a correção, verifique se a proteção contra exclusão está ativada no menu suspenso Informações adicionais na guia Configurações da tabela.

Correção de exposições para instâncias EC2

AWS O Security Hub pode gerar descobertas de exposição para instâncias do Amazon Elastic Compute Cloud (EC2).

No console do Security Hub, a EC2 instância envolvida em uma descoberta de exposição e suas informações de identificação estão listadas na seção Recursos dos detalhes da descoberta. Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

Características de configuração incorreta para instâncias EC2

Aqui estão as características de configuração incorreta das EC2 instâncias e as etapas de correção sugeridas.

A EC2 instância permite acesso ao IMDS usando a versão 1

Os metadados da instância são dados sobre sua EC2 instância da Amazon que os aplicativos podem usar para configurar ou gerenciar a instância em execução. O serviço de metadados da instância (IMDS) é um componente na instância que o código na instância usa para acessar metadados da instância com segurança. Se o IMDS não estiver protegido adequadamente, ele pode se tornar um potencial vetor de ataque, pois fornece acesso a credenciais temporárias e outros dados de configuração confidenciais. IMDSv2 fornece proteção mais forte contra exploração por meio de autenticação orientada à sessão, exigindo um token de sessão para solicitações de metadados e limitando a duração da sessão. Seguindo os princípios de segurança padrão, AWS recomenda que você configure as EC2 instâncias da Amazon para uso IMDSv2 e desativação IMDSv1.

Teste a compatibilidade do aplicativo

Antes de implementar IMDSv2, teste sua instância para garantir sua compatibilidade com IMDSv2 o. Alguns aplicativos ou scripts podem exigir IMDSv1 a funcionalidade principal e exigir configuração adicional. Para obter mais informações sobre ferramentas e caminhos recomendados para testar a compatibilidade de aplicativos, faça a transição para o uso do Instance Metadata Service versão 2 no Guia do usuário do Amazon Elastic Compute Cloud.

Atualize a instância a ser usada IMDSv2

Modifique as instâncias existentes para usar IMDSv2. Para obter mais informações, consulte Modificar opções de metadados de instância para instâncias existentes no Guia do usuário do Amazon Elastic Compute Cloud.

Aplique atualizações às instâncias em um grupo de Auto Scaling

Se sua instância fizer parte de um grupo de Auto Scaling, atualize seu modelo de execução ou configuração de execução com uma nova configuração e execute uma atualização da instância.

A função do IAM associada à EC2 instância da Amazon tem uma política de acesso administrativo.

As políticas de acesso administrativo fornecem às EC2 instâncias da Amazon amplas permissões Serviços da AWS e recursos. Essas políticas geralmente incluem permissões não necessárias para a funcionalidade da instância. Fornecer uma identidade do IAM com uma política de acesso administrativo em uma EC2 instância da Amazon (em vez do conjunto mínimo de permissões que a função associada ao seu perfil de instância precisa) pode aumentar o escopo de um ataque se a EC2 instância da Amazon for comprometida. Se uma instância for comprometida, os invasores poderão utilizar essas permissões excessivas para se mover lateralmente pelo ambiente, acessar dados ou manipular recursos. Seguindo os princípios de segurança padrão, recomendamos que você conceda privilégios mínimos, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

Revise e identifique políticas administrativas

No painel do IAM, encontre a função com o nome da função. Analise a política de permissões anexada à função do IAM. Se a política for AWS gerenciada, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações com `"Effect": "Allow", "Action": "*" "Resource": "*"` e.

Implemente o acesso de privilégio mínimo

Substitua as políticas administrativas por políticas que concedam somente as permissões específicas necessárias para que a instância funcione. Para obter mais informações sobre as melhores práticas de segurança para funções do IAM, consulte Aplicar permissões de privilégios mínimos em Práticas recomendadas de segurança no Guia do usuário.AWS Identity and Access Management Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário. Como alternativa, você pode criar uma nova função do IAM para evitar impactar outros aplicativos usando a função existente. Nesse cenário, crie uma nova função do IAM e associe a nova função do IAM à instância. Para obter instruções sobre como substituir uma função do IAM por uma instância, consulte Anexar uma função do IAM a uma instância no Guia do usuário do Amazon Elastic Compute Cloud.

Considerações sobre configuração segura

Se forem necessárias permissões administrativas em nível de serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

- Considerações sobre configuração segura

  - Autenticação multifatorial (MFA) — A MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas. Para obter mais informações, consulte Exigir autenticação multifator (MFA) no Guia AWS Identity and Access Management do usuário.
  - Condições do IAM — A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA. Para obter mais informações, consulte Condições de uso nas políticas do IAM para restringir ainda mais o acesso no Guia AWS Identity and Access Management do usuário.
  - Limites de permissões — Os limites de permissão estabelecem o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo. Para obter mais informações, consulte Usar limites de permissões para delegar o gerenciamento de permissões em uma conta no Guia do AWS Identity and Access Management usuário.

Aplique atualizações às instâncias em um grupo de auto scaling

Para EC2 instâncias da Amazon em um grupo de AWS auto scaling, atualize o modelo de execução ou a configuração de execução com o novo perfil de instância e execute uma atualização da instância. Para obter informações sobre a atualização de um modelo de lançamento, consulte

Modificar um modelo de lançamento (gerenciar versões do modelo de lançamento) no Guia do usuário do Amazon Elastic Compute Cloud. Para obter mais informações, consulte Usar uma atualização de instância para atualizar instâncias em um grupo do Auto Scaling. Para obter mais informações sobre o uso de funções do IAM com grupos do Auto Scaling, consulte Função do IAM para aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do Amazon Auto EC2 Scaling.

A função do IAM associada à EC2 instância da Amazon tem uma política de administração de serviços.

As políticas de acesso ao serviço fornecem às EC2 instâncias da Amazon amplas permissões para AWS serviços e recursos. Essas políticas geralmente incluem permissões que não são necessárias para a funcionalidade da instância. Fornecer uma identidade do IAM com uma política de acesso administrativo em uma EC2 instância da Amazon, em vez do conjunto mínimo de permissões que a função associada ao seu perfil de instância precisa, pode aumentar o escopo de um ataque se uma instância for comprometida. Seguindo os princípios de segurança padrão, recomendamos que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

Revise e identifique políticas administrativas

No painel do IAM, encontre a função com o nome da função. Analise a política de permissões anexada à função do IAM. Se a política for AWS gerenciada, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações com `"Effect": "Allow", "Action": "*"` `"Resource": "*"` e.

Implemente o acesso de privilégio mínimo

Substitua as políticas de administração do serviço por aquelas que concedem somente as permissões específicas necessárias para que a instância funcione. Para obter mais informações sobre as melhores práticas de segurança para funções do IAM, consulte Aplicar permissões de privilégios mínimos em Práticas recomendadas de segurança no Guia do usuário.AWS Identity and Access Management Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário. Como alternativa, você pode criar uma nova função do IAM para evitar o impacto de outros aplicativos que estão usando a função existente. Nesse cenário, crie uma nova função do IAM e associe a nova função do IAM à instância. Para obter informações

sobre a substituição de uma função do IAM por uma instância, consulte Anexar uma função do IAM a uma instância no Guia do usuário do Amazon Elastic Compute Cloud

Considerações sobre configuração segura

Se forem necessárias permissões administrativas em nível de serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

Considerações sobre configuração segura

Se forem necessárias permissões administrativas em nível de serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

- Autenticação multifatorial (MFA) — A MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas. Para obter mais informações, consulte Exigir autenticação multifator (MFA) no Guia AWS Identity and Access Management do usuário.
- Condições do IAM — A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA. Para obter mais informações, consulte Condições de uso nas políticas do IAM para restringir ainda mais o acesso no Guia AWS Identity and Access Management do usuário.
- Limites de permissões — Os limites de permissão estabelecem o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo. Para obter mais informações, consulte Usar limites de permissões para delegar o gerenciamento de permissões em uma conta no Guia do AWS Identity and Access Management usuário.

Aplique atualizações às instâncias no grupo Auto Scaling

Para EC2 instâncias da Amazon em um grupo de AWS auto scaling, atualize o modelo de execução ou a configuração de execução com o novo perfil de instância e execute uma atualização da instância. Para obter informações sobre a atualização de um modelo de lançamento, consulte Modificar um modelo de lançamento (gerenciar versões do modelo de lançamento) no Guia do usuário do Amazon Elastic Compute Cloud. Para obter mais informações, consulte Usar uma atualização de instância para atualizar instâncias em um grupo do Auto Scaling. Para obter mais informações sobre o uso de funções do IAM com grupos do Auto Scaling, consulte Função do IAM para aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do Amazon Auto EC2 Scaling.

A EC2 instância da Amazon tem um grupo de segurança ou ACL de rede que permite acesso SSH ou RDP.

Protocolos de acesso remoto, como SSH e RDP, permitem que os usuários se conectem e gerenciem EC2 instâncias da Amazon a partir de locais externos. Quando grupos de segurança permitem acesso irrestrito a esses protocolos pela Internet, eles aumentam a superfície de ataque de suas EC2 instâncias da Amazon ao permitir o acesso à sua instância pela Internet. Seguindo os princípios de segurança padrão, AWS recomenda limitar o acesso remoto a endereços IP ou intervalos específicos e confiáveis.

1. Modificar as regras do grupo de segurança

   Restrinja o acesso às suas EC2 instâncias da Amazon a endereços IP confiáveis específicos. Limite o acesso SSH e RDP a endereços IP confiáveis específicos ou use a notação CIDR para especificar intervalos de IP (por exemplo, 198.168.1.0/24). Para modificar as regras do grupo de segurança, consulte Configurar regras do grupo de segurança no Guia do usuário do Amazon Elastic Compute Cloud.

A EC2 instância da Amazon tem um grupo de segurança aberto

Os grupos de segurança atuam como firewalls virtuais para suas EC2 instâncias da Amazon para controlar o tráfego de entrada e saída. Grupos de segurança abertos, que permitem acesso irrestrito de qualquer endereço IP, podem expor suas instâncias ao acesso não autorizado. Seguindo os princípios de segurança padrão, AWS recomenda restringir o acesso do grupo de segurança a endereços IP e portas específicos.

Revise as regras do grupo de segurança e avalie a configuração atual

Avalie quais portas estão abertas e acessíveis a partir de amplos intervalos de IP, como`(0.0.0.0/0 or ::/0)`. Para obter instruções sobre como visualizar os detalhes do grupo de segurança, consulte DescribeSecurityGroupsa Referência de API do Assistente de Portabilidade para o.NET.

Modificar as regras do grupo de segurança

Modifique suas regras de grupo de segurança para restringir o acesso a intervalos ou endereços IP confiáveis específicos. Ao atualizar suas regras de grupo de segurança, considere separar os requisitos de acesso para diferentes segmentos de rede criando regras para cada intervalo de IP de origem necessário ou restringindo o acesso a portas específicas. Para modificar as regras do grupo de segurança, consulte Configurar regras do grupo de segurança no Guia EC2 do usuário da Amazon.

A EC2 instância da Amazon tem um endereço IP público

EC2 As instâncias da Amazon com endereços IP públicos podem ser acessadas publicamente pela Internet. Embora endereços IP públicos às vezes sejam necessários para instâncias que fornecem serviços a clientes externos, isso pode ser usado como um possível ataque a entidades não autorizadas. Seguindo os princípios de segurança padrão, AWS recomenda que você limite a exposição pública dos recursos sempre que possível.

Mova a instância para uma sub-rede privada

Se a instância não exigir acesso direto à Internet, considere movê-la para uma sub-rede privada dentro da sua VPC. Isso removerá seu endereço IP público e, ao mesmo tempo, permitirá que ele se comunique com outros recursos em sua VPC. Para obter mais informações, consulte Como faço para mover minha EC2 instância da Amazon para outra sub-rede, zona de disponibilidade ou VPC? no Centro de AWS Conhecimento.

Configure instâncias para execução sem endereços IP públicos

Se a instância foi executada em uma sub-rede pública que não exige endereços IP públicos, a configuração de execução pode ser modificada para impedir a atribuição automática de endereços IP públicos. Isso pode ser desativado no nível da sub-rede ou ao iniciar instâncias individuais. Para obter mais informações, consulte Modificar os atributos de endereçamento IP da sua sub-rede no Guia do usuário da Amazon Virtual Private Cloud e endereçamento EC2instance IP da Amazon Amazon no Guia do usuário do Amazon Elastic Compute Cloud.

Métodos alternativos de acesso

Considere as seguintes opções para métodos alternativos de acesso:

- Use um gateway NAT para conectividade de saída com a Internet —

  Para instâncias em sub-redes privadas que exigem acesso à Internet (por exemplo, para baixar atualizações), considere usar um gateway NAT em vez de atribuir um endereço IP público. Um gateway NAT permite que instâncias em sub-redes privadas iniciem conexões de saída com a Internet e, ao mesmo tempo, impeçam conexões de entrada da Internet. Para obter mais informações, consulte gateways NAT no Guia do usuário da Amazon Virtual Private Cloud.
- Use o Elastic Load Balancing — Para instâncias que estão executando aplicativos web, considere usar um Elastic Load Balancer (LB). LBs pode ser configurado para permitir que suas instâncias sejam executadas em sub-redes privadas enquanto o LB é executado em uma sub-rede pública e gerencia o tráfego da Internet. Para obter mais informações, consulte O que é o Elastic Load

Balancing? no Guia do usuário do AWS ELB. Consulte Sub-redes do balanceador de carga na Orientação AWS prescritiva para obter orientação sobre como escolher uma estratégia de aderência para seu LB.

Características de acessibilidade para instâncias EC2

Aqui estão as características de acessibilidade das EC2 instâncias e as etapas de remediação sugeridas.

A EC2 instância pode ser acessada pela Internet

EC2 Instâncias da Amazon com portas que podem ser acessadas pela Internet por meio de um gateway de Internet (incluindo instâncias por trás de Application Load Balancers ou Classic Load Balancers), uma conexão de emparelhamento de VPC ou um gateway virtual VPN podem expor sua instância à Internet. Seguindo os princípios de segurança padrão, recomendamos implementar controles de acesso à rede com privilégios mínimos restringindo o tráfego de entrada somente às fontes e portas necessárias.

Modificar ou remover regras do grupo de segurança

Na guia Recursos, abra o recurso para o Amazon EC2 Security Group. Verifique se o acesso à Internet é necessário para que a instância funcione. Modifique ou remova as regras de entrada do grupo de segurança que permitem acesso irrestrito (`0.0.0.0/0`ou`::/0`). Implemente regras mais restritivas com base em intervalos de IP ou grupos de segurança específicos. Se for necessário acesso público limitado, restrinja o acesso a portas e protocolos específicos necessários para a função da instância. Para obter instruções sobre como gerenciar regras de grupos de segurança, consulte Configurar regras de grupos de segurança no Guia EC2 do usuário da Amazon.

Atualizar rede ACLs

Analise e modifique as listas de controle de acesso à rede (ACLs) associadas à sub-rede da instância. Verifique se as configurações da ACL estão alinhadas com as alterações do grupo de segurança e não permitem o acesso público involuntariamente. Para obter instruções sobre como modificar a rede ACLs, consulte Trabalhar com rede ACLs no Guia do usuário da Amazon VPC.

Métodos alternativos de acesso

Considere as seguintes opções para métodos alternativos de acesso:

- Use o NAT Gateway para conectividade de saída com a Internet — Para instâncias em sub-redes privadas que exigem acesso à Internet (por exemplo, para baixar atualizações), considere usar um

NAT Gateway em vez de atribuir um endereço IP público. Um gateway NAT permite que instâncias em sub-redes privadas iniciem conexões de saída com a Internet e, ao mesmo tempo, impeçam conexões de entrada da Internet. s

- Use o Systems Manager Session Manager — O Session Manager fornece acesso seguro ao shell às suas EC2 instâncias da Amazon sem a necessidade de portas de entrada, gerenciamento de chaves SSH ou manutenção de bastion hosts.
- Use WAF e Elastic Load Balancing ou Application Load Balancer — Para instâncias que estão executando aplicativos web, considere usar um LB AWS combinado com o Web Application Firewall (WAF). LBs pode ser configurado para permitir que suas instâncias sejam executadas em sub-redes privadas enquanto o LB é executado em uma sub-rede pública e gerencia o tráfego da Internet. Adicionar um WAF ao seu balanceador de carga fornece proteção adicional contra explorações da web e bots.

A EC2 instância da Amazon pode ser acessada dentro da Amazon VPC

A Amazon Virtual Private Cloud (Amazon VPC) permite que você lance AWS recursos em uma rede virtual definida. As configurações de rede Amazon VPC que permitem acesso irrestrito entre instâncias podem aumentar o escopo de um ataque se uma instância for comprometida. Seguindo as melhores práticas de segurança, AWS recomenda a implementação de segmentação de rede e controles de acesso com privilégios mínimos nos níveis de sub-rede e grupo de segurança.

Analise os padrões de conectividade de rede Amazon VPC

Na descoberta de exposição, identifique o ID do grupo de segurança no ARN. Identifique quais instâncias precisam se comunicar entre si e em quais portas. Você pode usar o Amazon VPC Flow Logs para analisar os padrões de tráfego existentes em sua Amazon VPC para ajudar a identificar quais portas estão sendo usadas.

Modificar as regras do grupo de segurança

Modifique suas regras de grupo de segurança para restringir o acesso a intervalos ou endereços IP confiáveis específicos. Por exemplo, em vez de permitir todo o tráfego de todo o intervalo CIDR da VPC (por exemplo, 10.0.0.0/16), restrinja o acesso a grupos de segurança ou intervalos de IP específicos. Ao atualizar suas regras de grupo de segurança, considere separar os requisitos de acesso para diferentes segmentos de rede criando regras para cada intervalo de IP de origem necessário ou restringindo o acesso a portas específicas. Para modificar as regras do grupo de segurança, consulte Configurar regras do grupo de segurança no Guia EC2 do usuário da Amazon.

Considere organizar seus recursos da Amazon VPC em sub-redes com base nos requisitos ou funções de segurança. Por exemplo, coloque servidores web e servidores de banco de dados em sub-redes separadas. Para obter mais informações, consulte Sub-redes para sua VPC no Guia do usuário da Amazon Virtual Private Cloud.

Configurar a rede ACLs para proteção em nível de sub-rede

As listas de controle de acesso à rede (NACLs) fornecem uma camada adicional de segurança no nível da sub-rede. Diferentemente dos grupos de segurança, não NACLs têm estado e exigem que as regras de entrada e saída sejam definidas explicitamente. Para obter mais informações, consulte Controle o tráfego de sub-rede com listas de controle de acesso à rede no Guia do usuário da Amazon Virtual Private Cloud.

Considerações adicionais

Considere o seguinte ao restringir o acesso à sua Amazon VPC

- Transit Gateway ou Amazon VPC Peering com roteamento restritivo — Se sua arquitetura usa vários VPCs que precisam se comunicar, considere usar o Transit Gateway AWS e o Amazon VPC peering para fornecer conectividade entre a Amazon e, ao VPCs mesmo tempo, permitir que você controle quais sub-redes podem se comunicar entre si. Para obter mais informações, consulte Comece a usar os Amazon VPC Transit Gateways e as conexões de emparelhamento de VPC.
- Endpoints de serviço e links privados — Os endpoints do Amazon VPC podem ser usados para manter o tráfego na rede e se comunicar AWS com AWS os recursos, em vez de usar a Internet. Isso reduz a necessidade de conectividade direta entre instâncias que acessam os mesmos serviços. Para obter informações sobre endpoints de VPC, consulte O que são endpoints de VPC da Amazon? no Guia do usuário da Amazon Virtual Private Cloud. Para conectividade com serviços hospedados em outros Amazon VPCs, considere usar AWS PrivateLink.

Traços de vulnerabilidade para EC2 instâncias

Aqui estão as características de vulnerabilidade das EC2 instâncias e as etapas de correção sugeridas.

EC2 instância tem vulnerabilidades de software que podem ser exploradas pela rede com alta probabilidade de exploração

Pacotes de software instalados em EC2 instâncias podem ser expostos a vulnerabilidades e exposições comuns (). CVEs Os críticos CVEs representam riscos de segurança significativos

para seu AWS ambiente. Diretores não autorizados podem explorar essas vulnerabilidades não corrigidas para comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, ou para acessar outros sistemas. Vulnerabilidades críticas com alta probabilidade de exploração representam ameaças imediatas à segurança, pois o código de exploração pode já estar disponível publicamente e ser usado ativamente por invasores ou por ferramentas de verificação automatizadas. Recomendamos corrigir essas vulnerabilidades para proteger sua instância.

Atualizar instâncias afetadas

Revise a seção Referências na guia Vulnerabilidade da característica. A documentação do fornecedor pode incluir orientações específicas de remediação. Siga a remediação apropriada usando estas diretrizes gerais:

Use o Systems Manager Patch Manager para aplicar patches para sistemas operacionais e aplicativos. O Patch Manager ajuda você a selecionar e implantar patches de sistema operacional e software automaticamente em grandes grupos de instâncias. Se você não tiver o Patch Manager configurado, atualize manualmente o sistema operacional em cada instância afetada.

Atualize os aplicativos afetados para suas versões seguras mais recentes seguindo os procedimentos recomendados pelo fornecedor. Para gerenciar atualizações de aplicativos em várias instâncias, considere usar o Systems Manager State Manager para manter seu software em um estado consistente. Se as atualizações não estiverem disponíveis, considere remover ou desativar o aplicativo vulnerável até que um patch seja lançado ou outras mitigações, como restringir o acesso à rede ao aplicativo ou desativar recursos vulneráveis.

Siga as recomendações específicas de remediação fornecidas na descoberta do Amazon Inspector. Isso pode envolver a alteração das regras do grupo de segurança, a modificação das configurações da instância ou o ajuste das configurações do aplicativo.

Verifique se a instância faz parte do Auto Scaling Group. A correção de substituição de AMI é feita em infraestruturas imutáveis por meio da atualização do ID da AMI que está configurado para implantar novas instâncias da Amazon EC2 em um grupo de Auto Scaling. Se você estiver usando uma custom/golden AMI, crie uma instância com a nova AMI, personalize a instância e crie uma nova AMI dourada. Para obter mais informações, consulte Correção de atualizações de AMI (uso de patches AMIs para grupos de Auto Scaling).

Considerações futuras

Para evitar futuras ocorrências, considere implementar um programa de gerenciamento de vulnerabilidades. O Amazon Inspector pode ser configurado para verificar automaticamente

suas CVEs instâncias. O Amazon Inspector também pode ser integrado ao Security Hub para remediações automáticas. Considere implementar um cronograma regular de patches usando o Systems Manager Maintenance Windows para minimizar a interrupção em suas instâncias.

A EC2 instância da Amazon tem vulnerabilidades de software

Pacotes de software instalados na Amazon EC2instances podem ser expostos a vulnerabilidades e exposições comuns (). CVEs Os não críticos CVEs representam pontos fracos de segurança com menor gravidade ou capacidade de exploração em comparação com os críticos. CVEs Embora essas vulnerabilidades representem menos riscos imediatos, os invasores ainda podem explorar essas vulnerabilidades não corrigidas para comprometer a confidencialidade, a integridade ou a disponibilidade dos dados ou acessar outros sistemas. Seguindo as melhores práticas de segurança, AWS recomenda corrigir essas vulnerabilidades para proteger sua instância contra ataques.

Atualizar instâncias afetadas

Use o AWS Systems Manager Patch Manager para aplicar patches para sistemas operacionais. O Patch Manager ajuda você a selecionar e implantar patches de sistema operacional e software automaticamente em grandes grupos de instâncias. Se você não tiver o Patch Manager configurado, atualize manualmente o sistema operacional em cada instância afetada.

Atualize os aplicativos afetados para suas versões seguras mais recentes seguindo os procedimentos recomendados pelo fornecedor. Para gerenciar atualizações de aplicativos em várias instâncias, considere usar o AWS Systems Manager State Manager para manter seu software em um estado consistente. Se as atualizações não estiverem disponíveis, considere remover ou desativar o aplicativo vulnerável até que um patch seja lançado ou outras mitigações, como restringir o acesso à rede ao aplicativo ou desativar recursos vulneráveis.

Siga as recomendações específicas de remediação fornecidas na descoberta do Amazon Inspector. Isso pode envolver a alteração das regras do grupo de segurança, a modificação das configurações da instância ou o ajuste da configuração do aplicativo.

Verifique se a instância faz parte do Auto Scaling Group. A correção de substituição de AMI é feita em infraestruturas imutáveis por meio da atualização do ID da AMI que está configurado para implantar novas instâncias da Amazon EC2 em um grupo de Auto Scaling. Se você estiver usando uma custom/golden AMI, crie uma instância com a nova AMI, personalize a instância e crie uma nova AMI dourada. Para obter mais informações, consulte Correção de atualizações de AMI (uso de patches AMIs para grupos de Auto Scaling).

Considerações futuras

Para evitar futuras ocorrências, considere implementar um programa de gerenciamento de vulnerabilidades. O Amazon Inspector pode ser configurado para verificar automaticamente suas CVEs instâncias. O Amazon Inspector também pode ser integrado ao Security Hub para remediações automáticas. Considere implementar um cronograma regular de patches usando o Systems Manager Maintenance Windows para minimizar a interrupção em suas instâncias.

Correção de exposições para serviços do Amazon ECS

AWS O Security Hub pode gerar resultados de exposição para os serviços do Amazon Elastic Container Service (Amazon ECS).

O serviço Amazon ECS envolvido em uma descoberta de exposição e suas informações de identificação estão listados na seção Recursos dos detalhes da descoberta. Você pode recuperar esses detalhes do recurso no console do Security Hub ou programaticamente com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

- O serviço Amazon ECS usa uma definição de tarefa que permite que os contêineres acessem os sistemas de arquivos raiz.
- O serviço Amazon ECS usa uma definição de tarefa configurada para compartilhar o namespace de processo de um host
- O serviço Amazon ECS usa uma definição de tarefa configurada com credenciais de texto não criptografado nas variáveis de ambiente.
- O serviço Amazon ECS tem um grupo de segurança aberto
- O serviço Amazon ECS tem endereços IP públicos
- O serviço Amazon ECS usa uma definição de tarefa que é configurada com o modo de rede do host ativado.
- A função do IAM associada ao serviço Amazon ECS tem uma política de acesso administrativo
- Traços de vulnerabilidade para os serviços do Amazon ECS
  - O serviço Amazon ECS tem um contêiner com vulnerabilidades de software que podem ser exploradas pela rede e com alta probabilidade de exploração
  - O serviço Amazon ECS tem um contêiner com vulnerabilidades de software

Características de configuração incorreta dos serviços do Amazon ECS

Aqui estão as características de configuração incorreta dos serviços do Amazon ECS e as etapas de correção sugeridas.

O serviço Amazon ECS usa uma definição de tarefa configurada com privilégios elevados

Os contêineres do Amazon ECS executados com privilégios elevados têm recursos semelhantes aos do sistema host, potencialmente permitindo o acesso aos recursos do host e a outros contêineres. Essa configuração aumenta o risco de que um contêiner comprometido possa ser usado para acessar ou modificar recursos fora do escopo pretendido, o que pode levar à fuga do contêiner, ao acesso não autorizado ao host subjacente e a violações que afetam outros contêineres no mesmo host. Seguindo os princípios de segurança padrão, AWS recomenda que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

Revise e modifique a definição da tarefa

Na exposição, identifique o ARN da definição da tarefa. Abra a definição da tarefa no console do Amazon ECS. Na definição da tarefa, procure o sinalizador privilegiado definido como verdadeiro

nas definições do contêiner. Se o modo privilegiado não for necessário, crie uma nova revisão de definição de tarefa sem o sinalizador privilegiado. Se o modo privilegiado for necessário, considere configurar o contêiner para usar um sistema de arquivos somente para leitura para evitar modificações não autorizadas.

O serviço Amazon ECS tem um contêiner que pode assumir uma função do IAM

As funções do IAM permitem que as tarefas do Amazon ECS acessem com segurança outros AWS serviços usando credenciais temporárias. As funções de execução de tarefas podem ser necessárias para tarefas do Amazon ECS em que o contêiner precisa interagir com outros AWS recursos. Embora isso às vezes seja necessário para a funcionalidade do contêiner, funções configuradas incorretamente podem conceder privilégios excessivos que podem ser explorados por invasores se um contêiner for comprometido, potencialmente permitindo acesso não autorizado a AWS recursos, roubo de dados ou modificação não autorizada de sua infraestrutura. Seguindo os princípios de segurança padrão, AWS recomenda implementar o acesso com privilégios mínimos e revisar as funções do IAM associadas às suas tarefas do Amazon ECS.

Revise as funções anexadas

Acesse o painel do IAM e selecione a função identificada. Analise a política de permissões anexada à função do IAM. Se a tarefa exigir interação com outros AWS serviços, mantenha a função de execução da tarefa e considere aplicar permissões de privilégios mínimos. Caso contrário, crie uma nova revisão de definição de tarefa sem a função de execução.

O serviço Amazon ECS usa uma definição de tarefa que permite que os contêineres acessem os sistemas de arquivos raiz.

Os contêineres do Amazon ECS com acesso ao sistema de arquivos raiz do host podem potencialmente ler, modificar ou executar arquivos essenciais no sistema host. Essa configuração aumenta o risco de que um contêiner comprometido possa ser usado para acessar ou modificar recursos fora do escopo pretendido, potencialmente expondo dados confidenciais no sistema de arquivos do host. Seguindo os princípios de segurança padrão, AWS recomenda que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

Revise e modifique contêineres com acesso ao sistema de arquivos do host

Na descoberta de exposição, identifique o ARN da definição da tarefa. Abra a definição da tarefa no console do Amazon ECS. Procure a seção de volumes na definição da tarefa que define os

mapeamentos do caminho do host. Analise a definição da tarefa para determinar se o acesso ao sistema de arquivos do host é necessário para a funcionalidade do contêiner. s Se o acesso ao sistema de arquivos do host não for necessário, crie uma nova revisão da definição da tarefa e remova todas as definições de volume que usem caminhos do host. Se for necessário acessar o sistema de arquivos do host, considere configurar o contêiner para usar um sistema de arquivos somente para leitura para evitar modificações não autorizadas.

O serviço Amazon ECS usa uma definição de tarefa configurada para compartilhar o namespace de processo de um host

Os contêineres do Amazon ECS executados com namespaces expostos podem potencialmente acessar recursos do sistema do host e outros namespaces de contêineres. Essa configuração pode permitir que um contêiner comprometido escape de seu limite de isolamento, o que pode levar ao acesso a processos, interfaces de rede ou outros recursos fora do escopo pretendido. Um namespace de ID de processo (PID) fornece separação entre processos. Ele impede que os processos do sistema sejam visíveis e permite que 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. Esses fatores podem levar ao acesso não autorizado aos processos no próprio host, incluindo a capacidade de manipulá-los e encerrá-los. Seguindo os princípios de segurança padrão, AWS recomenda manter o isolamento adequado do namespace para contêineres.

Atualize as definições de tarefas com namespaces expostos

Abra a guia Recursos da exposição, identifique a definição da tarefa com o namespace exposto. Abra a definição da tarefa no console do Amazon ECS. Procure as configurações do PidMode com um valor de host, que compartilharia os namespaces de ID do processo com o host. Remova as configurações PIDMode: host de suas definições de tarefas para garantir que os contêineres sejam executados com o isolamento adequado do namespace.

O serviço Amazon ECS usa uma definição de tarefa configurada com credenciais de texto não criptografado nas variáveis de ambiente.

Os contêineres do Amazon ECS com credenciais de texto não criptografado em variáveis de ambiente expõem informações confidenciais de autenticação que podem ser comprometidas se um invasor obtiver acesso à definição da tarefa, ao ambiente do contêiner ou aos registros do contêiner. Isso cria um risco de segurança significativo, pois as credenciais vazadas podem ser usadas para acessar outros AWS serviços ou recursos.

Substitua as credenciais de texto não criptografado

Na descoberta de exposição, identifique a definição da tarefa com credenciais de texto não criptografado. Abra a definição da tarefa no console do Amazon ECS. Procure variáveis de ambiente na definição do contêiner que contenham valores confidenciais, como chaves de AWS acesso, senhas de banco de dados ou tokens de API.

Considere as seguintes alternativas para passar as credenciais:

- Em vez de usar chaves de AWS acesso, use funções de execução de tarefas e funções de tarefas do IAM para conceder permissões aos seus contêineres.
- Armazene as credenciais como AWS segredos no Secrets Manager e faça referência a elas na definição de sua tarefa.

Atualizar definições de tarefa

Crie uma nova revisão da definição de sua tarefa que gerencie com segurança as credenciais. Em seguida, atualize seu serviço Amazon ECS para usar a nova revisão da definição de tarefas.

O serviço Amazon ECS tem um grupo de segurança aberto

Grupos de segurança atuam como firewalls virtuais para suas tarefas do Amazon ECS para controlar o tráfego de entrada e saída. Grupos de segurança abertos, que permitem acesso irrestrito de qualquer endereço IP, podem expor seus contêineres ao acesso não autorizado, aumentando o risco de exposição a ferramentas de verificação automatizadas e ataques direcionados. Seguindo os princípios de segurança padrão, AWS recomenda restringir o acesso do grupo de segurança a endereços IP e portas específicos.

Revise as regras do grupo de segurança e avalie a configuração atual

Abra o recurso para o Amazon ECS Security Group. Avalie quais portas estão abertas e acessíveis a partir de amplos intervalos de IP, como`(0.0.0.0/0 or ::/0)`.

Modificar as regras do grupo de segurança

Modifique suas regras de grupo de segurança para restringir o acesso a intervalos ou endereços IP confiáveis específicos. Ao atualizar suas regras de grupo de segurança, considere separar os requisitos de acesso para diferentes segmentos de rede criando regras para cada intervalo de IP de origem necessário ou restringindo o acesso a portas específicas.

Modificar as regras do grupo de segurança

Considere as seguintes opções para métodos alternativos de acesso:

- O Session Manager fornece acesso seguro ao shell às suas EC2 instâncias da Amazon sem a necessidade de portas de entrada, gerenciamento de chaves SSH ou manutenção de bastion hosts.
- NACLs fornecem uma camada adicional de segurança no nível da sub-rede. Diferentemente dos grupos de segurança, não NACLs têm estado e exigem que as regras de entrada e saída sejam definidas explicitamente.

O serviço Amazon ECS tem endereços IP públicos

Os serviços do Amazon ECS com endereços IP públicos atribuídos às suas tarefas podem ser acessados diretamente pela Internet. Embora isso possa ser necessário para serviços que precisam estar disponíveis publicamente, aumenta a superfície de ataque e o potencial de acesso não autorizado.

Identifique serviços com endereços IP públicos

Na descoberta de exposição, identifique o serviço Amazon ECS que tem endereços IP públicos atribuídos às suas tarefas. Procure a `assignPublicIp` configuração com um valor de `ENABLED` na configuração do serviço.

Atualizar definições de tarefa

Crie uma nova revisão da definição de sua tarefa que desabilite endereços IP públicos. Em seguida, atualize seu serviço Amazon ECS para usar a nova revisão da definição de tarefas.

Implemente padrões de acesso à rede privada

Para instâncias que estão executando aplicativos web, considere usar um Load Balancer (LB). LBs pode ser configurado para permitir que suas instâncias sejam executadas em sub-redes privadas enquanto o LB é executado em uma sub-rede pública e gerencia o tráfego da Internet.

O serviço Amazon ECS usa uma definição de tarefa que é configurada com o modo de rede do host ativado.

Os contêineres do Amazon ECS executados no modo de rede do host compartilham o namespace da rede com o host, permitindo acesso direto às interfaces de rede, portas e tabelas de roteamento do host. Essa configuração ignora o isolamento de rede fornecido pelos contêineres, potencialmente expondo os serviços executados no contêiner diretamente às redes externas e permitindo que os

contêineres modifiquem as configurações da rede do host. Seguindo os princípios de segurança padrão, AWS recomenda manter o isolamento adequado da rede para contêineres.

Desativar o modo de rede do host

Na descoberta de exposição, identifique a definição da tarefa com o modo de rede do host. Abra a definição da tarefa no console do Amazon ECS. Procure a configuração NetworkMode com um valor de host na definição da tarefa.

Considere as seguintes opções para desativar o modo de rede do host:

- O modo `awsvpc` de rede fornece o nível mais forte de isolamento de rede, dando a cada tarefa sua própria interface de rede elástica.
- O modo `bridge` de rede fornece isolamento enquanto permite mapeamentos de portas para expor portas específicas de contêineres ao host.

Atualizar definições de tarefa

Crie uma nova revisão da definição de sua tarefa com a configuração atualizada do modo de rede. Em seguida, atualize seu serviço Amazon ECS para usar a nova revisão da definição de tarefas.

A função do IAM associada ao serviço Amazon ECS tem uma política de acesso administrativo

As funções do IAM com políticas de acesso administrativo anexadas às tarefas do Amazon ECS fornecem amplas permissões que excedem o que normalmente é necessário para a operação de contêineres. Essa configuração aumenta o risco de que um contêiner comprometido possa ser usado para acessar ou modificar recursos em todo o AWS ambiente. Seguindo os princípios de segurança padrão, AWS recomenda implementar o acesso com privilégios mínimos concedendo somente as permissões necessárias para que uma tarefa funcione.

Revise e identifique políticas administrativas

Na ID do recurso, identifique o nome da função do IAM. Acesse o painel do IAM e selecione a função identificada. Analise a política de permissões anexada à função do IAM. Se a política for uma política AWS gerenciada, procure`AdministratorAccess`. Caso contrário, no documento de política, procure declarações que tenham as declarações `"Effect": "Allow", "Action": "*", and "Resource": "*"` juntas.

Implemente o acesso de privilégio mínimo

Substitua as políticas administrativas por aquelas que concedem somente as permissões específicas necessárias para o funcionamento da instância. Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Como alternativa, você pode criar uma nova função do IAM para evitar o impacto de outros aplicativos que estão usando a função existente. Nesse cenário, crie uma nova função do IAM e associe a nova função do IAM à instância.

Considerações sobre configuração segura

Se forem necessárias permissões administrativas em nível de serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

- O MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas.
- A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA.

Atualizar definições de tarefa

Crie uma nova revisão da definição de sua tarefa que faça referência às funções novas ou atualizadas do IAM. Em seguida, atualize seu serviço Amazon ECS para usar a nova revisão da definição de tarefas.

Traços de vulnerabilidade para os serviços do Amazon ECS

Aqui estão as características de acessibilidade do Amazon ECS e as etapas de remediação sugeridas.

O serviço Amazon ECS tem um contêiner com vulnerabilidades de software que podem ser exploradas pela rede e com alta probabilidade de exploração

1. Entenda a exposição

   As descobertas de vulnerabilidade de pacotes identificam pacotes de software em seu AWS ambiente que estão expostos a vulnerabilidades e exposições comuns (). CVEs Os invasores podem explorar essas vulnerabilidades sem correção e comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, ou para acessar outros sistemas. As imagens de contêiner ECR podem conter descobertas de vulnerabilidade de pacotes.

2. Remedie a exposição
   a. Atualizar a versão do pacote

      Analise a descoberta da vulnerabilidade do pacote para sua função Lambda. Atualize a versão do pacote conforme sugerido pelo Amazon Inspector. Para obter informações, consulte Visualização dos detalhes de suas descobertas do Amazon Inspector no Guia do Usuário do Amazon Inspector. A seção Remediação dos detalhes da descoberta no console do Amazon Inspector informa quais comandos você pode executar para atualizar o pacote.

   b. Atualizar imagens básicas do contêiner

      Reconstrua e atualize as imagens básicas do contêiner regularmente para manter seus contêineres atualizados. Ao reconstruir a imagem, não inclua componentes desnecessários para reduzir a superfície de ataque. Para obter instruções sobre como reconstruir uma imagem de contêiner, consulte Reconstruir suas imagens com frequência.

O serviço Amazon ECS tem um contêiner com vulnerabilidades de software

Pacotes de software instalados nos contêineres do Amazon ECS podem ser expostos a vulnerabilidades e exposições comuns (). CVEs Vulnerabilidades de baixa prioridade representam pontos fracos de segurança com menor gravidade ou capacidade de exploração em comparação com vulnerabilidades de alta prioridade. Embora essas vulnerabilidades representem menos riscos imediatos, os invasores ainda podem explorar essas vulnerabilidades não corrigidas para comprometer a confidencialidade, a integridade ou a disponibilidade dos dados ou acessar outros sistemas.

Atualizar imagens de contêiner afetadas

Revise a seção Referências na guia Vulnerabilidade da característica. A documentação do fornecedor pode incluir orientações específicas de remediação.

Aplique a remediação apropriada seguindo estas diretrizes gerais:

- Atualize suas imagens de contêiner para usar versões corrigidas dos pacotes afetados.
- Atualize as dependências afetadas em seu aplicativo para as versões seguras mais recentes.

Depois de atualizar a imagem do contêiner, envie-a para o registro do contêiner e atualize a definição da tarefa do Amazon ECS para usar a nova imagem.

Considerações futuras

Para fortalecer ainda mais a postura de segurança de suas imagens de contêiner, considere seguir as melhores práticas de segurança de tarefas e contêineres do Amazon ECS. O Amazon Inspector pode ser configurado para digitalizar automaticamente CVEs em seus contêineres. O Amazon Inspector também pode ser integrado ao Security Hub para remediações automáticas. Considere implementar um cronograma regular de patches usando o Systems Manager Maintenance Windows para minimizar a interrupção em seus contêineres.

Correção de exposições para clusters do Amazon EKS

AWS O Security Hub pode gerar descobertas de exposição para clusters do Amazon Elastic Kubernetes Service (Amazon EKS).

O cluster Amazon EKS envolvido em uma descoberta de exposição e suas informações de identificação estão listados na seção Recursos dos detalhes da descoberta. Você pode recuperar esses detalhes do recurso no console do Security Hub ou programaticamente com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

  - O cluster Amazon EKS usa segredos não criptografados do Kubernetes
- Traços de vulnerabilidade para clusters do Amazon EKS
  - O cluster Amazon EKS tem um contêiner com vulnerabilidades de software exploráveis em rede com alta probabilidade de exploração
  - O cluster Amazon EKS tem um contêiner com vulnerabilidades de software

Características de configuração incorreta para clusters Amazon EKS

Aqui estão as características de configuração incorreta dos clusters do Amazon EKS e as etapas de correção sugeridas.

O cluster Amazon EKS permite acesso público

O endpoint do cluster Amazon EKS é o endpoint que você usa para se comunicar com o servidor da API Kubernetes do seu cluster. Por padrão, esse endpoint é público na Internet. Os endpoints públicos aumentam sua área de superfície de ataque e o risco de acesso não autorizado ao servidor da API Kubernetes, potencialmente permitindo que invasores acessem ou modifiquem recursos do cluster ou acessem dados confidenciais. Seguindo as melhores práticas de segurança, AWS recomenda restringir o acesso ao endpoint do cluster EKS somente aos intervalos de IP necessários.

Modificar o acesso ao endpoint

Na descoberta de exposição, abra o recurso. Isso abrirá o cluster Amazon EKS afetado. Você pode configurar seu cluster para usar acesso privado, acesso público ou ambos. Com o acesso privado, as solicitações da API Kubernetes que se originam na VPC do seu cluster usam o VPC endpoint privado. Com acesso público, as solicitações da API Kubernetes que se originam de fora da VPC do seu cluster usam o endpoint público.

Modificar ou remover o acesso público ao cluster

Para modificar o acesso ao endpoint para um cluster existente, consulte Modificar o acesso ao endpoint do cluster no Guia do usuário do Amazon Elastic Kubernetes Service. Implemente regras mais restritivas com base em intervalos de IP ou grupos de segurança específicos. Se for necessário acesso público limitado, restrinja o acesso a intervalos de blocos CIDR específicos ou use listas de prefixos.

O cluster Amazon EKS usa uma versão incompatível do Kubernetes

O Amazon EKS oferece suporte a cada versão do Kubernetes por um período limitado de tempo. A execução de clusters com versões incompatíveis do Kubernetes pode expor seu ambiente a

vulnerabilidades de segurança, pois os patches do CVE deixarão de ser lançados para versões desatualizadas. As versões não suportadas podem conter vulnerabilidades de segurança conhecidas que podem ser exploradas por invasores e não ter recursos de segurança que possam estar disponíveis em versões mais recentes. Seguindo as melhores práticas de segurança, AWS recomenda manter sua versão do Kubernetes atualizada.

Atualizar a versão do Kubernetes

Na descoberta de exposição, abra o recurso. Isso abrirá o cluster Amazon EKS afetado. Antes de atualizar seu cluster, consulte as versões disponíveis sobre suporte padrão no Guia do usuário do Amazon Elastic Kubernetes Service para obter uma lista das versões atualmente suportadas do Kubernetes.

O cluster Amazon EKS usa segredos não criptografados do Kubernetes

Por padrão, os segredos do Kubernetes são armazenados sem criptografia no armazenamento de dados subjacente (etcd) do servidor de API. Qualquer pessoa com acesso à API ou com acesso ao etcd pode recuperar ou modificar um segredo. Para evitar isso, você deve criptografar os segredos do Kubernetes em repouso. Se os segredos do Kubernetes não forem criptografados, eles estarão vulneráveis ao acesso não autorizado se o etcd for comprometido. Como os segredos geralmente contêm informações confidenciais, como senhas e tokens de API, sua exposição pode levar ao acesso não autorizado a outros aplicativos e dados. Seguindo as melhores práticas de segurança, AWS recomenda criptografar todas as informações confidenciais armazenadas nos segredos do Kubernetes.

Criptografe segredos do Kubernetes

O Amazon EKS oferece suporte à criptografia de segredos do Kubernetes usando chaves KMS por meio da criptografia de envelope. Para habilitar a criptografia de segredos do Kubernetes para seu cluster EKS, consulte Criptografar segredos do Kubernetes com o KMS em clusters existentes no Guia do usuário do Amazon EKS.

Traços de vulnerabilidade para clusters do Amazon EKS

Aqui estão as características de vulnerabilidade dos clusters Amazon EKS.

O cluster Amazon EKS tem um contêiner com vulnerabilidades de software exploráveis em rede com alta probabilidade de exploração

Pacotes de software instalados em clusters EKS podem ser expostos a vulnerabilidades e exposições comuns (). CVEs Os críticos CVEs representam riscos de segurança significativos para

seu AWS ambiente. Usuários não autorizados podem explorar essas vulnerabilidades não corrigidas para comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, ou para acessar outros sistemas. Vulnerabilidades críticas com alta probabilidade de exploração representam ameaças imediatas à segurança, pois o código de exploração pode já estar disponível publicamente e ser usado ativamente por invasores ou por ferramentas de verificação automatizadas. Seguindo as melhores práticas de segurança, AWS recomenda corrigir essas vulnerabilidades para proteger sua instância contra ataques.

Atualizar instâncias afetadas

Atualize suas imagens de contêiner para versões mais recentes que incluam correções de segurança para as vulnerabilidades identificadas. Isso normalmente envolve reconstruir suas imagens de contêiner com imagens básicas ou dependências atualizadas e, em seguida, implantar as novas imagens em seu cluster Amazon EKS.

O cluster Amazon EKS tem um contêiner com vulnerabilidades de software

Os pacotes de software instalados nos clusters do Amazon EKS podem ser expostos a vulnerabilidades e exposições comuns (). CVEs Os não críticos CVEs representam pontos fracos de segurança com menor gravidade ou capacidade de exploração em comparação com os críticos. CVEs Embora essas vulnerabilidades representem menos riscos imediatos, os invasores ainda podem explorar essas vulnerabilidades não corrigidas para comprometer a confidencialidade, a integridade ou a disponibilidade dos dados ou acessar outros sistemas. Seguindo as melhores práticas de segurança, AWS recomenda corrigir essas vulnerabilidades para proteger sua instância contra ataques.

Atualizar instâncias afetadas

Atualize suas imagens de contêiner para versões mais recentes que incluam correções de segurança para as vulnerabilidades identificadas. Isso normalmente envolve reconstruir suas imagens de contêiner com imagens básicas ou dependências atualizadas e, em seguida, implantar as novas imagens em seu cluster Amazon EKS.

Correção de exposições para usuários do IAM

AWS O Security Hub pode gerar descobertas de exposição para usuários AWS Identity and Access Management (IAM).

No console do Security Hub, o usuário do IAM envolvido em uma descoberta de exposição e suas informações de identificação estão listados na seção Recursos dos detalhes da descoberta.

Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

As melhores práticas do IAM recomendam que você crie funções do IAM ou use a federação com um provedor de identidade para acessar AWS usando credenciais temporárias em vez de criar usuários individuais do IAM. Se essa for uma opção para sua organização e caso de uso, recomendamos mudar para funções ou federação em vez de usar usuários do IAM. Para obter mais informações, consulte Usuários IAM no Manual do usuário IAM.

Sumário

Características de configuração incorreta para usuários do IAM

Aqui estão as características de configuração incorreta para usuários do IAM e as etapas de correção sugeridas.

O usuário do IAM tem uma política com acesso administrativo

As políticas do IAM concedem um conjunto de privilégios aos usuários do IAM ao acessar recursos. As políticas administrativas fornecem aos usuários do IAM amplas permissões para AWS serviços e recursos. Fornecer privilégios administrativos completos, em vez do conjunto mínimo de permissões que o usuário precisa, pode aumentar o escopo de um ataque se as credenciais forem comprometidas. Seguindo os princípios de segurança padrão, AWS recomenda que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

1. Revise e identifique políticas administrativas — No Resource ID, identifique o nome da função do IAM. Acesse o painel do IAM e selecione a função identificada. Analise a política de permissões anexada ao usuário do IAM. Se a política for AWS gerenciada, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações que tenham as declarações `"Effect": "Allow" "Action": "*"` terminadas`"Resource": "*"`.
2. Implemente o acesso com privilégios mínimos — substitua as políticas administrativas do serviço por aquelas que concedem somente as permissões específicas necessárias para que o usuário funcione. Para obter mais informações sobre as melhores práticas de segurança para políticas do IAM, consulte Aplicar permissões de privilégios mínimos no Guia do usuário.AWS Identity and Access Management Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário.
3. Considerações de configuração segura — Se as permissões administrativas do serviço forem necessárias para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:
   - Autenticação multifatorial (MFA) — A MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas. Para obter mais informações, consulte Exigir autenticação multifator (MFA) no Guia AWS Identity and Access Management do usuário.
   - Condições do IAM — A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de

origem ou idade da MFA. Para obter mais informações, consulte Condições de uso nas políticas do IAM para restringir ainda mais o acesso no Guia AWS Identity and Access Management do usuário.

- Limites de permissão — Os limites de permissão estabelecem o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo. Para obter mais informações, consulte Usar limites de permissões para delegar o gerenciamento de permissões em uma conta no Guia do AWS Identity and Access Management usuário.

O usuário do IAM não tem o MFA habilitado

A autenticação multifator (MFA) adiciona uma camada extra de proteção sobre um nome de usuário e senha. Quando a MFA é ativada e um usuário do IAM faz login em um AWS site, ele é solicitado a fornecer seu nome de usuário, senha e um código de autenticação do dispositivo de AWS MFA. O principal de autenticação deve conter um dispositivo que emite uma chave sensível ao tempo e deve ter conhecimento de uma credencial. Sem o MFA, se a senha de um usuário for comprometida, o invasor terá acesso total às permissões do usuário. AWS Seguindo os princípios de segurança padrão, AWS recomenda habilitar a MFA para todas as contas e usuários que tenham AWS Management Console acesso.

Analise os tipos de MFA

AWS suporta os seguintes tipos de MFA:

- Chaves de acesso e chaves de segurança
- Aplicações de autenticador virtual
- Tokens físicos de TOTP

Embora a autenticação com um dispositivo físico normalmente forneça uma proteção de segurança mais rigorosa, usar qualquer tipo de MFA é mais seguro do que ter a MFA desativada.

Habilitar MFA

Para habilitar o tipo de MFA adequado às suas necessidades, consulte a autenticação AWS multifator no IAM no Guia do usuário do IAM. Siga as etapas do tipo específico de MFA que você deseja implementar. Para organizações que gerenciam muitos usuários, talvez você queira impor o uso da MFA exigindo que a MFA acesse recursos confidenciais.

O usuário do IAM tem uma política com acesso administrativo a um AWS service (Serviço da AWS)

As políticas de administração de serviços fornecem aos usuários do IAM permissões para realizar todas as ações em um AWS serviço específico. Essas políticas geralmente incluem permissões que não são necessárias para que os usuários desempenhem suas funções de trabalho. Fornecer a um usuário do IAM privilégios de administrador do serviço, em vez do conjunto mínimo de permissões necessário, aumenta o escopo de um ataque se as credenciais forem comprometidas. Seguindo os princípios de segurança padrão, AWS recomenda que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

Revise e identifique as políticas de administração de serviços

No ID do recurso, identifique o nome da função do IAM. Acesse o painel do IAM e selecione a função identificada. Analise a política de permissões anexada ao usuário do IAM. Se a política for gerenciada pela AWS, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações que tenham as declarações `"Effect": "Allow" with "Action": "*" over "Resource": "*"`.

Implemente o acesso de privilégio mínimo

Substitua as políticas administrativas do serviço por aquelas que concedem somente as permissões específicas necessárias para que o usuário funcione. Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso.

Considerações sobre configuração segura

Se forem necessárias permissões administrativas do serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir a exposição:

- O MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas.
- Use elementos condicionais para restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA.
- Use limites de permissão para estabelecer o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo.

A AWS conta do usuário do IAM tem políticas de senha fracas

As políticas de senha ajudam a proteger contra acesso não autorizado ao impor requisitos mínimos de complexidade para senhas de usuário do IAM. Sem políticas de senha fortes, há um risco maior de que as contas dos usuários sejam comprometidas por meio de adivinhação de senhas ou ataques de força bruta. Seguindo os princípios de segurança padrão, AWS recomenda a implementação de uma política de senha forte para garantir que os usuários criem senhas complexas e difíceis de adivinhar.

Configurar uma política de senha forte

Acesse o painel do IAM e navegue até Configurações da conta. Revise as configurações atuais da política de senha da sua conta, incluindo o tamanho mínimo, os tipos de caracteres necessários e as configurações de expiração da senha.

No mínimo, AWS recomenda seguir estas práticas recomendadas ao definir sua política de senha:

- Exigir pelo menos um caractere maiúsculo.
- Exigir pelo menos um caractere minúsculo.
- Exija pelo menos um símbolo.
- Exija pelo menos um número.
- Exigir pelo menos oito caracteres.

Considerações adicionais sobre segurança

Considere estas medidas de segurança adicionais, além de uma política de senha forte:

- O MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas.
- Configurar elementos condicionais para restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA.

O usuário do IAM tem credenciais não utilizadas

Credenciais não utilizadas, incluindo senhas e chaves de acesso que permaneceram inativas por 90 dias ou mais, representam um risco de segurança para seu ambiente. AWS Essas credenciais

não utilizadas criam possíveis vetores de ataque para os atacantes e aumentam a superfície geral de ataque da sua organização. Seguindo as melhores práticas de segurança, AWS recomenda desativar ou remover credenciais que não tenham sido usadas em 90 dias ou mais para reduzir sua superfície de ataque.

Desativar ou remover credenciais não utilizadas

Na descoberta de exposição, abra o recurso. Isso abrirá a janela de detalhes do usuário. Antes de agir com as credenciais não utilizadas, avalie o impacto potencial em seu ambiente. A remoção de credenciais sem uma avaliação adequada pode interromper processos em segundo plano, trabalhos agendados e muito mais. Considere um breve período de desativação antes da remoção permanente para verificar o impacto da remoção das credenciais não utilizadas.

Execute a ação apropriada com base no tipo de credencial:

- Para senhas de console não utilizadas, considere primeiro alterar a senha e desativá-la temporariamente. Se nenhum problema surgir, prossiga com a desativação ou exclusão permanente.
- Para chaves de acesso não utilizadas, considere primeiro desativar a chave. Depois de confirmar que nenhum sistema foi afetado, prossiga com a desativação ou exclusão permanente.
- Para usuários não utilizados, considere desativar temporariamente o usuário anexando uma política restritiva antes da exclusão total.

O usuário do IAM tem chaves de acesso não rotacionadas

As chaves de acesso consistem em um ID de chave de acesso e uma chave de acesso secreta que permitem o acesso programático aos AWS recursos. Quando as chaves de acesso permanecem inalteradas por longos períodos de tempo, elas aumentam o risco de acesso não autorizado se forem comprometidas. Seguindo as melhores práticas de segurança, AWS recomenda a rotação das chaves de acesso a cada 90 dias para minimizar a janela de oportunidade para os invasores usarem credenciais comprometidas.

Gire as teclas de acesso

Na descoberta de exposição, abra o recurso. Isso abrirá a janela de detalhes do usuário. Para alternar as chaves de acesso, consulte Gerenciar chaves de acesso para usuários do IAM no Guia do usuário do IAM.

O usuário do IAM tem uma política que permite acesso irrestrito à decodificação da chave KMS

AWS KMS permite criar e gerenciar chaves criptográficas que são usadas para proteger seus dados. As políticas do IAM que permitem permissões de AWS KMS descriptografia irrestritas (por exemplo, `kms:Decrypt` ou`kms:ReEncryptFrom`) em todas as chaves do KMS podem levar ao acesso não autorizado aos dados se as credenciais de um usuário do IAM forem comprometidas. Se um invasor obtiver acesso a essas credenciais, ele poderá decifrar quaisquer dados criptografados em seu ambiente, o que pode incluir dados confidenciais. Seguindo as melhores práticas de segurança, AWS recomenda implementar o privilégio mínimo limitando as permissões de AWS KMS descriptografia somente às chaves específicas de que os usuários precisam para suas funções de trabalho.

Implemente o privilégio de acesso mínimo

Na descoberta de exposição, abra o recurso. Isso abrirá a janela de políticas do IAM. Procure permissões no KMS que permitam kms: Decrypt `kms:ReEncryptFrom` ou `KMS:*` com uma especificação de recurso de. `"*"` Atualize a política para restringir as permissões AWS KMS de decodificação somente às chaves específicas necessárias. Modifique a política para substituir o `"*"` recurso pelas AWS KMS chaves específicas ARNs necessárias.

Considerações sobre configuração segura

Considere adicionar condições para restringir ainda mais quando essas permissões podem ser usadas. Por exemplo, você pode limitar as operações de descriptografia a endpoints de VPC específicos ou intervalos de IP de origem. Você também pode configurar políticas de chaves para restringir ainda mais quem pode usar chaves KMS específicas.

Correção de exposições para funções Lambda

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

AWS O Security Hub pode gerar descobertas de exposição para AWS Lambda funções (Lambda).

No console do Security Hub, a função Lambda envolvida em uma descoberta de exposição e suas informações de identificação estão listadas na seção Recursos dos detalhes da descoberta. Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

- A função Lambda tem vulnerabilidades de software

Características de configuração incorreta para funções Lambda

Aqui estão as características de configuração incorreta das funções do Lambda e as etapas de correção sugeridas.

A função Lambda está executando um tempo de execução não suportado

O Lambda permite que os desenvolvedores executem código sem provisionar ou gerenciar servidores por meio de tempos de execução que executam seu código em um ambiente gerenciado. O Lambda aplica automaticamente patches e atualizações de segurança aos tempos de execução gerenciados e às imagens de base de contêineres correspondentes. Quando uma versão em tempo de execução não é mais suportada, ela não recebe mais atualizações de segurança, correções de bugs ou suporte técnico. Funções executadas em tempos de execução obsoletos podem ter vulnerabilidades de segurança e, eventualmente, parar de funcionar devido a problemas como a expiração do certificado. Além disso, tempos de execução sem suporte podem ser vulneráveis a falhas de segurança recém-descobertas sem os patches disponíveis. Seguindo as melhores práticas de segurança, recomendamos o uso de tempos de execução corrigidos e compatíveis para funções do Lambda.

Tempo de execução da função de atualização

Na guia Recursos da exposição, abra o recurso com o hiperlink. Isso abrirá a janela da função Lambda. Para atualizar sua função para um tempo de execução compatível, configure a configuração de gerenciamento de tempo de execução. Você pode optar por atualizar automaticamente sua função para a versão de tempo de execução mais recente, mas antes de selecionar essa opção, avalie se as atualizações automáticas podem afetar seus aplicativos em execução. Para obter mais informações, consulte Entendendo como o Lambda gerencia as atualizações da versão em tempo de execução.

A função Lambda é implantada fora de uma Amazon VPC

Por padrão, as funções Lambda são implantadas com acesso à Internet pública. Essa configuração padrão dá às funções do Lambda a capacidade de alcançar pontos finais AWS de serviço e externos APIs, mas também as expõe a possíveis riscos de segurança. Funções com acesso à Internet podem ser usadas para exfiltrar dados, comunicar-se com servidores não autorizados ou se tornar pontos de entrada para agentes externos, se comprometidas. A Amazon VPC fornece isolamento de rede ao restringir suas funções Lambda para se comunicarem somente com recursos dentro de sua

rede privada definida. Seguindo os princípios de segurança padrão, recomendamos a implantação de funções Lambda em uma VPC para melhorar a segurança por meio do isolamento da rede.

Anexar função ao VPC

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a janela da função Lambda. Para proteger sua função Lambda restringindo o acesso à rede, conecte-a a uma VPC que tenha os controles de rede apropriados. Antes de anexar sua função a uma VPC, planeje AWS qualquer acesso de serviço necessário, pois funções em sub-redes privadas sem gateways NAT ou endpoints de VPC não conseguirão acessar o serviço. AWS APIs Para obter informações sobre como anexar uma função Lambda a uma Amazon VPC em sua conta, consulte Anexar funções do Lambda a uma Amazon VPC no seu. Conta da AWS Considere usar VPC endpoints para conectividade de serviços sem acesso à Internet se sua função precisar acessar AWS serviços de dentro de uma sub-rede privada. Configure um gateway NAT se você precisar de conectividade de saída com a Internet a partir de sub-redes privadas.

A função Lambda é capaz de assumir uma função do IAM

As funções Lambda usam funções do IAM para interagir com AWS os serviços. Essas funções concedem permissões para a função Lambda acessar AWS recursos durante a execução. Embora essas funções às vezes sejam necessárias para que as funções do Lambda executem suas tarefas, elas devem seguir o princípio do privilégio mínimo. Seguindo os princípios de segurança padrão, AWS recomenda que você verifique se as permissões associadas à função são apropriadas com base na funcionalidade pretendida da função.

1. Determine se a função IAM anexada é necessária

   Determine se a função Lambda exige que uma função de execução do IAM seja configurada. A maioria das funções do Lambda precisa de permissões básicas para operar, como gravar registros em. CloudWatch Analise as permissões associadas à função de execução da função e determine se a função do IAM é necessária para a função. Para obter informações sobre as funções de execução do Lambda, consulte Definição de permissões da função Lambda com uma função de execução no Guia do desenvolvedor.AWS Lambda
2. Implemente o acesso de privilégio mínimo

   Substitua políticas excessivamente permissivas por aquelas que concedem somente as permissões específicas necessárias para que a função funcione. Para obter informações sobre as melhores práticas de segurança para funções do IAM, consulte Aplicar permissões de privilégios mínimos no Guia do usuário.AWS Identity and Access Management Para identificar permissões

desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário. Como alternativa, você pode criar uma nova função do IAM para evitar o impacto de outras funções do Lambda que estão usando a função existente. Nesse cenário, crie uma nova função do IAM e associe a nova função do IAM à instância. Para obter instruções sobre como substituir uma função do IAM por uma função, consulte Atualizar a função de execução de uma função no Guia do AWS Lambda desenvolvedor.

A função do IAM associada à função Lambda tem uma política de acesso administrativo

As políticas de acesso administrativo fornecem às funções do Lambda amplas permissões para AWS serviços e recursos. Essas políticas geralmente incluem permissões que não são necessárias para a funcionalidade. Fornecer uma identidade do IAM com uma política de acesso administrativo em uma função Lambda, em vez do conjunto mínimo de permissões que a função de execução precisa, pode aumentar o escopo de um ataque se a função for comprometida. Seguindo os princípios de segurança padrão, AWS recomenda que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

1. Revise e identifique políticas administrativas

   Na descoberta de exposição, identifique o nome da função. Acesse o painel do IAM e encontre a função com o nome da função identificado anteriormente. Analise a política de permissões anexada à função do IAM. Se a política for AWS gerenciada, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações que contenham as declarações `"Effect": "Allow", "Action": "*"` e `"Resource": "*"` juntas.

2. Implemente o acesso de privilégio mínimo

   Substitua as políticas administrativas por aquelas que concedem somente as permissões específicas necessárias para que a função funcione. Para obter mais informações sobre as melhores práticas de segurança para funções do IAM, consulte Aplicar permissões de privilégios mínimos no Guia do usuário.AWS Identity and Access Management Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário. Como alternativa, você pode criar uma nova função do IAM para evitar o impacto de outras funções do

Lambda usando a função existente. Nesse cenário, crie uma nova função do IAM. Em seguida, associe a nova função à instância. Para obter informações sobre a substituição de uma função do IAM por uma função, consulte Atualizar a função de execução de uma função no Guia do AWS Lambda desenvolvedor.

3. Considerações sobre configuração segura

   Se forem necessárias permissões de acesso administrativo para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

   - Autenticação multifatorial (MFA) — A MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas. Para obter mais informações, consulte Exigir autenticação multifator (MFA) no Guia AWS Identity and Access Management do usuário.
   - Condições do IAM — A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA. Para obter mais informações, consulte Condições de uso nas políticas do IAM para restringir ainda mais o acesso no Guia do usuário do IAM.
   - Limites de permissão — Os limites de permissão estabelecem o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo. Para obter mais informações, consulte Usar limites de permissões para delegar o gerenciamento de permissões em uma conta no Guia do AWS Identity and Access Management usuário.

A função do IAM associada à função Lambda tem uma política com acesso administrativo a um serviço AWS

As políticas de administração de serviços permitem que as funções do Lambda executem todas as ações em um serviço específico AWS . Essas políticas normalmente concedem mais permissões do que o necessário para a operação de uma função. Se uma função Lambda com uma política de administração de serviços for comprometida, um invasor poderá usar essas permissões para potencialmente acessar ou modificar dados ou serviços confidenciais em seu ambiente. AWS Seguindo os princípios de segurança padrão, recomendamos que você conceda o mínimo de privilégios, o que significa que você concede somente as permissões necessárias para realizar uma tarefa.

1. Revise e identifique políticas administrativas

   Na descoberta de exposição, identifique o nome da função no ARN. Acesse o painel do IAM e encontre o nome da função. Revise a política de permissões anexada à função. Se a política

for AWS gerenciada, procure `AdministratorAccess` ou`IAMFullAccess`. Caso contrário, no documento de política, procure declarações que contenham as declarações `"Effect": "Allow", "Action": "*"` `"Resource": "*"` e.

2. Implemente o acesso de privilégio mínimo

   Substitua as políticas administrativas por aquelas que concedem somente as permissões específicas necessárias para que a função funcione. Para obter mais informações, consulte Aplique permissões de privilégio mínimo, no Guia do usuário do AWS Identity and Access Management . Para identificar permissões desnecessárias, você pode usar o IAM Access Analyzer para entender como modificar sua política com base no histórico de acesso. Para obter mais informações, consulte Conclusões sobre acesso externo e não utilizado no Guia do AWS Identity and Access Management usuário. Como alternativa, você pode criar uma nova função do IAM para evitar o impacto de outras funções do Lambda que estão usando a função existente. Nesse cenário, crie uma nova função do IAM e associe a nova função do IAM à instância. Para obter instruções sobre como substituir uma função do IAM por uma função, consulte Atualizar a função de execução de uma função no Guia do AWS Lambda desenvolvedor.

3. Considerações sobre configuração segura

   Se forem necessárias permissões administrativas em nível de serviço para a instância, considere implementar esses controles de segurança adicionais para reduzir os riscos:

   - Autenticação multifatorial (MFA) — A MFA adiciona uma camada de segurança adicional ao exigir uma forma adicional de autenticação. Isso ajuda a evitar o acesso não autorizado, mesmo que as credenciais estejam comprometidas. Para obter mais informações, consulte Exigir autenticação multifator (MFA) no Guia AWS Identity and Access Management do usuário.
   - Condições do IAM — A configuração de elementos condicionais permite restringir quando e como as permissões administrativas podem ser usadas com base em fatores como IP de origem ou idade da MFA. Para obter mais informações, consulte Condições de uso nas políticas do IAM para restringir ainda mais o acesso no Guia AWS Identity and Access Management do usuário.
   - Limites de permissões — Os limites de permissão estabelecem o máximo de permissões que uma função pode ter, fornecendo proteções para funções com acesso administrativo. Para obter mais informações, consulte Usar limites de permissões para delegar o gerenciamento de permissões no Guia do AWS Identity and Access Management usuário.

Características de acessibilidade para funções Lambda

Aqui estão as características de acessibilidade das funções Lambda e as etapas de remediação sugeridas.

A função Lambda pode ser invocada publicamente

As políticas baseadas em recursos do Lambda determinam quem pode invocar suas funções. Uma função com uma política de recursos que inclui "*" como principal (ou nenhum principal) permite que qualquer AWS usuário autenticado a invoque. Isso cria um risco significativo, especialmente para funções que processam dados confidenciais, modificam recursos ou têm permissões elevadas. Usuários não autorizados podem explorar essa configuração para realizar operações indesejadas, potencialmente expondo dados, manipulando recursos ou abusando dos recursos da função. Seguindo as melhores práticas de segurança, recomendamos restringir o acesso à função Lambda somente aos diretores autorizados.

Modificar a política baseada em recursos da função

Na guia Recursos da exposição, abra o recurso com o hiperlink. Isso abrirá a janela da função Lambda. Restrinja o acesso à sua função Lambda especificando somente uma AWS conta autorizada IDs ou diretores específicos do IAM (usuários, funções ou serviços) na política baseada em recursos. Você só pode modificar as políticas baseadas em recursos de forma programática.

Traços de vulnerabilidade para funções Lambda

Aqui estão as características de vulnerabilidade das funções Lambda e as etapas de correção sugeridas.

A função Lambda tem vulnerabilidades de software que podem ser exploradas pela rede

Os pacotes de software usados no código da função Lambda podem conter vulnerabilidades e exposições comuns (CVEs) que têm uma grande chance de serem exploradas. Os críticos CVEs representam riscos de segurança significativos para seu AWS ambiente. Os invasores podem explorar essas vulnerabilidades sem correção e comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, ou para acessar outros sistemas. Vulnerabilidades críticas com alta probabilidade de exploração representam ameaças imediatas à segurança, pois o código de exploração pode já estar disponível publicamente e ser usado ativamente por invasores ou por ferramentas de verificação automatizadas. Seguindo as melhores práticas de segurança, recomendamos corrigir essas vulnerabilidades para proteger sua função contra ataques.

Atualize as funções afetadas

Consulte a seção Referências na guia Vulnerabilidade para ver a característica. A documentação do fornecedor pode incluir orientações específicas de remediação. Atualize as bibliotecas vulneráveis para suas versões seguras mais recentes seguindo os procedimentos recomendados pelo fornecedor. Normalmente, o fluxo de trabalho de remediação depende de você ter implantado o pacote Lambda fazendo o upload de um arquivo zip ou criando uma função Lambda com uma imagem de contêiner. Depois de atualizar as bibliotecas, atualize o código da função Lambda para usar a versão fixa. Depois, implante a versão atualizada.

A função Lambda tem vulnerabilidades de software

As funções Lambda geralmente usam bibliotecas e dependências de terceiros que podem conter vulnerabilidades de segurança com menor gravidade ou capacidade de exploração em comparação com as críticas. CVEs Embora essas vulnerabilidades não críticas possam não ser imediatamente exploráveis, elas ainda representam pontos fracos de segurança que podem ser encadeados a outras vulnerabilidades para comprometer sua função. Com o tempo, também podem surgir novas técnicas de exploração que aumentem o risco dessas vulnerabilidades. Seguindo os princípios de segurança padrão, recomendamos corrigir essas vulnerabilidades para manter um ambiente seguro.

Consulte a seção Referências na guia Vulnerabilidade para ver a característica. A documentação do fornecedor pode incluir orientações específicas de remediação. Atualize as bibliotecas vulneráveis para suas versões seguras mais recentes seguindo os procedimentos recomendados pelo fornecedor. Normalmente, o fluxo de trabalho de remediação depende de você ter implantado o pacote Lambda fazendo o upload de um arquivo zip ou criando uma função Lambda com uma imagem de contêiner. Depois de atualizar as bibliotecas, atualize o código da função Lambda para usar a versão fixa. Depois, implante a versão atualizada.

Correção de exposições para funções do Amazon RDS

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

AWS O Security Hub pode gerar descobertas de exposição para funções do Amazon RDS.

No console do Security Hub, a função do Amazon RDS envolvida em uma descoberta de exposição e suas informações de identificação estão listadas na seção Recursos dos detalhes da descoberta. Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação recomendadas para ajudar a mitigar o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

- A instância de banco de dados Amazon RDS usa a porta padrão para o mecanismo de banco de dados.
- A instância de banco de dados Amazon RDS não é coberta por um plano de backup

Características de configuração incorreta das funções do Amazon RDS

A seguir, descrevemos as características de configuração incorreta e as etapas de correção das funções do Amazon RDS.

A instância de banco de dados Amazon RDS está configurada com acesso público

As instâncias do Amazon RDS com acesso público são potencialmente acessíveis pela Internet por meio de seus endpoints. Embora o acesso público às vezes seja necessário, por exemplo, para a funcionalidade, essa configuração pode ser usada como um potencial vetor de ataque para que usuários não autorizados tentem acessar seu banco de dados. Bancos de dados acessíveis ao público podem ser expostos à varredura de portas, ataques de força bruta e tentativas de exploração. Seguindo os princípios de segurança padrão, recomendamos que você limite a exposição pública dos recursos do seu banco de dados.

1. Modificar configurações de acesso público

   Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Avalie se a instância de banco de dados exige acessibilidade pública com base na arquitetura do seu aplicativo. Para obter mais informações, consulte Configurar o acesso público ou privado no Amazon RDS.

O cluster de banco de dados Amazon RDS tem um snapshot que é compartilhado publicamente

Os instantâneos públicos podem ser acessados por qualquer pessoa Conta da AWS, potencialmente expondo dados confidenciais a usuários não autorizados. Qualquer pessoa Conta da AWS tem permissão para copiar esses instantâneos públicos e criar instâncias de banco de dados a partir deles, o que pode levar a violações de dados ou acesso não autorizado a dados. Seguindo as melhores práticas de segurança, recomendamos restringir o acesso aos seus snapshots do Amazon RDS somente para organizações confiáveis Contas da AWS .

1. Configurar um snapshot do Amazon RDS para acesso privado

Na descoberta de exposição, abra o recurso por meio do hiperlink. Para obter informações sobre como modificar as configurações de compartilhamento de instantâneos, consulte Compartilhamento

de um instantâneo no Guia do usuário do Amazon Aurora. Para obter informações sobre como parar de compartilhar snapshots, consulte Como interromper o compartilhamento de snapshots no Guia do usuário do Amazon Aurora. .

A instância de banco de dados Amazon RDS tem um snapshot que não está criptografado em repouso

Snapshots não criptografados da instância de banco de dados Amazon RDS podem expor dados confidenciais se o acesso não autorizado à camada de armazenamento for obtido. Sem criptografia, os dados em instantâneos poderiam ser expostos por meio de acesso não autorizado. Isso cria um risco de violações de dados e violações de conformidade. Seguindo as melhores práticas de segurança, recomendamos criptografar todos os recursos do banco de dados e seus backups para manter a confidencialidade dos dados.

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá o instantâneo afetado. Você não pode criptografar diretamente um snapshot não criptografado existente. Em vez disso, crie uma cópia criptografada do instantâneo não criptografado. Para obter instruções detalhadas, consulte Cópia de snapshots de cluster de banco de dados e criptografia de recursos do Amazon RDS no Guia do usuário do Amazon Aurora. ..

O cluster de banco de dados Amazon RDS tem um snapshot que não é criptografado em repouso

Os snapshots não criptografados do cluster de banco de dados do Amazon RDS podem expor dados confidenciais se o acesso não autorizado à camada de armazenamento for obtido. Sem criptografia, os dados em instantâneos poderiam ser expostos por meio de acesso não autorizado. Isso cria um risco de violações de dados e violações de conformidade. Seguindo as melhores práticas de segurança, recomendamos criptografar todos os recursos do banco de dados e seus backups para manter a confidencialidade dos dados.

1. Crie uma cópia criptografada do instantâneo

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá o instantâneo afetado. Você não pode criptografar diretamente um snapshot não criptografado existente. Em vez disso, crie uma cópia criptografada do instantâneo não criptografado. Para obter instruções detalhadas, consulte Cópia de snapshots de cluster de banco de dados e criptografia de recursos do Amazon RDS no Guia do usuário do Amazon Aurora. ..

A instância de banco de dados Amazon RDS tem um grupo de segurança aberto

Grupos de segurança atuam como firewalls virtuais para suas instâncias do Amazon RDS para controlar o tráfego de entrada e saída. Grupos de segurança abertos, que permitem acesso irrestrito

a partir de qualquer endereço IP, podem expor suas instâncias de banco de dados a acessos não autorizados e possíveis ataques. Seguindo os princípios de segurança padrão, recomendamos restringir o acesso do grupo de segurança a endereços IP e portas específicos para manter o princípio do menor privilégio.

Revise as regras do grupo de segurança e avalie a configuração atual

Na descoberta da exposição, abra o recurso para o grupo de segurança da instância de banco de dados. Avalie quais portas estão abertas e acessíveis a partir de amplos intervalos de IP, como`(0.0.0.0/0 or ::/0)`. Para obter informações sobre a visualização dos detalhes do grupo de segurança, consulte DescribeSecurityGroupsa Amazon Elastic Compute Cloud API Reference.

Modificar as regras do grupo de segurança

Modifique suas regras de grupo de segurança para restringir o acesso a intervalos ou endereços IP confiáveis específicos. Ao atualizar suas regras de grupo de segurança, considere separar os requisitos de acesso para diferentes segmentos de rede criando regras para cada intervalo de IP de origem necessário ou restringindo o acesso a portas específicas. Para modificar as regras do grupo de segurança, consulte Configurar regras do grupo de segurança no Guia EC2 do usuário da Amazon. Para modificar a porta padrão de uma instância de banco de dados existente do Amazon RDS, consulte Modificar o cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon Aurora.

A instância de banco de dados Amazon RDS tem a autenticação do banco de dados IAM desativada

A autenticação do banco de dados do IAM permite que você se autentique no seu banco de dados do Amazon RDS usando credenciais do IAM em vez de senhas do banco de dados. Isso fornece vários benefícios de segurança, como gerenciamento centralizado de acesso, credenciais temporárias e eliminação do armazenamento de senhas de banco de dados no código do aplicativo. 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. Como resultado, o tráfego de rede de e para a instância do banco de dados é criptografado usando SSL. Sem a autenticação do IAM, os bancos de dados geralmente dependem da autenticação baseada em senha, o que pode levar à reutilização de senhas e senhas fracas. Seguindo as melhores práticas de segurança, recomendamos ativar a autenticação do banco de dados do IAM.

Habilitar a autenticação do banco de dados

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Você pode ativar a autenticação do banco de dados do IAM nas opções do banco

de dados. Para obter mais informações, consulte Habilitar e desabilitar a autenticação do banco de dados do IAM no Guia do usuário do Amazon RDS. Depois de ativar a autenticação do IAM, atualize suas instâncias de banco de dados para usar a autenticação do IAM em vez da autenticação baseada em senha.

A instância de banco de dados Amazon RDS usa o nome de usuário de administrador padrão

Usar nomes de usuário padrão (por exemplo, “admin”, “root”) para instâncias de banco de dados aumenta o risco de segurança, pois elas são amplamente conhecidas e comumente alvo de ataques de força bruta. Os nomes de usuário padrão são previsíveis e facilitam a tentativa de acesso ao seu banco de dados por usuários não autorizados. Com nomes de usuário padrão, os invasores só precisam obter senhas, em vez de precisarem de ambas para obter acesso ao seu banco de dados. Seguindo as melhores práticas de segurança, recomendamos o uso de nomes de usuário de administrador exclusivos para sua instância de banco de dados para aprimorar a segurança por meio da obscuridade e reduzir o risco de tentativas de acesso não autorizado.

Configurar um nome de usuário de administrador exclusivo

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Considere quais regras de frequência de backup, período de retenção e ciclo de vida são melhores para seus aplicativos.

O cluster de banco de dados Amazon RDS usa o nome de usuário de administrador padrão

Usar nomes de usuário padrão (por exemplo, “admin”, “root”) para instâncias de banco de dados aumenta o risco de segurança, pois elas são amplamente conhecidas e comumente alvo de ataques de força bruta. Os nomes de usuário padrão são previsíveis e facilitam a tentativa de acesso ao seu banco de dados por usuários não autorizados. Com nomes de usuário padrão, os invasores só precisam obter senhas, em vez de precisarem de ambas para obter acesso ao seu banco de dados. Seguindo as melhores práticas de segurança, recomendamos o uso de nomes de usuário de administrador exclusivos para sua instância de banco de dados para aprimorar a segurança por meio da obscuridade e reduzir o risco de tentativas de acesso não autorizado.

Configurar um nome de usuário de administrador exclusivo

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Você não pode alterar o nome de usuário do administrador de uma instância de banco de dados Amazon RDS existente. Para criar um nome de administrador exclusivo, você precisa criar uma nova instância de banco de dados com um nome de usuário personalizado e migrar seus dados.

A instância de banco de dados Amazon RDS tem atualizações automáticas de versões secundárias desativadas

As atualizações automáticas de versões secundárias garantem que suas instâncias do Amazon RDS recebam automaticamente atualizações de versões secundárias do mecanismo quando estiverem disponíveis. Essas atualizações geralmente incluem patches de segurança e correções de erros importantes que ajudam a manter a segurança e a estabilidade do seu banco de dados. Seu banco de dados corre o risco de funcionar com vulnerabilidades de segurança conhecidas que foram corrigidas em versões secundárias mais recentes. Sem atualizações automáticas, as instâncias do banco de dados podem acumular vulnerabilidades de segurança à medida que novas CVEs são descobertas. Seguindo as melhores práticas de segurança, recomendamos ativar atualizações automáticas de versões secundárias para todas as instâncias do Amazon RDS.

Ativar atualizações automáticas de versões secundárias

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Você pode ver as configurações automáticas de atualização secundária na guia Manutenção e backups. Para obter mais informações, consulte Atualizações automáticas de versões secundárias do Amazon RDS for MySQL. Você também pode configurar sua janela de manutenção para ocorrer durante períodos de baixa atividade do banco de dados.

A instância de banco de dados Amazon RDS tem backups automatizados desativados

Os backups automatizados fornecem point-in-time recuperação para suas instâncias do Amazon RDS, permitindo que você restaure seu banco de dados em qualquer ponto dentro do período de retenção. Quando os backups automatizados são desativados, você corre o risco de perder dados em caso de exclusão maliciosa, corrupção de dados ou outros cenários de perda de dados. No caso de atividades maliciosas, como ataques de ransomware, exclusão de tabelas de banco de dados ou corrupção, a capacidade de restaurar até um ponto no tempo anterior ao incidente reduz o tempo necessário para se recuperar de um incidente. Seguindo as melhores práticas de segurança, recomendamos habilitar backups automatizados com um período de retenção adequado para todos os bancos de dados de produção.

A instância de banco de dados Amazon RDS tem a proteção de exclusão desativada

A proteção contra exclusão de banco de dados é um recurso que ajuda a impedir a exclusão de suas instâncias de banco de dados. Quando a proteção contra exclusão está desativada, seu banco de dados pode ser excluído por qualquer usuário com permissões suficientes, o que pode resultar em perda de dados ou tempo de inatividade do aplicativo. Os invasores podem excluir seu banco

de dados, causando interrupção do serviço, perda de dados e aumento do tempo de recuperação. Seguindo as melhores práticas de segurança, recomendamos ativar a proteção contra exclusão de suas instâncias de banco de dados do RDS para evitar exclusões maliciosas.

Ative a proteção de exclusão para seu cluster de banco de dados Amazon RDS

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá o cluster de banco de dados afetado.

O cluster de banco de dados Amazon RDS tem a proteção de exclusão desativada

A proteção contra exclusão de banco de dados é um recurso que ajuda a impedir a exclusão de suas instâncias de banco de dados. Quando a proteção contra exclusão está desativada, seu banco de dados pode ser excluído por qualquer usuário com permissões suficientes, o que pode resultar em perda de dados ou tempo de inatividade do aplicativo. Os invasores podem excluir seu banco de dados, causando interrupção do serviço, perda de dados e aumento do tempo de recuperação. Seguindo as melhores práticas de segurança, recomendamos habilitar a proteção contra exclusão para seus clusters de banco de dados do RDS para evitar exclusões mal-intencionadas.

Ative a proteção de exclusão para seu cluster de banco de dados Amazon RDS

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá o cluster de banco de dados afetado.

A instância de banco de dados Amazon RDS usa a porta padrão para o mecanismo de banco de dados.

As instâncias do Amazon RDS que usam portas padrão para mecanismos de banco de dados podem enfrentar maiores riscos de segurança, pois essas portas padrão são amplamente conhecidas e geralmente são alvo de ferramentas de verificação automatizadas. Modificar sua instância de banco de dados para usar portas não padrão adiciona uma camada adicional de segurança por meio da obscuridade, tornando mais difícil para usuários não autorizados realizar ataques automatizados ou direcionados ao seu banco de dados. As portas padrão geralmente são verificadas por pessoas não autorizadas e podem fazer com que sua instância de banco de dados seja direcionada. Seguindo as melhores práticas de segurança, recomendamos alterar a porta padrão para uma porta personalizada para reduzir o risco de ataques automatizados ou direcionados.

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada.

Atualizar cadeias de conexão do aplicativo

Depois de alterar a porta, atualize todos os aplicativos e serviços que se conectam à sua instância do Amazon RDS para usar o novo número da porta.

A instância de banco de dados Amazon RDS não é coberta por um plano de backup

AWS O Backup é um serviço de backup totalmente gerenciado que centraliza e automatiza o backup de dados. Serviços da AWS Se sua instância de banco de dados não estiver coberta por um plano de backup, você corre o risco de perder dados em caso de exclusão maliciosa, corrupção de dados ou outros cenários de perda de dados. No caso de atividades maliciosas, como ataques de ransomware, exclusão de tabelas de banco de dados ou corrupção, a capacidade de restaurar até um ponto no tempo anterior ao incidente reduz o tempo necessário para se recuperar de um incidente. Seguindo as melhores práticas de segurança, recomendamos incluir suas instâncias do Amazon RDS em um plano de backup para garantir a proteção dos dados.

Crie e atribua um plano de backup para sua instância de banco de dados

Na descoberta de exposição, abra o recurso com o hiperlink. Isso abrirá a instância de banco de dados afetada. Considere quais regras de frequência de backup, período de retenção e ciclo de vida são melhores para seus aplicativos.

Correção de exposições para buckets do Amazon S3

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

AWS O Security Hub pode gerar resultados de exposição para buckets do Amazon Simple Storage Service (S3).

No console do Security Hub, o bucket Amazon S3 envolvido em uma descoberta de exposição e suas informações de identificação estão listados na seção Recursos dos detalhes da descoberta. Programaticamente, você pode recuperar detalhes do recurso com a GetFindingsV2operação da API do Security Hub.

Depois de identificar o recurso envolvido em uma descoberta de exposição, você pode excluir o recurso se não precisar dele. A exclusão de um recurso não essencial pode reduzir seu perfil de exposição e AWS seus custos. Se o recurso for essencial, siga estas etapas de remediação

recomendadas para ajudar a reduzir o risco. Os tópicos de remediação são divididos com base no tipo de característica.

Uma única descoberta de exposição contém problemas identificados em vários tópicos de remediação. Por outro lado, você pode abordar uma descoberta de exposição e reduzir seu nível de gravidade abordando apenas um tópico de remediação. Sua abordagem para remediação de riscos depende de seus requisitos organizacionais e cargas de trabalho.

> **Note**
>
> A orientação de remediação fornecida neste tópico pode exigir consultas adicionais em outros AWS recursos.

Sumário

Características de configuração incorreta para buckets do Amazon S3

Aqui estão as características de configuração incorreta dos buckets do Amazon S3 e as etapas de correção sugeridas.

O bucket do Amazon S3 tem o versionamento desativado

O versionamento do Amazon S3 ajuda você a manter várias variantes de um objeto no mesmo bucket. Quando o controle de versão está desativado, o Amazon S3 armazena somente a versão mais recente de cada objeto, o que significa que, se os objetos forem excluídos ou substituídos acidentalmente ou maliciosamente, eles não poderão ser recuperados. Os buckets com controle de versão oferecem proteção contra exclusão acidental, falhas de aplicativos e incidentes de segurança, como ataques de ransomware, em que podem ocorrer modificações ou exclusões não autorizadas de dados. Seguindo as melhores práticas de segurança, recomendamos ativar o controle de versão para buckets contendo dados importantes que seriam difíceis ou impossíveis de recriar em caso de perda.

1. Habilitar versionamento — Para habilitar o versionamento do Amazon S3 em um bucket, consulte Habilitar o versionamento em buckets no Guia do usuário do Amazon Simple Storage Service. Ao ativar o controle de versão, considere a implementação de regras de ciclo de vida para gerenciar o armazenamento, pois o controle de versão manterá várias cópias dos objetos.

O bucket do Amazon S3 tem o Object Lock desativado

O Amazon S3 Object Lock fornece um modelo write-once-read-many (WORM) para objetos do Amazon S3, impedindo que eles sejam excluídos ou substituídos por um período fixo ou indefinidamente. Quando o Object Lock está desativado, seus objetos podem ficar vulneráveis à exclusão, modificação ou criptografia acidentais ou maliciosas por ransomware. O Object Lock é especialmente importante para a conformidade com os requisitos regulatórios que exigem armazenamento imutável de dados e para proteção contra ameaças sofisticadas, como ransomware, que podem tentar criptografar seus dados. Ao ativar o Object Lock, você pode aplicar políticas de retenção como uma camada adicional de proteção de dados e criar uma estratégia de backup imutável para seus dados críticos. Seguindo as melhores práticas de segurança, recomendamos que você ative o Object Lock para evitar modificações maliciosas de seus objetos.

1. Observe que o Object Lock só pode ser ativado ao criar um novo bucket, então você precisará criar um novo bucket com o Object Lock ativado. Para grandes migrações, considere usar Batch Operations para copiar objetos para o novo bucket. Antes de bloquear qualquer objeto, você também deve habilitar o versionamento e o bloqueio de objetos do Amazon S3 em um bucket. Como o Object Lock só pode ser ativado em novos buckets, você precisará migrar os dados existentes para um novo bucket com o Object Lock ativado. Configurar o Amazon S3 Object Lock — Para obter informações sobre como configurar o Object Lock em um bucket, consulte ConfiguringAmazon S3Object Lock no Guia do usuário do Amazon Simple Storage Service.

Depois de configurar o Object Lock, escolha um modo de retenção apropriado de acordo com seu ambiente.

O bucket do Amazon S3 não é criptografado em repouso com chaves AWS KMS

O Amazon S3 aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 como o nível padrão de criptografia para todos os novos buckets. Embora as chaves gerenciadas do Amazon S3 forneçam uma forte proteção de criptografia, elas não oferecem o mesmo nível de controle de acesso e recursos de auditoria que as AWS Key Management Service chaves. Ao usar chaves KMS, o acesso aos objetos requer permissões tanto para o bucket do Amazon S3 quanto para a chave KMS que criptografou o objeto. Isso é particularmente importante para dados confidenciais em que você precisa de controle granular sobre quem pode acessar os objetos criptografados e de um registro de auditoria abrangente do uso da chave de criptografia. Seguindo as melhores práticas de segurança, recomendamos o uso de chaves KMS para criptografar buckets contendo dados confidenciais ou para ambientes com requisitos rígidos de conformidade.

1. Configurar a chave de bucket do Amazon S3

   Para configurar um bucket para usar uma chave de bucket do Amazon S3 para novos objetos, consulte Como configurar seu bucket para usar uma chave de bucket do Amazon S3 com SSE-KMS para novos objetos no Guia do usuário do Amazon Simple Storage Service. Para obter informações sobre como criptografar um objeto existente, consulte Criptografar objetos com operações em lote do Amazon S3 no AWS blog de armazenamento.

Ao implementar a AWS KMS criptografia, considere o seguinte:

- Gerenciamento de chaves — Decida se deseja usar uma chave AWS gerenciada ou uma chave gerenciada pelo cliente (CMK). CMKs oferecem aos clientes controle total sobre o ciclo de vida e o uso de suas chaves. Para obter mais informações sobre a diferença entre esses dois tipos de chaves, consulte Chaves AWS KMS no Guia do AWS Key Management Service desenvolvedor.
- Rotação de chaves — Para medidas de segurança adicionais, ative a rotação automática de chaves para suas chaves KMS. Para obter mais informações, consulte Habilitar a rotação automática de chaves no Guia do AWS Key Management Service desenvolvedor.

A exclusão da autenticação multifator (MFA) está desativada em um bucket Amazon S3 versionado

A exclusão por autenticação multifator (MFA) fornece uma camada adicional de segurança para seu bucket do Amazon S3. Ela exige autenticação multifatorial para operações destrutivas do Amazon S3. Quando a exclusão da MFA é desativada, os usuários com as permissões apropriadas podem excluir permanentemente as versões do objeto ou suspender o controle de versão no seu bucket sem desafios adicionais de autenticação. Habilitar a exclusão do MFA ajuda a proteger contra a exclusão não autorizada ou acidental de seus dados, fornecendo proteção aprimorada contra ataques de ransomware, ameaças internas e erros operacionais. A exclusão de MFA é particularmente valiosa para buckets que contêm dados críticos ou sensíveis à conformidade que devem ser protegidos contra exclusão não autorizada. Seguindo as melhores práticas de segurança, recomendamos habilitar o MFA para seus buckets do Amazon S3.

1. Analise os tipos de MFA

   AWS suporta os seguintes tipos de MFA. Embora a autenticação com um dispositivo físico normalmente forneça uma proteção de segurança mais rigorosa, usar qualquer tipo de MFA é mais seguro do que ter a MFA desativada.

2. Aplique o MFA no nível da política de recursos

   Use a chave de `aws:MultiFactorAuthAge` condição em uma política de bucket para exigir MFA para operações confidenciais. Para obter mais informações, consulte Exigindo MFA no Guia do usuário do Amazon Simple Storage Service.

3. Ativar MFA

   Para habilitar a exclusão da MFA, primeiro, certifique-se de que o versionamento esteja habilitado em seu bucket do Amazon S3. A exclusão de MFA só é suportada em buckets com versionamento ativado. Para obter informações sobre como habilitar o controle de versão do Amazon S3, consulte Como ativar o controle de versão em buckets no Guia do usuário do Amazon Simple Storage Service. A exclusão de MFA não pode ser habilitada por meio do console do Amazon S3. Você deve usar a API do Amazon S3 ou o. AWS CLI Para obter mais informações, consulte Configurando a exclusão de MFA no Guia do usuário do Amazon Simple Storage Service.

O bucket do Amazon S3 permite que diretores de outras AWS contas modifiquem as permissões do bucket

As políticas de bucket do Amazon S3 controlam o acesso a buckets e objetos. Quando as políticas de bucket permitem que diretores de outras AWS contas modifiquem as permissões do bucket, usuários não autorizados podem reconfigurar seu bucket. Se as credenciais principais externas forem comprometidas, usuários não autorizados poderão obter controle sobre seu bucket, causando violações de dados ou interrupções no serviço. Seguindo os princípios de segurança padrão, AWS recomenda que você restrinja as ações de gerenciamento de permissões somente a diretores confiáveis.

1. Revise e identifique políticas de bucket

   Na exposição, identifique o bucket do Amazon S3 no campo ARN. No console do Amazon S3, selecione o bucket e navegue até a guia Permissions para revisar a política do bucket. Analise a política de permissões anexada ao bucket. Procure declarações de política que concedam ações como `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` declarações de política que permitam acesso a diretores fora de sua conta, conforme indicado na declaração principal.
2. Modifique a política do bucket

   Modifique a política do bucket para remover ou restringir ações concedidas a outras AWS contas:

   - Remova declarações de política que concedem ações de gerenciamento de permissões a contas externas.
   - Se o acesso entre contas for necessário, substitua as permissões `(s3:*)` amplas por ações específicas que não incluam o gerenciamento de permissões do bucket.

   Para obter informações sobre a modificação de uma política de bucket, consulte Adicionar uma política de bucket usando o console do Amazon S3 no Guia do usuário do Amazon S3.

Características de acessibilidade para buckets Amazon S3

Aqui estão as características de acessibilidade dos buckets do Amazon S3 e as etapas de remediação sugeridas.

O bucket do Amazon S3 tem acesso público

Por padrão, os buckets e objetos do Amazon S3 são privados, mas podem ser tornados públicos por meio de várias configurações. Se você modificar políticas de bucket, políticas de pontos de acesso ou permissões de objetos para permitir acesso público, corre o risco de expor dados confidenciais.

1. Avalie o bucket

   Avalie se seu bucket pode se tornar privado com base em sua política organizacional, requisitos de conformidade ou classificação de dados. Se você não pretendia conceder acesso ao bucket ao público ou a outros Contas da AWS, siga as instruções de remediação restantes.

2. Configure o bucket para ser privado

   Escolha uma das seguintes opções para configurar o acesso privado ao seu bucket do Amazon S3:

   - Nível da conta — Para bloquear o acesso público a todos os buckets em sua conta usando configurações em nível de conta, consulte Definir configurações de bloqueio de acesso público para sua conta no Guia do usuário do Amazon Simple Storage Service.
   - Nível do bucket — Para bloquear o acesso público a um bucket específico, consulte Definir configurações de bloqueio de acesso público para seus buckets do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.
   - ACL ou políticas do bucket — Para modificar a lista de controle de acesso (ACL) do bucket, a política do bucket, a política do ponto de acesso multirregional (MRAP) ou a política do ponto de acesso para remover o acesso público ao bucket, consulte Revisão e alteração do acesso ao bucket no Guia do usuário do Amazon Simple Storage Service. Se você bloquear o acesso público no nível da conta ou do bucket, esses bloqueios têm precedência sobre uma política que permite o acesso público.

O bucket do Amazon S3 tem acesso público de leitura

Os buckets do Amazon S3 com acesso público de leitura permitem que qualquer pessoa na Internet visualize o conteúdo do seu bucket. Embora isso possa ser necessário para sites acessíveis ao público ou recursos compartilhados, isso pode criar riscos de segurança se o bucket contiver dados confidenciais. O acesso público de leitura pode levar à visualização e ao download não autorizados, o que pode levar a violações de dados se dados confidenciais forem armazenados nesses compartimentos. Seguindo os princípios de segurança padrão, AWS recomenda restringir o acesso aos buckets do Amazon S3 aos usuários e sistemas necessários.

1. Bloqueie o acesso público no nível do bucket

   O Amazon S3 fornece configurações de bloqueio de acesso público que podem ser definidas nos níveis do bucket e da conta para impedir o acesso público, independentemente das políticas do bucket ou. ACLs Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service. Depois de bloquear o acesso público, revise a configuração do controle de acesso do bucket para garantir que ela esteja alinhada aos seus requisitos de acesso. Em seguida, revise sua política de bucket do Amazon S3 para definir explicitamente quem pode acessar seu bucket. Para obter exemplos de políticas de bucket, consulte Exemplos de políticas de bucket do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

2. Métodos alternativos de acesso

   Se for necessário acesso público de leitura, considere estas alternativas mais seguras:

   - CloudFront— Use CloudFront com uma Identidade de Acesso de Origem (OAI) ou Controle de Acesso de Origem (OAC) para permitir acesso de leitura a partir de um bucket privado do Amazon S3. Essa alternativa restringe o acesso direto ao seu bucket do Amazon S3 e, ao mesmo tempo, permite que o conteúdo seja acessível publicamente por meio de. CloudFront Para obter mais informações, consulte Restringir o acesso a uma origem do Amazon Amazon S3 no CloudFront Amazon Developer Guide.
   - Pré-assinado URLs — Use pré-assinado URLs para acesso temporário a objetos específicos. Para obter mais informações, consulte Compartilhamento de objetos com presignados URLs no Guia do Usuário do AWSAmazon S3.

O bucket do Amazon S3 tem acesso de gravação

Os buckets do Amazon S3 com acesso público de gravação permitem que qualquer pessoa na Internet faça upload, modifique ou exclua objetos em seu bucket. Isso cria riscos de segurança significativos, incluindo a possibilidade de alguém carregar arquivos maliciosos, modificar arquivos existentes e excluir dados. O acesso público de gravação cria vulnerabilidades de segurança que podem ser exploradas por invasores. Seguindo os princípios de segurança padrão, AWS recomenda restringir o acesso de gravação aos seus buckets do Amazon S3 somente aos usuários e sistemas necessários.

1. Bloqueie o acesso público no nível da conta e do bucket

O Amazon S3 fornece configurações de bloqueio de acesso público que podem ser definidas nos níveis do bucket e da conta para impedir o acesso público, independentemente das políticas do bucket ou. ACLs Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

2. Modificar políticas de bucket

   Para uma abordagem mais granular para remover o acesso público de gravação, revise a política do bucket. Você pode procurars3:PutObject,s3:DeleteObject, ous3:*. Para obter mais informações sobre o gerenciamento de políticas de bucket, consulte Políticas de bucket para o Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

3. Métodos de acesso alternativos Se o acesso público de leitura for necessário, considere estas alternativas mais seguras:

   - CloudFront— Use CloudFront com uma Identidade de Acesso de Origem (OAI) ou Controle de Acesso de Origem (OAC) para permitir acesso de leitura a partir de um bucket privado do Amazon S3. Essa alternativa restringe o acesso direto ao seu bucket do Amazon S3 e, ao mesmo tempo, permite que o conteúdo seja acessível publicamente por meio de. CloudFront Para obter mais informações, consulte Restringir o acesso a uma origem do Amazon S3 no CloudFront Amazon Developer Guide.
   - Pré-assinado URLs — Use pré-assinado URLs para acesso temporário a objetos específicos. Para obter mais informações, consulte Compartilhamento de objetos com objetos pré-assinados URLs no Guia do usuário do Amazon Simple Storage Service.

O ponto de acesso Amazon S3 tem configurações de acesso público habilitadas

Os pontos de acesso do Amazon S3 fornecem acesso personalizado a conjuntos de dados compartilhados em buckets do Amazon S3. Quando você ativa o acesso público a um ponto de acesso, qualquer pessoa na Internet pode acessar seus dados. Seguindo os princípios de segurança padrão, AWS recomenda restringir o acesso público aos pontos de acesso do Amazon S3.

1. Crie um novo ponto de acesso com o bloqueio de acesso público ativado

   O Amazon S3 não suporta a alteração das configurações de acesso público de um ponto de acesso após a criação de um ponto de acesso. Para obter informações sobre a criação de um ponto de acesso, consulte Gerenciamento do acesso público aos pontos de acesso para buckets de uso geral no Guia do usuário do Amazon S3. Para obter mais informações sobre o

gerenciamento do acesso público aos pontos de acesso, consulte Criação de pontos de acesso para buckets de uso geral no Guia do usuário do Amazon S3.

Características de dados confidenciais para buckets do Amazon S3

Aqui estão as características de dados confidenciais dos buckets do Amazon S3 e as etapas de remediação sugeridas.

Características de dados confidenciais para buckets do Amazon S3

Quando o Macie identifica dados confidenciais em seus buckets do Amazon S3, isso indica possíveis exposições de segurança e conformidade que exigem atenção imediata.

Os dados confidenciais podem incluir:

- Credenciais
- Informações de identificação pessoal
- Informações financeiras
- Conteúdo confidencial que requer proteção

Se dados confidenciais forem expostos por meio de configuração incorreta ou acesso não autorizado, isso poderá levar a violações de conformidade, violações de dados, roubo de identidade ou perda financeira. Seguindo as melhores práticas de segurança, AWS recomenda a classificação adequada dos dados e o monitoramento contínuo dos dados confidenciais em seus buckets do Amazon S3.

Implemente controles para dados confidenciais

Na descoberta de exposição, escolha o recurso Abrir. Analise o tipo de dados confidenciais detectados e sua localização no bucket. Para obter ajuda na interpretação das descobertas do Macie, consulte Tipos de descobertas do Macie no Guia do usuário do Amazon Macie.

Com base no tipo de dados confidenciais descobertos, implemente os controles de segurança apropriados:

- Restrinja o acesso ao bucket — revise as permissões do bucket para garantir que elas sigam o princípio do menor privilégio. Use políticas do IAM, políticas de bucket e ACLs para restringir o acesso. Para obter mais informações, consulte Identity and Access Management for Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

- Ativar criptografia do lado do servidor — Ative a criptografia do lado do servidor com chaves KMS para proteção adicional. Para obter mais informações, consulte Uso da criptografia do lado do servidor com chaves KMS (AWS SSE-KMS) no Guia do usuário do Amazon Simple Storage Service.
- Uso AWS Glue DataBrew — Use Glue DataBrew para preparação e limpeza de dados. Para obter mais informações, consulte O que está AWS Glue DataBrew no Guia do AWS Glue DataBrew desenvolvedor.

Descobertas da sequência de ataque no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Uma sequência de ataque é um tipo de ameaça à segurança. GuardDuty gera descobertas para sequências de ataque quando os eventos correspondem a um padrão de atividade suspeita. Se você habilitar GuardDuty, poderá acessar esse tipo de descoberta no console do Security Hub. Isso permite que você investigue e corrija todas as suas ameaças à segurança sem trocar de console. Você pode revisar as descobertas da sequência de ataque na tela Ameaças do console do Security Hub.

Analisando as descobertas da sequência de ataque

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Você pode revisar as descobertas da sequência de ataque na tela Ameaças do console do Security Hub. O tópico a seguir descreve como você analisa os detalhes de uma descoberta de sequência de ataque.

Analisando os detalhes das descobertas da sequência de ataque

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Este tópico descreve como analisar detalhes sobre as descobertas da sequência de ataque no console do Security Hub e com a API.

Analisando detalhes das sequências de ataque no console do Security Hub

A seguir, descrevemos como revisar os detalhes das sequências de ataque no console do Security Hub:

Para revisar as descobertas da sequência de ataque no console

1. Faça login usando suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, escolha Ameaças.
3. Na lista de descobertas da sequência de ataque, escolha a descoberta da sequência de ataque da qual você deseja ver os detalhes.

Analisando os detalhes das descobertas da sequência de ataque com a API

Você pode revisar as descobertas da sequência de ataque com a `GetFindingsV2`API ou AWS CLI o. Você pode filtrar os resultados com o `FindingProviderFields`parâmetro e fornecer um valor de filtro `TTPs/AttackSequence` se quiser retornar apenas as descobertas da sequência de ataque. Você pode filtrar por outros campos para restringir os resultados.

Exemplo de comando

Veja a seguir um AWS CLI exemplo que recupera as 10 descobertas da sequência de ataque gerada mais recentemente em sua conta. O exemplo está formatado para Linux, macOS e Unix, e o caractere de barra invertida (\) é usado para melhorar a legibilidade.

```
$ aws securityhub get-findings-v2 \
--filters '{"FindingProviderFieldsTypes":[{"Value": "TTPs/
AttackSequence","Comparison":"PREFIX"}]}' \
```

```
--sort-criteria '{ "Field": "LastObservedAt", "SortOrder": "desc"}' \
--max-items 10
```

Corrigindo as descobertas da sequência de ataque

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Para obter informações sobre como remediar as descobertas da sequência de ataques, consulte Como corrigir as descobertas de GuardDuty segurança detectadas no Guia GuardDuty do usuário da Amazon.

Regras de automação no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

As regras de automação do Security Hub são uma versão mais extensível e configurável das regras de automação CSPM do Security Hub. O Security Hub evoluiu de um sistema de automação específico de localização para uma plataforma de configuração mais ampla. Enquanto o Security Hub CSPM suporta ASFF, o Security Hub introduz suporte para OCSF e estabelece uma base para mais configurações. Um dos principais recursos das regras de automação do Security Hub é sua integração com a configuração do agregador. Isso oferece a capacidade de ajustar e implantar granularmente as configurações em um conjunto de configurações vinculadas, Regiões da AWS mantendo a flexibilidade de configurar a experiência regional por meio da desvinculação, uma por uma. Regiões da AWS

Os recursos do Security Hub em sua Conta da AWS mão Região da AWS, incluindo regras de automação, conectores e agregadores, deixarão de funcionar nos cenários abaixo.

- O autônomo Conta da AWS se torna membro de uma AWS organização com um administrador delegado
- A conta de gerenciamento da AWS organização remove o administrador delegado da organização e define um novo administrador delegado

- A configuração do agregador do administrador delegado ou autônomo Conta da AWS é alterada para tornar uma região desvinculada uma região vinculada

Nesses cenários, a conta do membro ainda pode gerenciar esses recursos por meio de operações de listar, obter e excluir AWS CLI apenas. Quando uma região desvinculada é transformada em região vinculada, o administrador delegado ou a AWS conta autônoma ainda pode gerenciar os recursos antigos em uma região vinculada por meio de operações de lista, obtenção e exclusão.

Principais aprimoramentos

As regras de automação no CSPM do Security Hub são regionais e se aplicam somente às descobertas no Regiões da AWS local em que foram criadas. As regras de automação no Security Hub podem ser configuradas uma vez em uma Região da AWS (região de agregação) e depois aplicadas em todas as configurações Regiões da AWS (regiões vinculadas) por meio da configuração do Aggregator V2. Um benefício desse recurso é a capacidade de automatizar e corrigir as descobertas de segurança em várias Regiões da AWS apenas configurando uma. Região da AWS Isso significa que, se uma descoberta for gerada em uma região vinculada, ela poderá ser corrigida automaticamente com base na configuração da região de agregação.

Integração externa

As regras de automação no Security Hub oferecem suporte a um tipo de ação para a criação de tíquetes ITSM. Isso permite que os clientes encaminhem descobertas selecionadas do OCSF diretamente para uma ou mais integrações de ITSM configuradas. Se uma descoberta do OCSF corresponder aos critérios, você poderá criar um ticket em Jira Cloud ou. ServiceNow ITSM Para obter mais informações, consulte Integrações de terceiros para o Security Hub.

Critérios suportados pelo OCSF

O CSPM do Security Hub suporta a avaliação dos campos do ASFF nas descobertas, enquanto o Security Hub combina os campos do OCSF. Por exemplo, o conjunto de filtros compatíveis com o `Criteria` parâmetro usado nas regras de automação V2 corresponde ao conjunto de filtros compatíveis com o `Criteria` parâmetro usado em `GetFindingsV2`. Isso significa que os filtros usados para recuperar as descobertas da V2 podem ser usados em uma regra de automação da V2 que corresponda às descobertas.

Campos OCSF para o `AutomationRulesFindingFieldsUpdate`

A lista de campos que podem ser atualizados `AutomationRulesFindingFieldsUpdate`no CSPM do Security Hub foi alterada no Security Hub. Para `AutomationRulesFindingFieldsUpdateV2`a lista de campos que podem ser atualizados, inclua o seguinte:

- `Comment`
- `SeverityId`
- `StatusId`

Integrações de terceiros para o Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Você pode aprimorar sua postura de segurança com integrações de terceiros para o AWS Security Hub. Com esse recurso, você pode habilitar integrações que consomem descobertas do Security Hub, permitindo incorporar suas ferramentas operacionais, de investigação e de resposta ao Security Hub. Atualmente, o Security Hub oferece suporte à integração com Jira Cloud ServiceNow e.

Crie uma chave KMS para criptografar credenciais

Os procedimentos de integração nesta seção oferecem a opção de criptografar suas credenciais com uma chave própria ou uma chave AWS gerenciada pelo cliente. Uma chave AWS própria é uma chave KMS que não está na sua Conta da AWS porque o AWS serviço que criptografa suas credenciais possui e gerencia a chave KMS. Se você quiser ter controle total sobre a chave KMS usada para criptografar suas credenciais, crie uma chave gerenciada pelo cliente. Uma chave gerenciada pelo cliente é uma chave KMS que você possui e gerencia.

Acesso às operações de criptografia do Security Hub

Essa declaração de política permite que o Security Hub use a AWS KMS chave para operações de criptografia. Ele permite que o Security Hub proteja os segredos do seu cliente usando essa chave. As permissões são restritas a operações relacionadas a conectores específicos do Security Hub por meio do bloco de condições que verifica o ARN de origem e o contexto de criptografia.

```
{
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName":
 "${CloudProviderName}"
        }
    }
}
```

> **Note**
>
> Para *CloudProviderName*, insira `JIRA_CLOUD` ou `SERVICENOW`. Para *Region* e *AccountId*, insira seu Conta da AWS ID Região da AWS e.

Acesso de leitura de chaves do Security Hub

Essa declaração de política permite que o Security Hub leia metadados sobre a chave KMS permitindo a `DescribeKey` operação. Essa permissão é necessária para que o Security Hub verifique o status e a configuração da chave. O acesso é limitado a conectores específicos do Security Hub por meio da condição ARN de origem.

```
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
        }
    }
}
```

> **Note**
>
> Para *Region* e*AccountId*, insira seu Conta da AWS ID Região da AWS e.

Acesso principal do IAM para operações do Security Hub

Essa declaração de política concede à função do IAM especificada permissões para realizar operações importantes (descrever, gerar, descriptografar, recriptografar e listar aliases) ao interagir com o Security Hub usando a V2 e a V2. CreateConnector CreateTicket APIs A condição garante que essas operações só possam ser executadas por meio do serviço Security Hub na região especificada.

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
```

```
                "securityhub.${Region}.amazonaws.com"
            ]
        },
        StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "SERVICENOW"
        }
    }
}

{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.${Region}.amazonaws.com"
            ]
        }
    }
}
```

> **Note**
>
> Para*RoleName*, insira o nome da função do IAM que está fazendo chamadas para o Security Hub. Para *Region* e*AccountId*, insira seu Conta da AWS ID Região da AWS e.

Integrações para o AWS Security Hub Jira Cloud

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Este tópico descreve como acessar o console do Security Hub para configurar uma integração paraJira Cloud. Antes de concluir qualquer um dos procedimentos neste tópico, você deve adquirir um plano de Jira Cloud assinatura. Para obter informações sobre planos de assinatura, consulte Preços no Atlassian site.

Para contas em uma organização, somente o administrador delegado pode configurar uma integração. O administrador delegado pode usar manualmente o recurso de criação de tíquete para descobrir qualquer conta de membro. Além disso, o administrador delegado pode usar regras de automação para criar automaticamente tickets para qualquer descoberta associada às contas dos membros. Ao definir uma regra de automação, o administrador delegado pode definir critérios, que podem incluir todas as contas de membros ou contas de membros específicas. Para obter informações sobre como configurar um administrador delegado, consulte Configurando uma conta de administrador delegado no Security Hub.

Para contas que não estão em uma organização, todos os aspectos desse recurso estão disponíveis.

Pré-requisitos

Você deve preencher os seguintes pré-requisitos antes de configurar uma integração para. Jira Cloud Caso contrário, sua integração entre o Security Hub Jira Cloud e o Security Hub não funcionará.

1. Instale o AWS Security Hub para o Jira Cloud aplicativo

O procedimento a seguir descreve como instalar o aplicativo.

1. Entre no seu Atlassian site como administrador.
2. Escolha Configurações e escolha Aplicativos.
3. Se for direcionado para a página do marketplace, escolha Encontrar novos aplicativos. Se direcionado para a página de aplicativos, escolha Explorar aplicativos e, em seguida, pesquise AWS Security Hub para Jira Cloud. Em seguida, escolha Obter agora.

2. Criar um projeto

Essa etapa é necessária se você não tiver criado um projeto. Para obter informações sobre como criar um projeto, consulte Criar um novo projeto na Jira Cloud Support documentação.

Requisitos para criar um projeto

Certifique-se de fazer o seguinte ao criar um novo projeto.

- Escolha Desenvolvimento de software para o modelo de projeto.
- Escolha Gerenciado pela empresa para o tipo de projeto.
- Anote a chave do projeto.

3. Adicione seus projetos de desenvolvimento de software ao AWS Security Hub para Jira Cloud aplicativos

O procedimento a seguir descreve como adicionar seus projetos de desenvolvimento de software ao Security Hub for Jira Cloud app.

1. Entre no seu Atlassian site como administrador.
2. Escolha Configurações e escolha Aplicativos.
3. Na lista de aplicativos, escolha AWS Security Hub para Jira Cloud.
4. Escolha a guia Configurações do conector.
5. Em Projetos ativados, escolha Adicionar projeto Jira.
    a. No menu suspenso, escolha Adicionar tudo ou selecione um projeto. Repita essa parte da etapa se quiser adicionar mais de um projeto, mas não todos os projetos.
    b. Escolha Salvar.

Você pode verificar quais projetos foram instalados com sucesso na guia Installation Manager. Você também pode verificar as configurações de campos, telas, status e fluxos de trabalho na guia Installation Manager.

> **Note**
>
> Você pode escolher a guia Installation Manager para verificar se todos os projetos selecionados foram instalados com êxito.

Para obter informações adicionais sobreJira Cloud, consulte Jira Cloudos recursos no Altlassian site.

Recomendações

A seguir estão as recomendações a serem consideradas antes de configurar uma integração paraJira Cloud.

- Crie uma conta de sistema dedicada emJira Cloud.
- Use uma conta do sistema por Jira Cloud instância.

Configure uma integração para Jira Cloud

O Security Hub cria problemas automaticamente em Jira Cloud. Essa integração permite que você envie descobertas do Security Hub paraJira Cloud, para que você possa gerenciá-las como parte de seus fluxos de trabalho operacionais. Por exemplo, você pode atribuir a propriedade a problemas que precisam de investigação e remediação. Você deve concluir o procedimento a seguir para cada um dos Jira Cloud projetos para os quais deseja enviar as descobertas do Security Hub.

> **Note**
>
> Ao criar um Jira Cloud conector, você é redirecionado do atual Região da AWS para`"https://3rdp.oauth.console.api.aws"`, para poder concluir o registro do conector. Depois, você retornará ao Região da AWS local onde o conector está sendo criado.

Para configurar uma integração para Jira Cloud

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, escolha Gerenciamento e, em seguida, selecione Integrações.
3. Escolha AdicionarJira Cloud.
4. Em Detalhes, insira um nome exclusivo e descritivo para sua integração e determine se deseja inserir uma descrição opcional para sua integração.
5. Para configurações de segurança, decida como criptografar suas Jira Cloud credenciais no Security Hub. Se você escolher a chave de propriedade do serviço, uma chave AWS própria será usada para criptografar seus dados. Se você escolher Chave personalizada, deverá inserir o ARN de uma chave personalizada existente ou criar uma nova chave escolhendo Criar uma AWS KMS chave. Para obter informações sobre como criar uma chave KMS, consulte Criar uma chave KMS de criptografia simétrica.

> **Note**
>
> Você não pode alterar essas configurações depois de concluir essa configuração. No entanto, se você escolher Chave personalizada, poderá editar sua política de chave personalizada a qualquer momento.

6. (Opcional) Para tags, crie e adicione uma tag à sua integração. É possível adicionar até 50 tags.
7. Em Autorizações, escolha Criar conector e autorizar. Um pop-up aparece onde você escolhe Permitir para concluir a autorização. Depois de concluir a autorização, uma caixa de seleção é exibida informando que a autorização foi bem-sucedida.
8. Em Configurações, insira o ID do Jira Cloud projeto.
9. Escolha Configuração completa. Depois de concluir a configuração, você pode visualizar suas integrações configuradas na guia Integrações configuradas.

Criação de um ticket para uma Jira Cloud integração

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Depois de criar uma integração comJira Cloud, você pode criar um ticket para uma descoberta.

> **Note**
>
> Uma descoberta sempre estará associada a um único ticket durante todo o seu ciclo de vida. Todas as atualizações subsequentes de uma descoberta após a criação inicial serão enviadas para o mesmo ticket. Se um conector associado a uma regra de automação for alterado, o conector atualizado será usado somente para descobertas novas e recebidas que correspondam aos critérios da regra.

Para criar um ticket para uma descoberta

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.

2. No painel de navegação, em Inventário, escolha Descobertas.
3. Escolha uma descoberta. Na descoberta, escolha Criar ticket.
4. Para Integração, abra o menu suspenso e escolha uma integração. Essa integração é a integração que você criou anteriormente quando configurou o Jira Cloud projeto. Escolha a integração para a qual você deseja que as descobertas sejam enviadas.
5. Escolha Criar.

Visualização de um ticket para uma Jira Cloud integração

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Depois de criar um ticket para uma descoberta, você pode abrir o ticket na sua Jira Cloud instância.

Para ver uma descoberta em sua Jira Cloud instância

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, em Inventário, escolha Descobertas.
3. Escolha a descoberta em que você criou o ticket.
4. Na descoberta, escolha o ID do ticket para visualizar o ticket em sua Jira Cloud instância ou Visualizar JSON.

Integrações para ServiceNow

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Este tópico descreve como acessar o console do Security Hub para configurar uma integração paraServiceNow ITSM. Antes de concluir qualquer um dos procedimentos deste tópico, você deve ter uma assinatura ServiceNow ITSM antes de poder adicionar essa integração. Para obter mais informações, consulte a página de preços no ServiceNow site.

Para contas em uma organização, somente o administrador delegado pode configurar uma integração. O administrador delegado pode usar manualmente o recurso de criação de tíquete para descobrir qualquer conta de membro. Além disso, o administrador delegado pode usar regras de automação para criar automaticamente tickets para qualquer descoberta associada às contas dos membros. Ao definir uma regra de automação, o administrador delegado pode definir critérios, que podem incluir todas as contas de membros ou contas de membros específicas. Para obter informações sobre como configurar um administrador delegado, consulte Configurando uma conta de administrador delegado no Security Hub.

Para contas que não estão em uma organização, todos os aspectos desse recurso estão disponíveis.

Pré-requisitos

Você deve preencher os seguintes pré-requisitos antes de configurar uma integração para. ServiceNow ITSM Caso contrário, sua integração entre o Security Hub ServiceNow ITSM e o Security Hub não funcionará.

1. Instale a integração do Security Hubfinding para gerenciamento de serviços de TI (ITSM)

O procedimento a seguir descreve como instalar o plug-in do Security Hub.

1. Faça login na sua ServiceNow ITSM instância e, em seguida, abra o navegador do aplicativo.
2. Navegue até a ServiceNow loja.
3. Pesquise a integração das descobertas do Security Hub para o Gerenciamento de Serviços de TI (ITSM) e escolha Obter para instalar o aplicativo.

> **Note**
>
> Nas configurações do aplicativo Security Hub, escolha qual ação tomar quando novas descobertas do Security Hub forem enviadas ao seu ServiceNow ITSM ambiente. Você pode escolher Não fazer nada, Criar incidente, Criar problema ou Criar ambos (incidente/problema)

2. Configurar o tipo de concessão de credenciais do cliente para solicitações de entrada OAuth

Você deve configurar esse tipo de concessão para OAuth solicitações de entrada. Para obter mais informações, consulte O tipo de concessão de credenciais de cliente para entrada OAuth é suportado na página da Web de ServiceNow Support.

3. Crie um OAuth aplicativo

Se você já criou um OAuth aplicativo, pode ignorar esse pré-requisito. Para obter informações sobre como criar um OAuth aplicativo, consulte Configuração OAuth.

Configure uma integração para ServiceNow ITSM

O Security Hub pode criar incidentes ou problemas automaticamente noServiceNow ITSM.

Para configurar uma integração para ServiceNow ITSM

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, escolha Gerenciamento e, em seguida, selecione Integrações.
3. Em ServiceNow ITSM, escolha Adicionar integração.
4. Em Detalhes, insira um nome para sua integração e determine se deseja inserir uma descrição opcional para sua integração.
5. Para configurações de segurança, decida como criptografar suas Jira Cloud credenciais no Security Hub. Se você escolher a chave de propriedade do serviço, uma chave AWS própria será usada para criptografar seus dados. Se você escolher Chave personalizada, deverá inserir o ARN de uma chave personalizada existente ou criar uma nova chave escolhendo Criar uma AWS KMS chave. Para obter informações sobre como criar uma chave KMS, consulte Criar uma chave KMS de criptografia simétrica.

   > **Note**
   >
   > Você não pode alterar essas configurações depois de concluir essa configuração. No entanto, se você escolher Chave personalizada, poderá editar sua política de chaves personalizadas a qualquer momento.

6. Em Autorizações, insira ServiceNow ITSM URL, ID do cliente e segredo do cliente.
7. Para Tags, determine se você deseja criar e adicionar uma tag opcional à sua integração.
8. Escolha Configuração completa. Depois de concluir a configuração, você pode visualizar suas integrações configuradas na guia Integrações configuradas.

Criação de um ticket para uma ServiceNow ITSM integração

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Depois de criar uma integração comServiceNow ITSM, você pode criar um ticket para uma descoberta.

> **Note**
>
> Uma descoberta sempre estará associada a um único ticket durante todo o seu ciclo de vida. Todas as atualizações subsequentes de uma descoberta após a criação inicial serão enviadas para o mesmo ticket. Se um conector associado a uma regra de automação for alterado, o conector atualizado será usado somente para descobertas novas e recebidas que correspondam aos critérios da regra.

Para criar um ticket para uma descoberta

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, em Inventário, escolha Descobertas.
3. Escolha uma descoberta. Na descoberta, escolha Criar ticket.
4. Para Integração, abra o menu suspenso e escolha uma integração.
5. Escolha Criar.

Visualização de um ticket para uma ServiceNow ITSM integração

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Depois de criar um ticket para uma descoberta, você pode abrir o ticket na sua ServiceNow ITSM instância.

Para ver uma descoberta em sua ServiceNow ITSM instância

1. Faça login na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home? região = us-east-1.
2. No painel de navegação, em Inventário, escolha Descobertas.
3. Escolha a descoberta em que você criou o ticket.
4. Na descoberta, escolha o ID do ticket para visualizar o ticket em sua ServiceNow ITSM instância ou Visualizar JSON.

Trabalhando no painel de resumo no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Este tópico descreve o painel Summary no console do Security Hub. Esta página mostra uma visão geral de suas exposições, ameaças, principais recursos e cobertura de serviços de segurança em vários widgets de segurança. Esses widgets ajudam você a visualizar exposições e ameaças por gravidade e conta por capacidade de segurança. Sempre que você abre essa página, os dados são atualizados automaticamente.

Você pode personalizar essa página adicionando e removendo diferentes widgets de segurança e definindo critérios de filtro para recuperar dados específicos em cada widget. As personalizações desta página são salvas para uso futuro. Se sua conta for a conta de administrador delegado de uma organização, as personalizações serão salvas independentemente das personalizações da conta do membro.

> **Note**
>
> Recomendamos que você não inclua informações confidenciais, sensíveis ou de identificação pessoal (PII) em filtros salvos, widgets personalizados ou outros campos de texto de formato livre relacionados.

Se sua conta for a conta de administrador delegado de uma organização, os dados incluem descobertas para sua conta e contas de membros. Se sua conta for uma conta de membro ou uma

conta independente, os dados incluirão apenas as descobertas da sua conta. Se você configurar a agregação entre regiões no Security Hub, esta página mostra as descobertas da sua agregação.

O widget de resumo da exposição

Esse widget mostra todas as suas exposições por gravidade. Você pode ver a frequência de cada exposição em seu ambiente. Exposições com maior severidade aparecem primeiro. As exposições são baseadas em uma análise de descobertas e características do Security Hub e de outros Serviços da AWS, como o Amazon Inspector. A lista de exposições neste widget é limitada às oito exposições mais altas com o maior número de descobertas críticas. Se duas ou mais exposições tiverem um número igual de descobertas críticas, a lista agrupa automaticamente essas descobertas por trás das descobertas críticas mais recentes.

O widget de resumo de ameaças

Esse widget mostra todas as suas ameaças por gravidade. Ameaças com maior severidade aparecem primeiro. As ameaças estão relacionadas a uma série de eventos e identificam possíveis ameaças em seu ambiente. Eles também se originam em GuardDuty. A lista de ameaças neste widget é limitada às oito ameaças com maior gravidade. Se duas ou mais ameaças tiverem a mesma gravidade, a lista agrupará automaticamente essas descobertas por trás das descobertas mais recentes. Você deve habilitar GuardDuty para receber dados neste widget.

O widget de cobertura de segurança

Esse widget mostra uma visão geral da sua cobertura de segurança e se baseia nas descobertas de cobertura dos serviços suportados. Ele exibe quais verificações de cobertura foram aprovadas, falharam ou não estão disponíveis. Não disponível indica que a verificação da cobertura não pôde ser concluída. Isso pode ser causado por um recurso excluído ou por uma falha no servidor.

As porcentagens das verificações de cobertura apontam para o número de verificações aprovadas e reprovadas. Por exemplo, uma verificação de cobertura é aprovada e uma verificação de cobertura falha. Isso indica que 50% de seus cheques foram aprovados e 50% de seus cheques falharam. Em alguns casos, as porcentagens são arredondadas para o número inteiro mais próximo.

Ao contrário de serviços de segurança como GuardDuty Amazon Inspector e Macie, o Security Hub CSPM publica uma descoberta de cobertura por conta, que PASS/FAIL depende dos padrões habilitados, como PASS, se pelo menos 1 padrão estiver habilitado. As porcentagens de cobertura do CSPM do Security Hub são o número de descobertas de cobertura do CSPM do Security Hub que passaram para o número total de descobertas de cobertura do CSPM do Security Hub.

> **Note**
>
> Recomendamos que você não inclua informações confidenciais, sensíveis ou de identificação pessoal (PII) em filtros salvos, widgets personalizados ou outros campos de texto de formato livre relacionados.

Visualizando detalhes sobre recursos no Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

A página Recursos rastreia recursos comuns em sua conta. Você pode acessar a página Recursos no console do Security Hub escolhendo Recursos no painel de navegação. Ao escolher um tipo de recurso, você pode revisar todos os recursos associados ao tipo de recurso. Você pode revisar qualquer descoberta associada a um recurso.

> **Note**
>
> O administrador delegado pode visualizar todos os recursos associados às contas dos membros. Se você configurou uma casa Região da AWS, você pode ver todos os seus recursos em sua casa Região da AWS a partir do link Regiões da AWS.

Se você escolher um recurso, poderá revisar os detalhes desse recurso. Esses detalhes incluem o nome, ID, ARN, tipo e categoria do recurso. Você pode revisar a ID da conta associada ao recurso, quando o recurso foi criado (carimbo de data/hora) e onde o recurso foi criado (Região da AWS). Você também pode revisar detalhes adicionais em um trecho JSON que pode ser copiado.

Se você alternar da guia Visão geral para a guia Descobertas, poderá revisar todas as descobertas associadas ao recurso. A guia Descobertas mostra o nome de cada descoberta, o tipo de cada descoberta e a gravidade de cada descoberta. Você pode agrupar as descobertas por diferentes campos e pesquisar as descobertas usando filtros. Se você escolher uma descoberta, poderá revisar uma visão geral da descoberta, que inclui informações sobre conformidade e como corrigir problemas associados à descoberta. Se você voltar ao recurso, poderá escolher Abrir recurso para

analisar o recurso no console quanto ao seu tipo de recurso. Por exemplo, se o recurso for um recurso do IAM, você pode abrir o recurso no console do IAM.

A página de recursos fornece maneiras diferentes de organizar e pesquisar recursos. Você pode agrupar recursos por tipo. Por exemplo, você pode agrupar recursos por ID da conta, tipo de descoberta Região da AWS, categoria do recurso, nome do recurso e tipo de recurso. Você pode pesquisar descobertas usando filtros. Os filtros rápidos ajudam você a analisar os recursos por categoria, contas e tipos de descoberta.

A vantagem da página Recursos é que ela ajuda você a monitorar sua postura de segurança, organizar seus recursos e analisar detalhes sobre seus recursos.

Visualizando exposições no Security Hub com o gráfico do caminho de ataque potencial

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

O gráfico do caminho do ataque potencial é uma visualização interativa que mostra como possíveis invasores podem acessar e assumir o controle dos recursos associados a uma descoberta de exposição. Você pode acessar esse gráfico somente no console do Security Hub e na tela Exposições. Quando você visualiza os detalhes de uma descoberta de exposição, a guia Visão geral inclui uma seção chamada Caminho potencial de ataque.

Nesta seção da guia Visão geral, você pode escolher e arrastar AWS recursos no gráfico do caminho de ataque potencial. Você pode se concentrar em áreas específicas do gráfico do caminho de ataque com os ícones de ampliação e redução. Você pode expandir o gráfico do caminho de ataque para dentro e para fora do modo de tela cheia por meio do ícone de tela cheia. A legenda codifica o recurso primário, o recurso envolvido e a contagem de características contribuintes por cor e mostra as categorias de características e o número de características no gráfico do caminho de ataque. Você pode visualizar os detalhes de um recurso escolhendo um recurso e escolhendo Exibir detalhes do recurso. Você também pode copiar o ID e o Conta da AWS número associados a um recurso. Os resultados da exposição com uma característica de acessibilidade mostram a Internet pública e o caminho de rede interrompido no gráfico do caminho de ataque. Você pode ver esses detalhes escolhendo o nó do caminho de rede reduzido.

Desabilitar o Security Hub

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Se sua conta não fizer parte de uma organização, você poderá desativar o Security Hub no console do Security Hub a qualquer momento. Quando você desativa o Security Hub, interrompe a ingestão de descobertas. Você também perde o acesso às descobertas e configurações existentes. O procedimento a seguir descreve como desabilitar o Security Hub.

Para desativar o Security Hub

1. Entre na sua AWS conta com suas credenciais e abra o console do Security Hub em https://console.aws.amazon.com/securityhub/v2/home.
2. No painel de navegação, escolha Geral.
3. No Security Hub, escolha Desativar. Na janela pop-up, insira Desativar e escolha Desativar.

Introdução ao AWS Security Hub CSPM

AWS O Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) fornece uma visão abrangente do seu estado de segurança AWS e ajuda você a avaliar seu AWS ambiente em relação aos padrões e melhores práticas do setor de segurança.

AWS O Security Hub CSPM coleta dados de segurança em Contas da AWS produtos de terceiros compatíveis e ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade. Serviços da AWS

Para ajudá-lo a gerenciar o estado de segurança da sua organização, o Security Hub CSPM oferece suporte a vários padrões de segurança. Isso inclui o padrão AWS Foundational Security Best Practices (FSBP) desenvolvido por e estruturas externas de conformidade AWS, como o Center for Internet Security (CIS), o Payment Card Industry Data Security Standard (PCI DSS) e o National Institute of Standards and Technology (NIST). Cada padrão inclui vários controles de segurança, cada um dos quais representa uma prática recomendada de segurança. O Security Hub CSPM executa verificações em relação aos controles de segurança e gera descobertas de controle para ajudá-lo a avaliar sua conformidade com as melhores práticas de segurança.

Além de gerar descobertas de controle, o Security Hub CSPM também recebe descobertas de outros, Serviços da AWS como Amazon, Amazon GuardDuty 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 CSPM do Security Hub para outros produtos Serviços da AWS e produtos de terceiros compatíveis.

O Security Hub CSPM oferece recursos de automação que ajudam você a fazer a triagem e corrigir problemas de segurança. Por exemplo, você pode 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

Benefícios do Security Hub CSPM

Aqui estão algumas das principais maneiras pelas quais o Security Hub CSPM 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 CSPM reduz o esforço de coletar e priorizar as descobertas de segurança em contas de produtos integrados Serviços da AWS e de parceiros. AWS O Security Hub CSPM processa a busca de dados usando o AWS Security Finding Format (ASFF), um formato de busca padrão. Isso elimina a necessidade de gerenciar descobertas de inúmeras fontes em vários formatos. O Security Hub CSPM também correlaciona as descobertas entre provedores para ajudar você a priorizar as mais importantes.

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

O Security Hub CSPM executa automaticamente verificações contínuas de configuração e segurança em nível de conta com base nas AWS melhores práticas e nos padrões do setor. O Security Hub CSPM 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 CSPM consolida suas descobertas de segurança em contas e produtos do provedor e exibe os resultados no console CSPM do Security Hub. Você também pode recuperar descobertas por meio da API CSPM do Security Hub ou. AWS CLI SDKs Com uma visão ampla do seu status de segurança atual, você pode detectar tendências, identificar possíveis problemas e tomar as medidas de correção necessárias.

Capacidade de automatizar a correção e atualização de descobertas

Você pode criar regras de automação que modificam ou suprimem descobertas com base nos critérios definidos. O Security Hub CSPM 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 CSPM do Security Hub

O Security Hub CSPM está disponível na maioria. Regiões da AWS Para obter uma lista das regiões em que o CSPM do Security Hub está disponível atualmente, consulte os endpoints e cotas do CSPM do AWS Security Hub no. Referência geral da AWS Para obter informações sobre como gerenciar Regiões da AWS seu Conta da AWS, consulte Especificação de qual Regiões da AWS conta pode ser usada no Guia de AWS Gerenciamento de contas referência.

Em cada região, você pode acessar e usar o CSPM do Security Hub de qualquer uma das seguintes formas:

Console CSPM do Security Hub

AWS Management Console É uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. Como parte desse console, o console CSPM do Security Hub fornece acesso à sua conta, dados e recursos do CSPM do Security Hub. Você pode executar tarefas CSPM do Security Hub usando o console CSPM do Security Hub — visualize descobertas, crie regras de automação, crie uma região de agregação e muito mais.

API CSPM do Security Hub

A API CSPM do Security Hub fornece acesso programático à sua conta, dados e recursos do CSPM do Security Hub. Com a API, você pode enviar solicitações HTTPS diretamente para o

CSPM do Security Hub. Para obter informações sobre a API, consulte a Referência da API CSPM do AWS Security Hub.

AWS CLI

Com o AWS CLI, você pode executar comandos na linha de comando do seu sistema para realizar tarefas CSPM do 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 como instalar e usar o AWS CLI, consulte o Guia AWS Command Line Interface do usuário.

AWS SDKs

AWS fornecimentos SDKs que consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação — por exemplo, Java, Go, Python, C++ e .NET. Eles SDKs fornecem acesso conveniente e programático ao Security Hub CSPM e outros Serviços da AWS no idioma de sua preferência. Eles também incluem tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter informações sobre como instalar e usar o AWS SDKs, consulte Ferramentas para construir AWS.

Important

O CSPM do Security Hub somente detecta e consolida as descobertas que são geradas após você habilitar o CSPM do Security Hub. Ele não detecta e consolida retroativamente as descobertas de segurança que foram geradas antes de você habilitar o CSPM do Security Hub.
O CSPM do Security Hub só recebe e processa descobertas na região em que você habilitou o CSPM do Security Hub em sua conta.
Para conformidade total com as verificações de segurança do CIS AWS Foundations Benchmark, você deve habilitar o CSPM do Security Hub em todas as regiões suportadas. AWS

Serviços relacionados

Para proteger ainda mais seu AWS ambiente, considere usar outro Serviços da AWS em combinação com o Security Hub CSPM. Alguns Serviços da AWS enviam suas descobertas para

o Security Hub CSPM, e o Security Hub CSPM normaliza as descobertas em um formato padrão. Alguns também Serviços da AWS podem receber descobertas do Security Hub CSPM.

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

O Security Hub CSPM usa regras vinculadas a serviços de AWS Config para executar verificações de segurança na maioria dos controles. Os controles se referem a AWS recursos específicos Serviços da AWS e específicos. Para obter uma lista dos controles CSPM do Security Hub, consulte. Referência de controle para o Security Hub CSPM Você deve habilitar AWS Config e registrar recursos no CSPM do Security Hub AWS Config para gerar a maioria das descobertas de controle. Para obter mais informações, consulte Considerações antes de ativar e configurar AWS Config.

Avaliação gratuita e preços do Security Hub CSPM

Quando você ativa o CSPM do Security Hub pela primeira vez, essa conta é automaticamente inscrita em um teste gratuito de 30 dias do Security Hub CSPM. Conta da AWS

Ao usar o Security Hub CSPM durante o teste gratuito, você é cobrado pelo uso de outros serviços com os quais o Security Hub CSPM interage, como itens. AWS Config Você não é cobrado por AWS Config regras que são ativadas somente pelos padrões de segurança CSPM do Security Hub.

Você não será cobrado pelo uso do CSPM do Security Hub até que seu teste gratuito termine.

Visualizar detalhes de uso e custo estimado

O Security Hub CSPM fornece informações de uso, incluindo um custo estimado de 30 dias para usar o CSPM 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 CSPM do Security Hub após o término do teste gratuito. As informações de uso também estão disponíveis após o término da avaliação gratuita.

Para exibir informações de uso (console)

1. Abra o console CSPM 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 do CSPM do Security Hub da sua conta 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 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 “Tipos de dados que são agregados”.

Detalhes de preço

Para obter mais informações sobre como o CSPM do Security Hub cobra pelas descobertas ingeridas e pelas verificações de segurança, consulte Preços do CSPM do Security Hub.

Conceitos e terminologia no Security Hub CSPM

No AWS Security Hub CSPM, nos baseamos em AWS conceitos e terminologias comuns e usamos esses termos adicionais.

Conta

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

Uma conta pode convidar outras contas para habilitar o CSPM do Security Hub e se associar a essa conta no CSPM do 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 de membro. As contas de administrador podem ver as descobertas em suas contas de membro.

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

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

Para obter mais informações, consulte Gerenciando contas de administrador e membro no Security Hub CSPM.

Conta de administrador

Uma conta no Security Hub CSPM que tem acesso para visualizar as descobertas das contas de membros 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 CSPM do Security Hub. Quando essas contas aceitam o convite, elas se tornam contas de 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 CSPM. A conta de administrador do Security Hub CSPM pode habilitar qualquer conta da organização como conta membro e também pode convidar outras contas para serem contas membros.

Uma conta só pode ter uma conta de administrador. Uma conta não pode ser uma conta de administrador e uma conta de 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.

Para obter mais informações, consulte the section called “Agregando dados em todas as regiões”.

Descoberta arquivada

Uma descoberta cujo estado de registro (`RecordState`) é`ARCHIVED`. O arquivamento de uma descoberta indica que o provedor da descoberta acredita que ela não é mais relevante. O estado do registro é diferente do status do fluxo de trabalho, que rastreia o status da investigação em uma descoberta.

Os provedores de localização podem usar a BatchImportFindingsoperação da API CSPM do Security Hub para arquivar as descobertas que eles criaram. O Security Hub CSPM arquiva automaticamente as descobertas de controle que atendem a determinados critérios. Para obter mais informações, consulte Gerando, atualizando e arquivando descobertas de controle.

No console CSPM do Security Hub, as configurações de filtro padrão excluem as descobertas arquivadas das listas e tabelas de busca. Você pode atualizar as configurações para incluir descobertas arquivadas. Se você recuperar descobertas usando a GetFindingsoperação da API

CSPM do Security Hub, a operação recuperará tanto as descobertas arquivadas quanto as ativas. Para excluir descobertas arquivadas, você pode filtrar os resultados. Por exemplo:

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

AWS Formato de descoberta de segurança (ASFF)

Um formato padronizado para o conteúdo das descobertas que o Security Hub CSPM agrega ou gera. O Formato AWS de descoberta de segurança permite que você use o CSPM do Security Hub para visualizar e analisar descobertas geradas por serviços de AWS segurança, soluções de terceiros ou pelo próprio CSPM do Security Hub a partir da execução de verificações de segurança. Para obter 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 controle IDs e títulos específicos do padrão. Atualmente, o Security Hub CSPM suporta controles padrão somente nas regiões da China e. AWS GovCloud (US) Regions Os controles de segurança são compatíveis com em todas as outras regiões.

Ação personalizada

Um mecanismo CSPM do Security Hub para enviar descobertas selecionadas para o. EventBridge Uma ação personalizada é criada no CSPM do Security Hub. Em seguida, ele 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 obter mais informações, consulte the section called “Criar uma ação personalizada”.

Conta de administrador delegado (Organizations)

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

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

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

Descoberta

O registro observável de uma verificação de segurança ou detecção relacionada à segurança. O Security Hub CSPM gera e atualiza as descobertas após concluir as verificações de segurança dos controles. Essas são chamadas de descobertas de controle. As descobertas também podem vir de integrações com outros produtos Serviços da AWS e produtos de terceiros.

Para obter mais informações, consulte the section called “Descobertas”.

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.

Para obter mais informações, consulte the section called “Agregando dados em todas as regiões”.

Descoberta de ingestão

A importação de descobertas para o Security Hub CSPM 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 CSPM oferece vários insights gerenciados (padrão) que você não pode modificar. Você também pode criar insights de CSPM personalizados do Security Hub para rastrear problemas de segurança exclusivos do seu AWS ambiente e uso. Para obter mais informações, consulte the section called “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.

Para obter mais informações, consulte the section called “Agregando dados em todas as 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 de 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 CSPM 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 que resulta em um `NOT_AVAILABLE` estado `PASSED` `FAILEDWARNING`,, ou. Executar uma verificação de segurança produz uma descoberta.

Conta de administrador do Security Hub CSPM

Uma conta organizacional que gerencia a associação ao CSPM do Security Hub para uma organização.

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

A conta de administrador do Security Hub CSPM também é a conta de administrador delegado do Security Hub CSPM in Organizations.

A conta de administrador do Security Hub CSPM pode habilitar qualquer conta da organização como uma conta membro. A conta de administrador do Security Hub CSPM 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 suportados no Security Hub CSPM. Para saber mais sobre os padrões de segurança no Security Hub CSPM, consulte. Entendendo os padrões de segurança no Security Hub CSPM

Gravidade

A severidade atribuída a um controle CSPM 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 mais sobre como o Security Hub CSPM atribui severidade a um controle, consulte. Níveis de severidade para resultados de controle

Status do fluxo de trabalho

O status de uma investigação sobre uma descoberta. Isso é rastreado usando o `Workflow.Status` atributo.

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 CSPM do Security Hub fornece uma opção para definir o status do fluxo de trabalho para as 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.

Habilitando o CSPM do Security Hub

Há duas maneiras de habilitar o CSPM do AWS Security Hub: integrando com 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, é necessário configurar o CSPM do Security Hub manualmente.

Verificação das permissões necessárias

Depois de se inscrever no Amazon Web Services (AWS), você deve habilitar o Security Hub CSPM para usar seus recursos e capacidades. Para habilitar o CSPM do Security Hub, primeiro você precisa configurar permissões que permitam acessar o console do CSPM do Security Hub e as operações da API. Você ou seu AWS administrador podem fazer isso usando AWS Identity and Access Management (IAM) para anexar a política AWS gerenciada chamada AWSSecurityHubFullAccess à sua identidade do IAM.

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

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

Habilitando o Security Hub CSPM com integração com Organizations

Para começar a usar o CSPM do Security Hub com AWS Organizations, a conta AWS Organizations de gerenciamento da organização designa uma conta como a conta delegada do administrador do CSPM do Security Hub para a organização. O CSPM do 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 CSPM console

Para designar o administrador delegado do CSPM do Security Hub durante a integração

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Escolha Ir para o Security Hub CSPM. 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 CSPM API

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

AWS CLI

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

Configuração central

Ao integrar o Security Hub CSPM e o Organizations, você tem a opção de usar um recurso chamado configuração central para configurar e gerenciar o CSPM do 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 CSPM do Security Hub em todas as contas e. OUs Regiões da AWS O administrador delegado configura o CSPM do Security Hub criando políticas de configuração. Em uma política de configuração, é possível especificar as configurações a seguir:

- Se o Security Hub CSPM 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, você pode criar uma única política de configuração para toda a organização ou políticas de configuração diferentes para suas várias contas e. OUs Por exemplo, contas de teste e contas de produção podem usar políticas de configuração diferentes.

As contas dos membros OUs que usam uma política de configuração são gerenciadas centralmente e só podem ser configuradas pelo administrador delegado. O administrador delegado pode designar contas de membros específicas e OUs ser autogerenciadas para dar ao membro a capacidade de definir suas próprias configurações em uma base. Region-by-Region

Se você não usa a configuração central, deve configurar amplamente o CSPM do Security Hub separadamente em cada conta e região. Isso é chamado de configuração local. Na configuração

local, o administrador delegado pode habilitar automaticamente o CSPM do Security Hub e um conjunto limitado de padrões de segurança em novas contas da organização na região atual. A configuração local não se aplica às contas existentes da organização ou a regiões que não sejam a região atual. A configuração local também não oferece suporte ao uso de políticas de configuração.

Habilitando o CSPM do Security Hub manualmente

Você deve habilitar o CSPM do Security Hub manualmente se tiver uma conta autônoma ou se não fizer integração com. AWS Organizations Contas autônomas não podem ser integradas AWS Organizations e devem usar a ativação manual.

Ao habilitar o CSPM do Security Hub manualmente, você designa uma conta de administrador do Security Hub CSPM e convida outras contas para se tornarem contas membros. 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 ativar o CSPM do Security Hub. Ao habilitar o Security Hub CSPM a partir do console, você também tem a opção de ativar os padrões de segurança suportados.

Security Hub CSPM console

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Ao abrir o console CSPM do Security Hub pela primeira vez, escolha Ir para o CSPM do Security Hub.
3. Na página de boas-vindas, a seção Padrões de segurança lista os padrões de segurança que o Security Hub CSPM suporta.

   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 mais informações sobre gerenciamento de padrões de segurança, consulte Entendendo os padrões de segurança no Security Hub CSPM.
4. Selecione Enable Security Hub (Habilitar o Security Hub).

Security Hub CSPM API

Invoque a API `EnableSecurityHub`. Quando você ativa o Security Hub CSPM a partir da API, ele ativa automaticamente os seguintes padrões de segurança padrão:

- AWS Melhores práticas básicas de segurança
- Referência de AWS fundamentos do Center for Internet Security (CIS) 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 Melhores práticas básicas de segurança
- Referência de AWS fundamentos do Center for Internet Security (CIS) 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 CSPM do Security Hub em várias contas e regiões.

O script de habilitação de várias contas do Security Hub CSPM GitHub permite que você habilite o CSPM do Security Hub em todas as contas e regiões. O script também automatiza o processo de envio de convites para contas de membros e habilitação do AWS Config.

O script ativa automaticamente a gravação de AWS Config recursos para todos os recursos, incluindo recursos globais, em todas as regiões. Ele não limita o registro de recursos globais a uma única região. Para economizar custos, recomendamos registrar recursos globais somente em uma única região. Se você usa a configuração central ou a agregação entre regiões, essa deve ser sua região de origem. Para obter mais informações, consulte Recursos de gravação em AWS Config.

Há um script correspondente para desativar o CSPM do Security Hub em contas e regiões.

Próximas etapas: gerenciamento de postura e integrações

Depois de ativar o CSPM do Security Hub, recomendamos ativar os padrões e controles de segurança para monitorar sua postura de segurança. Depois de habilitar os controles, o Security Hub CSPM começa a executar verificações de segurança e a gerar descobertas de controle que ajudam a detectar configurações incorretas em seu ambiente. AWS Para receber descobertas de controle, você deve habilitar e configurar AWS Config o Security Hub CSPM. Para obter mais informações, consulte Habilitando e configurando o AWS Config Security Hub CSPM.

Depois de habilitar o CSPM do Security Hub, você também pode aproveitar as integrações entre o CSPM do Security Hub e outras soluções e de terceiros para ver suas Serviços da AWS descobertas no CSPM do Security Hub. O Security Hub CSPM agrega descobertas de diferentes fontes e as ingere em um formato consistente. Para obter mais informações, consulte Entendendo as integrações no Security Hub CSPM.

Habilitando e configurando o AWS Config Security Hub CSPM

AWS O Security Hub CSPM usa AWS Config regras para executar verificações de segurança e gerar descobertas para a maioria dos controles. AWS Config fornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS. Ele usa regras para estabelecer uma configuração básica para seus recursos e um gravador de configuração para detectar se um determinado recurso viola as condições de uma regra. Algumas regras, chamadas de regras AWS Config gerenciadas, são predefinidas e desenvolvidas pela AWS Config. Outras regras são regras AWS Config personalizadas que o Security Hub CSPM desenvolve.

AWS Config as regras que o Security Hub CSPM usa para controles são chamadas de regras vinculadas a serviços. As regras vinculadas ao serviço permitem Serviços da AWS , como o CSPM do Security Hub, criar AWS Config regras em sua conta.

Para receber descobertas de controle no Security Hub CSPM, você deve habilitar AWS Config em sua conta e ativar a gravação dos recursos que seus controles habilitados avaliam. Esta página explica como habilitar o AWS Config CSPM do Security Hub e ativar a gravação de recursos.

Considerações antes de ativar e configurar AWS Config

Para receber descobertas de controle no CSPM do Security Hub, sua conta deve estar AWS Config habilitada em cada Região da AWS uma em que o CSPM do Security Hub esteja habilitado. Se você usa o Security Hub CSPM para um ambiente de várias contas, AWS Config deve estar habilitado em cada região para a conta de administrador e todas as contas de membros.

É altamente recomendável que você ative a gravação de recursos AWS Config antes de habilitar quaisquer padrões e controles CSPM do Security Hub. Isso ajuda a garantir que suas descobertas de controle sejam precisas.

Para ativar a gravação de recursos AWS Config, você deve ter permissões suficientes para registrar recursos na função AWS Identity and Access Management (IAM) anexada ao gravador de configuração. Além disso, certifique-se de que não haja uma política de IAM ou uma política gerenciada AWS Organizations que impeça a permissão AWS Config de registrar seus recursos. As verificações de controle CSPM do Security Hub avaliam a configuração de um recurso diretamente e não levam em conta AWS Organizations as políticas. Para obter mais informações sobre AWS Config gravação, consulte Como trabalhar com o gravador de configuração no Guia do AWS Config desenvolvedor.

Se você habilitar um padrão no CSPM do Security Hub, mas não tiver ativado AWS Config, o CSPM do Security Hub tentará criar AWS Config regras de acordo com o seguinte cronograma:

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

Se você usa a configuração central, o Security Hub CSPM também tenta criar AWS Config regras vinculadas a serviços sempre que você associa uma política de configuração que habilita um ou mais padrões a contas, unidades organizacionais (OUs) ou à raiz.

Recursos de gravação em AWS Config

Ao habilitar AWS Config, você deve especificar quais AWS recursos deseja que o gravador AWS Config de configuração registre. Por meio das regras vinculadas ao serviço, o gravador de configuração permite que o Security Hub CSPM detecte alterações nas configurações de seus recursos.

Para que o Security Hub CSPM gere descobertas de controle precisas, você deve ativar a gravação dos recursos que correspondem aos seus controles ativados. AWS Config São principalmente controles habilitados com um tipo de agendamento acionado por alterações que exigem registro de recursos. Alguns controles com um tipo de agendamento periódico também exigem o registro de recursos. Para obter uma lista desses controles e seus recursos correspondentes, consulteAWS Config Recursos necessários para descobertas de controle.

> **Warning**
>
> Se você não configurar a AWS Config gravação corretamente para os controles CSPM do Security Hub, isso pode resultar em descobertas de controle imprecisas, principalmente nos seguintes casos:
>
> - Você nunca registrou o recurso para um determinado controle ou desativou a gravação de um recurso antes de criar esse tipo de recurso. Nesses casos, você recebe uma `WARNING` descoberta para o controle em questão, mesmo que tenha criado recursos no escopo do controle depois de desativar a gravação. Essa `WARNING` descoberta é uma descoberta padrão que, na verdade, não avalia o estado de configuração do recurso.
> - Você desativa a gravação de um recurso que é avaliado por um controle específico. Nesse caso, o Security Hub CSPM retém as descobertas de controle que foram geradas antes de você desabilitar a gravação, mesmo que o controle não esteja avaliando recursos novos ou atualizados. O Security Hub CSPM também altera o status de conformidade das descobertas para. `WARNING` Essas descobertas retidas podem não refletir com precisão o estado atual da configuração de um recurso.

Por padrão, AWS Config registra todos os recursos regionais suportados que ele descobre no local Região da AWS em que está sendo executado. Para receber todas as descobertas de controle do CSPM do Security Hub, você também deve configurar AWS Config para registrar recursos globais. Para economizar custos, recomendamos registrar recursos globais somente em uma única região.

Se você usa a configuração central ou a agregação entre regiões, essa região deve ser sua região de origem.

Em AWS Config, você pode escolher entre gravação contínua e gravação diária de alterações no estado do recurso. 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 de CSPM do Security Hub para controles acionados por alterações até que um período de 24 horas seja concluído.

Para obter mais informações sobre AWS Config gravação, consulte AWS Recursos de gravação no Guia do AWS Config desenvolvedor.

Formas de habilitar e configurar AWS Config

Você pode ativar AWS Config e ativar a gravação de recursos de qualquer uma das seguintes formas:

- AWS Config console — Você pode ativar AWS Config uma conta usando o AWS Config console. Para obter instruções, consulte Configuração AWS Config com o console no Guia do AWS Config desenvolvedor.
- AWS CLI ou SDKs — Você pode ativar AWS Config uma conta usando o AWS Command Line Interface (AWS CLI). Para obter instruções, consulte Configuração AWS Config com o AWS CLI no Guia do AWS Config desenvolvedor. AWS kits de desenvolvimento de software (SDKs) também estão disponíveis para muitas linguagens de programação.
- CloudFormation modelo — AWS Config Para habilitar várias contas, recomendamos usar o AWS CloudFormation modelo chamado Ativar AWS Config. Para acessar esse modelo, consulte modelos de AWS CloudFormation StackSet amostra no Guia AWS CloudFormation do usuário.

  Por padrão, esse modelo exclui a gravação de recursos globais do IAM. Certifique-se de ativar a gravação dos recursos globais do IAM em apenas um Região da AWS para conservar os custos de gravação. Se você tiver a agregação entre regiões ativada, essa deverá ser sua região de origem do CSPM do Security Hub. Caso contrário, pode ser qualquer região em que o CSPM do Security Hub esteja disponível que ofereça suporte à gravação de recursos globais do IAM. Recomendamos executar um StackSet para registrar todos os recursos, incluindo recursos globais do IAM, na região de origem ou em outra região selecionada. Em seguida, execute um segundo StackSet para registrar todos os recursos, exceto os recursos globais do IAM em outras regiões.

- GitHub script — O Security Hub CSPM oferece um GitHubscript que habilita o CSPM do Security Hub e AWS Config para várias contas em todas as regiões. Esse script é útil se você não se integrou ou tem algumas contas de membros que não fazem parte de uma organização. AWS Organizations

Para obter mais informações, consulte a seguinte postagem no blog de AWS segurança: Otimize o CSPM do AWS Security Hub AWS Config para gerenciar com eficiência sua postura de segurança na nuvem.

Controle Config.1

No Security Hub CSPM, o controle Config.1 gera `FAILED` descobertas em sua conta se estiver desativado. AWS Config Ele também gera `FAILED` descobertas em sua conta se AWS Config estiver ativado, mas a gravação de recursos não estiver ativada.

Se AWS Config estiver habilitado e a gravação de recursos estiver ativada, mas a gravação de recursos não estiver ativada para um tipo de recurso verificado por um controle ativado, o Security Hub CSPM gerará uma `FAILED` descoberta para o controle Config.1. Além dessa `FAILED` descoberta, o Security Hub CSPM gera `WARNING` descobertas para o controle ativado e os tipos de recursos que o controle verifica. Por exemplo, se você habilitar o controle KMS.5 e a gravação de recursos não estiver ativada AWS KMS keys, o Security Hub CSPM gerará uma `FAILED` descoberta para o controle Config.1. O Security Hub CSPM também gera `WARNING` descobertas para o controle KMS.5 e suas chaves KMS.

Para receber uma `PASSED` descoberta para o controle Config.1, ative a gravação de recursos para todos os tipos de recursos que correspondem aos controles ativados. Além disso, desative os controles que não são necessários para sua organização. Isso ajuda a garantir que você não tenha lacunas de configuração em suas verificações de controle de segurança. Também ajuda a garantir que você receba descobertas precisas sobre recursos mal configurados.

Se você for o administrador delegado do CSPM do Security Hub de uma organização, a AWS Config gravação deve ser configurada corretamente para sua conta e suas contas de membros. Se você usar a agregação entre regiões, a AWS Config gravação deverá ser configurada corretamente na região de origem e em todas as regiões vinculadas. Os recursos globais não precisam ser registrados nas regiões vinculadas.

Gerar regras vinculadas ao serviço

Para cada controle que usa uma AWS Config regra vinculada ao serviço, o Security Hub CSPM cria instâncias da regra necessária em seu ambiente. AWS

Essas regras vinculadas ao serviço são específicas do CSPM do Security Hub. O CSPM do Security Hub cria essas regras vinculadas a serviços mesmo que já existam outras instâncias das mesmas regras. A regra vinculada ao serviço é adicionada `securityhub` antes do nome da regra original e um identificador exclusivo após o nome da regra. Por exemplo, para a regra AWS Config gerenciada`vpc-flow-logs-enabled`, o nome da regra vinculada ao serviço pode ser. `securityhub-vpc-flow-logs-enabled-12345`

Há cotas para o número de regras AWS Config gerenciadas que podem ser usadas para avaliar os controles. AWS Config as regras que o Security Hub CSPM cria não contam para essas cotas. Você pode ativar um padrão de segurança mesmo que já tenha atingido a AWS Config cota de regras gerenciadas em sua conta. Para saber mais sobre cotas para AWS Config regras, consulte Limites de serviço AWS Config no Guia do AWS Config desenvolvedor.

Considerações sobre custos

O Security Hub CSPM pode afetar os custos AWS Config do gravador de configuração atualizando o `AWS::Config::ResourceCompliance` item de configuração. As atualizações podem ocorrer sempre que um controle CSPM 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 CSPM e não usa esse item de configuração para outras finalidades, recomendamos desativar a gravação para ele no. AWS Config Isso pode reduzir os custos do AWS Config . Você não precisa registrar as verificações de segurança `AWS::Config::ResourceCompliance` para trabalhar no CSPM do Security Hub.

Para obter informações sobre os custos associados ao registro de recursos, consulte Preços e AWS Config preços do CSPM do AWS Security Hub.

Entendendo a configuração local no Security Hub CSPM

A configuração local é a forma padrão em que uma AWS organização é configurada no CSPM do Security Hub. Se você optar por usar e habilitar a configuração central, sua organização usará a configuração local por padrão.

Na configuração local, a conta delegada do administrador CSPM do Security Hub tem controle limitado sobre as configurações. As únicas configurações que o administrador delegado pode

aplicar são habilitar automaticamente o CSPM do Security Hub e os padrões de segurança padrão em novas contas da organização. Essas configurações se aplicam somente à região na qual você designou a conta de administrador delegado. Os padrões de segurança padrão são AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. As definições da configuração local não se aplicam às contas existentes da organização ou às regiões, exceto à região na qual a conta do administrador delegado foi designada.

Além de habilitar o CSPM e os padrões padrão do Security Hub em novas contas da organização em uma única região, você deve definir outras configurações de CSPM do Security Hub, incluindo padrões e controles, separadamente em cada região e conta. Como esse pode ser um processo que gere duplicações, recomendamos usar a configuração central para um ambiente com várias contas se uma ou mais das seguintes situações se aplicarem a você:

- Você deseja configurações diferentes para diversas partes da sua organização (por exemplo, diferentes padrões ou controles habilitados para diferentes equipes).
- Você opera em várias regiões e deseja reduzir o tempo e a complexidade da configuração do serviço nessas regiões.
- Você deseja que novas contas usem configurações específicas quando ingressam na organização.
- Você deseja que as contas da organização herdem configurações específicas de uma conta superior ou raiz.

Para obter informações sobre a configuração central, consulte Entendendo a configuração central no Security Hub CSPM.

Entendendo a configuração central no Security Hub CSPM

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

Na conta delegada do administrador do Security Hub CSPM, você pode habilitar o CSPM do Security Hub para as contas e unidades organizacionais () da sua organização em todas as regiões. OUs Você também pode ativar, configurar e desativar padrões de segurança e controles de segurança

individuais para contas e OUs entre regiões. É possível definir essas configurações em apenas algumas etapas a partir de uma região primária, chamada de região inicial.

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. Você pode 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 as políticas de configuração CSPM do Security Hub. As políticas de configuração permitem que o administrador delegado especifique se o CSPM do Security Hub está ativado ou desativado e quais padrões e controles estão ativados ou desativados. Eles também podem ser usados para personalizar parâmetros para 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. Especificar as regiões vinculadas é opcional. O administrador delegado pode criar uma única política de configuração para toda a organização ou criar várias políticas de configuração para definir configurações variáveis para contas diferentes e. OUs

> **Tip**
>
> Se você não usa a configuração central, deve configurar amplamente o CSPM do Security Hub separadamente em cada conta e região. Isso é chamado de configuração local. Na configuração local, o administrador delegado pode habilitar automaticamente o CSPM do Security Hub e um conjunto limitado de padrões de segurança em novas contas da organização na região atual. A configuração local não se aplica às contas existentes da organização ou a regiões que não sejam a região atual. A configuração local também não oferece suporte ao uso de políticas de configuração.

Esta seção fornece uma visão geral da configuração central.

Benefícios de usar a configuração central

Os benefícios da configuração central incluem os seguintes:

Simplifique a configuração do serviço e dos recursos CSPM do Security Hub

Quando você usa a configuração central, o Security Hub CSPM orienta você no processo de configuração das melhores práticas de segurança para sua organização. Ele também implanta as políticas de configuração resultantes em contas especificadas e OUs automaticamente. Se você tiver configurações de CSPM do Security Hub existentes, 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 CSPM do Security Hub exibe um resumo em tempo real de suas políticas de configuração e quais contas OUs usam cada política.

Configurar entre contas e regiões

Você pode usar a configuração central para configurar o CSPM do 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.

Acomode configurações diferentes em contas diferentes e OUs

Com a configuração central, você pode optar por configurar as contas da sua organização de OUs 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.

Quando usar a configuração central?

A configuração central é mais benéfica para AWS ambientes que incluem várias contas CSPM do Security Hub. Ele foi projetado para ajudar você a gerenciar centralmente o CSPM do Security Hub para várias contas.

Você pode usar a configuração central para configurar o serviço CSPM, 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 de segurança,

consulte Entendendo os padrões de segurança no Security Hub CSPM. Para obter mais informações sobre controles de segurança, consulte Entendendo os controles de segurança no Security Hub CSPM.

Termos e conceitos da configuração central

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

Configuração central

Um recurso CSPM do Security Hub que ajuda a conta delegada do administrador CSPM do Security Hub de uma organização a configurar o serviço CSPM, 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 CSPM 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 CSPM e. AWS Organizations

Região inicial

A Região da AWS partir da qual o administrador delegado configura centralmente o CSPM do 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 de origem também serve como a região de agregação CSPM do Security Hub, recebendo descobertas, insights e outros dados de 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. Especificar as regiões vinculadas é opcional.

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.

Destino

Uma Conta da AWS unidade organizacional (OU) ou a raiz da organização.

Política de configuração do CSPM do Security Hub

Uma coleção de configurações de CSPM do Security Hub que o administrador delegado pode definir para destinos gerenciados centralmente. Isso inclui:

- Se deve habilitar ou desabilitar o Security Hub CSPM.
- 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 CSPM desativa todos os outros controles (incluindo novos controles quando eles são lançados). Como alternativa, o administrador delegado pode fornecer uma lista de controles específicos que devem ser desativados, e o Security Hub CSPM habilita 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 CSPM do Security Hub, o administrador delegado pode escolher a política de configuração recomendada pelo CSPM do Security Hub ou criar políticas de configuração personalizadas. Com a API CSPM 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 CSPM, o padrão AWS Foundational Security Best Practices (FSBP) e todos os controles 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 diferentes e OUs criar uma política de configuração personalizada.

Configuração local

O tipo de configuração padrão para uma organização, depois de integrar o Security Hub CSPM e. AWS Organizations Com a configuração local, o administrador delegado pode optar por habilitar automaticamente o CSPM do 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 CSPM do Security Hub AWS Organizations ou tiver uma conta independente, deverá especificar configurações para cada conta separadamente em cada região. O gerenciamento manual de contas não oferece suporte ao uso de políticas de configuração.

Configuração central APIs

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

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`

- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Específico da conta APIs

Operações de CSPM do Security Hub que podem ser usadas para ativar ou desativar o CSPM, os padrões e os controles do Security Hub em uma base. account-by-account 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 qualquer `Describe` operação da `Get` API CSPM 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.

As contas autogerenciadas também podem usar as operações `*Invitations` e `*Members`. Porém, recomendamos que as contas autogerenciadas não usem essas operações. As associações de políticas podem não funcionar se uma conta-membro tiver seus os próprios membros e eles fizerem parte de uma organização diferente da organização do administrador delegado.

Unidade organizacional (UO)

No AWS Organizations Security Hub CSPM, um contêiner para um grupo de. Contas da AWS Uma unidade organizacional (OU) também pode conter outras OUs, permitindo que você crie uma hierarquia que se assemelhe a uma árvore invertida, com uma UO principal na parte superior e ramificações OUs que se estendem para baixo, 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 específicas ou à raiz para cobrir todas as contas e OUs em uma organização. OUs

Gerenciada centralmente

Um alvo que apenas o administrador delegado pode configurar em todas as regiões usando políticas de configuração.

A conta de administrador delegado especifica se um alvo é gerenciado centralmente. O administrador delegado também pode alterar o status de um alvo gerenciado centralmente para autogerenciado, ou vice-versa.

Autogerenciado

Um destino que gerencia suas próprias configurações de CSPM do Security Hub. Um alvo autogerenciado usa operações específicas da conta para configurar o CSPM do Security Hub separadamente em cada região. Isso é diferente das 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 um alvo é autogerenciado. O administrador delegado pode aplicar um comportamento autogerenciado a um alvo. Como alternativa, uma conta ou OU pode herdar o comportamento autogerenciado de um dos pais.

A conta de administrador delegado pode ela mesma ser uma conta autogerenciada. A conta de administrador delegado pode alterar o status de um alvo de autogerenciado para gerenciado centralmente, ou vice-versa.

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 ou à raiz. OUs 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 usam uma configuração diferente por meio de aplicativo ou herança do pai mais próximo.

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

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 CSPM, o nó principal de nível superior em uma organização. Se o administrador delegado aplicar uma política de configuração ao root, a política será associada a todas as contas e OUs na organização, a menos que elas usem uma política diferente, por meio de aplicativo 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 aplicativo 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.

Habilitando a configuração central no Security Hub CSPM

A conta delegada do administrador do AWS Security Hub CSPM pode usar a configuração central para configurar o CSPM, os padrões e os controles do Security Hub para várias contas e unidades organizacionais () em todas. OUs Regiões da AWS

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

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 deve integrar o Security Hub CSPM AWS Organizations e designar uma região de origem. Se você usa o console CSPM do Security Hub, esses pré-requisitos são incluídos no fluxo de trabalho opcional para configuração central.

Integrar ao Organizations

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

Para integrar esses serviços, você começa criando uma organização no Organizations. Na conta de gerenciamento do Organizations, você designa uma conta de administrador delegado CSPM do Security Hub. Para instruções, consulte Integrando o Security Hub CSPM 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 CSPM do Security Hub ou o CSPM do Security Hub APIs para alterar ou remover a conta do administrador delegado. Se a conta de gerenciamento do Organizations for usada AWS Organizations APIs para alterar ou remover o administrador delegado do CSPM do Security Hub, o CSPM do 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.

> **Note**
>
> A região de origem não pode ser uma região designada como uma região opcional. AWS 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 .

Outra opção é especificar uma ou mais regiões vinculadas configuráveis em uma região inicial.

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 exceção a isso são os controles que envolvem recursos globais. Se você usar a configuração central, o Security Hub CSPM desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Para obter mais informações, consulte Controles que usam recursos globais.

A região de origem também é sua região de agregação de CSPM do Security Hub, que recebe descobertas, insights e outros dados de 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 descoberta é um recurso CSPM do Security Hub que especifica a região de origem 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.

Instruções para habilitar a configuração central

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

Security Hub CSPM console

Para habilitar a configuração central (console)

1. Abra o console CSPM 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 CSPM do Security Hub, escolha Ir para o CSPM do 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.

Security Hub CSPM API

Para habilitação a configuração central (API)

1. Usando as credenciais da conta do administrador delegado, invoque a API UpdateOrganizationConfiguration a partir da região inicial.
2. Defina o campo `AutoEnable` como `false`.
3. Defina o campo `ConfigurationType` no objeto `OrganizationConfiguration` como `CENTRAL`. Essa ação:
   - Designa a conta de chamada como administradora delegada do CSPM do Security Hub em todas as regiões vinculadas.
   - Ativa o CSPM do Security Hub na conta de administrador delegado em todas as regiões vinculadas.
   - Designa a conta chamadora como administradora delegada do CSPM do Security Hub para contas novas e existentes que usam o CSPM do Security Hub e pertencem à organização. Isso ocorre na região inicial e em todas as regiões vinculadas. A conta de chamada é definida como administradora delegada para novas contas da organização somente se elas estiverem associadas a uma política de configuração que tenha o Security Hub CSPM ativado. A conta de chamada é definida como administradora delegada para contas existentes da organização somente se elas já tiverem o Security Hub CSPM ativado.
   - 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 você pode habilitar automaticamente o CSPM do 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 CSPM do Security Hub em sua organização. Para obter instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração.

Exemplo de solicitação de API:

```
{
```

```
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Para habilitação a configuração central (AWS CLI)

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 administradora delegada do CSPM do Security Hub em todas as regiões vinculadas.
   - Ativa o CSPM do Security Hub na conta de administrador delegado em todas as regiões vinculadas.
   - Designa a conta chamadora como administradora delegada do CSPM do Security Hub para contas novas e existentes que usam o CSPM do Security Hub e pertencem 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 é definida como administradora delegada para contas existentes da organização somente se elas já tiverem o Security Hub CSPM ativado.
   - 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 você pode habilitar automaticamente o CSPM do 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 CSPM do Security Hub em sua organização. Para obter

instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração.

Exemplo de comando:

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

Metas gerenciadas centralmente versus metas autogerenciadas

Quando você ativa a configuração central, o administrador delegado do CSPM do AWS Security Hub pode designar cada conta da organização, unidade organizacional (OU) e raiz como gerenciada centralmente ou autogerenciada. O tipo de gerenciamento de um alvo determina como você pode especificar suas configurações de CSPM do Security Hub.

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

Esta seção explica as diferenças entre uma designação gerenciada centralmente e autogerenciada, e como escolher o tipo de gerenciamento de uma conta, de uma UO ou da raiz.

Autogerenciado

O proprietário de uma conta autogerenciada, OU ou raiz deve definir suas configurações separadamente em cada uma Região da AWS. O administrador delegado não pode criar políticas de configuração para alvos autogerenciados.

Gerenciada centralmente

Somente o administrador delegado do CSPM do Security Hub pode definir configurações para contas gerenciadas centralmente ou a raiz na região de origem e regiões vinculadas. OUs As políticas de configuração podem ser associadas a contas gerenciadas centralmente e. OUs

O administrador delegado pode alternar o status de um alvo entre autogerenciado e gerenciado centralmente. Por padrão, todas as contas e UO são autogerenciadas quando você inicia a configuração central por meio da API CSPM do Security Hub. No console, o tipo de gerenciamento

dependerá da sua primeira política de configuração. As contas 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 anteriormente, as configurações da política substituirão a designação autogerenciada. A conta passará a ser gerenciada centralmente e adotará as configurações refletidas na política de configuração.

Se você alterar uma conta gerenciada centralmente para uma conta autogerenciada, as configurações que foram aplicadas anteriormente à conta por meio de uma política de configuração permanecerão em vigor. Por exemplo, uma conta gerenciada centralmente poderia inicialmente ser associada a uma política que habilitasse o Security Hub CSPM, habilitasse as melhores práticas de segurança AWS básicas e desabilitasse .1. CloudTrail Se você designar a conta como autogerenciada, todas as configurações permanecerão inalteradas. No entanto, o proprietário da conta pode alterar de forma independente as configurações da conta daqui para frente.

A criança conta e OUs pode herdar o comportamento autogerenciado de um pai autogerenciado, da mesma forma que contas secundárias e OUs pode herdar políticas de configuração de um pai gerenciado centralmente. Para obter mais informações, consulte Associação de políticas por meio de aplicação e herança.

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

Opções para definir configurações em 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 CSPM do Security Hub em cada região para definir suas configurações:

- `EnableSecurityHub` e `DisableSecurityHub` para ativar ou desativar o serviço CSPM do Security Hub (se uma conta autogerenciada tiver um administrador delegado do CSPM do Security Hub, o administrador deverá desassociar a conta antes que o proprietário da conta possa desativar o CSPM do Security Hub).
- `BatchEnableStandards` e `BatchDisableStandards` para habilitar ou desabilitar padrões
- `BatchUpdateStandardsControlAssociations` ou `UpdateStandardsControl` para habilitar ou desabilitar

As contas autogerenciadas também podem usar as operações `*Invitations` e `*Members`. Porém, recomendamos que as contas autogerenciadas não usem essas operações. As associações de políticas podem não funcionar se uma conta-membro tiver seus os próprios membros e eles fizerem parte de uma organização diferente da organização do administrador delegado.

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

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

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

Escolher o tipo de gerenciamento de um alvo

Escolha seu método preferido e siga as etapas para designar uma conta ou OU como gerenciada centralmente ou autogerenciada no AWS Security Hub CSPM.

Security Hub CSPM console

Para escolher o tipo de gerenciamento de uma conta ou OU

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
2. Escolher configuração.
3. Na guia Organização, selecione a conta ou OU de destino. Escolha 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 CSPM API

Para escolher o tipo de gerenciamento de uma conta ou OU

1. Invoque a StartConfigurationPolicyAssociationAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
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 start-configuration-policy-associationcomando na conta de administrador delegado CSPM do Security Hub na região de origem.
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 funcionam no Security Hub CSPM

O administrador delegado do CSPM do AWS Security Hub pode criar políticas de configuração para configurar o CSPM, os padrões de segurança e os controles de segurança do Security Hub para uma organização. Depois de criar uma política de configuração, o administrador delegado pode associá-la a contas específicas, unidades organizacionais (OUs) ou à raiz. A política então entra em vigor nas contas OUs especificadas ou na raiz.

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

Esta seção fornece uma visão geral detalhada das políticas de configuração.

Considerações sobre políticas

Antes de criar uma política de configuração no CSPM do 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, você pode associá-la a uma ou mais contas, unidades organizacionais (OUs) ou à raiz. Uma política de configuração pode ser associada a contas ou OUs por meio de aplicativo direto ou por meio de herança de uma OU principal.
- Uma conta ou UO só pode estar associada a uma única política de configuração: para evitar configurações conflitantes, uma conta ou UO só pode estar 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 são os controles que usam recursos globais. O Security Hub CSPM desativa automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem.

  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 sua política configura um controle que não está disponível na região de origem ou em uma ou mais regiões vinculadas, o Security Hub CSPM ignora a configuração de controle em regiões indisponíveis, mas aplica a configuração nas regiões em que o controle está disponível. Você não tem cobertura para um controle que não esteja disponível na região inicial ou em alguma das regiões vinculadas.
- 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:

- Ative ou desative o Security Hub CSPM.
- Habilitar um ou mais padrões de segurança.
- Indicar quais controles de segurança estão habilitados dentre todos os padrões habilitados. Você pode fazer isso fornecendo uma lista de controles específicos que devem ser habilitados, e o Security Hub CSPM desativa todos os outros controles, incluindo novos controles quando eles são lançados. Como alternativa, você pode fornecer uma lista de controles específicos que devem ser desativados, e o Security Hub CSPM habilita todos os outros controles, incluindo novos controles quando eles são 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 CSPM gere descobertas de controle. Para obter mais informações, consulte Considerações antes de ativar e configurar AWS Config.

Se você usar a configuração central, o Security Hub CSPM desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Os outros controles que você escolher habilitar por meio de uma política de configuração serão habilitados em todas as regiões em que estiverem 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.

Se um controle ativado que envolve recursos globais não for suportado na região de origem, o Security Hub CSPM tentará habilitar o controle em uma região vinculada onde o controle é suportado. Com a configuração central, você não tem cobertura para um controle que não está disponível na região de origem ou em qualquer uma das regiões vinculadas.

Para obter uma lista dos controles que envolvem recursos globais, consulte Controles que usam recursos globais.

Política de configuração recomendada

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

A política recomendada habilita o Security Hub CSPM, 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 ao root (todas as contas e OUs, tanto as novas quanto as 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.

Política de configuração personalizada

Em vez da política recomendada, o administrador delegado pode criar até 20 políticas de configuração personalizadas. Você pode associar uma única política personalizada a toda a sua organização ou políticas personalizadas diferentes a contas diferentes OUs e. 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 CSPM do 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. No entanto, você não vê a opção de criar a política de configuração recomendada no console CSPM 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 e contas autogerenciados 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. Ou então, o administrador delegado pode aplicar diretamente uma designação autogerenciada a uma conta, a uma UO ou à raiz.

Na ausência da aplicação direta, uma conta ou UO herda as configurações da entidade superior mais próxima que tenha uma política de configuração ou um 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 da política tem precedência sobre a herança. Em outras palavras, a herança não substitui uma política de configuração ou uma designação autogerenciada que o administrador delegado aplicou diretamente a uma conta ou UO.

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

Recomendamos aplicar uma política de configuração diretamente 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 ter certeza de que entendeu como as políticas de configuração funcionam, recomendamos que você crie uma política e a associe a uma conta ou uma UO de teste.

Para testar uma política de configuração

1. Crie uma política de configuração personalizada e verifique se as configurações especificadas para a ativação, os padrões e os controles do CSPM do Security Hub estão corretas. Para instruções, consulte Criação e associação de políticas de configuração.
2. Aplique a política de configuração a uma conta de teste ou UO que não tenha nenhuma conta secundária ou OUs.
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 em 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, você pode associá-la a outras contas OUs e.

Criação e associação de políticas de configuração

A conta delegada do administrador do AWS Security Hub CSPM pode criar políticas de configuração que especificam como o CSPM, os padrões e os controles do Security Hub são configurados em contas e unidades organizacionais especificadas (). OUs Uma política de configuração entra em vigor somente depois que o administrador delegado a associa a pelo menos uma conta ou unidade

organizacional (OUs) ou à raiz. O administrador delegado também pode associar uma configuração autogerenciada às contas ou à raiz. OUs

Se essa for a primeira vez que você está criando uma política de configuração, é recomendável analisar primeiro Como as políticas de configuração funcionam no Security Hub CSPM.

Escolha seu método de acesso preferido e siga as etapas para criar e associar uma política de configuração ou uma configuração autogerenciada. Ao usar o console CSPM do Security Hub, você pode associar uma configuração a várias contas ou OUs ao mesmo tempo. Ao usar a API CSPM 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 CSPM desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Os outros controles que você escolher habilitar por meio de uma política de configuração serão habilitados em todas as regiões em que estiverem 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.
> Se um controle ativado que envolve recursos globais não for suportado na região de origem, o Security Hub CSPM tentará habilitar o controle em uma região vinculada onde o controle é suportado. Com a configuração central, você não tem cobertura para um controle que não está disponível na região de origem ou em qualquer uma das regiões vinculadas.
> Para obter uma lista dos controles que envolvem recursos globais, consulte Controles que usam recursos globais.

Security Hub CSPM console

Para criar e associar políticas de configuração

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.

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 CSPM AWS recomendada do Security Hub em toda a minha organização para usar nossa política recomendada. A política recomendada ativa o CSPM do 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 ativar ou desativar o CSPM do Security Hub, quais padrões ativar e quais controles ativar 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 ou a raiz às quais você deseja que sua política de configuração se aplique. OUs

   - Escolha Todas as contas se quiser aplicar a política de configuração à raiz. Isso inclui todas as contas e OUs na organização que não têm outra política aplicada ou herdada.
   - Escolha Contas específicas se quiser aplicar a política de configuração a contas específicas ou OUs. Insira a conta IDs ou selecione as contas e a OUs partir da estrutura organizacional. Você pode aplicar a política a um máximo de 15 alvos (contas ou raiz) ao criá-la. OUs Para especificar um número maior, edite a política após criá-la e aplique-a aos alvos 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 OUs secundárias e os alvos

aplicados herdarão automaticamente essa política de configuração, a menos que sejam especificamente excluídas, autogerenciadas ou usem uma política de configuração diferente.

Security Hub CSPM API

Para criar e associar políticas de configuração

1. Invoque a CreateConfigurationPolicyAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
2. Em `Name`, insira um nome exclusivo para a política de configuração. Opcionalmente, em `Description`, forneça uma descrição para a política de configuração.
3. Para o `ServiceEnabled` campo, especifique se você deseja que o CSPM do Security Hub seja ativado ou desativado nessa política de configuração.
4. Para o `EnabledStandardIdentifiers` campo, especifique quais padrões CSPM do Security Hub você deseja habilitar nessa 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 CSPM. Somente controles selecionados oferecem suporte a valores de parâmetros personalizados. Para obter mais informações, consulte Entendendo os parâmetros de controle no Security Hub CSPM.
7. Para aplicar sua política de configuração às contas ou OUs, invocar a StartConfigurationPolicyAssociationAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
8. No campo `ConfigurationPolicyIdentifier`, forneça o nome do recurso da Amazon (ARN) ou o identificador único universal (UUID) da política. O ARN e o UUID são retornados

pela API `CreateConfigurationPolicy`. Para uma configuração autogerenciada, o campo `ConfigurationPolicyIdentifier` 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 secundárias e OUs do alvo selecionado herdarão automaticamente essa 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 create-configuration-policycomando a partir da conta de administrador delegado CSPM do Security Hub na região de origem.
2. Em `name`, insira um nome exclusivo para a política de configuração. Opcionalmente, em `description`, forneça uma descrição para a política de configuração.
3. Para o `ServiceEnabled` campo, especifique se você deseja que o CSPM do Security Hub seja ativado ou desativado nessa política de configuração.
4. Para o `EnabledStandardIdentifiers` campo, especifique quais padrões CSPM do Security Hub você deseja habilitar nessa 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 CSPM. Somente controles selecionados oferecem suporte a valores

de parâmetros personalizados. Para obter mais informações, consulte Entendendo os parâmetros de controle no Security Hub CSPM.

7. Para aplicar sua política de configuração às contas ou OUs, execute o start-configuration-policy-associationcomando na conta de administrador delegado CSPM do Security Hub na região de origem.
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 Revisar o status da associação de uma política de configuração.

Analisando o status e os detalhes das políticas de configuração

O administrador delegado do CSPM do AWS Security Hub pode visualizar as políticas de configuração de uma organização e seus detalhes. Isso inclui a quais contas e unidades organizacionais (OUs) uma política está associada.

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

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

Security Hub CSPM console

Para visualizar políticas de configuração (console)

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas para ter uma visão geral das políticas de configuração.
4. Selecione uma política de configuração e escolha Exibir detalhes para ver detalhes adicionais sobre ela, incluindo a quais contas OUs ela está associada.

Security Hub CSPM API

Para ver uma lista resumida de todas as suas políticas de configuração, use a ListConfigurationPoliciesoperação da API CSPM do Security Hub. Se você usar o AWS CLI, execute o list-configuration-policiescomando. A conta delegada do administrador CSPM do Security Hub deve invocar a operação na região de origem.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
```

```
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Para visualizar detalhes sobre uma política de configuração específica, use a operação GetConfigurationPolicy. Se você usar o AWS CLI, execute get-configuration-policyo. O administrador delegado deve invocar a operação na região inicial. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração cujos detalhes você deseja visualizar.

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

Para visualizar uma lista resumida de todas as suas políticas de configuração e suas associações de conta, use a operação ListConfigurationPolicyAssociations. Se você usar o AWS CLI, execute o list-configuration-policy-associationscomando. O administrador delegado deve invocar a operação na 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 list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Para visualizar as associações de uma conta específica, use a operação GetConfigurationPolicyAssociation. Se você usar o AWS CLI, execute o get-configuration-policy-associationcomando. O administrador delegado deve invocar a operação na região inicial. Em `target`, forneça o número da conta, ID da OU ou ID da raiz.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Revisar o status da associação de uma política de 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 está em um estado de sucesso ou falha para uma conta específica. Pode demorar até 24 horas para que o status mude de `PENDING` para `SUCCESS` ou `FAILED`. Um status de `SUCCESS` significa que todas as configurações especificadas na política de configuração estão associadas à conta. Um status de `FAILED` significa que uma ou mais configurações especificadas na política de configuração não foram associadas à conta. Apesar do `FAILED` status, a conta pode ser parcialmente configurada de acordo com a política. Por exemplo, você pode tentar associar uma conta a uma política de configuração que habilite o CSPM do Security Hub, habilite as melhores práticas de segurança AWS básicas e desabilite .1. CloudTrail As duas configurações iniciais podem ser bem-sucedidas, mas a configuração CloudTrail .1 pode falhar. Neste exemplo, o status da associação é `FAILED` mesmo que algumas configurações tenham sido definidas corretamente.

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` depende do status de associação da política em todas as regiões relevantes. 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 CSPM replicará suas associações existentes que estão em um `FAILED` estado `PENDINGSUCCESS`, ou na nova região.

Mesmo quando o status da associação é`SUCCESS`, o status de habilitação de um padrão que faz parte da política pode passar para um estado incompleto. Nesse caso, o Security Hub CSPM não pode gerar descobertas para os controles do padrão. Para obter mais informações, consulte Verificando o status de um padrão.

Solução de problemas de falha de associação

No AWS Security Hub CSPM, uma associação de política de configuração pode falhar pelos seguintes motivos comuns.

- 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 CSPM do AWS Security Hub ativado. Isso torna a conta de gerenciamento uma conta-membro na organização.
- AWS Config não está habilitado ou configurado corretamente — Para habilitar padrões em uma política de configuração, AWS Config ela 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 às contas de destino e OUs quando estiver conectado à conta de administrador delegada do CSPM do Security Hub.
- É necessário associar a partir da região de origem — Você só pode associar uma política às contas de destino e OUs quando estiver conectado à sua região de origem.
- 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

Depois de criar uma política de configuração, a conta delegada do administrador CSPM do AWS Security Hub pode atualizar os detalhes da política e as associações de políticas. Quando os detalhes da política são atualizados, as contas associadas à política de configuração começam automaticamente a usar a política atualizada.

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

O administrador delegado pode atualizar as seguintes configurações de política:

- Ative ou desative o Security Hub CSPM.
- Habilitar um ou mais padrões de segurança.
- Indicar quais controles de segurança estão habilitados dentre todos os padrões habilitados. Você pode fazer isso fornecendo uma lista de controles específicos que devem ser habilitados, e o Security Hub CSPM desativa todos os outros controles, incluindo novos controles quando eles são lançados. Como alternativa, você pode fornecer uma lista de controles específicos que devem ser desativados, e o Security Hub CSPM habilita todos os outros controles, incluindo novos controles quando eles são 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.

> **Note**
>
> Se você usar a configuração central, o Security Hub CSPM desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Os outros controles que você escolher habilitar por meio de uma política de configuração serão habilitados em todas as regiões em que estiverem 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.
>
> Se um controle ativado que envolve recursos globais não for suportado na região de origem, o Security Hub CSPM tentará habilitar o controle em uma região vinculada onde o controle é suportado. Com a configuração central, você não tem cobertura para um controle que não está disponível na região de origem ou em qualquer uma das regiões vinculadas.

Para obter uma lista dos controles que envolvem recursos globais, consulte Controles que usam recursos globais.

Console

Para atualizar políticas de configuração

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
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. Você pode associar ou desassociar a política a um máximo de 15 alvos (contas ou raiz) ao atualizá-la. OUs
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 UpdateConfigurationPolicyAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
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 StartConfigurationPolicyAssociationAPI da conta de administrador delegado CSPM do Security Hub na região de origem. Para remover uma ou mais associações atuais, invoque a StartConfigurationPolicyDisassociationAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
5. No campo `ConfigurationPolicyIdentifier`, forneça o ARN ou o ID da política de configuração cujas associações você deseja atualizar.
6. Para o `Target` campo, forneça as contas ou o ID raiz que você deseja associar ou desassociar. OUs Essa ação substitui associações de políticas anteriores para as contas OUs especificadas.

> **Note**
>
> Quando você invoca a `UpdateConfigurationPolicy` API, o Security Hub CSPM executa uma substituição completa da lista para os `EnabledStandardIdentifiers` campos, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, 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 update-configuration-policycomando na conta de administrador delegado CSPM do Security Hub na região de origem.
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 para essa política de configuração, execute o start-configuration-policy-associationcomando na conta de administrador delegado CSPM do Security Hub na região de origem. Para remover uma ou mais associações atuais, execute o

start-configuration-policy-disassociationcomando na conta de administrador delegado CSPM do Security Hub na região de origem.

5. No campo `configuration-policy-identifier`, forneça o ARN ou o ID da política de configuração cujas associações você deseja atualizar.
6. Para o `target` campo, forneça as contas ou o ID raiz que você deseja associar ou desassociar. OUs Essa ação substitui associações de políticas anteriores para as contas OUs especificadas.

> **Note**
>
> Quando você executa o `update-configuration-policy` comando, o Security Hub CSPM executa uma substituição completa da lista dos `EnabledSecurityControlIdentifiers` campos`EnabledStandardIdentifiers`,`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 Revisar o status da associação de uma política de configuração.

Exclusão de políticas de configuração

Depois de criar uma política de configuração, o administrador delegado do CSPM do AWS Security Hub pode excluí-la. Como alternativa, o administrador delegado pode manter a política, mas desassociá-la de contas ou unidades organizacionais específicas (OUs) ou da raiz. Para obter instruções para desassociar uma política, consulte Desassociar uma configuração dos seus alvos.

Para obter informações contextuais sobre os benefícios da configuração central e como ela funciona, consulte Entendendo a configuração central no Security Hub CSPM.

Esta seção explica como excluir políticas de configuração.

Quando você exclui uma política de configuração, ela deixa de existir para sua organização. As contas de OUs destino e a raiz da organização não podem 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.

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 deve desassociar a política de qualquer conta ou da raiz à qual ela se aplica atualmente. OUs

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 CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/

Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.

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 alguma conta ou OUs se você for solicitado a primeiro desassociar a política desses alvos antes de excluí-la.
4. Revise a mensagem de confirmação. Insira **`confirm`** e escolha Excluir.

API

Para excluir uma política de configuração

Invoque a DeleteConfigurationPolicyAPI da conta de administrador delegado CSPM do Security Hub na região de origem.

Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja excluir. Se você receber um `ConflictException` erro, a política de configuração ainda se aplica às contas ou OUs à 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 delete-configuration-policycomando a partir da conta de administrador delegado CSPM do Security Hub na região de origem.

Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja excluir. Se você receber um `ConflictException` erro, a política de configuração ainda se

aplica às contas ou OUs à 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"
```

Desassociar uma configuração dos seus alvos

Na conta delegada do administrador CSPM do AWS Security Hub, você pode desassociar uma política de configuração ou configuração autogerenciada de uma conta, UO ou raiz. A desassociação retém a política para uso futuro, mas remove as associações existentes de contas específicas ou da raiz. Você pode desassociar somente uma configuração aplicada diretamente OUs, não 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. Para obter instruções sobre como excluir uma política de configuração, consulte Exclusão de políticas de configuração. 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 CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
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. Escolha 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 substitui as configurações existentes de qualquer conta ou OUs que esteja no escopo, se essas configurações entrarem em conflito com suas seleções atuais.

API

Para desassociar uma conta ou OU de sua configuração atual

1. Invoque a StartConfigurationPolicyDisassociationAPI da conta de administrador delegado CSPM do Security Hub na região de origem.
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. Para`Target`, forneça as contas ou a raiz que você deseja dissociar dessa política de configuração. OUs

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 start-configuration-policy-disassociationcomando a partir da conta de administrador delegado CSPM do Security Hub na região de origem.
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. Para`target`, forneça as contas ou a raiz que você deseja dissociar dessa política de configuração. OUs

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"}'
```

Configurando um padrão ou controle no contexto

Quando você usa a configuração central no CSPM do AWS Security Hub, o administrador delegado do CSPM do Security Hub pode criar políticas de configuração que especificam como o CSPM, os padrões de segurança e os controles de segurança do Security Hub são configurados para uma organização. O administrador delegado pode associar políticas a contas e unidades organizacionais (OU) específicas. As políticas entram em vigor na sua região de origem e em todas as regiões vinculadas. O administrador delegado pode atualizar as políticas de configuração conforme necessário.

No console CSPM do Security Hub, o administrador delegado pode atualizar as políticas de configuração de duas maneiras: na página Configuração ou no contexto dos fluxos de trabalho existentes. O último pode ser benéfico porque, ao visualizar as descobertas de segurança, você pode 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 CSPM do Security Hub. Programaticamente, o administrador delegado deve invocar a UpdateConfigurationPolicyoperação da API CSPM do Security Hub para alterar a forma como os padrões ou controles específicos são configurados na organização.

Siga estas etapas para configurar um padrão ou controle CSPM do Security Hub no contexto.

Para configurar um padrão ou controle no contexto (console)

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
2. No painel de navegação, escolha uma das seguintes opções:

   - Para configurar um padrão, escolha Padrões de segurança e escolha um padrão específico.
   - Para configurar um controle, escolha Controles e escolha um controle específico.
3. O console lista suas políticas de configuração CSPM existentes do Security Hub e o status do padrão ou controle selecionado em cada uma. Escolha as opções para ativar ou desativar o padrão ou o controle em cada política de configuração existente. Para controles, você também pode optar por personalizar os parâmetros de controle. Você não pode criar uma nova política durante a configuração no contexto. Para criar uma nova política, você deve acessar a página Configuração, escolher a guia Políticas e depois escolher Criar política.
4. Depois de fazer suas alterações, escolha Avançar.
5. Revise suas alterações e escolha Aplicar. As atualizações afetam todas as contas e OUs estão associadas a uma política de configuração alterada. As atualizações também entram em vigor na região de origem e em todas as regiões vinculadas.

Desabilitando a configuração central no Security Hub CSPM

Quando você desabilita a configuração central no CSPM do AWS Security Hub, o administrador delegado perde a capacidade de configurar o CSPM, os padrões de segurança e os controles de segurança do Security Hub em várias Contas da AWS unidades organizacionais () e. OUs Regiões da AWS Em vez disso, você deve definir a maioria das configurações de cada conta em cada região separadamente.

> **Important**
>
> Antes de desativar a configuração central, você deve primeiro desassociar suas contas e OUs da configuração atual, seja uma política de configuração ou um comportamento autogerenciado.
> Para poder desabilitar a configuração central, você também deve excluir as políticas de configuração existentes.

Quando você desabilita a configuração central, as seguintes alterações 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 de CSPM do Security Hub deve ser definida separadamente em cada conta da organização e região. O administrador delegado pode optar por habilitar automaticamente o CSPM do Security Hub, os padrões de segurança padrão e todos os controles que fazem parte dos padrões padrão nas novas contas da organização. Os padrões padrão são AWS Foundational Security Best Practices (FSBP) e 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 CSPM console

Para desabilitar a configuração central (console)

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
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 que são 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. Escolha Confirmar.

Security Hub CSPM API

Para desabilitar a configuração central (API)

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 quiser habilitar automaticamente o CSPM do Security Hub em novas contas da organização, defina o `AutoEnable` campo como. `true` Por padrão, o valor desse campo é`false`, e o CSPM do 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 desabilitar a configuração central (AWS CLI)

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 quiser habilitar automaticamente o CSPM do Security Hub em novas contas da organização, inclua o `auto-enable` parâmetro. Por padrão, o valor desse parâmetro éno-`auto-enable`, e o CSPM do 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"}'
```

Gerenciando contas de administrador e membro no Security Hub CSPM

Se o seu AWS ambiente tiver várias contas, você poderá tratar as contas que usam o CSPM do AWS Security Hub como contas de membros 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.

Você pode associar contas de membros a um administrador de duas maneiras: integrando o CSPM do Security Hub AWS Organizations ou enviando e aceitando manualmente convites de associação no CSPM do Security Hub.

Gerenciando contas com AWS Organizations

AWS Organizations é um serviço global de gerenciamento de contas que permite AWS aos administradores 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. É oferecido sem custo adicional e se integra a vários, incluindo AWS Security Hub CSPM Serviços da AWS, Amazon Macie e Amazon. GuardDuty Para obter mais informações, consulte o Guia do usuário do AWS Organizations .

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

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

A configuração central permite que o administrador delegado personalize o CSPM do Security Hub em várias contas e regiões da organização, em vez de configurar. Region-by-Region Você pode criar uma política de configuração para toda a organização ou criar políticas de configuração diferentes para contas e contas diferentes OUs. As políticas especificam se o CSPM do Security Hub está ativado ou desativado 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 optar pela configuração central, o administrador delegado tem uma capacidade mais limitada de configurar o CSPM do Security Hub, chamada de configuração local. Na configuração local, o administrador delegado pode habilitar automaticamente o CSPM do 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 CSPM 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 deve gerenciar manualmente as contas dos membros por convite no Security Hub CSPM 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 integrar AWS Organizations e usar a configuração central se você adicionar outras contas no futuro.

Ao usar o gerenciamento manual de contas, você designa uma conta para ser a administradora do CSPM 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 CSPM do Security Hub convida outras contas para serem contas membros, e a relação administrador-membro é estabelecida quando uma conta de 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 CSPM do Security Hub definindo configurações variáveis para contas diferentes. Em vez disso, cada conta da organização deve habilitar e configurar o CSPM do 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 CSPM. 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 no Security Hub CSPM.

Recomendações para gerenciar várias contas no Security Hub CSPM

A seção a seguir resume algumas restrições e recomendações que você deve ter em mente ao gerenciar contas de membros no CSPM do AWS Security Hub.

Número máximo de contas-membro

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

Criar relações administrador-membro

> **Note**
>
> Se você usa a integração do Security Hub CSPM com AWS Organizations, e não convidou manualmente nenhuma conta 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 de membro só pode ser associada a uma conta de administrador. Se uma conta da organização for habilitada pela conta de administrador do CSPM do Security Hub, a conta não poderá aceitar um convite de outra conta. Se uma conta já aceitou um convite, a conta não pode ser habilitada pela conta de administrador do CSPM 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.

Filiação por meio de AWS Organizations

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

Recomendamos que você escolha a mesma conta de DA em todas as regiões. Se você usar a configuração central, o CSPM do Security Hub definirá a mesma conta DA em todas as regiões nas quais você configura o CSPM do 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 de 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 do administrador deve habilitar o CSPM do 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.

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros.

Coordenar contas de administrador entre serviços

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

No entanto, os relacionamentos administrador-membro que você configura nesses outros serviços não se aplicam automaticamente ao CSPM do Security Hub. O Security Hub CSPM 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 CSPM do Security Hub, os usuários da conta A não verão automaticamente GuardDuty as descobertas das contas B e C no CSPM do Security Hub. Uma relação administrador-membro do Security Hub CSPM também é necessária para essas contas.

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

Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations

Você pode integrar o CSPM do AWS Security Hub com e AWS Organizations, em seguida, gerenciar o CSPM do Security Hub para contas em sua organização.

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

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

A conta de administrador delegado do Security Hub CSPM pode realizar as seguintes ações nas contas dos membros:

- Se estiver usando a configuração central, configure centralmente o CSPM do Security Hub para contas de membros e OUs criando políticas de configuração do CSPM do Security Hub. As políticas de configuração podem ser usadas para ativar e desativar o CSPM do Security Hub, ativar e desativar padrões e ativar e desativar controles.
- Trate automaticamente novas contas como contas membros do CSPM do Security Hub quando elas ingressam na 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.
- Trate as contas existentes da organização como contas de membros do CSPM 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, você pode associar uma política de configuração que desabilita o CSPM do Security Hub a contas de membros específicas gerenciadas centralmente.

Se você fizer a opção de usar a configuração central, sua organização usará um tipo de configuração padrão denominado configuração local. Na configuração local, o administrador delegado tem uma capacidade mais limitada de aplicar configurações nas contas-membro. Para obter mais informações, consulte Entendendo a configuração local no Security Hub CSPM.

Para obter uma lista completa das ações que o administrador delegado pode realizar nas contas dos membros, consulte Ações permitidas por contas de administrador e membro no CSPM do Security Hub.

Os tópicos desta seção explicam como integrar o CSPM do Security Hub com AWS Organizations e como gerenciar o CSPM do 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 CSPM com AWS Organizations
- Habilitando automaticamente o CSPM do Security Hub em novas contas da organização
- Habilitando manualmente o CSPM do Security Hub em novas contas da organização
- Desassociando contas de membros do CSPM do Security Hub da sua organização

Integrando o Security Hub CSPM com AWS Organizations

Para integrar o AWS Security Hub CSPM 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 CSPM do Security Hub. Isso habilita o Security Hub CSPM como um serviço confiável em Organizations. Ele também ativa o CSPM do Security Hub no atual Região da AWS para a conta do administrador delegado e permite que o administrador delegado habilite o CSPM do Security Hub para contas de membros, visualize dados em contas de membros e execute outras ações permitidas em contas de membros.

Se você usar a configuração central, o administrador delegado também poderá criar políticas de configuração do CSPM do Security Hub que especificam como o serviço, os padrões e os controles do CSPM 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 do SDK AWS CLI APIs ou de um deles. Para obter instruções detalhadas, consulte Criação de uma organização no Guia do usuário do AWS 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. Você pode organizar as contas em uma estrutura hierárquica em forma de árvore com uma raiz na parte superior e unidades organizacionais (OUs) aninhadas abaixo da raiz. Cada conta pode estar diretamente abaixo da raiz ou colocada em uma das da OUs 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 CSPM 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, recomendamos designar essa conta como administrador delegado do CSPM do Security Hub.

Embora o CSPM APIs e o console do Security Hub permitam que a conta de gerenciamento da organização seja o administrador delegado do CSPM do Security Hub, recomendamos escolher duas contas diferentes. 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 CSPM do 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 CSPM designará automaticamente o mesmo administrador delegado em sua região de origem e em qualquer região vinculada.

Verificar as permissões para configurar o administrador delegado

Para designar e remover uma conta delegada de administrador do Security Hub CSPM, a conta de gerenciamento da organização deve ter permissões para as ações `EnableOrganizationAdminAccount` e as ações no CSPM do `DisableOrganizationAdminAccount` 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 pelo CSPM do Security Hub ao diretor do IAM da conta de gerenciamento da organização:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Designar o administrador delegado

Para designar a conta delegada de administrador do Security Hub CSPM, você pode usar o console CSPM do Security Hub, a API CSPM do Security Hub ou. AWS CLI O CSPM do 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 CSPM definirá automaticamente o mesmo administrador delegado na região de origem e nas regiões vinculadas.

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

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

Você deve designar o administrador delegado do CSPM do Security Hub usando um dos métodos a seguir. A designação do administrador delegado do CSPM do Security Hub com Organizations APIs não se reflete no CSPM do Security Hub.

Escolha seu método preferido e siga as etapas para designar a conta delegada do administrador CSPM do Security Hub.

Security Hub CSPM console

Para designar o administrador delegado durante o onboarding

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

2. Escolha Ir para o Security Hub CSPM. Você será orientado a fazer login 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 na página Configurações

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação CSPM do Security Hub, escolha Configurações. Em seguida, escolha Geral.
3. Se uma conta de administrador do Security Hub CSPM estiver atualmente atribuída, antes de designar uma nova conta, você deverá remover a conta atual.

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

   Você deve designar a mesma conta de administrador CSPM 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. Selecione Delegar.

Security Hub CSPM API, AWS CLI

Na conta de gerenciamento da organização, use a EnableOrganizationAdminAccountoperação da API CSPM do Security Hub. Se você estiver usando a AWS CLI, execute o comando enable-organization-admin-account. Forneça a Conta da AWS ID do administrador delegado do CSPM do Security Hub.

O exemplo a seguir designa o administrador delegado do CSPM do Security Hub. 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 enable-organization-admin-account --admin-account-id 123456789012
```

Remover ou alterar o administrador delegado

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

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

> **Warning**
>
> Ao usar a configuração central, você não pode usar o console CSPM do Security Hub ou o CSPM do Security Hub APIs para alterar ou remover a conta do administrador delegado. Se a conta de gerenciamento da organização usar o AWS Organizations console ou AWS Organizations APIs para alterar ou remover o administrador delegado do CSPM do Security Hub, o Security Hub CSPM 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.

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

A API CSPM do Security Hub remove somente a conta delegada do administrador do CSPM 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 CSPM do Security Hub, ela será removida automaticamente em todas as regiões.

Removendo o administrador delegado (Organizations API, AWS CLI)

Você pode usar Organizations para remover o administrador delegado do CSPM 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 de administrador delegada do CSPM do Security Hub com. AWS Organizations

Organizations API, AWS CLI

Para remover o administrador delegado do CSPM do Security Hub

Na conta de gerenciamento da organização, use a operação DeregisterDelegatedAdministrator da API do Organizations. Se você estiver usando a AWS CLI, execute o comando deregister-delegated-administrator. Forneça o ID da conta do administrador delegado e o responsável pelo serviço principal do Security Hub CSPM, que é. `securityhub.amazonaws.com`

O exemplo a seguir remove o administrador delegado do CSPM do Security Hub. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

Removendo o administrador delegado (console CSPM do Security Hub)

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

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

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

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

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

1. Abra o console CSPM do AWS Security Hub 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 delegada de administrador CSPM do Security Hub da página Configurações

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação CSPM do Security Hub, escolha Configurações. Em seguida, escolha Geral.
3. Em Administrador delegado, escolha Remover.

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

Você pode usar a API CSPM do Security Hub ou as operações CSPM do Security Hub AWS CLI para remover o administrador delegado do CSPM 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 CSPM 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 CSPM com o Security Hub CSPM.

Security Hub CSPM API, AWS CLI

Para remover o administrador delegado do CSPM do Security Hub

Na conta de gerenciamento da organização, use a DisableOrganizationAdminAccountoperação da API CSPM do Security Hub. Se você estiver usando o AWS CLI, execute o disable-organization-admin-accountcomando. Forneça a ID da conta do administrador delegado do CSPM do Security Hub.

O exemplo a seguir remove o administrador delegado do CSPM do Security Hub. 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 disable-organization-admin-account --admin-account-id 123456789012
```

Desativando a integração do Security Hub CSPM com AWS Organizations

Depois que uma AWS Organizations organização é integrada ao CSPM do AWS Security Hub, a conta de gerenciamento do Organizations pode posteriormente desativar a integração. Como usuário da conta de gerenciamento do Organizations, você pode fazer isso desativando o acesso confiável ao CSPM do Security Hub em. AWS Organizations

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

- O Security Hub CSPM perde seu status de serviço confiável em. AWS Organizations
- A conta de administrador delegado do Security Hub CSPM perde o acesso às configurações, dados e recursos do CSPM do Security Hub para todas as contas membros do CSPM do Security Hub. Regiões da AWS
- Se você estava usando a configuração central, o Security Hub CSPM interrompe automaticamente o uso 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 de membros do Security Hub CSPM se tornam contas independentes e mantêm suas configurações atuais. Se o CSPM do Security Hub estiver habilitado para uma conta de membro em uma ou mais regiões, o CSPM do Security Hub continuará ativado 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 desativar o acesso confiável ao serviço para o Security Hub CSPM. Para obter detalhes sobre as permissões necessárias, consulte Permissões necessárias para desabilitar o acesso confiável no Guia do Usuário do AWS Organizations .

Antes de desativar o acesso confiável, recomendamos trabalhar com o administrador delegado da sua organização para desativar o CSPM do Security Hub nas contas dos membros e limpar os recursos do CSPM do Security Hub nessas contas.

Escolha seu método preferido e siga as etapas para desativar o acesso confiável ao Security Hub CSPM.

Organizations console

Para desativar o acesso confiável para o Security Hub CSPM

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

Organizations API

Para desativar o acesso confiável para o Security Hub CSPM

Invoque a operação Disable AWSService Access da AWS Organizations API. Para o `ServicePrincipal` parâmetro, especifique o principal de serviço CSPM do Security Hub ()`securityhub.amazonaws.com`.

AWS CLI

Para desativar o acesso confiável para o Security Hub CSPM

Execute o disable-aws-service-accesscomando da AWS Organizations API. Para o `service-principal` parâmetro, especifique o principal de serviço CSPM do Security Hub ()`securityhub.amazonaws.com`.

Exemplo:

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

Habilitando automaticamente o CSPM do Security Hub em novas contas da organização

Quando novas contas ingressam na sua organização, elas são adicionadas à lista na página Contas do console CSPM do AWS Security Hub. Para contas da organização, o Tipo é Por organização. Por padrão, novas contas não se tornam membros do CSPM 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 CSPM do 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 de adesão opcional neste documento. Para habilitar automaticamente o CSPM do Security Hub em uma nova conta em uma região opcional, a conta deve ter essa região ativada primeiro. Apenas o proprietário da conta pode ativar a região de adesão opcional. 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 CSPM do Security Hub em contas novas e existentes da organização criando uma política de configuração na qual o CSPM do Security Hub esteja ativado. Em seguida, você pode associar a política à raiz da organização ou a unidades organizacionais específicas (OUs).

Se você associar uma política de configuração na qual o CSPM do Security Hub esteja habilitado a uma OU específica, o CSPM do Security Hub será habilitado automaticamente em todas as contas

(existentes e novas) que pertencem a essa OU. As novas contas que não pertencem à OU são autogerenciadas e não têm o CSPM do Security Hub ativado automaticamente. Se você associar uma política de configuração na qual o CSPM do Security Hub esteja habilitado à raiz, o CSPM do Security Hub será habilitado automaticamente em todas as contas (existentes e novas) que ingressam 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.

Habilitação automática de novas contas da organização (configuração local)

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

Depois de ativar a habilitação automática, os padrões de segurança também são habilitados automaticamente para as novas contas da região atual ao 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 sua organização ou habilitar padrões para contas selecionadas OUs, 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 CSPM do Security Hub em novas contas da organização. Essas instruções se aplicam somente se você usar a configuração local.

Security Hub CSPM console

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

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

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

Security Hub CSPM API

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

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

AWS CLI

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

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

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

Habilitando manualmente o CSPM do Security Hub em novas contas da organização

Se você não habilitar automaticamente o CSPM do Security Hub em novas contas da organização quando elas ingressarem na organização, você poderá adicionar essas contas como membros e habilitar o CSPM do Security Hub nelas manualmente depois que elas ingressarem na organização. Você também deve habilitar manualmente o CSPM do Security Hub, pois você Contas da AWS 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 CSPM do Security Hub em contas de membros e unidades organizacionais especificadas ()OUs. Você também pode ativar padrões e controles específicos nessas contas OUs e.

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

Você também não pode ativar o CSPM do Security Hub em uma conta atualmente suspensa. Se você tentar habilitar o serviço em uma conta suspensa, o status da conta mudará para Conta suspensa.

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

Para que o Security Hub CSPM 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 uma conta membro do CSPM do Security Hub.

Security Hub CSPM console

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

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

   Faça login usando as credenciais da conta do administrador delegado.
2. No painel de navegação CSPM 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 CSPM API

Para habilitar manualmente as contas da organização como membros do CSPM 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 CSPM 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"}]'
```

Desassociando contas de membros do CSPM do Security Hub da sua organização

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

> **Note**
>
> Se você usar a configuração central, a desassociação funcionará de forma diferente. Você pode criar uma política de configuração que desabilite o CSPM do Security Hub em uma ou mais contas de membros gerenciadas centralmente. Depois disso, essas contas ainda fazem parte da organização, mas não gerarão descobertas de CSPM 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 Conta da AWS e não é mais gerenciada pela integração do CSPM do Security Hub com. AWS Organizations

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

Security Hub CSPM console

Para desassociar uma conta-membro de uma organização

1. Abra o console CSPM do AWS Security Hub 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 CSPM API

Para desassociar uma conta-membro de uma organização

Invoque a API `DisassociateMembers` a partir da conta do administrador delegado. Você deve fornecer o 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 o 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, AWS CLI, ou 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 .

Gerenciando contas por convite no Security Hub CSPM

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

> **Note**
>
> Se você criar uma organização baseada em convites no CSPM do Security Hub, poderá posteriormente fazer a transição para o uso em vez disso. AWS Organizations Se você tiver mais de uma conta de membro, recomendamos usar AWS Organizations em vez dos convites do CSPM do Security Hub para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com 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. Porém, 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 CSPM do 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 compatíveis com contas-membro convidadas manualmente. Em vez disso, você deve definir as configurações de CSPM 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 CSPM do Security Hub. A conta de administrador do Security Hub CSPM deve enviar convites para contas pertencentes a outras organizações.

Na página Configuração do console CSPM do Security Hub, as contas que foram adicionadas por convite são listadas na guia Contas de convite. Se você usa a configuração central, mas também convida contas fora da sua organização, você pode ver as descobertas das contas baseadas em convites nesta guia. No entanto, o administrador do CSPM 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 de membros no Security Hub CSPM
- Respondendo a um convite para ser uma conta membro do CSPM do Security Hub

- Desassociando contas de membros no Security Hub CSPM
- Excluindo contas de membros no Security Hub CSPM
- Desassociando-se de uma conta de administrador do CSPM do Security Hub
- Fazendo a transição para Organizations para gerenciar contas no Security Hub CSPM

Adicionar e convidar contas de membros no Security Hub CSPM

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

Sua conta se torna a administradora do CSPM do AWS Security Hub para contas que aceitam seu convite para se tornarem uma conta membro do CSPM do Security Hub.

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 de membro.
2. A conta de administrador envia um convite para a conta de membro.
3. A conta-membro aceita o convite.

Adicionar contas-membro

No console CSPM do Security Hub, você pode adicionar contas à sua lista de contas de membros. No console CSPM do Security Hub, você pode selecionar contas individualmente ou carregar um `.csv` arquivo que contenha as informações da conta.

Para cada conta, você deve fornecer a ID da conta e um endereço de email. O endereço de e-mail deve ser o endereço de e-mail 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 CSPM console

Para adicionar contas à sua lista de contas-membro

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

   Faça login usando as credenciais da conta de administrador.
2. No painel esquerdo, escolha Settings (Configurações).
3. Na página Configurações, selecione Contas e em seguida Adicionar contas. Em seguida, você pode adicionar contas individualmente ou fazer upload de um arquivo `.csv`contendo 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 e-mail 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 de membro, primeiro crie o arquivo. O arquivo deve conter o ID da conta e o endereço de e-mail 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 a conta IDs 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 CSPM 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"}]'
```

Convidar contas de membros

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 CSPM console

Para convidar contas-membro em potencial

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

Faça login usando as credenciais da conta de administrador.

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 CSPM 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"
```

Respondendo a um convite para ser uma conta membro do CSPM do Security Hub

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

Você pode aceitar ou recusar um convite para ser uma conta membro do CSPM do AWS Security Hub.

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

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

Você pode aceitar apenas um convite para ser uma conta de membro.

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

Lembre-se de que todas as contas CSPM 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

Você pode enviar um convite para ser uma conta membro do CSPM do Security Hub a partir da conta de administrador. Em seguida, após fazer login na conta-membro, você pode aceitar o convite.

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

Security Hub CSPM console

Para aceitar um convite para se tornar membro

1. Abra o console CSPM do AWS Security Hub 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 CSPM 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 CSPM do Security Hub continua sendo usado. `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

Você pode recusar um convite para ser uma conta membro do CSPM do Security Hub. Quando você recusa um convite no console CSPM do Security Hub, sua conta é marcada como Resignada na lista de contas membros da conta do administrador. O status Resignado aparece somente quando você entra no console CSPM do Security Hub usando a conta de administrador. Porém, o convite permanece inalterado no console da conta-membro até você fazer login na conta do administrador e excluir o convite.

Para recusar um convite, você deve fazer login na conta-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 CSPM console

Para recusar um convite para se tornar membro

1. Abra o console CSPM do AWS Security Hub 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 CSPM 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"
```

Desassociando contas de membros no Security Hub CSPM

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

Uma conta de administrador do AWS Security Hub CSPM 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 de membro, ela permanece na sua lista de contas de membros com o status de Removida (Desassociada). Sua conta é removida das informações da conta do administrador da conta de membro.

Para continuar recebendo as descobertas da conta, você pode 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 CSPM console

Para desassociar uma conta-membro convidada manualmente

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

   Faça login usando as credenciais da conta de administrador.
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 CSPM API

Para desassociar uma conta-membro convidada manualmente

Invoque a API `DisassociateMembers` a partir da conta do administrador. Você deve fornecer as contas Conta da AWS IDs dos membros que 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 as contas Conta da AWS IDs dos membros que 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"
```

Excluindo contas de membros no Security Hub CSPM

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

Como conta de administrador do AWS Security Hub CSPM, 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 CSPM console

Para excluir uma conta-membro manualmente convidada

1. Abra o console CSPM do AWS Security Hub 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 CSPM API

Para excluir uma conta-membro manualmente convidada

Invoque a API `DeleteMembers` a partir da conta do administrador. Você deve fornecer as contas Conta da AWS IDs dos membros 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 as contas Conta da AWS IDs dos membros 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 de uma conta de administrador do CSPM do Security Hub

> **Note**
>
> Recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

Se sua conta foi adicionada como uma conta de membro do CSPM do AWS Security Hub por convite, você pode desassociar a conta de membro da conta de administrador. Depois de desassociar uma conta de membro, o CSPM do 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 CSPM do Security Hub pode desassociar contas de membros que são gerenciadas com 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 CSPM console

Para se dissociar da sua conta de administrador

1. Abra o console CSPM do AWS Security Hub 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 CSPM 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 CSPM do Security Hub continua sendo usado. `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`.

Fazendo a transição para Organizations para gerenciar contas no Security Hub CSPM

Ao gerenciar contas manualmente no CSPM do AWS Security Hub, você deve convidar contas de membros em potencial e configurar cada conta de membro separadamente em cada uma. Região da AWS

Ao integrar o Security Hub CSPM e AWS Organizations, você pode eliminar a necessidade de enviar convites e obter mais controle sobre como o CSPM do Security Hub é configurado e personalizado em sua organização. Por esse motivo, recomendamos usar, AWS Organizations em vez dos convites de CSPM do Security Hub, para gerenciar suas contas de membros. Para mais informações, consulte Gerenciando o CSPM do Security Hub para várias contas com AWS Organizations.

É possível usar uma abordagem combinada na qual você usa a AWS Organizations integração, mas também convida manualmente contas fora da sua organização. Entretanto, recomendamos usar

exclusivamente a integração do Organizations. A configuração central, um recurso que ajuda você a gerenciar o CSPM do 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.

Integrando o Security Hub CSPM com AWS Organizations

Primeiro, você deve integrar o Security Hub CSPM e. 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 .
- Na conta de gerenciamento do Organizations, designe uma conta de administrador delegado CSPM 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 CSPM com AWS Organizations.

Ao concluir as etapas anteriores, você concede acesso confiável ao CSPM do Security Hub em. AWS Organizations Isso também ativa o CSPM do Security Hub na conta atual Região da AWS do administrador delegado.

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

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

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

Ações permitidas por contas de administrador e membro no CSPM do Security Hub

As contas de administrador e membro têm acesso às ações CSPM do AWS Security Hub anotadas 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 com a qual você se conectou).
- Traço: indica que a conta não pode realizar a ação.

Conforme observado nas tabelas, as ações permitidas diferem com base na integração 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 AWS Organizations.

O CSPM do Security Hub não copia as descobertas da conta do membro para a conta do administrador. No Security Hub CSPM, 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-membro 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.

As tabelas a seguir especificam as permissões padrão para contas de administrador e membro. Você pode usar políticas personalizadas do IAM para restringir ainda mais o acesso aos recursos e funções do CSPM do Security Hub. Para obter orientação e exemplos, consulte a postagem do blog Alinhando as políticas do IAM às personas dos usuários do AWS Security Hub CSPM.

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

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

Ação	Conta de administrador delegada CSPM do Security Hub	Conta-membro gerenciada centralmente	Conta-membro autogerenciada
Criar e gerenciar políticas de configuração CSPM do Security Hub	Para contas gerenciadas automaticamente e centralmente	–	–
Visualizar contas da organização	Any	–	–
Desassociar conta de membro	Any	–	–
Excluir conta-membro	Qualquer conta que não seja da organização	–	–
Desativar o CSPM do Security Hub	Para a conta atual e contas gerenciadas centralmente	–	Atual (deve primeiro ser desassociada da conta de administrador)
Veja as descobertas e o histórico de descobertas	Any	Atual	Atual
Atualizar as descobertas	Any	Atual	Atual
Visualizar resultados do insight	Any	Atual	Atual
Visualizar detalhes do controle	Any	Atual	Atual

Ação	Conta de administrador delegada CSPM do Security Hub	Conta-membro gerenciada centralmente	Conta-membro autogerenciada
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
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 membro podem acessar as ações do CSPM do Security Hub da seguinte forma se você se integrar ao Organizations e usar a configuração local.

Ação	Conta de administrador delegada CSPM do Security Hub	Conta-membro
Criar e gerenciar políticas de configuração CSPM do Security Hub	–	–
Visualizar contas da organização	Any	–
Desassociar conta de membro	Any	–
Excluir conta-membro	–	–
Desativar o CSPM do 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
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

Ação	Conta de administrador delegada CSPM do Security Hub	Conta-membro
Ative automaticamente o CSPM e os padrões padrão do Security Hub 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 membro podem acessar as ações do CSPM do Security Hub da seguinte forma se você usar o método baseado em convite para gerenciar contas manualmente em vez de integrá-las com. AWS Organizations

Ação	Conta de administrador do Security Hub CSPM	Conta-membro
Criar e gerenciar políticas de configuração CSPM do Security Hub	–	–

Ação	Conta de administrador do Security Hub CSPM	Conta-membro
Visualizar contas da organização	Any	–
Desassociar conta de membro	Any	Atual
Excluir conta-membro	Any	–
Desativar o CSPM do 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
Ative automaticamente o CSPM e os padrões padrão do Security Hub em novas contas da organização	–	–
Habilitar e desabilitar controles	Atual	Atual
Habilitar e desabilitar integrações	Atual	Atual

Ação	Conta de administrador do Security Hub CSPM	Conta-membro
Configurar uma agregação entre regiões	Any	–
Configurar ações personalizadas	Atual	Atual
Configurar regras de automação	Any	–
Configurar insights personalizados	Atual	Atual

Efeito das ações da conta nos dados CSPM do Security Hub

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

CSPM do Security Hub desativado

Se você usar a configuração central, o administrador delegado (DA) poderá criar políticas de configuração do CSPM do Security Hub que desabilitem o CSPM do AWS Security Hub em contas e unidades organizacionais específicas (). OUs Nesse caso, o CSPM do Security Hub está desativado nas contas especificadas, OUs na sua região de origem e em qualquer região vinculada. Se você não usar a configuração central, deverá desativar o CSPM do Security Hub separadamente em cada conta e região em que o habilitou. Você não pode usar a configuração central se o CSPM do Security Hub estiver desativado na conta DA.

Nenhuma descoberta será gerada ou atualizada para a conta do administrador se o CSPM do Security Hub estiver desativado na conta do administrador. As descobertas arquivadas existentes são excluídas após 30 dias. As descobertas ativas existentes são 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 CSPM do Security Hub, incluindo ações personalizadas, insights e assinaturas de produtos de terceiros, são retidos por 90 dias.

Conta de membro desassociada da conta de administrador

Quando uma conta de membro é desassociada da conta de administrador, esta perde a permissão para visualizar as descobertas na conta de membro. No entanto, o Security Hub CSPM ainda está habilitado em ambas as contas.

Se você usar a configuração central, o DA não poderá configurar o CSPM do Security Hub para uma conta membro que esteja desassociada da conta 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, você poderá ter uma ação personalizada na conta do administrador usada como padrão de evento em uma EventBridge regra da Amazon. Entretanto, essa ação personalizada não pode ser usada na conta-membro.

Na lista de contas da conta de administrador do Security Hub CSPM, 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 CSPM do Security Hub perde a permissão para visualizar as descobertas na conta do membro. No entanto, o Security Hub CSPM ainda está habilitado em ambas as contas com as mesmas configurações que tinham antes da remoção.

Se você usar a configuração central, não poderá configurar o CSPM do 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 de contas da conta de administrador do Security Hub CSPM, uma conta removida tem o status Excluída.

A conta é suspensa

Quando um Conta da AWS é suspenso, a conta perde a permissão para visualizar suas descobertas no CSPM do Security Hub. Nenhuma descoberta é gerada ou atualizada para essa conta. A conta de administrador de uma conta suspensa pode ver as descobertas existentes da conta.

Para uma conta da organização, o status da conta de 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 reabilitada. Quando a conta é reativada, suas permissões de CSPM do Security Hub são restauradas. Se o status da conta de membro for Conta suspensa, a conta de administrador deverá habilitar a conta manualmente.

A conta é fechada

Quando um Conta da AWS é fechado, o Security Hub CSPM responde ao fechamento da seguinte forma.

Se a conta for uma conta de administrador do Security Hub CSPM, ela será removida como conta de administrador e todas as contas membros serão removidas. Se a conta for uma conta de membro, ela será desassociada e removida como membro da conta de administrador do CSPM do Security Hub.

O Security Hub CSPM retém as descobertas arquivadas existentes na conta por 30 dias. Para uma descoberta de controle, o cálculo de 30 dias é baseado no valor do `UpdatedAt` campo da descoberta. Para outro tipo de descoberta, o cálculo é baseado no valor do `ProcessedAt` campo `UpdatedAt` ou da descoberta, qualquer que seja a data mais recente. Ao final desse período de 30 dias, o Security Hub CSPM exclui permanentemente a descoberta da conta.

O Security Hub CSPM retém as descobertas ativas existentes na conta por 90 dias. Para uma descoberta de controle, o cálculo de 90 dias é baseado no valor do `UpdatedAt` campo da descoberta. Para outro tipo de descoberta, o cálculo é baseado no valor do `ProcessedAt` campo `UpdatedAt` ou da descoberta, qualquer que seja a data mais recente. Ao final desse período de 90 dias, o Security Hub CSPM exclui permanentemente a descoberta da conta.

Para retenção de longo prazo das descobertas existentes, você pode exportar as descobertas para um bucket do S3. Você pode fazer isso usando uma ação personalizada com uma EventBridge regra da Amazon. Para obter mais informações, consulte Usando EventBridge para resposta e remediação automatizadas.

> **Important**
>
> Para clientes em AWS GovCloud (US) Regions, faça backup e exclua os dados da apólice e outros recursos da conta antes de fechar sua conta. Você não terá acesso aos recursos e dados depois de fechar sua conta.

Para obter mais informações, consulte Fechar um Conta da AWS no Guia AWS Gerenciamento de contas de referência.

Entendendo a agregação entre regiões no Security Hub CSPM

> **Note**
>
> A região de agregação agora é denominada região inicial. Algumas operações da API CSPM do Security Hub ainda usam o termo antigo Região de agregação.

Ao usar a agregação entre regiões no AWS Security Hub CSPM, você pode agregar descobertas, encontrar atualizações, insights, controlar status de conformidade e pontuações de segurança de várias Regiões da AWS para uma única região de origem. Assim, você pode gerenciar todos esses dados na região inicial.

Suponha que você defina Leste dos EUA (Norte da Virgínia) como a região inicial 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.

> **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).

Se um controle estiver habilitado em uma região vinculada, mas desabilitado na região inicial, você poderá ver o status de conformidade do controle na região inicial, mas não poderá habilitar ou desabilitar esse controle na região inicial. A exceção é se você usar a configuração central. Se você usar a configuração central, o administrador delegado do CSPM do Security Hub poderá configurar controles na região de origem e nas regiões vinculadas da região de origem.

Se você definiu uma região inicial, as pontuações de segurança refletirão o status dos controles em todas as regiões vinculadas. Para ver as pontuações de segurança e os status de conformidade entre regiões, adicione as seguintes permissões à sua função do IAM que usa o CSPM do Security Hub:

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

Tipos de dados que são agregados

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

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

Além dos novos dados na lista anterior, o Security Hub CSPM também replica as atualizações desses dados entre as regiões vinculadas e a região de origem. As atualizações que ocorrem em uma região vinculada são replicadas na região inicial. As atualizações que ocorrem na região inicial são replicadas de volta para a região vinculada. Se houver atualizações conflitantes entre a região inicial e a região vinculada, a atualização mais recente será usada.

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

Na região inicial, a página Resumo fornece uma visão das descobertas ativas nas várias 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.

As pontuações de segurança da região inicial 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 Padrões de segurança da região inicial. 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 Reprovado nas páginas de detalhes dos padrões da região inicial. O número de verificações de segurança inclui descobertas de todas as regiões vinculadas.

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

É possível habilitar a agregação entre regiões sem que nenhuma região vinculada seja selecionada. Nesse caso, nenhuma replicação de dados ocorrerá.

Agregação para contas de administrador e contas-membro

Contas autônomas, contas-membro e contas de administrador podem configurar a agregação entre regiões. Se for configurada por um administrador, a presença da conta de administrador é essencial para que a agregação entre regiões funcione nas contas administradas. Se a conta de administrador for removida ou desassociada de uma conta-membro a agregação entre regiões será interrompida na conta de membro. Isso acontece mesmo que a conta tenha a agregação entre regiões habilitada antes que a relação de adminstrador-membro comece.

Quando uma conta de administrador habilita a agregação entre regiões, o CSPM do Security Hub replica os dados que a conta do administrador gera em todas as regiões vinculadas à região de origem. Além disso, o Security Hub CSPM 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 CSPM replica os dados que uma conta membro gera em todas as regiões vinculadas à região de origem.

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

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

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-membro convidada manualmente, o administrador deve convidar a conta na região inicial e em todas as regiões vinculadas para que a agregação entre regiões funcione. Além disso, a conta do membro deve ter o Security Hub CSPM ativado na região de origem e em todas as regiões vinculadas para que o administrador possa visualizar as descobertas da conta do membro. Se você não usa a região de origem para outros fins, pode desativar os padrões e integrações do CSPM do Security Hub nessa região para evitar cobranças.

Se você planejar usar a agregação entre regiões e tiver várias contas de administrador, recomendado as seguintes práticas:

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

> **Note**
>
> Para entender como a configuração central afeta a agregação entre regiões, consulte Efeito da configuração central na agregação entre regiões.

Efeito da configuração central na agregação entre regiões

A configuração central é um recurso opcional no AWS Security Hub CSPM que você pode usar se fizer a integração com o. AWS Organizations Se você usar a configuração central, a conta de administrador delegado poderá configurar o serviço, os padrões e os controles CSPM do Security Hub para contas e unidades organizacionais (OU) na organização. Para configurar contas e OUs, o administrador delegado cria políticas de configuração CSPM do Security Hub. As políticas de

configuração podem ser usadas para definir se o CSPM do Security Hub está ativado ou desativado e quais padrões e controles estão habilitados. O administrador delegado associa políticas de configuração a contas específicas ou à raiz (toda a organização). OUs

O administrador delegado pode criar e gerenciar políticas de configuração para a organização somente na região inicial. Além disso, as políticas de configuração têm efeito na região inicial 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. Para obter informações sobre agregação entre regiões, consulte Agregação entre regiões.

Para usar a configuração central, você deve designar uma região inicial. Ou então, você pode escolher uma ou mais regiões como regiões vinculadas. Você também pode escolher designar uma região inicial sem nenhuma 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 Entendendo a configuração central no Security Hub CSPM.

Habilitar a agregação entre regiões

> **Note**
>
> A região de agregação agora é denominada região inicial. Algumas operações da API CSPM do Security Hub ainda usam o termo antigo Região de agregação.

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

Para habilitar a agregação entre regiões, você cria um recurso CSPM do Security Hub chamado agregador de descoberta. O recurso agregador de descobertas especifica a região inicial e as regiões vinculadas (se for o caso).

Você não pode usar uma Região da AWS que esteja desativada por padrão como sua região de origem. Para obter uma lista de regiões desabilitadas por padrão, consulte Habilitar uma região no Referência geral da AWS.

Ao habilitar a agregação entre regiões, você escolhe se deseja especificar uma ou mais regiões vinculadas. Você também pode escolher se deseja vincular automaticamente novas regiões quando o CSPM do Security Hub começar a suportá-las e você tiver optado por elas.

Security Hub CSPM console

Habilitar a agregação entre regiões

1. Abra o console CSPM do AWS Security Hub 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 CSPM, escolha Configurações e, em seguida, Regiões.
4. Em Agregação de descoberta, escolha Configurar agregação de descoberta.

   Por padrão, a região inicial é definida como Região não de agregação.
5. Em Região de agregação, selecione a opção para designar a região atual como a região inicial.
6. Opcionalmente, em Regiões vinculadas, selecione as regiões das quais agregar dados.
7. Para agregar automaticamente dados de novas regiões na partição, pois o Security Hub CSPM os suporta e você opta por eles, selecione Link future Regions.
8. Escolha Salvar.

Security Hub CSPM API

Na região que você deseja usar como região de origem, use a `CreateFindingAggregator`operação da API CSPM do Security Hub. Se você usar o AWS CLI, execute o create-finding-aggregatorcomando.

Para `RegionLinkingMode`, selecione uma das seguintes opções:

- `ALL_REGIONS`— O Security Hub CSPM agrega dados de todas as regiões. O Security Hub CSPM também agrega dados de novas regiões à medida que eles são suportados, e você opta por usá-los.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— O Security Hub CSPM agrega dados de todas as regiões, exceto as regiões que você deseja excluir. O Security Hub CSPM também agrega dados de novas regiões à medida que eles são suportados, e você opta por usá-los. Use `Regions` para fornecer a lista de regiões a serem excluídas da agregação.
- `SPECIFIED_REGIONS`— O Security Hub CSPM agrega dados de uma lista selecionada de regiões. O Security Hub CSPM não agrega dados automaticamente de novas regiões. Use `Regions` para fornecer a lista de regiões das quais agregar.
- `NO_REGIONS`— O Security Hub CSPM não agrega dados porque você não seleciona nenhuma região vinculada.

O exemplo a seguir configura a agregação entre regiões. A região inicial é Leste dos EUA (Norte da Virgínia) . As regiões vinculadas são Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon). 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 create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Revisando as configurações de agregação entre regiões

> **Note**
>
> A região de agregação agora é denominada região inicial. Algumas operações da API CSPM do Security Hub ainda usam o termo antigo Região de agregação.

Você pode visualizar a configuração atual de agregação entre regiões no CSPM do AWS Security Hub a partir de qualquer um. Região da AWS A configuração inclui a região de origem, as regiões vinculadas (se houver) e se as novas regiões devem ser vinculadas automaticamente conforme o Security Hub CSPM as suporta.

As contas-membro também podem visualizar a agregação entre regiões que a conta de administrador configurou.

Escolha seu método preferido e siga as etapas para visualizar as configurações atuais de agregação entre regiões.

Security Hub CSPM console

Para visualizar as configurações de agregação entre regiões (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, escolha Configurações e depois escolha a guia Regiões.

Se a agregação entre regiões não estiver habilitada, a guia Regiões exibirá a opção de 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 inicial
- Se você deseja agregar automaticamente descobertas, insights, status de controle e pontuações de segurança de novas regiões que o Security Hub CSPM suporta e nas quais você opta
- A lista de regiões vinculadas (se alguma estiver selecionada)

Security Hub CSPM API

Para revisar as configurações de agregação entre regiões (API CSPM do Security Hub)

Use a `GetFindingAggregator`operação da API CSPM do Security Hub. Se você usar o AWS CLI, execute o get-finding-aggregatorcomando.

Quando fizer a solicitação, forneça o ARN do agregador de descobertas. Para obter o ARN do agregador de descobertas, use a operação `ListFindingAggregators` ou comando list-finding-aggregators.

O exemplo a seguir mostra as configurações de agregação entre regiões para o ARN do agregador de descobertas especificado. Esse exemplo é formatado para Linux, macOS ou Unix e usa o caractere barra invertida (\) de continuação de linha para melhorar a legibilidade

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Atualizar as configurações de agregação entre regiões

> **Note**
>
> A região de agregação agora é denominada região inicial. Algumas operações da API CSPM do Security Hub ainda usam o termo antigo Região de agregação.

Você pode atualizar suas configurações atuais de agregação entre regiões no CSPM do AWS Security Hub alterando as regiões vinculadas ou a região de origem atual. Você também pode alterar se deseja agregar automaticamente dados de novos Regiões da AWS dados nos quais o Security Hub CSPM é suportado.

Alterações na agregação entre regiões não são implementadas em uma região de adesão opcional até que você a habilite na sua 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 AWS Security Hub CSPM não remove nenhum dado agregado existente dessa região que esteja acessível na região de origem.

Você não pode usar os procedimentos de atualização desta seção para alterar a região inicial. Para alterar a região inicial, você deve fazer o seguinte:

1. Interrompa a agregação entre regiões. Para instruções, consulte the section called “Interromper a agregação”.
2. Altere para a região que você quer que seja a nova região inicial.

3. Habilitar a agregação entre regiões. Para instruções, consulte the section called “Habilitar a agregação”.

Você deve atualizar a configuração de agregação entre regiões na região inicial atual.

Security Hub CSPM console

Para alterar as regiões vinculadas

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

   Faça login na região de agregação atual.
2. No menu de navegação do Security Hub CSPM, escolha Configurações e, em seguida, selecione Regiões.
3. Em Agregação de descobertas, escolha Editar.
4. Em Regiões vinculadas, atualize as regiões vinculadas selecionadas.
5. Se necessário, altere se a opção Vincular regiões futuras estiver selecionada. Essa configuração determina se o Security Hub CSPM vincula automaticamente novas regiões à medida que adiciona suporte a elas e você opta por elas.
6. Escolha Salvar.

Security Hub CSPM API

Use a operação `UpdateFindingAggregator`. Se você usar o AWS CLI, execute o update-finding-aggregatorcomando. Para identificar o agregador de descoberta, você deve fornecer o ARN do agregador de descoberta. Para obter o ARN do agregador de localização, use `ListFindingAggregators`a operação list-finding-aggregatorsou o comando.

Se o modo de vinculação for `ALL_REGIONS_EXCEPT_SPECIFIED` ou `SPECIFIED_REGIONS`, você poderá alterar a lista de regiões excluídas ou incluídas. Se você quiser alterar o modo de vinculação de regiões para `NO_REGIONS`, não forneça uma lista de regiões.

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). Você deve fornecer uma lista de `Regions` que contenha Leste dos EUA (Ohio) e Oeste dos EUA (Oregon).

O exemplo a seguir atualiza a agregação entre regiões para as regiões selecionadas. O comando é executado na região inicial atual, que é Leste dos EUA (Norte da Virgínia). As regiões vinculadas são Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon). 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 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

> **Note**
>
> A região de agregação agora é denominada região inicial. Algumas operações da API CSPM do Security Hub ainda usam o termo antigo Região de agregação.

Se você não quiser que o AWS Security Hub CSPM agregue dados, você pode excluir seu agregador de descoberta. Como alternativa, você pode manter seu agregador de localização, mas não vincular nenhum Regiões da AWS à região de origem, atualizando o agregador existente para o modo de `NO_REGIONS` vinculação.

Para alterar a região inicial, você deve excluir o agregador de descobertas atual e criar outro.

Quando você exclui seu agregador de descoberta, o Security Hub CSPM para de agregar dados. Ele não remove nenhum dado agregado existente da região inicial.

Excluir o agregador de descobertas (console)

Você pode excluir o agregador de descobertas somente da região inicial atual.

Em regiões que não sejam a região de origem, o painel Encontrando agregação no console CSPM do Security Hub exibe uma mensagem informando que você deve editar a configuração na região de origem. Escolha essa mensagem para exibir um link e alternar para a região inicial.

Security Hub CSPM console

Para interromper a agregação entre regiões (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Certifique-se de ter feito login na região inicial atual.
3. No menu de navegação do Security Hub CSPM, 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. Escolha Confirmar.

Security Hub CSPM API

Use a `DeleteFindingAggregator`operação da API CSPM do Security Hub. Se você estiver usando o AWS CLI, execute o `delete-finding-aggregator`comando.

Para identificar o agregador de descobertas a ser excluído, forneça o ARN do agregador de descobertas. Para obter o ARN do agregador de descobertas, use a operação `ListFindingAggregators` ou comando `list-finding-aggregators`.

O exemplo a seguir exclui o agregador de descobertas. O comando é executado na região inicial atual, que é Leste dos EUA (Norte da Virgínia). 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 delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region us-east-1
```

Entendendo os padrões de segurança no Security Hub CSPM

No AWS Security Hub CSPM, um padrão de segurança é um conjunto de requisitos baseado em estruturas regulatórias, melhores práticas do setor ou políticas da empresa. Para obter detalhes

sobre os padrões que o Security Hub CSPM suporta atualmente, incluindo os controles de segurança que se aplicam a cada um, consulte o. Referência de padrões para o Security Hub CSPM

Quando você ativa um padrão, o Security Hub CSPM ativa automaticamente todos os controles que se aplicam ao padrão. Em seguida, o Security Hub CSPM executa verificações de segurança nos controles, o que gera descobertas do CSPM do Security Hub. Você pode desativar e depois reativar controles individuais conforme necessário. Você também pode desativar completamente um padrão. Se você desabilitar um padrão, o Security Hub CSPM interromperá a execução de verificações de segurança nos controles que se aplicam ao padrão. As descobertas não são mais geradas para os controles.

Além das descobertas, o Security Hub CSPM gera uma pontuação de segurança para cada padrão que você habilita. A pontuação é baseada no status dos controles que se aplicam ao padrão. Se você definir uma região de agregação, a pontuação de segurança de um padrão refletirá o status dos controles em todas as regiões vinculadas. Se você for o administrador do CSPM do Security Hub de uma organização, a pontuação reflete o status dos controles de todas as contas em sua organização. Para obter mais informações, consulte Calcular pontuações de segurança.

Para revisar e gerenciar padrões, você pode usar o console CSPM do Security Hub ou a API CSPM do Security Hub. No console, a página de padrões de segurança mostra todos os padrões de segurança que o Security Hub CSPM suporta atualmente. Isso inclui uma descrição de cada padrão e o status atual do padrão. Se você habilitar um padrão, também poderá usar essa página para acessar detalhes adicionais do padrão. Por exemplo, você pode revisar:

- A pontuação de segurança atual do padrão.
- Estatísticas agregadas para controles que se aplicam ao padrão.
- Uma lista de controles que se aplicam ao padrão e estão atualmente habilitados, incluindo o status de conformidade de cada um.
- Uma lista de controles que se aplicam ao padrão, mas estão atualmente desativados.

Para uma análise mais profunda, você pode filtrar e classificar os dados e detalhar para revisar os detalhes dos controles individuais que se aplicam ao padrão.

Você pode habilitar padrões individualmente para uma única conta Região da AWS e. No entanto, para economizar tempo e reduzir o desvio de configuração em ambientes com várias contas e várias regiões, recomendamos o uso da configuração central para habilitar e gerenciar padrões. Com a configuração central, o administrador delegado do CSPM do Security Hub pode criar políticas que especificam como configurar um padrão em várias contas e regiões.

Tópicos

Referência de padrões para o Security Hub CSPM

No AWS Security Hub CSPM, um padrão de segurança é um conjunto de requisitos baseado em estruturas regulatórias, melhores práticas do setor ou políticas da empresa. O Security Hub CSPM mapeia esses requisitos para controles e executa verificações de segurança nos controles para avaliar se os requisitos de um padrão estão sendo atendidos. Cada padrão inclui vários controles.

Atualmente, o Security Hub CSPM suporta os seguintes padrões:

- AWS Melhores práticas básicas de segurança — Desenvolvido por profissionais do setor AWS e por profissionais do setor, esse padrão é uma compilação das melhores práticas de segurança para organizações, independentemente do setor ou tamanho. Ele fornece um conjunto de controles que detectam quando seus recursos Contas da AWS e recursos se desviam das melhores práticas de segurança. Ele também fornece orientação prescritiva sobre como melhorar e manter sua postura de segurança.
- AWS Marcação de recursos — Desenvolvido pelo Security Hub CSPM, esse padrão pode ajudá-lo a determinar se seus AWS recursos têm tags. Uma tag é um par de valores-chave que atua como metadados para um recurso. AWS As tags podem ajudar você a identificar, categorizar, gerenciar e pesquisar AWS recursos. Por exemplo, você pode usar tags para categorizar recursos por finalidade, proprietário ou ambiente.
- CIS AWS Foundations Benchmark — Desenvolvido pelo Center for Internet Security (CIS), esse padrão fornece diretrizes de configuração segura para. AWS Ele especifica um conjunto de diretrizes de configuração de segurança e melhores práticas para um subconjunto de Serviços da AWS recursos, com ênfase em configurações básicas, testáveis e independentes de arquitetura. As diretrizes incluem procedimentos claros de step-by-step implementação e avaliação.
- NIST SP 800-53 Revisão 5 — Esse padrão se alinha aos requisitos do Instituto Nacional de Padrões e Tecnologia (NIST) para proteger a confidencialidade, integridade e disponibilidade de sistemas de informação e recursos críticos. A estrutura associada geralmente se aplica a

agências ou organizações federais dos EUA que trabalham com agências federais ou sistemas de informação dos EUA. No entanto, organizações privadas também podem usar os requisitos como uma estrutura orientadora.

- NIST SP 800-171 Revisão 2 — Esse padrão se alinha às recomendações e requisitos de segurança do NIST para proteger a confidencialidade de informações não classificadas controladas (CUI) em sistemas e organizações que não fazem parte do governo federal dos EUA. CUI são informações que não atendem aos critérios governamentais de classificação, mas são consideradas confidenciais e são criadas ou possuídas pelo governo federal dos EUA ou por outras entidades em nome do governo federal dos EUA.
- PCI DSS — Esse padrão está alinhado com a estrutura de conformidade do Payment Card Industry Data Security Standard (PCI DSS) definida pelo PCI Security Standards Council (SSC). A estrutura fornece um conjunto de regras e diretrizes para lidar com segurança com as informações do cartão de crédito e débito. A estrutura geralmente se aplica a organizações que armazenam, processam ou transmitem dados de titulares de cartões.
- Padrão gerenciado por serviços AWS Control Tower— Esse padrão ajuda você a configurar os controles proativos fornecidos AWS Control Tower junto com os controles de detetive fornecidos pelo Security Hub CSPM. AWS Control Tower oferece uma maneira simples de configurar e administrar um ambiente com AWS várias contas, seguindo as melhores práticas prescritivas. Ao habilitar controles proativos e detectivos para seu AWS ambiente, você pode aprimorar sua postura de segurança em diferentes estágios de desenvolvimento.

Os padrões e controles do Security Hub CSPM não garantem a conformidade com nenhuma estrutura regulatória ou auditoria. Em vez disso, eles fornecem uma maneira de avaliar e monitorar o estado de seus recursos Contas da AWS e de seus recursos. Recomendamos ativar cada padrão que seja relevante para suas necessidades comerciais, setor ou caso de uso.

Os controles individuais podem ser aplicados a mais de um padrão. Se você habilitar vários padrões, recomendamos que você também habilite descobertas de controle consolidadas. Se você fizer isso, o Security Hub CSPM gerará uma única descoberta para cada controle, mesmo que o controle se aplique a mais de um padrão. Se você não ativar as descobertas de controle consolidadas, o Security Hub CSPM gerará uma descoberta separada para cada padrão habilitado ao qual um controle se aplica. Por exemplo, se você habilitar dois padrões e um controle se aplicar a ambos, você receberá duas descobertas separadas para o controle, uma para cada padrão. Se você habilitar descobertas de controle consolidadas, receberá somente uma descoberta para o controle. Para obter mais informações, consulte Descobertas de controle consolidadas.

Referência detalhada por padrão

- AWS Padrão básico de melhores práticas de segurança no Security Hub CSPM
- AWS Padrão de marcação de recursos no Security Hub CSPM
- Referência do CIS AWS Foundations no Security Hub CSPM
- NIST SP 800-53 Revisão 5 no Security Hub CSPM
- NIST SP 800-171 Revisão 2 no Security Hub CSPM
- PCI DSS no Security Hub CSPM
- Padrões gerenciados de serviços no Security Hub CSPM

AWS Padrão básico de melhores práticas de segurança no Security Hub CSPM

Desenvolvido por profissionais do setor AWS e por profissionais do setor, o padrão AWS Foundational Security Best Practices (FSBP) é uma compilação das melhores práticas de segurança para organizações, independentemente do setor ou tamanho da organização. Ele fornece um conjunto de controles que detectam quando Contas da AWS e os recursos se desviam das melhores práticas de segurança. Ele também fornece orientação prescritiva sobre como melhorar e manter a postura de segurança da sua organização.

No AWS Security Hub CSPM, o padrão AWS Foundational Security Best Practices inclui controles que avaliam continuamente suas cargas de trabalho Contas da AWS e ajudam você a identificar áreas que se desviam das melhores práticas de segurança. 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 o controle se aplica. Para obter uma lista de categorias e detalhes adicionais, consulteCategorias de controle.

Controles que se aplicam ao padrão

A lista a seguir especifica quais controles CSPM do AWS Security Hub se aplicam ao padrão AWS Foundational Security Best Practices (v1.0.0). Para revisar os detalhes de um controle, escolha o controle.

[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS

[ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

[ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

[APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado

[APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

[APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado

[APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF

[APIGateway.5] Os dados do cache da API REST de Gateway devem ser criptografados em repouso

[APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização

[APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway

[AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso

[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

[AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API

[AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

[Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado

[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 em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 2 () IMDSv2

[Autoscaling.5] As instâncias da EC2 Amazon 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 da 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

[CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada

[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 habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs

[CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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

[CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso

[Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas

[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

[Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado

[DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso

[DataSync.1] DataSync as tarefas devem ter o registro ativado

[DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas

[DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

[DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

[DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado

[DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado

[DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado

[DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso

[DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

[DocumentDB.3] 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

[DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

[DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito

[DynamoDB.1] 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

[DynamoDB.3] 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 acelerador do DynamoDB devem ser criptografados em trânsito

[EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída

[EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso

[EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

[EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2

[EC2.9] EC2 As instâncias da Amazon não devem ter um endereço público IPv4

[EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2

[EC2.15] As EC2 sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos

[EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas

[EC2.17] EC2 As instâncias da Amazon não devem usar várias ENIs

[EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

[EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

[EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos

[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

[EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC

[EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados

[EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede

[EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado

[EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR

[EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry

[EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager

[EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts

[EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager

[EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2

[EC2.171] As conexões EC2 VPN devem ter o registro ativado

[EC2.172] As configurações do EC2 VPC Block Public Access devem bloquear o tráfego do gateway da Internet

[EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS

[EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada

[ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

[ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário

[ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

[ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host

[ECS.4] Os contêineres ECS devem ser executados sem privilégios

[ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz

[ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner

[ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log

[ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

[ECS.12] Os clusters do ECS devem usar Container Insights

[ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos

[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.3] Os pontos de acesso do EFS devem executar um diretório raiz

[EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário

[EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização

[EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados

[EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso

[EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público

[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

[EKS.3] Os clusters do 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 OSS) devem ter backups automáticos habilitados

[ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas

[ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado

[ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso

[ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito

[ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

[ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos

[ELB.5] O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado

[ELB.6] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada

[ELB.7] 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

[ELB.9] Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado

[ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade

[ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

[ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas

[ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito

[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

[EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso

[EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito

[ES.1] Os domínios do Elasticsearch devem ter a criptografia em repouso habilitada.

[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

[ES.3] 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.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

[ES.6] Os domínios do Elasticsearch devem ter pelo menos três nós de dados

[ES.7] 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] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes

[FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups

[FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ

[FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ

[FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ

[Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso

[Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue

[GuardDuty.1] GuardDuty deve ser ativado

[GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado

[GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada

[GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado

[GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado

[GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada

[GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada

[GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado

[GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado

[GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado

[IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do IAM 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 IAM 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

[IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

[Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2

[Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada

[Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada

[Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada

[Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso

[Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado

[KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

[KMS.2] 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

[KMS.5] As chaves do KMS não devem estar acessíveis ao público

[Lambda.1] As funções do Lambda.1 devem proibir o acesso público

[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis

[Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade

[Macie.1] O Amazon Macie deve estar habilitado

[Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada

[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch

[MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada

[MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

[MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito

[MSK.4] Os clusters MSK devem ter o acesso público desativado

[MSK.5] Os conectores MSK devem ter o registro ativado

[MSK.6] Os clusters MSK devem desativar o acesso não autenticado

[Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos

[Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada

[Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados

[Neptune.6] Os instantâneos do cluster 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

[Neptune.8] Os clusters de banco de dados do Neptune devem ser configurados para copiar tags para instantâneos

[NetworkFirewall.2] O registro em log do Network Firewall deve ser habilitado

[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 pacotes fragmentados.

[NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio

[NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada

[NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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

[Route53.2] 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 configuração PubliclyAccessible

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

[RDS.4] Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso

[RDS.5] As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade

[RDS.6] 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.8] As instâncias de banco de dados do RDS deve ter a proteção contra exclusão habilitada

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

[RDS.10] A autenticação do IAM deve ser configurada para instâncias do RDS

[RDS.11] As instâncias do RDS devem ter backups automáticos habilitados

[RDS.12] A autenticação do IAM deve ser configurada para clusters 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

[RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots

[RDS.17] As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos

[RDS.19] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

[RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados

[RDS.21] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

[RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados

[RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados

[RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

[RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

[RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso

[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

[RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

[RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch

[RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch

[RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch

[RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito

[RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch

[RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito

[RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado

[PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público

[Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

[Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

[Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

[Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas

[Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado

[Redshift.8] 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 somente na porta do cluster de origens restritas

[Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas

[RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC

[RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL

[RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público

[RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão

[RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch

[RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público habilitadas

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público para leitura

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público para gravação

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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 em log de acesso ao servidor habilitado

[S3.12] não ACLs deve ser usado 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

[S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas

[S3.25] Os buckets de diretório 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

[SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado

[SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis

[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.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público

[SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso

[SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público

[SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager

[SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch

[SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

[SSM.4] Os documentos SSM não devem ser públicos

[SSM.6] A automação de SSM deve ter o registro ativado CloudWatch

[SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada

[StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado

[Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints

[Transfer.3] Os conectores Transfer Family devem ter o registro ativado

[WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado

[WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição

[WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra

[WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras

[WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição

[WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra

[WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

[WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras

[WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch

[WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso

[WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

AWS Padrão de marcação de recursos no Security Hub CSPM

O padrão AWS Resource Tagging, desenvolvido pelo AWS Security Hub CSPM, ajuda você a determinar se seus AWS recursos não têm tags. As tags são pares de valores-chave que atuam como metadados para organizar recursos. AWS Com a maioria dos AWS recursos, você tem a

opção de adicionar tags a um recurso ao criar o recurso ou depois de criá-lo. Exemplos de recursos incluem CloudFront distribuições da Amazon, instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) e segredos em. AWS Secrets Manager As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar AWS 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, ou. `111122223333` `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 informações sobre como adicionar tags aos AWS recursos, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

Para cada controle que se aplica ao padrão AWS Resource Tagging no Security Hub CSPM, você pode, opcionalmente, usar o parâmetro suportado para especificar as chaves de tag que você deseja que o controle verifique. Se você não especificar nenhuma chave de tag, o controle verificará somente a existência de pelo menos uma chave de tag e falhará se um recurso não tiver nenhuma chave de tag.

Antes de ativar o padrão de marcação de AWS recursos, é importante primeiro ativar e configurar a gravação de recursos no AWS Config. Ao configurar o registro de recursos, certifique-se também de habilitá-lo para todos os tipos de AWS recursos que são verificados pelos controles que se aplicam ao padrão. Caso contrário, o Security Hub CSPM talvez não consiga avaliar os recursos apropriados e gerar descobertas precisas para os controles que se aplicam ao padrão. Para obter mais informações, incluindo uma lista dos tipos de recursos a serem registrados, consulte AWS Config Recursos necessários para descobertas de controle.

> **Note**
>
> O padrão AWS de marcação de recursos não está disponível no Oeste do Canadá (Calgary), na China e nas regiões. AWS GovCloud (US)

Depois de habilitar o padrão AWS Resource Tagging, você começa a receber descobertas de controles que se aplicam ao padrão. Observe que pode levar até 18 horas para que o Security Hub

CSPM gere descobertas para controles que usam a mesma regra AWS Config vinculada ao serviço que os controles que se aplicam a outros padrões habilitados. Para obter mais informações, consulte Programar a execução de verificações de segurança.

O padrão AWS de marcação de recursos 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 CSPM do Security Hub para encontrar o ARN de um padrão habilitado.

Controles que se aplicam ao padrão

A lista a seguir especifica quais controles CSPM do AWS Security Hub se aplicam ao padrão AWS Resource Tagging (v1.0.0). Para revisar os detalhes de um controle, escolha o controle.

- [ACM.3] Os certificados do ACM devem ser marcados
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.10] Grupos de 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
- [Batch.1] As filas de trabalhos em lote devem ser marcadas

- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas
- [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
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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
- [DynamoB.5] As tabelas do DynamoDB devem ser marcadas
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.35] interfaces EC2 de rede devem ser marcadas
- [EC2.36] os gateways EC2 do cliente devem ser marcados
- [EC2.37] Os endereços IP EC2 elásticos devem ser marcados
- [EC2.38] as EC2 instâncias devem ser marcadas
- [EC2.39] gateways de EC2 internet devem ser marcados
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.41] a EC2 rede ACLs deve ser marcada
- [EC2.42] tabelas de EC2 rotas devem ser marcadas
- [EC2.43] grupos EC2 de segurança devem ser marcados
- [EC2.44] EC2 sub-redes devem ser marcadas

- [EC2.45] EC2 volumes devem ser marcados
- [EC2.46] Amazon VPCs deve ser etiquetada
- [EC2.47] Os serviços de endpoint do Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento do Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de EC2 VPN devem ser marcados
- [EC2.52] gateways EC2 de trânsito devem ser marcados
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego 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 do 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 do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do EKS devem ser marcadas
- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [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] GuardDuty IPSets deve ser marcado

- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados

- [Lambda.6] As funções do Lambda devem ser marcadas
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [NetworkFirewall.7] Os firewalls do Network Firewall devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.28] Os clusters de bancos de dados do RDS devem ser marcados
- [RDS.29] Os snapshots de cluster de bancos de dados do RDS devem ser marcados
- [RDS.30] As instâncias de bancos de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.32] Os snapshots de banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes de banco de dados do RDS devem ser marcados
- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As notificações de assinatura de notificações eventos do Redshift devem ser marcadas
- [Redshift.13] Os snapshots de cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes de cluster do Redshift devem ser marcados
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens 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 do SQS devem ser marcadas
- [SSM.5] Os documentos SSM devem ser marcados
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.4] Os contratos da Transfer Family devem ser marcados

- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados

Referência do CIS AWS Foundations no Security Hub CSPM

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, os controles neste benchmark protegem os sistemas específicos que sua organização usa.

AWS O Security Hub CSPM oferece suporte às versões 3.0.0, 1.4.0 e 1.2.0 do CIS AWS Foundations Benchmark. Esta página lista os controles de segurança que cada versão suporta. Ele também fornece uma comparação das versões.

CIS AWS Foundations Benchmark versão 3.0.0

O Security Hub CSPM é compatível com a versão 3.0.0 (v3.0.0) do CIS Foundations Benchmark. AWS O Security Hub CSPM atendeu aos requisitos da Certificação de Software de Segurança CIS e recebeu a Certificação de Software de Segurança CIS pelos seguintes benchmarks do 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 versão 3.0.0

[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 habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3

[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

[EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2

[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

[EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor

[EC2.54] grupos EC2 de segurança 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 IAM 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 IAM 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.9] A MFA 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support

[IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas

[IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos

[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess

[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado

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 configuração PubliclyAccessible

[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 habilitadas

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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 em log os eventos de gravação ao nível do objeto

[S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto

CIS AWS Foundations Benchmark versão 1.4.0

O Security Hub CSPM é compatível com a versão 1.4.0 (v1.4.0) do CIS Foundations Benchmark. AWS

Controles que se aplicam ao CIS AWS Foundations Benchmark versão 1.4.0

[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 habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs

[CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente

[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3

CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”

[CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM

[CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do

[CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do

[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente

[CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3

[CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do

[CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança

[CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)

[CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede

[CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas

[CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC

[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

[IAM.1] As políticas do IAM 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 IAM 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.9] A MFA 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support

[IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias 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 habilitadas

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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

CIS AWS Foundations Benchmark versão 1.2.0

O Security Hub CSPM é compatível com a versão 1.2.0 (v1.2.0) do CIS Foundations Benchmark. AWS O Security Hub CSPM atendeu aos requisitos da Certificação de Software de Segurança CIS e recebeu a Certificação de Software de Segurança CIS pelos seguintes benchmarks do 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 versão 1.2.0

[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 habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs

[CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente

[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3

CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”

[CloudWatch.2] Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas

[CloudWatch.3] Certifique-se de que um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA

[CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM

[CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do

[CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do

[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente

[CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3

[CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do

[CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança

[CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)

[CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede

[CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas

[CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC

[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22

[EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389

[IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do IAM 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 IAM 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.8] As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.9] A MFA 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 um perfil de suporte tenha sido criado 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 as versões específicas do benchmark Center for Internet Security (CIS) AWS Foundations — v3.0.0, v1.4.0 e v1.2.0. AWS O Security Hub CSPM suporta cada uma dessas versões do CIS AWS Foundations Benchmark. No entanto, recomendamos usar a v3.0.0 para se manter atualizado com as melhores práticas de segurança. É possível habilitar várias versões do padrão ao mesmo tempo. Para obter informações sobre a habilitação de padrões, consulteHabilitar um padrão de segurança. Se você quiser atualizar para a v3.0.0, ative-a antes de desativar uma versão mais antiga. Isso evita falhas nas verificações de segurança. Se você usa a

integração CSPM do Security Hub AWS Organizations e deseja habilitar em lote a v3.0.0 em várias contas, recomendamos usar a configuração central.

Mapeamento de controles para os requisitos do CIS em cada versão

Entenda quais controles cada versão do CIS AWS Foundations Benchmark suporta.

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do 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.2] CloudTrail deve ter a criptografia em repouso habilitada	3.5	3.7	2.7
[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada	3.2	3.2	2.2
[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs	Não compatível: o CIS removeu esse requisito	3.4	2.4
[CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente	Não compatível: o CIS removeu esse requisito	3.3	2.3
[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3	3.4	3.6	2.6

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”	Não compatível: verificação manual	4.3	3.3
[CloudWatch.2] Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas	Não compatível: verificação manual	Não compatível: verificação manual	3.1
[CloudWatch.3] Certifique-se de que um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA	Não compatível: verificação manual	Não compatível: verificação manual	3.2
[CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM	Não compatível: verificação manual	4.4	3.4
[CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do	Não compatível: verificação manual	4.5	3.5
[CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do	Não compatível: verificação manual	4.6	3.6
[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente	Não compatível: verificação manual	4.7	3.7

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3	Não compatível: verificação manual	4.8	3.8
[CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do	Não compatível: verificação manual	4,9	3.9
[CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança	Não compatível: verificação manual	4.10	3.10
[CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)	Não compatível: verificação manual	4.11	3.11
[CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede	Não compatível: verificação manual	4.12	3.12
[CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas	Não compatível: verificação manual	4.13	3.13
[CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC	Não compatível: verificação manual	4.14	3,14

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos	3.3	3.5	2,5
[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída	5.4	5.3	4.3
[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs	3.7	3.9	2.9
[EC2.7] A criptografia padrão do EBS deve estar ativada	2.2.1	2.2.1	Não compatível
[EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2	5.6	Não compatível	Sem compatibilidade
[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22	Não compatível: substituído pelos requisitos 5.2 e 5.3	Não compatível: substituído pelos requisitos 5.2 e 5.3	4.1
[EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389	Não compatível: substituído pelos requisitos 5.2 e 5.3	Não compatível: substituído pelos requisitos 5.2 e 5.3	4.2
[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389	5.1	5.1	Não compatível

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administr ação remota do servidor	5.2	Não compatível	Sem compatibi lidade
[EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto	5.3	Não compatível	Sem compatibi lidade
[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS	2.4.1	Não compatível	Não compatível
[IAM.1] As políticas do IAM não devem permitir privilégios administr ativos completos "*"	Sem compatibi lidade	1.16	1,22
[IAM.2] Os usuários do IAM não devem ter políticas do IAM anexadas	1.15	Não compatível	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 IAM 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	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas	Não compatível: veja [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas em vez disso	Não compatível: veja [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas em vez disso	1.3
[IAM.9] A MFA 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 compatível: o CIS removeu esse requisito	Não compatível: 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 compatível: o CIS removeu esse requisito	Não compatível: o CIS removeu esse requisito	1.6
1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo	Não compatível: o CIS removeu esse requisito	Não compatível: o CIS removeu esse requisito	1,7
Certifique-se de que política de senha do IAM exija pelo menos um número	Não compatível: o CIS removeu esse requisito	Não compatível: 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	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do 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 compatível: o CIS removeu esse requisito	Não compatível: o CIS removeu esse requisito	1.11
[IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support	1.17	1.17	1.2
[IAM.20] Evite o uso do usuário raiz	Não compatível: o CIS removeu esse requisito	Não compatível: o CIS removeu esse requisito	1.1
[IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas	1.12	1.12	Não compatível: o CIS adicionou esse requisito em versões posteriores
[IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos	1,19	Não compatível: o CIS adicionou esse requisito em versões posteriores	Não compatível: o CIS adicionou esse requisito em versões posteriores
[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess	1,22	Não compatível: o CIS adicionou esse requisito em versões posteriores	Não compatível: o CIS adicionou esse requisito em versões posteriores

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado	1,20	Não compatível: o CIS adicionou esse requisito em versões posteriores	Não compatível: 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 habilitado	Não compatível: verificação manual	Não compatível: verificação manual	Não compatível: verificação manual
[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela configuração PubliclyAccessible	2.3.3	Não compatível: o CIS adicionou esse requisito em versões posteriores	Não compatível: 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 compatível: o CIS adicionou esse requisito em versões posteriores
[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas	2.3.2	Não compatível: o CIS adicionou esse requisito em versões posteriores	Não compatível: o CIS adicionou esse requisito em versões posteriores

Título e ID do controle	Necessidade do CIS v3.0.0	Necessidade do CIS v1.4.0	Necessidade do CIS v1.2.0
[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público habilitadas	2.1.4	2.1.5	Não compatível: o CIS adicionou esse requisito em versões posteriores
[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL	2.1.1	2.1.2	Não compatível: 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 compatível: 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 compatível: o CIS adicionou esse requisito em versões posteriores

ARNs para benchmarks do CIS AWS Foundations

Ao habilitar uma ou mais versões do CIS AWS Foundations Benchmark, você começa a receber descobertas no AWS Security Finding Format (ASFF). No ASFF, cada versão usa o seguinte nome do recurso da Amazon (ARN):

Referência do CIS AWS Foundations v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

Referência do CIS AWS Foundations v1.4.0

```
arn:aws:securityhub:region::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 CSPM do Security Hub para encontrar o ARN de um padrão habilitado.

Os valores anteriores são para o `StandardsArn`. No entanto, `StandardsSubscriptionArn` refere-se ao recurso de assinatura padrão que o Security Hub CSPM cria quando você assina um padrão ligando para uma BatchEnableStandardsregião.

> **Note**
>
> Quando você habilita uma versão do CIS AWS Foundations Benchmark, pode levar até 18 horas para que o Security Hub CSPM gere descobertas para controles que usam a mesma regra AWS Config vinculada ao serviço dos controles habilitados em outros padrões habilitados. Para obter mais informações sobre o cronograma de geração de descobertas de controles, consulte Programar a execução de verificações de segurança.

Os campos de descoberta serão diferentes se você ativar as descobertas de controles consolidadas. Para obter informações sobre essas diferenças, consulteImpacto da consolidação nos campos e valores do ASFF. Para obter exemplos de descobertas de controles, consulte Amostras de resultados de controle.

Requisitos do CIS que não são suportados no Security Hub CSPM

Conforme observado na tabela anterior, o CSPM do Security Hub não suporta todos os requisitos de CIS em todas as versões do CIS Foundations Benchmark. AWS Muitos dos requisitos não suportados só podem ser avaliados pela análise manual do estado de seus AWS recursos.

NIST SP 800-53 Revisão 5 no Security Hub CSPM

A Publicação Especial 800-53 Revisão 5 do NIST (NIST SP 800-53 Rev. 5) é uma estrutura de segurança cibernética e conformidade desenvolvida pelo Instituto Nacional de Padrões e Tecnologia (NIST), uma agência que faz parte do Departamento de Comércio dos EUA. Essa estrutura de

conformidade fornece um catálogo de requisitos de segurança e privacidade para proteger a confidencialidade, integridade e disponibilidade de sistemas de informação e recursos essenciais. Agências e prestadores de serviços do governo federal dos EUA devem cumprir esses requisitos para proteger seus sistemas e organizações. As organizações privadas também podem usar voluntariamente os requisitos como uma estrutura orientadora para reduzir o risco de segurança cibernética. Para obter mais informações sobre a estrutura e seus requisitos, consulte NIST SP 800-53 Rev. 5 no NIST Computer Security Resource Center.

AWS O Security Hub CSPM fornece controles de segurança que suportam um subconjunto dos requisitos do NIST SP 800-53 Revisão 5. Os controles realizam verificações de segurança automatizadas para determinados Serviços da AWS recursos. Para habilitar e gerenciar esses controles, você pode habilitar a estrutura NIST SP 800-53 Revision 5 como padrão no Security Hub CSPM. Observe que os controles não suportam os requisitos da revisão 5 do NIST SP 800-53, que exigem verificações manuais.

Ao contrário de outras estruturas, a estrutura NIST SP 800-53 Revisão 5 não é prescritiva sobre como seus requisitos devem ser avaliados. Em vez disso, a estrutura fornece diretrizes. No Security Hub CSPM, o padrão e os controles NIST SP 800-53 Revisão 5 representam a compreensão do serviço sobre essas diretrizes.

Tópicos

- Configurando a gravação de recursos para controles que se aplicam ao padrão
- Determinar quais controles se aplicam ao padrão

Configurando a gravação de recursos para controles que se aplicam ao padrão

Para otimizar a cobertura e a precisão das descobertas, é importante ativar e configurar o registro de recursos AWS Config antes de ativar o padrão NIST SP 800-53 Revisão 5 no AWS Security Hub CSPM. Ao configurar o registro de recursos, certifique-se também de habilitá-lo para todos os tipos de AWS recursos que são verificados pelos controles que se aplicam ao padrão. Isso é principalmente para controles que têm um tipo de agendamento acionado por alteração. No entanto, alguns controles com um tipo de agendamento periódico também exigem o registro de recursos. Se a gravação de recursos não estiver habilitada ou configurada corretamente, o Security Hub CSPM talvez não consiga avaliar os recursos apropriados e gerar descobertas precisas para os controles que se aplicam ao padrão.

Para obter informações sobre como o Security Hub CSPM usa a gravação de recursos em AWS Config, consulte. Habilitando e configurando o AWS Config Security Hub CSPM Para obter

informações sobre como configurar a gravação de recursos em AWS Config, consulte Como trabalhar com o gravador de configuração no Guia do AWS Config desenvolvedor.

A tabela a seguir especifica os tipos de recursos a serem registrados para controles que se aplicam ao padrão NIST SP 800-53 Revisão 5 no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
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`
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`
Nuvem de computação elástica da Amazon (Amazon 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`

AWS service (Serviço da AWS)	Tipos de recursos
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 Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
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::Alias` , `AWS::KMS::Key`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (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` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
SageMaker Inteligência Artificial da Amazon	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
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`

Determinar quais controles se aplicam ao padrão

A lista a seguir especifica os controles que suportam os requisitos do NIST SP 800-53 Revisão 5 e se aplicam ao padrão NIST SP 800-53 Revisão 5 no Security Hub CSPM. AWS Para obter detalhes sobre os requisitos específicos que um controle suporta, escolha o controle. Em seguida, consulte o campo Requisitos relacionados nos detalhes do controle. Esse campo especifica cada requisito do NIST que o controle suporta. Se o campo não especificar um requisito específico do NIST, o controle não suportará o requisito.

- [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
- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

- [APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado
- [APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF
- [APIGateway.5] Os dados do cache da API REST de Gateway devem ser criptografados em repouso
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado 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 em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 2 () IMDSv2
- [Autoscaling.5] As instâncias da EC2 Amazon 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 da 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 habilitada
- [CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada
- [CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CloudWatch.15] Os CloudWatch alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] Os grupos de CloudWatch log devem ser retidos por um período de tempo especificado
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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 e usar a função vinculada ao serviço para gravação de recursos
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
- [DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.1] 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
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] 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 acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente
- [EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs
- [EC2.7] A criptografia padrão do EBS deve estar ativada
- [EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.9] EC2 As instâncias da Amazon não devem ter um endereço público IPv4
- [EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2
- [EC2.12] A Amazon não utilizada EC2 EIPs deve ser removida

- [EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22
- [EC2.15] As EC2 sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos
- [EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas
- [EC2.17] EC2 As instâncias da Amazon não devem usar várias ENIs
- [EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário

- [ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização
- [EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters do 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 OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito

- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- [ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos
- [ELB.5] O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado
- [ELB.6] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada
- [ELB.7] 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
- [ELB.9] Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [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
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.1] Os domínios do Elasticsearch devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- [ES.3] 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.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado
- [ES.6] Os domínios do Elasticsearch devem ter pelo menos três nós de dados
- [ES.7] 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] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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

- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] 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
- [Lambda.1] As funções do Lambda.1 devem proibir o acesso público
- [Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis
- [Lambda.3] 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.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MSK.1] 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 agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos

- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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 configuração PubliclyAccessible
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- [RDS.4] Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- [RDS.5] As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- [RDS.6] 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.8] As instâncias de banco de dados do RDS deve ter a proteção contra exclusão habilitada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- [RDS.10] A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.11] As instâncias do RDS devem ter backups automáticos habilitados
- [RDS.12] A autenticação do IAM deve ser configurada para clusters 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
- [RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots
- [RDS.17] As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos
- [RDS.19] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

- [RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados
- [RDS.21] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados
- [RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados
- [RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público
- [Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.2] 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 habilitadas
- [S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público para leitura
- [S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público para gravação
- [S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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 em log de acesso ao servidor habilitado
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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 versionamento habilitado
- [S3.15] Os buckets de uso geral do S3 devem ter o Bloqueio de Objetos habilitado
- [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
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra

- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch

NIST SP 800-171 Revisão 2 no Security Hub CSPM

A Publicação Especial 800-171 Revisão 2 do NIST (NIST SP 800-171 Rev. 2) é uma estrutura de segurança cibernética e conformidade desenvolvida pelo Instituto Nacional de Padrões e Tecnologia (NIST), uma agência que faz parte do Departamento de Comércio dos EUA. Essa estrutura de conformidade fornece os requisitos de segurança recomendados para proteger a confidencialidade de informações não classificadas controladas em sistemas e organizações que não fazem parte do governo federal dos EUA. Informações não classificadas controladas, também conhecidas como CUI, são informações confidenciais que não atendem aos critérios governamentais de classificação, mas devem ser protegidas. São informações consideradas confidenciais e criadas ou possuídas pelo governo federal dos EUA ou por outras entidades em nome do governo federal dos EUA.

O NIST SP 800-171 Rev. 2 fornece os requisitos de segurança recomendados para proteger a confidencialidade da CUI quando:

- As informações residem em sistemas e organizações não federais,
- A organização não federal não está coletando ou mantendo informações em nome de uma agência federal ou usando ou operando um sistema em nome de uma agência, e
- Não há requisitos de proteção específicos para proteger a confidencialidade do CUI prescritos pela lei, regulamentação ou política governamental autorizadora para a categoria CUI listada no Registro CUI.

Os requisitos se aplicam a todos os componentes de sistemas e organizações não federais que processam, armazenam ou transmitem CUI ou fornecem proteção de segurança para os componentes. Para obter mais informações, consulte NIST SP 800-171 Rev. 2 no NIST Computer Security Resource Center.

AWS O Security Hub CSPM fornece controles de segurança que suportam um subconjunto dos requisitos do NIST SP 800-171 Revisão 2. Os controles realizam verificações de segurança automatizadas para determinados Serviços da AWS recursos. Para habilitar e gerenciar esses controles, você pode habilitar a estrutura NIST SP 800-171 Revisão 2 como padrão no Security Hub

CSPM. Observe que os controles não suportam os requisitos da Revisão 2 do NIST SP 800-171, que exigem verificações manuais.

Tópicos

Configurando a gravação de recursos para controles que se aplicam ao padrão

Para otimizar a cobertura e a precisão das descobertas, é importante habilitar e configurar o registro de recursos AWS Config antes de habilitar o padrão NIST SP 800-171 Revisão 2 no Security Hub AWS CSPM. Ao configurar o registro de recursos, certifique-se também de habilitá-lo para todos os tipos de AWS recursos que são verificados pelos controles que se aplicam ao padrão. Caso contrário, o Security Hub CSPM talvez não consiga avaliar os recursos apropriados e gerar descobertas precisas para os controles que se aplicam ao padrão.

Para obter informações sobre como o Security Hub CSPM usa a gravação de recursos em AWS Config, consulte. Habilitando e configurando o AWS Config Security Hub CSPM Para obter informações sobre como configurar a gravação de recursos em AWS Config, consulte Como trabalhar com o gravador de configuração no Guia do AWS Config desenvolvedor.

A tabela a seguir especifica os tipos de recursos a serem registrados para controles que se aplicam ao padrão NIST SP 800-171 Revisão 2 no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Nuvem de computação elástica da Amazon (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`

AWS service (Serviço da AWS)	Tipos de recursos
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SMS)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Determinar quais controles se aplicam ao padrão

A lista a seguir especifica os controles que suportam os requisitos do NIST SP 800-171 Revisão 2 e se aplicam ao padrão NIST SP 800-171 Revisão 2 no Security Hub CSPM. AWS Para obter detalhes sobre os requisitos específicos que um controle suporta, escolha o controle. Em seguida, consulte o campo Requisitos relacionados nos detalhes do controle. Esse campo especifica cada requisito do NIST que o controle suporta. Se o campo não especificar um requisito específico do NIST, o controle não suportará o requisito.

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas

- [CloudTrail.2] CloudTrail deve ter a criptografia em repouso habilitada
- [CloudTrail.3] Pelo menos uma CloudTrail trilha deve estar habilitada
- [CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada
- CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”
- [CloudWatch.2] Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas
- [CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM
- [CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do
- [CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do
- [CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente
- [CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3
- [CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do
- [CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança
- [CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)
- [CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede
- [CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas
- [CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC
- [CloudWatch.15] Os CloudWatch alarmes devem ter ações especificadas configuradas
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs
- [EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2

- [EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22
- [EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas
- [EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM não devem ter políticas do IAM anexadas
- [IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas

- [NetworkFirewall.2] O registro em log do Network Firewall deve ser habilitado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL
- [S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS
- [S3.9] Os buckets de uso geral do S3 devem ter o registro em log de acesso ao servidor habilitado
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.14] Os buckets de uso geral do S3 devem ter o versionamento habilitado
- [S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch

PCI DSS no Security Hub CSPM

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) é uma estrutura de conformidade terceirizada que fornece um conjunto de regras e diretrizes para lidar com segurança com informações de cartões de crédito e débito. O PCI Security Standards Council (SSC) cria e atualiza essa estrutura.

AWS O Security Hub CSPM fornece um padrão PCI DSS que pode ajudá-lo a manter a conformidade com essa estrutura de terceiros. Você pode usar esse padrão para descobrir vulnerabilidades de segurança em AWS recursos que lidam com dados de titulares de cartões. Recomendamos habilitar esse padrão para Contas da AWS que haja recursos que armazenem, processem ou transmitam dados do titular do cartão ou dados confidenciais de autenticação. As avaliações do PCI SSC validaram esse padrão.

O Security Hub CSPM oferece suporte para PCI DSS v3.2.1 e PCI DSS v4.0.1. Recomendamos usar a versão 4.0.1 para se manter atualizado com as melhores práticas de segurança. Você pode ter as

duas versões do padrão ativadas ao mesmo tempo. Para obter informações sobre a habilitação de padrões, consulteHabilitar um padrão de segurança. Se você usa atualmente a v3.2.1, mas deseja usar somente a v4.0.1, habilite a versão mais recente antes de desativar a versão mais antiga. Isso evita falhas nas verificações de segurança. Se você usa a integração CSPM do Security Hub com AWS Organizations e deseja habilitar em lote a v4.0.1 em várias contas, recomendamos usar a configuração central para fazer isso.

As seções a seguir especificam quais controles se aplicam ao PCI DSS v3.2.1 e ao PCI DSS v4.0.1.

Controles que se aplicam ao PCI DSS v3.2.1

A lista a seguir especifica quais controles CSPM do Security Hub se aplicam ao PCI DSS v3.2.1. Para revisar os detalhes de um controle, escolha o controle.

[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 habilitada

[CloudTrail.3] Pelo menos uma CloudTrail trilha deve estar habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs

CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”

[CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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 e usar a função vinculada ao serviço para gravação de recursos

[DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas

[EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

[EC2.12] A Amazon não utilizada EC2 EIPs deve ser removida

[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22

[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

[ES.1] Os domínios do Elasticsearch 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 IAM não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do IAM não devem ter políticas do IAM anexadas

[IAM.4] A chave de acesso do usuário raiz do IAM não deve existir

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.9] A MFA deve estar habilitada para o usuário raiz

[IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes

[IAM.19] A MFA deve estar habilitada para todos os usuários do IAM

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[Lambda.1] As funções do Lambda.1 devem proibir o acesso público

[Lambda.3] 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 configuração PubliclyAccessible

[PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público habilitadas

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público para leitura

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público para gravação

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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 EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager

[SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch

[SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

Controles que se aplicam ao PCI DSS v4.0.1

A lista a seguir especifica quais controles CSPM do Security Hub se aplicam ao PCI DSS v4.0.1. Para revisar os detalhes de um controle, escolha o controle.

[ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

[ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

[APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway

[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

[AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 2 () IMDSv2

[Autoscaling.5] As instâncias da EC2 Amazon lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos

[CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

[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.3] CloudFront as distribuições devem exigir criptografia em trânsito

[CloudFront.5] CloudFront as distribuições devem ter o registro ativado

[CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

[CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso habilitada

[CloudTrail.3] Pelo menos uma CloudTrail trilha deve estar habilitada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada

[CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente

[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3

[CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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

[DMS.1] As instâncias de replicação do 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado

[DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado

[DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

[DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

[DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado

[DMS.9] Os endpoints do DMS devem usar SSL

[DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

[DocumentDB.3] 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

[DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito

[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22

[EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389

[EC2.15] As EC2 sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos

[EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas

[EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2

[EC2.171] As conexões EC2 VPN devem ter o registro ativado

[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

[EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede

[EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado

[EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor

[EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto

[EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2

[ECR.1] Os repositórios privados do ECR devem ter a digitalização de imagens configurada

[ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

[ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos

[ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

[ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner

[EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário

[EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público

[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

[EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes

[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

[ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas

[ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito

[ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH ativado

[ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas

[ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch

[ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

[ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos

[ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config

[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.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

[ES.3] Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós

[ES.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

[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

[GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada

[GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada

[GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado

[GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada

[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

[IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.9] A MFA 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

Certifique-se de que política de senha do IAM exija pelo menos um número

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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support

[IAM.19] A MFA deve estar habilitada para todos os usuários do IAM

[Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2

[Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada

[Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada

[Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[Lambda.1] As funções do Lambda.1 devem proibir o acesso público

[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis

[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch

[MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada

[MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

[MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito

[Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch

[Neptune.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos

Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada

Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado

[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela configuração PubliclyAccessible

[RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados

[RDS.21] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

[RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados

[RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

[RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

[RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

[RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch

[RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

[PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público

[Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas

[Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

[Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

[Route53.2] 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 habilitadas

[S3.15] Os buckets de uso geral do S3 devem ter o Bloqueio de Objetos habilitado

[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

[S3.22] Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto

[S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto

[S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL

[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 em log de acesso ao servidor habilitado

[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

[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.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias

[SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch

[SSM.3] EC2 As instâncias da Amazon 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

[Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints

[WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado

[WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado

Padrões gerenciados de serviços no Security Hub CSPM

Um padrão gerenciado por serviços é um padrão de segurança AWS service (Serviço da AWS) gerenciado por outra pessoa, mas que você pode visualizar no CSPM do Security Hub. 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 CSPM 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 CSPM do Security Hub e não pode ser acessado pela API CSPM do Security Hub ou. AWS CLI

- Sem ativação automática dos controles — Quando você cria um padrão gerenciado pelo serviço, o CSPM do Security Hub e o serviço de gerenciamento não ativam automaticamente os controles que se aplicam ao padrão. Além disso, quando o Security Hub CSPM lança novos controles para o padrão, eles não são ativados automaticamente. Isso é um desvio dos padrões que o Security Hub CSPM gerencia. Para obter mais informações sobre a maneira usual de configurar controles no CSPM do Security Hub, consulte. Entendendo os controles de segurança no Security Hub CSPM
- 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 CSPM existentes do Security Hub.

Depois que o serviço de gerenciamento criar o padrão gerenciado pelo serviço e disponibilizar os controles para ele, você poderá acessar suas descobertas de controle, status de controle e pontuação de segurança padrão no console CSPM do Security Hub, na API CSPM 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 CSPM e. AWS Control Tower Ele permite que você configure os controles proativos AWS Control Tower junto com os controles de detetive do Security Hub CSPM no serviço. AWS Control Tower

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 CSPM. Por exemplo, você deve criar e excluir um padrão gerenciado por serviços no serviço de gerenciamento. Para obter mais informações, consulte Padrões gerenciados de serviços no Security Hub CSPM.

No console e na API do Security Hub CSPM, você pode ver o Service-Managed Standard: junto com outros padrões CSPM do AWS Control Tower 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 CSPM 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 CSPM do Security Hub, AWS Control Tower também habilita o CSPM do Security Hub para você.

Se você não tiver configurado AWS Control Tower, não poderá visualizar ou acessar esse padrão no console CSPM do Security Hub, na API CSPM do Security Hub ou. AWS CLI Mesmo se você tiver configurado AWS Control Tower, não poderá visualizar ou acessar esse padrão no CSPM do 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 CSPM 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 o `EnableControl`e `DisableControl` APIs)
- 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 CSPM do Security Hub.

No entanto, desabilitar um controle no CSPM do 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 CSPM do 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

Você pode exibir o status de habilitação de um controle usando um dos métodos a seguir:

- Console CSPM do Security Hub, API CSPM 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 no CSPM do `Disabled` Security Hub, a menos que você habilite explicitamente esse controle no CSPM do Security Hub.

O Security Hub CSPM calcula o status do controle com base no status do fluxo de trabalho e no status de conformidade das descobertas do controle. Para obter mais informações sobre o status de habilitação e o status de controle, consulte Analisando os detalhes dos controles no Security Hub CSPM.

Com base nos status de controle, o Security Hub CSPM calcula uma pontuação de segurança para o Service-Managed Standard:. AWS Control Tower Essa pontuação só está disponível no CSPM do Security Hub. Além disso, você só pode visualizar as descobertas de controle no CSPM do 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 CSPM pode levar até 18 horas para gerar descobertas para controles que usam uma regra vinculada ao serviço existente. AWS Config Você pode ter regras vinculadas a serviços existentes se tiver habilitado outros padrões e controles no CSPM do Security Hub. Para obter 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 CSPM do Security Hub, e você não pode mais acessá-lo usando a API CSPM do Security Hub ou. AWS CLI

> **Note**
>
> Desabilitar todos os controles do padrão no Security Hub CSPM não desativa nem exclui o padrão.

A desativação do serviço CSPM do 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 CSPM. O Security Hub CSPM 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. Amostras de resultados 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 para visualizar informações sobre ele, incluindo etapas de remediação 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 o controle de segurança independente do padrão. IDs No AWS Control Tower console, os controles IDs são formatados como SH. ***ControlID***(por exemplo, SH. CodeBuild.1). No Security Hub CSPM, se as descobertas de controle consolidadas estiverem desativadas em sua conta, o `ProductFields.ControlId` campo 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
- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado
- [APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF
- [APIGateway.5] Os dados do cache da API REST de Gateway devem ser criptografados em repouso
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado 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 em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 2 () IMDSv2
- [Autoscaling.5] As instâncias da EC2 Amazon 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 da 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 habilitada
- [CloudTrail.4] a validação do arquivo de CloudTrail log deve estar habilitada
- [CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
- [DMS.9] Os endpoints do DMS devem usar SSL
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DynamoDB.1] 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
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente
- [EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs

- [EC2.7] A criptografia padrão do EBS deve estar ativada
- [EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.9] EC2 As instâncias da Amazon não devem ter um endereço público IPv4
- [EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2
- [EC2.15] As EC2 sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos
- [EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas
- [EC2.17] EC2 As instâncias da Amazon não devem usar várias ENIs
- [EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário
- [ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner

- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] 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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH ativado
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de saúde 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- [ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos
- [ELB.5] O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado
- [ELB.6] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada
- [ELB.7] 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
- [ELB.9] Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado

- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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 Elasticsearch devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- [ES.3] 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.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado
- [ES.6] Os domínios do Elasticsearch devem ter pelo menos três nós de dados
- [ES.7] 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 IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] 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
- [Lambda.1] As funções do Lambda.1 devem proibir o acesso público
- [Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis
- [Lambda.3] As funções do Lambda devem estar em uma VPC
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado 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 configuração PubliclyAccessible
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- [RDS.4] Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- [RDS.5] As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- [RDS.6] O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS
- [RDS.8] As instâncias de banco de dados do RDS deve ter a proteção contra exclusão habilitada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- [RDS.10] A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.11] As instâncias do RDS devem ter backups automáticos habilitados
- [RDS.12] A autenticação do IAM deve ser configurada para clusters 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

- [RDS.17] As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.19] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster
- [RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados
- [RDS.21] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados
- [RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados
- [RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público
- [Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- [Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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 habilitadas
- [S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público para leitura
- [S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público para gravação
- [S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem 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 em log de acesso ao servidor habilitado
- [S3.12] não ACLs deve ser usado 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
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras

Para obter mais informações sobre esse padrão, consulte Controles CSPM do Security Hub no Guia do AWS Control Tower Usuário.

Habilitar um padrão de segurança

Quando você habilita um padrão de segurança no AWS Security Hub CSPM, o Security Hub CSPM cria e ativa automaticamente todos os controles que se aplicam ao padrão. O Security Hub CSPM também começa a executar verificações de segurança e a gerar descobertas para os controles.

Para otimizar a cobertura e a precisão das descobertas, ative e configure o registro de recursos AWS Config antes de ativar um padrão. Ao configurar o registro de recursos, certifique-se também de habilitá-lo para todos os tipos de recursos que são verificados pelos controles que se aplicam ao padrão. Caso contrário, o Security Hub CSPM talvez não consiga avaliar os recursos apropriados e gerar descobertas precisas para os controles que se aplicam ao padrão. Para obter mais informações, consulte Habilitando e configurando o AWS Config Security Hub CSPM.

Depois de habilitar um padrão, você pode desativar ou reativar posteriormente os controles individuais que se aplicam ao padrão. Se você desabilitar um controle para um padrão, o Security Hub CSPM interrompe a geração de descobertas para o controle. Além disso, o Security Hub CSPM ignora o controle ao calcular a pontuação de segurança do padrão. A pontuação de segurança é a porcentagem de controles aprovados na avaliação, em relação ao número total de controles que se aplicam ao padrão, estão habilitados e têm dados de avaliação.

Quando você habilita um padrão, o Security Hub CSPM gera uma pontuação de segurança preliminar para o padrão, normalmente dentro de 30 minutos após sua primeira visita à página Resumo ou Padrões de Segurança no console CSPM do Security Hub. As pontuações de segurança são geradas somente para padrões que são ativados quando você visita essas páginas no console. Além disso, o registro de recursos deve ser configurado AWS Config para que as pontuações apareçam. Nas regiões da China AWS GovCloud (US) Regions, pode levar até 24 horas para que o Security Hub CSPM gere uma pontuação de segurança preliminar para um padrão. Depois que o Security Hub CSPM gera uma pontuação preliminar, ele atualiza a pontuação a cada 24 horas. Para determinar quando uma pontuação de segurança foi atualizada pela última vez, você pode consultar um carimbo de data/hora que o Security Hub CSPM fornece para a pontuação. Para obter mais informações, consulte Calcular pontuações de segurança.

A forma como você habilita um padrão depende se você usa a configuração central para gerenciar o CSPM do Security Hub para várias contas e. Regiões da AWS Recomendamos que você use a configuração central se quiser habilitar padrões em ambientes com várias contas e várias regiões.

Você pode usar a configuração central se integrar o Security Hub CSPM com o. AWS Organizations Se você não usa a configuração central, deve habilitar cada padrão separadamente em cada conta e cada região.

Tópicos

Habilitando um padrão em várias contas e Regiões da AWS

Para habilitar e configurar um padrão de segurança em várias contas Regiões da AWS, use a configuração central. Com a configuração central, o administrador delegado do CSPM do Security Hub pode criar políticas de configuração do CSPM do Security Hub que habilitam um ou mais padrões. O administrador pode então associar uma política de configuração a contas individuais, unidades organizacionais (OUs) ou à raiz. Uma política de configuração afeta a região de origem, também chamada de região de agregação, e todas as regiões vinculadas.

As políticas de configuração oferecem opções de personalização. Por exemplo, você pode optar por habilitar somente o padrão AWS Foundational Security Best Practices (FSBP) para uma OU. Para outra UO, você pode optar por ativar o padrão FSBP e o padrão Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0. Para obter informações sobre a criação de uma política de configuração que habilite padrões específicos que você especifica, consulteCriação e associação de políticas de configuração.

Se você usa a configuração central, o Security Hub CSPM não habilita automaticamente nenhum padrão em contas novas ou existentes. Em vez disso, o administrador do CSPM do Security Hub especifica quais padrões devem ser habilitados em contas diferentes ao criar políticas de configuração do CSPM do Security Hub para sua organização. O Security Hub CSPM oferece uma política de configuração recomendada na qual somente o padrão FSBP está habilitado. Para obter mais informações, consulte Tipos de políticas de configuração.

> **Note**
>
> O administrador do CSPM do Security Hub pode usar políticas de configuração para habilitar qualquer padrão, exceto o padrão gerenciado pelo AWS Control Tower serviço. Para habilitar esse padrão, o administrador deve usar AWS Control Tower diretamente. Eles também

devem ser usados AWS Control Tower para ativar ou desativar controles individuais nesse padrão para uma conta gerenciada centralmente.

Se você quiser que algumas contas habilitem e configurem padrões para suas próprias contas, o administrador do CSPM do Security Hub pode designar essas contas como contas autogerenciadas. As contas autogerenciadas devem ativar e configurar padrões separadamente em cada região.

Habilitando um padrão em uma única conta e Região da AWS

Se você não usa a configuração central ou tem uma conta autogerenciada, não pode usar políticas de configuração para habilitar centralmente os padrões de segurança em várias contas ou. Regiões da AWS No entanto, você pode ativar um padrão em uma única conta e região. Você pode fazer isso usando o console CSPM do Security Hub ou a API CSPM do Security Hub.

Security Hub CSPM console

Siga estas etapas para habilitar um padrão em uma conta e região usando o console CSPM do Security Hub.

Para habilitar um padrão em uma conta e região

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Usando o Região da AWS seletor no canto superior direito da página, escolha a região na qual você deseja ativar o padrão.
3. No painel de navegação, escolha Padrões de segurança. A página de padrões de segurança lista todos os padrões que o Security Hub CSPM suporta atualmente. Se você já habilitou um padrão, a seção do padrão inclui a pontuação de segurança atual e detalhes adicionais do padrão.
4. Na seção do padrão que você deseja ativar, escolha Ativar padrão.

Para ativar o padrão em regiões adicionais, repita as etapas anteriores em cada região adicional.

Security Hub CSPM API

Para habilitar um padrão programaticamente em uma única conta e região, use a BatchEnableStandardsoperação. Ou, se você estiver usando o AWS Command Line Interface (AWS CLI), execute o batch-enable-standardscomando.

Em sua solicitação, use o `StandardsArn` parâmetro para especificar o Amazon Resource Name (ARN) do padrão que você deseja habilitar. Especifique também a região à qual sua solicitação se aplica. Por exemplo, o comando a seguir ativa o padrão AWS Foundational Security Best Practices (FSBP):

```
$ 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"}' \
--region us-east-1
```

Onde *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* está o ARN do padrão FSBP na região Leste dos EUA (Norte da Virgínia) e *us-east-1* a região na qual ativá-lo.

Para obter o ARN de um padrão, use a DescribeStandardsoperação ou, se estiver usando o AWS CLI, execute o describe-standardscomando.

Para primeiro revisar uma lista de padrões atualmente habilitados em sua conta, você pode usar a GetEnabledStandardsoperação. Se você estiver usando o AWS CLI, você pode executar o get-enabled-standardscomando para recuperar essa lista.

Depois de habilitar um padrão, o Security Hub CSPM começa a executar tarefas para habilitar o padrão na conta e na região especificada. Isso inclui a criação de todos os controles que se aplicam ao padrão. Para monitorar o status dessas tarefas, você pode verificar o status do padrão para a conta e a região.

Verificando o status de um padrão

Quando você habilita um padrão de segurança para uma conta, o Security Hub CSPM começa a criar todos os controles que se aplicam ao padrão na conta. O Security Hub CSPM também executa tarefas adicionais para habilitar o padrão para a conta, como gerar uma pontuação de segurança preliminar para o padrão. Enquanto o Security Hub CSPM executa essas tarefas, o status do padrão é Pendingpara a conta. O status do padrão então passa por estados adicionais, que você pode monitorar e verificar.

> **Note**
>
> Alterações nos controles individuais de um padrão não afetam o status geral do padrão. Por exemplo, se você ativar um controle que você desativou anteriormente, sua alteração não

afetará o status do padrão. Da mesma forma, se você alterar um valor de parâmetro para um controle ativado, sua alteração não afetará o status do padrão.

Para verificar o status de um padrão usando o console CSPM do Security Hub, escolha Padrões de segurança no painel de navegação. A página de padrões de segurança lista todos os padrões que o Security Hub CSPM suporta atualmente. Se o CSPM do Security Hub estiver atualmente executando tarefas para habilitar o padrão, a seção do padrão indica que o CSPM do Security Hub ainda está gerando uma pontuação de segurança para o padrão. Se um padrão estiver ativado, a seção do padrão incluirá a pontuação atual. Escolha Exibir resultados para revisar detalhes adicionais, incluindo o status dos controles individuais que se aplicam ao padrão. Para obter mais informações, consulte Programar a execução de verificações de segurança.

Para verificar o status de um padrão programaticamente com a API CSPM do Security Hub, use a operação. GetEnabledStandards Em sua solicitação, opcionalmente, use o `StandardsSubscriptionArns` parâmetro para especificar o Amazon Resource Name (ARN) do padrão cujo status você deseja verificar. Se você estiver usando o AWS Command Line Interface (AWS CLI), poderá executar o get-enabled-standardscomando para verificar o status de um padrão. Para especificar o ARN do padrão a ser verificado, use o `standards-subscription-arns` parâmetro. Para determinar qual ARN especificar, você pode usar a DescribeStandardsoperação ou, para o AWS CLI, executar o describe-standardscomando.

Se sua solicitação for bem-sucedida, o Security Hub CSPM responderá com uma matriz de objetos. `StandardsSubscription` Uma assinatura padrão é um AWS recurso que o Security Hub CSPM cria em uma conta quando um padrão é habilitado para a conta. Cada `StandardsSubscription` objeto fornece detalhes sobre um padrão que está atualmente ativado ou está sendo ativado ou desativado para a conta. Dentro de cada objeto, o `StandardsStatus` campo especifica o status atual do padrão para a conta.

O status de um padrão (`StandardsStatus`) pode ser um dos seguintes.

PENDING

O Security Hub CSPM está atualmente executando tarefas para habilitar o padrão para a conta. Isso inclui criar os controles que se aplicam ao padrão e gerar uma pontuação de segurança preliminar para o padrão. Pode levar vários minutos para que o Security Hub CSPM conclua todas as tarefas. Um padrão também pode ter esse status se já estiver habilitado para a conta e o Security Hub CSPM estiver adicionando novos controles ao padrão.

Se um padrão tiver esse status, talvez você não consiga recuperar os detalhes dos controles individuais que se aplicam ao padrão. Além disso, talvez você não consiga configurar ou desativar controles individuais para o padrão. Por exemplo, se você tentar desativar um controle usando a UpdateStandardsControloperação, ocorrerá um erro.

Para determinar se você pode configurar ou gerenciar controles individuais para o padrão, consulte o valor do `StandardsControlsUpdatable` campo. Se o valor desse campo for`READY_FOR_UPDATES`, você poderá começar a gerenciar controles individuais para o padrão. Caso contrário, espere até que o Security Hub CSPM conclua as tarefas adicionais de processamento para habilitar o padrão.

READY

Atualmente, o padrão está habilitado para a conta. O Security Hub CSPM pode executar verificações de segurança e gerar descobertas para todos os controles que se aplicam ao padrão e estão atualmente habilitados. O Security Hub CSPM também pode calcular uma pontuação de segurança para o padrão.

Se um padrão tiver esse status, você poderá recuperar os detalhes dos controles individuais que se aplicam ao padrão. Além disso, você pode configurar, desativar ou reativar os controles. Você também pode desativar o padrão.

INCOMPLETE

O Security Hub CSPM não conseguiu habilitar completamente o padrão para a conta. O Security Hub CSPM não pode executar verificações de segurança e gerar descobertas para todos os controles que se aplicam ao padrão e estão atualmente habilitados. Além disso, o Security Hub CSPM não pode calcular uma pontuação de segurança para o padrão.

Para determinar por que o padrão não foi ativado completamente, consulte as informações na `StandardsStatusReason` matriz. Essa matriz especifica problemas que impediram que o Security Hub CSPM habilitasse o padrão. Se ocorrer um erro interno, tente ativar o padrão para a conta novamente. Para outros tipos de problemas, verifique suas AWS Config configurações. Você também pode desativar controles individuais que não deseja verificar ou desativar completamente o padrão.

DELETING

No momento, o Security Hub CSPM está processando uma solicitação para desativar o padrão da conta. Isso inclui desativar os controles que se aplicam ao padrão e remover a pontuação de segurança associada. Pode levar vários minutos para que o CSPM do Security Hub conclua o processamento da solicitação.

Se um padrão tiver esse status, você não poderá reativá-lo nem tentar desativá-lo novamente para a conta. O CSPM do Security Hub deve primeiro concluir o processamento da solicitação atual. Além disso, você não pode recuperar os detalhes dos controles individuais que se aplicam ao padrão nem gerenciar os controles.

FAILED

O CSPM do Security Hub não conseguiu desativar o padrão da conta. Um ou mais erros ocorreram quando o Security Hub CSPM tentou desabilitar o padrão. Além disso, o Security Hub CSPM não pode calcular uma pontuação de segurança para o padrão.

Para determinar por que o padrão não foi completamente desativado, consulte as informações na `StandardsStatusReason` matriz. Essa matriz especifica problemas que impediram que o Security Hub CSPM desativasse o padrão.

Se um padrão tiver esse status, você não poderá recuperar os detalhes dos controles individuais que se aplicam ao padrão nem gerenciar os controles. No entanto, você pode reativar o padrão para a conta. Se você resolver os problemas que impediram o Security Hub CSPM de desabilitar o padrão, você também pode tentar desabilitar o padrão novamente.

Se o status de um padrão for`READY`, o Security Hub CSPM executará verificações de segurança e gerará descobertas para todos os controles que se aplicam ao padrão e estão atualmente habilitados. Para outros status, o Security Hub CSPM pode executar verificações e gerar descobertas para alguns controles habilitados, mas não para todos. Pode levar até 24 horas para gerar ou atualizar as descobertas de controle. Para obter mais informações, consulte Programar a execução de verificações de segurança.

Analisando os detalhes de um padrão de segurança

Depois de habilitar um padrão de segurança no AWS Security Hub CSPM, você pode usar o console para revisar os detalhes do padrão. No console , a página de detalhes de um padrão inclui as seguintes informações:

- A pontuação de segurança atual do padrão.
- Uma tabela de controles que se aplicam ao padrão.
- Estatísticas agregadas para controles que se aplicam ao padrão.
- Um resumo visual do status dos controles que se aplicam ao padrão.

- Um resumo visual das verificações de segurança dos controles que estão habilitados e se aplicam ao padrão. Se você fizer a integração com AWS Organizations, os controles habilitados em pelo menos uma conta da organização serão considerados ativados.

Para revisar esses detalhes, escolha Padrões de segurança no painel de navegação do console. Em seguida, na seção do padrão, escolha Exibir resultados. Para uma análise mais profunda, você pode filtrar e classificar os dados e detalhar para revisar os detalhes dos controles individuais que se aplicam ao padrão.

Tópicos

Entender a pontuação de segurança do padrão

No console CSPM do AWS Security Hub, a página de detalhes de um padrão exibe a pontuação de segurança do padrão. A pontuação é a porcentagem de controles aprovados na avaliação, em relação ao número total de controles que se aplicam ao padrão, estão habilitados e têm dados de avaliação. Abaixo da pontuação, há um gráfico que resume as verificações de segurança dos controles habilitados para o padrão. Isso inclui o número de verificações de segurança aprovadas e reprovadas. Para contas de administrador, a pontuação padrão e o gráfico refletem o status agregado da conta do administrador e de todas as contas dos membros. Para revisar as verificações de segurança que falharam em controles que têm uma severidade específica, escolha a severidade.

Quando você habilita um padrão, o Security Hub CSPM gera uma pontuação de segurança preliminar para o padrão, normalmente dentro de 30 minutos após sua primeira visita à página Resumo ou à página de Padrões de Segurança no console CSPM do Security Hub. As pontuações são geradas somente para os 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. Nas regiões da China AWS GovCloud (US) Regions, pode levar até 24 horas para que o Security Hub CSPM gere uma pontuação preliminar. Depois que o Security Hub CSPM gera uma pontuação preliminar para um padrão, ele atualiza a pontuação a cada 24 horas. Para obter mais informações, consulte Calcular pontuações de segurança.

Todos os dados nas páginas de detalhes dos padrões de segurança são específicos dos atuais, a Região da AWS menos que você defina uma região de agregação. Se você definir uma região de agregação, as pontuações de segurança se aplicarão a todas as regiões e incluirão descobertas

para todas as regiões vinculadas. Além disso, o status de conformidade dos controles reflete as descobertas das regiões vinculadas, e o número de verificações de segurança inclui as descobertas das regiões vinculadas.

Revisando os controles de um padrão

Ao usar o console CSPM do AWS Security Hub para revisar os detalhes de um padrão que você habilitou, você pode revisar uma tabela de controles de segurança que se aplicam ao padrão. Para cada controle, a tabela inclui as seguintes informações:

- O ID e o título do controle.
- O status do controle. Para obter mais informações, consulte Avaliando o status de conformidade e o status de controle.
- A severidade atribuída ao controle.
- O número de verificações reprovadas e o número total de verificações. Se aplicável, o campo Verificações falhadas também especifica o número de descobertas com o status Desconhecido.
- Se o controle é compatível com parâmetros personalizados. Para obter mais informações, consulte Entendendo os parâmetros de controle no Security Hub CSPM.

O Security Hub CSPM atualiza os status de controle e a contagem de verificações de segurança a cada 24 horas. Um carimbo de data/hora na parte superior da página indica quando o Security Hub CSPM atualizou esses dados mais recentemente.

Para contas de administrador, os status de controle e o número de verificações de segurança são agregados na conta do administrador e em todas as contas dos membros. A contagem de controles ativados inclui controles que estão habilitados para o padrão na conta do administrador ou de pelo menos uma conta de membro. A contagem de controles desativados inclui controles que estão desativados para o padrão na conta do administrador e em todas as contas dos membros.

Você pode filtrar a tabela de controles que se aplicam ao padrão. Usando as opções Filtrar por ao lado da tabela, você pode optar por visualizar somente os controles ativados ou desativados para o padrão. Se você exibir somente os controles ativados, poderá filtrar ainda mais a tabela pelo status do controle. Em seguida, você pode se concentrar nos controles que têm um status de controle específico. Além das opções Filtrar por, você pode inserir critérios de filtro na caixa Controles de filtro. Por exemplo, é possível filtrar por ID ou título do controle.

Escolha seu método de acesso preferido. Em seguida, siga as etapas para revisar os controles que se aplicam a um padrão que você ativou.

Security Hub CSPM console

Para revisar os controles de um padrão habilitado

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, selecione Padrões de segurança.
3. Na seção do padrão, escolha Exibir resultados.

A tabela na parte inferior da página lista todos os controles que se aplicam ao padrão. Você pode filtrar e classificar a tabela. Você também pode baixar a página atual da tabela como um arquivo CSV. Para fazer isso, escolha Baixar acima da tabela. Se você filtrar a tabela, o arquivo baixado incluirá somente os controles que correspondem às suas configurações de filtro atuais.

Security Hub CSPM API

Para revisar os controles de um padrão habilitado

1. Use a ListSecurityControlDefinitionsoperação da API CSPM do Security Hub. Se você estiver usando o AWS CLI, execute o list-security-control-definitionscomando.

   Especifique o Amazon Resource Name (ARN) do padrão para o qual você deseja revisar os controles. ARNs Para obter os padrões, use a DescribeStandardsoperação ou execute o comando describe-standards. Se você não especificar o ARN para um padrão, o CSPM do Security Hub retornará todo o controle de segurança. IDs
2. Use a ListStandardsControlAssociationsoperação da API CSPM do Security Hub ou execute o list-standards-control-associationscomando. Esta operação informa em quais padrões um controle está habilitado.

   Identifique o controle fornecendo o ARN ou o ID do controle de segurança. Os parâmetros de paginação são opcionais.

O exemplo a seguir diz em quais padrões o controle Config.1 está habilitado.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Desativando os padrões de segurança ativados automaticamente

Se sua organização não usa a configuração central, ela usa um tipo de configuração chamado configuração local. Com a configuração local, o AWS Security Hub CSPM pode habilitar automaticamente os padrões de segurança padrão para novas contas membros quando as contas ingressam na sua organização. Todos os controles que se aplicam a esses padrões padrão também são ativados automaticamente.

Atualmente, os padrões de segurança padrão são o padrão AWS Foundational Security Best Practices e o padrão Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Para obter informações sobre esses padrões, consulte Referência de padrões para o Security Hub CSPM o.

Se você preferir ativar manualmente os padrões de segurança para novas contas de membros, poderá desativar a ativação automática dos padrões padrão. Você só pode fazer isso se integrar AWS Organizations e usar a configuração local. Se você usar a configuração central, poderá criar uma política de configuração que habilite os padrões padrão e associe a política à raiz. Todas as contas da sua organização e OUs , em seguida, herdam essa política de configuração, a menos que estejam associadas a uma política diferente ou sejam autogerenciadas. Se você não fizer a integração com AWS Organizations, poderá desabilitar um padrão padrão ao habilitar inicialmente o Security Hub CSPM ou posterior. Para saber como, consulte Desabilitar um padrão.

Para desativar a ativação automática dos padrões padrão para novas contas de membros, você pode usar o console CSPM do Security Hub ou a API CSPM do Security Hub.

Security Hub CSPM console

Siga estas etapas para desativar a ativação automática dos padrões padrão usando o console CSPM do Security Hub.

Para desativar a ativação automática dos padrões padrão

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

   Faça login usando as credenciais da conta de administrador.
2. No painel de navegação, em Configurações, selecione Configuração.
3. Na seção Visão geral, selecione Editar.

4. Em Novas configurações de conta, desmarque a caixa de seleção Ativar os padrões de segurança padrão.
5. Escolha Confirmar.

Security Hub CSPM API

Para desativar a ativação automática dos padrões padrão de forma programática, na conta de administrador do Security Hub CSPM, use a operação da API CSPM UpdateOrganizationConfigurationdo Security Hub. Em sua solicitação, `NONE` especifique o `AutoEnableStandards` parâmetro.

Se você estiver usando o AWS CLI, execute o update-organization-configurationcomando para desativar a ativação automática dos padrões padrão. Para o parâmetro `auto-enable-standards`, especifique `NONE`. Por exemplo, o comando a seguir ativa automaticamente o CSPM do Security Hub para novas contas de membros e desativa a ativação automática dos padrões padrão para as contas.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Desabilitar um padrão de segurança

Quando você desabilita um padrão de segurança no CSPM do AWS Security Hub, ocorre o seguinte:

- Todos os controles que se aplicam ao padrão estão desativados, a menos que estejam associados a outro padrão atualmente ativado.
- As verificações de segurança dos controles desativados não são mais realizadas e nenhuma descoberta adicional é gerada para os controles desativados.
- As descobertas existentes para os controles desativados são arquivadas automaticamente após aproximadamente 3 a 5 dias.
- AWS Config as regras que o Security Hub CSPM criou para os controles desativados são excluídas.

A exclusão das AWS Config regras apropriadas geralmente ocorre alguns minutos após a desativação de um padrão. No entanto, pode levar mais tempo. Se a primeira solicitação não

conseguir excluir as regras, o Security Hub CSPM tentará novamente a cada 12 horas. No entanto, se você desativou o CSPM do Security Hub ou não tem nenhum outro padrão habilitado, o Security Hub CSPM não pode tentar novamente, o que significa que ele não pode excluir as regras. Se isso ocorrer e você precisar excluir as regras, entre em contato AWS Support.

Tópicos

Desativando um padrão em várias contas e Regiões da AWS

Para desativar um padrão de segurança em várias contas e Regiões da AWS use a configuração central. Com a configuração central, o administrador delegado do CSPM do Security Hub pode criar políticas de configuração do CSPM do Security Hub que desabilitam um ou mais padrões. O administrador pode então associar uma política de configuração a contas individuais, unidades organizacionais (OUs) ou à raiz. Uma política de configuração afeta a região de origem, também chamada de região de agregação, e todas as regiões vinculadas.

As políticas de configuração oferecem opções de personalização. Por exemplo, você pode optar por desativar o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) em uma OU. Para outra OU, você pode optar por desativar o padrão PCI DSS e o padrão SP 800-53 Rev. 5 do Instituto Nacional de Padrões e Tecnologia (NIST). Para obter informações sobre como criar uma política de configuração que habilite ou desabilite padrões individuais que você especificar, consulteCriação e associação de políticas de configuração.

> **Note**
>
> O administrador do CSPM do Security Hub pode usar políticas de configuração para desativar qualquer padrão, exceto o padrão gerenciado pelo AWS Control Tower serviço. Para desativar esse padrão, o administrador deve usar AWS Control Tower diretamente. Eles também devem ser usados AWS Control Tower para desativar ou ativar controles individuais nesse padrão para uma conta gerenciada centralmente.

Se você quiser que algumas contas configurem ou desabilitem padrões para suas próprias contas, o administrador do CSPM do Security Hub pode designar essas contas como contas autogerenciadas. As contas autogerenciadas devem desativar os padrões separadamente em cada região.

Desativando um padrão em uma única conta e Região da AWS

Se você não usa a configuração central ou tem uma conta autogerenciada, não pode usar políticas de configuração para desabilitar centralmente os padrões de segurança em várias contas ou. Regiões da AWS No entanto, você pode desativar um padrão em uma única conta e região. Você pode fazer isso usando o console CSPM do Security Hub ou a API CSPM do Security Hub.

Security Hub CSPM console

Siga estas etapas para desativar um padrão em uma conta e região usando o console CSPM do Security Hub.

Para desabilitar um padrão em uma conta e região

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Usando o Região da AWS seletor no canto superior direito da página, escolha a região na qual você deseja desativar o padrão.
3. No painel de navegação, escolha Padrões de segurança.
4. Na seção do padrão que você deseja desativar, escolha Desativar padrão.

Para desativar o padrão em regiões adicionais, repita as etapas anteriores em cada região adicional.

Security Hub CSPM API

Para desativar um padrão programaticamente em uma única conta e região, use a BatchDisableStandardsoperação. Ou, se você estiver usando o AWS Command Line Interface (AWS CLI), execute o batch-disable-standardscomando.

Em sua solicitação, use o `StandardsSubscriptionArns` parâmetro para especificar o Amazon Resource Name (ARN) do padrão que você deseja desativar. Se você estiver usando o AWS CLI, use o `standards-subscription-arns` parâmetro para especificar o ARN. Especifique também a região à qual sua solicitação se aplica. Por exemplo, o comando a seguir desativa o padrão AWS Foundational Security Best Practices (FSBP) para uma conta (): *123456789012*

```
$ aws securityhub batch-disable-standards \
```

```
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Onde *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* está o ARN do padrão FSBP para a conta na região Leste dos EUA (Norte da Virgínia) e *us-east-1* a região na qual desativá-la.

Para obter o ARN de um padrão, você pode usar a GetEnabledStandardsoperação. Essa operação recupera informações sobre os padrões atualmente habilitados em sua conta. Se você estiver usando o AWS CLI, você pode executar o get-enabled-standardscomando para recuperar essas informações.

Depois de desativar um padrão, o Security Hub CSPM começa a executar tarefas para desabilitar o padrão na conta e na região especificada. Isso inclui desativar todos os controles que se aplicam ao padrão. Para monitorar o status dessas tarefas, você pode verificar o status do padrão para a conta e a região.

Entendendo os controles de segurança no Security Hub CSPM

No AWS Security Hub CSPM, um controle de segurança, também chamado de 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 CSPM, um controle está relacionado a um recurso específico AWS .

Quando você habilita um controle em um ou mais padrões, o Security Hub CSPM começa a executar verificações de segurança nele. As verificações de segurança resultam nas descobertas do CSPM do Security Hub. Quando você desabilita um controle, o Security Hub CSPM para de executar verificações de segurança nele e as descobertas não são mais geradas.

Você pode ativar ou desativar os controles individualmente para uma única conta Região da AWS e. Para poupar tempo e reduzir desvios de configuração em ambientes com várias contas, recomendamos o uso da configuração central para habilitar e desabilitar controles. Com a configuração central, o administrador delegado do CSPM do Security Hub pode criar políticas que especificam como um controle deve ser configurado em várias contas e regiões. Para obter mais informações sobre como habilitar e desabilitar controles, consulte Habilitando controles no Security Hub CSPM.

Visualizar controles consolidados

A página Controles do console CSPM 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 CSPM atribui aos controles um ID, título e descrição de controle de segurança consistentes em todos os padrões. IDs Os 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 CSPM 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
- Detalhamento dos status de controle em todos os controles CSPM do Security Hub suportados
- O número de verificações de segurança aprovadas e reprovadas.
- O número de verificações de segurança de controles reprovadas com diferente gravidade e links para ver mais detalhes sobre essas verificações reprovadas.
- Uma lista de controles CSPM do Security Hub, com filtros para visualizar subconjuntos específicos de controles.

Na página Controles, você pode 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 obter mais informações, consulte Habilitando controles no Security Hub CSPM.

Para contas de administrador, a página Controles reflete o status dos controles nas contas dos membros. Se uma verificação de controle for reprovada em pelo menos uma conta-membro, o status do controle será Reprovado. 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 for reprovada em pelo menos uma região vinculada, o status do controle será Reprovado.

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 obter mais informações, consulte Visualização de controles consolidados - Alterações no ASFF.

Resumo da pontuação de segurança dos controles

A página Controles exibe um resumo da pontuação de segurança de 0 a 100%. Um resumo da pontuação de segurança baseada na proporção de controles aprovados em relação ao número total de controles habilitados com dados em vários padrões.

> **Note**
>
> Para ver a pontuação geral de segurança dos controles, você deve adicionar permissão para chamar a função do IAM que você usa **`BatchGetControlEvaluations`**para acessar o CSPM do Security Hub. Essa permissão não é necessária para visualizar as pontuações de segurança de padrões específicos.

Quando você ativa o CSPM do Security Hub, o CSPM do Security Hub calcula a pontuação de segurança inicial dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de segurança no console do CSPM 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) Regions.

Além da pontuação geral de segurança, o Security Hub CSPM calcula uma pontuação de segurança padrão para cada padrão ativado dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de segurança. Para ver uma lista dos padrões atualmente habilitados, usa a operação da API `GetEnabledStandards`.

AWS Config deve ser habilitado com a gravação de recursos para que as pontuações apareçam. Para obter informações sobre como o Security Hub CSPM calcula as pontuações de segurança, consulte. Calcular pontuações de segurança

Após a primeira geração de pontuação, o CSPM do Security Hub atualiza as pontuações de segurança a cada 24 horas. O CSPM do Security Hub exibe um carimbo de data/hora para indicar quando uma pontuação de segurança foi atualizada pela última vez.

Se você definiu uma região de agregação, as pontuações de segurança geral incluem as descobertas de controles em todas as regiões vinculadas.

Referência de controle para o Security Hub CSPM

Essa referência de controle fornece uma tabela dos controles CSPM disponíveis do AWS Security Hub com links para mais informações sobre cada controle. Na tabela, os controles são listados em

ordem alfabética por ID de controle. Somente os controles em uso ativo pelo Security Hub CSPM estão incluídos aqui. Os controles retirados são excluídos da tabela.

A tabela fornece as seguintes informações para cada controle:

- 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 CSPM do Security Hub exibe o controle de segurança IDs, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas em sua conta. No entanto, as descobertas do CSPM do Security Hub fazem referência ao controle de segurança IDs somente se as descobertas de controle consolidado estiverem ativadas em sua conta. Se as descobertas de controle consolidadas estiverem desativadas em sua conta, alguns controles IDs variam de acordo com o padrão em suas descobertas de controle. Para um mapeamento do controle específico do padrão IDs para o controle de segurança IDs, consulte. Como a consolidação afeta o controle IDs e os títulos

  Se quiser configurar automações para controles de segurança, recomendamos filtrar com base na ID do controle, e não no título ou na descrição. Embora o Security Hub CSPM possa ocasionalmente atualizar títulos ou descrições de controle, o controle IDs permanece o mesmo.

  O controle IDs pode pular números. Esses são espaços reservados para futuros controles.
- Título de controle de segurança: esse título se aplica a todos os padrões. O console CSPM do Security Hub exibe títulos de controle de segurança, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas em sua conta. No entanto, as descobertas do CSPM 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 do controle específico do padrão IDs para o controle de segurança IDs, consulte. Como a consolidação afeta o controle IDs e os títulos
- Padrões aplicáveis: indica a quais padrões um controle se aplica. Escolha um controle para analisar requisitos específicos de estruturas de conformidade de terceiros.
- Severidade: a severidade de um controle identifica sua importância do ponto de vista da segurança. Para obter informações sobre como o Security Hub CSPM determina a severidade do controle, consulte. Níveis de severidade para resultados de controle
- Oferece suporte a parâmetros personalizados: indica se o controle oferece suporte a valores personalizados para um ou mais parâmetros. Escolha um controle para revisar os detalhes do

parâmetro. Para obter mais informações, consulte Entendendo os parâmetros de controle no Security Hub CSPM.

- Tipo de programação: indica quando o controle é avaliado. Para obter mais informações, consulte Programar a execução de verificações de segurança.

Escolha um controle para revisar detalhes adicionais. Os controles são listados em ordem alfabética por ID de controle de segurança.

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Account.1	As informações de contato de segurança devem ser fornecidas para um Conta da AWS	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MÉDIO	 Não	Periódico
Account.2	Conta da AWS deve fazer parte de uma AWS Organizations organização	NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Não	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. 5 AWS Control Tower,	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 de programação
		NIST SP 800-171 Rev. 2, PCI DSS v4.0.1			
ACM.2	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, PCI DSS v4.0.1	HIGH (ALTO)	 Não	Acionado por alterações
ACM.3	Os certificados do ACM devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
Amplificar.1	Os aplicativos Amplify devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
Amplificar.2	As ramificações do Amplify 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 de programação
APIGateway1.	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.2	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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações
APIGateway.3	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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
APIGateway.4	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	Não	Acionado por alterações
APIGateway.5.	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	Não	Acionado por alterações
APIGateway.8.	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

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
APIGateway9.	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, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
AppConfig1.	AWS AppConfig os aplicativos devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
AppConfig.2	AWS AppConfig perfis de configuração devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
AppConfig.3	AWS AppConfig ambientes devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
AppConfig.4	AWS AppConfig associações de extensão 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 de programação
AppFlow1.	AppFlow Os fluxos da Amazon devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
AppRunner1.	Os serviços do App Runner devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
AppRunner.2	Os conectores VPC do App Runner devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
AppSync1.	AWS AppSync Os caches de API devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	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, PCI DSS v4.0.1	MÉDIO	 Sim	Acionado por alterações
AppSync.4	AWS AppSync GraphQL APIs deve ser marcado	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 de programação
AppSync5.	AWS AppSync O GraphQL não APIs deve ser autenticado com chaves de API	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Não	Acionado por alterações
AppSync.6	AWS AppSync Os caches de API devem ser criptografados em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
Athena.2	Os catálogos de dados do Athena devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Athena.3	Os grupos de trabalho do Athena devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Athena.4	Os grupos de trabalho do Athena devem ter o registro em log habilitado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
AutoScaling1.	Os grupos do 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	Não	Acionado por alterações
AutoScaling.2	O grupo Amazon EC2 Auto Scaling deve cobrir 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
AutoScaling.3	As configurações de lançamento em grupo do Auto Scaling devem configurar as EC2 instâncias para exigir 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, PCI DSS v4.0.1	HIGH (ALTO)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Auto Scaling	EC2 As instâncias da Amazon lançadas usando as configurações de lançamento 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, PCI DSS v4.0.1	HIGH (ALTO)	 Não	Acionado por alterações
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	 Não	Acionado por alterações
AutoScaling9.	EC2 Grupos de Auto Scaling devem usar EC2 modelos de lançamento	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	MÉDIO	 Não	Acionado por alterações
AutoScaling.10	EC2 Grupos de Auto Scaling 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 de programação
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	Não	Acionado por alterações
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
Backup.4	AWS Backup os planos de relatórios devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Backup.5	AWS Backup planos de backup devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Lote.1	As filas de trabalhos em lote 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 de programação
Lote.2	As políticas de agendamento em lote devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Lote.3	Ambientes de computação em lote devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Lote.4	As propriedades dos recursos computacionais em ambientes de computação gerenciados em Batch devem ser marcadas	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, PCI DSS v4.0.1	HIGH (ALTO)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudFront.3	CloudFront as distribuições devem exigir criptografia em trânsito	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	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	Não	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, PCI DSS v4.0.1	MÉDIO	Não	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, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
CloudFront.7.	CloudFront as distribuições devem usar certificados personalizados SSL/TLS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudFront.8.	CloudFront as distribuições devem usar o SNI para atender solicitações HTTPS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	BAIXO	Não	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, PCI DSS v4.0.1	MÉDIO	Não	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, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MÉDIO	Não	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, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
CloudFront.13	CloudFront as distribuições devem usar o controle de acesso de origem	AWS Melhores práticas básicas de segurança v1.0.0	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudFront.4	CloudFront distribuições devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
CloudFront.5	CloudFront as distribuições devem usar a política de segurança TLS recomendada	AWS Melhores práticas básicas de segurança v1.0.0	MÉDIO	Não	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 v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básica, padrão gerenciado por serviços:, NIST SP AWS 800-53 Rev. 5 AWS Control Tower	HIGH (ALTO)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudTrail.2	CloudTrail deve ter a criptografia em repouso ativada	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0 AWS AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Periódico
CloudTrail.3	Pelo menos uma CloudTrail trilha deve ser ativada	NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	HIGH (ALTO)	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudTrail.4	CloudTrail a validação do arquivo de log deve estar ativada	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudTrail.5.	CloudTrail as trilhas devem ser integradas ao Amazon CloudWatch Logs	CIS AWS Foundations Benchmark v1.2.0, CIS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	 Não	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 AWS Foundations v1.4.0, PCI DSS v4.0.1	CRÍTICO	 Não	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, Referência do CIS AWS Foundations v3.0.0, PCI DSS v4.0.1 AWS	BAIXO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudTrail9.	CloudTrail trilhas devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
CloudTrail.10	CloudTrail Os armazenamentos de dados de eventos do Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys	NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico
CloudWatch1.	Um filtro de métrica de log e um alarme devem existir para uso do usuário “raiz”	Referência do CIS AWS Foundations v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	BAIXO	Não	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, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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	Não	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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico
CloudWatch5.	Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração	Referência do CIS AWS Foundations v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudWatch7.	Certifique-se de que exista um filtro métrico de registro e um alarme para desativação ou exclusão programada do cliente criado CMKs	Referência do CIS AWS Foundations v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico
CloudWatch8.	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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico
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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico
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 v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico
CloudWatch1.4	Verificar se existe um alarme e um filtro de métrica de log para alterações de VPC	Referência do CIS AWS Foundations v1.4.0, Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	BAIXO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CloudWatch1.5	CloudWatch os alarmes devem ter ações especificadas configuradas	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (ALTO)	 Sim	Acionado por alterações
CloudWatch1.6	CloudWatch grupos de registros devem ser mantidos por um período de tempo especificado	NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Periódico
CloudWatch1.7	CloudWatch ações de alarme devem ser ativadas	NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Não	Acionado por alterações
CodeArtifact1.	CodeArtifact repositórios devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
CodeBuild1.	CodeBuild O repositório de origem do Bitbucket não URLs deve conter credenciais confidenciais	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CodeBuild.2	CodeBuild as variáveis de ambiente do projeto não devem conter credenciais de texto não criptografado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	Não	Acionado por alterações
CodeBuild.3	CodeBuild Os registros do S3 devem ser criptografados	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços:, AWS Control Tower	BAIXO	Não	Acionado por alterações
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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
CodeBuild 7.	CodeBuild as exportações do grupo de relatórios devem ser criptografadas em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
CodeGuruProfiler1.	CodeGuru Os grupos de criação de perfil do Profiler devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
CodeGuruReviewer1.	CodeGuru As associações do repositório do revisor devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Cognito.1	Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão	AWS Melhores práticas básicas de segurança	MÉDIO	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Cognito.2	Os grupos de identidades do Cognito não devem permitir identidades não autenticadas	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Acionado por alterações
Config.1	AWS Config deve ser habilitado e usar a função vinculada ao serviço para registro de recursos	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança básica, AWS NIST SP 800-53 Rev. 5, PCI AWS DSS v3.2.1	CRÍTICO	 Sim	Periódico
Conecte-se. 1	Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
Conecte-se.2	As instâncias do Amazon Connect devem ter CloudWatch o registro ativado	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DataFirehose1.	Os fluxos de entrega do Firehose devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Periódico
DataSync1.	DataSync as tarefas devem ter o registro ativado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
DataSync.2	DataSync as tarefas devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Detetive.1	Gráficos de comportamento do Detective devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
DMS.1	As instâncias de replicação do Database Migration Service não devem ser públicas	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DMS.2	Os certificados do 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
DMS.6	As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DMS.7	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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações
DMS.8	As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações
DMS.9	Os endpoints do DMS devem usar SSL	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações
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, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DMS.11	Os endpoints do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
DMS.12	Os endpoints do DMS para o Redis OSS devem ter o TLS habitado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
DocumentDB.1	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	Não	Acionado por alterações
DocumentDB.2	Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DocumentDB.3	Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	 Não	Acionado por alterações
DocumentDB.4	Os clusters do Amazon DocumentDB devem publicar registros de auditoria em Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações
DocumentDB.5	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	 Não	Acionado por alterações
DocumentDB.6	Os clusters do Amazon DocumentDB devem ser criptografados em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
DynamoDB.1	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

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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	Não	Acionado por alterações
DynamoDB 3	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	Não	Periódico
DynamoDB 4	As tabelas do DynamoDB devem estar presentes em um plano de backup	NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico
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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
DynamoDB 7	Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Periódico
EC21.	[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	CRÍTICO	Não	Periódico
EC2.2	Os grupos de segurança padrão da VPC não devem permitir o tráfego de entrada e saída	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP AWS Control Tower 800-53 Rev. 5 AWS	HIGH (ALTO)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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	 Não	Acionado por alterações
EC2.4	EC2 As instâncias 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 de programação
EC2.6	O registro de fluxo de VPC deve ser ativado em todos VPCs	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2 AWS	MÉDIO	Não	Periódico
EC27.	A criptografia padrão do EBS deve estar ativada	CIS AWS Foundations Benchmark v3.0.0, 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	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC28.	EC2 as instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2	CIS AWS Foundations Benchmark v3.0.0, Melhores práticas básicas de segurança AWS, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Acionado por alterações
EC29.	EC2 instâncias não devem ter um IPv4 endereço 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)	Não	Acionado por alterações
EC2.10	A Amazon EC2 deve ser configurada para usar endpoints 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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC21.2	Não utilizado EC2 EIPs deve ser removido	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	BAIXO	Não	Acionado por alterações
EC21.3	Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou de ::/0 na porta 22	Referência do CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (ALTO)	Não	Acionado por alterações e periódico
EC21.4	Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou de ::/0 na porta 3389	Referência do CIS AWS Foundations v1.2.0, PCI DSS v4.0.1	HIGH (ALTO)	Não	Acionado por alterações e periódico
EC21.5	EC2 as sub-redes não devem atribuir automaticamente endereços IP públicos	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços:, AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC21.6	As listas de controle de acesso à rede não utilizadas devem ser removidas	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão de gerenciamento de serviços:, AWS Control Tower	BAIXO	 Não	Acionado por alterações
EC21.7	EC2 instâncias não devem usar várias ENIs	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	BAIXO	 Não	Acionado por alterações
EC21.8	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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	HIGH (ALTO)	 Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC21.9	Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	CRÍTICO	 Não	Acionado por alterações e periódico
EC2.20	Ambos os túneis VPN de uma conexão AWS Site-to-Site VPN devem estar ativos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC22.1	A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Melhores práticas de segurança AWS fundamental, padrão gerenciado por serviços:, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2 AWS Control Tower, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
EC22.2	Grupos de EC2 segurança não utilizados devem ser removidos	Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Periódico
EC22.3	EC2 Os 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)	Não	Acionado por alterações
EC22.4	EC2 tipos de instância paravirtual não devem ser usados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC22,5	EC2 os modelos de lançamento não devem atribuir interfaces públicas IPs às de rede	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Acionado por alterações
EC22.8	Os volumes do EBS devem estar em um plano de backup	NIST SP 800-53 Rev. 5	BAIXO	Sim	Periódico
EC23.3	EC2 os anexos do gateway de trânsito devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC23.4	EC2 as tabelas de rotas do gateway de trânsito devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC23.5	EC2 interfaces de rede 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 de programação
EC23.6	EC2 os gateways do cliente devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC23.7	EC2 Endereços IP elásticos devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC23,8	EC2 instâncias devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC23.9	EC2 gateways de internet devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24,0	EC2 Os gateways NAT devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24.1	EC2 a rede ACLs deve ser marcada	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 de programação
EC24.2	EC2 tabelas de rotas devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24.3	EC2 grupos de segurança devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24.4	EC2 as sub-redes devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24,5	EC2 os volumes devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24.6	Amazon VPCs deve ser etiquetada	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EC24.7	Os serviços de endpoint da Amazon VPC 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 de programação
EC24.8	Os logs de fluxo da Amazon VPC devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC24.9	As conexões de emparelhamento da Amazon VPC devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC25,0	EC2 Os gateways de VPN devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC25.1	EC2 Os endpoints do Client VPN devem ter o registro de conexão do cliente ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	BAIXO	Não	Acionado por alterações
EC25.2	EC2 os gateways de trânsito 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 de programação
EC25.3	EC2 grupos de segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração do servidor remoto	Referência do CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
EC25,4	EC2 grupos de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto	Referência do CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
EC25.5	VPCs deve ser configurado com um endpoint de interface para a API ECR	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico
EC25,6	VPCs deve ser configurado com um endpoint de interface para o Docker Registry	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico
EC25,7	VPCs deve ser configurado com um endpoint de interface para Systems Manager	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC25,8	VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Periódico
EC26,0	VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Periódico
EC21.70	EC2 os modelos de lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	BAIXO	 Não	Acionado por alterações
EC21.71	EC2 As conexões VPN devem ter o registro ativado	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações
EC21.72	EC2 As configurações do VPC Block Public Access devem bloquear o tráfego do gateway da Internet	AWS Melhores práticas básicas de segurança	MÉDIO	 Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EC21.73	EC2 As solicitações do Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
EC21.74	EC2 Os conjuntos de opções DHCP devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC21.75	EC2 os modelos de lançamento devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC21.76	EC2 listas de prefixos devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC21.77	EC2 sessões de espelhos de tráfego 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 de programação
EC2.178	EC2 filtros de espelhos de trânsito devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC2.179	EC2 alvos de espelhos de tráfego devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
EC21.80	EC2 as interfaces de rede devem ter a source/destination verificação ativada	AWS Melhores práticas básicas de segurança v1.0.0	MÉDIO	Não	Acionado por alterações
ECR.1	Os repositórios privados do ECR devem ter a digitalização de imagens configurada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ECR.2	Os repositórios privados do ECR devem ter a imutabilidade de tags configurada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	MÉDIO	 Não	Acionado por alterações
ECR.3	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	 Não	Acionado por alterações
ECR.4	Os repositórios públicos do ECR devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
ECR.5	Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys	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 de programação
ECS.1	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)	 Não	Acionado por alterações
ECS.2	Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Acionado por alterações
ECS.3	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)	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ECS.4	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)	Não	Acionado por alterações
ECS.5	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)	Não	Acionado por alterações
ECS.8	Os segredos não devem ser passados como variáveis de ambiente do contêiner	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Acionado por alterações
ECS.9	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)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ECS.10	Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações
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	Não	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

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ECS.15	As definições de tarefa do ECS devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
ECS.16	Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Acionado por alterações
ECS.17	As definições de tarefas do ECS não devem usar o modo de rede host	NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
EFS.1	O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EFS.2	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	Não	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	Não	Acionado por alterações
EFS.4	Os pontos de acesso do EFS devem impor uma identidade de usuário	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	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 de programação
EFS.6	Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
EFS.7	Os sistemas de arquivos do EFS devem ter backups automáticos habilitados	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Acionado por alterações
EFS.8	Os sistemas de arquivos do EFS devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	 Sim	Acionado por alterações
EKS.1	Os endpoints do cluster EKS não devem ser acessíveis ao público	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (ALTO)	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EKS.2	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Acionado por alterações
EKS.3	Os clusters do EKS devem usar segredos criptografados do Kubernetes	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Periódico
EKS.6	Os clusters do EKS devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
EKS.7	As configurações do provedor de identidades do 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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ElastiCache1.	ElastiCache Os clusters (Redis OSS) devem ter backups automáticos habilitados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Sim	Periódico
ElastiCache.2	ElastiCache os clusters devem ter atualizações automáticas de versões secundárias habilitadas	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	HIGH (ALTO)	 Não	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	 Não	Periódico
ElastiCache.4	ElastiCache grupos de replicação devem ser encrypted-at-rest	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	 Não	Periódico
ElastiCache5.	ElastiCache grupos de replicação devem ser encrypted-in-transit	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ElastiCache.6	ElastiCache Grupos de replicação (Redis OSS) de versões anteriores devem ter o Redis OSS AUTH ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	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)	 Não	Periódico
ElasticBeanstalk1.	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	 Não	Acionado por alterações
ElasticBeanstalk.2	As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ElasticBeanstalk.3	O Elastic Beanstalk deve transmitir registros para CloudWatch	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	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	 Não	Periódico
ELB.2	Os balanceadores de carga clássicos com SSL/HTTPS ouvintes 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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ELB.3	Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações
ELB.4	O Application Load Balancer deve ser configurado para eliminar cabeçalhos http	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações
ELB.5	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	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ELB.6	A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
ELB.7	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	Não	Acionado por alterações
ELB.8	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, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ELB.9	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	Não	Acionado por alterações
ELB.10	O Classic Load Balancer deve abranger 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.12	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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ELB.13	Balanceadores de carga de aplicações, redes e gateways devem abranger 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.14	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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações
ELB.16	Os balanceadores de carga de aplicativos devem ser associados a uma ACL web do AWS WAF	NIST SP 800-53 Rev. 5	MÉDIO	 Não	Acionado por alterações
ELB.17	Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ELB.18	Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito	AWS Melhores práticas básicas de segurança v1.0.0	MÉDIO	 Não	Acionado por alterações
EMR.1	Os nós primários do cluster Amazon EMR não devem ter endereços IP públicos	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Periódico
EMR.2	A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	 Não	Periódico
EMR.3	As configurações de segurança do Amazon EMR devem ser criptografadas em repouso	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
EMR.4	As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
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	Não	Periódico
ES.2	Os domínios do Elasticsearch não devem ser publicamente acessíveis	AWS Melhores práticas básicas de segurança, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ES.3	Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços:, AWS Control Tower	MÉDIO	Não	Acionado por alterações
ES.4	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	Não	Acionado por alterações
ES.5	Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
ES.6	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	Não	Acionado por alterações
ES.7	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	Não	Acionado por alterações
ES.8	As conexões com os domínios do Elasticsearch devem ser criptografadas com a política de segurança TLS mais recente	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações
ES.9	Os domínios do Elasticsearch 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 de programação
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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAIXO	Não	Acionado por alterações
EventBridge.4	EventBridge endpoints globais devem ter a replicação de eventos ativada	NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
FraudDetector1.	Os tipos de entidade do Amazon Fraud Detector devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
FraudDetector.2	Os rótulos do Amazon Fraud Detector 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 de programação
FraudDetector.3	Os resultados do Amazon Fraud Detector devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
FraudDetector.4	As variáveis do Amazon Fraud Detector devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
FSx1.	FSx para OpenZFS, os sistemas de arquivos devem ser configurados para copiar tags para backups e volumes	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	BAIXO	 Não	Periódico
FSx.2	FSx para Lustre, os sistemas de arquivos devem ser configurados para copiar tags para backups	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	BAIXO	 Não	Periódico
FSx.3	FSx para OpenZFS, os sistemas de arquivos devem ser configurados para implantação Multi-AZ	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
FSx.4	FSx para sistemas de arquivos NetApp ONTAP, os sistemas de arquivos devem ser configurados para implantação Multi-AZ	AWS Melhores práticas básicas de segurança	MÉDIO	 Sim	Periódico
FSx5.	FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
Glue.1	AWS Glue os trabalhos devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
Glue.3	AWS Glue as transformações de aprendizado de máquina devem ser criptografadas em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Cola.4	AWS Glue Os trabalhos do Spark devem ser executados em versões compatíveis do AWS Glue	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
GlobalAccelerator1.	Os aceleradores do Global Accelerator devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
GuardDuty 1.	GuardDuty deve ser habilitado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Periódico
GuardDuty .2	GuardDuty os filtros 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 de programação
GuardDuty.3	GuardDuty IPSets deve ser marcado	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
GuardDuty.5.	GuardDuty O monitoramento do registro de auditoria do EKS deve estar ativado	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Periódico
GuardDuty.6	GuardDuty A Proteção Lambda deve estar ativada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
GuardDuty.7.	GuardDuty O monitoramento de tempo de execução do EKS deve estar ativado	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
GuardDuty 8.	GuardDuty A proteção contra malware para EC2 deve estar ativada	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Periódico
GuardDuty 9.	GuardDuty A proteção do RDS deve estar ativada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
GuardDuty .10	GuardDuty A proteção S3 deve estar ativada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
GuardDuty 1.1	GuardDuty O monitoramento de tempo de execução deve estar ativado	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Periódico
GuardDuty 1.2	GuardDuty O ECS Runtime Monitoring deve estar ativado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Periódico
GuardDuty 1.3	GuardDuty EC2 O monitoramento de tempo de execução deve estar ativado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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 AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	HIGH (ALTO)	 Não	Acionado por alterações
IAM.2	Os usuários do IAM não devem ter políticas do IAM anexadas	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP AWS Control Tower 800-171 Rev. 2	BAIXO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.3	As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básica, NIST SP 800-53 Rev. 5, AWS PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Periódico
IAM.4	A chave de acesso do usuário raiz do IAM não deve existir	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	CRÍTICO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.5	A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básica, NIST SP 800-53 Rev. 5, AWS PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.6	A MFA de hardware deve estar habilitada para o usuário raiz	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básica, NIST SP 800-53 Rev. 5, AWS PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	 Não	Periódico
IAM.7	Políticas de senha para usuários do IAM que devem ter configurações fortes	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.8	As credenciais de usuário do IAM não utilizadas devem ser removidas	CIS AWS AWS Foundations Benchmark v1.2.0, Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Periódico
IAM.9	A MFA deve estar habilitada para o usuário raiz	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. AWS 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	 Não	Periódico
IAM.10	Políticas de senha para usuários do IAM que devem ter configurações fortes	NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	MÉDIO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MÉDIO	 Não	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, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MÉDIO	 Não	Periódico
IAM.13	Certifique-se que política de senha do IAM exija pelo menos um símbolo	Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2	MÉDIO	 Não	Periódico
IAM.14	Certifique-se que política de senha do IAM exija pelo menos um número	Referência do CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MÉDIO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.15	Certifique-se que a política de senha do IAM exija um comprimento mínimo de 14 ou mais	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP AWS 800-171 Rev. 2	MÉDIO	 Não	Periódico
IAM.16	Certifique-se que a política de senha do IAM impeça a reutilização de senhas	Benchmark CIS AWS Foundations v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI AWS DSS v4.0.1	BAIXO	 Não	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, PCI DSS v4.0.1	BAIXO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.18	Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support	Benchmark CIS AWS Foundations v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI AWS DSS v4.0.1	BAIXO	 Não	Periódico
IAM.19	A MFA deve estar habilitada para todos os usuários do IAM	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MÉDIO	 Não	Periódico
IAM.21	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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	BAIXO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.22	As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas	Referência do CIS AWS Foundations v3.0.0, Referência do CIS AWS Foundations v1.4.0, NIST SP 800-171 Rev. 2	MÉDIO	Não	Periódico
IAM.23	Os analisadores do IAM Access Analyzer devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IAM.24	Os perfis do IAM devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IAM.25	Os usuários do IAM devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IAM.26	SSL/TLS Os certificados expirados gerenciados no IAM devem ser removidos	Referência do CIS AWS Foundations v3.0.0	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IAM.27	As identidades do IAM não devem ter a AWSCloud ShellFull Access política anexada	Referência do CIS AWS Foundations v3.0.0	MÉDIO	Não	Acionado por alterações
IAM.28	O analisador de acesso externo do IAM Access Analyzer deve ser habilitado	Referência do CIS AWS Foundations v3.0.0	HIGH (ALTO)	Não	Periódico
Inspector.1	O EC2 escaneamento do Amazon Inspector deve estar ativado	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
Inspector.2	A varredura do ECR pelo Amazon Inspector deve estar habilitada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
Inspector.3	A varredura de código do Lambda pelo Amazon Inspector deve estar habilitada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
Inspector.4	A varredura padrão do Lambda pelo Amazon Inspector deve estar habilitada	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
IoT.1	AWS IoT Device Defender 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
IoT.6	AWS IoT Core as políticas 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 de programação
IoT TEvents 1.1	AWS IoT Events as entradas devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IoT TEvents 1.2	AWS IoT Events modelos de detectores devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IoT TEvents 3.3	AWS IoT Events modelos de alarme devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Eu sou TSitesábio.1	AWS IoT SiteWise modelos de ativos devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Eu sou TSitesábio.2	AWS IoT SiteWise os painéis devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Eu sou TSitesábio.3	AWS IoT SiteWise gateways 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 de programação
Eu sou TSite sábio.4	AWS IoT SiteWise portais devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Eu sou TSite sábio.5	AWS IoT SiteWise projetos devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Io TTwin Maker. 1	AWS Os trabalhos de TwinMaker sincronização de IoT devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Io TTwin Maker.2	AWS Os TwinMaker espaços de trabalho de IoT devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Io TTwin Maker.3	AWS As TwinMaker cenas de IoT devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Io TTwin Maker.4	AWS As TwinMaker entidades de IoT 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 de programação
IoT TWireless 1.1	AWS Os grupos multicast do IoT Wireless devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IoT TWireless 1.2	AWS Os perfis de serviço IoT Wireless devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IoT TWireless 3.3	AWS As tarefas do IoT Wireless FUOTA devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IVS.1	Os pares de teclas de reprodução do IVS devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IV.2	As configurações de gravação IVS devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
IV.3	Os canais IVS 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 de programação
Espaços-chave. 1	Os keyspaces do Amazon Keyspaces devem ser marcados	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	Não	Acionado por alterações
Kinesis.2	Os fluxos do Kinesis devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Kinesis.3	Os fluxos do Kinesis devem ter um período de retenção de dados adequado	AWS Melhores práticas básicas de segurança	MÉDIO	Sim	Acionado por alterações
KMS.1	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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
KMS.2	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	Não	Acionado por alterações
KMS.3	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	CRÍTICO	Não	Acionado por alterações
KMS.4	AWS KMS key a rotação deve ser ativada	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. AWS 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
KMS.5	As chaves do KMS não devem ser acessíveis publicamente	AWS Melhores práticas básicas de segurança	CRÍTICO	Não	Acionado por alterações
Lambda.1	As funções do Lambda devem proibir o acesso público	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	Não	Acionado por alterações
Lambda.2	As funções do Lambda devem usar os tempos de execução compatíveis	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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
Lambda.6	As funções do Lambda devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Lambda.7	As funções Lambda devem ter o rastreamento AWS X-Ray ativo ativado	NIST SP 800-53 Rev. 5	BAIXO	Não	Acionado por alterações
Macie.1	O Amazon Macie deve ser habilitado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	Não	Periódico
Macie.2	A descoberta automatizada de dados confidenciais do Macie deve estar habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
MSK.1	Os clusters MSK devem ser criptografados em trânsito entre os nós do agente	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
MSK.2	Os clusters do MSK devem ter um monitoramento aprimorado configurado	NIST SP 800-53 Rev. 5	BAIXO	Não	Acionado por alterações
MSK.3	Os conectores da MSK Connect devem ser criptografados em trânsito	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
MÁSCARA	Os clusters MSK devem ter o acesso público desativado	AWS Melhores práticas básicas de segurança	CRÍTICO	Não	Acionado por alterações
MÁSCARA	Os conectores MSK devem ter o registro ativado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
MÁSCARA 6	Os clusters MSK devem desativar o acesso não autenticado	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
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, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
MQ.3	Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAIXO	Não	Acionado por alterações
MQ.4	Os agentes do Amazon MQ devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
MQ.5	Os corretores ActiveMQ devem usar o modo de implantação active/standby	NIST SP 800-53 Rev. 5, padrão gerenciado por serviços: AWS Control Tower	BAIXO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
MQ.6	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	 Não	Acionado por alterações
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	 Não	Acionado por alterações
Neptune.2	Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Neptune.3	Os instantâneos do cluster de banco de dados Neptune não devem ser públicos	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	 Não	Acionado por alterações
Neptune.4	O cluster de banco de dados do Neptune 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	 Não	Acionado por alterações
Neptune.5	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

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Neptune.6	Os instantâneos do cluster 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	Não	Acionado por alterações
Neptune.7	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	Não	Acionado por alterações
Neptune.8	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	Não	Acionado por alterações
Neptune.9	Os clusters de banco de dados Neptune devem ser implantados em várias zonas de disponibilidade	NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
NetworkFirewall1.	Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade	NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
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, NIST SP 800-171 Rev. 2	MÉDIO	Não	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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	Não	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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
NetworkFirewall5.	A ação sem estado padrão para políticas de firewall de rede deve ser descartar ou encaminhar pacotes fragmentados.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações
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. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações
NetworkFirewall7.	Os firewalls do Network Firewall 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

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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	Não	Acionado por alterações
NetworkFirewall.10	Os firewalls do Firewall de Rede devem ter a proteção contra alterações de sub-rede ativada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
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	Não	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	CRÍTICO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Opensearch.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	Não	Acionado por alterações
Opensearch.4	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	Não	Acionado por alterações
Opensearch.5	OpenSearch os domínios devem ter o registro de auditoria ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Opensearch.6	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	Não	Acionado por alterações
Opensearch.7	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)	Não	Acionado por alterações
Opensearch.8	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	Não	Acionado por alterações
Opensearch.9	OpenSearch domínios 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 de programação
Opensearch.10	OpenSearch os domínios devem ter a atualização de software mais recente instalada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAIXO	Não	Acionado por alterações
Opensearch.11	OpenSearch os domínios devem ter pelo menos três nós primários dedicados	NIST SP 800-53 Rev. 5	BAIXO	Não	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	Não	Periódico
PCA.2	AWS As autoridades certificadoras privadas da CA devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
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	CRÍTICO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.2	As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela configuração PubliclyAccessible	CIS AWS Foundations Benchmark v3.0.0, Melhores práticas básicas AWS de segurança, padrão gerenciado por serviços:, NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	 Não	Acionado por alterações
RDS.3	As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.	CIS AWS Foundations Benchmark v3.0.0, 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	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.4	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	Não	Acionado por alterações
RDS.5	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	Não	Acionado por alterações
RDS.6	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.7	O cluster de banco de dados do RDS deve ter a proteção contra exclusão habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	BAIXO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.8	As instâncias de banco de dados do RDS 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	 Não	Acionado por alterações
RDS.9	As instâncias de banco de dados do RDS devem publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações
RDS.10	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	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.11	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.12	A autenticação do IAM deve ser configurada para clusters do RDS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
RDS.13	As atualizações automáticas de versões secundárias do RDS devem estar habilitadas	CIS AWS Foundations Benchmark v3.0.0, Melhores práticas AWS básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	Acionado por alterações
RDS.14	Os clusters Amazon Aurora devem ter o backtracking habilitado	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 de programação
RDS.15	Os clusters de banco de dados do RDS devem ser configurados com várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	 Não	Acionado por alterações
RDS.16	Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	BAIXO	 Não	Acionado por alterações
RDS.17	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	 Não	Acionado por alterações
RDS.18	As instâncias do RDS devem ser implantadas em uma VPC	Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.19	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	Não	Acionado por alterações
RDS.20	As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	Não	Acionado por alterações
RDS.21	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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.22	Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	 Não	Acionado por alterações
RDS.23	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	 Não	Acionado por alterações
RDS.24	Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS.25	As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações
RDS.26	As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup	NIST SP 800-53 Rev. 5	MÉDIO	Sim	Periódico
RDS.27	Os clusters de banco de dados do RDS 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	Não	Acionado por alterações
RDS.28	Os clusters de bancos 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 de programação
RDS.29	Os snapshots de cluster de bancos de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
RDS.30	As instâncias de bancos de dados do RDS devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
RDS.31	Os grupos de segurança de bancos de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
RDS.32	Os snapshots de bancos 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 de bancos 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 de programação
RDS.34	Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
RDS.35	Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
RDS.36	O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	MÉDIO	Sim	Acionado por alterações
RDS.37	Os clusters de banco de dados Aurora PostgreSQL devem publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS. 38	O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
RDS. 39	O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
RDS.40	O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Acionado por alterações
RDS. 41	O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
RDS. 42	O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RDS. 44	O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Periódico
RDS. 45	Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Periódico
Redshift. 1	Os clusters do Amazon Redshift devem proibir o acesso público	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	CRÍTICO	Não	Acionado por alterações
Redshift. 2	As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Redshift.3	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
Redshift.4	Os clusters do Amazon Redshift devem ter o registro de auditoria ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Acionado por alterações
Redshift.6	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	Não	Acionado por alterações
Redshift.7	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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Redshift.8	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	Não	Acionado por alterações
Redshift.9	Os clusters do Redshift não devem usar o nome do banco de dados padrão	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	MÉDIO	Não	Acionado por alterações
Redshift.10	Os clusters do Redshift 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	Não	Acionado por alterações
Redshift.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 de programação
Redshift.12	As notificações de assinatura de eventos do Redshift devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Redshift.13	Os snapshots de clusters do Redshift devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Redshift.14	Os grupos de sub-redes de clusters do Redshift devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Redshift.15	Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster de origens restritas	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Periódico
Desvio para o vermelho.16	Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade	NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
Desvio para o vermelho.17	Os grupos de parâmetros do cluster Redshift devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Desvio para o vermelho.18	Os clusters do Redshift devem ter implantações Multi-AZ habilitadas	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
RedshiftServerless1.	Os grupos de trabalho sem servidor do Amazon Redshift devem usar o roteamento de VPC aprimorado	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Periódico
RedshiftServerless.2	As conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Periódico
RedshiftServerless.3	Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
RedshiftServerless.4	Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MÉDIO	 Sim	Periódico
RedshiftServerless.5.	Os namespaces sem servidor do Redshift não devem usar o nome de usuário de administrador padrão.	AWS Melhores práticas básicas de segurança	MÉDIO	 Sim	Periódico
RedshiftServerless.6	Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
RedshiftServerless.7.	Os namespaces sem servidor do Redshift não devem usar o nome do banco de dados padrão.	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	 Não	Periódico
Route53.1	As verificações de integridade 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 de programação
Route53.2	As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Acionado por alterações
S3.1	Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público habilitadas	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Melhores práticas de segurança AWS básica, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Não	Periódico
S3.2	Os buckets de uso geral do S3 devem bloquear o acesso público para 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	CRÍTICO	Não	Acionado por alterações e periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
S3.3	Os buckets de uso geral do S3 devem bloquear o acesso público para 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	CRÍTICO	 Não	Acionado por alterações e periódico
S3.5	Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Melhores práticas de segurança AWS fundamental, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	HIGH (ALTO)	 Não	Acionado por alterações
S3.7	Os buckets de uso geral do S3 devem usar replicação entre regiões	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	BAIXO	 Não	Acionado por alterações
S3.8	Os buckets de uso geral do S3 devem bloquear o acesso público	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Melhores práticas de segurança AWS básica, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
S3.9	Os buckets de uso geral do S3 devem ter o registro em log de acesso ao servidor habilitado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações
S3.10	Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida	NIST SP 800-53 Rev. 5	MÉDIO	 Não	Acionado por alterações
S3.11	Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MÉDIO	 Sim	Acionado por alterações
S3.12	ACLs não deve ser usado 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	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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 versionamento habilitado	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	BAIXO	 Não	Acionado por alterações
S3.15	Os buckets de uso geral do S3 devem ter o Bloqueio de Objetos habilitado	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	 Sim	Acionado por alterações
S3.17	Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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, PCI DSS v4.0.1	CRÍTICO	Não	Acionado por alterações
S3.20	Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada	Referência do CIS AWS Foundations v3.0.0, Referência do CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5	BAIXO	Não	Acionado por alterações
S3.22	Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto	Referência do CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MÉDIO	Não	Periódico
S3.23	Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto	Referência do CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MÉDIO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
S3.24	Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas	AWS Melhores práticas básicas de segurança, PCI DSS v4.0.1	HIGH (ALTO)	Não	Acionado por alterações
S3.25	Os buckets de diretório do S3 devem ter configurações de ciclo de vida	AWS Melhores práticas básicas de segurança	BAIXO	Sim	Acionado por alterações
SageMaker 1.	As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	Não	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)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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)	 Não	Acionado por alterações
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	 Não	Periódico
SageMaker.5.	SageMaker os modelos devem ter o isolamento de rede ativado	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Acionado por alterações
SageMaker.6	SageMaker as configurações de imagem do aplicativo devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
SageMaker.7.	SageMaker as imagens 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 de programação
SageMaker 8.	SageMaker instâncias de notebook devem ser executadas em plataformas compatíveis	AWS Melhores práticas básicas de segurança	MÉDIO	 Não	Periódico
SecretsManager1.	Os segredos do Secrets Manager devem ter a alternância automática ativada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	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, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
SecretsManager.3	Remover segredos do Secrets Manager não utilizados	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Sim	Periódico
SecretsManager.4	Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	MÉDIO	Sim	Periódico
SecretsManager5.	Os segredos do Secrets Manager devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
ServiceCatalog1.	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)	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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
SNS.1	Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações
SNS.3	Os tópicos do SNS devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
SNS.4	As políticas de acesso a tópicos do SNS não devem permitir o acesso público	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
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	 Não	Acionado por alterações
SQS.2	As filas do SQS devem ser marcadas	AWS Padrão de marcação de recursos	BAIXO	 Sim	Acionado por alterações
SQS.3	As políticas de acesso à fila do SQS não devem permitir acesso público	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	 Não	Acionado por alterações
SSM.1	EC2 as instâncias 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	 Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
SSM.2	EC2 as instâncias gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	HIGH (ALTO)	 Não	Acionado por alterações
SSM.3	EC2 as instâncias gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Padrão gerenciado por serviços: AWS Control Tower	BAIXO	 Não	Acionado por alterações
SSM.4	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	CRÍTICO	 Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
SSM. 5	Os documentos SSM devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
SSM. 6	A automação SSM deve ter o CloudWatch registro ativado	AWS Melhores práticas básicas de segurança v1.0.0	MÉDIO	Não	Periódico
SSM. 7	Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público ativada	AWS Melhores práticas básicas de segurança v1.0.0	CRÍTICO	Não	Periódico
StepFunctions1.	As máquinas de estado do Step Functions devem ter o registro ativado	AWS Melhores práticas básicas de segurança v1.0.0, PCI DSS v4.0.1	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
Transfer. 1	Os fluxos de trabalho do Transfer Family 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 de programação
Transfer.2	Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Periódico
Transferência.3	Os conectores Transfer Family devem ter o registro ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
Transferência.4	Os acordos Transfer Family devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Transferência.5	Os certificados Transfer Family devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Transferência.6	Os conectores Transfer Family devem ser marcados	AWS Padrão de marcação de recursos	BAIXO	Sim	Acionado por alterações
Transferência.7	Os perfis do Transfer Family 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 de programação
WAF.1	AWS O registro do WAF Classic Global Web ACL deve estar ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MÉDIO	Não	Periódico
WAF.2	AWS As regras regionais clássicas do WAF 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	Não	Acionado por alterações
WAF.3	AWS Os grupos de regras regionais clássicos do WAF 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	Não	Acionado por alterações
WAF.4	AWS A web regional clássica do WAF ACLs deve 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	Não	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
WAF.6	AWS As regras globais do WAF Classic devem ter pelo menos uma condição	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
WAF.7	AWS Os grupos de regras globais do WAF Classic devem ter pelo menos uma regra	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	MÉDIO	Não	Acionado por alterações
WAF.8	AWS A web global do WAF Classic ACLs deve 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	Não	Acionado por alterações
WAF.10	AWS A web do WAF ACLs deve 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	Não	Acionado por alterações
WAF.11	AWS O registro de WAF web ACL deve estar ativado	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAIXO	Não	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	Tipo de programação
WAF.12	AWS As regras do WAF devem ter CloudWatch métricas ativadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MÉDIO	Não	Acionado por alterações
WorkSpaces.1.	WorkSpaces os volumes do usuário devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações
WorkSpaces.2	WorkSpaces os volumes raiz devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança	MÉDIO	Não	Acionado por alterações

Registro de alterações dos controles CSPM do Security Hub

O registro de alterações a seguir rastreia alterações materiais nos controles de AWS segurança CSPM existentes do Security Hub, 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 CSPM avalia o status do controle, consulte. Avaliando o status de conformidade e o status de controle As alterações podem levar alguns dias após serem inseridas nesse registro para afetar tudo Regiões da AWS em que o controle está disponível.

Esse log rastreia as mudanças ocorridas desde abril de 2023. Escolha um controle para revisar detalhes adicionais sobre ele. As alterações no título são anotadas na descrição detalhada do controle por 90 dias.

Data da mudança	Título e ID do controle	Descrição de alteração
13 de agosto de 2025	[SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado	O Security Hub CSPM alterou o título e a descrição desse controle. O novo título e a descrição refletem com mais precisão que o controle verifica a configuração do `EnableNetworkIsolation` parâmetro dos modelos hospedados pela Amazon SageMaker AI. Anteriormente, o título desse controle era: SageMaker models should block inbound traffic.
13 de agosto de 2025	[EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização	O Security Hub CSPM alterou o título e a descrição desse controle. O novo título e a descrição refletem com mais precisão o escopo e a natureza da verificação que o controle executa. Anteriormente, o título desse controle era: EFS mount targets should

Data da mudança	Título e ID do controle	Descrição de alteração
		not be associated with a public subnet.
24 de julho de 2025	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	Esse controle verifica se um cluster Amazon EKS é executado em uma versão compatível do Kubernetes. O Security Hub CSPM alterou o valor do parâmetro para esse controle de `1.30` para. `1.31` O suporte padrão para o Kubernetes versão 1.30 no Amazon EKS terminou em 23 de julho de 2025.

Data da mudança	Título e ID do controle	Descrição de alteração
23 de julho de 2025	[EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS	O Security Hub CSPM alterou o título desse controle. O novo título reflete com mais precisão que o controle verifica apenas as solicitações do Amazon EC2 Spot Fleet que especific am parâmetros de lançamento. Anteriormente, o título desse controle era: EC2 Spot Fleet requests should enable encryption for attached EBS volumes.
30 de junho de 2025	1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo	O Security Hub CSPM removeu esse controle do padrão PCI DSS v4.0.1. O PCI DSS v4.0.1 não exige explicitamente o uso de símbolos em senhas.

Data da mudança	Título e ID do controle	Descrição de alteração
30 de junho de 2025	1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos	O Security Hub CSPM removeu esse controle do padrão NIST SP 800-171 Revisão 2. A revisão 2 do NIST SP 800-171 não exige explicitamente períodos de expiração de senha de 90 dias ou menos.
30 de junho de 2025	[RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots	O Security Hub CSPM alterou o título desse controle. O novo título reflete com mais precisão que o controle verifica apenas os clusters de banco de dados Amazon Aurora. Anteriormente, o título desse controle era: RDS DB clusters should be configure d to copy tags to snapshots.

Data da mudança	Título e ID do controle	Descrição de alteração
30 de junho de 2025	[SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis	Esse controle verifica se uma instância do notebook Amazon SageMaker AI está configurada para ser executada em uma plataforma compatível, com base no identificador da plataforma especificado para a instância do notebook. O Security Hub CSPM não oferece mais suporte `notebook-al2-v1` e `notebook-al2-v2` como valores de parâmetros para esse controle. As instâncias de notebook executadas nessas plataformas atingiram o fim do suporte em 30 de junho de 2025.

Data da mudança	Título e ID do controle	Descrição de alteração
30 de maio de 2025	[IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes	O Security Hub CSPM removeu esse controle do padrão PCI DSS v4.0.1. Esse controle verifica se as políticas de senha da conta para usuários do IAM atendem aos requisitos mínimos, incluindo um tamanho mínimo de senha de 7 caracteres. O PCI DSS v4.0.1 agora exige que as senhas tenham no mínimo 8 caracteres. O controle continua sendo aplicado ao padrão PCI DSS v3.2.1, que tem requisitos de senha diferentes. Para avaliar as políticas de senha da conta em relação aos requisitos do PCI DSS v4.0.1, você pode usar o controle IAM.7. Esse controle exige que as senhas tenham no mínimo 8 caracteres. Ele também oferece suporte a valores

Data da mudança	Título e ID do controle	Descrição de alteração
		personalizados para o tamanho da senha e outros parâmetros. O controle IAM.7 faz parte do padrão PCI DSS v4.0.1 no Security Hub CSPM.
8 de maio de 2025	[RDS.46] As instâncias de banco de dados do RDS não devem ser implantadas em sub-redes públicas com rotas para gateways da Internet	O Security Hub CSPM reverteu ao todo o lançamento do controle RDS.46. Regiões da AWS Anteriormente, esse controle era compatível com o padrão AWS Foundational Security Best Practices (FSBP).

Data da mudança	Título e ID do controle	Descrição de alteração
7 de abril de 2025	[ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas	Esse controle verifica se o ouvinte HTTPS para um Application Load Balancer ou o ouvinte TLS para um Network Load Balancer está configurado para criptografar dados em trânsito usando uma política de segurança recomendada. O Security Hub CSPM agora suporta dois valores de parâmetros adicionais para esse controle: e. `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`

Data da mudança	Título e ID do controle	Descrição de alteração
27 de março de 2025	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	Esse controle verifica se as configurações de tempo de execução de uma AWS Lambda função correspondem aos valores esperados para tempos de execução suportados em cada idioma. O Security Hub CSPM agora oferece suporte `ruby3.4` como um valor de parâmetro para esse controle. AWS Lambda adicionou suporte para esse tempo de execução.

Data da mudança	Título e ID do controle	Descrição de alteração
26 de março de 2025	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão compatível do Kubernetes. Para o `oldestVersionSupported` parâmetro, o Security Hub CSPM alterou o valor de `1.29` para. `1.30` A versão mais antiga compatível do Kubernetes agora é. `1.30`

Data da mudança	Título e ID do controle	Descrição de alteração
10 de março de 2025	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	Esse controle verifica se as configurações de tempo de execução de uma AWS Lambda função correspondem aos valores esperados para tempos de execução suportados em cada idioma. O Security Hub CSPM não oferece mais suporte `dotnet6` e `python3.8` como valores de parâmetros para esse controle. AWS Lambda não oferece mais suporte a esses tempos de execução.

Data da mudança	Título e ID do controle	Descrição de alteração
07 de março de 2025	[RDS.18] As instâncias do RDS devem ser implantadas em uma VPC	O Security Hub CSPM removeu esse controle do padrão AWS Foundatio nal Security Best Practices e automatiz ou as verificações dos requisitos do NIST SP 800-53 Rev. 5. Como a rede Amazon EC2 - Classic foi descontin uada, as instâncias do Amazon Relationa l Database Service (Amazon RDS) não podem mais ser implantadas fora de uma VPC. O controle continua fazendo parte do padrão AWS Control Tower ger enciado por serviços.
10 de janeiro de 2025	[Glue.2] Os trabalhos do AWS Glue devem ter o registro ativado	O Security Hub CSPM retirou esse controle e o removeu de todos os padrões.
20 de dezembro de 2024	EC26.1 a 1.69 EC2	O Security Hub CSPM reverteu o lançament o dos controles 6.1 a EC2 .169. EC2

Data da mudança	Título e ID do controle	Descrição de alteração
12 de dezembro de 2024	[RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados	O RDS.23 verifica se um cluster ou instância do Amazon Relational Database Service (Amazon RDS) usa uma porta diferente da porta padrão do mecanismo de banco de dados. Atualizam os o controle para que a AWS Config regra subjacente retorne o resultado `NOT_APPLICABLE` de quatro instâncias do RDS que fazem parte de um cluster.

Data da mudança	Título e ID do controle	Descrição de alteração
2 de dezembro de 2024	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM agora oferece suporte `nodejs22.x` como parâmetro.
26 de novembro de 2024	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão compatível do Kubernetes. A versão mais antiga suportada agora é `1.29`.

Data da mudança	Título e ID do controle	Descrição de alteração
20 de novembro de 2024	[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos	O Config.1 verifica se AWS Config está habilitado, usa a função vinculada ao serviço e registra os recursos dos controles habilitados. O Security Hub CSPM aumentou a severidade desse controle de `MEDIUM` para. `CRITICAL` O Security Hub CSPM também adicionou novos códigos de status e motivos de status para descobertas fracassadas do Config.1. Essas mudanças refletem a importância do Config.1 para a operação dos controles CSPM do Security Hub. Se você tiver AWS Config ou a gravação de recursos desativada, poderá receber descobertas de controle imprecisas. Para receber uma `PASSED` descoberta

Data da mudança	Título e ID do controle	Descrição de alteração
		para o Config.1, ative o registro de recursos para recursos que correspondam aos controles CSPM habilitados do Security Hub e desative os controles que não são necessários em sua organização. Para obter instruções sobre a configuração do AWS Config Security Hub CSPM, consulte. Habilitando e configurando o AWS Config Security Hub CSPM Para obter uma lista dos controles CSPM do Security Hub e seus recursos correspondentes, consulte. AWS Config Recursos necessários para descobertas de controle

Data da mudança	Título e ID do controle	Descrição de alteração
12 de novembro de 2024	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM agora oferece suporte `python3.13` como parâmetro.
11 de outubro de 2024	ElastiCache controles	Títulos de controle alterados para ElastiCache .3, ElastiCache .4, ElastiCache .5 e .7. ElastiCache Os títulos não mencionam mais o Redis OSS porque os controles também se aplicam ao Valkey ElastiCache .

Data da mudança	Título e ID do controle	Descrição de alteração
27 de setembro de 2024	[ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos	Título do controle alterado de O Application Load Balancer deve ser configurado para ignorar cabeçalhos http para O Application Load Balancer deve ser configurado para ignorar cabeçalhos http inválidos.
19 de agosto de 2024	Alterações de título para DMS.12 e controles ElastiCache	Títulos de controle alterados para DMS.12 e .1 a ElastiCache .7. ElastiCache Alteramos esses títulos para refletir uma mudança de nome no serviço Amazon ElastiCache (Redis OSS).

Data da mudança	Título e ID do controle	Descrição de alteração
15 de agosto de 2024	[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos	O Config.1 verifica se AWS Config está habilitado, usa a função vinculada ao serviço e registra os recursos dos controles habilitados. O Security Hub CSPM adicionou um parâmetro de controle personalizado chamado. `includeConfigServiceLinkedRoleCheck` Definindo esse parâmetro como `false`, você pode optar por não verificar se o AWS Config usa o perfil vinculado ao serviço.
31 de julho de 2024	[IoT.1] perfis de AWS IoT Device Defender segurança devem ser marcados	Título do controle alterado de Os perfis de segurança do AWS IoT Core devem ser marcados para Os perfis de segurança do AWS IoT Device Defender devem ser marcados.

Data da mudança	Título e ID do controle	Descrição de alteração
29 de julho de 2024	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM não oferece mais suporte `nodejs16.x` como parâmetro.
29 de julho de 2024	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão compatível do Kubernetes. A versão compatível mais antiga é a `1.28`.

Data da mudança	Título e ID do controle	Descrição de alteração
25 de junho de 2024	[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos	Esse controle verifica se AWS Config está ativado, usa a função vinculada ao serviço e registra os recursos dos controles habilitados. O Security Hub CSPM atualizou o título do controle para refletir o que o controle avalia.
14 de junho de 2024	[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch	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 Security Hub CSPM atualizou o controle para que ele não gere descobertas para clusters de banco de dados Aurora Serverless v1.

Data da mudança	Título e ID do controle	Descrição de alteração
11 de junho de 2024	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão compatível do Kubernetes. A versão compatível mais antiga é a `1.27`.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de junho de 2024	[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos	Esse controle verifica se AWS Config está ativado e se a gravação de AWS Config recursos está ativada. Anteriormente, o controle produzia uma descoberta `PASSED` somente se você configurasse a gravação para todos os recursos. O Security Hub CSPM atualizou o controle para produzir uma `PASSED` descoberta quando a gravação está ativada para os recursos necessários para os controles habilitados. O controle também foi atualizado para verificar se a função AWS Config vinculada ao serviço é usada, o que fornece permissões para registrar os recursos necessários.

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 da autenticação multifator (MFA) habilitada. Anteriormente, o controle produzia uma descoberta `FAILED` para buckets com uma configuração de ciclo de vida. Porém, a exclusão da MFA com versionamento não pode ser habilitada em um bucket com uma configuração de ciclo de vida. O Security Hub CSPM atualizou o controle para não produzir descobertas para buckets que têm uma configuração de ciclo de vida. O título de controle foi atualizado para refletir o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
2 de maio de 2024	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub CSPM 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`.
30 de abril de 2024	[CloudTrail.3] Pelo menos uma CloudTrail trilha deve estar habilitada	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	Título do controle alterado de Os grupos do Auto Scaling associados a um Classic Load Balancer devem usar verificações de integridade de balanceador de carga para Os grupos do Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB. Atualmente, esse controle avalia os balanceadores de carga de aplicações, gateways, redes e os balanceadores de carga 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 CSPM retirou esse controle e o removeu de todos os padrões. Os grupos de trabalho do Athena enviam logs para os buckets do Amazon Simple Storage Service (Amazon S3). O Amazon S3 agora fornece criptografia padrão com chaves gerenciadas do S3 (SS3-S3) em buckets S3 novos e existente s.
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 CSPM retirou esse controle e o removeu de todos os padrões. Os limites de salto de resposta de metadados para instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) 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 CSPM retirou esse controle e o removeu de todos os padrões. Integrar as pilhas do AWS CloudFormation a tópicos do Amazon SNS não é mais uma prática recomenda da de segurança. Embora a integraçã o 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 CSPM retirou 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] Evitar o uso do usuário-raiz	O Security Hub CSPM retirou esse controle e o removeu de todos os padrões. O objetivo desse controle é coberto por outro controle, CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”.
10 de abril de 2024	[SNS.2] O registro em log do status de entrega deve ser habilitado para mensagens de notificação enviadas a um tópico	O Security Hub CSPM retirou esse controle e o removeu de todos os padrões. Registrar em log o status de entrega dos tópicos do SNS não é mais uma prática recomendada de segurança. Embora o registro em log do status de entrega de tópicos importantes do SNS possa ser útil, não é necessário 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 versionamento habilitado devem ter configurações de ciclo de vida	O Security Hub CSPM removeu esse controle do AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower O objetivo desse controle é coberto por outros dois controles, [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida e [S3.14] Os buckets de uso geral do S3 devem ter o versionamento habilitado. 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 habilitadas	O Security Hub CSPM 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 CSPM removeu esse controle do AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower Por padrão, o SNS criptografa tópicos em repouso com criptografia em disco. Para obter mais informações, consulte Criptografia de dados. 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] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada	Título do controle alterado de A proteção contra exclusão do Application Load Balancer deve estar habilitada para Os balanceadores de carga de aplicações, gateways e redes devem ter a proteção contra exclusão habilita. Atualmente, esse controle avalia os balanceadores de carga de aplicações, 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 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 do controle foi atualizado 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	Título do controle alterado de As conexões com os domínios do Elasticsearch devem ser criptografadas usando o TLS 1.2 para As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente. Anteriorm ente, o controle verificava apenas se as conexões com os domínios do Elasticse arch usavam o TLS 1.2. O controle agora produz uma descobert a PASSED se os domínios do Elasticse arch forem criptogra fados usando a política de segurança TLS mais recente. O título do controle foi atualizado 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 habilitadas	Título alterado de A configuração de bloqueio do acesso público do S3 deve estar habilitada para Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público habilitadas. O Security Hub CSPM 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 para leitura	Título alterado de Os buckets do S3 devem proibir o acesso público para leitura para Os buckets de uso geral do S3 devem bloquear o acesso público para leitura. O Security Hub CSPM alterou o título para contabili zar 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 para gravação	Título alterado de Os buckets do S3 devem proibir o acesso público para gravação para Os buckets de uso geral do S3 devem bloquear o acesso público para gravação. O Security Hub CSPM 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 que as solicitações usem SSL	Título alterado de Os buckets do S3 devem exigir que as solicitações usem Secure Socket Layer para Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL. O Security Hub CSPM 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	Título alterado de As permissões do S3 concedidas a outras Contas da AWS nas políticas de bucket devem ser restritas para As políticas de bucket de uso geral do S3 devem restringir o acesso a outras Contas da AWS. O Security Hub CSPM 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	Título alterado de Os buckets do S3 devem ter a replicação entre regiões habilitada para Os buckets de uso geral do S3 devem usar replicação entre regiões. O Security Hub CSPM 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	Título alterado de Os buckets do S3 devem ter a replicação entre regiões habilitad a para Os buckets de uso geral do S3 devem usar replicaçã o entre regiões. O Security Hub CSPM 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	Título alterado de A configuração de bloqueio do acesso público do S3 deve estar habilitada ao nível do bucket para Os buckets de uso geral do S3 devem bloquear o acesso público. O Security Hub CSPM alterou o título para contabili zar 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 em log de acesso ao servidor habilitado	Título alterado de O registro em log de acesso ao servidor de buckets do S3 deve ser habilitado para O registro em log de acesso ao servidor deve ser habilitado para os buckets de uso geral do S3. O Security Hub CSPM 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 versionamento habilitado devem ter configurações de ciclo de vida	O título alterado de Os buckets do S3 com versionamento habilitado devem ter políticas de ciclo de vida configuradas para Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida. O Security Hub CSPM 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 habilitadas	Título alterado de Os buckets do S3 devem ter as notificações de eventos habilitadas para Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas. O Security Hub CSPM alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.12] não ACLs deve ser usado 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 e não ACLs deve ser usado para gerenciar o acesso do usuário aos buckets de uso geral do S3. O Security Hub CSPM 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	Título alterado de Os buckets do S3 devem ter políticas de ciclo de vida configuradas para Os buckets de uso geral do S3 devem ter configurações de ciclo de vida. O Security Hub CSPM 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 versionamento habilitado	Título alterado de Os buckets do S3 deve usar versionamento para Os buckets de uso geral do S3 devem ter o versionamento habilitado. O Security Hub CSPM 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 Bloqueio de Objetos habilitado	Título alterado de Os buckets do S3 devem ser configurados para usar o Bloqueio de Objetos para Os buckets de uso geral do S3 devem ter o Bloqueio de Objetos habilitado. O Security Hub CSPM 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	Título alterado de Os buckets do S3 devem ser criptografados em repouso com AWS KMS keys para Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys. O Security Hub CSPM 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 Lambda devem usar os tempos de execução compatíveis	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 CSPM agora suporta `nodejs20.x` e `ruby3.3` como parâmetros.
22 de fevereiro de 2024	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM agora oferece suporte `dotnet8` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
5 de fevereiro de 2024	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub CSPM 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] O repositório CodeBuild de origem do Bitbucket não URLs deve conter credenciais confidenciais	O título alterado de CodeBuild GitHub ou o repositório de origem do Bitbucket URLs deve ser usado OAuth para o repositório CodeBuild de origem do Bitbucket não URLs deve conter credencia is confidenciais. O Security Hub CSPM removeu a menção OAuth porque outros métodos de conexão também podem ser seguros. O CSPM do Security Hub removeu a menção GitHub porque não é mais possível ter um token de acesso pessoal ou nome de usuário e senha no repositór io de GitHub origem. URLs

Data da mudança	Título e ID do controle	Descrição de alteração
8 de janeiro de 2024	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM não oferece mais suporte `go1.x` e `java8` como parâmetros porque esses são tempos de execução descontinuados.

Data da mudança	Título e ID do controle	Descrição de alteração
29 de dezembro de 2023	[RDS.8] As instâncias de banco de dados do RDS deve ter a proteção contra exclusão habilitada	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 CSPM agora suporta `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 Lambda devem usar os tempos de execução compatíveis	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 CSPM agora suporta `java21` e `python3.12` como parâmetros. O Security Hub CSPM não oferece mais suporte `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 CSPM do Security Hub reduziu a severidade desse controle de CRÍTICO para ALTO porque adicionar o objeto raiz padrão é uma recomendação que depende do aplicativo do usuário e dos requisitos específicos.
5 de dezembro de 2023	[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a 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] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389	Título de controle alterado de Certifiqu e-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 CSPM 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
5 de dezembro de 2023	[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado	Esse controle verifica se os clusters do Amazon EKS têm o registro em log de auditoria habilitado. A AWS Config regra que o Security Hub CSPM usa para avaliar esse controle mudou de `eks-cluster-logging-enabled` para. `eks-cluster-log-enabled`

Data da mudança	Título e ID do controle	Descrição de alteração
17 de novembro de 2023	[EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	EC2.19 verifica se o tráfego de entrada irrestrito de um grupo de segurança está acessível às portas especificadas que são consideradas de alto risco. O Security Hub CSPM atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas são 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] Os CloudWatch 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 log devem ser retidos 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 CSPM atualizou o controle para produzir uma `PASSED` descoberta somente para um domínio do Elasticsearch que está configurado para enviar registros de erros para Logs. CloudWatch O controle também foi atualizado para excluir as versões do Elasticsearch que não oferecem suporte

Data da mudança	Título e ID do controle	Descrição de alteração
		a logs de erros da avaliação.
16 de outubro de 2023	[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22	EC2.13 verifica se os grupos de segurança permitem acesso de entrada irrestrito à porta 22. O Security Hub CSPM atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas são 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] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389	EC2.14 verifica se os grupos de segurança permitem acesso de entrada irrestrito à porta 3389. O Security Hub CSPM atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas são 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	[EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas	EC2.18 verifica se os grupos de segurança que estão em uso permitem tráfego de entrada irrestrito. O Security Hub CSPM atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas são 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 Lambda devem usar os tempos de execução compatíveis	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 CSPM 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 CSPM adicionou o parâmetro `ReplicationType` com um valor de `CROSS-REGION` para garantir que os buckets do 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	[EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub CSPM 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 ativada	O Security Hub CSPM retirou 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	[EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos	O Security Hub CSPM 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 produz uma descoberta aprovada se os grupos de segurança estiverem conectados a EC2 instâncias ou a uma interface de rede elástica. No entanto, para determina dos casos de uso, grupos de segurança independentes não representam um risco de segurança. Você pode usar outros EC2 controles, como EC2 .2, EC2 .13, EC2 .14, EC2 .18 e EC2 .19, para

Data da mudança	Título e ID do controle	Descrição de alteração
		monitorar seus grupos de segurança.
20 de setembro de 2023	[EC2.29] as EC2 instâncias devem ser iniciadas em uma VPC	O Security Hub CSPM retirou esse controle e o removeu de todos os padrões. A Amazon EC2 migrou as instâncias EC2 -Classic 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 CSPM retirou esse controle e o removeu de todos os padrões. O Amazon S3 agora fornece criptografia padrão com chaves gerenciadas do S3 (SS3-S3) em buckets 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] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou 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.9] A MFA 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	[RDS.19] 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	[RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados	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 AWS WAF Classic Regional 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 AWS WAF Classic Regional 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] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras	O título de controle alterado de Uma ACL da web regional do WAF deve ter pelo menos uma regra ou grupo de regras para a web regional AWS WAF clássica ACLs deve ter pelo menos uma regra ou grupo de regras.
14 de setembro de 2023	[WAF.6] As regras AWS WAF Classic Regional 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 AWS WAF Classic global 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] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras	O título de controle alterado de Uma ACL da Web global do WAF deve ter pelo menos uma regra ou grupo de regras para a Web global AWS WAF clássica ACLs deve ter pelo menos uma regra ou grupo de regras.
14 de setembro de 2023	[WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras	O título de controle alterado de Uma ACL WAFv2 da web deve ter pelo menos uma regra ou grupo de regras para a AWS WAF web ACLs deve 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 em log 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 CSPM atualizou esse controle para incluir criptografia de camada dupla no lado do servidor com chaves KMS (DSSE-KMS). O controle produz uma descoberta aprovada quando um bucket do S3 é 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 CSPM atualizou esse controle para incluir criptografia de camada dupla no lado do servidor com chaves KMS (DSSE-KMS). O controle produz uma descoberta aprovada quando um bucket do S3 é criptografado com SSE-KMS ou DSSE-KMS.
9 de junho de 2023	[EKS.2] 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 Lambda devem usar os tempos de execução compatíveis	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 CSPM agora oferece suporte `ruby3.2` como parâmetro.
5 de junho de 2023	[APIGateway.5] 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 CSPM atualizou o controle para avaliar a criptografia de um método específico somente quando o armazenamento em cache está 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 Lambda devem usar os tempos de execução compatíveis	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 CSPM agora oferece suporte `java17` como parâmetro.
18 de maio de 2023	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM não oferece mais suporte `nodejs12.x` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
23 de abril de 2023	[ECS.10] 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. CodeDeplo y O Security Hub CSPM atualizou esse controle para produzir descobert as 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 CSPM atualizou o controle para considerar as condicionais em uma política de bucket.
18 de abril de 2023	[Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis	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 CSPM 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 Lambda devem usar os tempos de execução compatíveis	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 CSPM não oferece mais suporte `dotnetcore3.1` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
17 de abril de 2023	[RDS.11] 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 CSPM 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.

Controles do Security Hub para Contas da AWS

Esses controles do Security Hub avaliam as Contas da AWS.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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: `AWS::::Account`

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 Suporte, 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 Atualizar os contatos alternativos para você Conta da AWS no Guia de referência de gerenciamento de AWS contas.

[A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Severidade: alta

Tipo de recurso: `AWS::::Account`

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. AWS Você pode 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 um membro Conta da AWS para participar da sua organização no Guia do AWS Organizations usuário.

Controles do Security Hub para AWS Amplify

Esses controles do Security Hub avaliam o AWS Amplify serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Amplify.1] Os aplicativos Amplify devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Amplify::App`

Regra do AWS Config : amplify-app-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS Amplify aplicativo tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o aplicativo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o aplicativo não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um AWS Amplify aplicativo, consulte Suporte à marcação de recursos no Guia do usuário do AWS Amplify Hosting.

[Amplify.2] As ramificações do Amplify devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Amplify::Branch`

Regra do AWS Config : amplify-branch-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma AWS Amplify ramificação tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a ramificação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a ramificação não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por

finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a uma AWS Amplify ramificação, consulte Suporte à marcação de recursos no Guia do usuário do AWS Amplify Hosting.

Controles do Security Hub para o Amazon API Gateway

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon API Gateway. Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::ApiGateway::Stage`,`AWS::ApiGatewayV2::Stage`

Regra do AWS Config : api-gw-execution-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 um Amazon API Gateway REST ou WebSocket API têm o registro em log 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 da API de Gateway WebSocket REST ou da API devem ter logs relevantes habilitados. O API Gateway WebSocket REST e o registro de execução da API fornecem registros detalhados das solicitações feitas nos estágios API Gateway WebSocket REST e API. Os estágios incluem respostas de back-end de integração de API, respostas do autorizador Lambda e `requestId` os endpoints de integração de for. AWS

Correção

Para habilitar o registro em log para operações de WebSocket API e REST, consulte Configurar CloudWatch o registro em log usando o console da API Gateway no Guia do desenvolvedor da API Gateway.

[APIGateway.2] 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-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.15 NIST.800-53.r5 SC-8

Categoria: Proteger > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ApiGateway::Stage`

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.

[APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::ApiGateway::Stage`

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 .

[APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso: `AWS::ApiGateway::Stage`

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 (ACL) AWS WAF da web do. Esse controle falhará se uma ACL AWS WAF da web do não estiver conectada a um estágio API REST Gateway.

AWS WAF O é um firewall de aplicativo web que ajuda a proteger aplicativos web APIs contra ataques. Isso permite configurar um ACL, que é conjunto de regras 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 API Gateway esteja associado a uma ACL AWS WAF da web do 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 do AWS WAF Regional a um estágio de API do API do API Gateway existente, consulte Usar AWS WAF para proteger sua APIs no Guia do desenvolvedor do API Gateway.

[APIGateway.5] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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::ApiGateway::Stage`

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 avalia 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 na. 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.

[APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização

Requisitos relacionados: NIST.800-53.r5 CM-2 NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::ApiGatewayV2::Route`

Regra do AWS Config : api-gwv2-authorization-type-configured

Tipo de programação: Periódico

Parâmetros:

Parameter	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, você pode restringir o acesso à sua API somente a usuários ou processos autorizados.

Correção

Para definir um tipo de autorização para HTTP APIs, 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 Controlar e gerenciar o acesso a uma WebSocket API no API Gateway no Guia do desenvolvedor do API Gateway.

[APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::ApiGatewayV2::Stage`

Regra do AWS Config : 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 REST APIs no Guia do desenvolvedor do API Gateway.

Correção

Para habilitar o registro em log, consulte Configurar o registro em log CloudWatch da API usando o console da API Gateway no Guia do desenvolvedor da API Gateway.

Controles do Security Hub para AWS AppConfig

Esses controles do Security Hub avaliam o AWS AppConfig serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[AppConfig.1] os AWS AppConfig aplicativos devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppConfig::Application`

Regra do AWS Config : `appconfig-application-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS AppConfig aplicativo tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o aplicativo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o aplicativo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um AWS AppConfig aplicativo, consulte TagResource, na Referência de APIs do AWS AppConfig .

[AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppConfig::ConfigurationProfile`

Regra do AWS Config : `appconfig-configuration-profile-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um perfil de AWS AppConfig configuração tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o perfil de configuração não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o perfil de configuração não estiver marcado

com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um perfil AWS AppConfig de configuração, consulte TagResource, na Referência de APIs do AWS AppConfig .

[AppConfig.3] AWS AppConfig ambientes devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppConfig::Environment`

Regra do AWS Config : `appconfig-environment-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS AppConfig ambiente tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o ambiente não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o ambiente não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um AWS AppConfig ambiente, consulte TagResource, na Referência de APIs do AWS AppConfig .

[AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppConfig::ExtensionAssociation`

Regra do AWS Config : `appconfig-extension-association-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma associação de AWS AppConfig extensão tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a associação de extensão não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a associação da extensão não estiver

marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma associação AWS AppConfig de extensão, consulte TagResource, na Referência de APIs do AWS AppConfig .

Controles do Security Hub para Amazon AppFlow

Esses controles do Security Hub avaliam o AppFlow serviço e os recursos da Amazon.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppFlow::Flow`

Regra do AWS Config : `appflow-flow-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AppFlow fluxo da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o fluxo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o fluxo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um AppFlow fluxo da Amazon, consulte Criação de fluxos na Amazon AppFlow no Guia AppFlow do usuário da Amazon.

Controles do Security Hub para AWS App Runner

Esses AWS Security Hub controles avaliam o AWS App Runner serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[AppRunner.1] Os serviços do App Runner devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppRunner::Service`

Regra do AWS Config : apprunner-service-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS App Runner serviço tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o serviço App Runner não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o serviço App Runner não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para obter informações sobre como adicionar tags a um AWS App Runner serviço, consulte TagResource, na Referência de APIs do AWS App Runner .

[AppRunner.2] Os conectores VPC do App Runner devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppRunner::VpcConnector`

Regra do AWS Config : apprunner-vpc-connector-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um conector AWS App Runner VPC tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o conector VPC não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro. `requiredKeyTags` Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o conector VPC não estiver marcado com nenhuma

chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para obter informações sobre como adicionar tags a um conector AWS App Runner VPC, consulte TagResource, na Referência de APIs do AWS App Runner .

Controles do Security Hub para AWS AppSync

Esses controles do Security Hub avaliam o AWS AppSync serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regra do AWS Config : appsync-cache-ct-encryption-at-rest

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cache de AWS AppSync API está criptografado em repouso. O controle falhará se o cache de AP não for criptografado em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Você não pode alterar as configurações de criptografia depois de ativar o armazenamento em cache para sua AWS AppSync API. Em vez disso, você deve excluir o cache e recriá-lo com a criptografia habilitada. Para obter mais informações, consulte Cache encryption no AWS AppSync Developer Guide.

[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regra do AWS Config : `appsync-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`fieldLoggingLevel`	Nível de registro em log de campo	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	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 AWS AppSync, consulte Instalação e configuração no Guia do AWS AppSync desenvolvedor.

[AppSync.4] AWS AppSync APIs GraphQL deve ser marcado

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regra AWS Config : `tagged-appsync-graphqlapi` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 do 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 verificará apenas a existência de uma chave de tag e falhará se a API do GraphQL não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 API AWS AppSync GraphQL, consulte TagResource, na Referência de APIs do AWS AppSync .

[AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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: `AWS::AppSync::GraphQLApi`

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.

[AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::AppSync::ApiCache`

Regra do AWS Config : appsync-cache-ct-encryption-in-transit

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cache de AWS AppSync API está criptografado em trânsito. O controle falhará se o cache de AP não for criptografado em trânsito.

Dados em trânsito se referem a dados que se movem de um local para outro, como entre os nós do cluster ou entre o cluster e a aplicação. Os dados podem se mover pela Internet ou em uma rede privada. Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede.

Correção

Você não pode alterar as configurações de criptografia depois de ativar o armazenamento em cache para sua AWS AppSync API. Em vez disso, você deve excluir o cache e recriá-lo com a criptografia habilitada. Para obter mais informações, consulte Cache encryption no AWS AppSync Developer Guide.

Controles do Security Hub para Amazon Athena

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Athena. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Athena.1] Os grupos de trabalho do Athena devem ser criptografados em repouso

> **Important**
>
> O Security Hub descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Severidade: média

Tipo de recurso: `AWS::Athena::WorkGroup`

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 falha se um grupo de trabalho do Athena não estiver criptografado em repouso.

No Athena, você pode 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Athena::DataCatalog`

Regra AWS Config : `tagged-athena-datacatalog` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o catálogo de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags

às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcar recursos do Athena com tags no Guia do usuário do Amazon Athena.

[Athena.3] Os grupos de trabalho do Athena devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Athena::WorkGroup`

Regra AWS Config : `tagged-athena-workgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	`No default value`

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

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 verificará apenas a existência de uma chave de tag e falhará se o grupo de trabalho não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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.

[Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Athena::WorkGroup`

Regra do AWS Config : athena-workgroup-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de trabalho do Amazon Athena tem o registro ativado. O controle falhará se o grupo de trabalho não tiver o registro ativado.

Os logs de auditoria rastreiam e monitoram as atividades do sistema. Eles fornecem um registro de eventos que pode ajudar você a detectar as violações de segurança, investigar os incidentes e cumprir os regulamentos. Os logs de auditoria também aprimoram a responsabilização e a transparência da organização em geral.

Correção

Para obter informações sobre como habilitar o registro em um grupo de trabalho do Athena, consulte Habilitar métricas de CloudWatch consulta no Athena no Guia do usuário do Amazon Athena.

Controles do Security Hub para AWS Backup

Esses controles do Security Hub avaliam o AWS Backup serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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: `AWS::Backup::RecoveryPoint`

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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Backup::RecoveryPoint`

Regra AWS Config: `tagged-backup-recoverypoint` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o ponto de recuperação não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 adicionar pares de valor-chave.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.3] os AWS Backup cofres devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Backup::BackupVault`

Regra AWS Config: `tagged-backup-backupvault` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

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 verificará apenas a existência de uma chave de tag e falhará se o ponto de recuperação não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Tags de cofre de backup, escolha Gerenciar tags.
5. Insira a chave e o valor da tag. Escolha Adicionar nova tag para adicionar pares de valor-chave.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.4] os planos de AWS Backup relatórios devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Backup::ReportPlan`

Regra AWS Config: `tagged-backup-reportplan` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 relatórios 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 plano de relatórios não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Tags de cofre de backup, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.5] os planos de AWS Backup backup devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Backup::BackupPlan`

Regra AWS Config: `tagged-backup-backupplan` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

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 verificará apenas a existência de uma chave de tag e falhará se o plano de backup não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como

uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Tags de cofre de backup, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

Controles do Security Hub para AWS Batch

Esses controles do Security Hub avaliam o AWS Batch serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Batch.1] As filas de trabalhos em lote devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Batch::JobQueue`

Regra do AWS Config : batch-job-queue-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma fila de AWS Batch trabalhos tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a fila de trabalhos não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a fila de trabalhos não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma fila de trabalhos do Batch, consulte Marcar seus recursos no Guia do AWS Batch usuário.

[Batch.2] As políticas de agendamento em lote devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Batch::SchedulingPolicy`

Regra do AWS Config : batch-scheduling-policy-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma política AWS Batch de agendamento tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a política de agendamento não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a política de agendamento não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma política de agendamento de Batch, consulte Marcar seus recursos no Guia do AWS Batch usuário.

[Batch.3] Ambientes de computação em lote devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Batch::ComputeEnvironment`

Regra do AWS Config : batch-compute-environment-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um ambiente AWS Batch computacional tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o ambiente computacional não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o ambiente de computação não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um ambiente de computação Batch, consulte Marcar seus recursos no Guia do AWS Batch usuário.

[Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Batch::ComputeEnvironment`

Regra do AWS Config : batch-managed-compute-env-compute-resources-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se a propriedade de recursos computacionais em um ambiente de AWS Batch computação gerenciado tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a propriedade compute resources não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se uma propriedade de recursos computacionais não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo. Esse controle não avalia ambientes computacionais não gerenciados nem ambientes gerenciados que usam AWS Fargate recursos.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags aos recursos computacionais em um ambiente AWS Batch computacional gerenciado, consulte Marcar seus recursos no Guia do AWS Batch usuário.

Controles do Security Hub para o AWS Certificate Manager

Esses AWS Security Hub controles avaliam o serviço e os recursos do AWS Certificate Manager (ACM). Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

Requisitos relacionados: NIST.800-53.r5 SC-2 8 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ACM::Certificate`

Regra do AWS Config : acm-certificate-expiration-check

Tipo de agendamento: acionado por alterações e periódico

Parâmetros:

Parameter	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 ACM renova automaticamente os certificados que usam validação do 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 e-mail quando a expiração da validade estiver se aproximando. Esses serviços são fornecidos para certificados públicos e privados do ACM.

Para domínios validados por e-mail

Quando um certificado está a 45 dias da expiração, o ACM envia ao proprietário do domínio um e-mail para cada nome de domínio. Para validar os domínios e concluir a renovação, você deve responder às notificações por e-mail.

Para obter mais informações, consulte Renovação de domínios validados por e-mail no Guia do usuário do AWS Certificate Manager .

Para domínios validados por 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 Renovação de domínios validados pelo DNS no Guia do usuário do AWS Certificate Manager .

[ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

Requisitos relacionados: PCI DSS v4.0.1/4.2.1

Categoria: Identificar > Inventário > Serviços de inventário

Severidade: alta

Tipo de recurso: `AWS::ACM::Certificate`

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 da 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 para o ACM, consulte Pré-requisitos para importação de certificados no Guia do usuário do AWS Certificate Manager .

[ACM.3] Os certificados do ACM devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ACM::Certificate`

Regra AWS Config : `tagged-acm-certificate` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um certificado do 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 verificará apenas a existência de uma chave de tag e falhará se o certificado não estiver marcado com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS,

incluindo o 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.

Controles do Security Hub para AWS CloudFormation

Esses controles do Security Hub avaliam o AWS CloudFormation serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM 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: `AWS::CloudFormation::Stack`

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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CloudFormation::Stack`

Regra AWS Config : `tagged-cloudformation-stack` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se a pilha não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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.

Controles do Security Hub para Amazon CloudFront

Esses AWS Security Hub controles avaliam o CloudFront serviço e os recursos da Amazon. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0.1/2.2.6

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::CloudFront::Distribution`

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-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso: `AWS::CloudFront::Distribution`

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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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. Esse controle avalia apenas se o registro padrão (legado) está habilitado para uma distribuição.

CloudFront os registros de acesso fornecem informações detalhadas sobre cada solicitação do usuário que CloudFront recebe. Cada registro em 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 mais informações sobre a análise de registros de acesso, consulte Consultar CloudFront registros da Amazon no Guia do usuário do Amazon Athena.

Correção

Para configurar o registro padrão (legado) para uma CloudFront distribuição, consulte Configurar o registro padrão (legado) no Amazon CloudFront Developer Guide.

[CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0.1/6.4.2

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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 ao AWS WAF Classic ou à AWS WAF web ACLs. 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 os aplicativos da web e APIs 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-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.15 NIST.800-53.r5 SC-8

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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 SSL/TLS certificado padrão CloudFront fornecido. Esse controle passa se a CloudFront distribuição usar um SSL/TLS certificado personalizado. Esse controle falhará se a CloudFront distribuição usar o SSL/TLS certificado padrão.

Os personalizados SSL/TLS permitem que seus usuários acessem o conteúdo usando nomes de domínio alternativos. Você pode 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 SSL/TLS certificado 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 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso: `AWS::CloudFront::Distribution`

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 SSL/TLS certificado personalizado e estão configuradas para usar o SNI para atender solicitações HTTPS. Esse controle falhará se um SSL/TLS certificado personalizado estiver associado, mas o método de SSL/TLS suporte 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 do seu nome de domínio é determinado durante a negociação do SSL/TLS handshake; 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. Para obter informações sobre certificados SSL personalizados, consulte Requisitos para usar SSL/TLS certificados com CloudFront.

[CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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 Exigindo 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-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, (4),, NIST.800-53.r5 SC-1 (1), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 (NIST.800-53.r5

SC-12) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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 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), PCI DSS v4.0.1/2.2.6

Categoria: Identificar > Configuração de recursos

Severidade: alta

Tipo de recurso: `AWS::CloudFront::Distribution`

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 > Recursos não acessíveis ao público

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

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 HTTP/HTTPS solicitações que usam o método POST Regiões da AWS que exigem o AWS Signature Version 4 (SigV4). 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CloudFront::Distribution`

AWS Config regra: `tagged-cloudfront-distribution` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se a distribuição não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 CloudFront distribuição, consulte Como marcar CloudFront distribuições da Amazon no Amazon CloudFront Developer Guide.

[CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::CloudFront::Distribution`

Regra do AWS Config : cloudfront-ssl-policy-check

Tipo de programação: acionado por alterações

Parâmetros:`securityPolicies`: `TLSv1.2_2021` (não personalizável)

Esse controle verifica se uma CloudFront distribuição da Amazon está configurada para usar a política de segurança TLS recomendada. O controle falhará se a CloudFront distribuição não estiver configurada para usar a política de segurança TLS recomendada.

Se você configurar uma CloudFront distribuição da Amazon para exigir que os espectadores usem HTTPS para acessar o conteúdo, você precisará escolher uma política de segurança e especificar a versão mínima do SSL/TLS protocolo a ser usada. Isso determina qual versão do protocolo CloudFront usa para se comunicar com os espectadores e as cifras CloudFront usadas para criptografar as comunicações. Recomendamos usar a política de segurança mais recente que CloudFront fornece. Isso garante o CloudFront uso dos pacotes de criptografia mais recentes para criptografar dados em trânsito entre um visualizador e uma distribuição. CloudFront

> **Note**
>
> Esse controle gera descobertas somente para CloudFront distribuições que estão configuradas para usar certificados SSL personalizados e não estão configuradas para oferecer suporte a clientes legados.

Correção

Para obter informações sobre como configurar a política de segurança para uma CloudFront distribuição, consulte Atualizar uma distribuição no Amazon CloudFront Developer Guide. Ao configurar a política de segurança de uma distribuição, escolha a política de segurança mais recente.

Controles do Security Hub para o AWS CloudTrail

Esses AWS Security Hub controles do avaliam o AWS CloudTrail serviço e os recursos da. Os controles da podem não estar disponíveis em todos os Regiões da AWS. Para obter 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 AWS Foundations Benchmark v1.4.0/3.1, CIS Foundations Benchmark v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), (26), (9),

(9), (22) AWS NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 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 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

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso: `AWS::::Account`

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 do que capture eventos de gerenciamento de leitura e gravação. O controle falhará se CloudTrail estiver desabilitado ou se não houver pelo menos uma CloudTrail trilha que capture eventos de gerenciamento de leitura e gravação.

AWS CloudTrail registra chamadas à AWS API da da da sua conta e fornece os arquivos de log. 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 pelas AWS Management Console ferramentas de linha de comando do. AWS SDKs O histórico também inclui chamadas de API de serviços de nível superior dos Serviços da AWS , como. AWS CloudFormation

O histórico de chamadas de AWS API da gerado pelo CloudTrail possibilita a realização de análises de segurança, rastreamento de alteração 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 de várias regiões, os eventos de gerenciamento para todas as operações de leitura e gravação garantem que as operações de gerenciamento de CloudTrail registros em todos os recursos de 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	Habilitada
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 habilitada

Requisitos relacionados: CIS AWS 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 CM-3(6), NIST.800-53.r5 SC-1 3, 8, 8 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 SI-7 (6),

NIST.800-171.r2 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 3.3.8, AWS PCI DSS v3.2.1/3.4 DSS v4.0.1/10.3.2 NIST.800-53.r5 SC-7

Categoria: Proteger > Proteção de dados > Criptografia do data-at-rest

Severidade: média

Tipo de recurso: `AWS::CloudTrail::Trail`

Regra do AWS Config : cloud-trail-encryption-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o CloudTrail está configurado para usar a criptografia do lado do servidor (SSE) do. AWS KMS key O controle falha se `KmsKeyId` não estiver definido.

Para obter uma camada adicional de segurança para arquivos de CloudTrail log confidenciais, é necessário usar a criptografia do lado do servidor com AWS KMS keys (SSE-KMS) para os arquivos de CloudTrail log para criptografia em repouso. Por padrão, os arquivos de log entregues CloudTrail aos seus buckets são criptografados criptografia 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 estar habilitada

Requisitos relacionados: NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.3, 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 3.2.1/10.3.6, PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso: `AWS:::Account`

Regra do AWS Config : cloudtrail-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma AWS CloudTrail trilha do está habilitada na sua Conta da AWS. O controle falhará se sua conta não tiver pelo menos uma CloudTrail trilha habilitada.

Entretanto, alguns AWS serviços da não habilitam o registro de todos APIs os eventos. Você deve implementar quaisquer trilhas de auditoria adicionais que não CloudTrail sejam e revisar a documentação de cada serviço em Integrações e serviços CloudTrail compatíveis.

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 habilitada

Requisitos relacionados: CIS AWS 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), NIST.800-53.r5 SI-7 (3) 3.r5 SI-7 (7), NIST.800-171.r2 3.3.8, AWS PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, PCI DSS v4.0.1/10.3.2

Categoria: Proteção de dados > Integridade dos dados

Severidade: baixa

Tipo de recurso: `AWS::CloudTrail::Trail`

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 do arquivo de log do está habilitada na CloudTrail trilha.

CloudTrail A validação do arquivo de log cria um arquivo de resumo com assinatura digital que contém um hash de cada log que CloudTrail grava para o Amazon S3. Você pode usar esses

arquivos de resumo para determinar se um arquivo de log foi modificado, excluído ou inalterado depois que o log foi CloudTrail entregue.

O Security Hub recomenda que você ative a validação de arquivos em todas as trilhas. Arquivo validação do arquivo de log fornece verificação de integridade adicional de CloudTrail logs.

Correção

Para habilitar a validação do arquivo de CloudTrail log, consulte Habilitar a validação da integridade do arquivo CloudTrail de log para o Guia AWS CloudTrail do usuário.

[CloudTrail.5] CloudTrail trilhas devem ser integradas ao 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, (26), (9),, (9),, (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-2 (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 AC-4 (20), NIST.800-53.r5 AC-6 Nist.800-53.R5 SI-4 NIST.800-53.r5 SC-7 (5), Nist.800-53.R5 SI-7 (8) AWS 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

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso: `AWS::CloudTrail::Trail`

Regra do AWS Config : cloud-trail-cloud-watch-logs-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se as CloudTrail trilhas do estão configuradas para enviar registros ao CloudWatch Logs. O controle falhará se a propriedade `CloudWatchLogsLogGroupArn` da trilha estiver vazia.

CloudTrail registra chamadas de AWS API da que são feitas em uma determinada conta. As informações gravadas incluem o seguinte:

- Identidade do chamador da API
- Hora da chamada da API

- O endereço IP de origem do chamador da API
- Parâmetros de solicitação
- 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 do S3 especificado para análise de longo prazo. Para realizar análise em tempo real, você pode configurar CloudTrail o envio de CloudWatch logs ao Logs.

Para uma trilha que está ativada em todas as regiões em uma conta, CloudTrail envia arquivos de log de todas as regiões a um grupo de CloudWatch logs 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 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 logs ao Logs facilita o registro de atividades do histórico e em tempo real com base no usuário, API, recurso e endereço IP. Você pode usar essa abordagem para 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] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.3, CIS AWS Foundations Benchmark v1.4.0/3.3, PCI DSS v1.4.0/3.3, PCI DSS v4.0./3.3, PCI DSS v4.0/3.3, PCI DSS v4.0/3.3, PC AWS

Categoria: Identificar > Registro em log

Severidade: crítica

Tipo de recurso: `AWS::S3::Bucket`

AWS Config Regra: (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 na sua conta. Esses arquivos de log são armazenados em um bucket do S3. O CIS recomenda que a política do bucket do S3 ou a lista de controle de acesso (ACL) aplicada ao bucket do S3 desses CloudTrail logs impeça o acesso público aos logs. CloudTrail Permitir o acesso público ao conteúdo do CloudTrail log pode ajudar um adversário a identificar vulnerabilidades no uso ou na configuração da conta afetada.

Para executar essa verificação, o Security Hub primeiro usa lógica personalizada para procurar o bucket em que seus CloudTrail logs estão armazenados. Em seguida, ele usa as regras AWS Config gerenciadas para verificar se o bucket está acessível publicamente.

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 acessível ao público, a verificação gerará uma descoberta com falha.

Correção

Para bloqueio de acesso público para seu bucket CloudTrail S3, consulte Configurar bloqueio do acesso público aos seus buckets S3 no Guia do usuário do Amazon Simple Storage Service. Selecione todas as quatro configurações de bloqueio de acesso público do Amazon S3.

[CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.6, CIS Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4, PCI DSS v4.0.1/10.2.1 AWS

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso: `AWS::S3::Bucket`

AWS Config Regra: (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

O registro de acesso ao bucket do S3 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 ative 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 logs estão armazenados e usa a regra AWS Config gerenciada pelo para verificar se o registro em log está habilitado.

Se CloudTrail entregar arquivos de log de várias Contas da AWS em um único bucket do Amazon S3 de destino, o Security Hub avaliará 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.

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.

[CloudTrail.9] CloudTrail trilhas devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CloudTrail::Trail`

Regra AWS Config : `tagged-cloudtrail-trail` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma AWS CloudTrail trilha do 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 verificará apenas a existência de uma chave de tag e falhará se a trilha não estiver marcada com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, incluindo o 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.

[CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys

Requisitos relacionados: 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-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia do data-at-rest

Severidade: média

Tipo de recurso: `AWS::CloudTrail::EventDataStore`

Regra do AWS Config : event-data-store-cmk-encryption-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`kmsKeyArns`	Uma lista de nomes de recursos da Amazon (ARNs) AWS KMS keys a serem incluídos na avaliação. O controle gera uma `FAILED` descoberta se um armazenamento de dados	StringList (máximo de 3 itens)	1—3 ARNs das chaves KMS existentes. Por exemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-`	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de eventos não estiver criptografado com uma chave KMS na lista.		`123456789 0ab` .	

Esse controle verifica se um armazenamento de dados de eventos do AWS CloudTrail Lake é criptografado em repouso com um gerenciamento gerenciado pelo cliente AWS KMS key. O controle falhará se o armazenamento de dados do evento não for criptografado com uma chave KMS gerenciada pelo cliente. Opcionalmente, você pode especificar uma lista de chaves KMS para o controle incluir na avaliação.

Por padrão, o AWS CloudTrail Lake criptografa armazenamentos de dados de eventos com chaves gerenciadas pelo Amazon S3 (SSE-S3) usando um algoritmo AES-256. Para controle adicional, você pode configurar o CloudTrail Lake para criptografar um armazenamento de dados de eventos com um cliente gerenciado AWS KMS key (SSE-KMS) em vez disso. Uma chave do KMS gerenciada pelo cliente é uma AWS KMS key que você cria, detém e gerencia na sua Conta da AWS. Você tem controle total sobre esse tipo de chave KMS. Isso inclui definir e manter a política de chaves, gerenciar concessões, alternar material criptográfico, atribuir tags, criar aliases e ativar e desativar a chave. Você pode usar uma chave KMS gerenciada pelo cliente em operações criptográficas para seu uso de CloudTrail dados e auditoria com CloudTrail registros.

Correção

Para obter informações sobre como criptografar um armazenamento de dados de eventos do AWS CloudTrail Lake com um AWS KMS key que você especifica, consulte Atualizar um armazenamento de dados de eventos no Guia do AWS CloudTrail usuário. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

Controles do Security Hub para o Amazon CloudWatch

Esses AWS Security Hub controles do avaliam o CloudWatch serviço e os recursos da Amazon. Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS Foundations Benchmark v1.4.0/1.7, CIS Foundations Benchmark v1.4.0/3.3, NIST.800-Foundations Benchmark v1.4.0/3.3, CIS AWS Foundations Benchmark v1.4.0/3.3, CIS Foundations Benchmark v1.4.0/3.3, CIS Foundations Benchmark v1.4.0/3.3, CIS Foundations Benchmark v1.4.0/3.3, CIS AWS Foundations Benchmark v1.4.0/3.3, CIS Foundations Benchmark v1.4.0/3.3, CIS Foundations B AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

O usuário raiz tem acesso irrestrito a todos os serviços e recursos da Conta da AWS. É altamente recomendável que você evite usar o usuário raiz para tarefas diárias. Minimizar o uso do usuário raiz 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 as políticas do AWS Identity and Access Management (IAM) diretamente a grupos e perfis, 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs 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 Criar 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
que…	**`1`**

[CloudWatch.2] Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda que você crie um filtro de métrica e um alarme para fazer 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.1 no CIS AWS 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs 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	`{($.errorCode="*Unauthorized0peration") \|\| ($.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 Criar 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
que…	**`1`**

[CloudWatch.3] Certifique-se de que um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.2

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs 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") }`

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 Criar 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
que…	**`1`**

[CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.4, CIS Foundations Benchmark v1.4.0/4.4, NIST.800-171.r2 3.14.6, NIST.800-171.r2 AWS 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se você monitora as chamadas de API em tempo real, direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda que você crie um filtro de métrica e um alarme para fazer alterações em políticas do IAM. Monitorar essas alterações ajuda a garantir que os controles de autenticação e autorização permaneçam intactos.

> **Note**
>
> Quando o Security Hub executa 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:
>
> - Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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`

Campo	Valor
	`) || ($.eventName=PutRolePolicy) \|\| ($.eventName=PutUserPolicy) || ($.eventName=CreatePolicy) \|\| ($.eventName=DeletePolicy) || ($.eventName=CreatePolicyVersion) \|\| ($.eventName=DeletePolicyVersion) || ($.eventName=AttachRolePolicy) \|\| ($.eventName=DetachRolePolicy) || ($.eventName=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPolicy) \|\| ($.eventName=DetachGroupPolicy))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criar 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
que…	**`1`**

[CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/3.3, NIST.800-171.r2 3.8, NIST.800-171.r2 AWS 3.14, NIST.800-171.r2 3.14

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda que você crie um filtro de métrica e um alarme para fazer alterações em opções de configuração do CloudTrail. Monitorar essas alterações ajuda a garantir visibilidade sustentada para atividades na conta.

Para executar essa verificação, o usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criar 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
que…	**`1`**

[CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6, NIST.800-171.r2 3.14.6, NIST.800-171.r2 AWS 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:
>
> - Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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")}`

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 Criar 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
que…	**`1`**

[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.7, CIS Foundations Benchmark v1.4.0/4.7, NIST.800-171.r2 3.13 10, AWS NIST.800-171.r2 3.3.16, NIST.800-171.r2 3.14

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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. O controle também falhará se `ExcludeManagementEventSources` contiver `kms.amazonaws.com`.

> **Note**
>
> Quando o Security Hub executa 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:
>
> - Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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 Criar 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
que…	**1**

[CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8, NIST.800-171.r2 3.14.6, NIST.800-171.r2 AWS 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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 Criar 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
que…	**1**

[CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9, NIST.800-171.r2 3.8, NIST.800-171.r2 3.4.8, AWS NIST.800-171.r2 3.14

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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 Criar 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
que…	**1**

[CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.10, CIS Foundations Benchmark v1.4.0/4.10, NIST.800-171.r2 3.14.6, NIST.800-171.r2 AWS 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes. Os grupos de segurança são um filtro de pacote com estado que controla o tráfego de entrada e saída em uma VPC.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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 Criar 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

Campo	Valor
Sempre que *your-metric-name* for...	Maior/Igual
que…	**1**

[CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em 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, NIST.800-171.r2 3.14.6, NIST.800-171.r2 AWS 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes. NACLs são usados como um filtro de pacotes sem estado para controlar o tráfego de entrada e saída de sub-redes em uma VPC.

O CIS recomenda que você crie um filtro de métrica e um alarme para fazer alterações em NACLs. O monitoramento dessas mudanças ajuda a garantir que AWS os recursos e serviços não sejam expostos acidentalmente.

Para executar essa verificação, o usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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 Criar 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

Campo	Valor
Sempre que *your-metric-name* for...	Maior/Igual
que…	**1**

[CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.12, CIS Foundations Benchmark v1.4.0/4.12, NIST.800-171.r2 3.3.1, AWS NIST.800-171.r2 3.1

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes. Os gateways de rede são necessários para enviar e receber tráfego para um destino fora de uma VPC.

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criar 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

Campo	Valor
que…	**1**

[CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.13, CIS Foundations Benchmark v1.4.0/4.13, NIST.800-171.r2 3.3.1, NIST.800-171.r2 AWS 3.1.r2 3.1.r2 3.13.1, NIST.800-171.r2 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se você monitora as chamadas de API em tempo real, direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes. As tabelas de rotas encaminham o tráfego de rede entre sub-redes e gateways de rede.

O CIS recomenda 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criar 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

Campo	Valor
Sempre que *your-metric-name* for...	Maior/Igual
que…	**1**

[CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.14, CIS Foundations Benchmark v1.4.0/4.14, NIST.800-171.r2 3.3.1, NIST.800-171.r2 AWS 3.1.r2 3.1.r2 3.13.1, NIST.800-171.r2 3.14.7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regra: (regra personalizada do Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode fazer o monitoramento de chamadas de API em tempo real direcionando CloudTrail os CloudWatch logs para Logs e estabelecendo alarmes e filtros de métrica de métrica de métrica correspondentes. Você pode 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 elas. VPCs

O CIS recomenda 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 usa lógica personalizada para realizar as etapas de auditoria exatas prescritas para o controle 3.14 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 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:

- Um trilha multirregional é baseada 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 de 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. Você pode 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. Crie um tópico do Amazon SNS. Para instruções, 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 todas as Regiões da AWS. Para instruções, consulte Criação de uma trilha no Guia do usuário do AWS CloudTrail .

   Anote o nome do grupo de CloudWatch logs de logs 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) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.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 Criar 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
que…	**1**

[CloudWatch.15] Os CloudWatch alarmes devem ter ações especificadas configuradas

Requisitos relacionados: NIST.800-53.r5 IR-4 (1) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (5), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 (5) 2 3.4, NIST.800-171.r2 3.14

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::CloudWatch::Alarm`

AWS Config regra: **`cloudwatch-alarm-action-check`**

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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	Booleano	Não personalizável	`true`

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	uma ação quando o estado do alarme mudar para `ALARM`.			
`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 de CloudWatch métrica. Os alarmes de métrica podem fazer parte de alarmes compostos que têm as ações especificadas configuradas. O controle gera descobertas `FAILED` nos seguintes casos:
>
> - As ações especificadas não estão configuradas para um alarme de métrica.
> - O alarme de métrica faz parte de um alarme composto que têm as ações especificadas configuradas.

Esse controle se concentra em saber se um CloudWatch alarme tem alguma ação de alarme configurada, o CloudWatch.17 se concentra no status de ativação de uma ação de CloudWatch alarme.

Recomendamos usar 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 log devem ser retidos 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::Logs::LogGroup`

AWS Config regra: **`cw-loggroup-retention-period-check`**

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`minRetentionTime`	Período mínimo de retenção em dias para	Enum	`365`, `400`, `545`,	`365`	

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
	grupos de CloudWatch logs		`731, 1827, 3653`		

Esse controle verifica se um grupo de CloudWatch logs 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 logs centralizam os logs de todos os sistemas, aplicações 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 em suas instâncias do Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, no Amazon Route 53 ou em outras origens. 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] as ações CloudWatch de alarme devem ser ativadas

Categoria: Detectar > Serviços de detecção

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4 (12)

Severidade: alta

Tipo de recurso: `AWS::CloudWatch::Alarm`

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`deve ser definido como verdadeiro). 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 de CloudWatch métrica. Os alarmes de métrica podem fazer parte de alarmes compostos que têm ações de alarme ativadas. O controle gera descobertas `FAILED` nos seguintes casos:
>
> - As ações especificadas não estão configuradas para um alarme de métrica.
> - O alarme de métrica 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, o CloudWatch3.14 se concentra em saber se alguma `ALARM` ação está configurada em um CloudWatch alarme.

As ações de alarme alertam 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, em Alarmes, escolha 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.

Controles do Security Hub para CodeArtifact

Esses controles do Security Hub avaliam o AWS CodeArtifact serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[CodeArtifact.1] CodeArtifact repositórios devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CodeArtifact::Repository`

Regra AWS Config : `tagged-codeartifact-repository` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o repositório não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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.

Controles do Security Hub para CodeBuild

Esses controles do Security Hub avaliam o AWS CodeBuild serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve conter credenciais confidenciais

Requisitos relacionados: PCI DSS v3.2.1/8.2.1 NIST.800-53.r5 SA-3, PCI DSS v4.0.1/8.3.2

Categoria: Proteger > Desenvolvimento seguro

Severidade: crítica

Tipo de recurso: `AWS::CodeBuild::Project`

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 repositórios Bitbucket de fontes 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 fonte de projetos, consulte Multiple input sources and output artifacts sample no AWS CodeBuild User Guide.

As credenciais de login nunca devem ser armazenadas ou transmitidas em texto puro ou aparecer no 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 pessoais ou credenciais de login poderia resultar em exposição não intencional de dados ou acesso não autorizado.

Correção

Você pode atualizar seu CodeBuild projeto para usar 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 Conectar usando OAuth e, em seguida, escolha Conectar a 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: NIST.800-53.r5 IA-5 (7), PCI DSS v3.2.1/8.2.1 NIST.800-53.r5 SA-3, PCI DSS v4.0.1/8.3.2

Categoria: Proteger > Desenvolvimento seguro

Severidade: crítica

Tipo de recurso: `AWS::CodeBuild::Project`

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-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 (6), PCI DSS v4.0.1/10.3.2

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: baixa

Tipo de recurso: `AWS::CodeBuild::Project`

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: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::CodeBuild::Project`

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 o S3 ou para CloudWatch os 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 descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM do Security Hub.

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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-5, 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: alta

Tipo de recurso: `AWS::CodeBuild::Project`

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. Este parâmetro só deve ser definido como true 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 ao Docker APIs e 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.

[CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::CodeBuild::ReportGroup`

Regra do AWS Config : `codebuild-report-group-encrypted-at-rest`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os resultados do teste de um grupo de AWS CodeBuild relatórios que são exportados para um bucket do Amazon Simple Storage Service (Amazon S3) estão criptografados em repouso. O controle falhará se o grupo de relatórios não for criptografado em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para criptografar a exportação do grupo de relatórios para o S3, consulte Update a report group no AWS CodeBuild User Guide.

Controles do Security Hub para Amazon CodeGuru Profiler

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon CodeGuru Profiler.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CodeGuruProfiler::ProfilingGroup`

Regra do AWS Config : `codeguruprofiler-profiling-group-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um grupo de CodeGuru criação de perfil do Amazon Profiler tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o grupo

de criação de perfil não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de criação de perfil não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um grupo de criação de CodeGuru perfil do Profiler, consulte Como marcar grupos de criação de perfil no Guia do usuário do Amazon CodeGuru Profiler.

Controles do Security Hub para Amazon CodeGuru Reviewer

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon CodeGuru Reviewer.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CodeGuruReviewer::RepositoryAssociation`

Regra do AWS Config : `codegurureviewer-repository-association-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma associação de repositório do Amazon CodeGuru Reviewer tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se a associação do repositório não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a associação do repositório não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como

uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma associação de repositório de CodeGuru revisores, consulte Como marcar uma associação de repositório no Guia do usuário do Amazon CodeGuru Reviewer.

Controles do Security Hub para o Amazon Cognito

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Cognito. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::Cognito::UserPool`

Regra do AWS Config : cognito-user-pool-advanced-security-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`SecurityMode`	O modo de fiscalização da proteção contra ameaças que o controle verifica.	String	`AUDIT`, `ENFORCED`	`ENFORCED`

Esse controle verifica se um grupo de usuários do Amazon Cognito tem a proteção contra ameaças ativada com o modo de fiscalização definido como funcional completo para autenticação padrão. O controle falhará se o grupo de usuários tiver a proteção contra ameaças desativada ou se o modo de fiscalização não estiver configurado para funcionar totalmente para a autenticação padrão. A menos que você forneça valores de parâmetros personalizados, o Security Hub usa o valor padrão do `ENFORCED` modo de imposição definido como função completa para autenticação padrão.

Depois de criar um grupo de usuários do Amazon Cognito, você pode ativar a proteção contra ameaças e personalizar as ações que são tomadas em resposta a diferentes riscos. Ou você pode usar o modo de auditoria para coletar métricas sobre os riscos detectados sem aplicar nenhuma mitigação de segurança. No modo de auditoria, a proteção contra ameaças publica métricas na Amazon CloudWatch. Você pode ver as métricas depois que o Amazon Cognito gera seu primeiro evento.

Correção

Para obter informações sobre a ativação da proteção contra ameaças para um grupo de usuários do Amazon Cognito, consulte Segurança avançada com proteção contra ameaças no Guia do desenvolvedor do Amazon Cognito.

[Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso: `AWS::Cognito::IdentityPool`

Regra do AWS Config : cognito-identity-pool-unauth-access-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um pool de identidades do Amazon Cognito está configurado para permitir identidades não autenticadas. O controle falhará se o acesso de convidado for ativado (o `AllowUnauthenticatedIdentities` parâmetro está definido como`true`) para o grupo de identidades.

Se um grupo de identidades do Amazon Cognito permitir identidades não autenticadas, o grupo de identidades fornecerá AWS credenciais temporárias aos usuários que não se autenticaram por meio de um provedor de identidade (convidados). Isso cria riscos de segurança porque permite acesso anônimo aos AWS recursos. Se você desativar o acesso de convidado, poderá ajudar a garantir que somente usuários devidamente autenticados possam acessar seus AWS recursos, o que reduz o risco de acesso não autorizado e possíveis violações de segurança. Como prática recomendada, um grupo de identidades deve exigir autenticação por meio de provedores de identidade compatíveis. Se o acesso não autenticado for necessário, é importante restringir cuidadosamente as permissões para identidades não autenticadas e revisar e monitorar seu uso regularmente.

Correção

Para obter informações sobre como desativar o acesso de convidados a um grupo de identidades do Amazon Cognito, consulte Ativar ou desativar o acesso de convidados no Guia do Desenvolvedor do Amazon Cognito.

Controles do Security Hub para AWS Config

Esses controles do Security Hub avaliam o AWS Config serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

Requisitos relacionados: CIS AWS 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

AWS CM-6 (1), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (2), PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5

Categoria: Identificar > Inventário

Severidade: crítica

Tipo de recurso: `AWS::::Account`

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`includeConfigServiceLinkedRoleCheck`	O controle não avalia se AWS Config usa a função vinculada ao serviço se o parâmetro estiver definido como. `false`	Booleano	`true` ou `false`	`true`

Esse controle verifica se AWS Config está ativado em sua conta na atual Região da AWS, registra todos os recursos que correspondem aos controles ativados na região atual e usa a função vinculada ao serviço AWS Config. O nome da função vinculada ao serviço é. AWSServiceRoleForConfig Se você não usar a função vinculada ao serviço e não definir o `includeConfigServiceLinkedRoleCheck` parâmetro como`false`, o controle falhará porque outras funções podem não ter as permissões necessárias AWS Config para registrar seus recursos com precisão.

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 nos recursos. Recursos globais são recursos disponíveis em qualquer região.

O controle é avaliado da seguinte maneira:

- Se a região atual for definida como sua região de agregação, o controle produzirá PASSED descobertas somente se os recursos globais AWS Identity and Access Management (IAM) forem registrados (se você tiver ativado controles que os exijam).
- Se a região atual for definida como uma região vinculada, o controle não avaliará se os recursos globais do IAM são registrados.
- Se a região atual não estiver no agregador ou se a agregação entre regiões não estiver configurada em sua conta, o controle produzirá descobertas PASSED somente se os recursos globais do IAM estiverem registrados (se você tiver ativado controles que os exijam).

Os resultados do controle não são afetados se você escolher o registro diário ou o registro contínuo das alterações no estado dos recursos do AWS Config. Porém, os resultados desse controle poderão mudar quando novos controles forem liberados se você tiver configurado a habilitação automática de novos controles ou tiver uma política de configuração central que habilite automaticamente novos controles. Nesses casos, se você não registrar todos os recursos, deverá configurar a gravação dos recursos associados a novos controles para receber uma descoberta PASSED.

As verificações de segurança do Security Hub funcionam conforme o esperado somente se você habilitar AWS Config em todas as regiões e configurar a gravação de recursos para controles que a exijam.

> **Note**
>
> O Config.1 exige que AWS Config esteja habilitado em todas as regiões nas quais você usa o Security Hub.
> Como o Security Hub é um serviço regional, a verificação realizada nesse controle avalia somente a região atual da conta.
> Para permitir verificações de segurança em recursos globais do IAM em uma região, você deve registrar os recursos globais do IAM nessa região. As regiões que não têm os recursos globais do IAM registrados receberão uma descoberta PASSED padrão para controles que verificam os recursos globais do IAM. Como os recursos globais do IAM são idênticos Regiões da AWS, recomendamos que você registre os recursos globais do IAM somente na região de origem (se a agregação entre regiões estiver ativada em sua conta). Os recursos do IAM serão registrados somente na região em que a gravação global de recursos estiver ativada.
> Os tipos de recursos registrados globalmente pelo IAM que são AWS Config compatíveis são usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM. Você pode considerar a desativação dos controles do Security Hub que verificam esses tipos de recursos em

regiões onde a gravação global de recursos está desativada. Para obter mais informações, consulte Controles sugeridos para desativar no Security Hub CSPM.

Correção

Na região de origem e nas regiões que não fazem parte de um agregador, registre todos os recursos necessários para os controles habilitados na região atual, incluindo os recursos globais do IAM, se você tiver controles habilitados que exijam esses recursos.

Nas regiões vinculadas, você pode usar qualquer modo de AWS Config gravação, desde que esteja gravando todos os recursos que correspondem aos controles ativados na região atual. Nas regiões vinculadas, se você tiver ativado controles que exigem o registro dos recursos globais do IAM, você não receberá uma `FAILED` descoberta (seu registro de outros recursos é suficiente).

O `StatusReasons` campo no `Compliance` objeto de sua descoberta pode ajudá-lo a determinar por que você teve uma descoberta malsucedida para esse controle. Para obter mais informações, consulte Detalhes de conformidade para resultados de controle.

Para obter uma lista dos recursos que devem ser registrados para cada controle, consulte AWS Config Recursos necessários para descobertas de controle. Para obter informações gerais sobre como habilitar AWS Config e configurar a gravação de recursos, consulteHabilitando e configurando o AWS Config Security Hub CSPM.

Controles do Security Hub para o Amazon Connect

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Connect.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::CustomerProfiles::ObjectType`

Regra do AWS Config : `customerprofiles-object-type-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um tipo de objeto Amazon Connect Customer Profiles tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o tipo de objeto não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o tipo de objeto não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da

AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um tipo de objeto Customer Profiles, consulte Adicionar tags aos recursos no Amazon Connect no Guia do administrador do Amazon Connect.

[Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Connect::Instance`

Regra do AWS Config : connect-instance-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância do Amazon Connect está configurada para gerar e armazenar registros de fluxo em um grupo de CloudWatch registros da Amazon. O controle falhará se a instância do Amazon Connect não estiver configurada para gerar e armazenar registros de fluxo em um grupo de CloudWatch registros.

Os registros de fluxo do Amazon Connect fornecem detalhes em tempo real sobre eventos nos fluxos do Amazon Connect. Um fluxo define a experiência do cliente com uma central de atendimento do Amazon Connect do início ao fim. Por padrão, quando você cria uma nova instância do Amazon Connect, um grupo de CloudWatch registros da Amazon é criado automaticamente para armazenar os registros de fluxo da instância. Os registros de fluxo podem ajudar você a analisar fluxos, encontrar erros e monitorar métricas operacionais. Você também pode configurar alertas para eventos específicos que podem ocorrer em um fluxo.

Correção

Para obter informações sobre como habilitar registros de fluxo para uma instância do Amazon Connect, consulte Habilitar registros de fluxo do Amazon Connect em um grupo de CloudWatch registros do Amazon Connect no Guia do administrador do Amazon Connect.

Controles do Security Hub para o Amazon Data Firehose

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Data Firehose.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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-1 2, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::KinesisFirehose::DeliveryStream`

Regra do AWS Config : `kinesis-firehose-delivery-stream-encrypted`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um fluxo de entrega do Amazon Data Firehose é criptografado em repouso com criptografia no servidor. Esse controle falhará se um fluxo de entrega do Firehose não for criptografado em repouso com criptografia no 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 fluxo do Data Firehose e são descriptografados depois de recuperados do armazenamento. Isso permite que você cumpra os requisitos regulatórios e aumente a segurança dos dados.

Correção

Para habilitar a criptografia no servidor dos fluxos de entrega do Firehose, consulte Proteção de dados no Amazon Data Firehose no Guia do usuário do Amazon Data Firehose.

Controles do Security Hub para AWS DataSync

Esses controles do Security Hub avaliam o AWS DataSync serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[DataSync.1] DataSync as tarefas devem ter o registro ativado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::DataSync::Task`

Regra do AWS Config : datasync-task-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma AWS DataSync tarefa tem o registro ativado. O controle falhará se a tarefa não tiver o registro em log habilitado.

Os logs de auditoria rastreiam e monitoram as atividades do sistema. Eles fornecem um registro de eventos que pode ajudar você a detectar as violações de segurança, investigar os incidentes e cumprir os regulamentos. Os logs de auditoria também aprimoram a responsabilização e a transparência da organização em geral.

Correção

Para obter informações sobre como configurar o registro em log para AWS DataSync tarefas, consulte Monitoramento de transferências de dados com o Amazon CloudWatch Logs no Guia do AWS DataSync usuário.

[DataSync.2] DataSync as tarefas devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DataSync::Task`

Regra do AWS Config : datasync-task-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma AWS DataSync tarefa tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a tarefa não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a tarefa não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a uma AWS DataSync tarefa, consulte Como marcar suas AWS DataSync tarefas no Guia do AWS DataSync usuário.

Controles do Security Hub para Amazon Detective

Esse AWS Security Hub controle avalia o serviço e os recursos do Amazon Detective. O controle pode não estar disponível em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Detective.1] Os gráficos de comportamento do Detective devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Detective::Graph`

Regra AWS Config : `tagged-detective-graph` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o gráfico de comportamento não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 do Detective, consulte Adding tags to a behavior graph no Amazon Detective Administration Guide.

Controles do Security Hub para AWS DMS

Esses controles do Security Hub avaliam o serviço AWS Database Migration Service (AWS DMS) e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21),,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.2 3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::DMS::ReplicationInstance`

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. 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 do DMS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DMS::Certificate`

Regra AWS Config : `tagged-dms-certificate` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o certificado não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política

de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 certificado do DMS, consulte Tagging resources in AWS Database Migration Service no AWS Database Migration Service User Guide.

[DMS.3] As assinaturas de eventos do DMS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DMS::EventSubscription`

Regra AWS Config : `tagged-dms-eventsubscription` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	`No default value`

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

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 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 verificará apenas a existência de uma chave de tag e falhará se a assinatura de eventos não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 eventos do DMS, consulte Tagging resources in AWS Database Migration Service no AWS Database Migration Service User Guide.

[DMS.4] As instâncias de replicação do DMS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DMS::ReplicationInstance`

Regra AWS Config : `tagged-dms-replicationinstance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se a instância de replicação não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 replicação do DMS, consulte Tagging resources in AWS Database Migration Service no AWS Database Migration Service User Guide.

[DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DMS::ReplicationSubnetGroup`

Regra AWS Config : `tagged-dms-replicationsubnetgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas 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 de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 replicação do DMS, consulte Tagging resources in AWS Database Migration Service no AWS Database Migration Service User Guide.

[DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

Requisitos relacionados: 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), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::DMS::ReplicationInstance`

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 falha se a atualização automática de versões secundárias não estiver habilitada para uma instância de replicação do DMS.

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 .

[DMS.7] 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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::DMS::ReplicationTask`

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, você pode especificar quais atividades de componente serão registradas e qual quantidade de informações será gravada no log. Você deve especificar o registro das seguintes tarefas:

- `TARGET_APPLY`: as afirmações 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 Suporte. 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.

[DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: AWS::DMS::ReplicationTask

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, você pode especificar quais atividades de

componente serão registradas e qual quantidade de informações será gravada no log. Você deve especificar o registro das seguintes tarefas:

- `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 Suporte. 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.

[DMS.9] Os endpoints do DMS devem usar SSL

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::DMS::Endpoint`

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 conexões entre as instâncias de replicação DMS e seu banco de dados. O uso de um certificado fornece uma camada extra de segurança, validando se a conexão está sendo feita com o banco de dados esperado. Para isso, ele verifica o certificado de servidor que é instalado automaticamente em todas as instâncias 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-1 7 NIST.800-53.r5 AC-6, NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0.1/7.3.1

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso: `AWS::DMS::Endpoint`

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. AWS Com o IAM, você pode especificar quem pode acessar quais serviços e recursos e em quais condições. Com as políticas do IAM, você gerencia as permissões da força de trabalho e dos sistemas para garantir permissões com privilégio mínimo. 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 Using Amazon Neptune as a target for AWS Database Migration Service no AWS Database Migration Service User Guide.

[DMS.11] Os endpoints do DMS para o 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, PCI DSS v4.0.1/7.3.1

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso: `AWS::DMS::Endpoint`

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 do 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 usá-las 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 em endpoints do DMS para MongoDB, consulte Using MongoDB as a source for AWS DMS no AWS Database Migration Service User Guide.

[DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 3, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::DMS::Endpoint`

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 OSS está configurado com uma conexão TLS. O controle falhará se o endpoint não tiver o TLS habilitado.

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 o endpoint do 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 do DMS para o Redis, consulte Using Redis as a target for AWS Database Migration Service no AWS Database Migration Service User Guide.

Controles do Security Hub para o Amazon DocumentDB

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon DocumentDB (com compatibilidade com o MongoDB). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[DocumentDB.1] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::RDS::DBCluster`

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 falha se um cluster do Amazon DocumentDB 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. 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

Você pode ativar a criptografia em repouso ao criar um cluster Amazon DocumentDB. Não é possível alterar as configurações de criptografia após a criação de um cluster. Para obter mais informações, consulte Habilitar criptografia em repouso para um cluster do Amazon DocumentDB no Guia do desenvolvedor do Amazon DocumentDB.

[DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

Requisitos relacionados: NIST.800-53.r5 SI-12, PCI DSS v4.0.1/3.2.1

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : docdb-cluster-backup-retention-check

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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.

[DocumentDB.3] Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

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, a menos que haja razão para tanto. 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, você pode usar a operação Amazon DocumentDB `modify-db-snapshot-attribute`. Defina `attribute-name` como `restore` e `values-to-remove` como `all`.

[DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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.

O Amazon DocumentDB (compatível com MongoDB) permite 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.

[DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 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: média

Tipo de recurso: `AWS::RDS::DBCluster`

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 no console do Amazon DocumentDB.

Correção

Para habilitar a proteção contra exclusão para um cluster 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.

[DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : docdb-cluster-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros:`excludeTlsParameters`:`disabled`, `enabled` (não personalizável)

Isso controla se um cluster Amazon DocumentDB requer TLS para conexões com o cluster. O controle falhará se o grupo de parâmetros do cluster associado ao cluster não estiver sincronizado ou se o parâmetro do cluster TLS estiver definido como `disabled` ou`enabled`.

Você pode usar o TLS para criptografar a conexão entre um aplicativo e um cluster do Amazon DocumentDB. O uso do TLS pode ajudar a proteger os dados de serem interceptados enquanto os dados estão em trânsito entre um aplicativo e um cluster do Amazon DocumentDB. A criptografia em trânsito para um cluster Amazon DocumentDB é gerenciada usando o parâmetro TLS no grupo de parâmetros do cluster associado ao cluster. Ao habilitar a criptografia em trânsito, as conexões seguras usando o TLS são obrigatórias para se conectar ao cluster. Recomendamos usar os seguintes parâmetros TLS: `tls1.2+tls1.3+`, e. `fips-140-3`

Correção

Para obter informações sobre como alterar as configurações de TLS para um cluster do Amazon DocumentDB, consulte Criptografar dados em trânsito no Guia do desenvolvedor do Amazon DocumentDB.

Controles do Security Hub para o DynamoDB

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon DynamoDB. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[DynamoDB.1] As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::DynamoDB::Table`

Regra do AWS Config : `dynamodb-autoscaling-enabled`

Tipo de programação: Periódico

Parâmetros:

Parameter	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 que usam o modo de capacidade sob demanda são limitadas apenas pelas cotas de tabelas padrão de throughput do DynamoDB. Para aumentar essas cotas, você pode registrar um ticket de suporte com Suporte. As tabelas do DynamoDB que usam o modo provisionado com ajuste de escala automático ajustam dinamicamente a capacidade de throughput 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 o ajuste automático do DynamoDB nas tabelas existentes no modo de capacidade, consulte Habilitar 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 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::DynamoDB::Table`

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.

[DynamoDB.3] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::DAX::Cluster`

Regra do AWS Config : `dax-encryption-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DynamoDB Accelerator (DAX) é criptografado em repouso. O controle falhará se um cluster do DAX não for criptografado em repouso.

Criptografar dados em repouso reduz o risco de os dados armazenados em disco serem acessados por um usuário não autenticado. AWS A criptografia 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 de 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.

[DynamoDB.4] As tabelas do DynamoDB devem estar presentes em um plano de backup

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::DynamoDB::Table`

AWS Config regra: **`dynamodb-resources-protected-by-backup-plan`**

Tipo de programação: Periódico

Parâmetros:

Parameter	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

[DynamoB.5] As tabelas do DynamoDB devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::DynamoDB::Table`

Regra AWS Config : `tagged-dynamodb-table` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma tabela de rotas 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 verificará apenas a existência de uma chave de tag e falhará se a tabela não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcar recursos no DynamoDB no Guia do desenvolvedor do Amazon DynamoDB.

[DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 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: média

Tipo de recurso: `AWS::DynamoDB::Table`

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 acelerador do DynamoDB devem ser criptografados em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-1 7, 3, NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 3 NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::DAX::Cluster`

Regra do AWS Config : `dax-tls-endpoint-encryption`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DynamoDB Accelerator (DAX) é criptografado em trânsito, com o tipo de criptografia de endpoint definido como TLS. O controle falhará se um cluster do DAX não for 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 deve permitir que somente conexões criptografadas por TLS acessem clusters do DAX. Porém, a criptografia de dados em trânsito pode afetar a performance. Você deve testar a aplicação com a criptografia ativada para entender o perfil de performance e o impacto do TLS.

Correção

Você não pode alterar as configurações de criptografia TLS depois de criar um cluster do DAX. Para criptografar um cluster do DAX existente, crie um novo cluster com a criptografia em trânsito habilitada, desvie o tráfego da aplicação para ele e exclua o cluster antigo. Para obter mais informações, consulte Usar a proteção contra exclusão no Guia do desenvolvedor do Amazon DynamoDB.

Controles do Security Hub para Amazon EC2

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Elastic Compute Cloud (Amazon EC2). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[EC2.1] Os snapshots 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 v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7), (21),,, (11), (16), (20) NIST.800-53.r5 AC-3, (21), (3) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (4), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS:::::Account`

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.

Correção

Para tornar um snapshot público do EBS privado, consulte Compartilhar um snapshot no Guia do usuário da Amazon EC2 . Em Ações, modificar permissões, escolha Privado.

[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou 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,, (21), (11), (16 AWS), (21), (4), (5)) AWS NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

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 não use o grupo 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 tráfego não intencional se o grupo de segurança padrão for configurado acidentalmente para recursos como EC2 instâncias.

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 EC2 instâncias. Para obter instruções, consulte Alterar o grupo de segurança de uma instância no Guia EC2 do usuário da Amazon.

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 Configurar regras de grupo de segurança no Manual do usuário da 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::EC2::Volume`

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 a criptografia do Amazon EBS no Guia EC2 do usuário da Amazon.

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 Amazon EBS e escolher uma chave simétrica gerenciada pelo cliente.

Para obter mais informações, consulte Criação de um volume do Amazon EBS e Cópia de um snapshot do Amazon EBS no Guia do usuário da Amazon EC2 .

[EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso: `AWS::EC2::Instance`

Regra do AWS Config : `ec2-stopped-instance`

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`AllowedDays`	Número de dias em que a EC2 instância pode ficar em um estado interrompido antes de gerar uma descoberta com falha.	Inteiro	1 para 365	30

Esse controle verifica se uma EC2 instância da Amazon foi interrompida por mais tempo do que o número permitido de dias. O controle falhará se uma EC2 instância 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 EC2 instância 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 EC2 instância ao longo do tempo em um estado inativo, inicie-a periodicamente para manutenção e depois a interrompa após a manutenção. Idealmente, esse deve ser um processo automatizado.

Correção

Para encerrar uma EC2 instância inativa, consulte Encerrar uma instância no Guia do usuário da Amazon EC2 .

[EC2.6] O registro de fluxo de VPC deve ser ativado em todos 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, NIST.800-53.r5 AC-4 (26),

NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20 AWS , NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4 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, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`

Regra do AWS Config : `vpc-flow-logs-enabled`

Tipo de programação: Periódico

Parâmetros:

- `trafficType`: `REJECT` (não personalizável)

Esse controle verifica se os registros de fluxo da Amazon VPC foram encontrados e habilitados para. VPCs O tipo de tráfego está definido como `Reject`. O controle falhará se os registros de fluxo de VPC não estiverem habilitados VPCs em sua conta.

> **Note**
>
> Esse controle não verifica se os logs de fluxo da Amazon VPC estão habilitados por meio do Amazon Security Lake para a Conta da AWS.

Com o recurso VPC Flow Logs, você pode 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.

O Security Hub recomenda que você habilite o registro de fluxo para rejeições de pacotes 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 da Amazon VPC, escolha Seu. VPCs Em Filtrar, escolha Rejeitar ou Todos.

[EC2.7] A criptografia padrão do EBS deve estar ativada

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS AWS Foundations Benchmark v3.0.0/2.2.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 SI-7 (6) NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS:::::Account`

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 volumes do Amazon Elastic Block Store (Amazon EBS). O controle falhará se a criptografia no nível da conta não estiver habilitada para volumes do EBS.

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 Criptografia por padrão no Guia EC2 do usuário da Amazon.

Correção

Para configurar a criptografia padrão para volumes do Amazon EBS, consulte Criptografia por padrão no Guia do EC2 usuário da Amazon.

[EC2.8] as EC2 instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/5.6,, NIST.800-53.r5 AC-3 (15), (7) NIST.800-53.r5 AC-3, PCI DSS NIST.800-53.r5 AC-3 v4.0.1/2.2.6 NIST.800-53.r5 AC-6

Categoria: Proteger > Segurança de rede

Severidade: alta

Tipo de recurso: `AWS::EC2::Instance`

Regra do AWS Config : `ec2-imdsv2-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a versão de metadados da EC2 instância está configurada com o Instance Metadata Service Version 2 ()IMDSv2. O controle passa se `HttpTokens` estiver definido como necessário para IMDSv2. O controle falha se `HttpTokens` estiver definido como `optional`.

Você usa os metadados da instância 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 EC2 instância. 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 EC2 instâncias com IMDSv2.

Correção

Para configurar EC2 instâncias com IMDSv2, consulte Caminho recomendado para a solicitação IMDSv2 no Guia EC2 do usuário da Amazon.

[EC2.9] EC2 As instâncias da Amazon não devem ter um endereço público IPv4

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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: alta

Tipo de recurso: `AWS::EC2::Instance`

Regra do AWS Config : `ec2-instance-no-public-ip`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se EC2 as instâncias têm um endereço IP público. O controle falhará se o `publicIp` campo estiver presente no item de configuração da EC2 instância. Esse controle se aplica somente aos IPv4 endereços.

Um IPv4 endereço público é um endereço IP que pode ser acessado pela Internet. Se você iniciar sua instância com um endereço IP público, ela EC2 poderá ser acessada pela Internet. Um IPv4 endereço privado é um endereço IP que não pode ser acessado pela Internet. Você pode usar IPv4 endereços privados para comunicação entre EC2 instâncias na mesma VPC ou na sua rede privada conectada.

IPv6 os endereços são globalmente exclusivos e, portanto, podem ser acessados pela Internet. No entanto, por padrão, todas as sub-redes têm o atributo de IPv6 endereçamento definido como false. Para obter mais informações sobre isso IPv6, consulte o endereçamento IP em sua VPC no Guia do usuário da Amazon VPC.

Se você tiver um caso de uso legítimo para manter EC2 instâncias com endereços IP públicos, poderá suprimir as descobertas desse controle. Para obter mais informações sobre as opções de arquitetura front-end, consulte o blog de AWS arquitetura ou a série de AWS vídeos da série This Is My Architecture.

Correção

Use uma VPC não padrão para que um endereço IP público não seja atribuído à instância por padrão.

Quando você executa uma EC2 instância em uma VPC padrão, ela recebe um endereço IP público. Quando você executa uma EC2 instância 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 novas EC2 instâncias na sub-rede recebem um endereço IP público do pool de IPv4 endereços públicos.

Você pode desassociar um endereço IP público atribuído automaticamente da sua instância. EC2 Para obter mais informações, consulte IPv4 Endereços públicos e nomes de host DNS externos no Guia EC2 do usuário da Amazon.

[EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, (21) NIST.800-53.r5 AC-4,,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6, (16) NIST.800-53.r5 SC-7, 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 NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1

Categoria: Proteger > Configuração de rede segura > Acesso privado a API

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`

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 a Amazon foi EC2 criado para cada VPC. O controle falhará se uma VPC não tiver um VPC endpoint criado para o serviço da 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 VPCs que `FAILED` as descobertas são compartilhadas entre contas. O Security Hub recomenda que você suprima essas descobertas `FAILED`.

Para melhorar a postura de segurança da sua VPC, você pode configurar a EC2 Amazon para usar uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLink, uma

tecnologia que permite que você acesse as operações de EC2 API da Amazon de forma privada. Ele restringe todo o tráfego de rede entre sua VPC e a EC2 Amazon à rede 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 Amazon EC2 API para outras regiões.

Para saber mais sobre a criação de VPC endpoints para a Amazon, EC2 consulte Amazon e faça a EC2 interface de VPC endpoints no Guia do usuário da Amazon. EC2

Correção

Para criar um endpoint de interface para a Amazon a EC2 partir do console Amazon VPC, consulte Criar um endpoint de VPC no Guia.AWS PrivateLink Em Nome do serviço, escolha com.amazonaws. ***region***.ec2.

Você também pode criar e anexar uma política de endpoint ao seu VPC endpoint para controlar o acesso à API da Amazon. EC2 Para obter instruções sobre como criar uma política de VPC endpoint, consulte Criar uma política de endpoint no Guia do usuário da Amazon. EC2

[EC2.12] A Amazon não utilizada EC2 EIPs deve ser removida

Requisitos relacionados: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CM-8(1)

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso: `AWS::EC2::EIP`

Regra do AWS Config : `eip-attached`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os endereços IP elásticos (EIP) alocados a uma VPC estão conectados a EC2 instâncias ou interfaces de rede elástica em uso (). ENIs

Uma falha na descoberta indica que você pode não ter usado EC2 EIPs.

Isso ajudará você a manter um inventário preciso de ativos EIPs em seu ambiente de dados de titulares de cartões (CDE).

Correção

Para liberar um EIP não utilizado, consulte Liberar um endereço IP elástico no Guia EC2 do usuário da Amazon.

[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/4.1,, (21), (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.13.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.1 2.2.2, PCI DSS v4.0.1/1.3.1 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regra do AWS Config : `restricted-ssh`

Tipo de agendamento: acionado por alterações e periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de EC2 segurança da Amazon permite a entrada de 0.0.0.0/0 ou: :/0 para a 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 EC2 do usuário da Amazon. Depois de selecionar um grupo de segurança no EC2 console da Amazon, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22.

[EC2.14] 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, PCI DSS v4.0.1/1.3.1

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

AWS Config regra: **`restricted-common-ports`**(a regra criada é`restricted-rdp`)

Tipo de agendamento: acionado por alterações e periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de EC2 segurança da Amazon permite a entrada de 0.0.0.0/0 ou: :/0 para a 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 3389, 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 3389.

[EC2.15] As EC2 sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso: `AWS::EC2::Subnet`

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 público IPs nas `MapPublicIpOnLaunch` sub-redes da Amazon Virtual Private Cloud (Amazon VPC) foi definida 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 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 IPv4 endereçamento público para sua sub-rede no Guia do usuário da Amazon VPC. Desmarque a caixa de seleção Ativar atribuição automática de IPv4 endereço público.

[EC2.16] As listas de controle de acesso à rede não utilizadas devem ser removidas

Requisitos relacionados: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0.1/1.2.7

Categoria: Proteger > Segurança de rede

Severidade: baixa

Tipo de recurso: `AWS::EC2::NetworkAcl`

Regra do AWS Config : `vpc-network-acl-unused-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se há alguma lista de controle de acesso à rede (rede ACLs) não utilizada na sua nuvem privada virtual (VPC). O controle falhará se a ACL da rede não estiver associada a uma sub-rede. O controle não gerará descobertas para uma ACL de rede padrão não utilizada.

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.

[EC2.17] EC2 As instâncias da Amazon não devem usar várias ENIs

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoria: Proteger > Segurança de rede

Severidade: baixa

Tipo de recurso: `AWS::EC2::Instance`

Regra do AWS Config : `ec2-instance-multiple-eni-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma EC2 instância usa várias Elastic Network Interfaces (ENIs) 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 permitidos ENIs. Esse controle também falhará se uma EC2 instância pertencente a um cluster Amazon EKS usar mais de uma ENI. Se suas EC2 instâncias precisarem ter várias ENIs como parte de um cluster Amazon EKS, você poderá suprimir essas descobertas de controle.

Várias 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 EC2 instância, consulte Separar uma interface de rede de uma instância no Guia do EC2 usuário da Amazon.

[EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 NIST.800-53.r5 SC-7 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regra do AWS Config : `vpc-sg-open-only-to-authorized-ports`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`authorizedTcpPorts`	Lista de portas TCP autorizadas	IntegerList (mínimo de 1 item e máximo de 32 itens)	1 para `65535`	`[80,443]`
`authorizedUdpPorts`	Lista de portas UDP autorizadas	IntegerList (mínimo de 1 item e máximo de 32 itens)	1 para `65535`	Nenhum valor padrão

Esse controle verifica se um grupo de EC2 segurança da Amazon permite tráfego de entrada irrestrito de 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.

Os grupos de segurança fornecem filtragem stateful de tráfego de rede de entrada e saída para 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.

[EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (1), NIST.800-53.r5 CA-9 (11), (16) NIST.800-53.r5 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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

Categoria: Proteger > Acesso restrito à rede

Severidade: crítica

Tipo de recurso: `AWS::EC2::SecurityGroup`

AWS Config regra: **`restricted-common-ports`**(a regra criada é`vpc-sg-restricted-common-ports`)

Tipo de agendamento: acionado por alterações e periódico

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 de um grupo EC2 de segurança da Amazon 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)
- 10 (POP3)
- 135 (RPM)
- 143 (IMAPA)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 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 EC2 do usuário da Amazon.

[EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.1.13, NIST.800-171.r2 3.1.20

Categoria: Recuperação > Resiliência > 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 conexão AWS Site-to-Site VPN. 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 AWS Site-to-Site VPN 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 Site-to-Site VPN no Guia do usuário da AWS Site-to-Site VPN.

[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/5.1, AWS CIS Foundations Benchmark v3.0.0/5.1, (21), (1), NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-53.r5 CA-9 NIST.800-171.r2 3.1.20 NIST.800-53.r5 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 NIST.800-171.r2 3.13.1, PCI DSS v4.0.1/1.3.1

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 (Network ACL) permite acesso irrestrito às portas TCP padrão para SSH/RDP tráfego de entrada. O controle falhará se a entrada de ingresso da ACL de rede permitir um bloco CIDR de origem de '0.0.0.0/0' ou '::/0' para as portas TCP 22 ou 3389. O controle não gera descobertas para uma ACL de rede padrão.

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 editar as regras de tráfego da ACL de rede, consulte Trabalhar com rede ACLs no Guia do usuário da Amazon VPC.

[EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso: `AWS::EC2::NetworkInterface`,`AWS::EC2::SecurityGroup`

Regra do AWS Config : `ec2-security-group-attached-to-eni-periodic`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os grupos de segurança estão conectados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma interface de rede elástica. O controle falhará se o grupo de segurança não estiver associado a uma EC2 instância da Amazon ou a uma interface de rede elástica.

> **Important**
>
> Em 20 de setembro de 2023, o Security Hub removeu esse controle dos padrões AWS Foundational Security Best Practices e NIST SP 800-53 Revision 5. Esse controle continua fazendo parte do padrão AWS Control Tower gerenciado por serviços. Esse controle produz uma descoberta aprovada se os grupos de segurança estiverem conectados a EC2 instâncias ou a uma interface de rede elástica. No entanto, para determinados casos de uso, grupos de segurança independentes não representam um risco de segurança. Você pode usar outros EC2 controles, como EC2 .2, EC2 .13, EC2 .14, EC2 .18 e EC2 .19, para monitorar seus grupos de segurança.

Correção

Para criar, atribuir e excluir grupos de segurança, consulte Grupos de segurança para suas EC2 instâncias no Guia EC2 do usuário da Amazon.

[EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

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 EC2 trânsito 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.

[EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > 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

Esse controle verifica se o tipo de virtualização de uma EC2 instância é paravirtual. O controle falhará se o `virtualizationType` da EC2 instância estiver definido como`paravirtual`.

O Linux Amazon Machine Images (AMIs) usa um dos dois tipos de virtualização: paravirtual (PV) ou máquina virtual de hardware (HVM). As principais diferenças entre PV e HVM AMIs são a maneira pela qual eles inicializam e se podem aproveitar as extensões de hardware especiais (CPU, rede e armazenamento) para obter melhor desempenho.

Historicamente, os hóspedes fotovoltaicos tinham melhor desempenho do que os convidados HVM em muitos casos, mas devido aos aprimoramentos na virtualização de HVM e à disponibilidade de drivers fotovoltaicos para HVM, isso não é mais verdade. AMIs Para obter mais informações, consulte os tipos de virtualização do Linux AMI no Guia do EC2 usuário da Amazon.

Correção

Para atualizar uma EC2 instância para um novo tipo de instância, consulte Alterar o tipo de instância no Guia EC2 do usuário da Amazon.

[EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

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 EC2 lançamento da Amazon estão configurados para atribuir endereços IP públicos às interfaces de rede no lançamento. O controle falhará se um modelo de EC2 execução 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 aquele 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. EC2 os recursos não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional às suas cargas de trabalho.

Correção

Para atualizar um modelo de EC2 lançamento, consulte Alterar as configurações padrão da interface de rede 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 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Severidade: baixa

Tipo de recurso: `AWS::EC2::Volume`

AWS Config regra: **`ebs-resources-protected-by-backup-plan`**

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`backupVaultLockCheck`	O controle produzirá uma descoberta `PASSED` se o parâmetro estiver definido como `true` e o recurso usar o Vault Lock do AWS Backup .	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 EC2 trânsito devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TransitGatewayAttachment`

Regra AWS Config : `tagged-ec2-transitgatewayattachment` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um anexo do Amazon EC2 Transit Gateway 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 verificará apenas a existência de uma chave de tag e falhará se o anexo do gateway de trânsito não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um anexo de gateway de EC2 trânsito, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TransitGatewayRouteTable`

Regra AWS Config : `tagged-ec2-transitgatewayroutetable` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma tabela de rotas do Amazon EC2 Transit Gateway 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 verificará apenas 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 de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte [Tagging your AWS resources] na Referência geral da AWS.

Correção

Para adicionar tags a uma tabela de rotas de gateway de EC2 trânsito, consulte [Marcar seus EC2 recursos da Amazon] no Guia EC2 do usuário da Amazon.

[EC2.35] interfaces EC2 de rede devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::NetworkInterface`

Regra AWS Config : `tagged-ec2-networkinterface` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma interface EC2 de rede da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se a interface de rede não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma interface EC2 de rede, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.36] os gateways EC2 do cliente devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::CustomerGateway`

Regra AWS Config : `tagged-ec2-customergateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um gateway de EC2 cliente da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se o gateway do cliente não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um gateway EC2 do cliente, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.37] Os endereços IP EC2 elásticos devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::EIP`

Regra AWS Config : `tagged-ec2-eip` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um endereço IP EC2 elástico da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se o endereço IP elástico não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um endereço IP EC2 elástico, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.38] as EC2 instâncias devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::Instance`

Regra AWS Config : `tagged-ec2-instance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma EC2 instância da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a instância 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 verificará apenas a existência de uma chave de tag e falhará se a instância não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma EC2 instância, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.39] gateways de EC2 internet devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::InternetGateway`

Regra AWS Config : `tagged-ec2-internetgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um gateway de EC2 internet da Amazon 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 de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um gateway de EC2 internet, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.40] Os gateways EC2 NAT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::NatGateway`

Regra AWS Config : `tagged-ec2-natgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um gateway de tradução de endereços de EC2 rede (NAT) da Amazon 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 ele 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 NAT não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um gateway EC2 NAT, consulte Marcar seus EC2 recursos da Amazon no Guia do EC2 usuário da Amazon.

[EC2.41] a EC2 rede ACLs deve ser marcada

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::NetworkAcl`

Regra AWS Config : `tagged-ec2-networkacl` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma lista de controle de acesso à EC2 rede da Amazon (Network ACL) tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a ACL 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 verificará apenas a existência de uma chave de tag e falhará se a ACL de rede não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma ACL de EC2 rede, consulte Marcar seus EC2 recursos da Amazon no Guia do EC2 usuário da Amazon.

[EC2.42] tabelas de EC2 rotas devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::RouteTable`

Regra AWS Config : `tagged-ec2-routetable` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma tabela de EC2 rotas da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se a tabela de rotas não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma tabela de EC2 rotas, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.43] grupos EC2 de segurança devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regra AWS Config : `tagged-ec2-securitygroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um grupo EC2 de segurança da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se o grupo de segurança não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um grupo EC2 de segurança, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.44] EC2 sub-redes devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::Subnet`

Regra AWS Config : `tagged-ec2-subnet` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma EC2 sub-rede da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a ACL de rede não tiver

nenhuma chave de tag ou se a sub-rede 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 sub-rede não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma EC2 sub-rede, consulte Marcar seus EC2 recursos da Amazon no Guia do EC2 usuário da Amazon.

[EC2.45] EC2 volumes devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::Volume`

Regra AWS Config : `tagged-ec2-volume` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um EC2 volume da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a ACL de rede não tiver nenhuma chave de tag ou se o volume 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 volume não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um EC2 volume, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.46] Amazon VPCs deve ser etiquetada

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::VPC`

Regra AWS Config : `tagged-ec2-vpc` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 VPC de rede não

tiver nenhuma chave de tag ou se o volume 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 Amazon VPC não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma VPC, consulte Marcar EC2 seus recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.47] Os serviços de endpoint do Amazon VPC devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::VPCEndpointService`

Regra AWS Config : `tagged-ec2-vpcendpointservice` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um serviço de endpoint da Amazon VPV 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 verificará apenas a existência de uma chave de tag e falhará se o serviço de endpoint não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na 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 no Guia do AWS PrivateLink .

[EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::FlowLog`

Regra AWS Config : `tagged-ec2-flowlog` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 log 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 verificará apenas a existência de uma chave de tag e falhará se o log de fluxo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na 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 do Amazon VPC devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::VPCPeeringConnection`

Regra AWS Config : `tagged-ec2-vpcpeeringconnection` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se a conexão de emparelhamento não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma conexão de emparelhamento do Amazon VPC, consulte Marcar seus EC2 recursos da Amazon no Guia do usuário da Amazon EC2 .

[EC2.50] Os gateways de EC2 VPN devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::VPNGateway`

Regra AWS Config : `tagged-ec2-vpngateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um gateway Amazon EC2 VPN tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o gateway da 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 da VPN não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um gateway EC2 VPN, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), (26), NIST.800-53.r5 AC-2 (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-6 (8) 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-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.12, ist.800-171.r2 3.1.20, PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso: `AWS::EC2::ClientVpnEndpoint`

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] gateways EC2 de trânsito devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TransitGateway`

Regra AWS Config : `tagged-ec2-transitgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um gateway de EC2 trânsito da Amazon 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 verificará apenas a existência de uma chave de tag e falhará se o gateway de trânsito não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da

AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a um gateway de EC2 trânsito, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.53] grupos de EC2 segurança 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, PCI DSS v4.0.1/1.3.1

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regra do AWS Config : `vpc-sg-port-restriction-check`

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`ipType`	A versão de 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 EC2 segurança da Amazon 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 permite a entrada de 0.0.0.0/0 na porta 22 ou 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 permita acesso irrestrito às portas de administração de servidor remoto, como SSH à porta 22 e RDP à porta 3389, usando os protocolos TDP (6), UDP (17) ou ALL (-1). Permitir o acesso público a essas portas aumenta a superfície de ataque e o risco de comprometimento dos recursos.

Correção

Para atualizar uma regra EC2 de grupo de segurança para proibir o tráfego de entrada nas portas especificadas, consulte Atualizar regras do grupo de segurança no Guia EC2 do usuário da Amazon. Depois de selecionar um grupo de segurança no EC2 console da Amazon, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22 ou 3389.

[EC2.54] grupos EC2 de segurança 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, PCI DSS v4.0.1/1.3.1

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regra do AWS Config : `vpc-sg-port-restriction-check`

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`ipType`	A versão de 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 EC2 segurança da Amazon 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 na porta 22 ou 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 permita acesso irrestrito às portas de administração de servidor remoto, como SSH à porta 22 e RDP à porta 3389, usando os protocolos TDP (6), UDP (17) ou ALL (-1). Permitir o acesso público a essas portas aumenta a superfície de ataque e o risco de comprometimento dos recursos.

Correção

Para atualizar uma regra EC2 de grupo de segurança para proibir o tráfego de entrada nas portas especificadas, consulte Atualizar regras do grupo de segurança no Guia EC2 do usuário da Amazon. Depois de selecionar um grupo de segurança no EC2 console da Amazon, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22 ou 3389.

[EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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)

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`,`AWS::EC2::VPCEndpoint`

Regra do AWS Config : vpc-endpoint-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`serviceNames`	Obrigatório	O nome do serviço que o controle avalia	String	Não personalizável	`ecr.api`
`vpcIds`	Opcional	Lista separada por vírgulas do Amazon VPC IDs para VPC endpoints. Se fornecido, o controle falhará se os serviços especificados no `serviceName` parâmetro não tiverem um desses VPC endpoints.	StringList	Personalize com uma ou mais VPC IDs	Nenhum valor padrão

Esse controle verifica se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para a API do Amazon ECR. O controle falhará se a VPC não tiver uma interface VPC endpoint para a API ECR. Esse controle avalia os recursos em uma única conta.

AWS PrivateLink permite que os clientes AWS acessem serviços hospedados de forma altamente disponível e escalável, mantendo todo o tráfego da rede dentro da AWS rede. Os usuários do serviço podem acessar de forma privada os serviços fornecidos por meio PrivateLink de sua VPC ou local, sem usar o IPs público e sem exigir que o tráfego percorra a Internet.

Correção

Para configurar um VPC endpoint, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia.AWS PrivateLink

[EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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)

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`,`AWS::EC2::VPCEndpoint`

Regra do AWS Config : vpc-endpoint-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`serviceNames`	Obrigatório	O nome do serviço que	String	Não personalizável	`ecr.dkr`

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
		o controle avalia			
`vpcIds`	Opcional	Lista separada por vírgulas do Amazon VPC IDs para VPC endpoints. Se fornecido, o controle falhará se os serviços especificados no `serviceName` parâmetro não tiverem um desses VPC endpoints.	StringList	Personalize com uma ou mais VPC IDs	Nenhum valor padrão

Esse controle verifica se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para Docker Registry. O controle falhará se a VPC não tiver uma interface VPC endpoint para o Docker Registry. Esse controle avalia os recursos em uma única conta.

AWS PrivateLink permite que os clientes AWS acessem serviços hospedados de forma altamente disponível e escalável, mantendo todo o tráfego da rede dentro da AWS rede. Os usuários do serviço podem acessar de forma privada os serviços fornecidos por meio PrivateLink de sua VPC ou local, sem usar o IPs público e sem exigir que o tráfego percorra a Internet.

Correção

Para configurar um VPC endpoint, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia.AWS PrivateLink

[EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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)

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`,`AWS::EC2::VPCEndpoint`

Regra do AWS Config : vpc-endpoint-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`serviceNames`	Obrigatório	O nome do serviço que o controle avalia	String	Não personalizável	`ssm`
`vpcIds`	Opcional	Lista separada por	StringList	Personalize com uma ou	Nenhum valor padrão

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
		vírgulas do Amazon VPC IDs para VPC endpoints. Se fornecido, o controle falhará se os serviços especificados no `serviceName` parâmetro não tiverem um desses VPC endpoints.		mais VPC IDs	

Esse controle verifica se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para. AWS Systems Manager O controle falhará se a VPC não tiver uma interface VPC endpoint para Systems Manager. Esse controle avalia os recursos em uma única conta.

AWS PrivateLink permite que os clientes AWS acessem serviços hospedados de forma altamente disponível e escalável, mantendo todo o tráfego da rede dentro da AWS rede. Os usuários do serviço podem acessar de forma privada os serviços fornecidos por meio PrivateLink de sua VPC ou local, sem usar o IPs público e sem exigir que o tráfego percorra a Internet.

Correção

Para configurar um VPC endpoint, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia.AWS PrivateLink

[EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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)

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`,`AWS::EC2::VPCEndpoint`

Regra do AWS Config : vpc-endpoint-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`serviceNames`	Obrigatório	O nome do serviço que o controle avalia	String	Não personalizável	`ssm-contacts`
`vpcIds`	Opcional	Lista separada por vírgulas do Amazon VPC IDs	StringList	Personalize com uma ou mais VPC IDs	Nenhum valor padrão

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
		para VPC endpoints. Se fornecido, o controle falhará se os serviços especificados no `serviceName` parâmetro não tiverem um desses VPC endpoints.			

Esse controle verifica se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para contatos do Incident Manager. AWS Systems Manager O controle falhará se a VPC não tiver uma interface VPC endpoint para os contatos do Systems Manager Incident Manager. Esse controle avalia os recursos em uma única conta.

AWS PrivateLink permite que os clientes AWS acessem serviços hospedados de forma altamente disponível e escalável, mantendo todo o tráfego da rede dentro da AWS rede. Os usuários do serviço podem acessar de forma privada os serviços fornecidos por meio PrivateLink de sua VPC ou local, sem usar o IPs público e sem exigir que o tráfego percorra a Internet.

Correção

Para configurar um VPC endpoint, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia.AWS PrivateLink

[EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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)

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::EC2::VPC`,`AWS::EC2::VPCEndpoint`

Regra do AWS Config : vpc-endpoint-enabled

Tipo de programação: Periódico

Parâmetros:

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`serviceNames`	Obrigatório	O nome do serviço que o controle avalia	String	Não personalizável	`ssm-incidents`
`vpcIds`	Opcional	Lista separada por vírgulas do Amazon VPC IDs para VPC endpoints. Se fornecido,	StringList	Personalize com uma ou mais VPC IDs	Nenhum valor padrão

Parameter	Obrigatório	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
		o controle falhará se os serviços especificados no `serviceName` parâmetro não tiverem um desses VPC endpoints.			

Esse controle verifica se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para o Incident Manager. AWS Systems Manager O controle falhará se a VPC não tiver uma interface VPC endpoint para o Systems Manager Incident Manager. Esse controle avalia os recursos em uma única conta.

AWS PrivateLink permite que os clientes AWS acessem serviços hospedados de forma altamente disponível e escalável, mantendo todo o tráfego da rede dentro da AWS rede. Os usuários do serviço podem acessar de forma privada os serviços fornecidos por meio PrivateLink de sua VPC ou local, sem usar o IPs público e sem exigir que o tráfego percorra a Internet.

Correção

Para configurar um VPC endpoint, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia.AWS PrivateLink

[EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2

Requisitos relacionados: PCI DSS v4.0.1/2.2.6

Categoria: Proteger > Segurança de rede

Severidade: baixa

Tipo de recurso: `AWS::EC2::LaunchTemplate`

Regra do AWS Config : ec2-launch-template-imdsv2-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um modelo de EC2 lançamento da Amazon está configurado com o Instance Metadata Service versão 2 (IMDSv2). O controle falha se `HttpTokens` estiver definido como `optional`.

Executar os recursos em versões de software compatíveis garante a performance, a segurança e o acesso ideais aos recursos mais novos. Atualizações regulares protegem contra vulnerabilidades, o que ajuda a garantir uma experiência de usuário estável e eficiente.

Correção

Para solicitar um modelo IMDSv2 de EC2 lançamento, consulte Configurar as opções do serviço de metadados da instância no Guia do EC2 usuário da Amazon.

[EC2.171] As conexões EC2 VPN devem ter o registro ativado

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/5.3, PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::EC2::VPNConnection`

Regra do AWS Config : ec2-vpn-connection-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma conexão AWS Site-to-Site VPN tem o Amazon CloudWatch Logs habilitado para os dois túneis. O controle falhará se uma conexão Site-to-Site VPN não tiver CloudWatch registros habilitados para os dois túneis.

AWS Site-to-Site Os registros de VPN fornecem uma visibilidade mais profunda de suas implantações de Site-to-Site VPN. Com esse recurso, você tem acesso aos registros de conexão Site-to-Site VPN que fornecem detalhes sobre o estabelecimento do túnel IP Security (IPsec), negociações do Internet Key Exchange (IKE) e mensagens do protocolo Dead Peer Detection (DPD). Site-to-Site Os registros de VPN podem ser publicados em CloudWatch Registros. Esse recurso fornece aos clientes uma maneira única e consistente de acessar e analisar registros detalhados de todas as suas conexões Site-to-Site VPN.

Correção

Para ativar o registro em túneis em uma conexão EC2 VPN, consulte os registros de AWS Site-to-Site AWS Site-to-Site VPN no Guia do usuário de VPN.

[EC2.172] As configurações do EC2 VPC Block Public Access devem bloquear o tráfego do gateway da Internet

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: média

Tipo de recurso: `AWS::EC2::VPCBlockPublicAccessOptions`

Regra AWS Config : `ec2-vpc-bpa-internet-gateway-blocked` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`vpcBpaInternetGatewayBlockMode`	Valor da string do modo de opções do VPC BPA.	Enum	`block-bidirectional` , `block-ingress`	Nenhum valor padrão

Esse controle verifica se as configurações do Amazon EC2 VPC Block Public Access (BPA) estão definidas para bloquear o tráfego do gateway de internet para toda a Amazon VPCs no. Conta da AWS O controle falhará se as configurações de VPC BPA não estiverem definidas para bloquear o tráfego do gateway de Internet. Para que o controle seja aprovado, o VPC BPA `InternetGatewayBlockMode` deve ser definido como ou. `block-bidirectional` `block-ingress` Se o parâmetro `vpcBpaInternetGatewayBlockMode` for fornecido, o controle passará somente se o valor de BPA da VPC `InternetGatewayBlockMode` corresponder ao parâmetro.

Definir as configurações de VPC BPA para sua conta em Região da AWS an permite impedir que recursos e sub-redes que você possui nessa região VPCs cheguem ou sejam acessados pela Internet por meio de gateways de Internet e gateways de Internet somente de saída. Se você precisar de sub-redes específicas VPCs para acessar ou ser acessado pela Internet, você pode excluí-las configurando as exclusões de VPC BPA. Para obter instruções sobre como criar e excluir exclusões, consulte Criar e excluir exclusões no Guia do usuário da Amazon VPC.

Correção

Para ativar o BPA bidirecional no nível da conta, consulte Habilitar o modo bidirecional do BPA para sua conta no Guia do usuário da Amazon VPC. Para ativar o BPA somente de entrada, consulte Alterar o modo VPC BPA para somente entrada. Para habilitar o VPC BPA no nível da organização, consulte Habilitar o VPC BPA no nível da organização.

[EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::EC2::SpotFleet`

Regra do AWS Config : ec2-spot-fleet-request-ct-encryption-at-rest

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma solicitação do Amazon EC2 Spot Fleet que especifica parâmetros de execução está configurada para permitir a criptografia para todos os volumes do Amazon Elastic Block Store (Amazon EBS) anexados às instâncias. EC2 O controle falhará se a solicitação do Spot Fleet especificar parâmetros de lançamento e não habilitar a criptografia para um ou mais volumes do EBS especificados na solicitação.

Para uma camada adicional de segurança, você deve habilitar a criptografia para volumes do Amazon EBS. As operações de criptografia então ocorrem nos servidores que hospedam as EC2 instâncias da Amazon, o que ajuda a garantir a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu armazenamento EBS conectado. A criptografia do Amazon EBS é uma solução de criptografia simples para recursos do EBS associados às suas instâncias. EC2 Com a criptografia do EBS, você não precisa criar, manter e proteger sua própria infraestrutura de gerenciamento de chaves. A criptografia do EBS é usada AWS KMS keys ao criar volumes criptografados.

> **Observações**
>
> Esse controle não gera descobertas para solicitações do Amazon EC2 Spot Fleet que usam modelos de lançamento. Também não gera descobertas para solicitações do Spot Fleet que não especificam explicitamente um valor para o `encrypted` parâmetro.
> Em 23 de julho de 2025, o Security Hub alterou o título desse controle. Anteriormente, o título desse controle era: EC2 Spot Fleet requests should enable encryption for attached EBS volumes. O novo título reflete com mais precisão que o controle verifica apenas as solicitações do Spot Fleet que especificam os parâmetros de lançamento.

Correção

Não há uma forma direta de criptografar um volume Amazon EBS existente e não criptografado. Você pode criptografar um novo volume somente ao criá-lo.

No entanto, se você habilitar a criptografia por padrão, o Amazon EBS criptografa novos volumes usando sua chave padrão para criptografia do EBS. Se você não habilitar a criptografia por padrão, poderá habilitar a criptografia ao criar um volume individual. Em ambos os casos, você pode substituir a chave padrão para criptografia do EBS e escolher uma chave gerenciada pelo cliente. AWS KMS key Para obter mais informações sobre a criptografia do EBS, consulte a criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

Para obter informações sobre a criação de uma solicitação de frota EC2 spot da Amazon, consulte Criar uma frota spot no Guia do usuário do Amazon Elastic Compute Cloud.

[EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::DHCPOptions`

Regra do AWS Config : ec2-dhcp-options-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um conjunto de opções de EC2 DHCP da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o conjunto de opções não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o conjunto de opções não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um conjunto de opções de EC2 DHCP da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia do EC2 usuário da Amazon.

[EC2.175] modelos de EC2 lançamento devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::LaunchTemplate`

Regra do AWS Config : ec2-launch-template-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um modelo de EC2 lançamento da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o modelo de execução não

tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o modelo de execução não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um modelo de EC2 lançamento da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.176] as listas de EC2 prefixos devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::PrefixList`

Regra do AWS Config : ec2-prefix-list-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma lista de EC2 prefixos da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a lista de prefixos não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a lista de prefixos não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a uma lista de EC2 prefixos da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia do EC2 usuário da Amazon.

[EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TrafficMirrorSession`

Regra do AWS Config : ec2-traffic-mirror-session-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma sessão de espelho de EC2 tráfego da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a sessão não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a sessão não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por

finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a uma sessão de espelhamento de EC2 tráfego da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TrafficMirrorFilter`

Regra do AWS Config : ec2-traffic-mirror-filter-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um filtro de espelho de EC2 tráfego da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o filtro não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o filtro não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um filtro de espelhamento de EC2 tráfego da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EC2::TrafficMirrorTarget`

Regra do AWS Config : ec2-traffic-mirror-target-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um alvo do espelho de EC2 tráfego da Amazon tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o destino não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o destino não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um destino de espelhamento de EC2 tráfego da Amazon, consulte Marcar seus EC2 recursos da Amazon no Guia EC2 do usuário da Amazon.

[EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso: `AWS::EC2::NetworkInterface`

Regra do AWS Config : ec2-enis-source-destination-check-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a source/destination verificação está habilitada para uma interface de rede EC2 elástica (ENI) da Amazon gerenciada pelos usuários. O controle falhará se a source/destination verificação for desativada para a ENI gerenciada pelo usuário. Esse controle verifica somente os seguintes tipos de ENIs: `aws_codestar_connections_managed branchefa`,`interface`,`lambda`,, `quicksight` e.

Source/destination checking for Amazon EC2 instances and attached ENIs should be enabled and configured consistently across your EC2 instances. Each ENI has its own setting for source/destination checks. If source/destination checking is enabled, Amazon EC2 enforces source/destinationvalidação de endereço, que garante que uma instância seja a origem ou o destino de qualquer tráfego recebido. Isso fornece uma camada adicional de segurança de rede, impedindo que os recursos manipulem tráfego não intencional e impedindo a falsificação de endereços IP.

> **Note**
>
> Se você estiver usando uma EC2 instância como instância NAT e tiver desativado a source/destination verificação de sua ENI, poderá usar um gateway NAT em vez disso.

Correção

Para obter informações sobre como habilitar source/destination verificações para uma Amazon EC2 ENI, consulte Modificar atributos da interface de rede no Guia do EC2 usuário da Amazon.

Controles do Security Hub para o Auto Scaling

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon EC2 Auto Scaling.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 CP-2 (2) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

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 do Auto Scaling não usar as verificações de integridade do ELB.

As verificações de integridade do ELB garantem que o 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 de Auto EC2 Scaling.

Correção

Para adicionar verificações de saúde do Elastic Load Balancing, consulte Adicionar verificações de saúde do Elastic Load Balancing no Guia do usuário do Amazon Auto EC2 Scaling.

[AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regra do AWS Config : `autoscaling-multiple-az`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 de 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 usa um valor padrão de dois AZs.

Um grupo de Auto Scaling que não abrange várias não AZs pode 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

AZs Para adicionar a um grupo existente do Auto Scaling, consulte Adicionar e remover zonas de disponibilidade no Guia do usuário do Amazon Auto EC2 Scaling.

[AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 2 () IMDSv2

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.6

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

Regra do AWS Config : `autoscaling-launchconfig-requires-imdsv2`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se IMDSv2 está habilitado em todas as instâncias iniciadas pelos grupos do Amazon EC2 Auto Scaling. O controle falhará se a versão do Instance Metadata Service (IMDS) não estiver incluída na configuração de execução ou estiver configurada como`token optional`, o que é uma configuração que permite ou IMDSv1 . IMDSv2

O IMDS fornece dados da instância que você pode usar para configurar ou gerenciar a instância em execução.

A versão 2 do IMDS adiciona novas proteções que não estavam disponíveis IMDSv1 para proteger ainda mais suas instâncias. 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 lançamento de um grupo de Auto Scaling, use uma configuração de inicialização existente como base para uma nova configuração de inicialização com IMDSv2 habilitada. Para obter mais informações, consulte Configurar opções de metadados de instância para novas instâncias no Guia do EC2 usuário da Amazon.

[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 descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

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 Instance Metadata Service (IMDS) fornece informações de metadados sobre uma EC2 instância da Amazon e é útil para configuração de aplicativos. Restringir a PUT resposta HTTP do serviço de metadados somente à EC2 instância 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 EC2. IMDSv2 protege EC2 instâncias que podem ter sido configuradas incorretamente como roteadores abertos, firewalls de camada 3, túneis ou dispositivos NAT VPNs, o que impede que usuários não autorizados recuperem metadados. Com IMDSv2, a PUT resposta que contém o token secreto não pode sair da instância porque o limite de salto de resposta de metadados padrão está definido como. 1 No entanto, se esse valor for maior que1, o token poderá sair da EC2 instância.

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 EC2 do usuário da Amazon.

[Autoscaling.5] As instâncias da EC2 Amazon lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

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.

EC2 As instâncias da Amazon em uma configuração de lançamento em grupo do Auto Scaling não devem ter um endereço IP público associado, exceto em casos extremos limitados. EC2 As

instâncias da Amazon só devem ser acessadas 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 Auto EC2 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 atualização de instâncias do Auto Scaling, consulte Atualizar instâncias do Auto Scaling no Guia do usuário do Amazon Auto EC2 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 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

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 de Auto Scaling com vários tipos de instância, consulte Grupos de Auto Scaling com vários tipos de instância e opções de compra no Guia do usuário do Amazon Auto EC2 Scaling.

[AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento da Amazon EC2

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regra do AWS Config : `autoscaling-launch-template`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo do Amazon EC2 Auto Scaling foi criado a partir de um modelo de EC2 lançamento. 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.

Um grupo de EC2 Auto Scaling pode ser criado a partir de um modelo de EC2 execução ou de uma configuração de execução. No entanto, 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 de Auto Scaling com um modelo de EC2 lançamento, consulte Criar um grupo de Auto Scaling usando um modelo de lançamento no Guia do usuário do Amazon Auto EC2

Scaling. Para obter informações sobre como substituir uma configuração de lançamento por um modelo de lançamento, consulte Substituir uma configuração de lançamento por um modelo de lançamento no Guia EC2 do usuário da Amazon.

[AutoScaling.10] Grupos de EC2 Auto Scaling devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regra AWS Config : `tagged-autoscaling-autoscalinggroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 do 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 verificará apenas a existência de uma chave de tag e falhará se o grupo do Auto Scaling não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 do Auto Scaling, consulte Grupos e instâncias do Tag Auto Scaling no Guia do usuário do Amazon Auto EC2 Scaling.

Controles do Security Hub para o Amazon ECR

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Elastic Container Registry (Amazon ECR).

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ECR.1] Os repositórios privados do ECR devem ter a digitalização de imagens configurada

Requisitos relacionados: PCI DSS v4.0.1/6.2.3 NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.4

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso: `AWS::ECR::Repository`

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 ECR 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 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8 (1)

Categoria: Identificar > Inventário > Marcação

Severidade: média

Tipo de recurso: `AWS::ECR::Repository`

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.

[ECR.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::ECR::Repository`

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, você pode 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ECR::PublicRepository`

Regra AWS Config : `tagged-ecr-publicrepository` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um repositório Public do Amazon ECR Public tem tags com 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 verificará apenas a existência de uma chave de tag e falhará se o repositório público não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Tagging an Amazon ECR public repository no Amazon Elastic Container Registry User Guide.

[ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys

Requisitos relacionados: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), (1), NIST.800-53.r5 SC-7 NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 NIST.800-53.r5 CA-9 (6), NIST.800-53.r5 AU-9

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::ECR::Repository`

Regra do AWS Config : ecr-repository-cmk-encryption-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`kmsKeyArns`	Uma lista de nomes de recursos da Amazon (ARNs) AWS KMS keys a serem	StringList (máximo de 10 itens)	1 a 10 ARNs das chaves KMS	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	incluídos na avaliação. O controle gera uma `FAILED` descoberta se um repositório ECR não estiver criptografado com uma chave KMS na lista.		existentes. Por exemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	

Esse controle verifica se um repositório Amazon ECR está criptografado em repouso com um cliente gerenciado. AWS KMS key O controle falhará se o repositório ECR não estiver criptografado com uma chave KMS gerenciada pelo cliente. Opcionalmente, você pode especificar uma lista de chaves KMS para o controle incluir na avaliação.

Por padrão, o Amazon ECR criptografa os dados do repositório com as chaves gerenciadas do Amazon S3 (SSE-S3), usando um algoritmo AES-256. Para controle adicional, você pode configurar o Amazon ECR para criptografar os dados com um AWS KMS key (SSE-KMS ou DSSE-KMS) em vez disso. A chave KMS pode ser: uma Chave gerenciada pela AWS que o Amazon ECR cria e gerencia para você e tem o alias`aws/ecr`, ou uma chave gerenciada pelo cliente que você cria e gerencia no seu. Conta da AWS Com uma chave KMS gerenciada pelo cliente, você tem controle total da chave. Isso inclui definir e manter a política de chaves, gerenciar concessões, alternar material criptográfico, atribuir tags, criar aliases e ativar e desativar a chave.

> **Note**
>
> AWS KMS oferece suporte ao acesso entre contas às chaves KMS. Se um repositório ECR for criptografado com uma chave KMS de propriedade de outra conta, esse controle não executará verificações entre contas ao avaliar o repositório. O controle não avalia se

o Amazon ECR pode acessar e usar a chave ao realizar operações criptográficas para o repositório.

Correção

Você não pode alterar as configurações de criptografia de um repositório ECR existente. No entanto, você pode especificar configurações de criptografia diferentes para repositórios ECR que você criar posteriormente. O Amazon ECR suporta o uso de diferentes configurações de criptografia para repositórios individuais.

Para obter mais informações sobre as opções de criptografia para repositórios ECR, consulte Criptografia em repouso no Guia do usuário do Amazon ECR. Para obter mais informações sobre gerenciamento de clientes AWS KMS keys, consulte AWS KMS keyso Guia do AWS Key Management Service desenvolvedor.

Controles do Security Hub para o Amazon ECS

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Elastic Container Service (Amazon ECS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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-5, NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

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.

[ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::ECS::Service`

Regra AWS Config : `ecs-service-assign-public-ip-disabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

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 IP 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

Primeiro, você deve criar uma definição de tarefa para o cluster que use o modo de rede `awsvpc` e especifique FARGATE em `requiresCompatibilities`. Depois, em Configuração de computação, escolha Tipo de inicialização e FARGATE. Por fim, no campo Rede, desative IP público para desabilitar a atribuição automática de um IP público para seu serviço.

[ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identificar > Configuração de recursos

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regra do AWS Config : 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 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.

[ECS.4] Os contêineres ECS devem ser executados sem privilégios

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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-5, NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Restrições de acesso do usuário raiz

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

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 do privilégio é `true`, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

Correção

Para configurar o parâmetro `privileged` na definição de uma tarefa, consulte Parâmetros avançados de definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

[ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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-5, NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regra do AWS Config : ecs-containers-readonly-access

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um contêiner do Amazon ECS tem acesso somente de leitura ao seu sistema de arquivos raiz. O controle falhará se o `readonlyRootFilesystem` parâmetro estiver definido como ou se `false` o parâmetro não existir na definição do contêiner dentro da definição da tarefa. Esse controle avalia somente a última revisão ativa de uma definição de tarefa do Amazon ECS.

Se o `readonlyRootFilesystem` parâmetro estiver definido como `true` em uma definição de tarefa do Amazon ECS, o contêiner ECS receberá acesso somente de leitura ao seu sistema de arquivos raiz. Isso reduz os vetores de ataque à segurança porque o sistema de arquivos raiz da instância do contêiner não pode ser adulterado ou gravado sem montagens de volume explícitas que tenham permissões de leitura e gravação para pastas e diretórios do sistema de arquivos. A ativação dessa opção também segue o princípio do menor privilégio.

Correção

Para dar a um contêiner do Amazon ECS acesso somente de leitura ao seu sistema de arquivos raiz, adicione o `readonlyRootFilesystem` parâmetro à definição da tarefa do contêiner e defina o valor do parâmetro como. `true` Para obter informações sobre parâmetros de definição de tarefas e como adicioná-los a uma definição de tarefa, consulte Definições de tarefas do Amazon ECS e Atualização de uma definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

[ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/8.6.2

Categoria: Proteger > Desenvolvimento seguro > Credenciais sem codificação rígida

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

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.

[ECS.9] 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 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

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), você pode desativar 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.

[ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

Requisitos relacionados: 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), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::ECS::Service`

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)

Esse controle 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, uma nova versão pode ter sido lançada para o kernel ou haver atualizações para o 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.

[ECS.12] Os clusters do ECS devem usar Container Insights

Requisitos relacionados: 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-2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::ECS::Cluster`

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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ECS::Service`

Regra AWS Config : `tagged-ecs-service` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o serviço não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcação de recursos do Amazon ECS, no Guia do Desenvolvedor do Amazon Elastic Container Service.

[ECS.14] Os clusters do ECS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ECS::Cluster`

Regra AWS Config : `tagged-ecs-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcação de 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regra AWS Config : `tagged-ecs-taskdefinition` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 de 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 verificará apenas a existência de uma chave de tag e falhará se a definição de tarefa não estiver marcada com

nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcação de recursos do Amazon ECS, no Guia do Desenvolvedor do Amazon Elastic Container Service.

[ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos

Requisitos relacionados: PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::ECS::TaskSet`

Regra AWS Config : `ecs-taskset-assign-public-ip-disabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um conjunto de tarefas do Amazon ECS está configurado para atribuir automaticamente endereços IP públicos. O controle falha se `AssignPublicIP` estiver definido como `ENABLED`.

Um endereço IP público é acessível pela Internet. Se você configurar seu conjunto de tarefas com um endereço IP público, os recursos associados ao conjunto de tarefas poderão ser acessados pela internet. Os conjuntos de tarefas do ECS não devem ser acessíveis ao público, pois isso pode permitir acesso não pretendido aos servidores de aplicações de contêiner.

Correção

Para atualizar um conjunto de tarefas do ECS para que ele não use um endereço IP público, consulte Atualização de um serviço do Amazon ECS usando o console no Guia do desenvolvedor do Amazon Elastic Container Service.

[ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regra do AWS Config : ecs-task-definition-network-mode-not-host

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a última revisão ativa de uma definição de tarefa do Amazon ECS usa o modo `host` de rede. O controle falhará se a última revisão ativa da definição de tarefa do ECS usar o modo `host` de rede.

Ao usar o modo de `host` rede, a rede de um contêiner do Amazon ECS é vinculada diretamente ao host subjacente que está executando o contêiner. Consequentemente, esse modo permite que os

contêineres se conectem a serviços de rede de loopback privados no host e representem o host. Outras desvantagens significativas são que não há como remapear uma porta de contêiner ao usar o modo de `host` rede e você não pode executar mais do que uma única instanciação de uma tarefa em cada host.

Correção

Para obter informações sobre modos e opções de rede para tarefas do Amazon ECS hospedadas em EC2 instâncias da Amazon, consulte as opções de rede de tarefas do Amazon ECS para o tipo de EC2 lançamento no Amazon Elastic Container Service Developer Guide. Para obter informações sobre como criar uma nova revisão de uma definição de tarefa e especificar um modo de rede diferente, consulte Atualização de uma definição de tarefa do Amazon ECS nesse guia.

Se a definição de tarefa do Amazon ECS foi criada por AWS Batch, consulte Modos de rede para AWS Batch trabalhos para aprender sobre os modos de rede e o uso típico dos tipos de AWS Batch trabalho e escolher uma opção segura.

Controles do Security Hub para o Amazon EFS

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Elastic File System (Amazon EFS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::EFS::FileSystem`

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 Amazon EFS, você deve criar sistemas de arquivos criptografados. O Amazon EFS é compatível com criptografia de sistemas de arquivos em repouso. É possível ativar a criptografia em repouso ao criar um sistema de arquivos do Amazon EFS. Para obter mais informações sobre a criptografia Amazon EFS, consulte Criptografia de dados no Amazon EFS no Guia 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 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups

Severidade: média

Tipo de recurso: `AWS::EFS::FileSystem`

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 .

[EFS.3] Os pontos de acesso do EFS devem executar um diretório raiz

Requisitos relacionados: NIST.800-53.r5 AC-6 (10)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::EFS::AccessPoint`

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.

[EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário

Requisitos relacionados: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0.1/7.3.1

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::EFS::AccessPoint`

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 executar uma identidade de usuário. 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EFS::AccessPoint`

Regra AWS Config: `tagged-efs-accesspoint` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o ponto de acesso não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 de acesso do EFS, consulte Tagging Amazon EFS resources no Amazon Elastic File System User Guide.

[EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização

Categoria: Proteger > Segurança de rede > Recursos não acessíveis ao público

Severidade: média

Tipo de recurso: `AWS::EFS::FileSystem`

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 sub-redes que atribuem endereços IP públicos na inicialização. O controle falhará se o destino de montagem estiver associado a sub-redes que atribuem endereços IP públicos na inicialização.

Todas as sub-redes têm um atributo que determina se uma interface de rede criada na sub-rede recebe automaticamente um endereço público. IPv4 Os destinos de montagem do Amazon EFS que são lançados em sub-redes com esse atributo ativado têm um endereço IP público atribuído à sua interface de rede primária.

Note

Em 13 de agosto de 2025, o Security Hub alterou o título e a descrição desse controle. O novo título e a descrição refletem com mais precisão o escopo e a natureza da verificação que o controle executa. Anteriormente, o título desse controle era: EFS mount targets should not be associated with a public subnet.

Correção

Para associar um destino de montagem existente a uma sub-rede diferente, você deve criar um novo destino de montagem em uma sub-rede que não atribua endereços IP públicos na inicialização e, em seguida, remover o destino de montagem antigo. Para obter informações sobre o gerenciamento de destinos de montagem, consulte Creating and managing mount targets and security groups no Amazon Elastic File System User Guide.

[EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::EFS::FileSystem`

Regra do AWS Config : efs-automatic-backups-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um sistema de arquivos do Amazon EFS tem backups automáticos habilitados. Esse controle falhará se o sistema de arquivos EFS não tiver backups automáticos habilitados.

Um backup de dados é uma cópia dos dados do sistema, da configuração ou da aplicação que é armazenada separa do original. Habilitar backups regulares ajuda a proteger dados valiosos contra eventos imprevistos, como falhas no sistema, ataques cibernéticos ou exclusões acidentais. Ter uma estratégia de backup robusta também facilita recuperações mais rápidas, continuidade dos negócios e tranquilidade diante da possível perda de dados.

Correção

Para obter informações sobre o uso AWS Backup de sistemas de arquivos EFS, consulte Backup de sistemas de arquivos EFS no Guia do usuário do Amazon Elastic File System.

[EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::EFS::FileSystem`

Regra do AWS Config : efs-filesystem-ct-encrypted

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um sistema de arquivos do Amazon EFS criptografa dados com AWS Key Management Service (AWS KMS). O controle falhará se um sistema de arquivos não for criptografado.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para habilitar a criptografia em repouso de um novo sistema de arquivos do EFS, consulte Encrypting data at rest no Amazon Elastic File System User Guide.

Controles do Security Hub para o Amazon EkS

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Elastic Kubernetes Service (Amazon EKS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::EKS::Cluster`

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 novo cluster, o Amazon EKS cria um endpoint para o servidor gerenciado de API do Kubernetes que é usado para comunicação com o cluster. 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, você pode 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. Você pode 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.

[EKS.2] 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-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), PCI DSS v4.0.1/12.3.4

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso: `AWS::EKS::Cluster`

Regra do AWS Config : eks-cluster-supported-version

Tipo de programação: acionado por alterações

Parâmetros:

- `oldestVersionSupported`: `1.31` (não personalizável)

Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão compatível do Kubernetes. O controle falhará se o cluster do EKS for executado em uma versão não compatível.

Se a sua aplicação não exigir uma versão específica do Kubernetes, recomendamos que você use a versão do Kubernetes mais recente disponível compatível com o EKS para seus clusters. Para obter

mais informações, consulte o calendário de lançamento do Kubernetes do Amazon EKS e entenda o ciclo de vida da versão do Kubernetes no Amazon EKS no Guia do usuário do Amazon EKS.

Correção

Para atualizar um cluster EKS, consulte Atualizar um cluster existente para uma nova versão do Kubernetes no Guia do usuário do Amazon EKS.

[EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, PCI DSS v4.0.1/8.3.2

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::EKS::Cluster`

Regra do AWS Config : eks-cluster-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 forem 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 habilitada por padrão para todos os dados (incluindo segredos) armazenados no etcd como parte de um cluster do EKS. Usar criptografia de segredos para o cluster do EKS permite implantar uma estratégia de defesa em profundidade para aplicações do Kubernetes, criptografando os segredos do Kubernetes com uma chave do KMS que você define e gerencia.

Correção

Para habilitar a criptografia de segredos em um cluster do EKS, consulte Habilitar a criptografia de segredos em um cluster existente no Manual do usuário do Amazon EKS.

[EKS.6] Os clusters do EKS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EKS::Cluster`

Regra AWS Config : `tagged-eks-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Marcar recursos do Amazon EKS com tags no Manual do usuário do Amazon EKS.

[EKS.7] As configurações do provedor de identidades do EKS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::EKS::IdentityProviderConfig`

Regra AWS Config : `tagged-eks-identityproviderconfig` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se a configuração de um provedor de identidades 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 verificará apenas a existência de uma chave de tag e falhará se a configuração não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 identidades EKS, consulte Marcar recursos do Amazon EKS com tags no Manual do usuário do Amazon EKS.

[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::EKS::Cluster`

Regra do AWS Config : eks-cluster-log-enabled

Tipo de programação: acionado por alterações

Parâmetros:

- `logTypes: audit` (não personalizável)

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.

> **Note**
>
> Esse controle não verifica se o registro em log de auditoria do Amazon EKS é habilitado por meio do Amazon Security Lake para Conta da AWS.

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 log 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.

Controles do Security Hub para ElastiCache

Esses AWS Security Hub controles avaliam o ElastiCache serviço e os recursos da Amazon.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`,`AWS:ElastiCache:ReplicationGroup`

Regra do AWS Config : elasticache-redis-cluster-automatic-backup-check

Tipo de programação: Periódico

Parâmetros:

Parameter	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 (Redis OSS) 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 (Redis OSS) 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. Você pode 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 (Redis OSS), consulte Programação de backups automáticos no Guia do usuário da Amazon ElastiCache .

[ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas

Requisitos relacionados: 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) PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`

Regra do AWS Config : `elasticache-auto-minor-version-upgrade-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle avalia se a Amazon aplica ElastiCache automaticamente atualizações de versões menores a um cluster de cache. O controle falhará se o cluster de cache não tiver atualizações de versão secundárias aplicadas automaticamente.

> **Note**
>
> Esse controle não se aplica aos clusters do ElastiCache Memcached.

A atualização automática de versões secundárias é um recurso que você pode ativar na Amazon ElastiCache para atualizar automaticamente seus clusters de cache quando uma nova versão secundária do mecanismo de cache estiver disponível. Essas atualizações podem incluir patches de segurança e correções de erros. Continuar up-to-date com a instalação do patch é uma etapa importante para proteger os sistemas.

Correção

Para aplicar automaticamente pequenas atualizações de versões a um cluster de ElastiCache cache existente, consulte Gerenciamento de versões ElastiCache no Guia do ElastiCache usuário da Amazon.

[ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regra do AWS Config : `elasticache-repl-grp-auto-failover-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de ElastiCache replicação tem o failover automático ativado. O controle falhará se o failover automático não estiver habilitado para um grupo de replicação.

Quando o failover automático é habilitado para um grupo de replicação, o perfil 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, reduzindo o tempo de interrupção geral em caso de falha.

Correção

Para habilitar o failover automático para um grupo de ElastiCache replicação existente, consulte Modificação de um ElastiCache cluster no Guia do usuário da Amazon ElastiCache . Se você usa o ElastiCache console, defina o failover automático como ativado.

[ElastiCache.4] os grupos de ElastiCache 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::ElastiCache::ReplicationGroup`

Regra do AWS Config : `elasticache-repl-grp-encrypted-at-rest`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de ElastiCache replicação está criptografado em repouso. O controle falhará se o grupo de replicação 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 Os grupos de replicação (Redis OSS) devem ser criptografados em repouso para uma camada adicional de segurança.

Correção

Para configurar a criptografia em repouso em um grupo de ElastiCache replicação, consulte Habilitar a criptografia em repouso no Guia do usuário da Amazon ElastiCache .

[ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regra do AWS Config : `elasticache-repl-grp-encrypted-in-transit`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de ElastiCache replicação está criptografado em trânsito. O controle falhará se o grupo de replicação não estiver criptografado em trânsito.

Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede. A ativação da criptografia em trânsito em um grupo de ElastiCache replicação 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 ElastiCache replicação, consulte Habilitar a criptografia em trânsito no Guia do usuário da Amazon ElastiCache .

[ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.3.1

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regra do AWS Config : `elasticache-repl-grp-redis-auth-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de replicação ElastiCache (Redis OSS) tem o Redis OSS AUTH ativado. O controle falhará se a versão do Redis OSS dos nós do grupo de replicação for abaixo de 6.0 e o `AuthToken` não estiver em uso.

Ao usar os tokens de autenticação do Redis, ou senhas, o Redis exige 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 grupo de replicação ElastiCache (Redis OSS), consulte Modificação do token AUTH em um cluster existente ElastiCache (Redis OSS) 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 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: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`

Regra do AWS Config : `elasticache-subnet-group-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um ElastiCache cluster está configurado com um grupo de sub-rede personalizado. O controle falhará se `CacheSubnetGroupName` for um ElastiCache cluster 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.

Controles do Security Hub para o Elastic Beanstalk

Esses AWS Security Hub controles avaliam o AWS Elastic Beanstalk serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de saúde aprimorados habilitados

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

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 integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas. O agente de saúde do Elastic Beanstalk, incluído nas Amazon Machine AMIs Images () suportadas, avalia registros e métricas de instâncias do ambiente. EC2

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 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

Regra do AWS Config : `elastic-beanstalk-managed-updates-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

Regra do AWS Config : `elastic-beanstalk-logs-to-cloudwatch`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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

Controles do Security Hub para o Elastic Load Balancing

Esses AWS Security Hub controles avaliam o serviço e os recursos do Elastic Load Balancing. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-1 7 (2), (1), 2 (3), 3 NIST.800-53.r5 AC-4, 3, 3 NIST.800-53.r5 IA-5 (3), (4), NIST.800-53.r5 SC-1 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

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 receptores HTTP dos Application Load Balancers. 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 seu balanceador de cargas. Para executar a criptografia em trânsito, você deve usar ações de redirecionamento com os Application Load Balancers para redirecionar uma solicitação HTTP do cliente para uma solicitação do HTTPS na porta 443.

Para saber mais, consulte Receptores para seus Application Load Balancers 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. Para Protocolo : Porta, escolha HTTP e insira **80**. 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. Para Protocolo : Porta, escolha HTTP e insira **80**. Em Adicionar ação, Redirecionar para, escolha HTTPS e, em seguida, insira **443**.

[ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (5), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-171.r2 3.13.8 NIST.800-53.r5 SC-8

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regra do AWS Config : elb-acm-certificate-required

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o Classic Load Balancer usa HTTPS/SSL certificados fornecidos pelo AWS Certificate Manager (ACM). O controle falhará se o Classic Load Balancer configurado com o HTTPS/SSL ouvinte não usar um certificado fornecido pelo ACM.

Para criar um certificado, você pode usar o ACM ou uma ferramenta que ofereça suporte aos protocolos SSL e TLS, como OpenSSL. O Security Hub recomenda que você use o ACM para criar ou importar certificados para o balanceador de carga.

O ACM se integra aos Classic Load Balancers 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 SSL/TLS certificado ACM a um Classic Load Balancer, consulte AWS o artigo do Knowledge Center Como posso associar um certificado SSL/TLS ACM a um Classic, Application ou Network Load Balancer?

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (3), (4), NIST.800-53.r5 SC-1, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

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 falha se o receptor não estiver configurado com TLS ou HTTPS para conexões front-end.

Antes de começar a usar um balanceador de cargas, 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 ouvintes podem suportar tanto HTTP quanto HTTPS/TLS protocolos. 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 transformar todos os ouvintes não compatíveis em ouvintes TLS/HTTPS

1. Abra o EC2 console da Amazon 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.

[ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos

Requisitos relacionados: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/6.2.4

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regra do AWS Config : alb-http-drop-invalid-header-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle avalia seu um Application Load Balancers está configurado para descartar cabeçalhos HTTP inválidos. O controle falha se o valor de `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.

> **Note**
>
> Recomendamos desabilitar esse controle se o ELB.12 estiver habilitado em sua conta. Para obter mais informações, consulte [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso.

Correção

Para corrigir esse problema, configure seu balanceador de carga para eliminar campos de cabeçalho inválidos.

Para configurar o balanceador de carga para eliminar campos de cabeçalho inválidos

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Load balancers.
3. Escolha um Application Load Balancer
4. Em Ações, escolha Editar atributos.
5. Em Eliminar campos de cabeçalho inválidos, escolha Habilitar.
6. Escolha Salvar.

[ELB.5] 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 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`,`AWS::ElasticLoadBalancingV2::LoadBalancer`

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` for `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 saber mais, consulte Logs de acesso para seu 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] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regra do AWS Config : elb-deletion-protection-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um balanceador de carga de aplicação, gateway ou rede tem a proteção contra exclusão habilitada. O controle falhará se a proteção contra exclusão não estiver habilitada.

Habilite a proteção contra exclusão para proteger o balanceador de aplicação, de gateway ou de rede contra 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 habilitar a proteção contra exclusão de um balanceador de carga de aplicação, consulte Deletion protection no User Guide for Application Load Balancers. Para habilitar a proteção contra exclusão de um balanceador de carga de gateway, consulte Deletion protection no User Guide for Application Load Balancers. Para habilitar a proteção contra exclusão de um balanceador de carga de rede, consulte Deletion protection no User Guide for Application Load Balancers.

[ELB.7] Os Classic Load Balancers devem ter a drenagem da conexão ativada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Recuperação > Resiliência

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

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-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (3), (4), NIST.800-53.r5 SC-1, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

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 HTTPS/SSL ouvintes do Classic Load Balancer usam a política predefinida. `ELBSecurityPolicy-TLS-1-2-2017-01` O controle falhará se os HTTPS/SSL ouvintes 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 de ordem do 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 Políticas de segurança SSL predefinidas para Classic Load Balancers 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.

[ELB.9] 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

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 ativado para os Classic Load Balancers (). CLBs O controle falhará se o balanceamento de carga entre zonas não estiver habilitado para um CLB.

Um 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 detalhes, consulte Balanceamento de carga entre zonas no Guia 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.

[ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regra do AWS Config : clb-multiple-az

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 pelo 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 usa um valor padrão de dois AZs.

Um Classic Load Balancer pode ser configurado para distribuir solicitações recebidas entre EC2 instâncias da Amazon 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.

[ELB.12] 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-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/6.2.4

Categoria: Proteção > Integridade dos dados

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regra do AWS Config : alb-desync-mode-check

Tipo de programação: acionado por alterações

Parâmetros:

- `desyncMode`: `defensive, strictest` (não personalizável)

Esse controle verifica se um Application Load Balancer está 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.

[ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regra do AWS Config : elbv2-multiple-az

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 (Load Balancer de aplicativo, rede ou gateway) registrou instâncias de pelo 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 usa um valor padrão de dois AZs.

O Elastic Load Balancing distribui automaticamente seu tráfego de entrada em vários destinos, como EC2 instâncias, 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-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/6.2.4

Categoria: Proteção > Integridade dos dados

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regra do AWS Config : clb-desync-mode-check

Tipo de programação: acionado por alterações

Parâmetros:

- `desyncMode`: `defensive, strictest` (não personalizável)

Esse controle verifica se um Classic Load Balancer está 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 sequestro de credenciais ou à execução de comandos não autorizados. Os Classic 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 AC-4 (21)

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

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 `Enabled` campo da AWS WAF configuração estiver definido como`false`.

AWS WAF é um firewall de aplicativos da web que ajuda a proteger os aplicativos da web e APIs 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 AWS WAF uma ACL da web 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

[ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::Listener`

Regra do AWS Config : elbv2-predefined-security-policy-ssl-check

Tipo de programação: acionado por alterações

Parâmetros:`sslPolicies`: `ELBSecurityPolicy-TLS13-1-2-2021-06, ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04` (não personalizável)

Esse controle verifica se o ouvinte HTTPS para um Application Load Balancer ou o ouvinte TLS para um Network Load Balancer está configurado para criptografar dados em trânsito usando uma política de segurança recomendada. O controle falhará se o ouvinte HTTPS ou TLS de um balanceador de carga não estiver configurado para usar uma política de segurança recomendada.

O Elastic Load Balancing usa uma configuração de negociação SSL, conhecida como política de segurança, para negociar conexões entre um cliente e um balanceador de carga. A política de segurança especifica uma combinação de protocolos e cifras. O protocolo estabelece uma conexão

segura entre um cliente e um servidor. A cifra é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. Durante o processo de negociação de conexão, o cliente e o load balancer apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. Usar uma política de segurança recomendada para um balanceador de carga pode ajudar você a atender aos padrões de conformidade e segurança.

Correção

Para obter informações sobre as políticas de segurança recomendadas e como atualizar os ouvintes, consulte as seguintes seções dos Guias do Usuário do Elastic Load Balancing: Políticas de segurança para Application Load Balancers, Políticas de segurança para Network Load Balancers, Atualização de um ouvinte HTTPS para seu Application Load Balancer e Atualização de um ouvinte para seu Network Load Balancer.

[ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::ElasticLoadBalancingV2::Listener`

Regra do AWS Config : elbv2-listener-encryption-in-transit

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o ouvinte de um Application Load Balancer ou Network Load Balancer está configurado para usar um protocolo seguro para criptografia de dados em trânsito. O controle falhará se um ouvinte do Application Load Balancer não estiver configurado para usar o protocolo HTTPS ou se um ouvinte do Network Load Balancer não estiver configurado para usar o protocolo TLS.

Para criptografar dados transmitidos entre um cliente e um balanceador de carga, os ouvintes do Elastic Load Balancer devem ser configurados para usar protocolos de segurança padrão do setor: HTTPS para Application Load Balancers ou TLS para Network Load Balancers. Caso contrário, os dados transmitidos entre um cliente e um balanceador de carga ficam vulneráveis à interceptação, adulteração e acesso não autorizado. O uso de HTTPS ou TLS por um ouvinte se alinha às melhores práticas de segurança e ajuda a garantir a confidencialidade e a integridade

dos dados durante a transmissão. Isso é particularmente importante para aplicativos que lidam com informações confidenciais ou precisam estar em conformidade com padrões de segurança que exigem criptografia de dados em trânsito.

Correção

Para obter informações sobre como configurar protocolos de segurança para ouvintes, consulte as seguintes seções dos Guias do Usuário do Elastic Load Balancing: Crie um ouvinte HTTPS para seu Application Load Balancer e Crie um ouvinte para seu Network Load Balancer.

Security Hub para Elasticsearch

Esses AWS Security Hub controles avaliam o serviço e os recursos do Elasticsearch.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[ES.1] Os domínios do Elasticsearch devem ter a criptografia em repouso habilitada.

Requisitos relacionados: PCI DSS v3.2.1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regra do AWS Config : `elasticsearch-encrypted-at-rest`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os domínios do Elasticsearch 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, como `t.small` e `t.medium`, 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 v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),, (11), (16), (20), (21), (3), (4), (9) NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura > Recursos na VPC

Severidade: crítica

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regra do AWS Config : `elasticsearch-in-vpc-only`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os domínios do Elasticsearch 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 Elasticsearch 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 Guia 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. VPCs forneça 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 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.

[ES.3] Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

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 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 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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7, NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar – Registro em log

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

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 aos 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.

[ES.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

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.

[ES.6] Os domínios do Elasticsearch devem ter pelo menos três nós de dados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

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.

[ES.7] 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

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 indicará falha se o domínio não usar nós primários dedicados. Esse controle indicará sucesso se os domínios do Elasticsearch tiverem cinco nós primários dedicados. Porém, usar 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 garantir alta disponibilidade e tolerância a falhas. Os recursos dedicados do nó primário podem ser sobrecarregados durante blue/green as implantações dos nós de dados porque há nós adicionais para gerenciar. A implantação de um domínio do Elasticsearch com pelo menos três nós primários dedicados garante suficiente capacidade de recursos dos nós primários e operações do 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-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regra AWS Config : `elasticsearch-https-required` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica 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 HTTPs não estiver habilitado. A política de segurança TLS mais recente compatível atualmente é a `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 habilitar a criptografia TLS, use a operação da API UpdateDomainConfig para configurar o objeto DomainEndpointOptions. Isso define a `TLSSecurityPolicy`.

[ES.9] Os domínios do Elasticsearch devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regra AWS Config : `tagged-elasticsearch-domain` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o domínio não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política

de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 domínio do Elasticsearch, consulte Como trabalhar com tags no Amazon OpenSearch Service Developer Guide.

Controles do Security Hub para o Amazon EMR

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon EMR (anteriormente chamado de Amazon Elastic MapReduce). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4, 1, (7), (21),, (11), (16), (20)), (21), (3), (4), (9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::EMR::Cluster`

AWS Config regra: 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

Durante a execução, você pode controlar se sua instância em uma sub-rede padrão ou não padrão recebe um endereço público IPv4 . Por padrão, as sub-redes padrão têm esse atributo definido como `true`. As sub-redes não padrão têm o atributo de endereçamento IPv4 público definido como`false`, a menos que tenham sido criadas pelo assistente de instância de EC2 inicialização da Amazon. Nesse caso, o atributo é definido como `true`.

Após o lançamento, você não pode desassociar manualmente um IPv4 endereço público da sua instância.

Para corrigir uma falha na descoberta, você deve iniciar um novo cluster em uma VPC com uma sub-rede privada que tenha IPv4 o atributo de endereçamento público definido como. `false` Para obter instruções, consulte Executar clusters 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: PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21) NIST.800-53.r5 AC-4,,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, 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), (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS:::Account`

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 abre portas para os endereços IP públicos IPv4 0.0.0.0/0 ou IPv6 : :/0, e essas portas não forem especificadas como exceções para sua 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.

[EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), 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: `AWS::EMR::SecurityConfiguration`

Regra do AWS Config : emr-security-configuration-encryption-rest

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma configuração de segurança do Amazon EMR tem a criptografia em repouso ativada. O controle falhará se a configuração de segurança não habilitar a criptografia em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para habilitar a criptografia em repouso em uma configuração de segurança do Amazon EMR, consulte Configurar criptografia de dados no Guia de gerenciamento do Amazon EMR.

[EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-4, 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 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::EMR::SecurityConfiguration`

Regra do AWS Config : emr-security-configuration-encryption-transit

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma configuração de segurança do Amazon EMR tem a criptografia em trânsito ativada. O controle falhará se a configuração de segurança não habilitar a criptografia em trânsito.

Dados em trânsito se referem a dados que se movem de um local para outro, como entre os nós do cluster ou entre o cluster e a aplicação. Os dados podem se mover pela Internet ou em uma rede privada. Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede.

Correção

Para habilitar a criptografia em trânsito em uma configuração de segurança do Amazon EMR, consulte Configurar criptografia de dados no Guia de gerenciamento do Amazon EMR.

Controles do Security Hub para EventBridge

Esses AWS Security Hub controles avaliam o EventBridge serviço e os recursos da Amazon.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Events::EventBus`

AWS Config regra: `tagged-events-eventbus` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o barramento de eventos não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7),,, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/10.3.1

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: baixa

Tipo de recurso: `AWS::Events::EventBus`

Regra do AWS Config : custom-eventbus-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, você pode 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 Usando políticas baseadas em recursos para a Amazon no Guia EventBridge do usuário da Amazon. EventBridge

[EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Events::Endpoint`

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, você pode 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 Security Hub para o Amazon Fraud Detector

Esses controles do Security Hub avaliam o serviço e os recursos do Amazon Fraud Detector.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FraudDetector::EntityType`

Regra do AWS Config : `frauddetector-entity-type-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um tipo de entidade do Amazon Fraud Detector tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o tipo de entidade não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o tipo de entidade não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags

às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um tipo de entidade do Amazon Fraud Detector (console)

1. Abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação, escolha Entidades.
3. Selecione um tipo de entidade na lista.
4. Na seção tags de tipo de entidade, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FraudDetector::Label`

Regra do AWS Config : `frauddetector-label-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma etiqueta do Amazon Fraud Detector tem etiquetas com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o rótulo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o rótulo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS,

inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma etiqueta do Amazon Fraud Detector (console)

1. Abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação, escolha Rótulos.
3. Selecione um rótulo na lista.
4. Na seção etiquetas de etiquetas, escolha Gerenciar etiquetas.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FraudDetector::Outcome`

Regra do AWS Config : `frauddetector-outcome-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

Esse controle verifica se um resultado do Amazon Fraud Detector tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o resultado não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o resultado não for marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um resultado do Amazon Fraud Detector (console)

1. Abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação, escolha Resultados.
3. Selecione um resultado na lista.
4. Na seção tags de resultados, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FraudDetector::Variable`

Regra do AWS Config : `frauddetector-variable-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma variável do Amazon Fraud Detector tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a variável não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a variável não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma variável do Amazon Fraud Detector (console)

1. Abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação, escolha Variáveis.
3. Selecione uma variável na lista.
4. Na seção tags de variáveis, escolha Gerenciar tags.

5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares de chave-valor adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

Controles do Security Hub para Amazon FSx

Esses AWS Security Hub controles avaliam o FSx serviço e os recursos da Amazon. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FSx::FileSystem`

Regra do AWS Config : fsx-openzfs-copy-tags-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um sistema de arquivos Amazon FSx for 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 obter informações sobre como configurar um sistema de arquivos FSx para OpenZFS para copiar tags para backups e volumes, consulte Atualizando um sistema de arquivos no Guia do usuário do Amazon FSx for OpenZFS.

[FSx.2] FSx para sistemas de arquivos 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::FSx::FileSystem`

Regra do AWS Config : fsx-lustre-copy-tags-to-backups

Tipo de programação: Periódico

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 obter informações sobre como configurar um FSx sistema de arquivos for Lustre para copiar tags para backups, consulte Como copiar backups dentro do mesmo Conta da AWS no Guia do usuário do Amazon FSx for Lustre.

[FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::FSx::FileSystem`

Regra do AWS Config : fsx-openzfs-deployment-type-check

Tipo de programação: Periódico

Parâmetros: `deploymentTypes: MULTI_AZ_1` (não personalizável)

Esse controle verifica se um sistema de arquivos Amazon FSx for OpenZFS está configurado para usar o tipo de implantação de várias zonas de disponibilidade (Multi-AZ). O controle falhará se o sistema de arquivos não estiver configurado para usar o tipo de implantação Multi-AZ.

O Amazon FSx for OpenZFS oferece suporte a vários tipos de implantação para sistemas de arquivos: Multi-AZ (HA), Single-AZ (HA) e Single-AZ (não HA). Os tipos de implantação oferecem diferentes níveis de disponibilidade e durabilidade. Os sistemas de arquivos Multi-AZ (HA) são compostos por um par de servidores de arquivos de alta disponibilidade (HA) distribuídos em duas zonas de disponibilidade ()AZs. Recomendamos usar o tipo de implantação Multi-AZ (HA) para a maioria das cargas de trabalho de produção devido ao modelo de alta disponibilidade e durabilidade que ele fornece.

Correção

Você pode configurar um sistema de arquivos Amazon FSx for OpenZFS para usar o tipo de implantação Multi-AZ ao criar o sistema de arquivos. Você não pode alterar o tipo de implantação de um sistema de arquivos existente FSx para OpenZFS.

Para obter informações sobre tipos e opções de implantação FSx para sistemas de arquivos OpenZFS, consulte Disponibilidade e durabilidade do Amazon FSx para OpenZFS e Gerenciamento de recursos do sistema de arquivos no Guia do usuário do Amazon FSx for OpenZFS.

[FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::FSx::FileSystem`

Regra do AWS Config : fsx-ontap-deployment-type-check

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`deploymentTypes`	Uma lista dos tipos de implantação a serem incluídos na avaliação. O controle gera uma `FAILED` descoberta se um sistema de arquivos não estiver configurado para usar um tipo de implantação especificado na lista.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Esse controle verifica se um sistema de arquivos Amazon FSx for NetApp ONTAP está configurado para usar um tipo de implantação de várias zonas de disponibilidade (Multi-AZ). O controle falhará se o sistema de arquivos não estiver configurado para usar um tipo de implantação Multi-AZ. Opcionalmente, você pode especificar uma lista de tipos de implantação para incluir na avaliação.

O Amazon FSx for NetApp ONTAP oferece suporte a vários tipos de implantação para sistemas de arquivos: Single-AZ 1, Single-AZ 2, Multi-AZ 1 e Multi-AZ 2. Os tipos de implantação oferecem diferentes níveis de disponibilidade e durabilidade. Recomendamos usar um tipo de implantação Multi-AZ para a maioria das cargas de trabalho de produção devido ao modelo de alta disponibilidade e durabilidade que os tipos de implantação Multi-AZ oferecem. Os sistemas de arquivos multi-AZ oferecem suporte a todos os recursos de disponibilidade e durabilidade dos sistemas de arquivos single-AZ. Além disso, eles foram projetados para fornecer disponibilidade contínua aos dados, mesmo quando uma zona de disponibilidade (AZ) não está disponível.

Correção

Você não pode alterar o tipo de implantação de um sistema de arquivos Amazon FSx for NetApp ONTAP existente. No entanto, você pode fazer backup dos dados e restaurá-los em um novo sistema de arquivos que usa um tipo de implantação Multi-AZ.

Para obter informações sobre os tipos e opções de implantação dos sistemas de arquivos ONTAP, consulte Disponibilidade, durabilidade e opções de implantação e Gerenciamento de sistemas de arquivos no Guia do FSx usuário do ONTAP. FSx

[FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::FSx::FileSystem`

Regra do AWS Config : fsx-windows-deployment-type-check

Tipo de programação: Periódico

Parâmetros: `deploymentTypes: MULTI_AZ_1` (não personalizável)

Esse controle verifica se um sistema de arquivos do Amazon FSx para Windows File Server está configurado para usar o tipo de implantação de várias zonas de disponibilidade (Multi-AZ). O controle falhará se o sistema de arquivos não estiver configurado para usar o tipo de implantação Multi-AZ.

O Amazon FSx para Windows File Server oferece suporte a dois tipos de implantação para sistemas de arquivos: Single-AZ e Multi-AZ. Os tipos de implantação oferecem diferentes níveis de disponibilidade e durabilidade. Os sistemas de arquivos single-AZ são compostos por uma única instância do servidor de arquivos do Windows e um conjunto de volumes de armazenamento em uma única zona de disponibilidade (AZ). Os sistemas de arquivos Multi-AZ são compostos por um cluster de alta disponibilidade de servidores de arquivos Windows distribuídos em duas zonas de disponibilidade. Recomendamos usar o tipo de implantação Multi-AZ para a maioria das cargas de trabalho de produção devido ao modelo de alta disponibilidade e durabilidade que ele fornece.

Correção

Você pode configurar um sistema de arquivos Amazon FSx para Windows File Server para usar o tipo de implantação Multi-AZ ao criar o sistema de arquivos. Você não pode alterar o tipo de implantação de um sistema de arquivos existente FSx para Windows File Server.

Para obter informações sobre os tipos de implantação e as opções de sistemas de arquivos do Windows File Server, consulte Disponibilidade e durabilidade: sistemas de arquivos Single-AZ e Multi-AZ e Introdução ao Amazon FSx para Windows File Server no Guia do usuário do Amazon FSx para Windows File Server. FSx

Controles do Security Hub para o Global Accelerator

Esses AWS Security Hub controles avaliam o AWS Global Accelerator serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::GlobalAccelerator::Accelerator`

Regra AWS Config : `tagged-globalaccelerator-accelerator` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 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 acelerador não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 acelerador global do Global Accelerator, consulte Tagging in AWS Global Accelerator no AWS Global Accelerator Developer Guide.

Controles do Security Hub para AWS Glue

Esses AWS Security Hub controles avaliam o AWS Glue serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

Os AWS Glue trabalhos [Glue.1] devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Glue::Job`

Regra AWS Config : `tagged-glue-job` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se o trabalho não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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.

[Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::Glue::MLTransform`

Regra do AWS Config : glue-ml-transform-encrypted-at-rest

Tipo de programação: acionado por alterações

Parâmetros: não

Esse controle verifica se uma transformação AWS Glue de aprendizado de máquina está criptografada em repouso. Esse controle falhará se a transformação de machine learning não for criptografada em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para configurar a criptografia para transformações AWS Glue de aprendizado de máquina, consulte Como trabalhar com transformações de aprendizado de máquina no Guia do AWS Glue usuário.

[Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-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: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::Glue::Job`

Regra do AWS Config : glue-spark-job-supported-version

Tipo de programação: acionado por alterações

Parâmetros:`minimumSupportedGlueVersion`: `3.0` (não personalizável)

Esse controle verifica se uma AWS Glue tarefa do Spark está configurada para ser executada em uma versão compatível do AWS Glue. O controle falhará se a tarefa do Spark estiver configurada para ser executada em uma versão anterior à versão mínima suportada. AWS Glue

> **Note**
>
> Esse controle também gera uma `FAILED` descoberta AWS Glue para uma tarefa do Spark se a propriedade AWS Glue version (`GlueVersion`) não existir ou for nula no item de configuração (CI) da tarefa. Nesses casos, a descoberta inclui a seguinte anotação:. `GlueVersion is null or missing in glueetl job configuration` Para resolver esse tipo de `FAILED` descoberta, adicione a `GlueVersion` propriedade à configuração do trabalho. Para obter uma lista das versões compatíveis e dos ambientes de execução, consulte AWS Glue Versões no Guia AWS Glue do usuário.

A execução de trabalhos do AWS Glue Spark nas versões atuais do AWS Glue pode otimizar o desempenho, a segurança e o acesso aos recursos mais recentes do AWS Glue. Também pode ajudar na proteção contra vulnerabilidades de segurança. Por exemplo, uma nova versão pode ser lançada para fornecer atualizações de segurança, solucionar problemas ou introduzir novos recursos.

Correção

Para obter informações sobre como migrar uma tarefa do Spark para uma versão compatível do AWS Glue, consulte Migração AWS Glue para tarefas do Spark no Guia do usuário.AWS Glue

Controles do Security Hub para a Amazon GuardDuty

Esses AWS Security Hub controles do avaliam o GuardDuty serviço e os recursos da Amazon. Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[GuardDuty.1] GuardDuty deve ser ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), 1 (1), 1 (6) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, 5 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (2), 5 (8), (19), (25), (NIST.800-53.r5 SA-11), (3), NIST.800-53.r5 SA-1 NISt.800-53.r5 SI-20, NIST.800-53.r5 SA-1 NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SA-1 NIST.800-53.R5 SI-4, NIST.800-53.r5 SA-8 NISt.800-53.R5 SI-4, NIST.800-53.r5 SA-8 NISt.800-53.R5 SI-4, NIST.800-53.r5 SA-8 NISt.800-53.R5 SI-4 NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5 NISt.800-53.R5 SI-4, NISt.800-53.R5 SI-4, NISt.800-53.R5 SI-4, NISt.800-53.R5 SI-4, NISt.800-53.R5 SI-4, NISt.800-53.R5 800-53.R5 SI-4 NIST.800-53.r5 SC-5 (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), NIST.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/11.4 , PCI DSS v4.0.1/11.5.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::Account`

Regra do AWS Config : guardduty-enabled-centralized

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Amazon GuardDuty está habilitada na GuardDuty conta e na região.

É altamente recomendável que você ative GuardDuty em todas as AWS regiões da compatíveis. Isso permite GuardDuty gerar descobertas sobre atividades incomuns ou não autorizadas, mesmo em regiões que você não usa ativamente. Isso também permite GuardDuty monitorar CloudTrail eventos para globais Serviços da AWS , como o IAM.

Correção

Para habilitar GuardDuty, consulte Introdução GuardDuty no Guia do GuardDuty usuário da Amazon.

[GuardDuty.2] GuardDuty os filtros devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::GuardDuty::Filter`

Regra AWS Config : `tagged-guardduty-filter` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um GuardDuty volume 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 verificará apenas a existência de uma chave de tag e falhará se o filtro não estiver marcado com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, incluindo o 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] GuardDuty IPSets deve ser marcado

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::GuardDuty::IPSet`

Regra AWS Config : `tagged-guardduty-ipset` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma Amazon GuardDuty IPSet tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se 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 verificará apenas a existência de uma chave de tag e falhará se IPSet não estiver marcado com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, incluindo o 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra AWS Config : `tagged-guardduty-detector` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um GuardDuty detector 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 de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS,

incluindo o 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.

[GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-eks-protection-audit-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o Monitoramento de Logs de Auditoria do GuardDuty EKS está habilitado. Para uma conta autônoma, o controle falhará se o Monitoramento de Logs de Auditoria do GuardDuty EKS estiver desabilitado na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem o Monitoramento de Logs de Auditoria do EKS ativado.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Monitoramento de Logs de Auditoria do EKS nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha o Monitoramento de Logs de Auditoria do GuardDuty EKS ativado. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

GuardDuty O Monitoramento de logs de auditoria do EKS ajuda você a detectar atividades potencialmente suspeitas em seus clusters do Amazon Elastic Kubernetes Service (Amazon EKS). O Monitoramento de logs de auditoria do EKS usa registros de auditoria do Kubernetes para

capturar atividades cronológicas de usuários e aplicações usando a API Kubernetes e o ambiente de gerenciamento.

Correção

Para habilitar o GuardDuty Monitoramento de Logs de Auditoria do EKS, consulte EKS Audit Log Monitoring no Amazon GuardDuty User Guide.

[GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-lambda-protection-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Proteção do GuardDuty Lambda está habilitada. Para uma conta autônoma, o controle falhará se a Proteção do GuardDuty Lambda estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem a Proteção do Lambda do Guardda habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Proteção do Lambda do GuardDuty nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha a Proteção do GuardDuty Lambda do Guardda habilitada. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

GuardDuty A Proteção do Lambda ajuda você a identificar possíveis ameaças à segurança quando uma AWS Lambda função do é invocada. Depois que você habilita a Proteção do Lambda, GuardDuty começa a monitorar os logs de atividades da rede do Lambda associados às funções do Lambda no seu. Conta da AWS Quando uma função do Lambda é invocada e GuardDuty identifica tráfego de rede suspeito que indica a presença de um código potencialmente mal-intencionado em sua função do Lambda, gera uma descoberta. GuardDuty

Correção

Para habilitar a Proteção GuardDuty Lambda, consulte Configuração da Proteção Lambda no Guia do Usuário da Amazon. GuardDuty

[GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-eks-protection-runtime-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o Monitoramento de Runtime do GuardDuty EKS com gerenciamento automatizado de agentes está habilitado. Para uma conta autônoma, o controle falhará se o Monitoramento de Runtime do GuardDuty EKS com gerenciamento automatizado de agentes estiver desabilitado na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem o Monitoramento de Runtime do EKS com Gerenciamento Automatizado de Agentes habilitado.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Monitoramento de Runtime do EKS do GuardDuty com gerenciamento automatizado de agentes nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha o Monitoramento de Runtime do GuardDuty EKS ativado. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

A Proteção do EKS na Amazon GuardDuty fornece cobertura de detecção de ameaças para ajudar você a proteger clusters do Amazon EKS no seu AWS ambiente da. O Monitoramento de Runtime do EKS usa eventos ao nível do sistema operacional para ajudar a detectar possíveis ameaças nos nós e contêineres do EKS em seus clusters do EKS.

Correção

Para habilitar o Monitoramento de Runtime do EKS com Gerenciamento Automatizado de Agentes, consulte GuardDuty Enabling Runtime Monitoring no Amazon GuardDuty User Guide.

[GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-malware-protection-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Proteção contra GuardDuty Malware está habilitada. Para uma conta autônoma, o controle falhará se a Proteção contra GuardDuty Malware estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem a Proteção contra Malware habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Proteção contra Malware nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha a Proteção contra GuardDuty Malware habilitada. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

GuardDuty A Proteção contra malware EC2 ajuda você a detectar a presença de malware ao examinar os volumes do Amazon Elastic Block Store (Amazon EBS) que são anexados às instâncias do Amazon Elastic Compute Cloud (EC2Amazon) e workloads de contêiner. A Proteção contra malware fornece opções de verificação nas quais você pode decidir se deseja incluir ou excluir EC2 instâncias específicas e workloads de contêineres no momento da verificação. Ela também oferece a opção de reter os snapshots dos volumes do EBS anexados às EC2 instâncias ou às workloads de contêineres em suas contas. GuardDuty Os snapshots são retidos somente quando o malware é encontrado e as descobertas da Proteção contra malware são geradas.

Correção

Para ativar a proteção contra GuardDuty malware EC2, consulte Configuração da verificação de GuardDuty malware iniciada no Guia GuardDuty do usuário da Amazon.

[GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-rds-protection-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Proteção GuardDuty do RDS está habilitada. Para uma conta autônoma, o controle falhará se a Proteção do GuardDuty RDS estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem a Proteção do RDS habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Proteção do RDS nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha a Proteção do GuardDuty RDS habilitada. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

A proteção do RDS em GuardDuty analisa e traça o perfil da atividade de login do RDS em busca de possíveis ameaças de acesso aos seus bancos de dados Amazon Aurora (Aurora MySQL-Compatible Edition) e Aurora PostgreSQL-Compatible Edition). Esse recurso permite identificar comportamentos de login potencialmente suspeitos. A Proteção do RDS não requer infraestrutura adicional. Ela foi projetada para não afetar a performance de suas instâncias de banco de dados. Quando a Proteção do RDS do GuardD's detecta uma ameaça em potencial, GuardDuty gera uma nova descoberta com detalhes sobre o banco de dados possivelmente comprometido.

Correção

Para ativar a Proteção GuardDuty do RDS, consulte a Proteção GuardDuty do RDS no Guia GuardDuty do Usuário da Amazon.

[GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-s3-protection-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Proteção GuardDuty do S3 está habilitada. Para uma conta autônoma, o controle falhará se a Proteção do GuardDuty S3 estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de GuardDuty administrador delegado e todas as contas-membro não tiverem a Proteção do S3 habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de GuardDuty administrador delegado. Apenas o administrador delegado pode habilitar ou desabilitar o atributo Proteção do S3 nas contas-membro da organização. GuardDuty As contas-membro não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o GuardDuty administrador delegado tiver uma conta-membro suspensa que não tenha a Proteção do GuardDuty S3 habilitada. Para receber uma `PASSED` descoberta, o administrador delegado deve desassociar essas contas suspensas em. GuardDuty

A Proteção do S3 permite GuardDuty monitorar operações de API por objeto para identificar possíveis riscos de segurança para dados em seus buckets do Amazon Storage Service (Amazon S3). GuardDuty monitora ameaças contra seus recursos do S3 analisando os eventos AWS CloudTrail de gerenciamento do e os eventos de dados CloudTrail do S3.

Correção

Para ativar a Proteção do GuardDuty S3, consulte a Proteção do Amazon S3 na GuardDuty Amazon no Guia do Usuário da GuardDuty Amazon.

[GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-runtime-monitoring-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o Monitoramento de Runtime está habilitado na Amazon GuardDuty. Para uma conta autônoma, o controle falhará se o Monitoramento GuardDuty de Runtime estiver desabilitado para a conta. Em um ambiente com várias contas, o controle falhará se o Monitoramento GuardDuty de Runtime estiver desabilitado para a conta de GuardDuty administrador delegado e todas as contas-membro.

Em um ambiente com várias contas, somente o GuardDuty administrador delegado pode habilitar ou desabilitar o Monitoramento GuardDuty de Runtime para contas em sua organização. Além disso, somente o GuardDuty administrador pode configurar e gerenciar os agentes de segurança GuardDuty usados para monitorar o tempo de execução das AWS cargas de trabalho e dos recursos das contas na organização. GuardDuty as contas dos membros não podem ativar, configurar ou desativar o Runtime Monitoring para suas próprias contas.

GuardDuty O monitoramento de runtime observa e analisa eventos em nível de sistema operacional, rede e arquivos para ajudar você a detectar possíveis ameaças em AWS workloads do específicas do seu ambiente. Ele usa agentes GuardDuty de segurança que adicionam visibilidade ao comportamento de runtime, como acesso a arquivos, execução de processos, argumentos de linha de comando e conexões de rede. Você pode habilitar e gerenciar o agente de segurança para cada tipo de recurso que você deseja monitorar para possíveis ameaças, como clusters do Amazon EKS e EC2 instâncias da Amazon.

Correção

Para obter informações sobre como configurar e ativar o monitoramento em GuardDuty tempo de execução, consulte Monitoramento GuardDuty de tempo de execução e ativação do monitoramento em GuardDuty tempo de execução no Guia GuardDuty do usuário da Amazon.

[GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-ecs-protection-runtime-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o agente de segurança GuardDuty automatizado da Amazon está habilitado para o monitoramento em tempo de execução dos clusters do Amazon ECS em AWS Fargate. Para uma conta autônoma, o controle falhará se o Security Agent estiver desabilitado para a conta. Em um ambiente com várias contas, o controle falhará se o agente de segurança estiver desabilitado para a conta de GuardDuty administrador delegado e todas as contas-membro.

Em um ambiente com várias contas, esse controle gera descobertas somente na conta de GuardDuty administrador delegado. Isso ocorre porque somente o GuardDuty administrador delegado pode ativar ou desativar o monitoramento de tempo de execução dos recursos do ECS-Fargate para contas em sua organização. GuardDuty As contas-membro não podem fazer isso com suas próprias contas. Além disso, esse controle gera `FAILED` descobertas se GuardDuty for suspenso para uma conta de membro e o monitoramento de tempo de execução dos recursos do ECS-Fargate estiver desativado para a conta do membro. Para receber uma `PASSED` descoberta, o GuardDuty administrador deve desassociar a conta de membro suspensa de sua conta de administrador usando GuardDuty.

GuardDuty O monitoramento de runtime observa e analisa eventos em nível de sistema operacional, rede e arquivos para ajudar você a detectar possíveis ameaças em AWS workloads do específicas do seu ambiente. Ele usa agentes GuardDuty de segurança que adicionam visibilidade ao comportamento de runtime, como acesso a arquivos, execução de processos, argumentos de linha de comando e conexões de rede. Você pode habilitar e gerenciar o agente de segurança do para cada tipo de recurso que deseja monitorar para possíveis ameaças. Isso inclui clusters do Amazon ECS ativados. AWS Fargate

Correção

Para habilitar e gerenciar o agente de segurança para monitoramento GuardDuty de tempo de execução dos recursos do ECS-Fargate, você deve usá-lo diretamente. GuardDuty Você não pode

habilitá-lo ou gerenciá-lo manualmente para recursos do ECS-Fargate. Para obter informações sobre como habilitar e gerenciar o agente de segurança, consulte Pré-requisitos para suporte (somente para AWS Fargate Amazon ECS) e Gerenciamento do agente de segurança automatizado para (somente AWS Fargate Amazon ECS) no Guia do usuário da Amazon. GuardDuty

[GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso: `AWS::GuardDuty::Detector`

Regra do AWS Config : guardduty-ec2-protection-runtime-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o agente de segurança GuardDuty automatizado da Amazon está habilitado para o monitoramento em tempo de execução das EC2 instâncias da Amazon. Para uma conta autônoma, o controle falhará se o Security Agent estiver desabilitado para a conta. Em um ambiente com várias contas, o controle falhará se o agente de segurança estiver desabilitado para a conta de GuardDuty administrador delegado e todas as contas-membro.

Em um ambiente com várias contas, esse controle gera descobertas somente na conta de GuardDuty administrador delegado. Isso ocorre porque somente o GuardDuty administrador delegado pode ativar ou desativar o monitoramento de tempo de execução de EC2 instâncias da Amazon para contas em sua organização. GuardDuty As contas-membro não podem fazer isso com suas próprias contas. Além disso, esse controle gera `FAILED` descobertas se GuardDuty for suspenso para uma conta de membro e o monitoramento de tempo de execução de EC2 instâncias for desativado para a conta de membro. Para receber uma `PASSED` descoberta, o GuardDuty administrador deve desassociar a conta de membro suspensa de sua conta de administrador usando GuardDuty.

GuardDuty O monitoramento de runtime observa e analisa eventos em nível de sistema operacional, rede e arquivos para ajudar você a detectar possíveis ameaças em AWS workloads do específicas do seu ambiente. Ele usa agentes GuardDuty de segurança que adicionam visibilidade ao comportamento de runtime, como acesso a arquivos, execução de processos, argumentos de linha de comando e conexões de rede. Você pode habilitar e gerenciar o agente de segurança do para

cada tipo de recurso que deseja monitorar para possíveis ameaças. Isso inclui EC2 instâncias da Amazon.

Correção

Para obter informações sobre como configurar e gerenciar o agente de segurança automatizado para monitoramento em tempo de GuardDuty execução de EC2 instâncias, consulte Pré-requisitos para suporte a instâncias da EC2 Amazon e Habilitação do agente de segurança automatizado para instâncias da EC2 Amazon no Guia do usuário da Amazon GuardDuty .

Controles do Security Hub para AWS Identity and Access Management

Esses AWS Security Hub controles avaliam o serviço e os recursos AWS Identity and Access Management (IAM). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.22, CIS AWS Foundations Benchmark v1.4.0/1.16,, NIST.800-53.r5 AC-2 (1),, (15), (7),, NIST.800-53.r5 AC-2, (10), (2) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (3), NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.4 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI NIST.800-53.r5 AC-6 DSS v3.2.1/7.2.1 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso: `AWS::IAM::Policy`

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 IAM definem um conjunto de privilégios concedidos a usuários, grupos ou perfis. 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. No entanto, 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 IAM não devem ter políticas do IAM anexadas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.15, AWS CIS Foundations Benchmark v1.2.0/1.16,, NIST.800-53.r5 AC-2 (1),, (15), (7),, (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-2, NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.7, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.3.9 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.13.3, PCI DSS v3.2.1/7.2.1

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS::IAM::User`

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**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. No entanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar os recursos globais somente em uma região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registrar os recursos globais.

Correção

Para resolver esse problema, crie um grupo do IAM e anexe a política ao grupo. Depois, 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, (1), (3), (15), PCI DSS AWS v4.0.1/8.3.9, PCI DSS v4.0.1/8.6.3 NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::User`

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 IAM. 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 Security Hub 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 AWS CLI partir do Tools for Windows PowerShell, do 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. No entanto, 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 IAM 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, AWS PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/2.2, PCI DSS v3.2.1/7.2.1, (1), (15), (7), (10), (2) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso: `AWS::::Account`

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 presente.

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 Security Hub 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, (1), (15), NIST.800-53.r5 AC-2 (1), (2), (6), (8), AWS NIST.800-53.r5 AC-3 PCI DSS v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::User`

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 do 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. No entanto, 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 aidiconar MPA a usuários do IAM, 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, AWS PCI DSS v3.2.1/8.3.1, (1), (15), (1), (2), (6), NIST.800-53.r5 AC-2 (8), PCI DSS v4.0.1/8.4.2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso: `AWS:::Account`

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 de hardware não estiver habilitada ou se os dispositivos virtuais de MFA tiverem 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 que você use um dispositivo de MFA virtual somente enquanto aguarda a aprovação da compra do hardware ou a chegada do hardware. Para saber mais, consulte Atribuir um dispositivo de MFA virtual (console) no Guia do usuário do IAM.

> **Note**
>
> O Security Hub avalia esse controle com base na presença das credenciais do usuário raiz (perfil de login) em um. Conta da AWS O controle gera descobertas `PASSED` nos seguintes casos:
>
> - As credenciais do usuário raiz estão presentes na conta e o MFA de hardware está habilitado para o usuário raiz.
> - As credenciais do usuário root não estão presentes na conta.
>
> O controle gera uma `FAILED` descoberta se as credenciais do usuário raiz estiverem presentes na conta e a MFA de hardware não estiver habilitada para o usuário raiz.

Correção

Para obter informações sobre como habilitar a MFA de hardware para o usuário raiz, consulte Autenticação multifator Usuário raiz da conta da AWS no Guia do usuário do IAM.

Estamos oferecendo uma chave de segurança de MFA gratuita para clientes qualificados. Para determinar se você está qualificado, consulte o Programa de Chave de Segurança da MFA. FAQs

[IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (3), (15), NIST.800-53.r5 AC-2 (1), NIST.800-171.r2 3.5.2, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.9, PCI PCI DSS v4.0.1/8.3.10.1, PCI DSS v4.0.1/8.6.3 NIST.800-53.r5 IA-5

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::::Account`

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros:

Parameter	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 o Guia do usuário do AWS IAM Identity Center .

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. 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.

[IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.3,, NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2, (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-2 NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 PCI DSS v3.2.1/8.1.4 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.2.6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::User`

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.

O Security Hub 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. No entanto, 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 usuário sem atividade por 90 dias ou mais. Você pode 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.9] A MFA deve estar habilitada para o usuário raiz

Requisitos relacionados: PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, 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, (1), (15), (1), (2), (6), (AWS 8) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso: `AWS:::::Account`

Regra do AWS Config : `root-account-mfa-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a autenticação multifator (MFA) está habilitada para que o usuário raiz do IAM de Conta da AWS an faça login no. AWS Management Console O controle falhará se o MFA não estiver habilitado para o usuário raiz da conta.

O usuário raiz do IAM de an Conta da AWS tem acesso completo a todos os serviços e recursos da conta. Se o MFA estiver ativado, o usuário deverá inserir um nome de usuário, uma senha e um código de autenticação do dispositivo de AWS MFA para entrar no. AWS Management Console O MFA adiciona uma camada extra de proteção além do nome de usuário e senha.

Esse controle gera `PASSED` descobertas nos seguintes casos:

- As credenciais do usuário raiz estão presentes na conta e o MFA está ativado para o usuário raiz.
- As credenciais do usuário root não estão presentes na conta.

O controle gera `FAILED` descobertas se as credenciais do usuário raiz estiverem presentes na conta e o MFA não estiver habilitado para o usuário raiz.

Correção

Para obter informações sobre como habilitar o MFA para o usuário raiz de um Conta da AWS, consulte Autenticação multifator Usuário raiz da conta da AWS no Guia do usuário.AWS Identity and Access Management

[IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes

Requisitos relacionados: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, 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: `AWS::::Account`

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.

- `RequireUppercaseCharacters`: exige pelo menos um caractere maiúsculo na senha. (Padrão = `true`)
- `RequireLowercaseCharacters`: exige pelo menos um caractere minúsculo na senha. (Padrão = `true`)
- `RequireNumbers`: exige pelo menos um número na senha. (Padrão = `true`)
- `MinimumPasswordLength`: tamanho mínimo da senha. (Padrão = 7 ou mais)
- `PasswordReusePrevention`: número de senhas antes de permitir a reutilização. (Padrão = 4)
- `MaxPasswordAge`— Número de dias antes da expiração da senha. (Padrão = 0)

> **Note**
>
> Em 30 de maio de 2025, o Security Hub removeu esse controle do padrão PCI DSS v4.0.1. O PCI DSS v4.0.1 agora exige que as senhas tenham no mínimo 8 caracteres. Esse controle continua sendo aplicado ao padrão PCI DSS v3.2.1, que tem requisitos de senha diferentes. Para avaliar as políticas de senha da conta em relação aos requisitos do PCI DSS v4.0.1, você pode usar o controle IAM.7. Esse controle exige que as senhas tenham no mínimo 8 caracteres. Ele também suporta valores personalizados para o tamanho da senha e outros parâmetros. O controle IAM.7 faz parte do padrão PCI DSS v4.0.1 no Security Hub.

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, NIST.800-171.r2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS:::Account`

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.

O CIS recomenda 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 alterar sua política de senha,, 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 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, NIST.800-171.r2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS:::Account`

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. O CIS recomenda 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 alterar sua política de senha,, 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 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, NIST.800-171.r2 3.5.7

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::::Account`

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.

O CIS recomenda 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 alterar sua política de senha,, 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, NIST.800-171.r2 3.5.7, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.6.3

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS:::Account`

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.

O CIS recomenda 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 alterar sua política de senha,, 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 número.

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, NIST.800-171.r2 3.5.7 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS:::Account`

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 tenham pelo menos um determinado comprimento.

O CIS recomenda 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 alterar sua política de senha,, 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, NIST.800-171.r2 3.5.8, PCI DSS v4.0.1/8.3.7 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS:::Account`

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 IAM podem impedir a reutilização de uma determinada senha pelo mesmo usuário.

O CIS recomenda 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 alterar sua política de senha,, 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, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.10.1

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS::::Account`

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha do IAM podem exigir a mudança ou expiração de senhas após um determinado número de dias.

O CIS recomenda 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 alterar sua política de senha,, 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.17, CIS Foundations Benchmark v1.4.0/1.17, CIS AWS Foundations Benchmark v1.2.0/1.20, NIST.800-171.r2 3.1.2, PCI DSS v4.0.1/12.10.3 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS::::Account`

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 um perfil do IAM para permitir que usuários autorizados gerenciem incidentes com o AWS 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. Suporte

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. No entanto, 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 um perfil para permitir que usuários autorizados gerenciem incidentes do Suporte .

Para criar a função a ser usada para Suporte acesso

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do IAM, escolha Perfis e escolha Criar perfil.
3. Em Tipo de perfil, escolha Outra 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: tags.
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. Escolha 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 do perfil, insira uma descrição para o novo perfil.

13. Revise a função e selecione Create role (Criar função).

[IAM.19] A MFA deve estar habilitada para todos os usuários do IAM

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (15), (1), NIST.800-53.r5 AC-3 (2), (6), NIST.800-53.r5 IA-2 (8), NIST.800-53.r5 IA-2 NIST.800-171.r2 3.3.8, NIST.800-53.r5 IA-2 NIST.800-171.r2 3.5.3, NIST.800-53.r5 IA-2 NIST.800-171.r2 3.5.4, NIST.800-171.r2 3.7.5, PCI DSS v3.2.1/8.3.1, PCI DSS v4.4.0,1/8.4.2,

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::User`

Regra do AWS Config : `iam-user-mfa-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os usuários do IAM têm a autenticação multifator (MFA) habilitada.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. No entanto, 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.

[IAM.20] Evite o uso do usuário raiz

> **Important**
>
> O Security Hub descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM 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: `AWS::IAM::User`

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 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 um status de controle `NO_DATA` se uma ou mais das seguintes afirmações forem verdadeiras:

- Um trilha multirregional é baseada 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 um status de controle `WARNING` se uma ou mais das seguintes afirmações forem 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 usar 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 do 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. Você pode 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 IAM diretamente a grupos e perfis, mas não aos usuários. Para obter instruções sobre como configurar um administrador para uso diário, consulte Criar seu primeiro usuário administrador e grupo de administradores do IAM 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 Amazon SNS 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 de métricas 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. Em Ações, escolha Criar filtro de métrica.
5. Em 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 Nome do filtro, insira um nome para o filtro de métricas.
   b. Em 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 Nome da métrica, insira um nome para a nova métrica. Lembre-se do 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 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 do filtro. Selecione Criar alarme.
10. Em Especificar métrica e condições, faça o seguinte.
    a. Na seção Condições, em Tipo de limite, escolha Estático.
    b. Para Definir a condição de alarme, escolha Maior/igual.
    c. Em Definir o valor do limite, insira **1**.
    d. Escolha Próximo.
11. Em Configurar ações, faça o seguinte:
    a. Em Gatilho do estado do alarme, escolha 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 Enviar notificação para, insira o nome do tópico do SNS que você criou no procedimento anterior.

d. Escolha Próximo.

12. Em Adicionar uma descrição, insira um Nome e uma Descrição para o alarme, como **`CIS-1.1-RootAccountUsage`**. Escolha Próximo.
13. Em Visualizar e criar, revise a configuração do alarme. Escolha Criar alarme.

[IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

Requisitos relacionados: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1),, (15), (7),,, (10) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-3 (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.2, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.5, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.8, Nist.IsT.800-171.r2 3.3.8 800-171.r2 3.3.9, NIST.800-171.r2 3.13.3, NIST.800-171.r2 3.13.4 NIST.800-53.r5 AC-6

Categoria: Detectar > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS::IAM::Policy`

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, você pode desejar permitir ações do IAM com um prefixo semelhante, como `DescribeFlowLogs` e `DescribeAvailabilityZones`. Nesses casos autorizados, você pode 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 aprovada.

```
"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. No entanto, 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 Editar políticas do IAM no Guia do usuário do IAM.

[IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas

Requisitos relacionados: CIS Foundations Benchmark v3.0.0/1.12, CIS AWS Foundations Benchmark v1.4.0/1.12, NIST.800-171.r2 3.1.2 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::User`

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 45 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.

O CIS recomenda que você remova ou desative todas as credenciais que não foram usadas em 45 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 IAM 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. No entanto, 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. Você pode 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AccessAnalyzer::Analyzer`

AWS Config regra: `tagged-accessanalyzer-analyzer` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o analisador não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 analisador, consulteTagResource na AWS IAM Access Analyzer API Reference.

[IAM.24] Os perfis do IAM devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IAM::Role`

AWS Config regra: `tagged-iam-role` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

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 o perfil 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 perfil não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 perfil do IAM, consulte Tags para recursos do IAM no Guia do usuário do IAM.

[IAM.25] Os usuários do IAM devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IAM::User`

AWS Config regra: `tagged-iam-user` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o usuário não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 usuário do IAM, consulte Tags para recursos do IAM no Guia do usuário do IAM.

[IAM.26] SSL/TLS Certificados 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::IAM::ServerCertificate`

AWS Config regra: **`iam-server-certificate-expiration-check`**

Tipo de programação: Periódico

Parâmetros: nenhum

Isso controla se um certificado de SSL/TLS servidor ativo gerenciado no IAM expirou. O controle falhará se o certificado expirado SSL/TLS do servidor não for removido.

Para habilitar conexões HTTPS com seu site ou aplicativo em AWS, você precisa de um certificado de SSL/TLS servidor. 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 carregar um certificado do ACM no IAM. Além disso, não pode gerenciar certificados no console do IAM. A remoção de SSL/TLS certificados 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 Gerenciar certificados de servidor no IAM no Guia do usuário do IAM.

[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.22

Categoria: Proteger > Gerenciamento de acesso seguro > políticas do IAM seguras

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/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/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 política `AWSCloudShellFullAccess`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 desanexar a política `AWSCloudShellFullAccess` 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 ser habilitado

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::AccessAnalyzer::Analyzer`

AWS Config regra: **`iam-external-access-analyzer-enabled`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um Conta da AWS analisador de acesso externo do IAM Access Analyzer está ativado. O controle falhará se a conta não tiver um analisador de acesso externo habilitado na Região da AWS atualmente selecionada.

Os analisadores de acesso externo do IAM Access Analyzer ajudam a identificar recursos, como buckets do Amazon Simple Storage Service (Amazon S3) ou funções do IAM, que são compartilhados com uma entidade externa. Isso ajuda a evitar o acesso não pretendido aos recursos e dados. O IAM Access Analyzer é regional e deve ser habilitado em cada região. Para identificar recursos que são compartilhados com entidades externas, um analisador de acesso usa raciocínio baseado em lógica para analisar políticas baseadas em recursos em seu ambiente. AWS Ao criar um analisador de acesso externo, você pode criá-lo e ativá-lo para toda a sua organização ou contas individuais.

> **Note**
>
> Se uma conta fizer parte de uma organização em AWS Organizations, esse controle não considera os analisadores de acesso externo que especificam a organização como a zona de confiança e estão habilitados para a organização na região atual. Se sua organização usa esse tipo de configuração, considere desativar esse controle para contas de membros individuais em sua organização na região.

Correção

Para obter informações sobre como habilitar um analisador de acesso externo em uma região específica, consulte Introdução ao IAM Access Analyzer no Guia do usuário do IAM. Você deve habilitar um analisador em cada região na qual deseja monitorar o acesso aos recursos.

Controles do Security Hub para o Amazon Inspector

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Inspector.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2

Requisitos relacionados: PCI DSS v4.0.1/11.3.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::::Account`

Regra do AWS Config : `inspector-ec2-scan-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o EC2 escaneamento do Amazon Inspector está habilitado. Para uma conta autônoma, o controle falhará se a digitalização do Amazon EC2 Inspector estiver desativada na conta. Em um ambiente com várias contas, o controle falha se a conta delegada de administrador do Amazon Inspector e todas as contas membros não EC2 tiverem a verificação ativada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de administrador delegado do Amazon Inspector. Somente o administrador delegado pode ativar ou desativar o recurso de EC2 escaneamento das contas dos membros na organização. As contas-membro do Amazon Inspector não podem modificar essa configuração nas suas contas. Esse controle gera `FAILED` descobertas se o administrador delegado tiver uma conta de membro suspensa que não tenha a verificação do Amazon EC2 Inspector ativada. Para receber uma descoberta `PASSED`, o administrador delegado deve desassociar essas contas suspensas no Amazon Inspector.

O EC2 escaneamento do Amazon Inspector extrai metadados da sua instância do Amazon Elastic Compute Cloud (EC2Amazon) e, em seguida, compara esses metadados com regras coletadas de consultorias de segurança para produzir descobertas. O Amazon Inspector varre as instâncias em busca de vulnerabilidades de pacotes e problemas de acessibilidade de rede. Para obter informações sobre sistemas operacionais compatíveis, incluindo quais sistemas operacionais podem ser escaneados sem um agente SSM, consulte Sistemas operacionais compatíveis: escaneamento da Amazon EC2 .

Correção

Para habilitar o EC2 escaneamento do Amazon Inspector, consulte Ativação de escaneamentos no Guia do Usuário do Amazon Inspector.

[Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.3.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::::Account`

Regra do AWS Config : `inspector-ecr-scan-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a varredura do ECR do Amazon Inspector está habilitada. Para uma conta autônoma, o controle falhará se a varredura do ECR do Amazon Inspector estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de administrador delegado do Amazon Inspector e todas as contas-membro não tiverem a varredura do ECR habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de administrador delegado do Amazon Inspector. Somente o administrador delegado pode habilitar ou desabilitar o atributo de varredura do ECR para as contas-membro da organização. As contas-membro do Amazon Inspector não podem modificar essa configuração nas suas contas. Esse controle gerará descobertas `FAILED` se o administrador delegado tiver uma conta-membro suspensa que não tenha a varredura do ECR do Amazon Inspector habilitada. Para receber uma descoberta `PASSED`, o administrador delegado deve desassociar essas contas suspensas no Amazon Inspector.

O Amazon Inspector varre as imagens de contêineres armazenadas no Amazon Elastic Container Registry (Amazon ECR) em busca de vulnerabilidades de software para gerar descobertas de vulnerabilidade de pacote. Ao ativar as verificações do Amazon Inspector para o Amazon ECR, você define o Amazon Inspector como seu serviço de verificação preferido para seu registro privado. Isso substitui o escaneamento básico, que é fornecido gratuitamente pelo Amazon ECR, pela varredura avançada que é fornecida e cobrada por meio do Amazon Inspector. O escaneamento avançado oferece o benefício de varrer para encontrar vulnerabilidades para pacotes de sistemas operacionais e de linguagens de programação ao nível do registro. Analise as descobertas usando o escaneamento avançado no nível da imagem, para cada camada da imagem, no console do Amazon ECR. Além disso, você pode analisar e trabalhar com essas descobertas em outros serviços não disponíveis para descobertas básicas de escaneamento, incluindo AWS Security Hub a Amazon EventBridge.

Correção

Para habilitar a varredura do ECR do Amazon Inspector, consulte Activating scans no Amazon Inspector User Guide.

[Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::Account`

Regra do AWS Config : `inspector-lambda-code-scan-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a varredura de código do Lambda do Amazon Inspector está habilitada. Para uma conta autônoma, o controle falhará se a varredura de código do Lambda do Amazon Inspector estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de administrador delegado do Amazon Inspector e todas as contas-membro não tiverem a varredura de código do Lambda habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de administrador delegado do Amazon Inspector. Somente o administrador delegado pode habilitar ou desabilitar

o atributo de varredura de código do Lambda para as contas-membro da organização. As contas-membro do Amazon Inspector não podem modificar essa configuração nas suas contas. Esse controle gerará descobertas `FAILED` se o administrador delegado tiver uma conta-membro suspensa que não tenha a varredura do varredura de código do Lambda do Amazon Inspector habilitada. Para receber uma descoberta `PASSED`, o administrador delegado deve desassociar essas contas suspensas no Amazon Inspector.

O escaneamento de código Lambda do Amazon Inspector escaneia o código do aplicativo personalizado dentro de uma AWS Lambda função em busca de vulnerabilidades de código com base nas melhores práticas de segurança. AWS O escaneamento de código do Lambda pode detectar falhas de injeção, vazamentos de dados, criptografia fraca ou criptografia ausente em seu código. Esse recurso está disponível Regiões da AWS somente de forma específica. Você pode ativar a varredura de código do Lambda junto com a varredura padrão do Lambda (consulte [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada).

Correção

Para habilitar varredura de código do Lambda do Amazon Inspector, consulte Activating scans no Amazon Inspector User Guide.

[Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::::Account`

Regra do AWS Config : `inspector-lambda-standard-scan-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a varredura padrão do Lambda do Amazon Inspector está habilitada. Para uma conta autônoma, o controle falhará se a varredura padrão do Lambda do Amazon Inspector estiver desabilitada na conta. Em um ambiente com várias contas, o controle falhará se a conta de administrador delegado do Amazon Inspector e todas as contas-membro não tiverem a varredura padrão do Lambda habilitada.

Em um ambiente com várias contas, o controle gera descobertas somente na conta de administrador delegado do Amazon Inspector. Somente o administrador delegado pode habilitar ou desabilitar o atributo de varredura padão do Lambda para as contas-membros na organização. As contas-membro do Amazon Inspector não podem modificar essa configuração nas suas contas. Esse controle gerará descobertas `FAILED` se o administrador delegado tiver uma conta-membro suspensa que não tenha a varredura do varredura padrão do Lambda do Amazon Inspector habilitada. Para receber uma descoberta `PASSED`, o administrador delegado deve desassociar essas contas suspensas no Amazon Inspector.

O escaneamento padrão do Amazon Inspector Lambda identifica vulnerabilidades de software nas dependências do pacote de aplicativos que você adiciona ao seu código de função e camadas. AWS Lambda Se o Amazon Inspector detectar uma vulnerabilidade nas dependências do pacotes de aplicação da função do Lambda, o Amazon Inspector produzirá uma descoberta detalhada do tipo `Package Vulnerability`. Você pode ativar a varredura de código do Lambda junto com a varredura padrão do Lambda (consulte [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada).

Correção

Para habilitar a varredura padrão do Lambda do Amazon Inspector, consulte Activating scans no Amazon Inspector User Guide.

Controles do Security Hub para AWS IoT

Esses AWS Security Hub controles avaliam o AWS IoT serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[IoT.1] perfis de AWS IoT Device Defender segurança devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::SecurityProfile`

Regra AWS Config : `tagged-iot-securityprofile` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um perfil de AWS IoT Device Defender 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 verificará apenas a existência de uma chave de tag e falhará se o perfil de segurança não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 perfil AWS IoT Device Defender 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::MitigationAction`

Regra AWS Config : `tagged-iot-mitigationaction` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se a ação de mitigação não estiver marcada com

nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::Dimension`

Regra AWS Config : `tagged-iot-dimension` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se a dimensão não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::Authorizer`

Regra AWS Config : `tagged-iot-authorizer` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o autorizador não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::RoleAlias`

Regra AWS Config : `tagged-iot-rolealias` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 de perfil 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 alias de perfil não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoT::Policy`

Regra AWS Config : `tagged-iot-policy` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se a política não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 AWS IoT Core política, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

Controles do Security Hub para eventos AWS de IoT

Esses AWS Security Hub controles avaliam o serviço e os recursos do AWS IoT Events.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTEvents::Input`

Regra do AWS Config : `iotevents-input-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma entrada de AWS IoT Events tem tags com as chaves específicas definidas no `requiredKeyTags` parâmetro. O controle falhará se a entrada não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a entrada não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma entrada AWS do IoT Events, consulte Como marcar AWS IoT Events seus recursos no Guia AWS IoT Events do desenvolvedor.

[Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTEvents::DetectorModel`

Regra do AWS Config : `iotevents-detector-model-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um modelo de detector de eventos de AWS IoT tem tags com as chaves específicas definidas no `requiredKeyTags` parâmetro. O controle falhará se o modelo do detector não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o modelo do detector não estiver

marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um modelo de detector de eventos do AWS IoT, consulte Como marcar AWS IoT Events seus recursos no Guia AWS IoT Events do desenvolvedor.

[Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTEvents::AlarmModel`

Regra do AWS Config : `iotevents-alarm-model-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um modelo de alarme do AWS IoT Events tem tags com as chaves específicas definidas no `requiredKeyTags` parâmetro. O controle falhará se o modelo de alarme não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o modelo de alarme não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da

AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um modelo de alarme do AWS IoT Events, consulte Como marcar AWS IoT Events seus recursos no Guia AWS IoT Events do desenvolvedor.

Controles do Security Hub para AWS IoT SiteWise

Esses AWS Security Hub controles avaliam o SiteWise serviço e os recursos de AWS IoT.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTSiteWise::AssetModel`

Regra do AWS Config : `iotsitewise-asset-model-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um modelo de SiteWise ativo de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o modelo de ativos não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o modelo de ativo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um modelo de SiteWise ativo de AWS IoT, consulte Marcar seus AWS IoT SiteWise recursos no Guia do AWS IoT SiteWise usuário.

[Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTSiteWise::Dashboard`

Regra do AWS Config : `iotsitewise-dashboard-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um SiteWise painel de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o painel não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o painel não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um SiteWise painel de AWS IoT, consulte Marcar seus AWS IoT SiteWise recursos no Guia do AWS IoT SiteWise usuário.

[Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTSiteWise::Gateway`

Regra do AWS Config : `iotsitewise-gateway-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um SiteWise gateway de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o gateway não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o gateway não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um SiteWise gateway de AWS IoT, consulte Marcar seus AWS IoT SiteWise recursos no Guia do AWS IoT SiteWise usuário.

[Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTSiteWise::Portal`

Regra do AWS Config : `iotsitewise-portal-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um SiteWise portal de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o portal não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle somente verificará a existência de uma chave de tag e falhará se o portal não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um SiteWise portal de AWS IoT, consulte Marcar seus AWS IoT SiteWise recursos no Guia do AWS IoT SiteWise usuário.

[Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTSiteWise::Project`

Regra do AWS Config : `iotsitewise-project-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um SiteWise projeto de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o projeto não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o projeto não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um SiteWise projeto de AWS IoT, consulte Marcar seus AWS IoT SiteWise recursos no Guia do AWS IoT SiteWise usuário.

Controles do Security Hub para AWS IoT TwinMaker

Esses AWS Security Hub controles avaliam o TwinMaker serviço e os recursos de AWS IoT.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTTwinMaker::SyncJob`

Regra do AWS Config : `iottwinmaker-sync-job-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um trabalho de TwinMaker sincronização de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se a tarefa de sincronização não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o trabalho de sincronização não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como

uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um trabalho de TwinMaker sincronização de AWS IoT, consulte TagResource no AWS IoT TwinMaker Guia do usuário.

[Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTTwinMaker::Workspace`

Regra do AWS Config : `iottwinmaker-workspace-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um TwinMaker espaço de trabalho de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o espaço de trabalho não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o espaço de trabalho não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um espaço de TwinMaker trabalho de AWS IoT, consulte TagResource no AWS IoT TwinMaker Guia do usuário.

[Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTTwinMaker::Scene`

Regra do AWS Config : `iottwinmaker-scene-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma TwinMaker cena de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se a cena não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave

de tag e falhará se a cena não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma TwinMaker cena de AWS IoT, consulte TagResource no AWS IoT TwinMaker Guia do usuário.

[Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTTwinMaker::Entity`

Regra do AWS Config : `iottwinmaker-entity-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma TwinMaker entidade de AWS IoT tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se a entidade não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a entidade não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma TwinMaker entidade de AWS IoT, consulte TagResource no AWS IoT TwinMaker Guia do usuário.

Controles do Security Hub para AWS IoT Wireless

Esses AWS Security Hub controles avaliam o serviço e os recursos do AWS IoT Wireless.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTWireless::MulticastGroup`

Regra do AWS Config : `iotwireless-multicast-group-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um grupo multicast do AWS IoT Wireless tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o grupo multicast não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo multicast não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um grupo multicast do AWS IoT Wireless, consulte Como marcar AWS IoT Wireless seus recursos no AWS IoT Wireless Guia do desenvolvedor.

[Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTWireless::ServiceProfile`

Regra do AWS Config : `iotwireless-service-profile-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um perfil de serviço AWS IoT Wireless tem tags com as chaves específicas definidas no `requiredKeyTags` parâmetro. O controle falhará se o perfil de serviço não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o perfil de serviço não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um perfil de serviço AWS IoT Wireless, consulte Como marcar AWS IoT Wireless seus recursos no Guia AWS IoT Wireless do desenvolvedor.

[Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IoTWireless::FuotaTask`

Regra do AWS Config : `iotwireless-fuota-task-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma tarefa de over-the-air atualização de firmware do AWS IoT Wireless (FUOTA) tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se a tarefa FUOTA não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se a tarefa FUOTA não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma tarefa FUOTA do AWS IoT Wireless, consulte Como marcar AWS IoT Wireless seus recursos no AWS IoT Wireless Guia do desenvolvedor.

Controles do Security Hub para Amazon IVS

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Interactive Video Service (IVS).

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IVS::PlaybackKeyPair`

Regra do AWS Config : `ivs-playback-key-pair-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um par de chaves de reprodução do Amazon IVS tem tags com as teclas específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o par de chaves de reprodução não tiver nenhuma chave de tag ou se não tiver todas as teclas especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o par de teclas de reprodução não estiver marcado com nenhuma tecla. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um par de chaves de reprodução IVS, consulte TagResourcena referência da API de streaming em tempo real do Amazon IVS.

[IVS.2] As configurações de gravação IVS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IVS::RecordingConfiguration`

Regra do AWS Config : `ivs-recording configuration-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma configuração de gravação do Amazon IVS tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a configuração de gravação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a configuração de gravação não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte

Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma configuração de gravação IVS, consulte TagResourcena referência da API de streaming em tempo real do Amazon IVS.

[IVS.3] Os canais IVS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::IVS::Channel`

Regra do AWS Config : `ivs-channel-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um canal do Amazon IVS tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se o canal não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e

falhará se o canal não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um canal IVS, consulte TagResourcena referência da API de streaming em tempo real do Amazon IVS.

Controles do Security Hub para Amazon Keyspaces

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Keyspaces.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Cassandra::Keyspace`

Regra do AWS Config : `cassandra-keyspace-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um keyspace do Amazon Keyspaces tem tags com as chaves específicas definidas no parâmetro. `requiredKeyTags` O controle falhará se o keyspace não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o keyspace não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a um keyspace do Amazon Keyspaces, consulte Adicionar tags a um keyspace no Amazon Keyspaces Developer Guide.

Controles do Security Hub para o Kinesis

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Kinesis.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Kinesis.1] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::Kinesis::Stream`

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 falha se um fluxo do Kinesis não estiver 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 um AWS KMS key. 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 fluxos do Kinesis, consulte Como começar a criptografia no lado do servidor? no Guia do desenvolvedor do Amazon Kinesis.

[Kinesis.2] Os fluxos do Kinesis devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Kinesis::Stream`

Regra AWS Config: `tagged-kinesis-stream` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um fluxo 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 de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 fluxo de dados do Kinesis, consulte Tagging your streams in Amazon Kinesis Data Streams no Amazon Kinesis Developer Guide.

[Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado

Severidade: média

Tipo de recurso: `AWS::Kinesis::Stream`

Regra do AWS Config: kinesis-stream-backup-retention-check

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`minimumBackupRetentionPeriod`	Número mínimo de horas durante as quais os dados devem ser retidos.	String	24 a 8.760	168

Esse controle verifica se um fluxo de dados do Amazon Kinesis tem um período de retenção de dados maior ou igual ao período de tempo especificado. O controle falhará se o período de retenção de dados for inferior ao período de tempo especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção de dados, o Security Hub usará um valor padrão de 168 horas.

No Kinesis Data Streams, um fluxo de dados é uma sequência ordenada de registros de dados destinada a ser gravada e lida em tempo real. Os registros de dados são armazenados em fragmentos no fluxo temporariamente. O período entre o momento de adição de um registro e o momento em que ele deixa de estar acessível é chamado de período de retenção. O Kinesis Data Streams torna os registros mais antigos que o novo período de retenção acessíveis quase imediatamente após a redução do período de retenção. Por exemplo, alterar o período de retenção de 24 horas para 48 horas significa que os registros adicionados ao fluxo 23 horas 55 minutos antes ainda estarão disponíveis depois de 24 horas.

Correção

Para alterar o período de retenção de backup do Amazon Kinesis Data Streams, consulte Change the data retention period no Amazon Kinesis Data Streams Developer Guide.

Controles do Security Hub para AWS KMS

Esses AWS Security Hub controles avaliam o AWS Key Management Service (AWS KMS) serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[KMS.1] 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 AC-2, NIST.800-53.r5 AC-2 (1) 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-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::IAM::Policy`

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. Em outras palavras, você deve conceder apenas as permissões `kms:Decrypt` ou `kms:ReEncryptFrom` necessárias e apenas para a 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 `kms:Decrypt` somente com chaves em uma região específica para sua conta. Ao adotar o princípio do privilégio mínimo, você pode 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.

[KMS.2] 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 AC-2, NIST.800-53.r5 AC-2 (1) 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-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

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, você pode 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-1 2, NIST.800-53.r5 SC-1 2 (2)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: crítica

Tipo de recurso: `AWS::KMS::Key`

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: CIS AWS Foundations Benchmark v3.0.0/3.6, CIS Foundations Benchmark v1.4.0/3.8, CIS AWS Foundations Benchmark v1.2.0/2.8, 2, 2 (2), 8 (3), PCI DSS AWS v3.2.1/3.6.4, PCI DSS v4.0.1/3.7.4 NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::KMS::Key`

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 .

[KMS.5] As chaves do KMS não devem estar acessíveis ao público

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::KMS::Key`

Regra do AWS Config : kms-key-policy-no-public-access

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Isso controla se um AWS KMS key está acessível ao público. O controle falhará se a chave do KMS estiver acessível ao público.

A implementação do privilégio de acesso mínimo é fundamental para reduzir o risco de segurança e o impacto de erros ou usuários mal-intencionados. Se a política de chaves do an AWS KMS key permitir o acesso de contas externas, terceiros poderão criptografar e descriptografar dados usando a chave. Isso pode resultar em uma ameaça interna ou externa extraindo dados Serviços da AWS desse uso da chave.

> **Note**
>
> Esse controle também retorna uma `FAILED` descoberta para um AWS KMS key caso suas configurações AWS Config impeçam o registro da política de chaves no Item de

Configuração (CI) da chave KMS. AWS Config Para preencher a política de chaves no CI para a chave KMS, a AWS Config função deve ter acesso para ler a política de chaves usando a chamada de GetKeyPolicyAPI. Para resolver esse tipo de `FAILED` descoberta, verifique as políticas que podem impedir que a AWS Config função tenha acesso de leitura à política de chaves da chave KMS. Por exemplo, verifique o seguinte:

- A política de chaves para a chave KMS.
- As políticas de controle de serviços (SCPs) e as políticas de controle de recursos (RCPs) AWS Organizations que se aplicam à sua conta.
- Permissões para a AWS Config função, se você não estiver usando a função AWS Config vinculada ao serviço.

Além disso, esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política de chaves devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

Correção

Para obter informações sobre como atualizar a política de chaves para um AWS KMS key, consulte Políticas principais AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Controles do Security Hub para AWS Lambda

Esses AWS Security Hub controles avaliam o AWS Lambda serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Lambda.1] As funções do Lambda.1 devem proibir o acesso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21),,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20), (21) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 3.2.1/7.2.1, PCI DSS v4.0.1/7.2.1 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::Lambda::Function`

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 Lambda 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.

> **Note**
>
> Esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política da função Lambda devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

A função do Lambda não deve ser publicamente acessível, pois isso pode permitir o acesso não intencional ao seu código de 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": "*" }`.

Você pode editar uma política a partir do 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 Lambda devem usar os tempos de execução compatíveis

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-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), PCI DSS v4.0.1/12.3.4

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso: `AWS::Lambda::Function`

Regra do AWS Config : lambda-function-settings-check

Tipo de programação: acionado por alterações

Parâmetros:

- `runtime`: `dotnet8, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, ruby3.4, 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, conforme observado na seção Parâmetros. O Security Hub ignora as funções que têm um tipo de pacote de `Image`.

Os tempos de execução do Lambda 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 componente de runtime obsoleto, a função ainda continuará disponível

para processar eventos de invocação. Recomendamos garantir que as funções do Lambda estejam atualizadas e não usem ambientes de runtime obsoletos. Para obter uma lista dos runtimes compatíveis, consulte Runtimes do Lambda no Guia do desenvolvedor do AWS Lambda .

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 runtime para ajudar a reduzir o risco de impacto para as workloads no caso raro de uma incompatibilidade de versão de runtime.

[Lambda.3] 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 v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7), (21),,, (11), (16), (20) NIST.800-53.r5 AC-3, (21), (3) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (4), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso: `AWS::Lambda::Function`

AWS Config regra: lambda-inside-vpc

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma função do Lambda está em uma nuvem privada virtual (VPC). O controle falhará se a função do Lambda não estiver implantada em uma VPC. O Security Hub não avalia a configuração de roteamento da sub-rede da VPC para determinar a acessibilidade pública. Você pode ver falhas nas descobertas dos recursos do Lambda @Edge.

A implantação de recursos em uma VPC aumenta 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 das aplicações.

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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Lambda::Function`

Regra do AWS Config : lambda-vpc-multi-az-check

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 Zona 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 usa um valor padrão de dois AZs.

A implantação de recursos em vários 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 sua função para se conectar a uma VPC em sua conta, especifique sub-redes em várias AZs para garantir alta disponibilidade. Para obter instruções, consulte Configurar acesso à VPC no Guia do desenvolvedor do AWS Lambda .

O Lambda executa automaticamente outras funções em várias AZs para garantir que esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

[Lambda.6] As funções do Lambda devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Lambda::Function`

Regra AWS Config : `tagged-lambda-function` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma AWS Lambda função 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 verificará apenas a existência de uma chave de tag e falhará se a função não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para saber mais sobre as práticas recomendadas de marcação, consulte Tagging your AWS resources na Referência geral da AWS.

Correção

Para adicionar tags a uma função do Lambda, consulte Utilizar etiquetas em funções do Lambda no Guia do desenvolvedor do AWS Lambda .

[Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso: `AWS::Lambda::Function`

Regra do AWS Config : lambda-function-xray-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o rastreamento ativo com AWS X-Ray está habilitado para uma AWS Lambda função. O controle falhará se o rastreamento ativo com o X-Ray for desativado para a função Lambda.

AWS X-Ray pode fornecer recursos de rastreamento e monitoramento para AWS Lambda funções, o que pode economizar tempo e esforço na depuração e operação de funções Lambda. Ele pode ajudá-lo a diagnosticar erros e identificar gargalos de desempenho, lentidão e tempos limite ao detalhar a latência das funções Lambda. Também pode ajudar com os requisitos de privacidade e conformidade de dados. Se você habilitar o rastreamento ativo para uma função Lambda, o X-Ray fornece uma visão holística do fluxo e processamento de dados na função Lambda, o que pode ajudá-lo a identificar possíveis vulnerabilidades de segurança ou práticas de tratamento de dados não compatíveis. Essa visibilidade pode ajudar você a manter a integridade, a confidencialidade e a conformidade dos dados com as regulamentações relevantes.

> **Note**
>
> AWS X-Ray Atualmente, o rastreamento não é suportado para funções Lambda com Amazon Managed Streaming para Apache Kafka (Amazon MSK), Apache Kafka autogerenciado, Amazon MQ com ActiveMQ e RabbitMQ ou mapeamentos de origem de eventos do Amazon DocumentDB.

Correção

Para obter informações sobre como habilitar o rastreamento ativo para uma AWS Lambda função, consulte Visualize invocações de funções Lambda usando no Guia do desenvolvedor. AWS X-RayAWS Lambda

Controles do Security Hub para o Macie

Esses AWS Security Hub controles avaliam o serviço Amazon Macie.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Macie.1] O Amazon Macie deve estar habilitado

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.r5 SI-4

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso: `AWS:::Account`

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 estar habilitada

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.r5 SI-4

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS:::Account`

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 em uma conta de administrador do Amazon Macie. Esse controle falhará se a descoberta automatizada de dados confidenciais não estiver habilitada em uma conta de administrador do Macie. Esse controle se aplica somente a contas de administrador.

O Macie automatiza a descoberta e a geração 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 do S3 representativos em seus buckets. O Macie então recupera e analisa os objetos selecionados, inspecionando-os para detectar dados confidenciais. Conforme a análise progride, o Macie também atualiza estatísticas, dados de inventário e outras informações que ele fornece sobre os 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 Configuring automated sensitive data discovery for your account no Amazon Macie User Guide.

Controles do Security Hub para o Amazon MSK

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Managed Streaming for Apache Kafka (Amazon MSK). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::MSK::Cluster`

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 é criptografado em trânsito com HTTPS (TLS) entre os nós de agente 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. Entretanto, 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 obter informações sobre a atualização das configurações de criptografia de um cluster Amazon MSK, consulte Atualização das 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 CA-7, NIST.800-53.r5 SI-2

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::MSK::Cluster`

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 Amazon MSK em https://console.aws.amazon.com/msk/casa? 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 as métricas do Amazon MSK para monitorar corretores padrão CloudWatch no Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka.

[MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito

Requisitos relacionados: PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::KafkaConnect::Connector`

Regra AWS Config : `msk-connect-connector-encrypted` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um conector do Amazon MSK Connect é criptografado em trânsito. Esse controle falhará se o conector não for criptografado em trânsito.

Dados em trânsito se referem a dados que se movem de um local para outro, como entre os nós do cluster ou entre o cluster e a aplicação. Os dados podem se mover pela Internet ou em uma

rede privada. Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede.

Correção

Você pode habilitar a criptografia em trânsito ao criar um conector do MSK Connect. Não é possível alterar as configurações de criptografia após a criação de um conector. Para obter mais informações, consulte IAM access control (Controle de acesso do IAM) no Create a connector no Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.4] Os clusters MSK devem ter o acesso público desativado

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::MSK::Cluster`

Regra do AWS Config : msk-cluster-public-access-disabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o acesso público está desabilitado para um cluster Amazon MSK. O controle falhará se o acesso público estiver habilitado para o cluster MSK.

Por padrão, os clientes podem acessar um cluster Amazon MSK somente se estiverem na mesma VPC do cluster. Toda comunicação entre clientes Kafka e um cluster MSK é privada por padrão e os dados de streaming não atravessam a Internet. No entanto, se um cluster MSK estiver configurado para permitir acesso público, qualquer pessoa na Internet poderá estabelecer uma conexão com os corretores Apache Kafka que estão sendo executados no cluster. Isso pode levar a problemas como acesso não autorizado, violações de dados ou exploração de vulnerabilidades. Se você restringir o acesso a um cluster exigindo medidas de autenticação e autorização, poderá ajudar a proteger informações confidenciais e manter a integridade de seus recursos.

Correção

Para obter informações sobre como gerenciar o acesso público a um cluster do Amazon MSK, consulte Ativar o acesso público a um cluster provisionado pelo MSK no Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka.

[MSK.5] Os conectores MSK devem ter o registro ativado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::KafkaConnect::Connector`

Regra do AWS Config : msk-connect-connector-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro está habilitado para um conector Amazon MSK. O controle falhará se o registro estiver desativado para o conector MSK.

Os conectores Amazon MSK integram sistemas externos e serviços da Amazon com o Apache Kafka copiando continuamente dados de streaming de uma fonte de dados para um cluster do Apache Kafka ou copiando continuamente dados de um cluster para um coletor de dados. O MSK Connect pode gravar eventos de log que podem ajudar a depurar um conector. Ao criar um conector, você pode especificar zero ou mais dos seguintes destinos de log: Amazon CloudWatch Logs, Amazon S3 e Amazon Data Firehose.

> **Note**
>
> Valores confidenciais de configuração podem aparecer nos registros do conector se um plug-in não definir esses valores como secretos. O Kafka Connect trata valores de configuração indefinidos da mesma forma que qualquer outro valor de texto simples.

Correção

Para habilitar o registro em log para um conector Amazon MSK existente, você precisa recriar o conector com a configuração de registro apropriada. Para obter informações sobre as opções de configuração, consulte Logging for MSK Connect no Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka.

[MSK.6] Os clusters MSK devem desativar o acesso não autenticado

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso: `AWS::MSK::Cluster`

Regra do AWS Config : msk-unrestricted-access-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o acesso não autenticado está habilitado para um cluster Amazon MSK. O controle falhará se o acesso não autenticado estiver habilitado para o cluster MSK.

O Amazon MSK oferece suporte a mecanismos de autenticação e autorização de clientes para controlar o acesso a um cluster. Esses mecanismos verificam a identidade dos clientes que se conectam ao cluster e determinam quais ações os clientes podem realizar. Um cluster MSK pode ser configurado para permitir acesso não autenticado, o que permite que qualquer cliente com conectividade de rede publique e assine tópicos do Kafka sem fornecer credenciais. Executar um cluster MSK sem exigir autenticação viola o princípio do privilégio mínimo e pode expor o cluster ao acesso não autorizado. Ele pode permitir que qualquer cliente acesse, modifique ou exclua dados nos tópicos do Kafka, o que pode resultar em violações de dados, modificações de dados não autorizadas ou interrupções no serviço. Recomendamos ativar mecanismos de autenticação, como autenticação IAM, SASL/SCRAM ou TLS mútuo, para garantir o controle de acesso adequado e manter a conformidade de segurança.

Correção

Para obter informações sobre como alterar as configurações de autenticação de um cluster Amazon MSK, consulte as seguintes seções do Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka: Atualizar as configurações de segurança de um cluster Amazon MSK e Autenticação e autorização para o Apache Kafka. APIs

Controles do Security Hub para o Amazon MQ

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon MQ.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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, PCI DSS v4.0.1/10.3.3

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::AmazonMQ::Broker`

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 agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SI-2, PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: baixa

Tipo de recurso: `AWS::AmazonMQ::Broker`

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 têm a atualização automática de versões secundárias habilitada. O controle falhará se o corretor não tiver a atualização automática de versões secundárias habilitada.

À medida que o Amazon MQ lança e torna-se compatível com novas versões do mecanismo de agente, as alterações são compatíveis com as versões anteriores de uma aplicação existente e não tornam a funcionalidade existente obsoleta. As atualizações automáticas da versão do mecanismo de agente protegem você contra riscos de segurança, ajudam a corrigir erros e aprimoram a funcionalidade.

> **Note**
>
> Quando o agente associado à atualização automática de versões secundárias está em sua correção mais recente e torna-se incompatível, você deve fazer a atualização manualmente.

Correção

Para habilitar a atualização automática de versões secundárias para um agente MQ, consulte Automatically upgrading the minor engine version no Amazon MQ Developer Guide.

[MQ.4] Os agentes do Amazon MQ devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::AmazonMQ::Broker`

Regra AWS Config : `tagged-amazonmq-broker` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 agente 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 agente não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 agente do Amazon MQ, consulte Tagging resources no Amazon MQ Developer Guide.

[MQ.5] 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso: `AWS::AmazonMQ::Broker`

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 Agente ativo/em espera. 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.

[MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso: `AWS::AmazonMQ::Broker`

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 RabbitMQ está definido como implantação em cluster. 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 RabbitMQ com modo de implantação em cluster, consulte Criar e conectar um agente RabbitMQ no Guia do desenvolvedor do Amazon MQ. Em Modo de implantação, escolha Implantação em cluster. 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 Security Hub para o Neptune

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Neptune.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Neptune.1] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::RDS::DBCluster`

Regra do AWS Config : `neptune-cluster-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Neptune 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

Você pode ativar a criptografia em repouso ao criar um cluster de banco de dados do Neptune. 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), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-20 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 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7 (8), PCI DI SS v4.0.1/10.3.3

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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.

[Neptune.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

Regra do AWS Config : `neptune-cluster-snapshot-public-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo manual de cluster de banco de dados do Neptune é público. O controle falhará se o instantâneo manual do cluster de banco de dados do Neptune 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 CA-9 (1), NIST.800-53.r5 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::RDS::DBCluster`

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 de banco de dados do Neptune 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 de banco de dados do Neptune 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.

[Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados

Requisitos relacionados: NIST.800-53.r5 SI-12

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : `neptune-cluster-backup-retention-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 de banco de dados do Neptune você poderá 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 Período de reteção de backup, escolha um valor maior ou igual a 7.

[Neptune.6] Os instantâneos do cluster 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

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 instantâneos de clusters de banco de dados do Neptune 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, você pode 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-2 (1) 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: `AWS::RDS::DBCluster`

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.

[Neptune.8] Os clusters de banco de dados do Neptune devem ser configurados para copiar tags para instantâneos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBCluster`

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 e o inventário 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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 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 que você crie 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 uma instância AZs diferente da primária.

Correção

Para implantar um cluster de banco de dados Neptune em AZs vários, consulte Instâncias de banco de dados de leitura de réplicas em um cluster de banco de dados Neptune no Guia do usuário do Neptune.

Controles do Security Hub para o AWS Network Firewall

Esses AWS Security Hub controles do avaliam o AWS Network Firewall serviço e os recursos da. Os controles da podem não estar disponíveis em todos os Regiões da AWS. Para obter 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regra do AWS Config : netfw-multi-az-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle avalia se um firewall gerenciado pelo AWS Network Firewall é implantado em várias zonas de disponibilidade ()AZs. O controle falhará se um firewall for implantado em apenas uma AZ.

AWS A infraestrutura global da inclui várias Regiões da AWS. 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 da 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 em log do Network Firewall deve ser habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), (9),, (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-2 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 AC-4 NIST.800-53.r5 SI-4 NIST.800-53.r5 AC-6 (20), NIST.800-53.r5 SI-7 (8) 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-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 IST.800-171.r2 3.13.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::LoggingConfiguration`

Regra do AWS Config : netfw-logging-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro em log está habilitado para um AWS Network Firewall firewall do. 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 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

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 de regras, consulte Grupos de regras no 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 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

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 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 alterar sua política de firewall, 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 pacotes fragmentados.

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

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 fragmentados 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 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 alterar sua política de firewall, 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 Firewall de Rede sem estado não deve estar vazio

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), (11), (16), (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::RuleGroup`

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 em 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. No entanto, 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 Network Firewall devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regra AWS Config : `tagged-networkfirewall-firewall` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um AWS Network Firewall firewall do 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 verificará apenas a existência de uma chave de tag e falhará se o firewall não estiver marcado com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode associar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, incluindo o 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 Tagging AWS Network Firewall resources no AWS Network Firewall Developer Guide.

[NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

Regra AWS Config : `tagged-networkfirewall-firewallpolicy` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma política de AWS Network Firewall firewall do 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 verificará apenas a existência de uma chave de tag e falhará se a política de firewall não estiver marcada com nenhuma chave. As tags de sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso da 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode associar tags a entidades do IAM (usuários ou perfis) e a AWS recursos da. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso. Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos Serviços da AWS, incluindo o 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 Network Firewall devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

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 habilitada. 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`

[NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede ativada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regra do AWS Config : netfw-subnet-change-protection-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a proteção contra alterações de sub-rede está habilitada para um AWS Network Firewall firewall do. O controle falhará se a proteção contra alterações de sub-rede não estiver habilitada para o firewall.

AWS Network Firewall é um firewall de rede gerenciado e com estado e serviço de detecção de intrusões que você pode usar para inspecionar e filtrar o tráfego de, para ou entre suas nuvens privadas virtuais (). VPCs Se você habilitar a proteção contra alterações de sub-rede para um firewall do Firewall de Rede, poderá proteger o firewall contra alterações acidentais nas associações de sub-rede do firewall.

Correção

Para obter informações sobre como ativar a proteção contra alterações de sub-rede em um firewall de Firewall de Rede existente, consulte Atualização de um firewall no Guia do AWS Network Firewall Desenvolvedor.

Controles do Security Hub para Amazon OpenSearch Service

Esses AWS Security Hub controles avaliam o OpenSearch serviço e os recursos do Amazon OpenSearch Service (Service). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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, (1), 3, 8, 8 (1), Nist.800-53.r5 SI-7 (6) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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 v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1,, (7),, (21),, (11), (16), (20), (21), (3), (4 NIST.800-53.r5 AC-3) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5

AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura > Recursos na VPC

Severidade: crítica

Tipo de recurso: `AWS::OpenSearch::Domain`

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 Guia 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. VPCs forneça 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 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 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (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)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7, NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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.

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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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`.

Para obter alta disponibilidade e tolerância a falhas em nível de cluster, um OpenSearch domínio deve ter pelo menos três nós de dados. 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 que `3`. Se estiver fazendo implantações em três zonas 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 AC-2 (1) 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-5, NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Ações confidenciais de API restritas

Severidade: alta

Tipo de recurso: `AWS::OpenSearch::Domain`

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-1 7 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::OpenSearch::Domain`

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 mais recente suportada ou se 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 especificar o valor para`TLSSecurityPolicy`. Para obter mais informações, consulte Node-to-node criptografia no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.9] devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::OpenSearch::Domain`

Regra AWS Config : `tagged-opensearch-domain` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o domínio não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como

uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 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 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: baixa

Tipo de recurso: `AWS::OpenSearch::Domain`

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-3 6, Nist.800-53.r5 SI-13

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso: `AWS::OpenSearch::Domain`

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 realiza tarefas de gerenciamento de cluster, mas não retem dados nem responde a 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.

Controles do Security Hub para AWS Private CA

Esses AWS Security Hub controles avaliam o AWS Private Certificate Authority (AWS Private CA) serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso: `AWS::ACMPCA::CertificateAuthority`

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 uma subordinada CAs. Você deve minimizar o uso da CA raiz para tarefas diárias, especialmente em ambientes de produção. A CA raiz só deve ser usada para emitir certificados intermediários CAs. Isso permite que a CA raiz seja armazenada fora de perigo, enquanto o intermediário CAs executa 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 .

[PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::ACMPCA::CertificateAuthority`

Regra do AWS Config : `acmpca-certificate-authority-tagged`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma autoridade de certificação de CA AWS privada tem tags com as chaves específicas definidas no parâmetro`requiredKeyTags`. O controle falhará se a autoridade de certificação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredKeyTags`. Se o parâmetro `requiredKeyTags` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a autoridade de certificação não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag

do recurso. Para obter mais informações, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Melhores práticas e estratégias no Guia do usuário dos AWS recursos de marcação e do editor de tags.

Correção

Para adicionar tags a uma autoridade de CA AWS privada, consulte Adicionar tags para sua CA privada no Guia do AWS Private Certificate Authority usuário.

Controles do Security Hub para o Amazon RDS

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Relational Database Service (Amazon RDS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, (7),, (21),, (11), (16), (20), (21), (3), (4 NIST.800-53.r5 AC-3) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`,`AWS::RDS::DBSnapshot`

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 Guia do usuário do Amazon RDS.

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 configuração PubliclyAccessible

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.3, (21), (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 SC-7, PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 3.6, PCI DSS v3.2.1/7.2.1, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : `rds-instance-public-access-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as instâncias do Amazon 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. No entanto, esse controle ainda pode gerar descobertas para esses recursos. Você pode 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`. 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. Em Acesso público, escolha 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 AWS Foundations Benchmark v1.4.0/2.3.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 SI-7 (6) NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

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 Amazon RDS.

Esse controle é destinado às instâncias de banco de dados do RDS. No entanto, 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, você poderá 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 Amazon RDS 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.

A criptografia do Amazon RDS 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 são compatíveis com a criptografia do Amazon RDS, consulte Criptografar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

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.

[RDS.4] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Regra do AWS Config : `rds-snapshot-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo do banco de dados RDS está criptografado. 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. No entanto, ele também pode gerar descobertas para os instantâneos 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, você poderá suprimi-las.

Criptografar dados em repouso reduz o risco de um usuário não autenticado ter acesso aos dados armazenados em disco. Os dados nos instantâneos do RDS 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 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.

[RDS.5] 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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : `rds-multi-az-support`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a alta disponibilidade está ativada para suas instâncias de banco de dados do RDS. O controle falhará se uma instância de banco de dados do RDS não estiver configurada com várias zonas de disponibilidade (AZs). Esse controle não se aplica às instâncias de banco de dados do RDS que fazem parte de uma implantação de cluster de banco de dados Multi-AZ.

A configuração de instâncias de banco de dados do Amazon RDS AZs ajuda a garantir 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, modifique 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.

[RDS.6] O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : `rds-enhanced-monitoring-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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. Essas mudanças no desempenho podem resultar na falta de disponibilidade dos dados. O monitoramento aprimorado fornece métricas em tempo real para o sistema operacional no qual a instância do banco de dados do RDS é executada. Um agente está instalado 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-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : `rds-cluster-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do RDS tem a proteção contra exclusão habilitada. O controle falhará se o cluster de banco de dados do RDS não tiver a proteção contra exclusão habilitada.

Esse controle é destinado às instâncias de banco de dados do RDS. No entanto, 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, você poderá 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 uma entidade não autorizada.

Quando a proteção contra exclusão estiver ativada, o cluster de banco de dados do RDS não poderá ser excluído. 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 do RDS, consulte Modificar o cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon RDS. Em Proteção contra exclusão, escolha Habilitar proteção contra exclusão.

[RDS.8] As instâncias de banco de dados do RDS deve ter a proteção contra exclusão habilitada

Requisitos relacionados: NIST.800-53.r5 CM-3, 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: `AWS::RDS::DBInstance`

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 a instância de banco de dados do RDS não tiver a proteção contra exclusão habilitada.

A ativação da proteção contra exclusão de instâncias oferece uma camada adicional de proteção contra a exclusão acidental do banco de dados ou a exclusão por uma entidade não autorizada.

Embora a proteção contra exclusão esteja ativada, uma instância de banco de dados do RDS não pode ser excluída. 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. Em Proteção contra exclusão, escolha Habilitar proteção contra exclusão.

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), 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 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

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: Alerta, auditoria, rastreamento, ouvinte
- PostgreSQL: Postgresql, atualização
- MySQL: Auditoria, Erro, Geral, SlowQuery
- MariaDB: Auditoria, Erro, Geral, SlowQuery
- SQL Server: erro, agente
- Aurora: Auditoria, erro, geral, SlowQuery
- Aurora-MySQL: auditoria, erro, geral, SlowQuery
- Aurora-postgreSQL: Postgresql

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 bancos de dados podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

Correção

Para obter informações sobre a publicação de 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.

[RDS.10] A autenticação do IAM deve ser configurada para instâncias do RDS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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: `AWS::RDS::DBInstance`

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 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.11] As instâncias do RDS devem ter backups automáticos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : `db-instance-backup-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`backupRetentionMinimum`	Período mínimo de retenção de backups em dias	Inteiro	7 para 35	7
`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 habilitar backups automatizados para uma instância de banco de dados do RDS, consulte Habilitar backups automatizados no Guia do usuário da Amazon RDS.

[RDS.12] A autenticação do IAM deve ser configurada para clusters do RDS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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: `AWS::RDS::DBCluster`

Regra do AWS Config : `rds-cluster-iam-authentication-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Amazon 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 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 IAM em um cluster de banco de dados, consulte Habilitar e desabilitar a autenticação de banco de dados do IAM no Guia do usuário do Amazon Aurora.

[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), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso: `AWS::RDS::DBInstance`

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.

As atualizações automáticas de versões secundárias atualizam periodicamente um banco de dados para versões recentes do mecanismo de banco de dados. No entanto, a atualização nem sempre inclui a versão mais recente do mecanismo de banco de dados. Se precisar manter seus bancos de dados em determinadas versões em momentos específicos, recomendamos atualizar manualmente para as versões de banco de dados necessárias de acordo com o cronograma exigido. Em casos de problemas críticos de segurança ou quando uma versão atinge sua end-of-support data, o Amazon RDS pode aplicar uma atualização de versão secundária, mesmo que você não tenha habilitado a opção de atualização automática de versão secundária. Para obter mais informações, consulte a documentação de atualização do Amazon RDS para seu mecanismo de banco de dados específico:

- Atualizações automáticas de versões secundárias do RDS for MariaDB
- Atualizações automáticas de versões secundárias do RDS for MySQL
- Atualizações automáticas de versões secundárias do RDS for PostgreSQL
- Db2 nas versões do Amazon RDS
- Atualizações de versões secundárias do Oracle
- Atualizações do mecanismo de banco de dados Microsoft SQL Server

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 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : `aurora-mysql-backtracking-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`BacktrackWindowInHours`	Número de horas para retroceder um cluster do Aurora MySQL	Duplo	`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 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : `rds-cluster-multi-az-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a alta disponibilidade está ativada para seus clusters 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 vários AZs para garantir a disponibilidade dos dados armazenados. A implantação em vários 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 seus clusters de banco de dados em vários AZs, modifique 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 mais informações, consulte Adicionar réplicas do Aurora a um cluster de banco de dados no Guia do usuário do Amazon Aurora.

[RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBCluster`

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 Amazon Aurora está configurado para copiar automaticamente tags para snapshots do cluster de banco de dados quando os snapshots são criados. O controle falhará se o cluster de banco de dados Aurora não estiver configurado para copiar automaticamente as tags para os snapshots do cluster quando os snapshots forem criados.

A identificação e o inventário de seus ativos de TI é um aspecto essencial de governança e segurança. Você precisa ter visibilidade de todos os seus clusters de banco de dados Amazon Aurora para poder avaliar sua postura de segurança e agir em possíveis áreas de fraqueza. Os snapshots de banco de dados do Aurora devem ter as mesmas tags dos clusters de banco de dados principais. No Amazon Aurora, você pode configurar um cluster de banco de dados para copiar automaticamente todas as tags do cluster para snapshots do cluster. A ativação dessa configuração garante que os DB snapshots herdem as mesmas tags que seus clusters de banco de dados principais.

> **Note**
>
> Em 30 de junho de 2025, o Security Hub alterou o título desse controle. Anteriormente, o título desse controle era: RDS DB clusters should be configured to copy tags to snapshots. O novo título reflete com mais precisão que o controle verifica somente os clusters de banco de dados Amazon Aurora.

Correção

Para obter informações sobre como configurar um cluster de banco de dados Amazon Aurora para copiar automaticamente tags para DB snapshots, consulte Modificar um cluster de banco de dados Amazon Aurora no Guia do usuário do Amazon Aurora.

[RDS.17] As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBInstance`

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 as instâncias de banco de dados RDS estão configuradas para copiar todas as tags para instantâneos quando os instantâneos são criados.

A identificação e o inventário de seus ativos de TI é um aspecto essencial de governança e segurança. Você precisa ter visibilidade de todos as instâncias de bancos de dados do RDS para avaliar seus procedimentos de segurança e atuar em possíveis pontos fracos. 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 suas instâncias 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. Selecione Copiar tags para instantâneos.

[RDS.18] As instâncias do RDS devem ser implantadas em uma VPC

Categoria: Proteger > Configuração de rede segura > Recursos na VPC

Severidade: alta

Tipo de recurso: `AWS::RDS::DBInstance`

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.

VPCs forneça vários controles de rede para proteger o acesso aos recursos do RDS. Esses controles incluem VPC Endpoints ACLs, 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.

[RDS.19] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso: `AWS::RDS::EventSubscription`

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 sobre notificações de eventos do RDS, consulte Usar a notificação de evento do Amazon RDS no Guia 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

[RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados

Requisitos relacionados: NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso: `AWS::RDS::EventSubscription`

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 instâncias 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 sobre notificações de eventos do RDS, consulte Usar a notificação de evento do Amazon RDS no Guia do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de instâncias 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

[RDS.21] 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 CA-7, Nist.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso: `AWS::RDS::EventSubscription`

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 tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento. O controle é aprovado se não houver assinaturas de eventos existentes em sua conta.

```
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 sobre notificações de eventos do RDS, consulte Usar a notificação de evento do Amazon RDS no Guia do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de grupos de parâmetros de bancos de dados 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	Todos os grupos de parâmetros
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

[RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados

Requisitos relacionados: NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso: `AWS::RDS::EventSubscription`

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 tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento. O controle é aprovado se não houver assinaturas de eventos existentes em sua conta.

```
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 sobre notificações de eventos do RDS, consulte Usar a notificação de evento do Amazon RDS no Guia do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de instâncias 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	Todos os grupos de segurança
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

[RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados

Requisitos relacionados: 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: baixa

Tipo de recurso: `AWS::RDS::DBInstance`

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. Esse controle não se aplica às instâncias do RDS que fazem parte de um cluster.

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 modificar a porta padrão 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.

[RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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.

[RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

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). Esse controle falha se o nome de usuário do administrador estiver definido com o valor padrão. O controle não se aplica aos mecanismos do tipo neptune (Neptune DB) ou docdb (DocumentDB) e às instâncias do RDS que fazem parte de um cluster.

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 de modo a reduzir o risco de acesso acidental.

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.

[RDS.26] 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 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regra: **`rds-resources-protected-by-backup-plan`**

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`backupVaultLockCheck`	O controle produz uma `PASSED` descoberta se o parâmetro estiver definido como verdadeiro e o recurso usar o AWS Backup Vault Lock.	Booleano	`true` ou `false`	Nenhum valor padrão	

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 instâncias de bancos de dados do RDS 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.

[RDS.27] Os clusters de banco de dados do RDS 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::RDS::DBCluster`

AWS Config regra: **`rds-cluster-encrypted-at-rest`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados RDS é criptografado em repouso. O controle falhará se um cluster de banco de dados do RDS 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 RDS 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

Você pode ativar a criptografia em repouso ao criar um cluster de banco de dados do RDS. Não é possível alterar as configurações de criptografia após a criação de um cluster. Para obter mais informações, consulte Criptografar um cluster de banco de dados do Amazon Aurora no Guia do usuário do Amazon Aurora.

[RDS.28] Os clusters de bancos de dados do RDS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regra: `tagged-rds-dbcluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará

apenas a existência de uma chave de tag e falhará se o cluster de banco de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 de banco de dados do RDS, consulte Marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.29] Os snapshots de cluster de bancos de dados do RDS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

AWS Config regra: `tagged-rds-dbclustersnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 de 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 verificará apenas a existência de uma chave de tag e falhará se o snapshot de cluster de banco de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 snapshot de cluster de banco de dados do RDS, consulte Marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.30] As instâncias de bancos de dados do RDS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regra: `tagged-rds-dbinstance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma instância de banco de dados do 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

verificará apenas a existência de uma chave de tag e falhará se a instância de banco de dados não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 banco de dados do RDS, consulte Marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBSecurityGroup`

AWS Config regra: `tagged-rds-dbsecuritygroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um grupo de segurança de banco de dados do Amazon RDS tem tags com chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o grupo de segurança 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 verificará apenas a existência de uma chave de tag e falhará se o grupo de segurança de banco de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 de banco de dados do RDS, consulte Marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.32] Os snapshots de banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBSnapshot`

AWS Config regra: `tagged-rds-dbsnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um snapshot de banco de dados do Amazon RDS tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o snapshot 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

verificará apenas a existência de uma chave de tag e falhará se o snapshot de banco de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 snapshot do RDS, consulte Marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.33] Os grupos de sub-redes de banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::RDS::DBSubnetGroup`

AWS Config regra: `tagged-rds-dbsubnetgroups` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 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 verificará apenas a existência de uma chave de tag e falhará se o grupo de sub-redes de banco de dados não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 banco de dados do RDS, consulte 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-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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. O controle não gera descobertas para clusters de banco de dados do Aurora Serverless v1.

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`. No entanto, 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.

[RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

Requisitos relacionados: 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), PCI DSS v4.0.1/6.3.3

Categoria: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

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 Multi-AZ do Amazon RDS. O controle falhará se a atualização automática de versões secundárias não estiver habilitada para um cluster de bancos de dados Multi-AZ.

O RDS fornece a atualização automática de versões secundárias para que você possa manter o cluster de bancos 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 automaticamente durante o período de manutenção.

Correção

Para habilitar a atualização automática de versões secundárias em clusters de banco de dados Multi-AZ, consulte Modificar um cluster de banco de dados Multi-AZ no Guia do usuário do Amazon RDS.

[RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-postgresql-logs-to-cloudwatch

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`logTypes`	Lista separada por vírgula dos tipos de registro a serem publicados no Logs CloudWatch	StringList	Não personalizável	`postgresql`

Esse controle verifica se uma instância de banco de dados Amazon RDS for PostgreSQL está configurada para publicar registros no Amazon Logs. CloudWatch O controle falhará se a instância

de banco de dados PostgreSQL não estiver configurada para publicar os tipos de log mencionados `logTypes` no parâmetro em Logs. CloudWatch

O registro em log de banco de dados fornece registros detalhados das solicitações feitas a uma instância do RDS. O PostgreSQL gera arquivos de log de eventos que contêm informações úteis para os administradores. A publicação desses registros no CloudWatch Logs centraliza o gerenciamento de registros e ajuda você a realizar análises em tempo real dos dados de registro. CloudWatch O Logs retém os registros em um armazenamento altamente durável. Você também pode criar alarmes e visualizar métricas noCloudWatch.

Correção

Para publicar registros CloudWatch da instância de banco de dados PostgreSQL no Logs, consulte Publicação de logs do PostgreSQL no Amazon Logs no Guia do usuário do CloudWatch Amazon RDS.

[RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : rds-aurora-postgresql-logs-to-cloudwatch

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Amazon Aurora PostgreSQL está configurado para publicar logs no Amazon Logs. CloudWatch O controle falhará se o cluster de banco de dados Aurora PostgreSQL não estiver configurado para publicar registros do PostgreSQL no Logs. CloudWatch

O registro em log de banco de dados fornece registros detalhados das solicitações feitas a um cluster do RDS. O PostgreSQL do Aurora gera arquivos de log de eventos que contêm informações

úteis para os administradores. A publicação desses registros no CloudWatch Logs centraliza o gerenciamento de registros e ajuda você a realizar análises em tempo real dos dados de registro. CloudWatch O Logs retém os registros em um armazenamento altamente durável. Você também pode criar alarmes e visualizar métricas no CloudWatch.

Correção

Para publicar registros do cluster de banco de dados Aurora PostgreSQL no Logs, CloudWatch consulte Publicação de logs do Aurora PostgreSQL no Amazon Logs no Guia do usuário do Amazon RDS. CloudWatch

[RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-postgres-instance-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma conexão com uma instância Amazon RDS for PostgreSQL de banco de dados (DB) está criptografada em trânsito. O controle falhará se o `rds.force_ssl` parâmetro do grupo de parâmetros associado à instância estiver definido como `0` (desativado). Esse controle não avalia as instâncias de banco de dados do RDS que fazem parte de um cluster de banco de dados.

Dados em trânsito se referem a dados que se movem de um local para outro, como entre os nós do cluster ou entre o cluster e a aplicação. Os dados podem se mover pela Internet ou em uma rede privada. Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede.

Correção

Para exigir que todas as conexões com sua instância de banco de dados RDS for PostgreSQL usem SSL, consulte Como usar SSL com uma instância de banco de dados PostgreSQL no Guia do usuário do Amazon RDS.

[RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-mysql-instance-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma conexão com uma instância Amazon RDS for MySQL de banco de dados (DB) está criptografada em trânsito. O controle falhará se o `rds.require_secure_transport` parâmetro do grupo de parâmetros associado à instância estiver definido como `0` (desativado). Esse controle não avalia as instâncias de banco de dados do RDS que fazem parte de um cluster de banco de dados.

Dados em trânsito se referem a dados que se movem de um local para outro, como entre os nós do cluster ou entre o cluster e a aplicação. Os dados podem se mover pela Internet ou em uma rede privada. Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede.

Correção

Para exigir que todas as conexões com sua instância de banco de dados RDS for MySQL usem SSL, consulte Suporte SSL/TLS para instâncias de banco de dados MySQL no Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (10), (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 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-sql-server-logs-to-cloudwatch

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`logTypes`	Uma lista dos tipos de registros que uma instância de banco de dados do RDS para SQL Server deve ser configurada para publicar no CloudWatch Logs. Esse controle falhará se uma instância de banco de dados não estiver configurada para publicar um tipo de log especificado na lista.	EnumList (máximo de 2 itens)	`agent`, `error`	`agent`, `error`

Esse controle verifica se uma instância de banco de dados Amazon RDS for Microsoft SQL Server está configurada para publicar logs no CloudWatch Amazon Logs. O controle falhará se a instância de banco de dados do RDS for SQL Server não estiver configurada para publicar registros no CloudWatch Logs. Opcionalmente, você pode especificar os tipos de registros que uma instância de banco de dados deve ser configurada para publicar.

O registro do banco de dados fornece registros detalhados das solicitações feitas a uma instância de banco de dados Amazon RDS. A publicação de registros no CloudWatch Logs centraliza o gerenciamento de registros e ajuda você a realizar análises em tempo real dos dados de log. CloudWatch O Logs retém os registros em um armazenamento altamente durável. Além disso, você pode usá-lo para criar alarmes para erros específicos que podem ocorrer, como reinicializações frequentes registradas em um registro de erros. Da mesma forma, você pode criar alarmes para erros ou avisos registrados nos logs do SQL Server Agent relacionados aos trabalhos do SQL Agent.

Correção

Para obter informações sobre a publicação de registros em CloudWatch Logs para uma instância de banco de dados RDS for SQL Server, consulte os arquivos de log do banco de dados do Amazon RDS for Microsoft SQL Server no Guia do Usuário do Amazon Relational Database Service.

[RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-sqlserver-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma conexão com uma instância de banco de dados Amazon RDS for Microsoft SQL Server está criptografada em trânsito. O controle falhará se o `rds.force_ssl` parâmetro do grupo de parâmetros associado à instância de banco de dados estiver definido como`0 (off)`.

Dados em trânsito se referem aos dados que se movem de um local para outro, como entre nós em um cluster de banco de dados ou entre um cluster de banco de dados e um aplicativo cliente. Os dados podem se mover pela Internet ou dentro de uma rede privada. A criptografia de dados em trânsito reduz o risco de usuários não autorizados espionarem o tráfego da rede.

Correção

Para obter informações sobre como habilitar SSL/TLS conexões com instâncias de banco de dados do Amazon RDS executando o Microsoft SQL Server, consulte Como usar SSL com uma instância de banco de dados Microsoft SQL Server no Guia do usuário do Amazon Relational Database Service.

[RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), (10) 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-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : mariadb-publish-logs-to-cloudwatch-logs

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`logTypes`	Uma lista dos tipos de registros que uma instância de banco de dados MariaDB deve ser configurada para publicar no Logs. CloudWatch O controle gera uma `FAILED` descoberta se uma instância de banco de dados não estiver configurada para publicar um tipo de log especificado na lista.	EnumList (máximo de 4 itens)	`audit`, `error`, `general`, `slowquery`	`audit, error`

Esse controle verifica se uma instância de banco de dados Amazon RDS for MariaDB está configurada para publicar determinados tipos de registros no Amazon Logs. CloudWatch O controle falhará se a instância de banco de dados MariaDB não estiver configurada para publicar os registros no Logs. CloudWatch Opcionalmente, você pode especificar quais tipos de registros uma instância de banco de dados MariaDB deve ser configurada para publicar.

O registro do banco de dados fornece registros detalhados das solicitações feitas a uma instância de banco de dados Amazon RDS for MariaDB. A publicação de registros no Amazon CloudWatch Logs centraliza o gerenciamento de registros e ajuda você a realizar análises em tempo real dos dados de log. Além disso, o CloudWatch Logs mantém os registros em um armazenamento durável, que pode oferecer suporte a análises e auditorias de segurança, acesso e disponibilidade. Com o CloudWatch Logs, você também pode criar alarmes e analisar métricas.

Correção

Para obter informações sobre como configurar uma instância de banco de dados Amazon RDS for MariaDB para publicar registros no Amazon Logs, consulte Publicação de registros do MariaDB no CloudWatch Amazon Logs no Guia do usuário CloudWatch do Amazon Relational Database Service.

[RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RDS::DBInstance`

Regra do AWS Config : rds-mariadb-instance-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se as conexões com uma instância de banco de dados Amazon RDS for MariaDB estão criptografadas em trânsito. O controle falhará se o grupo de parâmetros do banco de dados associado à instância de banco de dados não estiver sincronizado ou se o `require_secure_transport` parâmetro do grupo de parâmetros não estiver definido como`ON`.

> **Note**
>
> Esse controle não avalia as instâncias de banco de dados do Amazon RDS que usam versões do MariaDB anteriores à versão 10.5. O `require_secure_transport` parâmetro é suportado somente para as versões 10.5 e posteriores do MariaDB.

Dados em trânsito se referem aos dados que se movem de um local para outro, como entre nós em um cluster de banco de dados ou entre um cluster de banco de dados e um aplicativo cliente. Os

dados podem se mover pela Internet ou dentro de uma rede privada. A criptografia de dados em trânsito reduz o risco de usuários não autorizados espionarem o tráfego da rede.

Correção

Para obter informações sobre como habilitar SSL/TLS conexões com uma instância de banco de dados Amazon RDS for MariaDB, SSL/TLS consulte Exigindo todas as conexões com uma instância de banco de dados MariaDB no Guia do usuário do Amazon Relational Database Service.

[RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9) 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-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RDS::DBCluster`

Regra do AWS Config : aurora-mysql-cluster-audit-logging

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Amazon Aurora MySQL tem o registro de auditoria ativado. O controle falhará se o grupo de parâmetros do banco de dados associado ao cluster de banco de dados não estiver sincronizado, se o `server_audit_logging` parâmetro não estiver definido como ou se o `server_audit_events` parâmetro estiver definido como um valor vazio. 1

Os registros do banco de dados podem ajudar nas auditorias de segurança e acesso e ajudar a diagnosticar problemas de disponibilidade. 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.

Correção

Para obter informações sobre como habilitar o registro em log para um cluster de banco de dados Amazon Aurora MySQL, consulte Publicação de registros do Amazon Aurora MySQL no Amazon Logs CloudWatch no Guia do usuário do Amazon Aurora.

Controles do Security Hub para o Amazon Redshift

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Redshift. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21),,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20), (21) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::Redshift::Cluster`

Regra do AWS Config : redshift-cluster-public-access-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os clusters Amazon Redshift estão acessíveis 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. Quando um cluster é configurado com `PubliclyAccessible` em `true`, ele será uma instância voltada para a internet com um nome de DNS que pode ser resolvido publicamente, resultando em um endereço IP público.

Se um cluster não for acessível publicamente, ele 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 Acessível ao público como Sim.

[Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

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 `require_ssl` como verdadeiro.

[Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-13 (5)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

Regra do AWS Config : redshift-backup-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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.

[Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

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 do Amazon Redshift 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 Registros em logo de auditoria de bancos de dados no Guia de gerenciamento 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.

[Redshift.6] 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-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (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: Identificar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

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. Essas atualizações podem incluir patches de segurança e correções de erros. 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 e `--allow-version-upgrade` defina o atributo. *`clustername`*é o nome do seu cluster do Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado

Requisitos relacionados: 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 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Proteger > Configuração de rede segura > Acesso privado a API

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

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.

O roteamento aprimorado de VPC força todo o tráfego `COPY` e `UNLOAD` entre o cluster e os repositórios de dados a passar pela sua VPC. Em seguida, você pode 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.

[Redshift.8] Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

Regra do AWS Config : redshift-default-admin-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon Redshift 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 cluster do Redshift, 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

Você não pode alterar o nome de usuário do administrador do cluster do Amazon Redshift depois que ele é criado. Para criar um novo cluster com um nome de usuário não padrão, consulte Etapa 1: Criar uma amostra de cluster do Amazon Redshift no Guia de conceitos básicos do Amazon Redshift.

[Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

Regra do AWS Config : redshift-default-db-name-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon Redshift alterou o nome do banco de dados de seu valor padrão. Esse controle falhará se o nome do banco de dados de um cluster do Redshift estiver definido como `dev`

Ao criar um cluster do Redshift, você deve alterar o nome do banco de dados padrão para um valor exclusivo. Os nomes 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 nome do banco de dados do seu cluster do Amazon Redshift depois que ele é criado. Para instruções sobre a criação de novo cluster, 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

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, pois ela adiciona uma camada de gerenciamento de acesso aos seus dados. Criptografar clusters Redshift 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Redshift::Cluster`

Regra AWS Config : `tagged-redshift-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Redshift, consulte Marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.12] As notificações de assinatura de notificações eventos do Redshift devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Redshift::EventSubscription`

Regra AWS Config : `tagged-redshift-eventsubscription` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um snapshop de cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o snapshot de 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 snapshot de cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 notificação de eventos do Redshift, consulte Marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.13] Os snapshots de cluster do Redshift devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Redshift::ClusterSnapshot`

Regra AWS Config : `tagged-redshift-clustersnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se um snapshop de cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o snapshot de 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 snapshot de cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 snapshot de cluster do Redshift, consulte Marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.14] Os grupos de sub-redes de cluster do Redshift devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Redshift::ClusterSubnetGroup`

Regra AWS Config : `tagged-redshift-clustersubnetgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se o grupo de sub-redes de cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o grupo de sub-redes de 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 grupo de sub-redes de cluster não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 cluster do Redshift, consulte Marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas

Requisitos relacionados: PCI DSS v4.0.1/1.3.1

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso: `AWS::Redshift::Cluster`

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 privilégio mínimo 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 as regras nas quais o intervalo de portas corresponda à porta do cluster do Redshift e o intervalo de portas IP seja 0.0.0.0/0.

[Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Redshift::ClusterSubnetGroup`

Regra do AWS Config : redshift-cluster-subnet-group-multi-az

Tipo de programação: acionado por alterações

Parâmetros: nenhum

O controle verifica se um grupo de sub-redes do cluster Amazon Redshift tem sub-redes de mais de uma zona de disponibilidade (AZ). O controle falhará se o grupo de sub-redes do cluster não tiver sub-redes de pelo menos duas sub-redes diferentes. AZs

A configuração de sub-redes em várias AZs ajuda a garantir que seu data warehouse do Redshift possa continuar operando mesmo quando ocorrerem eventos de falha.

Correção

Para modificar um grupo de sub-redes de cluster do Redshift para abranger vários AZs, consulte Modificação de um grupo de sub-redes de cluster no Guia de gerenciamento do Amazon Redshift.

[Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Redshift::ClusterParameterGroup`

Regra do AWS Config : redshift-cluster-parameter-group-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um grupo de parâmetros de cluster do Amazon Redshift tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o grupo de parâmetros não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags`

parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o grupo de parâmetros não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre a adição de tags a um grupo de parâmetros de cluster do Amazon Redshift, consulte Recursos de tags no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster`

Regra do AWS Config : redshift-cluster-multi-az-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se várias implantações de zonas de disponibilidade (Multi-AZ) estão habilitadas para um cluster do Amazon Redshift. O controle falhará se as implantações Multi-AZ não estiverem habilitadas para o cluster Amazon Redshift.

O Amazon Redshift oferece suporte a várias implantações de zonas de disponibilidade (Multi-AZ) para clusters provisionados. Se as implantações Multi-AZ estiverem habilitadas para um cluster, um data warehouse do Amazon Redshift poderá continuar operando em cenários de falha quando um evento inesperado acontecer em uma zona de disponibilidade (AZ). Uma implantação Multi-AZ implanta recursos computacionais em mais de uma AZ e esses recursos computacionais podem ser acessados por meio de um único endpoint. No caso de uma falha completa da AZ, os recursos computacionais restantes em outra AZ estão disponíveis para continuar processando as cargas de trabalho. Você pode converter um data warehouse Single-AZ existente em um data warehouse Multi-AZ. Recursos computacionais adicionais são então provisionados em uma segunda AZ.

Correção

Para obter informações sobre a configuração de implantações Multi-AZ para um cluster do Amazon Redshift, consulte Convertendo um data warehouse Single-AZ em um data warehouse Multi-AZ no Guia de Gerenciamento do Amazon Redshift.

Controles do Security Hub sem servidor

Esses AWS Security Hub controles do avaliam o serviço e os recursos do Amazon Redshift sem servidor. Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC

Categoria: Proteger > Configuração de rede segura > Recursos na VPC

Severidade: alta

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regra do AWS Config : redshift-serverless-workgroup-routes-within-vpc

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o roteamento aprimorado da VPC está habilitado para um grupo de trabalho do Amazon Redshift sem servidor. O controle falhará se o roteamento aprimorado da VPC for desabilitado para o grupo de trabalho.

Se o roteamento aprimorado da VPC estiver desabilitado para um grupo de trabalho do Amazon Redshift sem servidor, o Amazon Redshift sem servidor, o Amazon Redshift Serverless, incluindo o tráfego para outros serviços na rede. AWS Se você habilitar o roteamento aprimorado da VPC para um grupo de trabalho, o Amazon Redshift forçará todo o `UNLOAD` tráfego entre seu cluster `COPY` e seus repositórios de dados por meio de sua Virtual Private Cloud (VPC) com base no serviço Amazon VPC. Com o roteamento aprimorado da VPC, você pode usar os recursos da VPC padrão para controlar o fluxo de dados entre seu cluster do Amazon Redshift e outros recursos. Isso inclui recursos como grupos de segurança de VPC e políticas de endpoint, listas de controle de acesso à rede (ACLs) e servidores de Sistema de Nomes de Domínio (DNS). Você também pode usar os logs de fluxo da VPC para monitorar `COPY` e `UNLOAD` trafegar.

Correção

Para obter mais informações sobre o roteamento de VPC aprimorado e como habilitá-lo para um grupo de trabalho, consulte Controlando o tráfego de rede com o roteamento de VPC aprimorado do Redshift no Guia de Gerenciamento do Amazon Redshift.

[RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL

Categoria: Proteger > Proteção > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regra do AWS Config : redshift-serverless-workgroup-encrypted-in-transit

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se as conexões com um grupo de trabalho do Amazon Redshift sem servidor são necessárias para criptografar os dados em trânsito. O controle falhará se o parâmetro `require_ssl` de configuração do grupo de trabalho estiver definido como. `false`

Um grupo de trabalho do Amazon Redshift sem servidor é uma coleção de recursos de computação que agrupa recursos de computação, como grupos de sub-redes da RPUs VPC e grupos de

segurança. As propriedades de um grupo de trabalho incluem configurações de rede e segurança. Essas configurações especificam se as conexões com um grupo de trabalho devem ser obrigadas a usar SSL para criptografar dados em trânsito.

Correção

Para obter informações sobre como atualizar as configurações de um grupo de trabalho sem servidor do Amazon Redshift para exigir conexões SSL, consulte Conectando-se ao Amazon Redshift Serverless no Guia de gerenciamento do Amazon Redshift.

[RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regra do AWS Config : redshift-serverless-workgroup-no-public-access

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o acesso público está desabilitado para um grupo de trabalho do Amazon Redshift sem servidor. Ele avalia a `publiclyAccessible` propriedade de um grupo de trabalho do Redshift sem servidor. O controle falhará se o acesso público estiver habilitado (`true`) para o grupo de trabalho.

A configuração de acesso público (`publiclyAccessible`) para um grupo de trabalho do Amazon Redshift sem servidor especifica se o grupo de trabalho pode ser acessado de uma rede pública. Se o acesso público estiver habilitado (`true`) para um grupo de trabalho, o Amazon Redshift cria um endereço IP elástico que torna o grupo de trabalho acessível publicamente de fora da VPC. Se você não quiser que um grupo de trabalho seja acessível ao público, desative o acesso público a ele.

Correção

Para obter informações sobre como alterar a configuração de acesso público para um grupo de trabalho sem servidor do Amazon Redshift, consulte Visualização das propriedades de um grupo de trabalho no Guia de gerenciamento do Amazon Redshift.

[RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys

Requisitos relacionados: 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-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SI-7 (6)

Categoria: Proteger > Proteção > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regra do AWS Config : redshift-serverless-namespace-cmk-encryption

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`kmsKeyArns`	Uma lista de nomes de recursos da Amazon (ARNs) AWS KMS keys a serem incluídos na avaliação. O controle gera uma `FAILED` descoberta se um namespace Redshift Serverless não estiver criptografado com uma	StringList (máximo de 3 itens)	1—3 ARNs das chaves KMS existentes. Por exemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	chave KMS na lista.			

Esse controle verifica se um namespace do Amazon Redshift sem servidor é criptografado em repouso com um cliente gerenciado. AWS KMS key O controle falhará se o namespace Redshift Serverless não for criptografado com uma chave KMS gerenciada pelo cliente. Opcionalmente, você pode especificar uma lista de chaves KMS para o controle incluir na avaliação.

No Amazon Redshift Serverless, um namespace define um contêiner lógico para objetos de banco de dados. Esse controle verifica periodicamente se as configurações de criptografia de um namespace especificam uma chave KMS gerenciada pelo cliente AWS KMS key, em vez de uma chave AWS gerenciada do KMS, para criptografia de dados no namespace. Com uma chave do KMS gerenciada pelo cliente, você tem controle total da chave. Isso inclui definir e manter a política de chaves, gerenciar concessões, alternar material criptográfico, atribuir tags, criar aliases e ativar e desativar a chave.

Correção

Para obter informações sobre a atualização das configurações de criptografia de um namespace sem servidor do Amazon Redshift e a especificação de um cliente gerenciado AWS KMS key, consulte Alteração de um AWS KMS key namespace no Guia de gerenciamento do Amazon Redshift.

[RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regra do AWS Config : redshift-serverless-default-admin-check

Tipo de programação: Periódico

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`validAdminUserNames`	Uma lista de nomes de usuário administrativos que os namespaces do Redshift Serverless devem usar. O controle gera uma `FAILED` descoberta se um namespace usa um nome de usuário de administrador que não está na lista. A lista não pode especificar o valor padrão,`admin`.	StringList (máximo de 6 itens)	1—6 nomes de usuário administrativos válidos para namespaces Redshift Serverless.	Nenhum valor padrão

Esse controle verifica se o nome de usuário do administrador de um namespace Amazon Redshift Serverless é o nome de usuário padrão do administrador,. `admin` O controle falhará se o nome de usuário do administrador do namespace Redshift Serverless for. `admin` Você pode opcionalmente especificar uma lista de nomes de usuário do administrador para o controle incluir na avaliação.

Ao criar um namespace Amazon Redshift Serverless, você deve especificar um nome de usuário de administrador personalizado para o namespace. O nome de usuário padrão do administrador é de conhecimento público. Ao especificar um nome de usuário de administrador personalizado, você pode, por exemplo, ajudar a reduzir o risco ou a eficácia dos ataques de força bruta contra o namespace.

Correção

Você pode alterar o nome de usuário do administrador de um namespace Amazon Redshift Serverless usando o console ou a API do Amazon Redshift Serverless. Para alterá-lo usando o console, escolha a configuração do namespace e escolha Editar credenciais de administrador no menu Ações. Para alterá-la programaticamente, use a UpdateNamespaceoperação ou, se estiver usando a AWS CLI, execute o comando update-namespace. Se você alterar o nome de usuário do administrador, também deverá alterar a senha do administrador ao mesmo tempo.

[RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regra do AWS Config : redshift-serverless-publish-logs-to-cloudwatch

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um namespace do Amazon Redshift sem servidor está configurado para exportar logs de conexão e usuário para o Amazon Logs. CloudWatch O controle falhará se o namespace do Redshift sem servidor não estiver configurado para exportar os logs para o Logs. CloudWatch

Se você configurar o Amazon Redshift Serverless para exportar dados de log de conexão (`connectionlog`) e log de usuário (`userlog`) para um grupo de log no Amazon CloudWatch Logs, poderá coletar e armazenar seus registros de log em armazenamento durável, que pode oferecer suporte a análises e auditorias de segurança, acesso e disponibilidade. Com o CloudWatch Logs, é possível realizar análise em tempo real de dados e usar o CloudWatch para criar alarmes e analisar métricas.

Correção

Para exportar os dados de log de um Amazon Redshift sem servidor para o Amazon CloudWatch Logs, os respectivos logs deverão ser selecionados para exportação nas configurações de log de auditoria do namespace. Para obter informações sobre a atualização dessas configurações, consulte Edição de segurança e criptografia no Guia de gerenciamento do Amazon Redshift.

[RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regra do AWS Config : redshift-serverless-default-db-name-check

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um namespace sem servidor do Amazon Redshift usa o nome do banco de dados padrão,. `dev` O controle falhará se o namespace Redshift Serverless usar o nome padrão do banco de dados,. `dev`

Ao criar um namespace Amazon Redshift Serverless, você deve especificar um valor exclusivo e personalizado para o nome do banco de dados e não usar o nome padrão do banco de dados, que é. `dev` O nome do banco de dados padrão é de conhecimento público. Ao especificar um nome de banco de dados diferente, você pode reduzir riscos, como usuários não autorizados obterem acesso inadvertidamente aos dados no namespace.

Correção

Você não pode alterar o nome do banco de dados de um Amazon Redshift sem servidor depois de criar o namespace. No entanto, você pode especificar um nome de banco de dados personalizado para um namespace Redshift Serverless ao criar o namespace. Para obter informações sobre a criação de um namespace, consulte Grupos de trabalho e namespaces no Guia de gerenciamento do Amazon Redshift.

Controles do Security Hub para o Route 53

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Route 53.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[Route53.1] As verificações de integridade do Route 53 devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Route53::HealthCheck`

AWS Config regra: `tagged-route53-healthcheck` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma verificação de integridade 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 de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags

às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 integridade do Route 53, consulte Nomear e adicionar tags às verificações de integridade no Guia do desenvolvedor do Amazon Route 53.

[Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, 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 CA-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Route53::HostedZone`

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 não estiver habilitado para uma zona hospedada pública do 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.

Controles do Security Hub para o Amazon S3

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Simple Storage Service (Amazon S3). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 habilitadas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11) NIST.800-53.r5 AC-3, (16), (20) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (3), (4) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1 v3.2.1/1.3.2, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS:::Account`

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 bloqueio de acesso público do Amazon S3 estão configuradas ao nível da conta para o bucket de uso geral do S3. O controle falhará se uma ou mais configurações de bloqueio de acesso público 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 é concedido a buckets e objetos por meio de listas de controle de acesso (ACLs), políticas de bucket ou ambas.

A menos que você queira que os buckets do S3 sejam acessíveis publicamente, configure o recurso Acesso público de bloco do Amazon S3 no nível da conta.

Para obter mais informações, consulte Usar o bloqueio de acesso público do Amazon S3 no Guia do usuário 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 para leitura

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),, (11), (16), (20), (21), (3), (4)) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::S3::Bucket`

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 para 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 para leitura.

> **Note**
>
> Se um bucket do S3 tiver uma política de bucket, esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política do bucket devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

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 bloqueio de acesso público para seu bucket S3 do Amazon S3, consulte Configurar bloqueio do acesso público aos seus buckets S3 no Guia do usuário do Amazon Simple Storage Service.

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público para gravação

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, 1,, (7), (21),, (11), (16), (20)), (21), (3), (4), (9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso: `AWS::S3::Bucket`

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 para 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 para gravação.

> **Note**
>
> Se um bucket do S3 tiver uma política de bucket, esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política do bucket devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

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 bloqueio de gravação pública para seu bucket S3 do Amazon S3, consulte Configurar bloqueio do acesso público aos seus buckets S3 no Guia do usuário do Amazon Simple Storage Service.

[S3.5] Os buckets de uso geral do S3 devem exigir que as solicitações usem SSL

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.1, CIS AWS Foundations Benchmark v1.4.0/2.1.2, NIST.800-53.r5 AC-1 7 (2), (1), 2 (3), 3, 3, 3 (3), (4),, (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-1 NIST.800-171.r2 3.13.8, NIST.800-53.r5 SC-7 Nist.800.R2 3.13.8 800-171.r2 3.13.15,

NIST.800-53.r5 SC-8 PCI DSS v3.2.1/4.1, PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

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.

Adicione uma declaração de política semelhante à da política a seguir. Substitua `amzn-s3-demo-bucket` pelo nome do bucket que você está modificando.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-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

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

Categoria: Proteger > Gerenciamento de acesso seguro > Ações de operações de API confidenciais restritas

Severidade: alta

Tipo de recurso: `AWS::S3::Bucket`

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 a política de bucket de uso geral do Amazon S3 impede que as entidades principais de outras Contas da AWS executem ações negadas em recursos de bucket do S3. O controle falhará se a política de bucket permitir alguma das ações anteriores para uma entidade principal em outra Conta da AWS.

A implementação do privilégio de acesso mínimo é fundamental para reduzir o risco de segurança e o impacto 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 remover permissões, 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

Requisitos relacionados: PCI DSS v3.2.1/2.2, NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-3 6 (2), (2), NIST.800-53.r5 NIST.800-53.r5 SC-5 SI-13 (5)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso: `AWS::S3::Bucket`

AWS Config regra: s3-bucket-cross-region-replication-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o bucket de uso geral do Amazon S3 tem a replicação entre regiões habilitada. O controle falhará se o bucket não tiver a replicação entre regiões habilitada.

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.

Esse controle produzirá uma descoberta `FAILED` para um bucket de destino de replicação se ele não tiver a replicação entre regiões habilitada. Se houver um motivo legítimo para o bucket de destino não precisar ter a replicação entre regiões habilitada, você poderá suprimir descobertas para esse bucket.

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, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21) NIST.800-53.r5 AC-3,,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI NIST.800-53.r5 SC-7 DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoria: Proteger > Gerenciamento de acesso seguro > Controle de acesso

Severidade: alta

Tipo de recurso: `AWS::S3::Bucket`

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 permite acesso público ao nível do bucket. O controle falhará se alguma das seguintes configurações estiver definida como `false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

O bloqueio de acesso público no nível do bucket do S3 oferece controles para garantir que os objetos nunca tenham acesso público. O acesso público é concedido a buckets e objetos por meio de listas de controle de acesso (ACLs), políticas de bucket ou ambas.

A menos que você queira que os buckets do S3 sejam acessíveis publicamente, configure o recurso Bloqueio de acesso público do Amazon S3 no nível do bucket.

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 em log de acesso ao servidor habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.3.8, PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : s3-bucket-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro em log de acesso ao servidor está habilitado para buckets de uso geral do S3. Esse controle falhará se o registro em log de acesso ao servidor não estiver habilitado. 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 registros detalhados 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 em log de acesso ao servidor Amazon S3, consulte Habilitar registro em log de acesso ao servidor do Amazon S3 no Guia do usuário do Amazon S3.

[S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

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 o bucket do S3 para ajudar 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 habilitadas

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4), Nist.800-171.r2 3.3.8

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : s3-event-notifications-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpira`	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			tion:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:Object	

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			`Removed:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replic`	

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			`ation: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 parâmetro `eventTypes`, o controle será aprovado somente se as notificações de eventos estiverem habilitadas para os tipos de eventos especificados.

Quando habilita as notificações de eventos do S3, você recebe alertas quando ocorrem eventos específicos que afetam seus buckets do S3. Por exemplo, você pode 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] não ACLs deve ser usado para gerenciar o acesso do usuário aos buckets de uso geral do S3

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) 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 > Controle de acesso

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

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 de usuários nos buckets do S3.

ACLs são mecanismos legados de controle de acesso anteriores ao IAM. Em vez disso 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 desabilitar ACLs seus buckets do S3. Para obter instruções, consulte Controle da propriedade de objetos e desativação ACLs do seu bucket no Guia do usuário do Amazon Simple Storage Service.

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

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Proteger > Proteção de dados

Severidade: baixa

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : s3-lifecycle-policy-check

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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`,	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			`GLACIER_IR, DEEP_ARCHIVE`	

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 o bucket do S3 define as ações que você deseja que o Amazon S3 realize durante a vida útil de um objeto. Por exemplo, é possível fazer 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 políticas de 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 no Guia do usuário do Amazon S3.

[S3.14] Os buckets de uso geral do S3 devem ter o versionamento habilitado

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Requisitos relacionados: NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.3.8

Severidade: baixa

Tipo de recurso: `AWS::S3::Bucket`

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 habilitado. O controle falhará se o versionamento for suspenso para o bucket.

O versionamento mantém diversas variantes de um objeto no mesmo bucket do S3. Você pode usar o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do S3. O versionamento 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 versionamento, 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 de objetos versionados no 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 Bloqueio de Objetos habilitado

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Requisitos relacionados: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0.1/10.5.1

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : s3-bucket-default-lock-enabled

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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 Bloqueio de Objetos habilitado. O controle falhará se o Bloqueio de Objetos 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 em buckets S3 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

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Requisitos relacionados: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), (1), NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6), NIST.800-53.r5 CA-9 NIST.800-53.r5 NIST.800-53.r5 SC-2 AU-9, NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11, NIST.800-171.r2 3.13.16, PCI DSS v4.0.1/3.5.1

Severidade: média

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : 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 do S3 for criptografado com a 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-2 1, 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 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::S3::AccessPoint`

Regra do AWS Config : 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 AWS Foundations Benchmark v1.4.0/2.1.3, (1), (2) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso: `AWS::S3::Bucket`

Regra do AWS Config : 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 para um bucket de uso geral do Amazon S3. O controle falhará se a exclusão de MFA não estiver habilitada para o bucket. O controle não produz descobertas para buckets que têm uma configuração de ciclo de vida.

Se você habilitar o controle de versão para um bucket de uso geral do S3, poderá, opcionalmente, adicionar outra camada de segurança configurando a exclusão de MFA para o bucket. Se você fizer isso, o proprietário do bucket deverá incluir duas formas de autenticação em qualquer solicitação para excluir uma versão de um objeto no bucket ou alterar o estado de versionamento do bucket. A exclusão de MFA fornece segurança adicional se, por exemplo, as credenciais de segurança do proprietário do bucket forem comprometidas. A exclusão de MFA também pode ajudar a evitar exclusões acidentais de intervalos, exigindo que o usuário que inicia a ação de exclusão prove a posse física de um dispositivo de MFA com um código de MFA, o que adiciona uma camada extra de atrito e segurança à ação de exclusão.

> **Note**
>
> Esse controle produz uma `PASSED` descoberta somente se a exclusão de MFA estiver habilitada para o bucket de uso geral do S3. Para habilitar a exclusão de MFA para um bucket, o versionamento também deve ser habilitado para o bucket. O controle de versão do bucket é um método de armazenar várias variações de um objeto do S3 no mesmo bucket. Além disso, somente o proprietário do bucket que está conectado como usuário root pode ativar a exclusão do MFA e realizar ações de exclusão no bucket. Você não pode usar o MFA delete com um bucket que tenha uma configuração de ciclo de vida.

Correção

Para obter informações sobre como ativar o controle de versão e configurar a exclusão de MFA para um bucket do S3, consulte Como configurar a exclusão de MFA no Guia do usuário do Amazon Simple Storage Service.

[S3.22] Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.8, PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::::Account`

Regra do AWS Config : 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 nenhuma trilha multirregional que registre eventos de dados de gravação para buckets do S3.

As operações ao nível do objeto do S3, como `GetObject`, `DeleteObject` e `PutObject`, são denominadas 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. Quando você habilita registro em log ao nível do objeto, pode registrar em log 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 produzirá uma descoberta `PASSED` se você configurar uma trilha multirregional que registre em log os eventos apenas de gravação ou todos os tipos de eventos de dados em 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 em log os eventos de leitura ao nível do objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.9, PCI DSS v4.0.1/10.2.1

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::::Account`

Regra do AWS Config : 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 nenhuma trilha multirregional que registre eventos de dados de leitura para buckets do S3.

As operações ao nível do objeto do S3, como `GetObject`, `DeleteObject` e `PutObject`, são denominadas 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. Quando você habilita o registro em log de eventos de dados de leitura ao nível do objeto, pode registrar em log 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 produzirá uma descoberta `PASSED` se você configurar uma trilha multirregional que registre em log os eventos apenas de leitura ou todos os tipos de eventos de dados em 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.

[S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas

Requisitos relacionados: PCI DSS v4.0.1/1.4.4

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::S3::MultiRegionAccessPoint`

Regra AWS Config : `s3-mrap-public-access-blocked` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um ponto de acesso multirregional do Amazon S3 tem configurações de bloqueio de acesso público habilitadas. O controle falhará quando o ponto de acesso multirregional não tiver as configurações de bloqueio de acesso público habilitadas.

Recursos publicamente acessíveis podem levar a acesso não autorizado, violações de dados ou exploração de vulnerabilidades. Restringir o acesso por meio de medidas de autenticação e autorização ajuda a proteger as informações confidenciais e a manter a integridade dos recursos.

Correção

Por padrão, todas as configurações de bloqueio de acesso público são habilitadas para pontos de acesso multirregionais. Para obter mais informações, consulte Bloqueio de acesso público de pontos de acesso multirregionais do Amazon S3 no Guia do usuário do Amazon Simple Storage Service. Você não pode alterar as configurações de bloqueio de acesso público de um ponto de acesso multirregional após a criação dele.

[S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida

Categoria: Proteger > Proteção de dados

Severidade: baixa

Tipo de recurso: `AWS::S3Express::DirectoryBucket`

Regra do AWS Config : s3express-dir-bucket-lifecycle-rules-check

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`targetExpirationDays`	O número de dias, após a criação do objeto, em que os objetos devem expirar.	Inteiro	1 para 2147483647	Nenhum valor padrão

Esse controle verifica se as regras de ciclo de vida estão configuradas para um bucket de diretório do S3. O controle falhará se as regras de ciclo de vida não estiverem configuradas para o bucket do diretório ou se uma regra de ciclo de vida para o bucket especificar configurações de expiração que não correspondam ao valor do parâmetro que você especifica opcionalmente.

No Amazon S3, uma configuração de ciclo de vida é um conjunto de regras que definem ações para o Amazon S3 serem aplicadas a um grupo de objetos em um bucket. Para um bucket de diretório do S3, você pode criar uma regra de ciclo de vida que especifica quando os objetos expiram com base na idade (em dias). Você também pode criar uma regra de ciclo de vida que exclua carregamentos incompletos de várias partes. Diferentemente de outros tipos de buckets S3, como buckets de uso geral, os buckets de diretório não oferecem suporte a outros tipos de ações para regras de ciclo de vida, como a transição de objetos entre classes de armazenamento.

Correção

Para definir uma configuração de ciclo de vida para um bucket de diretório do S3, crie uma regra de ciclo de vida para o bucket. Para obter mais informações, consulte Criação e gerenciamento de uma configuração de ciclo de vida para seu bucket de diretórios no Guia do usuário do Amazon Simple Storage Service.

Controles do Security Hub para SageMaker IA

Esses AWS Security Hub controles avaliam o serviço e os recursos de SageMaker IA da Amazon. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21),,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

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 notebook SageMaker AI. O controle falhará se o campo `DirectInternetAccess` estiver habilitado para a instância de notebook.

Se você configurar sua instância de SageMaker IA 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, a 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 SageMaker AI Developer Guide. Você também deve garantir que o acesso à sua configuração de SageMaker IA seja limitado somente aos usuários autorizados. Restrinja as permissões do IAM que permitem que os usuários alterem as configurações e os recursos de SageMaker IA.

Correção

Você não pode alterar a configuração do acesso à internet depois de criar uma instância do notebook. Em vez disso, você pode 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 AI 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-2 1 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 na VPC

Severidade: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regra do AWS Config : sagemaker-notebook-instance-inside-vpc

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância de notebook Amazon SageMaker AI é executada em uma nuvem privada virtual (VPC) personalizada. Esse controle falhará se uma instância do notebook de SageMaker IA não for iniciada em uma VPC personalizada ou se for iniciada na VPC do serviço de SageMaker IA.

Sub-redes são intervalos 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 de suas instâncias de SageMaker AI Studio e notebook.

Correção

Você não pode alterar a configuração da VPC depois de criar uma instância do notebook. Em vez disso, você pode parar, excluir e recriar a instância. Para obter instruções, consulte Usar instâncias de notebook para criar modelos: Limpeza no Amazon SageMaker AI Developer Guide.

[SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

Requisitos relacionados: 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 > Restrições de acesso do usuário raiz

Severidade: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

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 notebook Amazon SageMaker AI. O controle falhará se o acesso root estiver ativado para uma instância de notebook de SageMaker IA.

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 notebook SageMaker AI, consulte Controlar o acesso root a uma instância do notebook SageMaker AI no Amazon SageMaker AI 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-3 6, NIST.800-53.r5 SA-1 3

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso: `AWS::SageMaker::EndpointConfig`

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 endpoint de SageMaker IA 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.

As variantes de produção executadas com uma contagem de instâncias maior que 1 permitem a redundância de instâncias Multi-AZ gerenciada pela IA. 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 na instância.

Correção

Para obter mais informações sobre os parâmetros da configuração do endpoint, consulte Criar uma configuração de endpoint no Amazon SageMaker AI Developer Guide.

[SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: média

Tipo de recurso: `AWS::SageMaker::Model`

Regra do AWS Config : sagemaker-model-isolation-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um modelo hospedado pela Amazon SageMaker AI tem o isolamento de rede ativado. O controle falhará se o `EnableNetworkIsolation` parâmetro do modelo hospedado estiver definido como`False`.

SageMaker O treinamento de IA e os contêineres de inferência implantados são habilitados para a Internet por padrão. Se você não quiser que a SageMaker IA forneça acesso externo à rede aos seus contêineres de treinamento ou inferência, você pode ativar o isolamento da rede. Se você habilitar o isolamento de rede, nenhuma chamada de rede de entrada ou saída poderá ser feita de ou para o contêiner do modelo, incluindo chamadas de ou para outros. Serviços da AWS Além disso, nenhuma AWS credencial é disponibilizada para o ambiente de execução do contêiner. Ativar o isolamento da rede ajuda a impedir o acesso não intencional aos seus recursos de SageMaker IA pela Internet.

> **Note**
>
> Em 13 de agosto de 2025, o Security Hub alterou o título e a descrição desse controle. O novo título e a descrição refletem com mais precisão que o controle verifica a configuração do `EnableNetworkIsolation` parâmetro dos modelos hospedados pela Amazon

SageMaker AI. Anteriormente, o título desse controle era: SageMaker models should block inbound traffic.

Correção

Para obter mais informações sobre isolamento de rede para modelos de SageMaker IA, consulte Executar contêineres de treinamento e inferência no modo sem internet no Amazon SageMaker AI Developer Guide. Ao criar um modelo, você pode ativar o isolamento de rede definindo o valor do `EnableNetworkIsolation` parâmetro como`True`.

[SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SageMaker::AppImageConfig`

Regra do AWS Config : sagemaker-app-image-config-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma configuração de imagem do aplicativo Amazon SageMaker AI (`AppImageConfig`) tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro.

O controle falhará se a configuração da imagem do aplicativo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a configuração da imagem do aplicativo não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para adicionar tags a uma configuração de imagem do aplicativo Amazon SageMaker AI (`AppImageConfig`), você pode usar a AddTagsoperação da API SageMaker AI ou, se estiver usando a AWS CLI, executar o comando add-tags.

[SageMaker.7] SageMaker as imagens devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SageMaker::Image`

Regra do AWS Config : sagemaker-image-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se uma imagem do Amazon SageMaker AI tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se a imagem não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se a imagem não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para adicionar tags a uma imagem de SageMaker IA da Amazon, você pode usar a AddTagsoperação da API de SageMaker IA ou, se estiver usando a AWS CLI, executar o comando add-tags.

[SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regra do AWS Config : sagemaker-notebook-instance-platform-version

Tipo de programação: Periódico

Parâmetros:

- `supportedPlatformIdentifierVersions`: `notebook-al2-v3` (não personalizável)

Esse controle verifica se uma instância do notebook Amazon SageMaker AI está configurada para ser executada em uma plataforma compatível, com base no identificador da plataforma especificado para a instância do notebook. O controle falhará se a instância do notebook estiver configurada para ser executada em uma plataforma que não é mais suportada.

Se a plataforma de uma instância de notebook Amazon SageMaker AI não for mais suportada, ela poderá não receber patches de segurança, correções de bugs ou outros tipos de atualizações. As instâncias do notebook podem continuar funcionando, mas não receberão atualizações de segurança de SageMaker IA nem correções críticas de bugs. Você assume os riscos associados ao uso de uma plataforma sem suporte. Para obter mais informações, consulte o controle de JupyterLabversão no Amazon SageMaker AI Developer Guide.

Correção

Para obter informações sobre as plataformas que a Amazon SageMaker AI suporta atualmente e como migrar para elas, consulte as instâncias do notebook Amazon Linux 2 no Amazon SageMaker AI Developer Guide.

Controles do Security Hub para o Secrets Manager

Esses AWS Security Hub controles avaliam o AWS Secrets Manager serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter 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 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso: `AWS::SecretsManager::Secret`

Regra do AWS Config : `secretsmanager-rotation-enabled-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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. O Secrets inclui credenciais de banco de dados, senhas, chaves de API de terceiros. Você pode 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. Você pode 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 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso: `AWS::SecretsManager::Secret`

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` for `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. O Secrets inclui credenciais de banco de dados, senhas, chaves de API de terceiros. Você pode 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. Você pode 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 Secrets Manager, use 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 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::SecretsManager::Secret`

Regra do AWS Config : `secretsmanager-secret-unused`

Tipo de programação: Periódico

Parâmetros:

Parameter	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 prazo 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 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso: `AWS::SecretsManager::Secret`

Regra do AWS Config : `secretsmanager-secret-periodic-rotation`

Tipo de programação: Periódico

Parâmetros:

Parameter	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. Exemplos incluem 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.

Você pode configurar a alternância automática para segredos no AWS Secrets Manager. Com a alternância automática, você pode substituir os segredos de longo prazo por outros de curto prazo, reduzindo significativamente o risco de comprometimento. Recomendamos que você configure uma programação de alternância automática para seus segredos do Secrets Manager. 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SecretsManager::Secret`

Regra AWS Config : `tagged-secretsmanager-secret` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o segredo não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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.

Controles do Security Hub para AWS Service Catalog

Esse AWS Security Hub controle avalia o AWS Service Catalog serviço e os recursos. O controle pode não estar disponível em todos Regiões da AWS. Para obter 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: `AWS::ServiceCatalog::Portfolio`

Regra do AWS Config : service-catalog-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 falhará se os portfólios não forem compartilhados dentro de uma organização.

O compartilhamento de portfólio apenas dentro de organizações ajuda a garantir que um portfólio não seja compartilhado com Contas da AWS incorretas. 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 controlando o acesso concedido à conta em toda a organização. Se houver uma necessidade comercial de compartilhar os portfólios do Service Catalog com uma conta externa, você poderá suprimir automaticamente as descobertas desse controle ou desabilitá-lo.

Correção

Para habilitar o compartilhamento de portfólio com AWS Organizations, consulte Compartilhamento com AWS Organizations no Guia AWS Service Catalog do Administrador.

Controles do Security Hub para o Amazon SES

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Simple Email Service (Amazon SES).

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[SES.1] As listas de contatos do SES devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SES::ContactList`

Regra AWS Config: `tagged-ses-contactlist` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um agente do Amazon SES tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se o contato 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 contato não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 lista de contatos do Amazon SES, consulte TagResourcena Referência da API v2 do Amazon SES.

[SES.2] Os conjuntos de configuração do SES devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SES::ConfigurationSet`

Regra AWS Config: `tagged-ses-configurationset` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 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 verificará apenas a existência de uma chave de tag e falhará se o conjunto de configurações não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 conjunto de configurações do Amazon SES, consulte TagResourcena Referência da API v2 do Amazon SES.

Controles do Security Hub para o Amazon SNS

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Simple Notification Service (Amazon SNS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-26), NIST.800-171.r2 3.13.11, NIST.800-171.r2 3.13.16

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::SNS::Topic`

Regra do AWS Config : `sns-encrypted-kms`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um tópico do Amazon SNS é criptografado em repouso usando chaves gerenciadas no AWS Key Management Service (AWS KMS). Os controles falharão se o tópico do SNS não usar uma chave do 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, em vez disso, escolher usar uma chave do KMS para criptografia. Isso adiciona uma camada adicional de segurança e fornece mais flexibilidade de 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 de API são necessárias para descriptografar os dados antes que eles possam ser lidos. Recomendamos criptografar os tópicos do SNS com chaves do KMS para uma camada adicional de segurança.

Correção

Para habilitar o SSE para um tópico do SNS, consulte Enabling server-side encryption (SSE) for an Amazon SNS topic no Amazon Simple Notification Service Developer Guide. 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.

[SNS.2] O registro em log do status de entrega deve ser habilitado para mensagens de notificação enviadas a um tópico

> **Important**
>
> O Security Hub descontinuou esse controle em abril de 2024. Para obter mais informações, consulte Registro de alterações dos controles CSPM do Security Hub.

Requisitos relacionados: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::SNS::Topic`

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 registro em log é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho dos serviços. O registro de status de entrega de mensagens proporciona um melhor insight operacional, como, 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SNS::Topic`

Regra AWS Config : `tagged-sns-topic` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`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 verificará apenas a existência de uma chave de tag e falhará se o tópico não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 tópico do SNS, consulte Configuring Amazon SNS topic tags no Amazon Simple Notification Service Developer Guide.

[SNS.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::SNS::Topic`

Regra do AWS Config : sns-topic-no-public-access

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a política de acesso a tópicos do SNS permite o acesso público. Esse controle falhará se a política de acesso a tópicos do SNS permitir o acesso público.

Você usa uma política de acesso do Amazon SNS com um tópico específico para restringir quem pode trabalhar com esse tópico (por exemplo, quem pode publicar mensagens nele ou quem pode se inscrever nele). As políticas do SNS podem conceder acesso a outras Contas da AWS pessoas ou a usuários dentro da sua Conta da AWS. Fornecer um caractere curinga (*) no campo `Principal` da política de tópicos e a falta de condições para limitar a política de tópicos podem resultar em exfiltração de dados, negação de serviço ou injeção indesejada de mensagens no serviço por um invasor.

> **Note**
>
> Esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política de acesso do Amazon SNS para um tópico devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

Correção

Para atualizar as políticas de acesso para um tópico do SNS, consulte Overview of managing access in Amazon SNS no Amazon Simple Notification Service Developer Guide.

Controles do Security Hub para o Amazon SQS

Esses AWS Security Hub controles avaliam o serviço e os recursos do Amazon Simple Queue Service (Amazon SQS). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[SQS.1] 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-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (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: `AWS::SQS::Queue`

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 do SQS, consulte Configuring server-side encryption (SSE) for a queue (console) no Amazon Simple Queue Service Developer Guide.

[SQS.2] As filas do SQS devem ser marcadas

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SQS::Queue`

Regra AWS Config : `tagged-sqs-queue` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

Esse controle verifica se uma fila do Amazon SQS tem tags com 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 verificará apenas a existência de uma chave de tag e falhará se a fila não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política

de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 fila existente usando o console do Amazon SQS, Configuring cost allocation tags for an Amazon SQS queue (console) no Amazon Simple Queue Service Developer Guide.

[SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso: `AWS::SQS::Queue`

Regra do AWS Config : sqs-queue-no-public-access

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Isso controla se uma política de acesso do Amazon SQS permite acesso público a uma fila do SQS. O controle falhará se uma política de acesso do SQS permitir acesso público à fila.

Uma política de acesso do Amazon SQS pode permitir acesso público a uma fila SQS, o que pode permitir que um usuário anônimo ou qualquer identidade AWS IAM autenticada acesse a fila. As políticas de acesso do SQS geralmente fornecem esse acesso especificando o caractere curinga (*) no `Principal` elemento da política, não usando condições adequadas para restringir o acesso à fila, ou ambos. Se uma política de acesso do SQS permitir acesso público, terceiros poderão realizar

tarefas como receber mensagens da fila, enviar mensagens para a fila ou modificar a política de acesso da fila. Isso pode resultar em eventos como exfiltração de dados, negação de serviço ou injeção de mensagens na fila por um agente de ameaça.

> **Note**
>
> Esse controle não avalia as condições da política que usam caracteres curinga ou variáveis. Para produzir uma `PASSED` descoberta, as condições na política de acesso do Amazon SQS para uma fila devem usar somente valores fixos, que são valores que não contêm caracteres curinga ou variáveis de política. Para obter informações sobre variáveis de política, consulte Variáveis e tags no Guia AWS Identity and Access Management do usuário.

Correção

Para obter informações sobre como configurar a política de acesso do SQS para uma fila do SQS, consulte Usando políticas personalizadas com a linguagem de política de acesso do Amazon SQS no Guia do desenvolvedor do Amazon Simple Queue Service.

Controles do Security Hub para o Step Functions

Esses AWS Security Hub controles avaliam o AWS Step Functions serviço e os recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::StepFunctions::StateMachine`

Regra do AWS Config : `step-functions-state-machine-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	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, você pode 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 > Marcação

Severidade: baixa

Tipo de recurso: `AWS::StepFunctions::Activity`

AWS Config regra: `tagged-stepfunctions-activity` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	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 verificará apenas a existência de uma chave de tag e falhará se a atividade não estiver marcada com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 Tagging in Step Functions no AWS Step Functions Developer Guide.

Controles do Security Hub para o Systems Manager

Esses AWS Security Hub controles avaliam o serviço e os recursos AWS Systems Manager (SSM). Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager

Requisitos relacionados: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9 (1), 5 (2), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-1 5 (8), NIST.800-53.r5 SA-1 NIST.800-53.r5 SI-2 (3) NIST.800-53.r5 SA-3

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 EC2 instâncias paradas 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 Systems Manager verifica as instâncias gerenciadas interrompidas e em execução. 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 Guia do usuário do AWS Systems Manager .

Correção

Para gerenciar EC2 instâncias com o Systems Manager, consulte Gerenciamento de EC2 host da Amazon no Guia AWS Systems Manager do usuário. Na seção Opções de configuração, você pode manter as opções padrão ou alterá-las conforme necessário para sua configuração preferida.

[SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch

Requisitos relacionados: NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (3), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), NIST.800-171.r2 7.1, PCI DSS v3.2.1/6.2, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso: `AWS::SSM::PatchCompliance`

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 Systems Manager é `COMPLIANT` ou `NON_COMPLIANT` após a instalação do patch na instância. O controle falhará se o status de conformidade for `NON_COMPLIANT`. O controle verifica somente as instâncias gerenciadas pelo gerenciador de patches do Systems Manager.

A correção de suas EC2 instâncias conforme exigido por sua organização reduz a superfície de ataque de suas 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 Gerenciamento de nós, escolha Executar comando e, depois, 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 Conformidade.

[SSM.3] EC2 As instâncias da Amazon 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-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 (3), PCI DSS vs 3.2.1/2.4, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso: `AWS::SSM::AssociationCompliance`

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 State Manager 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 reprovada pode estar relacionada a motivos diferentes, incluindo destinos e nomes de documentos Systems Manager. 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, você pode 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 .

[SSM.4] Os documentos SSM não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1 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: `AWS::SSM::Document`

Regra do AWS Config : ssm-document-not-public

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se AWS Systems Manager os documentos pertencentes a uma conta são públicos. O controle falhará se os documentos do Systems Manager que tem `Self` como proprietário forem públicos.

Documentos Systems Manager que são públicos podem permitir acesso não pretendido aos documentos. Um documento do Systems Manager 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 o compartilhamento público de documentos do Systems Manager que tenha `Self` como proprietário.

Correção

Para obter informações sobre como configurar o compartilhamento de documentos do Systems Manager, consulte Compartilhar um documento SSM no Guia do AWS Systems Manager Usuário.

[SSM.5] Os documentos SSM devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::SSM::Document`

Regra do AWS Config : ssm-document-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

Esse controle verifica se um AWS Systems Manager documento tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o documento não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o documento não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo. O controle não avalia os documentos do Systems Manager que são de propriedade da Amazon.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para adicionar tags a um AWS Systems Manager documento, você pode usar a AddTagsToResourceoperação da AWS Systems Manager API ou, se estiver usando a AWS CLI,

executar o add-tags-to-resourcecomando. Você também pode usar o console do AWS Systems Manager .

[SSM.6] A automação de SSM deve ter o registro ativado CloudWatch

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS:::::Account`

Regra do AWS Config : ssm-automation-logging-enabled

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o CloudWatch registro na Amazon está habilitado para automação AWS Systems Manager (SSM). O controle falhará se o CloudWatch registro não estiver habilitado para a automação SSM.

O SSM Automation é uma AWS Systems Manager ferramenta que ajuda você a criar soluções automatizadas para implantar, configurar e gerenciar AWS recursos em grande escala usando runbooks predefinidos ou personalizados. Para atender aos requisitos operacionais ou de segurança da sua organização, talvez seja necessário fornecer um registro dos scripts que ela executa. Você pode configurar o SSM Automation para enviar a saída das `aws:executeScript` ações em seus runbooks para um grupo de CloudWatch logs do Amazon Logs que você especificar. Com o CloudWatch Logs, você pode monitorar, armazenar e acessar arquivos de log de vários Serviços da AWS.

Correção

Para obter informações sobre como ativar o CloudWatch registro para a automação SSM, consulte Saída da ação do Logging Automation com CloudWatch registros no Guia do AWS Systems Manager usuário.

[SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso: `AWS::::Account`

Regra do AWS Config : ssm-automation-block-public-sharing

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a configuração de bloqueio de compartilhamento público está habilitada para AWS Systems Manager documentos. O controle falhará se a configuração de bloqueio de compartilhamento público estiver desativada para documentos do Systems Manager.

A configuração de bloqueio de compartilhamento público para documentos AWS Systems Manager (SSM) é uma configuração no nível da conta. Ativar essa configuração pode impedir o acesso indesejado aos seus documentos SSM. Se você habilitar essa configuração, sua alteração não afetará nenhum documento SSM que você esteja compartilhando atualmente com o público. A menos que seu caso de uso exija que você compartilhe documentos SSM com o público, recomendamos que você ative a configuração de bloqueio de compartilhamento público. A configuração pode ser diferente para cada um Região da AWS.

Correção

Para obter informações sobre como ativar a configuração de bloqueio de compartilhamento público para documentos AWS Systems Manager (SSM), consulte Bloquear compartilhamento público para documentos SSM no Guia do AWS Systems Manager usuário.

Controles do Security Hub para AWS Transfer Family

Esses AWS Security Hub controles avaliam o AWS Transfer Family serviço e os recursos. Os controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Transfer::Workflow`

Regra AWS Config : `tagged-transfer-workflow` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	A lista de chaves que não são de sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	`No default value`

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 verificará apenas a existência de uma chave de tag e falhará se o fluxo de trabalho não estiver marcado com nenhuma chave. As tags de 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 tags, é possível implementar o controle de acesso por atributo (ABAC) como uma estratégia de autorização, que define permissões com base nas tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política de ABAC ou um conjunto separado de políticas para as entidades do IAM. Você pode criar essas políticas de ABAC para permitir operações quando a tag da entidade principal 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) nem outras informações confidenciais ou sigilosas em 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 fluxo de trabalho do Transfer Family (console)

1. Abra o AWS Transfer Family console.
2. No painel de navegação, escolha Workflows (Fluxos de trabalho). Em seguida, selecione o fluxo de trabalho que você deseja marcar.
3. Escolha Gerenciar tags e, em seguida, adicione as tags.

[Transfer.2] Os servidores do 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, PCI DSS v4.0.1/4.2.1

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso: `AWS::Transfer::Server`

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 um cliente se conectar 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. O uso de SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) ou 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 Edit the file transfer protocols no AWS Transfer Family User Guide.

[Transfer.3] Os conectores Transfer Family devem ter o registro ativado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) 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-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::Transfer::Connector`

Regra do AWS Config : transfer-connector-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o Amazon CloudWatch Logging está habilitado para um AWS Transfer Family conector. O controle falhará se o CloudWatch registro não estiver habilitado para o conector.

A Amazon CloudWatch é um serviço de monitoramento e observabilidade que fornece visibilidade de seus AWS recursos, incluindo AWS Transfer Family recursos. Para Transfer Family, CloudWatch fornece auditoria e registro consolidados para o progresso e os resultados do fluxo de trabalho. Isso inclui várias métricas que a Transfer Family define para fluxos de trabalho. Você pode configurar o Transfer Family para registrar automaticamente os eventos do conector CloudWatch. Para fazer isso, você especifica uma função de registro para o conector. Para a função de registro, você cria uma função do IAM e uma política do IAM baseada em recursos que define as permissões para a função.

Correção

Para obter informações sobre como ativar o CloudWatch registro em um conector Transfer Family, consulte CloudWatch Registro na Amazon para AWS Transfer Family servidores no Guia AWS Transfer Family do usuário.

[Transfer.4] Os contratos da Transfer Family devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Transfer::Agreement`

Regra do AWS Config : transfer-agreement-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS Transfer Family contrato tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o contrato não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o contrato não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso

baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um AWS Transfer Family contrato, consulte Métodos de marcação de recursos no Guia do usuário de AWS recursos de marcação e do editor de tags.

[Transfer.5] Os certificados Transfer Family devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Transfer::Certificate`

Regra do AWS Config : transfer-certificate-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

Esse controle verifica se um AWS Transfer Family certificado tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o certificado não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o certificado não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um AWS Transfer Family certificado, consulte Métodos de marcação de recursos no Guia do usuário de AWS recursos de marcação e do editor de tags.

[Transfer.6] Os conectores Transfer Family devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Transfer::Connector`

Regra do AWS Config : transfer-connector-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos requisitos AWS .	Nenhum valor padrão

Esse controle verifica se um AWS Transfer Family conector tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o conector não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o conector não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações

sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um AWS Transfer Family conector, consulte Métodos de marcação de recursos no Guia do usuário de AWS recursos de marcação e do editor de tags.

[Transfer.7] Os perfis do Transfer Family devem ser marcados

Categoria: Identificar > Inventário > Marcação

Severidade: baixa

Tipo de recurso: `AWS::Transfer::Profile`

Regra do AWS Config : transfer-profile-tagged

Tipo de programação: acionado por alterações

Parâmetros:

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredKeyTags`	Uma lista de chaves de tag que não são do sistema que devem ser atribuídas a um recurso avaliado. Chaves	StringList (máximo de 6 itens)	1 a 6 chaves de tag que atendem aos	Nenhum valor padrão

Parameter	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	de tag fazem distinção entre maiúsculas e minúsculas.		requisitos AWS .	

Esse controle verifica se um AWS Transfer Family perfil tem as chaves de tag especificadas pelo `requiredKeyTags` parâmetro. O controle falhará se o perfil não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas pelo `requiredKeyTags` parâmetro. Se você não especificar nenhum valor para o `requiredKeyTags` parâmetro, o controle verificará somente a existência de uma chave de tag e falhará se o perfil não tiver nenhuma chave de tag. O controle ignora as tags do sistema, que são aplicadas automaticamente e têm o `aws:` prefixo. O controle avalia perfis locais e perfis de parceiros.

Uma tag é um rótulo que você cria e atribui a um AWS recurso. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Eles podem ajudá-lo a identificar, organizar, pesquisar e filtrar recursos. Eles também podem ajudar você a rastrear ações e notificações dos proprietários de recursos. Você também pode usar tags para implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização. Para obter mais informações sobre estratégias ABAC, consulte Definir permissões com base em atributos com autorização ABAC no Guia do usuário do IAM. Para obter mais informações sobre tags, consulte o Guia do usuário dos AWS recursos de marcação e do editor de tags.

> **Note**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por muitos Serviços da AWS. Eles não devem ser usados para dados privados ou confidenciais.

Correção

Para obter informações sobre como adicionar tags a um AWS Transfer Family perfil, consulte Métodos de marcação de recursos no Guia do usuário de AWS recursos de marcação e do editor de tags.

Controles do Security Hub para o AWS WAF

Esses AWS Security Hub controles do avaliam o AWS WAF serviço e os recursos. Os controles da podem não estar disponíveis em todas as Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::WAF::WebACL`

Regra do AWS Config : `waf-classic-logging-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro em log 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 da AWS WAF globalmente. 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 habilitar o registro em log de AWS WAF web ACLs, consulte Registrar em log as informações de tráfego da ACL da web no Guia do AWS WAF desenvolvedor do.

[WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição

Requisitos relacionados: 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)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAFRegional::Rule`

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 AWS WAF Classic Regional devem ter pelo menos uma regra

Requisitos relacionados: 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)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAFRegional::RuleGroup`

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 regional tem pelo menos uma regra. O controle falhará se não houver regras no grupo de regras.

Um grupo de regras WAF regional 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 regras, o tráfego passa sem inspeção. Um grupo de regras regionais do WAF sem regras, 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 Classic e Adicionar e remover condições em uma regra no Guia do AWS WAF desenvolvedor do.

[WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAFRegional::WebACL`

Regra do AWS Config : `waf-regional-webacl-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma ACL AWS WAF Classic regional da web contém alguma regra do WAF ou grupos de regras do 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 do AWS WAF Classic Regional vazia, consulte Editar uma ACL da web no Guia do AWS WAF desenvolvedor do.

[WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAF::Rule`

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 global 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 global 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 AWS WAF Classic global devem ter pelo menos uma regra

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAF::RuleGroup`

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 regras, o tráfego passa sem inspeção. Um grupo de regras globais do WAF sem regras, 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 Criar um grupo de regras AWS WAF Classic no Guia do AWS WAF desenvolvedor do.

[WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: 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)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAF::WebACL`

Regra do AWS Config : `waf-global-webacl-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma ACL da web AWS WAF global contém pelo menos uma regra do WAF ou grupos de regras do WAF. Esse controle falhará se uma ACL da web não contiver nenhuma regra ou grupo de regras do WAF.

Uma ACL da web global 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 Editar uma web ACL no Guia do AWS WAF desenvolvedor do. Em Filtro, escolha Global (CloudFront).

[WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso: `AWS::WAFv2::WebACL`

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 (ACL da web) 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.

A web ACL é um recurso que oferece controle detalhado sobre todas as solicitações web HTTP (S) às quais o recurso protegido responde. Uma web ACL deve 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, AWS WAF dependendo da ação padrão.

Correção

Para adicionar regras ou grupos de regras a uma ACL WAFV2 da web vazia, consulte Editar uma ACL da web no Guia do AWS WAF desenvolvedor do.

[WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10) 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 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso: `AWS::WAFv2::WebACL`

AWS Config regra: **`wafv2-logging-enabled`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro em log está ativado para uma lista de controle de acesso à web AWS WAF V2 (ACL da web). Esse controle falhará se o registro em log não estiver habilitado para a web ACL.

> **Note**
>
> Esse controle não verifica se o registro em log de ACL AWS WAF da web está habilitado para uma conta por meio do Amazon Security Lake.

O registro em log 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, você pode solucionar problemas de comportamento do aplicativo.

Correção

Para ativar o registro em log de uma ACL AWS WAF da web, consulte Gerenciar o registro de uma ACL da web no Guia do AWS WAF desenvolvedor do.

[WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10), NIST.800-53.r5 SC-7 (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 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso: `AWS::WAFv2::RuleGroup`

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 do tem CloudWatch métricas da Amazon habilitadas. O controle falhará se a regra ou o grupo de regras não tiver CloudWatch as métricas habilitadas.

A configuração das CloudWatch métricas em AWS WAF regras e grupos de regras do fornece visibilidade do fluxo de tráfego. Você pode 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. Defina o campo `CloudWatchMetricsEnabled` como `true`. Quando você usa o AWS WAF console do para criar regras ou grupos de regras, CloudWatch as métricas são habilitadas automaticamente.

Controles do Security Hub para WorkSpaces

Esses AWS Security Hub controles avaliam o WorkSpaces serviço e os recursos da Amazon.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para obter mais informações, consulte Disponibilidade de controles por região.

[WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::WorkSpaces::Workspace`

Regra do AWS Config : `workspaces-user-volume-encryption-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o volume de um usuário em uma Amazon WorkSpaces WorkSpace está criptografado em repouso. O controle falhará se o volume WorkSpace do usuário não estiver criptografado em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para criptografar um volume de WorkSpaces usuário, consulte Criptografar um WorkSpace no Guia de WorkSpaces Administração da Amazon.

[WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso: `AWS::WorkSpaces::Workspace`

Regra do AWS Config : `workspaces-root-volume-encryption-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um volume raiz em uma Amazon WorkSpaces WorkSpace está criptografado em repouso. O controle falhará se o volume WorkSpace raiz não estiver criptografado em repouso.

Dados em repouso se referem a dados armazenados em um armazenamento persistente e não volátil por qualquer período. Criptografar os dados em repouso ajuda a proteger sua confidencialidade, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para criptografar um volume WorkSpaces raiz, consulte Criptografar um WorkSpace no Guia de WorkSpaces Administração da Amazon.

Permissões necessárias para configurar controles no Security Hub CSPM

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 o CSPM do AWS Security Hub precisa de permissões para chamar as seguintes operações da API CSPM do Security Hub.

Para obter as permissões necessárias, você pode usar as políticas gerenciadas do Security Hub CSPM. Como alternativa, você pode atualizar as políticas de IAM personalizadas para incluir esas ações .

- 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 uma substituição em lote para a operação `UpdateStandardsControl` existente.
- BatchUpdateStandardsControlAssociations: usado para habilitar ou desabilitar um lote de controles de segurança em padrões que os incluem. Esse é uma substituição em lote para a operação `UpdateStandardsControl` existente.
- UpdateStandardsControl: usado para habilitar ou desabilitar um único controle de segurança em padrões que o incluem
- DescribeStandardsControl: retorna detalhes sobre os controles de segurança especificados.

Além do anterior APIs, você deve adicionar permissão `BatchGetControlEvaluations` para chamar sua função do IAM. Essa permissão é necessária para visualizar o status de habilitação e conformidade de um controle, a contagem de descobertas para um controle e a pontuação geral de segurança dos controles no console CSPM do Security Hub. Como somente o console chama`BatchGetControlEvaluations`, essa permissão não corresponde diretamente ao CSPM APIs ou AWS CLI aos comandos do Security Hub documentados publicamente.

Habilitando controles no Security Hub CSPM

No AWS Security Hub CSPM, um controle é uma proteção dentro de um padrão de segurança que ajuda a organização a proteger a confidencialidade, integridade e disponibilidade de suas informações. Cada controle CSPM do Security Hub está relacionado a um recurso específico AWS . Quando você ativa um controle, o Security Hub CSPM começa a executar verificações de segurança para o controle e gera descobertas para ele. O Security Hub CSPM também considera todos os controles habilitados ao calcular as pontuações de segurança.

Você pode escolher habilitar um controle em todos os padrões aos quais ele se aplica. Ou pode configurar o status de habilitação de maneira diferente para padrões diferentes. Recomendamos a primeira opção, na qual o status de habilitação de um controle está alinhado com todos os padrões habilitados. Para obter instruções para habilitar um controle em todos os padrões a que ele se aplica, consulte Habilitar um controle em todos os padrões. Para obter instruções para habilitar um controle em padrões específicos, consulte Habilitando um controle em um padrão específico.

Se você habilitar a agregação entre regiões e entrar em uma região de agregação, o console CSPM do Security Hub mostrará controles que estão disponíveis em pelo menos uma região vinculada. 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.

Você pode ativar e desativar controles em cada região usando o console CSPM do Security Hub, a API CSPM do Security Hub ou. AWS CLI

As instruções para habilitar e desabilitar os controles variam de acordo com o uso ou não da configuração central. Este tópico descreve as diferenças. A configuração central está disponível para usuários que integram o Security Hub CSPM e. AWS Organizations Recomendamos usar a configuração central para simplificar o processo de habilitação e desabilitação de controles em ambientes com várias contas e várias regiões. Se você usar a configuração central, poderá habilitar um controle em várias contas e regiões usando políticas de configuração. Se você não usar a configuração central, deverá habilitar um controle separadamente em cada conta e em cada região.

Habilitar um controle em todos os padrões

Recomendamos habilitar um controle CSPM do AWS Security Hub em todos os padrões aos quais o controle se aplica. Se você ativar as descobertas de controles consolidadas, receberá uma descoberta por verificação de controle, mesmo que um controle pertença a mais de um padrão.

Habilitação em vários padrões em ambientes com várias contas e várias regiões

Para habilitar um controle de segurança em vários Contas da AWS e Regiões da AWS, você deve estar conectado à conta delegada de administrador CSPM do Security Hub e usar a configuração central.

Na configuração central, o administrador delegado pode criar políticas de configuração CSPM do Security Hub que habilitam controles específicos em todos os padrões habilitados. Em seguida, você pode associar a política de configuração a contas e unidades organizacionais específicas (OUs) 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 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.

> **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 em vários 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 CSPM console

Para habilitar um controle em padrões em uma conta e região

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, escolha Controles.
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 CSPM 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) de quaisquer padrões nos quais o controle não esteja habilitado. Para obter o padrão ARNs, execute `DescribeStandards`.
3. Defina o parâmetro `AssociationStatus` igual a `ENABLED`. Se você seguir essas etapas para um controle que já está ativado, 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) de quaisquer padrões nos quais o controle não esteja habilitado. Para obter o padrão ARNs, execute o `describe-standards` comando.
3. Defina o parâmetro `AssociationStatus` igual a `ENABLED`. Se você seguir essas etapas para um controle que já está ativado, o comando 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.

Habilitando um controle em um padrão específico

Quando você habilita um padrão no AWS Security Hub CSPM, todos os controles que se aplicam a ele são automaticamente habilitados nesse padrão (a exceção são os padrões gerenciados por serviços). Você pode desabilitar e re-habilitar controles específicos no padrão. Entretanto, recomendamos alinhar o status de habilitação de um controle em todos os seus padrões habilitados. Para obter instruções sobre como habilitar um controle em todos os padrões, consulte Habilitar um controle em todos os padrões.

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 do padrão, você também pode habilitar os controles em um padrão específico. Você deve habilitar controles em padrões específicos separadamente em cada Conta da AWS Região da AWS e. Quando você habilita um control em padrões específicos, ele afeta apenas a conta e a região atual.

Para ativar um controle em um padrão, você deve primeiro ativar pelo menos um padrão ao qual o controle se aplica. Para obter instruções sobre a habilitação de um controle, consulte Habilitar um padrão de segurança. Quando você habilita um controle em um ou mais padrões, o Security Hub CSPM começa a gerar descobertas para esse controle. O CSPM do Security Hub inclui o status do controle no cálculo da pontuação geral de segurança e das pontuações de segurança 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 habilitar um controle CSPM 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 em vários padrões em uma única conta e região.

Security Hub CSPM console

Para habilitar um controle em um padrão específico

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Selecione Padrões de segurança no painel de navegação.
3. Escolha Exibir resultados para o respectivo 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 CSPM 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 um ARN padrão, execute `DescribeStandards`. Essa API retorna controle de segurança independente do padrão IDs, não controle específico do padrão. IDs

   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` igual a `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 o comando `list-security-control-definitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter um ARN padrão, execute `describe-standards`. Esse comando retorna o controle de segurança independente do padrão IDs, não o controle específico do padrão. IDs

```
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 o comando `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` igual a `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"}]'
```

Habilitar novos controles em padrões habilitados automaticamente

AWS O Security Hub CSPM lança regularmente novos controles e os adiciona a um ou mais padrões. É possível escolher se deseja habilitar automaticamente novos controles nos padrões habilitados.

Recomendamos usar a configuração central CSPM 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 obter mais informações, consulte Entendendo a configuração central no Security Hub CSPM.

O Security Hub CSPM 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 automaticamente novos controles em padrões habilitados.

> **Note**
>
> Ao ativar automaticamente novos controles usando as instruções a seguir, você pode interagir com os controles no console e programaticamente imediatamente após o lançamento. No entanto, os controles ativados automaticamente têm um status padrão temporário de Desativado. Pode levar vários dias para que o Security Hub CSPM processe a liberação do controle e designe o controle como Ativado em sua conta. Durante o período de processamento, você pode ativar ou desativar manualmente um controle, e o Security Hub CSPM manterá essa designação, independentemente de você ter a ativação automática do controle ativada.

Security Hub CSPM console

Para habilitar automaticamente novos controles

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, selecione Configurações e em seguida Geral.
3. Em Controles, escolha Editar.
4. Ative a Ativação automática de novos controles nos padrões habilitados.
5. Escolha Salvar.

Security Hub CSPM 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, especifique os `--auto-enable-controls`. Se você não quiser habilitar automaticamente novos controles, especifique os `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Exemplo de comando

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Se você não habilitar automaticamente os novos controles, deverá habilitá-los manualmente. Para instruções, consulte Habilitando controles no Security Hub CSPM.

Desativando controles no Security Hub CSPM

Para reduzir o ruído de localização, pode ser útil desativar os controles que não são relevantes para o seu ambiente. No AWS Security Hub CSPM, você pode desativar um controle em todos os padrões de segurança ou somente em padrões específicos.

Se você desabilitar um controle em todos os padrões, ocorrerá o seguinte:

- As verificações de segurança do controle não são mais realizadas.
- Nenhuma descoberta adicional é gerada para o controle.

- As descobertas existentes não são mais atualizadas para o controle.
- As descobertas existentes para o controle são arquivadas automaticamente, normalmente em 3 a 5 dias, com base no melhor esforço.
- O Security Hub CSPM remove todas AWS Config as regras relacionadas que ele criou para o controle.

Se você desabilitar um controle somente para padrões específicos, o Security Hub CSPM interromperá a execução de verificações de segurança para o controle somente para esses padrões. Isso também remove o controle dos cálculos da pontuação de segurança de cada um desses padrões. Se o controle estiver habilitado em outros padrões, o Security Hub CSPM reterá a AWS Config regra associada, se aplicável, e continuará executando verificações de segurança para o controle dos outros padrões. O CSPM do Security Hub também inclui o controle ao calcular a pontuação de segurança para cada um dos outros padrões, o que afeta sua pontuação de segurança resumida.

Se você desabilitar um padrão, todos os controles que se aplicam ao padrão serão desativados automaticamente para esse padrão. No entanto, os controles podem continuar sendo habilitados em outros padrões. Quando você desabilita um padrão, o CSPM do Security Hub não rastreia quais controles foram desativados para o padrão. Consequentemente, se você reativar posteriormente o mesmo padrão, todos os controles que se aplicam a ele serão ativados automaticamente. Para informações sobre como desativar um padrão, consulte Desabilitar um padrão.

Desabilitar um controle não é uma ação permanente. Suponha que você desabilite um controle e, em seguida, habilite um padrão que inclua o controle. O controle é então ativado para esse padrão. Quando você habilita um padrão no Security Hub CSPM, todos os controles que se aplicam ao padrão são habilitados automaticamente. Para obter informações sobre como habilitar um padrão, consulteHabilitar um padrão.

Tópicos

- Desabilitar um controle em todos os padrões
- Habilitar um controle em um padrão específico
- Controles sugeridos para desativar no Security Hub CSPM

Desabilitar um controle em todos os padrões

Recomendamos desativar um controle CSPM do AWS Security Hub em todos os padrões para manter o alinhamento em toda a organização. Se você desabilitar um controle somente em padrões específicos, continuará recebendo descobertas para o controle se ele estiver habilitado em outros padrões.

Desabilitação de vários padrões, em várias contas e regiões

Para desativar um controle de segurança em vários Contas da AWS e Regiões da AWS, você deve usar a configuração central.

Quando você usa a configuração central, o administrador delegado pode criar políticas de configuração CSPM do Security Hub que desabilitam os controles especificados nos padrões habilitados. Em seguida, você pode associar a política de configuração a OUs 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.

> **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 vários 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. No entanto, você pode desativar um controle em uma única conta e região.

Security Hub CSPM console

Para desabilitar um controle em padrões em uma conta e região

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, escolha Controles.
3. Escolha a opção ao lado de um controle.
4. Escolha Desativar controle. Essa opção não aparece em um controle que já está desativado.
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 CSPM 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 de quaisquer padrões nos quais o controle não esteja habilitado. Para obter o padrão ARNs, execute `DescribeStandards`.
3. Defina o parâmetro `AssociationStatus` igual a `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 de quaisquer padrões nos quais o controle não esteja habilitado. Para obter o padrão ARNs, execute o `describe-standards` comando.
3. Defina o parâmetro `AssociationStatus` igual a `DISABLED`. Se você seguir essas etapas para um controle que já está desativado, o comando 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.

Habilitar um controle em um padrão específico

Você pode desativar um controle somente em padrões de segurança específicos, em vez de em todos os padrões. Se o controle se aplicar a outros padrões habilitados, o AWS Security Hub CSPM continuará executando verificações de segurança para o controle e você continuará recebendo descobertas para o controle.

Porém, recomendamos alinhar o status de habilitação de um controle em todos os padrões habilitados. Para obter informações sobre como desativar um controle em todos os padrões aos quais ele se aplica, consulteDesabilitar um controle em todos os padrões.

Na página de detalhes do padrão, você também pode desabilitar controles em padrões específicos. Você deve desativar os controles em padrões específicos separadamente em cada Conta da AWS Região da AWS e. Quando você desativa um controle em padrões específicos, ele afeta somente a conta atual e a região.

Escolha seu método preferido e siga estas etapas para desativar um controle em um ou mais padrões específicos.

Security Hub CSPM console

Para desabilitar um controle em um padrão específico

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Selecione Padrões de segurança no painel de navegação. Escolha Exibir resultados para o respectivo padrão.
3. Selecione um controle.
4. Escolha Desativar controle. Essa opção não aparece em um controle que já está desativado.
5. Forneça um motivo para desativar o controle e confirme escolhendo Desativar.

Security Hub CSPM 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 um ARN padrão, execute `DescribeStandards`. Essa API retorna controle de segurança independente do padrão IDs, não controle específico do padrão. IDs

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 desativar o controle.
4. Defina o parâmetro `AssociationStatus` igual a `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 o comando `list-security-control-definitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter um ARN padrão, execute `describe-standards`. Esse comando retorna o controle de segurança independente do padrão IDs, não o controle específico do padrão. IDs

```
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 o comando 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 desativar o controle.
4. Defina o parâmetro `AssociationStatus` igual a `DISABLED`. Se você seguir essas etapas para um controle que já está ativado, o comando 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"}]'
```

Controles sugeridos para desativar no Security Hub CSPM

Recomendamos desativar alguns controles CSPM do AWS Security Hub para reduzir o ruído de localização e os custos de uso.

Controles que usam 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, no entanto, o Security Hub CSPM ainda executa verificações de segurança em todas as regiões em que um controle está ativado e cobra com base no número de verificações por conta por região. Assim, para reduzir o ruído de localização e economizar no custo do CSPM 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 envolve recursos globais, mas está disponível somente em uma região, desabilitá-lo nessa região impede que você obtenha descobertas para o recurso subjacente. Nesse caso, recomendamos que você mantenha o controle habilitado. 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 na região Leste dos EUA (Norte da Virgínia)
- GlobalAccelerator.1 — Disponível somente na região Oeste dos EUA (Oregon)
- Route53.2 — Disponível somente na região Leste dos EUA (Norte da Virgínia)
- WAF.1, WAF.6, WAF.7, WAF.8 — Disponível somente na região Leste dos EUA (Norte da Virgínia)

> **Note**
>
> Se você usar a configuração central, o Security Hub CSPM desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Os outros controles que você escolher habilitar por meio de uma política de configuração serão habilitados em todas as regiões em que estiverem 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.
>
> Se um controle ativado que envolve recursos globais não for suportado na região de origem, o Security Hub CSPM tentará habilitar o controle em uma região vinculada onde o controle é suportado. Com a configuração central, você não tem cobertura para um controle que não está disponível na região de origem ou em qualquer uma das regiões vinculadas.
>
> Para obter mais informações sobre a configuração central, consulte Entendendo a configuração central no Security Hub CSPM.

Para controles que têm um tipo de agendamento periódico, é necessário desativá-los no CSPM do Security Hub para evitar o faturamento. Definir o AWS Config parâmetro como `false` não afeta `includeGlobalResourceTypes` os controles CSPM periódicos do Security Hub.

Os seguintes controles CSPM do Security Hub usam 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

CloudTrail controles de 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, precisará ativar esse controle somente 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 habilitada

CloudWatch controles de alarme

Se você preferir usar a Amazon GuardDuty para detecção de anomalias em vez dos CloudWatch alarmes da Amazon, você pode desativar os seguintes controles, que se CloudWatch concentram nos alarmes:

- CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário "raiz"
- [CloudWatch.2] Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas
- [CloudWatch.3] Certifique-se de que um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA
- [CloudWatch.4] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM
- [CloudWatch.5] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do
- [CloudWatch.6] Certifique-se de que um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do
- [CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas pelo cliente
- [CloudWatch.8] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3
- [CloudWatch.9] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do
- [CloudWatch.10] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança
- [CloudWatch.11] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)
- [CloudWatch.12] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações em gateways de rede

- [CloudWatch.13] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas
- [CloudWatch.14] Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC

Entendendo as verificações e pontuações de segurança no Security Hub CSPM

Para cada controle que você habilita, o AWS Security Hub CSPM executa verificações de segurança. Uma verificação de segurança produz uma descoberta que informa se um AWS recurso específico está 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 obter mais informações, consulte 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 e ativar o registro de recursos para os recursos necessários. Para obter mais informações sobre a configuração AWS Config, consulteHabilitando e configurando o AWS Config Security Hub CSPM. Para obter uma lista dos AWS Config recursos que você deve registrar para cada padrão, consulteAWS Config Recursos necessários para descobertas de controle. Outros controles usam funções personalizadas do Lambda, que são gerenciadas pelo Security Hub CSPM e não exigem nenhum pré-requisito.

À medida que o Security Hub CSPM executa verificações de segurança, ele gera descobertas e atribui a elas um status de conformidade. Para obter mais informações sobre o status de conformidade, consulte Avaliação do status de conformidade das descobertas do CSPM do Security Hub.

O Security Hub CSPM usa o status de conformidade das descobertas de controle para determinar um status geral de controle. Com base no status do controle, o Security Hub CSPM 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 “Calcular pontuações de segurança”.

Se você ativou as descobertas de controle consolidadas, o Security Hub CSPM gera uma única descoberta mesmo quando um controle está associado a mais de um padrão. Para obter mais informações, consulte Descobertas de controle consolidadas.

Tópicos

AWS Config Recursos necessários para descobertas de controle

No AWS Security Hub CSPM, alguns controles usam AWS Config regras vinculadas a serviços que detectam alterações de configuração em seus recursos. AWS Para que o Security Hub CSPM gere descobertas precisas para esses controles, você deve habilitar AWS Config e ativar o registro de recursos em. AWS Config Para obter informações sobre como o Security Hub CSPM usa AWS Config regras e como habilitar e configurar AWS Config, consulte. Habilitando e configurando o AWS Config Security Hub CSPM Para obter informações detalhadas sobre a gravação de recursos, consulte Como trabalhar com o gravador de configuração no Guia do AWS Config desenvolvedor.

Para receber resultados de controle precisos, você deve ativar o registro de AWS Config recursos para controles habilitados com um tipo de agendamento acionado por alteração. Alguns controles com um tipo de agendamento periódico também exigem o registro de recursos. Esta página lista os recursos necessários para esses controles CSPM do Security Hub.

Os controles CSPM do Security Hub podem se basear em AWS Config regras gerenciadas ou em regras personalizadas de CSPM do Security Hub. Certifique-se de que não haja políticas AWS Identity and Access Management (IAM) ou políticas AWS Organizations gerenciadas que AWS Config impeçam a permissão de registrar seus recursos. Os controles CSPM do Security Hub avaliam as configurações de recursos diretamente e não levam em conta AWS Organizations as políticas.

> **Note**
>
> Regiões da AWS Quando um controle não está disponível, o recurso correspondente não está disponível em AWS Config. Para obter uma lista desses limites, consulteLimites regionais nos controles CSPM do Security Hub.

Tópicos

Recursos necessários para todos os controles CSPM do Security Hub

Para que o Security Hub CSPM gere descobertas para controles acionados por alterações que estejam habilitados e usem uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Essa tabela também indica quais controles avaliam um determinado tipo de recurso. Um único controle pode avaliar mais de um tipo de recurso.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS Amplify	`AWS::Amplify::App`	Amplificar.1
	`AWS::Amplify::Branch`	Amplificar.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway1. APIGateway2.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
		APIGateway3. APIGateway4. APIGateway5.
	`AWS::ApiGatewayV2::Stage`	APIGateway1. APIGateway9.
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig1.
	`AWS::AppConfig::ConfigurationProfile`	AppConfig2.
	`AWS::AppConfig::Environment`	AppConfig3.
	`AWS::AppConfig::ExtensionAssociation`	AppConfig4.
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow1.
AWS App Runner	`AWS::AppRunner::Service`	AppRunner1.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::AppRunner::VpcConnector`	AppRunner2.
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync2. AppSync4. AppSync5.
	`AWS::AppSync::ApiCache`	AppSync1. AppSync.6
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	Lote.3 Lote.4
	`AWS::Batch::JobQueue`	Lote.1

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::Batch::SchedulingPolicy`	Lote.2
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation2.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront1. CloudFront3. CloudFront4. CloudFront5. CloudFront.6 CloudFront7. CloudFront8. CloudFront9. CloudFront.10 CloudFront1.3 CloudFront1.4 CloudFront1.5
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail9.
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch1.5 CloudWatch1.7
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact1.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild1. CodeBuild2. CodeBuild3. CodeBuild4.
	`AWS::CodeBuild::ReportGroup`	CodeBuild7.
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler1.
CodeGuru Revisor da Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer1.
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2
	`AWS::Cognito::UserPool`	Cognito.1
Amazon Connect	`AWS::CustomerProfiles::ObjectType`	Conecte-se. 1

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::Connect::Instance`	Conecte-se. 2
AWS DataSync	`AWS::DataSync::Task`	DataSync1. DataSync2.
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
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Nuvem de computação elástica Amazon () EC2	`AWS::EC2::ClientVpnEndpoint`	EC25.1
	`AWS::EC2::CustomerGateway`	EC23.6
	`AWS::EC2::DHCPOptions`	EC21.74
	`AWS::EC2::EIP`	EC21.2 EC23.7
	`AWS::EC2::FlowLog`	EC24.8

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::EC2::Instance`	EC24. EC28. EC29. EC21.7 EC22.4 EC23,8 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC23.9
	`AWS::EC2::LaunchTemplate`	EC22,5 EC21.70 EC21.75
	`AWS::EC2::NatGateway`	EC24,0
	`AWS::EC2::NetworkAcl`	EC21.6 EC22.1 EC24.1

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::EC2::NetworkInterface`	EC22.2 EC23.5 EC21.80
	`AWS::EC2::PrefixList`	EC21.76
	`AWS::EC2::RouteTable`	EC24.2
	`AWS::EC2::SecurityGroup`	EC22. EC21.3 EC21.4 EC21.8 EC21.9 EC24.3
	`AWS::EC2::SpotFleet`	EC21.73
	`AWS::EC2::Subnet`	EC21.5 EC24.4 ElastiCache7.
	`AWS::EC2::TrafficMirrorFilter`	EC21.78

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::EC2::TrafficMirrorSession`	EC21.77
	`AWS::EC2::TrafficMirrorTarget`	EC21.79
	`AWS::EC2::TransitGateway`	EC22.3 EC25.2
	`AWS::EC2::TransitGatewayAttachment`	EC23.3
	`AWS::EC2::TransitGatewayRouteTable`	EC23.4
	`AWS::EC2::Volume`	EC23. EC24,5
	`AWS::EC2::VPC`	EC2.6 EC24.6
	`AWS::EC2::VPCBlockPublicAccessOptions`	EC21.72

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::EC2::VPCEndpointService`	EC24.7
	`AWS::EC2::VPCPeeringConnection`	EC24.9
	`AWS::EC2::VPNConnection`	EC220. EC21.71
	`AWS::EC2::VPNGateway`	EC25,0
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling1. AutoScaling2. AutoScaling.6 AutoScaling9. AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling3. Autoscaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3 APROX. 5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
	`AWS::EFS::FileSystem`	EFS.7 EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	eks.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk1. ElasticBeanstalk2. ElasticBeanstalk3.
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.1 ELB.3 ELB.5 ELB.7 ELB.1 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge2. EventBridge3.
	`AWS::Events::Endpoint`	EventBridge4.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector1.
	`AWS::FraudDetector::Label`	FraudDetector2.
	`AWS::FraudDetector::Outcome`	FraudDetector3.
	`AWS::FraudDetector::Variable`	FraudDetector4.
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator1.
AWS Glue	`AWS::Glue::Job`	Glue.1 Cola.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty4.
	`AWS::GuardDuty::Filter`	GuardDuty2.

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::GuardDuty::IPSet`	GuardDuty3.
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`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 service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS Eventos de IoT	`AWS::IoTEvents::AlarmModel`	IoT TEvents 3.3
	`AWS::IoTEvents::DetectorModel`	IoT TEvents 1.2
	`AWS::IoTEvents::Input`	IoT TEvents 1.1
AWS IoT SiteWise	`AWS::IoTSiteWise::AssetModel`	Eu sou TSite sábio.1
	`AWS::IoTSiteWise::Dashboard`	Eu sou TSite sábio.2
	`AWS::IoTSiteWise::Gateway`	Eu sou TSite sábio.3
	`AWS::IoTSiteWise::Portal`	Eu sou TSite sábio.4
	`AWS::IoTSiteWise::Project`	Io TSite Wise.5
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity`	Io TTwin Maker.4

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::IoTTwinMaker::Scene`	Io TTwin Maker.3
	`AWS::IoTTwinMaker::SyncJob`	Io TTwin Maker. 1
	`AWS::IoTTwinMaker::Workspace`	Io TTwin Maker.2
AWS IoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoT TWireless 1.1
	`AWS::IoTWireless::ServiceProfile`	IoT TWireless 1.2
	`AWS::IoTWireless::FuotaTask`	IoT TWireless 3.3
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`	Espaços-chave. 1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MASCARA.5

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall1. NetworkFirewall7. NetworkFirewall9. NetworkFirewall.10
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall3. NetworkFirewall4. NetworkFirewall5. NetworkFirewall8.
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
		RDS.35 RDS.37
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::RDS::DBInstance`	RDS 2 RDS. 3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS. 3 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	`AWS::RDS::DBSecurityGroup`	RDS.31

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Redshift.11 Redshift.18

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Desvio para o vermelho.17
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Desvio para o vermelho.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail7. 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::S3::MultiRegionAccessPoint`	S3.24

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::S3Express::DirectoryBucket`	S3.25
SageMaker IA da Amazon	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker7.
	`AWS::SageMaker::Model`	SageMaker5.
	`AWS::SageMaker::NotebookInstance`	SageMaker2. SageMaker3.
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager1. SecretsManager2. SecretsManager5.
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog1.
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2
	`AWS::SES::ContactList`	SES.1

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQ.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions1.
	`AWS::StepFunctions::Activity`	StepFunctions2.
AWS Systems Manager (SMS)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transferência.4
	`AWS::Transfer::Certificate`	Transferência.5
	`AWS::Transfer::Connector`	Transferência.3 Transferência.6
	`AWS::Transfer::Profile`	Transferência.7

AWS service (Serviço da AWS)	Tipos de recursos	Controles relacionados
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces1. WorkSpaces2.

Recursos necessários para o padrão AWS Foundational Security Best Practices

Para que o CSPM do Security Hub relate com precisão as descobertas de controles acionados por alterações que se aplicam ao padrão AWS Foundational Security Best Practices (v.1.0.0), esteja habilitado e use uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consulteAWS Padrão básico de melhores práticas de segurança no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::ApiCache` , `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`
AWS CodeBuild	`AWS::CodeBuild::Project` , `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool` , `AWS::Cognito::UserPool`
Amazon Connect	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Nuvem de computação elástica da Amazon (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `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` , `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint` , `AWS::EFS::FileSystem`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`

AWS service (Serviço da AWS)	Tipos de recursos
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
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::DBProxy` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift sem servidor	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket` , `AWS::S3::MultiRegionAccessPoint` , `AWS::S3Express::DirectoryBucket`
SageMaker IA da Amazon	`AWS::SageMaker::Model` , `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
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`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

Recursos necessários para o CIS AWS Foundations Benchmark

Para executar verificações de segurança para controles habilitados que se aplicam ao benchmark de AWS fundamentos do Center for Internet Security (CIS), o Security Hub CSPM executa as etapas de auditoria exatas prescritas para as verificações ou usa regras gerenciadas específicas. AWS Config Para obter informações sobre esse padrão no Security Hub CSPM, consulte. Referência do CIS AWS Foundations no Security Hub CSPM

Recursos obrigatórios para o CIS v3.0.0

Para que o Security Hub CSPM relate com precisão as descobertas dos controles acionados por alterações do CIS v3.0.0 habilitados que usam uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config

AWS service (Serviço da AWS)	Tipos de recursos
Nuvem de computação elástica da Amazon (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 CSPM relate com precisão as descobertas dos controles acionados por alterações do CIS v1.4.0 habilitados que usam uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config

AWS service (Serviço da AWS)	Tipos de recursos
Nuvem de computação elástica da Amazon (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`

AWS service (Serviço da AWS)	Tipos de recursos
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 v1.2.0

Para que o Security Hub CSPM relate com precisão as descobertas dos controles acionados por alterações do CIS v1.2.0 habilitados que usam uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config

AWS service (Serviço da AWS)	Tipos de recursos
Nuvem de computação elástica da Amazon (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Recursos necessários para o padrão NIST SP 800-53 Revisão 5

Para que o Security Hub CSPM relate com precisão as descobertas de controles acionados por alterações que se aplicam ao padrão NIST SP 800-53 Revisão 5, esteja habilitado e use uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consulteNIST SP 800-53 Revisão 5 no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`

AWS service (Serviço da AWS)	Tipos de recursos
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
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`
Nuvem de computação elástica da Amazon (Amazon 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`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
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::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS service (Serviço da AWS)	Tipos de recursos
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` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
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`
SageMaker IA da Amazon	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`

AWS service (Serviço da AWS)	Tipos de recursos
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 padrão NIST SP 800-171 Revisão 2

Para que o Security Hub CSPM relate com precisão as descobertas de controles acionados por alterações que se aplicam ao padrão NIST SP 800-171 Revisão 2, esteja habilitado e use uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consulteNIST SP 800-171 Revisão 2 no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Nuvem de computação elástica da Amazon (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`

AWS service (Serviço da AWS)	Tipos de recursos
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SMS)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Recursos obrigatórios para o PCI DSS v3.2.1

Para que o Security Hub CSPM reporte com precisão as descobertas dos controles que se aplicam à v3.2.1 do Payment Card Industry Data Security Standard (PCI DSS), esteja habilitado e use uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consultePCI DSS no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
AWS CodeBuild	`AWS::CodeBuild::Project`
Nuvem de computação elástica da Amazon (Amazon 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`

AWS service (Serviço da AWS)	Tipos de recursos
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::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

Recursos necessários para o padrão AWS de marcação de recursos

Todos os controles que se aplicam ao padrão AWS Resource Tagging são acionados por alterações e usam uma AWS Config regra. Para que o Security Hub CSPM relate com precisão as descobertas desses controles, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consulteAWS Padrão de marcação de recursos no Security Hub CSPM.

AWS service (Serviço da AWS)	Tipos de recursos
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::ConfigurationProfile` , `AWS::AppConfig::En`

AWS service (Serviço da AWS)	Tipos de recursos
	`vironment` , `AWS::AppConfig::Extensi onAssociation`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` , `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan` , `AWS::Backup::BackupVault` , `AWS::Backup::RecoveryPlan` , `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment` , `AWS::Batch::JobQueue` , `AWS::Batch::SchedulingPolicy`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup` , `AWS::CodeGuruReviewer::RepositoryAssociation`
Amazon Connect	`AWS::CustomerProfiles::ObjectType`

AWS service (Serviço da AWS)	Tipos de recursos

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate` , `AWS::DMS::EventSubscription`
	
	`AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationSubnetGroup`

AWS DataSync	`AWS::DataSync::Task`
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`
Nuvem de computação elástica Amazon () EC2	`AWS::EC2::CustomerGateway` , `AWS::EC2::DHCPOptions` , `AWS::EC2::EIP` , `AWS::EC2::FlowLog` , `AWS::EC2::Instance` , `AWS::EC2::InternetGateway` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NatGateway` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::PrefixList` , `AWS::EC2::RouteTable` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TrafficMirrorFilter` , `AWS::EC2::TrafficMirrorSession` , `AWS::EC2::TrafficMirrorTarget` , `AWS::EC2::TransitGateway` , `AWS::EC2::TransitGatewayAttachment` , `AWS::EC2::TransitGatewayRouteTable` , `AWS::EC2::Volume` , `AWS::EC2::VPC` , `AWS::EC2::VPCEndpointService` , `AWS::EC2::VPCPeeringConnection` , `AWS::EC2::VPNGateway`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
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	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`

Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label`
	
	`AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`

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 service (Serviço da AWS)	Tipos de recursos
AWS Identity and Access Management Access Analyzer (Analisador de acesso IAM)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`
AWS IoT Eventos	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoT Sem fio	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSecurityGroup` , `AWS::RDS::DBSnapshot` , `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterParameterGroup` , `AWS::Redshift::ClusterSnapshot` , `AWS::Redshift::ClusterSubnetGroup` , `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
SageMaker IA da Amazon	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
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`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager (SMS)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Recursos necessários para o padrão AWS Control Tower gerenciado por serviços

Para que o Security Hub CSPM relate com precisão as descobertas dos controles acionados por alterações que se aplicam ao padrão AWS Control Tower gerenciado pelo serviço, estejam habilitados e usem uma AWS Config regra, você deve registrar os seguintes tipos de recursos em. AWS Config Para obter informações sobre esse padrão, consulte[Padrão gerenciado por serviços: AWS Control Tower](#).

AWS service (Serviço da AWS)	Tipos de recursos
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Nuvem de computação elástica Amazon () EC2	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`

AWS service (Serviço da AWS)	Tipos de recursos

	`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`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS service (Serviço da AWS)	Tipos de recursos

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::Alias` `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`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`

AWS service (Serviço da AWS)	Tipos de recursos
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

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, o AWS Security Hub CSPM começa a executar todas as verificações em duas horas. A maioria das verificações começa a ser executada em 25 minutos. O Security Hub CSPM 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, pode levar até 24 horas para que o Security Hub CSPM gere 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 controle Lambda.1 no padrão AWS Foundational Security Best Practices (FSBP), o Security Hub CSPM cria a regra vinculada ao serviço e normalmente gera descobertas em minutos. Depois disso, se você ativar o controle Lambda.1 no Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS), poderá levar até 24 horas para o Security Hub CSPM gerar descobertas para o controle, pois ele usa a mesma regra vinculada ao serviço.

Após a verificação inicial, a programação para cada controle pode ser periódica ou acionada por alterações. 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 especifica se a regra é acionada por alterações ou periódica.

Verificações de segurança periódicas

As verificações periódicas são executadas automaticamente dentro de 12 ou 24 horas após a última execução. O CSPM do 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 controle KMS.4 (a AWS KMS key rotação deve ser ativada) e, em seguida, corrigir a descoberta, o CSPM do 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`.

As verificações que usam as funções Lambda personalizadas do Security Hub CSPM são periódicas.

Verificações de segurança acionadas por alterações

As verificações de segurança acionadas por alterações 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 CSPM do Security Hub até que um período de 24 horas seja concluído. Independentemente do período de gravação escolhido, o CSPM do Security Hub verifica a cada 18 horas para garantir que nenhuma atualização de recursos tenha AWS Config sido perdida.

Em geral, o Security Hub CSPM 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.

Gerando e atualizando descobertas de controle

AWS O Security Hub CSPM gera e atualiza as descobertas de controle quando executa verificações nos controles de segurança. As descobertas de controle usam o AWS Security Finding Format (ASFF).

O Security Hub CSPM normalmente cobra por cada verificação de segurança de um controle. No entanto, se vários controles usarem a mesma AWS Config regra, o Security Hub CSPM cobrará somente uma vez por cada verificação contra a regra. Por exemplo, a AWS Config `iam-password-policy` regra é usada por vários controles no padrão CIS AWS Foundations Benchmark e no padrão AWS Foundational Security Best Practices. Cada vez que o Security Hub CSPM executa uma verificação em relação a essa regra, ele gera uma descoberta de controle separada para cada controle relacionado, mas cobra apenas uma vez pela verificação.

Se o tamanho de uma descoberta de controle exceder o máximo de 240 KB, o Security Hub CSPM removerá o `Resource.Details` objeto da descoberta. Para controles que são apoiados por AWS Config recursos, você pode revisar os detalhes dos recursos usando o AWS Config console.

Tópicos

Descobertas de controle consolidadas

Se as descobertas de controle consolidadas estiverem habilitadas para sua conta, o Security Hub CSPM gerará uma única descoberta ou atualização de descoberta para cada verificação de segurança de um controle, mesmo que um controle se aplique a vários padrões habilitados. Para obter uma lista dos controles e dos padrões aos quais eles se aplicam, consulte Referência de controle para o Security Hub CSPM o. Recomendamos habilitar as descobertas de controles consolidadas para reduzir o ruído das descobertas.

Se você habilitou o Security Hub CSPM Conta da AWS antes de 23 de fevereiro de 2023, você pode habilitar descobertas de controle consolidadas seguindo as instruções mais adiante nesta seção. Se

você habilitar o Security Hub CSPM em ou após 23 de fevereiro de 2023, as descobertas de controle consolidadas serão habilitadas automaticamente para sua conta.

Se você usar a integração CSPM do Security Hub com AWS Organizations ou convidar contas de membros por meio de um processo de convite manual, as descobertas de controle consolidado serão habilitadas para contas de membros somente se estiverem habilitadas para a conta de administrador. Se o recurso estiver desativado para a conta do administrador, ele será desativado para as contas dos membros. Esse comportamento se aplica a contas de membros novas e existentes. Além disso, se o administrador usar a configuração central para gerenciar o CSPM do Security Hub para várias contas, ele não poderá usar políticas de configuração central para habilitar ou desabilitar descobertas de controle consolidadas para as contas.

Se você desabilitar as descobertas de controle consolidadas para sua conta, o Security Hub CSPM gerará ou atualizará uma descoberta de controle separada para cada padrão habilitado que inclui um controle. Por exemplo, se você habilitar quatro padrões que compartilham um controle, receberá quatro descobertas separadas após uma verificação de segurança do controle. Se você habilitar as descobertas de controles consolidadas, receberá somente uma descoberta.

Quando você habilita descobertas de controle consolidadas, o Security Hub CSPM cria novas descobertas independentes de padrão e arquiva as descobertas originais baseadas em padrões. Alguns campos e valores de localização de controle mudarão, o que pode afetar seus fluxos de trabalho existentes. Para obter informações sobre essas mudanças, consulteDescobertas de controle consolidadas - Alterações no ASFF. Habilitar descobertas de controle consolidadas também pode afetar as descobertas que produtos integrados de terceiros recebem do Security Hub CSPM. Se você usa a solução Automated Security Response na AWS v2.0.0, observe que ela oferece suporte a descobertas de controle consolidadas.

Para habilitar ou desabilitar as descobertas de controles consolidadas, você deve fazer login em uma conta de administrador ou a uma conta autônoma.

> **Note**
>
> Depois de habilitar as descobertas de controle consolidadas, pode levar até 24 horas para que o Security Hub CSPM gere novas descobertas consolidadas e arquive as descobertas existentes baseadas em padrões. Da mesma forma, depois de desativar as descobertas de controle consolidadas, pode levar até 24 horas para que o Security Hub CSPM gere novas descobertas baseadas em padrões e arquive as descobertas consolidadas existentes.

Durante esses períodos, você pode ver uma combinação de descobertas independentes de padrões e baseadas em padrões em sua conta.

Security Hub CSPM console

Para habilitar ou desabilitar descobertas de controle consolidadas

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, em Configurações, selecione Geral.
3. Na seção Controles, escolha Editar.
4. Use a opção Consolidated Control Discovery para habilitar ou desabilitar descobertas de controle consolidadas.
5. Escolha Salvar.

Security Hub CSPM API

Para ativar ou desativar as descobertas de controle consolidadas de forma programática, use a UpdateSecurityHubConfigurationoperação da API CSPM do Security Hub. Ou, se você estiver usando o AWS CLI, execute o update-security-hub-configurationcomando.

Para o `control-finding-generator` parâmetro, especifique `SECURITY_CONTROL` para permitir descobertas de controle consolidadas. Para desativar as descobertas de controle consolidadas, especifique`STANDARD_CONTROL`.

Por exemplo, o AWS CLI comando a seguir permite descobertas de controle consolidadas.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

O AWS CLI comando a seguir desativa as descobertas de controle consolidadas.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Gerando, atualizando e arquivando descobertas de controle

O Security Hub CSPM executa verificações de segurança em um cronograma. Na primeira vez que o Security Hub CSPM executa uma verificação de segurança para um controle, ele gera uma nova descoberta para cada AWS recurso verificado pelo controle. Cada vez que o Security Hub CSPM executa posteriormente uma verificação de segurança para o controle, ele atualiza as descobertas existentes para relatar os resultados da verificação. Isso significa que você pode usar os dados fornecidos por descobertas individuais para rastrear alterações de conformidade de recursos específicos em relação a controles específicos.

Por exemplo, se o status de conformidade de um recurso mudar de `PASSED` para `FAILED` para um controle específico, o CSPM do Security Hub não gerará uma nova descoberta. Em vez disso, o Security Hub CSPM atualiza a descoberta existente para o controle e o recurso. Na descoberta, o Security Hub CSPM altera o valor do campo status de conformidade (`Compliance.Status`) para. `PASSED` O CSPM do Security Hub também atualiza os valores dos campos adicionais para refletir os resultados da verificação — por exemplo, o rótulo de gravidade, o status do fluxo de trabalho e os registros de data e hora que indicam quando o CSPM do Security Hub executou a verificação mais recentemente e atualizou a descoberta.

Ao relatar alterações no status de conformidade, o CSPM do Security Hub pode atualizar qualquer um dos seguintes campos em uma descoberta de controle:

- `Compliance.Status`— O novo status de conformidade do recurso para o controle especificado.
- `FindingProviderFields.Severity.Label`— A nova representação qualitativa da gravidade da descoberta, como`LOW`,`MEDIUM`, ou`HIGH`.
- `FindingProviderFields.Severity.Original`— A nova representação quantitativa da gravidade da descoberta, como `0` para um recurso compatível.
- `FirstObservedAt`— Quando o status de conformidade do recurso foi alterado mais recentemente.
- `LastObservedAt`— Quando o Security Hub CSPM executou mais recentemente a verificação de segurança do controle e do recurso especificados.
- `ProcessedAt`— Quando o Security Hub CSPM começou a processar a descoberta mais recentemente.
- `ProductFields.PreviousComplianceStatus`— O status de conformidade anterior (`Compliance.Status`) do recurso para o controle especificado.
- `UpdatedAt`— Quando o Security Hub CSPM atualizou a descoberta mais recentemente.

- `Workflow.Status`— O status da investigação sobre a descoberta, com base no novo status de conformidade do recurso para o controle especificado.

Se o CSPM do Security Hub atualiza um campo depende principalmente dos resultados da verificação de segurança mais recente para o controle e o recurso aplicáveis. Por exemplo, se o status de conformidade de um recurso mudar de `FAILED` para `PASSED` para um controle específico, o CSPM do Security Hub alterará o status do fluxo de trabalho da descoberta para. `NEW` Para acompanhar as atualizações de descobertas individuais, você pode consultar o histórico de uma descoberta. Para obter detalhes sobre campos individuais nas descobertas, consulte Formato AWS de descoberta de segurança (ASFF).

Em certos casos, o Security Hub CSPM gera novas descobertas para verificações subsequentes por um controle, em vez de atualizar as descobertas existentes. Isso pode ocorrer se houver um problema com a AWS Config regra que apóia um controle. Se isso acontecer, o Security Hub CSPM arquiva a descoberta existente e gera uma nova descoberta para cada verificação. Nas novas descobertas, o status de conformidade é `NOT_AVAILABLE` e o estado do registro é`ARCHIVED`. Depois de resolver o problema com a AWS Config regra, o Security Hub CSPM gera novas descobertas e começa a atualizá-las para rastrear alterações subsequentes no status de conformidade de recursos individuais.

Além de gerar e atualizar as descobertas de controle, o Security Hub CSPM arquiva automaticamente as descobertas de controle que atendem a determinados critérios. O Security Hub CSPM arquiva uma descoberta se o controle estiver desativado, se o recurso especificado for excluído ou se o recurso especificado não existir mais. Um recurso pode não existir mais porque o serviço associado não é mais usado. Mais especificamente, o Security Hub CSPM arquiva automaticamente uma descoberta de controle se a descoberta atender a um dos seguintes critérios:

- A descoberta não foi atualizada por 3 a 5 dias. Observe que o arquivamento com base nesse período de tempo é feito da melhor maneira possível e não é garantido.
- A AWS Config avaliação associada retornou `NOT_APPLICABLE` para o status de conformidade do recurso especificado.

Para determinar se uma descoberta está arquivada, você pode consultar o campo record state (`RecordState`) da descoberta. Se uma descoberta for arquivada, o valor desse campo será`ARCHIVED`.

O Security Hub CSPM armazena descobertas de controle arquivadas por 30 dias. Após 30 dias, as descobertas expiram e o Security Hub CSPM as exclui permanentemente. Para determinar se uma descoberta de controle arquivada expirou, o Security Hub CSPM baseia seu cálculo no valor do `UpdatedAt` campo da descoberta.

Para armazenar descobertas de controle arquivadas por mais de 30 dias, você pode exportar as descobertas para um bucket do S3. Você pode fazer isso usando uma ação personalizada com uma EventBridge regra da Amazon. Para obter mais informações, consulte Usando EventBridge para resposta e remediação automatizadas.

> **Note**
>
> Antes de 3 de julho de 2025, o Security Hub CSPM gerava e atualizava as descobertas de controle de forma diferente quando o status de conformidade de um recurso mudava para um controle. Anteriormente, o Security Hub CSPM criava uma nova descoberta de controle e arquivava a descoberta existente para um recurso. Portanto, você pode ter várias descobertas arquivadas para um determinado controle e recurso até que essas descobertas expirem (após 30 dias).

Automação e supressão de resultados de controle

Você pode usar as regras de automação CSPM do Security Hub para atualizar ou suprimir descobertas de controle específicas. Se você suprimir uma descoberta, poderá continuar a acessá-la. No entanto, a supressão indica sua crença de que nenhuma ação é necessária para resolver a descoberta.

Ao suprimir as descobertas, você pode reduzir o ruído das descobertas. Por exemplo, você pode suprimir as descobertas de controle geradas nas contas de teste. Ou você pode suprimir descobertas relacionadas a recursos específicos. Para saber mais sobre como atualizar ou suprimir descobertas automaticamente, consulteEntendendo as regras de automação no Security Hub CSPM.

As regras de automação são apropriadas quando você deseja atualizar ou suprimir descobertas de controle específicas. No entanto, se um controle não for relevante para sua organização ou caso de uso, recomendamos desativar o controle. Se você desabilitar um controle, o Security Hub CSPM não executará verificações de segurança e você não será cobrado por ele.

Detalhes de conformidade para resultados de controle

Nas descobertas geradas pelas verificações de segurança dos controles, o objeto de conformidade e os campos no Formato de descoberta de AWS segurança (ASFF) fornecem detalhes de conformidade para recursos individuais verificados por um controle. Isso inclui as seguintes informações:

- `AssociatedStandards`— Os padrões habilitados nos quais o controle está habilitado.
- `RelatedRequirements`— Os requisitos relacionados para o controle em todos os padrões habilitados. Esses requisitos derivam de estruturas de segurança de terceiros para o controle, como o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) ou o padrão NIST SP 800-171 Revisão 2.
- `SecurityControlId`— O identificador para o controle dos padrões que o Security Hub CSPM suporta.
- `Status`— O resultado da verificação mais recente de que o Security Hub CSPM executou para o controle. Os resultados das verificações anteriores são mantidos no histórico da descoberta.
- `StatusReasons`— Uma matriz que lista os motivos do valor especificado pelo `Status` campo. Para cada motivo, isso inclui um código de motivo e uma descrição.

A tabela a seguir lista os códigos de motivos e as descrições que uma descoberta pode incluir na `StatusReasons` matriz. As etapas de remediação variam de acordo com o controle que gerou uma descoberta com um código de motivo especificado. Para revisar a orientação de remediação de um controle, consulte o. Referência de controle para o Security Hub CSPM

Código do motivo	Compliance status (Status de conformidade)	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.

Código do motivo	Compliance status (Status de conformidade)	Descrição
`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.
`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 (Status de conformidade)	Descrição
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(para Config.1)	O AWS Config gravador usa uma função personalizada do IAM em vez da função AWS Config vinculada ao serviço, e o parâmetro `includeConfigServiceLinkedRoleCheck` personalizado para Config.1 não está definido como. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(para Config.1)	AWS Config não está habilitado com o gravador de configuração ligado.
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(para Config.1)	AWS Config não está registrando todos os tipos de recursos que correspondem aos controles CSPM habilitados do Security Hub. Ative a gravação para os seguintes recursos: *`Resources that aren't being recorded`*.

Código do motivo	Compliance status (Status de conformidade)	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 (Status de conformidade)	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 (Status de conformidade)	Descrição
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Ocorreu um erro desconhecido.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	O CSPM do Security Hub não consegue realizar uma verificação em relação a um tempo de execução Lambda personalizado.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	A descoberta está em um `WARNING` estado 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 (Status de conformidade)	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.

ProductFields detalhes das descobertas de controle

Nas descobertas geradas pelas verificações de segurança dos controles, o ProductFieldsatributo no Formato de descoberta de AWS segurança (ASFF) pode incluir os seguintes campos.

`ArchivalReasons:0/Description`

Descreve por que o Security Hub CSPM arquivou uma descoberta.

Por exemplo, o Security Hub CSPM arquiva descobertas existentes quando você desabilita um controle ou padrão, ou ativa ou desabilita descobertas de controle consolidadas.

`ArchivalReasons:0/ReasonCode`

Especifica por que o Security Hub CSPM arquivou uma descoberta.

Por exemplo, o Security Hub CSPM arquiva descobertas existentes quando você desabilita um controle ou padrão, ou ativa ou desabilita descobertas de controle consolidadas.

`PreviousComplianceStatus`

O status de conformidade anterior (`Compliance.Status`) do recurso para o controle especificado, a partir da atualização mais recente da descoberta. Se o status de conformidade do recurso não tiver sido alterado durante a atualização mais recente, esse valor será igual ao valor do `Compliance.Status` campo da descoberta. Para obter uma lista de valores possíveis, consulte Avaliando o status de conformidade e o status de controle.

`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 dos `Compliance.AssociatedStandards` se você habilitar as descobertas de controles 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 se você habilitar as descobertas de controles consolidadas.

`RuleId` ou `ControlId`

O identificador do controle.

Para o padrão CIS AWS Foundations Benchmark, o campo é. `RuleId` Para outros padrões, o campo é `ControlId`.

Esses campos serão removidos em favor dos `Compliance.SecurityControlId` se você habilitar as descobertas de controles consolidadas.

`RecommendationUrl`

O URL para informações de remediação para o controle. Esse campo será removido em favor dos `Remediation.Recommendation.Url` se você habilitar as descobertas de controles consolidadas.

`RelatedAWSResources:0/name`

O nome do recurso associado à descoberta.

`RelatedAWSResource:0/type`

O tipo de recurso associado ao controle.

`StandardsControlArn`

O ARN do controle. Esse campo será removido se você habilitar as descobertas de controles consolidadas.

`aws/securityhub/ProductName`

Para descobertas de controle, o nome do produto é`Security Hub`.

`aws/securityhub/CompanyName`

Para descobertas de controle, o nome da empresa é`AWS`.

`aws/securityhub/annotation`

Uma descrição do problema descoberto pelo controle.

`aws/securityhub/FindingId`

O identificador da descoberta.

Esse campo não referenciará um padrão se você habilitar as descobertas de controles consolidadas.

Níveis de severidade para resultados de controle

A severidade atribuída a um controle CSPM do Security Hub indica 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 recursos ou de seus recursos Serviços da AWS .

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.

No entanto, 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 um aplicativo de missão crítica é mais crítico do que aquele associado a testes de não 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 improvável	Comprometimento altamente improvável
Muito fácil de explorar	Crítico	Crítico	Alto	Médio
Um pouco fácil de explorar	Crítico	Alto	Médio	Médio
Um pouco difícil de explorar	Alto	Médio	Médio	Baixo
Muito difícil de explorar	Médio	Médio	Baixo	Baixo

Definições de severidade

Os rótulos de severidade são definidos da seguinte forma.

Crítico: 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 atores maliciosos buscam 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.

Alto: o problema deve ser tratado como prioridade de curto prazo.

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 CSPM recomenda que você trate uma constatação de alta gravidade 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.

O Security Hub CSPM recomenda que você investigue o recurso implicado o mais rápido possível. Você também deve considerar a importância do recurso.

Baixo: 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 `PASSED`, `WARNING` ou `NOT AVAILABLE`.

Não há ação recomendada. As descobertas informativas ajudam os clientes a demonstrar que estão em um estado de conformidade.

Avaliando o status de conformidade e o status de controle

O `Compliance.Status` campo do Formato de descoberta de AWS segurança descreve o resultado de uma descoberta de controle. AWS O Security Hub CSPM 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 CSPM do Security Hub.

Avaliação do status de conformidade das descobertas do CSPM do Security Hub

Ao status de conformidade de cada descoberta é atribuído um dos seguintes valores:

- PASSED— Indica que o controle passou na verificação de segurança da descoberta. Isso configura automaticamente o CSPM Workflow.Status do Security Hub como. RESOLVED
- FAILED— Indica que o controle não passou na verificação de segurança da descoberta.
- WARNING— Indica que o CSPM do Security Hub não pode determinar se o recurso está em um estado PASSED ouFAILED. Por exemplo, a gravação de AWS Config recursos não está ativada para o tipo de recurso correspondente.
- 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 foiNOT_APPLICABLE. Se o resultado da AWS Config avaliação forNOT_APPLICABLE, o Security Hub CSPM arquiva automaticamente a descoberta.

Se o status de conformidade de uma descoberta mudar de PASSED para FAILEDWARNING, ou ou e for ouNOT_AVAILABLE, Workflow.Status o Security Hub CSPM Workflow.Status mudará automaticamente para. NOTIFIED RESOLVED NEW

Se você não tiver recursos correspondentes a um controle, o Security Hub CSPM 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 CSPM cria uma NOT_AVAILABLE descoberta e a arquiva imediatamente. Após 18 horas, você recebe uma PASSED descoberta porque não tem mais recursos correspondentes ao controle.

Derivar o status do controle do status de conformidade

O Security Hub CSPM deriva um status geral de controle do status de conformidade das descobertas de controle. Ao determinar o status do controle, o Security Hub CSPM ignora as descobertas que têm um RecordState de ARCHIVED e as descobertas que têm um de. Workflow.Status SUPPRESSED

Ao status do controle é atribuído um dos valores a seguir:

- Aprovado: indica que o status de conformidade de todas as descobertas é PASSED.
- Reprovado: indica que o status de conformidade de pelo menos um descoberta é FAILED.
- Desconhecido: indica que o status de conformidade de pelo menos uma descoberta é WARNING ou NOT_AVAILABLE. Nenhuma descoberta tem um status de conformidade 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 CSPM comece a gerar descobertas para ele. Um

controle também tem esse status se todas as suas descobertas estiverem SUPPRESSED ou não disponíveis no momento Região da AWS.

- Desabilitado: indica que o controle está desabilitado na conta e região atual. Nenhuma verificação de segurança está sendo feita para esse controle nessa conta e nessa região. Porém, as descobertas de um controle desabilitado podem ter um de status de conformidade por até 24 horas após a desabilitação.

Para uma conta de administrador, o status de controle reflete o status de controle da conta de administrador e das contas de membros. Especificamente, o status geral de um controle aparece como Reprovado se o controle tiver uma ou mais descobertas reprovadas na conta do administrador ou em alguma das contas-membro. Se você definiu uma região de agregação, o status do controle na região de agregação refletirá o status do controle na região de agregação e nas regiões vinculadas. Especificamente, o status geral de um controle aparece como Reprovado se o controle tiver uma ou mais descobertas reprovadas na região de agregação ou em alguma das regiões vinculadas.

O CSPM do Security Hub normalmente gera o status de controle inicial dentro de 30 minutos após sua primeira visita à página Resumo ou à página de padrões de segurança no console CSPM do Security Hub. A gravação de recursos do AWS Config deve estar configurada para que o status do controle seja exibido. Depois que os status de controle são gerados pela primeira vez, o Security Hub CSPM atualiza os status de controle a cada 24 horas com base nas descobertas das 24 horas anteriores. Um timestamp na página de detalhes do controle indica a última vez que o status do controle foi atualizado.

> **Note**
>
> Depois de ativar um controle pela primeira vez, pode levar até 24 horas para que os status de controle sejam gerados nas regiões da China e na AWS GovCloud (US) Region.

Calcular pontuações de segurança

No console CSPM do AWS Security Hub, a página Resumo e a página Controles exibem uma pontuação de segurança resumida em todos os padrões habilitados. Na página de padrões de segurança, o Security Hub CSPM também exibe uma pontuação de segurança de 0 a 100 por cento para cada padrão habilitado.

Quando você ativa o CSPM do Security Hub pela primeira vez, o CSPM do 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 Padrões de Segurança no console. As pontuações são geradas somente para os padrões que são ativados quando você visita essas páginas no console. 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. Para revisar uma lista de padrões atualmente habilitados, você pode usar a GetEnabledStandardsoperação da API CSPM do Security Hub.

Após a primeira geração de pontuação, o CSPM do Security Hub atualiza as pontuações de segurança a cada 24 horas. O CSPM do Security Hub exibe um carimbo de data/hora para indicar quando uma pontuação de segurança foi atualizada pela última vez. Observe que pode levar até 24 horas para que as pontuações de segurança pela primeira vez sejam geradas nas regiões da China e. AWS GovCloud (US) Regions

Se você ativar as descobertas de controle consolidadas, pode 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 CSPM gere novas pontuações de segurança que incluam dados das regiões atualizadas.

Método de cálculo das pontuações de segurança

A pontuação de segurança representa a proporção de controles no estado 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 CSPM calcula uma pontuação de segurança resumida em todos os seus padrões habilitados. O Security Hub CSPM também calcula uma pontuação de segurança para cada padrão habilitado. 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 CSPM ignora as 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 status de controle, consulte Avaliando o status de conformidade e o status de controle.

Exemplo de pontuação:

Padrão	Controles aprovados	Falha nos controles	Controles desconhecidos	Pontuação 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%
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 de segurança resumida, o Security Hub CSPM 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 CSPM 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.

Você pode ter uma pontuação resumida diferente da pontuação de segurança padrão, mesmo que tenha ativado somente um padrão em sua conta na região atual. Isso pode ocorrer se você estiver

conectado a uma conta de administrador e as contas de membros 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 de 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 de membros 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 de membros e em todas as regiões vinculadas.

Categorias de controle no Security Hub CSPM

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
- 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.

Inventory

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 Amazon EC2 Systems Manager e Service Catalog?

Registro em log

Você habilitou com segurança todos os registros em log relevantes para o serviço? São exemplos de arquivos de log:

- Logs de fluxo do Amazon VPC
- Logs de acesso do Elastic Load Balancing
- CloudFront Registros da Amazon
- CloudWatch Registros da Amazon
- Registros em log do 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 IAM 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 o usuário 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 está sendo usado VPCs corretamente? Por exemplo, os trabalhos são necessários para serem executados 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 CSPM, 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?

Analisando os detalhes dos controles no Security Hub CSPM

Selecionar um controle na página Controles ou na página de detalhes padrão do console CSPM do Security Hub leva você a uma página de detalhes do controle.

A parte superior da página de detalhes do controle indica o status do controle. O status do controle resume a performance do controle com base no status de conformidade das descobertas do controle. O CSPM do Security Hub normalmente gera o status de controle inicial dentro de 30 minutos após sua primeira visita à página Resumo ou à página de padrões de segurança no console CSPM do Security Hub. Os status só estão disponíveis para controles que são ativados quando você visita essas páginas.

A página de detalhes do controle também fornece um detalhamento do status de conformidade das descobertas de controle nas últimas 24 horas. Para obter mais informações sobre status de controle e status de conformidade, consulte Avaliando o status de conformidade e o status de controle.

AWS Config a gravação de 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 CSPM atualiza o status do controle a cada 24 horas com base nas descobertas das 24 horas anteriores.

As contas de administrador refletem 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 status de controle, consulte the section called “Status de conformidade e status de controle”.

Você também pode habilitar ou desabilitar o controle na página de detalhes do 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) Regions.

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 guia Verificações lista as descobertas ativas do controle nas últimas 24 horas. As descobertas de controle são geradas e atualizadas quando o Security Hub CSPM executa verificações de segurança para o controle. A lista nessa guia não inclui descobertas arquivadas.

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 obter mais informações, consulte Revisando e gerenciando descobertas de controle.

Visualizar detalhes de um controle

Escolha seu método de acesso preferido e siga estas etapas para revisar os detalhes de um controle. Os detalhes se aplicam à conta e região atuais e incluem o seguinte:

- O título e a descrição do controle.
- Um link para a orientação de remediação para descobertas de controle malsucedidas.
- A severidade do controle.
- O status do controle.

No console, você também pode revisar uma lista de descobertas recentes do controle. Para fazer isso programaticamente, você pode usar a GetFindingsoperação da API CSPM do Security Hub.

Security Hub CSPM console

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, escolha Controles.
3. Selecione um controle.

Security Hub CSPM API

1. Execute `ListSecurityControlDefinitions` e forneça um ou mais padrões ARNs para obter uma lista de controle IDs para esse padrão. Para obter o padrão ARNs, execute `DescribeStandards`. Se você não fornecer um ARN padrão, essa API retornará todo o controle CSPM do Security Hub. IDs Essa API retorna o controle de segurança independente do padrão IDs, não o controle baseado em padrões IDs que existia antes do lançamento desses recursos.

   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 `list-security-control-definitions` comando e forneça um ou mais padrões ARNs para obter uma lista de controle IDs. Para obter o padrão ARNs, execute o `describe-standards` comando. Se você não fornecer um ARN padrão, esse comando retornará todo o controle CSPM do Security Hub. IDs Esse comando retorna o controle de segurança independente do padrão IDs, não o controle baseado em padrões IDs que existia antes desses lançamentos de recursos.

   ```
   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 o comando `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"]'
```

Controles de filtragem e classificação no Security Hub CSPM

No console CSPM do AWS Security Hub, você pode usar a página Controles para revisar uma tabela dos controles que estão disponíveis no atual. Região da AWS A exceção é uma região de agregação. Se você configurou uma região de agregação e entrou nessa região, o console mostra os controles que estão disponíveis na região de agregação ou em uma ou mais regiões vinculadas.

Para se concentrar em um subconjunto específico de controles, você pode classificar e filtrar a tabela de controles. As opções Filtrar por ao lado da tabela podem ajudar você a se concentrar rapidamente nesses subconjuntos específicos:

- Todos os controles habilitados, que são controles habilitados em pelo menos um padrão habilitado.
- Todos os controles desativados, que são controles desativados em todos os padrões.
- Todos os controles ativados que têm um status de controle específico, como Falha. A opção Sem dados exibe somente os controles que não têm descobertas no momento. Para obter informações sobre o status do controle, consulteAvaliando o status de conformidade e o status de controle.

Além das opções Filtrar por, você pode filtrar a tabela inserindo critérios de filtro na caixa Controles de filtro acima da tabela. Por exemplo, é possível filtrar por ID ou gravidade.

Por padrão, os controles com status de Falha são listados primeiro, em ordem decrescente por gravidade. Você pode alterar a ordem de classificação escolhendo um título de coluna diferente.

> **Tip**
>
> Se você tiver fluxos de trabalho automatizados com base nas descobertas do controle, recomendamos usar os campos `SecurityControlId` ou `SecurityControlArn` ASFF como filtros, em vez dos campos `Title` ou`Description`. Os últimos campos podem mudar ocasionalmente, enquanto o ID de controle e o ARN são identificadores estáticos.

Se você estiver conectado a uma conta de administrador do CSPM do Security Hub, os controles habilitados incluem controles habilitados em pelo menos uma conta de membro. Se você configurou uma região de agregação, os controles ativados incluem controles habilitados em pelo menos uma região vinculada.

Se você selecionar a opção ao lado de um controle ativado, um painel será exibido e exibirá os padrões nos quais o controle está atualmente ativado. Você também pode ver os padrões nos quais o controle está atualmente desativado. Nesse painel, você pode desativar um controle em todos os padrões. Para obter mais informações, consulte Desativando controles no Security Hub CSPM. Para contas de administrador, as informações no painel refletem as configurações de todas as suas contas de membros.

Para recuperar uma lista de controles programaticamente, você pode usar a ListSecurityControlDefinitionsoperação da API CSPM do Security Hub. Para recuperar os detalhes dos controles individuais, use a BatchGetSecurityControlsoperação.

Entendendo os parâmetros de controle no Security Hub CSPM

Alguns controles no AWS Security Hub CSPM usam parâmetros que afetam a forma como o controle é avaliado. Normalmente, esses controles são avaliados em relação aos valores de parâmetros padrão que o Security Hub CSPM define. Porém, para um subconjunto desses controles, você pode personalizar os valores dos parâmetros. Quando você modifica um valor de parâmetro de controle, o Security Hub CSPM 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 CSPM gerará uma descoberta. `PASSED` Se o recurso não atender ao valor personalizado, o CSPM do Security Hub gerará uma `FAILED` descoberta.

Ao personalizar os parâmetros de controle, você pode refinar as melhores práticas de segurança recomendadas e monitoradas pelo Security Hub CSPM 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 de modificação de parâmetros de controles e definição de valores 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 aborda o que deverá ser considerado quando você modificar os parâmetros de controle.

Efeito da modificação dos valores dos parâmetros de controle

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 CSPM gera novas descobertas de controle com base no novo valor. Durante atualizações periódicas para controlar as descobertas, o Security Hub CSPM também usa 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 CSPM não realizará nenhuma verificação de segurança usando os novos valores. Você precisa habilitar pelo menos um padrão relevante para o Security Hub CSPM avaliar o controle com base no novo valor do parâmetro.

Um controle pode ter um ou mais parâmetros personalizáveis. Os possíveis tipos de dados para cada parâmetro de controle incluem o seguinte:

- Booleano
- Duplo
- Enum
- EnumList
- Inteiro
- IntegerList
- String
- StringList

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 nos controles CSPM do Security Hub.

Em alguns controles, os valores aceitáveis dos parâmetros devem estar em intervalo especificado para serem válidos. Nesses casos, o Security Hub CSPM fornece o intervalo aceitável.

O Security Hub CSPM 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 rastreamento de atualizações no valor CSPM padrão do Security Hub, mesmo que o valor personalizado do parâmetro corresponda ao valor padrão atual definido pelo CSPM do 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 CSPM do Security Hub alterar o valor padrão para`14`, o parâmetro neste exemplo não rastreará essa alteração. Ele manterá um valor de `30`.

Se você quiser rastrear as atualizações do valor CSPM padrão do Security Hub para um parâmetro, defina o `ValueType` campo como `DEFAULT` em vez de. `CUSTOM` Para obter mais informações, consulte Reverter os parâmetros de controles ao padrão em uma única conta e região.

Controles que oferecem suporte a parâmetros personalizados

Para obter uma lista de controles de segurança que oferecem suporte a parâmetros personalizados, consulte a página Controles do console CSPM do Security Hub ou o. Referência de controle para

o Security Hub CSPM Para recuperar essa lista programaticamente, é possível usar a operação ListSecurityControlDefinitions. Na resposta, o objeto `CustomizableProperties` indica quais controles oferecem suporte a parâmetros personalizáveis.

Revisar os valores dos parâmetros de controles atuais

Pode ser útil saber o valor atual de um parâmetro de controle antes de modificá-lo.

É possível revisar os valores atuais dos parâmetros de controle individuais em sua conta. Se você usar a configuração central, o administrador delegado do CSPM do AWS 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 CSPM console

Para revisar os valores atuais dos parâmetros de controles (console)

1. Abra o console CSPM do AWS Security Hub 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 CSPM API

Para revisar os valores atuais dos parâmetros de controles (API)

Invoque a BatchGetSecurityControlsAPI e forneça um ou mais controles de segurança IDs ou ARNs. O objeto `Parameters` na resposta mostra os valores dos parâmetros atuais para os controles especificados.

Por exemplo, o AWS CLI comando a seguir mostra os valores dos parâmetros atuais para `APIGatway.1CloudWatch.15`, `IAM.7` e. 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 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 CSPM console

Para revisar os valores atuais dos parâmetros em uma política de configuração (console)

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
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 CSPM API

Para revisar os valores atuais dos parâmetros em uma política de configuração (API)

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.

Por exemplo, o AWS CLI comando a seguir recupera os valores dos parâmetros de controle atuais na 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.

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

As descobertas de controles também incluem os valores atuais dos parâmetros de controle. Em AWS Formato de descoberta de segurança (ASFF), esses valores aparecem no campo `Parameters` do objeto `Compliance`. Para revisar as descobertas no console CSPM do Security Hub, escolha Descobertas no painel de navegação. Para analisar as descobertas de forma programática, use a GetFindingsoperação da API CSPM do Security Hub.

Personalizar parâmetros de controles

As instruções para personalizar os parâmetros de controle variam de acordo com o uso da configuração central no CSPM do AWS Security Hub. A configuração central é um recurso que o administrador delegado do CSPM do Security Hub pode usar para configurar os recursos do CSPM do Security Hub em contas e unidades Regiões da AWS organizacionais (). OUs

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 de membros gerenciadas centralmente e OUs entram em vigor na sua região de origem 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.

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.

Personalizar os parâmetros dos controles em várias contas e regiões

Se você for o administrador delegado do CSPM do Security Hub de uma organização que usa a configuração central, escolha seu método preferido e siga as etapas para personalizar os parâmetros de controle em várias contas e regiões.

Security Hub CSPM console

Para personalizar os parâmetros de controles em várias contas e regiões (console)

1. Abra o console CSPM do AWS Security Hub 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 valores de parâmetros de controles 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 às OUs quais você deseja aplicar a política.
   6. Escolha Próximo.
   7. Escolha Criar política e aplicar. Na sua região de origem e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs que estão 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 personalizar valores de parâmetros de controles 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 às OUs 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 de origem e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs que estão 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 CSPM API

Para personalizar os parâmetros de controles em várias contas e regiões (API)

Para criar uma nova política de configuração com valores de parâmetros de controles 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 personalizar valores de parâmetros de controles 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.

Por exemplo, o AWS CLI comando a seguir cria uma nova política de configuração com um valor personalizado para o `daysToExpiration` parâmetro de`ACM.1`. 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 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 usar a configuração central ou sua conta for autogerenciada, poderá personalizar os parâmetros de controles da conta em uma região de cada 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 CSPM console

Para personalizar os valores dos parâmetros de controles em uma única conta e região (console)

1. Abra o console CSPM do AWS Security Hub 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 CSPM API

Para personalizar os valores dos parâmetros de controles em uma única conta e região (API)

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.

Por exemplo, o AWS CLI comando a seguir define um valor personalizado para o `daysToExpiration` parâmetro de`ACM.1`. 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 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"
```

Revertendo para valores de parâmetros de controle padrão

Um parâmetro de controle pode ter um valor padrão definido pelo AWS Security Hub CSPM. Ocasionalmente, o Security Hub CSPM atualiza o valor padrão de um parâmetro para refletir as práticas recomendadas de segurança em evolução. 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. As instruções para reversão dependem de você usar a configuração central no CSPM do Security Hub. A configuração central é um recurso que o administrador delegado do CSPM do Security Hub pode usar para configurar os recursos do CSPM do Security Hub em contas e unidades Regiões da AWS organizacionais (). OUs

> **Note**
>
> Nem todos os parâmetros de controle têm um valor CSPM padrão do Security Hub. Nesses casos, quando `ValueType` definido como`DEFAULT`, não há um valor padrão específico que o Security Hub CSPM use. Em vez disso, o Security Hub CSPM ignora o parâmetro na ausência de um valor personalizado.

Para reverter os parâmetros de controles ao padrão em várias contas e regiões

Se você usar a configuração central, poderá reverter os parâmetros de controle para várias contas gerenciadas centralmente e na região de origem e OUs nas regiões vinculadas.

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 CSPM console

Para reverter os parâmetros aos valores padrão em várias contas e regiões (console)

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

   Faça login usando as credenciais da conta delegada de administrador CSPM do Security Hub na região de origem.
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 às OUs 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 de origem e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs que estão 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 CSPM API

Para reverter os parâmetros aos valores padrão em várias contas e regiões (API)

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 CSPM do 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 `SecurityControlCustomParameters` campo, o CSPM do 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.

Por exemplo, o AWS CLI comando a seguir reverte o parâmetro de `daysToExpiration` controle `ACM.1` para seu valor padrão na 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.

```
$ 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"}}}]}}}'
```

Reverter os parâmetros de controles ao padrão 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 CSPM do Security Hub, seus parâmetros de controle personalizados serão redefinidos. Se você habilitar o Security Hub CSPM novamente no futuro, todos os controles usarão valores de parâmetros padrão para começar.

Security Hub CSPM console

Para reverter os parâmetros de controles aos valores padrão em uma única conta e região (console)

1. Abra o console CSPM do AWS Security Hub 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 CSPM padrão do Security Hub e rastreia futuras atualizações para o valor padrão.
4. Repita a etapa anterior para cada valor de parâmetro que desejar reverter.

Security Hub CSPM API

Para reverter os parâmetros de controles aos valores padrão em uma única conta e região (API)

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 CSPM do Security Hub o ignorará.
4. Opcionalmente, em `LastUpdateReason`, forneça um motivo para reverter aos valores padrão dos parâmetros.

Por exemplo, o AWS CLI comando a seguir reverte o parâmetro `daysToExpiration` de controle `ACM.1` para seu valor padrão. 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 update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Verificar o status de alterações nos parâmetros de controle

Quando você tenta personalizar um parâmetro de controle ou revertê-lo ao valor padrão, pode validar se as alterações desejadas tiveram efeito. Isso ajuda a garantir que um controle funcione conforme o esperado e forneça o valor de segurança pretendido. Se a atualização de um parâmetro não for bem-sucedida, o Security Hub CSPM reterá o valor atual do parâmetro.

Para verificar se a atualização de um parâmetro foi bem-sucedida, você pode revisar os detalhes do controle no console CSPM do Security Hub. No console, escolha Controles no painel de navegação. Depois, escolha um 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 que talvez nem as todas descobertas já incluam os valores dos parâmetros atualizados. Quando o valor de `UpdateState` muda para`READY`, o Security Hub CSPM usa os valores atualizados dos parâmetros de controle ao executar verificações de segurança do controle. As descobertas incluem os valores atualizados dos parâmetros.

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 talvez você tenha especificado um valor que não usa o tipo de dados correto. Envie sua solicitação novamente com informações válidas.

Se ocorrer uma falha interna ao tentar atualizar um valor de parâmetro, o Security Hub CSPM tentará novamente automaticamente se você tiver habilitado. AWS Config Para obter mais informações, consulte Considerações antes de ativar e configurar AWS Config.

Revisando e gerenciando descobertas de controle no Security Hub CSPM

A página de detalhes do controle exibe uma lista das descobertas ativas de um controle. A lista não inclui descobertas arquivadas.

A página de detalhes do controle é compatível com a agregação entre regiões. 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.

Você também pode usar a API CSPM do AWS Security Hub para recuperar uma lista de descobertas e detalhes da descoberta.

Para obter mais informações, consulte Revisar os detalhes e o histórico das descobertas.

Para refletir o status atual da sua investigação da descoberta de um controle, você define o status do fluxo de trabalho. Para obter mais informações, consulte the section called “Definir o status do fluxo de trabalho das descobertas”.

Você também pode enviar descobertas selecionadas do CSPM do Security Hub para uma ação personalizada na Amazon. EventBridge Para obter mais informações, consulte the section called “Enviar descobertas para uma ação personalizada”.

Tópicos

- Filtrar e classificar descobertas de controles
- Amostras de resultados de controle

Filtrar e classificar descobertas de controles

Selecionar um controle na página Controles do console CSPM do AWS Security Hub ou na página de detalhes de um padrão leva você à página de detalhes do controle.

A página de detalhes do controle mostra o título e a descrição do controle, o status geral do controle e um detalhamento das verificações de segurança do controle nas últimas 24 horas.

Use as opções Filtrar por ao lado da lista de verificações do controle para se concentrar rapidamente nas descobertas com um determinado status de fluxo de trabalho ou status de conformidade.

Além das opções Filtrar por, você pode usar a caixa Adicionar filtro para filtrar a lista de verificação por outros campos, como Conta da AWS ID ou ID do recurso.

Por padrão, as descobertas com um status de conformidade APROVADO são listadas primeiro. Você pode alterar a classificação padrão escolhendo outra opção nos cabeçalhos das colunas.

Na página de detalhes do controle, você pode escolher Baixar para baixar a página atual de descobertas de controles para um arquivo .csv.

Se você filtrar a lista de descobertas, o arquivo baixado incluirá somente os controles que correspondem ao filtro. Se você selecionar descobertas específicas na lista, o download incluirá somente as descobertas selecionadas.

Para obter mais informações sobre filtragem, consulte Filtrando descobertas no Security Hub CSPM.

Amostras de resultados de controle

Os exemplos a seguir fornecem exemplos de descobertas de controle CSPM do AWS Security Hub no AWS Security Finding Format (ASFF). O conteúdo das descobertas de controle varia dependendo se você habilitou as descobertas de controle consolidadas.

Se você habilitar descobertas de controle consolidadas, o Security Hub CSPM gerará uma única descoberta para um controle, mesmo que o controle se aplique a vários padrões habilitados. Se você não habilitar esse recurso, o Security Hub CSPM gerará uma descoberta de controle separada para cada padrão habilitado ao qual um controle se aplica. Por exemplo, se você habilitar dois padrões e um controle se aplicar a ambos, você receberá duas descobertas separadas para o controle, uma para cada padrão. Se você habilitar descobertas de controle consolidadas, receberá somente uma descoberta para o controle. Para obter mais informações, consulte Descobertas de controle consolidadas.

Os exemplos desta página fornecem exemplos para os dois cenários. Os exemplos incluem: descobertas de controle para padrões CSPM individuais do Security Hub quando as descobertas de controle consolidadas estão desativadas e uma descoberta de controle para vários padrões CSPM do Security Hub quando as descobertas de controle consolidadas estão habilitadas.

Amostras de resultados de controle

- Exemplo de descoberta do padrão AWS Boundational Security Best Practices
- Exemplo de descoberta para o CIS AWS Foundations Benchmark v3.0.0
- Exemplo de descoberta para o CIS AWS Foundations Benchmark v1.4.0
- Exemplo de descoberta para o CIS AWS Foundations Benchmark v1.2.0
- Exemplo de descoberta para o padrão NIST SP 800-53 Revisão 5
- Exemplo de descoberta para o padrão NIST SP 800-171 Revisão 2
- Exemplo de descoberta do Padrão de Segurança de Dados do Setor de Cartões de Pagamento v3.2.1
- Amostra de descoberta para o padrão AWS Resource Tagging
- Amostra de descoberta para o padrão AWS Control Tower gerenciado por serviços
- Exemplo de descoberta consolidada para vários padrões

> **Note**
>
> Os resultados do controle fazem referência a diferentes campos e valores nas regiões e AWS GovCloud (US) regiões da China. Para obter mais informações, consulte Impacto da consolidação nos campos e valores do ASFF.

Exemplo de descoberta do padrão AWS Boundational Security Best Practices

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao padrão AWS Foundational Security Best Practices (FSBP). Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao CIS AWS Foundations Benchmark v3.0.0. Neste exemplo, os resultados do controle consolidado estão desativados.


```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao CIS AWS Foundations Benchmark v1.4.0. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao CIS AWS Foundations Benchmark v1.2.0. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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 padrão NIST SP 800-53 Revisão 5

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao padrão NIST SP 800-53 Revisão 5. Neste exemplo, os resultados do controle consolidado estão desativados.


```
{
  "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 CSPM",
  "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
 CSPM 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 CSPM",
    "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 o padrão NIST SP 800-171 Revisão 2

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao padrão NIST SP 800-171 Revisão 2. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
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-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
```

```
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "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 information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
```

```
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Exemplo de descoberta do Padrão de Segurança de Dados do Setor de Cartões de Pagamento v3.2.1

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao Payment Card Industry Data Security Standard (PCI DSS) v3.2.1. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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"
```

```
    ]
  }
}
```

Amostra de descoberta para o padrão AWS Resource Tagging

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao padrão AWS Resource Tagging. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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"
}
```

Amostra de descoberta para o padrão AWS Control Tower gerenciado por serviços

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica ao padrão AWS Control Tower gerenciado por serviços. Neste exemplo, os resultados do controle consolidado estão desativados.

```
{
  "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 CSPM",
  "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 CSPM 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 CSPM",
    "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 consolidada para vários padrões

O exemplo a seguir fornece um exemplo de uma descoberta para um controle que se aplica a vários padrões habilitados. Nesta amostra, as descobertas de controle consolidadas estão habilitadas.

```
{
```

```
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/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": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "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 information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
```

```
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
```

```
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```

Entendendo as integrações no Security Hub CSPM

AWS O Security Hub CSPM pode ingerir descobertas de segurança de várias soluções de segurança Serviços da AWS de terceiros AWS Partner Network compatíveis. Essas integrações podem ajudá-lo a obter uma visão abrangente da segurança e da conformidade em todo o seu AWS ambiente. O Security Hub CSPM ingere descobertas de soluções integradas e as converte no AWS Security Finding Format (ASFF).

> **Important**
>
> Para integrações de produtos compatíveis AWS e de terceiros, o Security Hub CSPM recebe e consolida descobertas que são geradas somente após você habilitar o CSPM do Security Hub para seu. Contas da AWS O serviço não recebe e consolida retroativamente as descobertas de segurança que foram geradas antes de você habilitar o CSPM do Security Hub.

A página Integrações do console CSPM do Security Hub fornece acesso às integrações de produtos disponíveis AWS e de terceiros. A API CSPM do Security Hub também tem operações para gerenciar integrações.

Uma integração pode não estar disponível em todos Regiões da AWS. Se uma integração não for suportada na região em que você está atualmente conectado no console CSPM do Security Hub, ela não aparecerá na página Integrações do console. Para obter uma lista das integrações que

estão disponíveis nas regiões da China AWS GovCloud (US) Regions, consulteDisponibilidade de integrações por região.

Além das integrações AWS service (Serviço da AWS) incorporadas de terceiros, você pode integrar produtos de segurança personalizados com o Security Hub CSPM. Em seguida, você pode enviar as descobertas desses produtos para o CSPM do Security Hub usando a API CSPM do Security Hub. Você também pode usar a API para atualizar as descobertas existentes que o Security Hub CSPM recebeu de um produto de segurança personalizado.

Tópicos

Analisando uma lista de integrações CSPM do Security Hub

Escolha seu método preferido e siga as etapas para revisar uma lista de integrações no AWS Security Hub CSPM ou detalhes sobre uma integração específica.

Security Hub CSPM console

Para revisar as opções e os detalhes da integração (console)

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

Security Hub CSPM API

Para revisar as opções e os detalhes da integração (API)

Para obter uma lista de integrações, use a operação DescribeProducts. Se você estiver usando o AWS CLI, execute o describe-productscomando.

Para recuperar detalhes de uma integração de produto específica, use o `ProductArn` parâmetro para especificar o Amazon Resource Name (ARN) da integração.

Por exemplo, o AWS CLI comando a seguir recupera detalhes sobre a integração do CSPM do Security Hub com 3. CORESec

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Habilitando o fluxo de descobertas de uma integração CSPM do Security Hub

Na página Integrações do console CSPM do AWS Security Hub, você pode ver as etapas necessárias para habilitar cada integração.

Para a maioria das integrações com outros Serviços da AWS, a única etapa necessária para habilitar a integração é habilitar o outro serviço. As informações de integração incluem um link para a página inicial do outro serviço. Quando você habilita o outro serviço, uma permissão em nível de recurso que permite que o CSPM do Security Hub receba descobertas do serviço é criada e aplicada automaticamente.

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 que você deseja assinar e escolha Continuar assinando. 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 que o CSPM do Security Hub precisa para receber descobertas desse produto.

Depois que você conclui todas as etapas preliminares para habilitar uma integração, pode desabilitar e reabilitar o fluxo de descobertas dessa integração. Na página Integrações, para integrações que enviam descobertas, a informação de Status indica se você está aceitando descobertas no momento.

Security Hub CSPM console

Para habilitar o fluxo de descobertas em uma integração (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação CSPM do Security Hub, escolha Integrações.
3. Para integrações que enviam descobertas, as informações de status indicam se o Security Hub CSPM está atualmente aceitando descobertas dessa integração.
4. Escolha Aceitar descobertas.

Security Hub CSPM API

Use a operação EnableImportFindingsForProduct. Se você estiver usando o AWS CLI, execute o enable-import-findings-for-productcomando. Para habilitar que o Security Hub receba descobertas de uma integração, você precisa do ARN do produto. Para obter as ARNs integrações

disponíveis, use a DescribeProductsoperação. Se você estiver usando o. AWS CLI, execute describe-productso.

Por exemplo, o AWS CLI comando a seguir permite que o Security Hub CSPM receba descobertas da integração com o CrowdStrike Falcon. 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 enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Desabilitando o fluxo de descobertas de uma integração CSPM do Security Hub

Escolha seu método preferido e siga as etapas para desativar o fluxo de descobertas de uma integração CSPM do AWS Security Hub.

Security Hub CSPM console

Para desabilitar o fluxo de descobertas de uma integração (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação CSPM do Security Hub, escolha Integrações.
3. Para integrações que enviam descobertas, as informações de status indicam se o Security Hub CSPM está atualmente aceitando descobertas dessa integração.
4. Escolha Parar de aceitar descobertas.

Security Hub CSPM API

Use a operação DisableImportFindingsForProduct. Se você estiver usando o AWS CLI, execute o disable-import-findings-for-productcomando. Para desabilitar o fluxo de descobertas de uma integração, você precisa do ARN da assinatura da integração habilitada. Para obter o ARN da assinatura, use a operação ListEnabledProductsForImport. Se você estiver usando o. AWS CLI, execute list-enabled-products-for-importo.

Por exemplo, o AWS CLI comando a seguir desativa o fluxo de descobertas para o Security Hub CSPM a partir da integração com o CrowdStrike Falcon. 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 disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Visualizando descobertas de uma integração CSPM do Security Hub

Quando você começa a aceitar descobertas de uma integração CSPM do AWS Security Hub, a página Integrações do console CSPM do Security Hub exibe o Status da integração como Aceitando descobertas. Para revisar uma lista de descobertas da integração, 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. the section called “Agregando dados em todas as 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 Security Hub CSPM

AWS O Security Hub CSPM suporta integrações com vários outros. Serviços da AWS Essas integrações podem ajudar você a obter uma visão abrangente da segurança e da conformidade em todo o seu ambiente da AWS .

Salvo indicação em contrário abaixo, AWS service (Serviço da AWS) as integrações que enviam descobertas para o CSPM do Security Hub são ativadas automaticamente após você habilitar o CSPM do Security Hub e o outro serviço. As integrações que recebem descobertas do CSPM do Security Hub podem exigir etapas adicionais para ativação. Analise as informações sobre cada integração para saber mais.

Algumas integrações não estão disponíveis em todas Regiões da AWS. No console CSPM do Security Hub, uma integração não aparece na página Integrações se não for suportada na região atual. Para obter uma lista das integrações que estão disponíveis nas regiões da China AWS GovCloud (US) Regions, consulteDisponibilidade de integrações por região.

Visão geral das integrações de AWS serviços com o Security Hub CSPM

A tabela a seguir fornece uma visão geral dos AWS serviços que enviam descobertas para o Security Hub CSPM ou recebem descobertas do Security Hub CSPM.

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 Serviço integrado	Direction	
Amazon Route 53 Resolver Firewall DNS	Envia descobertas	
AWS Systems Manager Patch Manager	Envia descobertas	
AWS Audit Manager	Recebe descobertas	
Amazon Q Developer em aplicações de chat	Recebe descobertas	
Amazon Detective	Recebe descobertas	
Amazon Security Lake	Recebe descobertas	
AWS Systems Manager Explorer e OpsCenter	Recebe e atualiza as descobertas	
AWS Trusted Advisor	Recebe descobertas	

AWS serviços que enviam descobertas para o Security Hub CSPM

Os itens a seguir Serviços da AWS se integram e podem enviar descobertas para o CSPM do Security Hub. O Security Hub CSPM converte as descobertas no AWS Security Finding Format.

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 CSPM do Security Hub. Essas descobertas podem ser visualizadas junto com outras descobertas do CSPM 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 para o Security Hub CSPM. O Security Hub CSPM transforma as avaliações de regras em descobertas que seguem o Security Finding Format.AWS Em seguida, o Security Hub CSPM enriquece as descobertas com base no melhor esforço, obtendo mais informações sobre os recursos afetados, como o Amazon Resource Name (ARN), tags de recursos e data de criação.

Para mais informações sobre esta integração, consulte as seções a seguir.

Como AWS Config envia descobertas para o Security Hub CSPM

Todas as descobertas no Security Hub CSPM usam o formato JSON padrão 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 CSPM via. EventBridge O Security Hub CSPM transforma as avaliações de regras em descobertas que seguem o ASFF e enriquece as descobertas com base no melhor esforço.

Tipos de descobertas AWS Config enviadas ao CSPM do Security Hub

Depois que a integração for ativada, AWS Config envia avaliações de todas as regras AWS Config gerenciadas e personalizadas para o Security Hub CSPM. Somente as avaliações que foram realizadas após a ativação do CSPM do Security Hub são enviadas. Por exemplo, suponha que uma avaliação de regra do AWS Config revele cinco recursos reprovados. Se eu habilitar o CSPM do Security Hub depois disso e a regra revelar um sexto recurso com falha, AWS Config enviará somente a sexta avaliação do recurso para o CSPM do Security Hub.

As avaliações de AWS Config regras vinculadas a serviços, como aquelas usadas para executar verificações nos controles CSPM do Security Hub, estão excluídas.

Enviando AWS Config descobertas para o Security Hub CSPM

Quando a integração for ativada, o Security Hub CSPM atribuirá automaticamente as permissões necessárias para receber as descobertas. AWS Config O Security Hub CSPM usa permissões de service-to-service nível que fornecem uma maneira segura de ativar essa integração e importar descobertas via AWS Config Amazon. EventBridge

Latência para enviar descobertas

Quando AWS Config cria uma nova descoberta, geralmente você pode visualizá-la no CSPM do Security Hub em cinco minutos.

Tentando novamente quando o Security Hub CSPM não está disponível

AWS Config envia as descobertas para o CSPM do Security Hub com base no melhor esforço, por meio de. EventBridge Quando um evento não é entregue com sucesso ao CSPM do 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 CSPM

Depois de AWS Config enviar uma descoberta para o Security Hub CSPM, ele pode enviar atualizações da mesma descoberta para o Security Hub CSPM 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 CSPM do Security Hub. O Security Hub CSPM exclui as descobertas 90 dias após a atualização mais recente ou 90 dias após a criação se nenhuma atualização ocorrer.

O Security Hub CSPM não arquiva as descobertas enviadas, AWS Config mesmo que você exclua o recurso associado.

Regiões nas quais existem descobertas AWS Config

AWS Config as descobertas ocorrem em uma base regional. AWS Config envia as descobertas para o Security Hub CSPM na mesma região ou regiões em que as descobertas ocorrem.

Visualizando AWS Config descobertas no Security Hub CSPM

Para visualizar suas AWS Config descobertas, escolha Findings no painel de navegação CSPM 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 nomes de AWS Config busca no CSPM do Security Hub

O Security Hub CSPM transforma as 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 CSPM do 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	<partition><region>“arn:: hub de segurança:::” product/aws/ config
	ProductName	“Config”
	CompanyName	"AWS"
	Região	“eu-central-1”
configRuleArn	GeneratorId, ProductFields	
detalhe. ConfigRuleARN/find ing/hash	Id	
detalhe. configRuleName	Título, ProductFields	
detalhe. configRuleName	Descrição	“Essa descoberta foi criada para uma alteração de conformidade de recurso para a regra de configuração: `${detail.ConfigRul eName}` ”
Item de configuração “ARN” ou ARN computado CSPM do Security Hub	Resources[i].id	

Tipo de descoberta da avaliação da regra de configuração	Tipo de descoberta do ASFF	Valor codificado
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"
	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 CSPM 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 1.024 caracteres, ela será truncada para 1.024 caracteres e dirá "(truncada)" no 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:::amzn-s3-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 CSPM, essa integração é ativada automaticamente. AWS Config imediatamente começa a enviar as descobertas para o Security Hub CSPM.

Interrompendo a publicação de descobertas no Security Hub CSPM

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

Para obter instruções para interromper o fluxo de descobertas, consulte Habilitando o fluxo de descobertas de uma integração CSPM do Security Hub.

AWS Firewall Manager (Envia descobertas)

O Firewall Manager envia descobertas para o Security Hub CSPM quando uma política de firewall de aplicativo web (WAF) para recursos ou uma regra de lista de controle de acesso à web (web ACL) 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 CSPM, essa integração é ativada automaticamente. O Firewall Manager começa imediatamente a enviar as descobertas para o CSPM do Security Hub.

Para saber mais sobre a integração, consulte a página Integrações no console CSPM do Security Hub.

Para saber mais sobre o Firewall Manager, consulte Guia do desenvolvedor do AWS WAF .

Amazon GuardDuty (envia descobertas)

GuardDuty envia todos os tipos de descoberta que ele gera para o CSPM do Security Hub. Alguns tipos de descoberta têm pré-requisitos, requisitos de capacitação ou limitações regionais. Para obter mais informações, consulte GuardDuty encontrar tipos no Guia do GuardDuty usuário da Amazon.

As novas descobertas GuardDuty são enviadas ao Security Hub CSPM 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 CSPM recebe as descobertas de amostra e omite o prefixo `[Sample]` no tipo de descoberta. Por exemplo, o exemplo de tipo de descoberta em GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` é exibido como `Recon:IAMUser/ResourcePermissions` no CSPM do Security Hub.

Depois de habilitar o Security Hub CSPM, essa integração é ativada automaticamente. GuardDutyimediatamente começa a enviar as descobertas para o Security Hub CSPM.

Para obter mais informações sobre a GuardDuty integração, consulte Integração com o AWS Security Hub CSPM no Guia do usuário da Amazon GuardDuty .

AWS Health (Envia descobertas)

AWS Health fornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de seu Serviços da AWS Contas da AWS e. 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 CSPM do Security Hub.

Para mais informações sobre a integração, consulte as seções a seguir.

Como AWS Health envia descobertas para o Security Hub CSPM

No Security Hub CSPM, 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 CSPM também tem um conjunto de regras que ele usa para detectar problemas de segurança e gerar descobertas.

O Security Hub CSPM fornece ferramentas para gerenciar descobertas de todas essas fontes. Você pode exibir e filtrar listas de descobertas e exibir detalhes de uma descoberta. Consulte Analisando os detalhes e o histórico da descoberta no Security Hub CSPM. Você também pode rastrear o status de uma investigação em uma descoberta. Consulte Definindo o status do fluxo de trabalho das descobertas no Security Hub CSPM.

Todas as descobertas no Security Hub CSPM usam um formato JSON padrão chamado de. 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 CSPM.

Tipos de descobertas AWS Health enviadas ao CSPM do Security Hub

Depois que a integração for habilitada, AWS Health envia as descobertas que atendem a uma ou mais das especificações listadas para o Security Hub CSPM. O Security Hub CSPM ingere as descobertas no. AWS Formato de descoberta de segurança (ASFF)

- Descobertas que contêm algum dos seguintes valores para AWS service (Serviço da AWS):
  - RISK
  - ABUSE
  - ACM
  - CLOUDHSM
  - CLOUDTRAIL
  - CONFIG
  - CONTROLTOWER
  - DETECTIVE
  - EVENTS
  - GUARDDUTY
  - IAM
  - INSPECTOR
  - KMS
  - MACIE
  - SES
  - SECURITYHUB
  - SHIELD
  - SSO
  - COGNITO
  - IOTDEVICEDEFENDER
  - NETWORKFIREWALL
  - ROUTE53
  - WAF
  - FIREWALLMANAGER
  - SECRETSMANAGER
  - BACKUP
  - AUDITMANAGER
  - ARTIFACT
  - CLOUDENDURE

- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB

- Descobertas com as palavras securityabuse, ou certificate no AWS Health typeCode campo
- Descobertas de onde o AWS Health serviço está risk ou abuse

Enviando AWS Health descobertas para o Security Hub CSPM

Quando você optar por aceitar as descobertas AWS Health, o Security Hub CSPM atribuirá automaticamente as permissões necessárias para receber as descobertas. AWS Health O Security Hub CSPM usa permissões de service-to-service nível que fornecem uma maneira segura e fácil de habilitar essa integração e importar descobertas via AWS Health Amazon EventBridge em seu nome. Escolher Aceitar descobertas concede ao Security Hub CSPM permissão para consumir descobertas de. AWS Health

Latência para enviar descobertas

Quando AWS Health cria uma nova descoberta, ela geralmente é enviada ao CSPM do Security Hub em cinco minutos.

Tentando novamente quando o Security Hub CSPM não está disponível

AWS Health envia as descobertas para o CSPM do Security Hub com base no melhor esforço, por meio de. EventBridge Quando um evento não é entregue com sucesso ao CSPM do Security Hub, EventBridge tenta enviar o evento novamente por 24 horas.

Atualizando as descobertas existentes no Security Hub CSPM

Depois de AWS Health enviar uma descoberta para o CSPM do Security Hub, ele pode enviar atualizações para a mesma descoberta para refletir observações adicionais da atividade de descoberta para o CSPM do Security Hub.

Regiões nas quais existem descobertas

Para eventos globais, AWS Health envia as descobertas para o Security Hub CSPM em us-east-1 (partição AWS), cn-northwest-1 (partição da China) e -1 (partição). gov-us-west GovCloud AWS Health envia eventos específicos da região para o CSPM do Security Hub na mesma região ou regiões em que os eventos ocorrem.

Visualizando AWS Health descobertas no Security Hub CSPM

Para ver suas AWS Health descobertas no Security Hub CSPM, 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 nomes de AWS Health busca no CSPM do Security Hub

AWS Health envia as descobertas para o Security Hub CSPM usando o. AWS Formato de descoberta de segurança (ASFF) AWS Health a descoberta usa um padrão de evento diferente em comparação com o formato CSPM ASFF do Security Hub. A tabela abaixo detalha todos os campos de AWS Health descoberta com seus equivalentes do ASFF conforme eles aparecem no CSPM do 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	
<region>“arn: aws: hub de segurança:::” product/aws/health	ProductArn	

Tipo de descoberta de saúde	Tipo de descoberta do ASFF	Valor codificado
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 campo `service` na descoberta AWS Health tiver o valor de `Risk`
  - O campo `typeCode` na descoberta AWS Health tiver o valor de `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - O campo `typeCode` na descoberta AWS Health tiver o valor de `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - O campo `typeCode` na descoberta AWS Health tiver o valor de `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  Gravidade ALTA se:
  - O campo `service` na descoberta AWS Health tiver o valor de `Abuse`
  - O campo `typeCode` na descoberta AWS Health contiver o valor de `SECURITY_NOTIFICATION`

- O campo `typeCode` na descoberta AWS Health contiver o valor de `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 CSPM usando o. AWS Formato de descoberta de segurança (ASFF) 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 CSPM, essa integração é ativada automaticamente. AWS Health imediatamente começa a enviar as descobertas para o Security Hub CSPM.

Interrompendo a publicação de descobertas no Security Hub CSPM

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

Para obter instruções para interromper o fluxo de descobertas, consulte Habilitando o fluxo de descobertas de uma integração CSPM do Security Hub.

AWS Identity and Access Management Access Analyzer (Envia descobertas)

Com o IAM Access Analyzer, todas as descobertas são enviadas ao CSPM do 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 CSPM 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 CSPM do AWS Security Hub 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 EC2 instâncias da Amazon e imagens de contêineres 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 CSPM, essa integração é ativada automaticamente. O Amazon Inspector começa imediatamente a enviar todas as descobertas geradas para o Security Hub CSPM.

Para obter mais informações sobre a integração, consulte Integração com o AWS Security Hub CSPM no Guia do usuário do Amazon Inspector.

O Security Hub CSPM também pode receber descobertas do Amazon Inspector Classic. O Amazon Inspector Classic envia descobertas para o CSPM do 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 CSPM 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",
```

> **Note**
>
> As descobertas de segurança geradas pelo Amazon Inspector Code Security não estão disponíveis para essa integração. No entanto, você pode acessar essas descobertas específicas no console do Amazon Inspector e por meio da API do Amazon Inspector.

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 habilitar ambos AWS IoT Device Defender e o CSPM do Security Hub, visite a página Integrações do console do Security Hub CSPM 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 CSPM.

AWS IoT Device Defender A auditoria envia resumos de verificação para o Security Hub CSPM, 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 CSPM. A auditoria também envia atualizações de localização para o CSPM do Security Hub.

Para obter mais informações sobre essa integração, consulte Integração com o AWS Security Hub CSPM no Guia do AWS IoT Desenvolvedor.

Amazon Macie (envia descobertas)

O Amazon Macie é um serviço de segurança de dados que 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. Uma descoberta da Macie pode indicar que existe uma possível violação de política ou dados confidenciais em seu patrimônio de dados do Amazon S3.

Depois de habilitar o CSPM do Security Hub, o Macie começa automaticamente a enviar as descobertas da política para o CSPM do Security Hub. Você pode configurar a integração para também enviar descobertas de dados confidenciais para o CSPM do Security Hub.

No Security Hub CSPM, o tipo de descoberta de uma política ou descoberta de dados confidenciais é alterado para um valor compatível com o ASFF. Por exemplo, o tipo de `Policy:IAMUser/S3BucketPublic` descoberta no Macie é exibido como `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` no CSPM do Security Hub.

Macie também envia amostras de descobertas geradas para o Security Hub CSPM. 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 Avaliação das descobertas do Macie com o Security Hub no Guia do usuário do Amazon Macie.

Amazon Route 53 Resolver Firewall DNS (envia descobertas)

Com o Amazon Route 53 Resolver DNS Firewall, você pode filtrar e regular o tráfego DNS de saída para sua nuvem privada virtual (VPC). Você faz isso criando coleções reutilizáveis de regras de filtragem nos grupos de regras do Firewall do DNS, associando os grupos de regras à sua VPC e monitorando a atividade nos registros e métricas do Firewall do DNS. Com base na atividade, você pode ajustar o comportamento do DNS Firewall. O Firewall DNS é um recurso do Route 53 Resolver.

O Route 53 Resolver DNS Firewall pode enviar vários tipos de descobertas para o Security Hub CSPM:

- Descobertas relacionadas a consultas bloqueadas ou alertadas para domínios associados às listas de domínios AWS gerenciados, que são listas de domínios gerenciadas. AWS
- Descobertas relacionadas a consultas bloqueadas ou alertadas para domínios associados a uma lista de domínios personalizada que você define.
- Descobertas relacionadas a consultas bloqueadas ou alertadas pelo DNS Firewall Advanced, que é um recurso do Route 53 Resolver que pode detectar consultas associadas a ameaças avançadas de DNS, como algoritmos de geração de domínio () DGAs e tunelamento de DNS.

Depois de habilitar o Security Hub CSPM e o Route 53 Resolver DNS Firewall, o DNS Firewall começa automaticamente a enviar as descobertas de AWS Managed Domain Lists e DNS Firewall Advanced para o Security Hub CSPM. Para também enviar descobertas de uma lista de domínios personalizada ao CSPM do Security Hub, habilite manualmente a integração no CSPM do Security Hub.

No Security Hub CSPM, todas as descobertas do Route 53 Resolver DNS Firewall têm o seguinte tipo:. `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Para obter mais informações, consulte Enviando descobertas do Route 53 Resolver DNS Firewall para o Security Hub no Amazon Route 53 Developer Guide.

AWS Systems Manager Gerenciador de patches (envia descobertas)

AWS Systems Manager O Patch Manager envia as descobertas ao CSPM do 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 aplicação de patches em instâncias gerenciadas com atualizações relacionadas à segurança e outros tipos de atualizações.

Depois de habilitar o Security Hub CSPM, essa integração é ativada automaticamente. O Systems Manager Patch Manager começa imediatamente a enviar as descobertas para o Security Hub CSPM.

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 CSPM

Os AWS serviços a seguir são integrados ao Security Hub CSPM e recebem descobertas do Security Hub CSPM. Onde observado, o serviço integrado também pode atualizar as descobertas. Nesse

caso, encontrar atualizações feitas no serviço integrado também será refletido no CSPM do Security Hub.

AWS Audit Manager (Recebe descobertas)

AWS Audit Manager recebe descobertas do Security Hub CSPM. 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 de CSPM do Security Hub suportadas por AWS Audit Manager listam os controles para os quais o CSPM do Security Hub envia as descobertas ao Audit Manager.

Amazon Q Developer em aplicativos de bate-papo (recebe descobertas)

O Amazon Q Developer em aplicativos de bate-papo 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.

O Amazon Q Developer em aplicativos de bate-papo recebe descobertas do Security Hub CSPM.

Para saber mais sobre a integração do Amazon Q Developer em aplicativos de bate-papo com o Security Hub CSPM, consulte a visão geral da integração do CSPM do Security Hub no Guia do administrador do Amazon Q Developer em aplicativos de bate-papo.

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 CSPM com o Detective permite que você passe das descobertas da Amazon no GuardDuty Security Hub CSPM 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 CSPM ou no Detective.

Para descobertas recebidas de outros Serviços da AWS, o painel de detalhes da descoberta no console CSPM 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 CSPM 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 CSPM como fonte no console do Security Lake, na API do Security Lake ou. AWS CLI Depois de concluir essas etapas, o Security Hub CSPM começa a enviar todas as descobertas para o Security Lake.

O Security Lake normaliza automaticamente as descobertas do CSPM 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 CSPM do Security Hub.

Para obter mais informações sobre essa integração, incluindo instruções sobre como adicionar o CSPM do Security Hub como fonte e criar assinantes, consulte Integração com o CSPM do 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 CSPM e atualize essas descobertas no Security Hub CSPM.

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 CSPM do Security Hub Trusted Advisor e o Security Hub, a integração é atualizada automaticamente.

O Security Hub CSPM envia os resultados de suas AWS verificações de melhores práticas de segurança básica para. Trusted Advisor

Para obter mais informações sobre a integração do CSPM do Security Hub com Trusted Advisor, consulte Visualizando os controles do CSPM do AWS Security Hub no Support AWS User AWS Trusted Advisor Guide.

Integrações de produtos de terceiros com o Security Hub CSPM

AWS O Security Hub CSPM se integra a vários produtos de parceiros terceirizados. Uma integração pode realizar uma ou mais das seguintes ações:

- Envie as descobertas que ele gera para o Security Hub CSPM
- Receba descobertas do Security Hub CSPM
- Atualize as descobertas no Security Hub CSPM

As integrações que enviam descobertas para o Security Hub CSPM têm um Amazon Resource Name (ARN).

Uma integração pode não estar disponível em todos Regiões da AWS. Se uma integração não for suportada na região em que você está atualmente conectado no console CSPM do Security Hub, ela não aparecerá na página Integrações do console. Para obter uma lista das integrações que estão disponíveis nas regiões da China AWS GovCloud (US) Regions, consulteDisponibilidade de integrações por região.

`<Se você tiver uma solução de segurança e estiver interessado em se tornar um pa`
Para obter mais informações, consulte o Guia de integração de parceiros.

Visão geral das integrações de terceiros com o Security Hub CSPM

A tabela a seguir fornece uma visão geral das integrações de terceiros que podem enviar descobertas para o Security Hub CSPM ou receber descobertas do Security Hub CSPM.

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>:679703615338:product/armordefense/armoranywhere`
AttackIQ – AttackIQ	Envia descobertas	`arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform`

Integração	Direction	ARN (se aplicável)
Barracuda Networks – Cloud Security Guardian	Envia descobertas	`arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurityguardian`
BigID – BigID Enterprise	Envia descobertas	`arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise`
Blue Hexagon – Blue Hexagon forAWS	Envia descobertas	`arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws`
Check Point – CloudGuard IaaS	Envia descobertas	`arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas`
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`

Integração	Direction	ARN (se aplicável)
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`
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`

Integração	Direction	ARN (se aplicável)
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`
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`

Integração	Direction	ARN (se aplicável)
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`
NETSCOUT – NETSCOUT Cyber Investigator	Envia descobertas	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Envia descobertas	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`

Integração	Direction	ARN (se aplicável)
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`
SecureCloudDB – SecureCloudDB	Envia descobertas	`arn:aws:securityhub: <REGION>::product/securecloudddb/securecloudddb`

Integração	Direction	ARN (se aplicável)
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>:064897671886: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`
Symantec – Cloud Workload Protection	Envia descobertas	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`

Integração	Direction	ARN (se aplicável)
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
Dynatrace	Recebe descobertas	Não aplicável
Fortinet – FortiCNP	Recebe descobertas	Não aplicável
IBM – QRadar	Recebe descobertas	Não aplicável
Logz.io Cloud SIEM	Recebe descobertas	Não aplicável
MetricStream	Recebe descobertas	Não aplicável

Integração	Direction	ARN (se 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
Caveonix – Caveonix Cloud	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`

Integração	Direction	ARN (se aplicável)
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 CSPM

As seguintes integrações de produtos de parceiros terceirizados podem enviar descobertas para o Security Hub CSPM. O Security Hub CSPM transforma as descobertas no formato de descoberta de AWS segurança.

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 CSPM 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`

Aqua Cloud Native Security Platform (CSP)fornece segurança de ciclo de vida completo para aplicativos baseados em contêineres e sem servidor, desde seu CI/CD pipeline até ambientes de produção em tempo de execução.

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

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`

Claroty xDomeajuda as organizações a proteger seus sistemas ciberfísicos em toda a Internet das Coisas (XIoT) estendida em ambientes industriais (OT), de saúde (IoT) 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`

Contrast Security Contrast Assessé uma ferramenta IAST que oferece detecção de vulnerabilidades em tempo real em aplicativos da web e microsserviços. APIs Contrast Assessintegra-se ao Security Hub CSPM para ajudar a fornecer visibilidade e resposta centralizadas para todas as suas cargas de trabalho.

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.

AWS Link do Marketplace

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 e recursos de nuvem em busca de falhas de segurança e lacunas na privacidade de dados para evitar violações de AppSec dados. APIs

Link do produto

Documentação do parceiro

Drata

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataé uma plataforma de automação de conformidade que ajuda você a alcançar e manter a conformidade com várias estruturas SOC2, como ISO e GDPR. A integração entre o Security Hub Drata e o CSPM 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

Orca Cloud Security Platform

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Ele Orca Cloud Security Platform identifica, prioriza e corrige riscos e problemas de conformidade em todo o seu ambiente de nuvem. Orca'sA plataforma orientada por IA, sem agentes, oferece uma cobertura abrangente de detecção de vulnerabilidades, configurações incorretas, movimentos laterais, riscos de API, dados confidenciais, eventos e comportamentos anômalos e identidades excessivamente permissivas.

Orcaintegra-se ao Security Hub CSPM para trazer telemetria profunda de segurança em nuvem para o Security Hub CSPM. Orca, usando sua SideScanning tecnologia, prioriza o risco em toda a infraestrutura de nuvem, cargas de trabalho, aplicativos, dados APIs, identidades e muito mais.

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`

Prisma Cloud Computeé uma plataforma de cibersegurança nativa da 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 Security Hub Plerion e o CSPM 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`

Rapid7 InsightVMfornece gerenciamento de vulnerabilidades para ambientes modernos, permitindo que você encontre, priorize e corrija vulnerabilidades com eficiência.

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 CSPM como descobertas, ajudando desenvolvedores e equipes de segurança a visualizá-los e priorizá-los junto com o restante de suas descobertas de segurança. AWS

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

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`

Cloud Workload Protectionfornece proteção completa para suas EC2 instâncias da Amazon com antimalware, prevenção de intrusões e monitoramento da 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 CSPM do Security Hub em tempo real, aumentando a visibilidade de seus AWS recursos e detalhes do Trend Micro Cloud One evento no CSPM do 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 CSPM para visualizar e responder aos problemas que o Wiz detecta no console CSPM do Security Hub.

AWS Link do Marketplace

Documentação do parceiro

Integrações de terceiros que recebem descobertas do Security Hub CSPM

As seguintes integrações de produtos de parceiros terceirizados podem receber descobertas do Security Hub CSPM. Onde indicado, o produto também pode atualizar as descobertas. Nesse caso, as atualizações feitas nas descobertas no produto do parceiro também são refletidas no CSPM do Security Hub.

Atlassian - Jira Service Management

Tipo de integração: recebimento e atualização

O AWS Service Management Connector for Jira envia as descobertas do CSPM do Security Hub para. Jira Jiraos problemas são criados com base nas descobertas. Quando os Jira problemas são atualizados, as descobertas correspondentes são atualizadas no CSPM do 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 CSPM — Integração bidirecional com. 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 CSPM do Security Hub para. Jira As descobertas desencadeiam a criação de problemas no Jira Service Management

Cloud. Quando você atualiza esses problemas noJira Service Management Cloud, as descobertas correspondentes também são atualizadas no CSPM do 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 CSPM garante que incidentes essenciais relacionados à segurança sejam encaminhados às equipes apropriadas para resolução imediata.

Link do produto

Documentação do parceiro

Dynatrace

Tipo de integração: recebimento

A Dynatrace integração com o Security Hub CSPM ajuda a unificar, visualizar e automatizar as descobertas de segurança em todas as ferramentas e ambientes. Adicionar contexto Dynatrace de tempo de execução às descobertas de segurança permite uma priorização mais inteligente, ajuda a reduzir o ruído dos alertas e concentra suas DevSecOps equipes na correção eficiente dos problemas críticos que afetam seus ambientes de produção e aplicativos.

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 CSPM, 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

New Relic Vulnerability Managementrecebe descobertas de segurança do Security Hub CSPM, para que você possa ter uma visão centralizada da segurança junto 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 combinado com os alertas de segurança agregados e organizados do Security Hub CSPM, PagerDuty permite que as equipes automatizem seu 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

Palo Alto VM-Seriesa integração com o Security Hub CSPM coleta inteligência sobre ameaças e a envia para o firewall de VM-Series próxima geração 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 ServiceNow integração com o Security Hub CSPM permite que as descobertas de segurança do Security Hub CSPM sejam visualizadas internamente. ServiceNow ITSM Você também pode configurar ServiceNow para criar automaticamente um incidente ou problema ao receber uma descoberta do Security Hub CSPM.

Qualquer atualização desses incidentes e problemas resultará em atualizações das descobertas no CSPM do Security Hub.

Para uma visão geral da integração e de como ela funciona, assista ao vídeo AWS Security Hub CSPM - 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 CSPM 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 para o AWS Security Hub CSPM, 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 CSPM

As seguintes integrações de produtos de parceiros terceirizados podem enviar e receber descobertas do Security Hub CSPM.

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 e contêineres nativos da nuvem. VMs Integrado ao AWS Security Hub CSPM, 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

Integrando o Security Hub CSPM com produtos personalizados

Além das descobertas geradas por AWS serviços integrados e produtos de terceiros, o CSPM do AWS Security Hub pode consumir descobertas geradas por outros produtos de segurança personalizados.

Você pode enviar essas descobertas para o CSPM do Security Hub usando a BatchImportFindingsoperação da API CSPM do Security Hub. Você pode usar a mesma operação para atualizar descobertas de produtos personalizados que você já enviou para o CSPM do Security Hub.

Ao configurar a integração personalizada, use as diretrizes e listas de verificação fornecidas no Guia de integração de parceiros CSPM do Security Hub.

Requisitos e recomendações para integrações de produtos personalizados

Antes de invocar com êxito a operação da `BatchImportFindings`API, você deve habilitar o CSPM do Security Hub.

Você também deve fornecer detalhes da descoberta para o produto personalizado usando o the section called “Formato de busca: ASFF”. Revise os seguintes requisitos e recomendações para integrações de produtos personalizados:

Configurar o ARN do produto

Quando você ativa o CSPM do Security Hub, um produto padrão Amazon Resource Name (ARN) para o Security Hub CSPM 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 os nomes da empresa e do produto

Você pode usar `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 CSPM.

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 CSPM do Security Hub e no JSON de cada descoberta. Consulte BatchImportFindings para encontrar fornecedores.

Definindo a descoberta IDs

Você deve fornecer, gerenciar e incrementar sua própria descoberta usando IDs o `Id`atributo.

Cada nova descoberta deve ter um ID de descoberta exclusivo. Se o produto personalizado enviar várias descobertas com o mesmo ID de descoberta, o CSPM do 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 seguintes integrações de produtos personalizados como um guia para criar sua própria solução personalizada:

Enviando descobertas de Chef InSpec escaneamentos para o Security Hub CSPM

Você pode criar um AWS CloudFormation modelo que executa uma verificação de Chef InSpec conformidade e, em seguida, envia as descobertas para o CSPM do Security Hub.

Para obter mais detalhes, consulte Monitoramento contínuo de conformidade com o Chef InSpecAWS Security Hub CSPM.

Enviando vulnerabilidades de contêiner detectadas pelo Trivy Security Hub CSPM

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 CSPM.

Para obter mais detalhes, consulte Como criar um CI/CD pipeline para verificação de vulnerabilidades de contêineres com Trivy o AWS Security Hub CSPM.

Criando e atualizando descobertas no Security Hub CSPM

No AWS Security Hub CSPM, uma descoberta é um registro observável de uma verificação de segurança ou detecção relacionada à segurança. Uma descoberta pode se originar de uma das seguintes fontes:

- Uma verificação de segurança para um controle no Security Hub CSPM.
- Uma integração com outra AWS service (Serviço da AWS).
- Uma integração com um produto de terceiros.
- Uma integração personalizada.

O Security Hub CSPM normaliza as descobertas de todas as fontes em uma sintaxe e formato padrão chamados AWS Security Finding Format (ASFF). Para obter informações detalhadas sobre esse formato, incluindo descrições de campos individuais do ASFF, consulteAWS Formato de descoberta de segurança (ASFF). Se você habilitar a agregação entre regiões, o Security Hub CSPM também agregará automaticamente descobertas novas e atualizadas de todas as regiões vinculadas a uma região de agregação especificada por você. Para obter mais informações, consulte Entendendo a agregação entre regiões no Security Hub CSPM.

Depois que uma descoberta é criada, ela pode ser atualizada da seguinte forma:

- Um provedor de busca pode usar a BatchImportFindingsoperação da API CSPM do Security Hub para atualizar informações gerais sobre a descoberta. Os provedores de descoberta só podem atualizar as descobertas que eles criaram.
- Um cliente pode usar o console CSPM do Security Hub ou a BatchUpdateFindingsoperação da API CSPM do Security Hub para atualizar o status da investigação sobre a descoberta. A `BatchUpdateFindings` operação também pode ser usada por um SIEM, emissão de bilhetes, gerenciamento de incidentes, SOAR ou outro tipo de ferramenta em nome de um cliente.

Para reduzir o ruído de busca e agilizar o rastreamento e a análise de descobertas individuais, o Security Hub CSPM exclui automaticamente as descobertas que não foram atualizadas recentemente. O tempo em que o Security Hub CSPM faz isso depende se a descoberta está ativa ou arquivada:

- Uma descoberta ativa é uma descoberta cujo estado de registro (`RecordState`) é`ACTIVE`. O Security Hub CSPM armazena descobertas ativas por 90 dias. Se uma descoberta ativa não for atualizada por 90 dias, ela expirará e o Security Hub CSPM a excluirá permanentemente.
- Uma descoberta arquivada é uma descoberta cujo estado de registro (`RecordState`) é`ARCHIVED`. O Security Hub CSPM armazena as descobertas arquivadas por 30 dias. Se uma descoberta arquivada não for atualizada por 30 dias, ela expirará e o Security Hub CSPM a excluirá permanentemente.

Para descobertas de controle, que são descobertas que o Security Hub CSPM gera a partir de verificações de segurança para controles, o Security Hub CSPM determina se uma descoberta expirou com base no valor do campo da `UpdatedAt` descoberta. Se esse valor foi há mais de 90 dias para uma descoberta ativa, o Security Hub CSPM exclui permanentemente a descoberta. Se esse valor foi há mais de 30 dias para uma descoberta arquivada, o Security Hub CSPM exclui permanentemente a descoberta.

Para todos os outros tipos de descobertas, o Security Hub CSPM determina se uma descoberta expirou com base nos valores dos `UpdatedAt` campos `ProcessedAt` e da descoberta. O Security Hub CSPM compara os valores desses campos e determina qual é o mais recente. Se o valor mais recente foi há mais de 90 dias para uma descoberta ativa, o Security Hub CSPM exclui permanentemente a descoberta. Se o valor mais recente foi há mais de 30 dias para uma descoberta arquivada, o Security Hub CSPM exclui permanentemente a descoberta. A localização de provedores pode alterar o valor do `UpdatedAt` campo de uma ou mais descobertas usando a BatchImportFindingsoperação da API CSPM do Security Hub.

Para retenção de resultados a longo prazo, você pode exportar descobertas para um bucket do S3. Você pode fazer isso usando uma ação personalizada com uma EventBridge regra da Amazon. Para obter mais informações, consulte Usando EventBridge para resposta e remediação automatizadas.

Tópicos

- BatchImportFindings para encontrar fornecedores
- BatchUpdateFindings para clientes
- Analisando os detalhes e o histórico da descoberta no Security Hub CSPM
- Filtrando descobertas no Security Hub CSPM
- Agrupando as descobertas no Security Hub CSPM
- Definindo o status do fluxo de trabalho das descobertas no Security Hub CSPM
- Enviando descobertas para uma ação CSPM personalizada do Security Hub

- AWS Formato de descoberta de segurança (ASFF)

BatchImportFindings para encontrar fornecedores

Os provedores de localização podem usar a BatchImportFindingsoperação para criar novas descobertas no CSPM do AWS Security Hub. Eles também podem usar essa operação para atualizar as descobertas que criaram. Encontrar fornecedores não pode atualizar descobertas que eles não criaram.

Clientes SIEMs, emissão de bilhetes, SOAR e outros tipos de ferramentas devem usar a BatchUpdateFindingsoperação para fazer atualizações relacionadas à investigação das descobertas de fornecedores. Para obter mais informações, consulte the section called “BatchUpdateFindings para clientes”.

Quando o Security Hub CSPM recebe uma `BatchImportFindings` solicitação para criar ou atualizar uma descoberta, ele gera automaticamente um Security Hub Findings - Importedevento na Amazon. EventBridge Você pode realizar ações automatizadas em relação a esse evento. Para obter mais informações, consulte the section called “Resposta e remediação automatizadas”.

Pré-requisitos para usar o **`BatchImportFindings`**

`BatchImportFindings` deve ser um dos seguintes:

- A conta da AWS associada com as descobertas. O identificador da conta associada deve corresponder ao valor do atributo `AwsAccountId` da descoberta.
- Uma conta que está listada como uma integração oficial de parceiros CSPM do Security Hub.

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

Determinar se uma descoberta deve ser criada ou atualizada

Para determinar se uma descoberta deve ser criada ou atualizada, o Security Hub CSPM verifica o `ID` campo. Se o valor de `ID` não corresponder a uma descoberta existente, o Security Hub CSPM cria uma nova descoberta.

Se `ID` corresponder a uma descoberta existente, o Security Hub CSPM verifica a atualização `UpdatedAt` no campo e procede da seguinte forma:

- Se `UpdatedAt` a atualização corresponder ou ocorrer antes `UpdatedAt` na descoberta existente, o CSPM do Security Hub ignorará a solicitação de atualização.
- Se `UpdatedAt` a atualização ocorrer após `UpdatedAt` a descoberta existente, o Security Hub CSPM atualizará a descoberta existente.

Restrições a atualizações de descobertas com **`BatchImportFindings`**

Para uma descoberta existente, os provedores de descobertas não podem usar `BatchImportFindings` para atualizar os seguintes atributos e objetos:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

O CSPM do Security Hub ignora qualquer conteúdo fornecido em uma `BatchImportFindings` solicitação desses atributos. Clientes ou entidades que atuam em seu nome (como ferramentas de criação de tíquetes) podem usar `BatchUpdateFindings` para atualizar esses atributos.

Atualizar descobertas com FindingProviderFields

Os provedores de busca também não devem ser usados `BatchImportFindings` para atualizar os seguintes atributos de nível superior no AWS Security Finding Format (ASFF):

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Em vez disso, os provedores de descobertas devem usar 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 `BatchImportFindings` solicitações, o Security Hub CSPM manipula valores nos atributos de nível superior e da seguinte forma `FindingProviderFields`.

(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 CSPM atualiza o valor do atributo em. `FindingProviderFields`

Ele só replica o valor para o atributo de nível superior se o atributo ainda não foi atualizado por `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 CSPM usa o valor para atualizar o atributo em. `FindingProviderFields` Ele sobrescreve qualquer valor existente.

O Security Hub CSPM atualiza o atributo de nível superior somente se o atributo ainda não tiver sido atualizado pelo. `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 CSPM 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 CSPM usa os dois valores. No entanto, ele atualiza o atributo de nível superior somente se o atributo ainda não tiver sido atualizado por `BatchUpdateFindings`.

BatchUpdateFindings para clientes

AWS Os clientes do CSPM do Security Hub e as entidades que atuam em seu nome podem usar a BatchUpdateFindingsoperação para atualizar as informações relacionadas ao processamento das descobertas do CSPM do Security Hub na busca de fornecedores. Como cliente, você pode usar essa operação diretamente. Ferramentas de SIEM, emissão de tíquetes, gerenciamento de incidentes e SOAR também podem usar essa operação em nome de um cliente.

Você não pode usar a `BatchUpdateFindings` operação para criar novas descobertas. No entanto, você pode usá-lo para atualizar até 100 descobertas existentes por vez. Em uma `BatchUpdateFindings` solicitação, você especifica quais descobertas atualizar, quais campos do Formato de Descoberta de AWS Segurança (ASFF) devem ser atualizados para as descobertas e os novos valores para os campos. Em seguida, o Security Hub CSPM atualiza as descobertas conforme especificado em sua solicitação. Esse processo pode levar alguns minutos. Se você atualizar as descobertas usando a `BatchUpdateFindings` operação, suas atualizações não afetarão os valores existentes no `UpdatedAt` campo das descobertas.

Quando o Security Hub CSPM recebe uma `BatchUpdateFindings` solicitação para atualizar uma descoberta, ele gera automaticamente um Security Hub Findings – Importedevento na Amazon. EventBridge Opcionalmente, você pode usar esse evento para realizar uma ação automática na descoberta especificada. Para obter mais informações, consulte the section called “Resposta e remediação automatizadas”.

Campos disponíveis para BatchUpdateFindings

Se você estiver conectado a uma conta de administrador do Security Hub CSPM, você pode usar `BatchUpdateFindings` para atualizar as descobertas que foram geradas pela conta do administrador ou pelas contas dos membros. As contas-membro só podem usar `BatchUpdateFindings` para atualizar descobertas para sua própria conta.

Os clientes podem usar `BatchUpdateFindings` para atualizar os seguintes campos e objetos:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Configurar o acesso ao BatchUpdateFindings

Você pode configurar políticas AWS Identity and Access Management (IAM) para restringir o acesso ao uso `BatchUpdateFindings` para atualizar campos de busca 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`, você pode 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 instrução a seguir indica que `BatchUpdateFindings` não pode ser usado para atualizar o campo `Workflow.Status` das descobertas.

```
{
    "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"
        ]
    }
}
```

Analisando os detalhes e o histórico da descoberta no Security Hub CSPM

No AWS Security Hub CSPM, uma descoberta é um registro observável de uma verificação de segurança ou detecção relacionada à segurança. O Security Hub CSPM gera uma descoberta ao concluir uma verificação de segurança de um controle e ao ingerir uma descoberta de um produto integrado AWS service (Serviço da AWS) ou de terceiros. Cada descoberta inclui um histórico de alterações e outros detalhes, como uma classificação de gravidade e informações sobre os recursos afetados.

Você pode revisar o histórico e outros detalhes de descobertas individuais no console CSPM do Security Hub ou programaticamente com a API CSPM do Security Hub ou o. AWS CLI

Para ajudá-lo a simplificar sua análise, o console CSPM do Security Hub exibe um painel de descoberta quando você escolhe uma descoberta específica. O painel inclui diferentes menus e guias para revisar detalhes específicos de uma descoberta.

Menu Ações

Nesse menu, você pode revisar o JSON completo de uma descoberta ou adicionar observações. Uma descoberta só pode ter uma nota anexada a ela por vez. Esse menu também fornece opções para definir o status do fluxo de trabalho de uma descoberta ou enviar uma descoberta para uma ação personalizada na Amazon EventBridge.

Menu Investigar

Nesse menu, é possível investigar uma descoberta no Amazon Detective. Detective extrai entidades, como endereços IP e AWS usuários, de uma descoberta e visualiza suas atividades. Você pode usar a atividade da entidade como ponto de partida para investigar a causa e o impacto de uma descoberta.

Guia visão geral

Essa guia fornece um resumo de uma descoberta. Por exemplo, você pode determinar quando uma descoberta foi criada e atualizada pela última vez, em qual conta ela existe e a origem da descoberta. Para descobertas de controle, essa guia também mostra o nome da AWS Config regra associada e um link para a orientação de remediação na documentação do CSPM do Security Hub.

No instantâneo de recursos na guia Visão geral, você pode obter uma breve visão geral dos recursos envolvidos em uma descoberta. Para alguns recursos, isso inclui uma opção de recurso aberto, vinculada diretamente a um recurso afetado no AWS service (Serviço da AWS) console relevante. O snapshot Histórico mostra até duas alterações feitas na descoberta na data mais recente de acompanhamento do histórico. Por exemplo, se você fez uma alteração ontem e outra hoje, o instantâneo mostra a alteração de hoje. Para revisar as entradas anteriores, vá para a guia Histórico.

A linha Conformidade se expande para mostrar mais detalhes. Por exemplo, se um controle incluir parâmetros, você poderá revisar os valores dos parâmetros que o Security Hub CSPM usa atualmente ao realizar verificações de segurança para o controle.

Guia Recursos

Essa guia fornece detalhes sobre os recursos envolvidos em uma descoberta. Se você estiver conectado à conta proprietária de um recurso, poderá revisar o recurso no AWS service (Serviço da AWS) console aplicável. Se você não for o proprietário de um recurso, essa guia exibirá o Conta da AWS ID do proprietário.

A linha Detalhes mostra detalhes específicos do recurso em uma descoberta. Ela mostra a ResourceDetailsseção da descoberta no formato JSON.

A linha Tags mostra as chaves e os valores das tags que são atribuídos aos recursos envolvidos em uma descoberta. Os recursos compatíveis com a operação GetResources da AWS Resource Groups Tagging API podem ser marcados. O Security Hub CSPM chama essa operação usando uma função vinculada ao serviço ao processar descobertas novas ou atualizadas e recupera as tags de recursos se o campo AWS Security Finding Format (ASFF) `Resource.Id` for preenchido com o ARN de um recurso. O CSPM do Security Hub ignora o recurso inválido. IDs Para obter mais informações sobre a inclusão de tags de recursos nas descobertas, consulte Tags.

Aba Histórico

Essa guia rastreia o histórico de uma descoberta. O histórico da descoberta está disponível para descobertas ativas e arquivadas. Ele fornece uma trilha imutável das alterações feitas em uma descoberta ao longo do tempo, incluindo qual campo ASFF foi alterado, quando a alteração ocorreu e por qual usuário. Cada página na guia exibe até 20 alterações. As alterações mais recentes são exibidas primeiro.

Para descobertas ativas, o histórico de descobertas está disponível por até 90 dias. Para descobertas arquivadas, o histórico de descobertas está disponível por até 30 dias. O histórico de localização inclui alterações que foram feitas manualmente ou automaticamente pelas regras de automação CSPM do Security Hub. Ela não inclui alterações nos campos de carimbo de data/hora de nível superior, como os `CreatedAt` campos e. `UpdatedAt`

Se você estiver conectado a uma conta de administrador do CSPM do Security Hub, o histórico de localização é para a conta do administrador e para todas as contas dos membros.

Guia Ameaça

Essa guia inclui dados dos objetos Action, Malware e ProcessDetails do ASFF, incluindo o tipo de ameaça e se um recurso é o alvo ou o agente. Esses detalhes geralmente se aplicam às descobertas originadas na Amazon GuardDuty.

Guia Vulnerabilidades

Essa guia exibe dados do objeto Vulnerability do ASFF, incluindo se há explorações ou correções disponíveis associadas a uma descoberta. Esses detalhes normalmente se aplicam às descobertas originadas no Amazon Inspector.

As linhas em cada guia incluem uma opção de cópia ou filtro. Por exemplo, se você abrir o painel para uma descoberta que tem um status de fluxo de trabalho de Notificado, você pode escolher a opção de filtro ao lado da linha de status do fluxo de trabalho. Se você escolher Mostrar todas as descobertas com esse valor, o Security Hub CSPM filtra a tabela de descobertas e exibe somente as descobertas com o mesmo status de fluxo de trabalho.

Revisar os detalhes e o histórico das descobertas

Escolha seu método preferido e siga as etapas para verificar a localização de detalhes no CSPM do Security Hub.

Se você habilitar a agregação entre regiões e fizer login na região de agregação, os dados da descoberta incluirão os dados da região de agregação e das regiões vinculadas. Em outras regiões, os dados da descoberta são específicos apenas daquela região. Para obter mais informações sobre agregação entre regiões, consulte the section called “Agregando dados em todas as regiões”.

Security Hub CSPM console

Revisar os detalhes e o histórico das descobertas

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Para exibir uma lista de descobertas, execute um destes procedimentos:
   - No painel de navegação, selecione Descobertas. Adicione filtros de pesquisa conforme necessário para restringir a lista de descobertas.
   - No painel de navegação, escolha Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação, selecione Integrações. Escolha Ver descobertas para obter uma integração.
   - No painel de navegação, escolha Controles.
3. Escolha uma descoberta. O painel de descoberta exibe os detalhes da descoberta.
4. No painel de localização, faça o seguinte:
   - Para revisar detalhes específicos da descoberta, escolha uma guia.
   - Para agir sobre a descoberta, escolha uma opção no menu Ações.
   - Para investigar a descoberta no Amazon Detective, escolha uma opção Investigar.

> **Note**
>
> Se você se integrar AWS Organizations e estiver conectado a uma conta de membro, o painel de localização incluirá o nome da conta. Para contas de membros que são convidadas manualmente, em vez de por meio de Organizations, o painel de descoberta inclui apenas o ID da conta.

Security Hub CSPM API

Use a GetFindingsoperação da API CSPM do Security Hub ou, se estiver usando a AWS CLI, execute o get-findingscomando. Você pode fornecer um ou mais valores para o `Filters` parâmetro para restringir as descobertas a serem recuperadas.

Se o volume de resultados for muito grande, poderá usar o parâmetro `MaxResults` para limitar as descobertas a um determinado número e o parâmetro `NextToken` para paginar as descobertas. Use o parâmetro `SortCriteria` para classificar as descobertas por um campo específico.

Por exemplo, o AWS CLI comando a seguir recupera as descobertas que correspondem aos critérios de filtro especificados e classifica os resultados em ordem decrescente pelo `LastObservedAt` campo. 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
```

Para revisar o histórico da descoberta, use a operação GetFindingHistory. Se você estiver usando o AWS CLI, execute o get-finding-historycomando. Identifique a descoberta da qual você deseja obter o histórico com os campos `Id` e `ProductArn`. Para obter informações sobre esses campos, consulte AwsSecurityFindingIdentifier. Cada solicitação pode recuperar o histórico de apenas uma descoberta.

Por exemplo, o AWS CLI comando 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"
```

PowerShell

Use o cmdlet `Get-SHUBFinding`. Opcionalmente, preencha o `Filter` parâmetro para restringir as descobertas a serem recuperadas.

Por exemplo, o cmdlet a seguir recupera as descobertas que correspondem aos filtros especificados.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Se você filtrar as descobertas por `CompanyName` ou`ProductName`, o Security Hub CSPM usará os valores que fazem parte do objeto `ProductFields` ASFF. O Security Hub CSPM não usa o nível superior e os campos`CompanyName`. `ProductName`

Filtrando descobertas no Security Hub CSPM

AWS O Security Hub CSPM gera suas próprias descobertas a partir de verificações de segurança e recebe descobertas de produtos integrados. Você pode exibir uma lista de descobertas nas páginas Findings, Integrations e Insights do console CSPM do Security Hub. Você pode adicionar filtros para restringir uma lista de descobertas para que a lista seja relevante para sua organização ou caso de uso.

Para obter informações sobre a filtragem de descobertas para um controle de segurança específico, consultethe section called “Filtrar e classificar descobertas de controles”. As informações nesta página se aplicam às páginas Descobertas, Insights e Integrações.

Filtros padrão nas listas de busca

Por padrão, as listas de localização no console CSPM do Security Hub são filtradas com base nos `Workflow.Status` campos `RecordState` e do AWS Security Finding Format (ASFF). Isso é um acréscimo aos filtros para uma visão ou integração específica.

O estado do registro indica se uma descoberta está ativa ou arquivada. Por padrão, uma lista de descobertas mostra apenas descobertas ativas. Um provedor de descobertas pode arquivar uma descoberta se ela não estiver mais ativa ou não for mais importante. O Security Hub CSPM também arquiva automaticamente as descobertas de controle se o recurso associado for excluído.

O status do fluxo de trabalho indica o status da investigação de uma descoberta. Por padrão, uma lista de descobertas mostra somente as descobertas cujo fluxo de trabalho tem o status `NEW` ou `NOTIFIED`. Você pode atualizar o status do fluxo de trabalho de uma descoberta.

Instruções para adicionar filtros

Você pode filtrar uma lista de descobertas por até dez atributos. Para cada atributo, você pode fornecer até 20 valores de filtro.

Ao filtrar a lista de descobertas, o Security Hub CSPM aplica a `AND` lógica ao conjunto de filtros. Uma descoberta só corresponde 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, o Security Hub CSPM exibirá descobertas que correspondem a esses dois critérios.

O Security Hub CSPM aplica a `OR` lógica aos filtros que usam o mesmo atributo, mas valores diferentes. Por exemplo, se você adicionar ambos GuardDuty e o Amazon Inspector como valores de filtro para o nome do produto, o Security Hub CSPM exibirá descobertas que foram geradas por um ou pelo Amazon GuardDuty Inspector.

Para adicionar filtros a uma lista de descobertas (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Para exibir uma lista de descobertas, execute uma das seguintes ações no painel de navegação:
   - Escolha Descobertas.
   - Escolha Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - Escolha Integrations (Integrações). Escolha Ver descobertas para obter uma integração.
3. Na caixa Adicionar filtros, selecione um ou mais campos pelos quais filtrar.

   Quando você filtra por nome da empresa ou nome do produto, o console usa o nível superior `CompanyName` e os `ProductName` campos do Formato de descoberta de AWS segurança (ASFF). A API usa os valores que estão aninhados abaixo`ProductFields`.

4. Selecione o tipo de correspondência do filtro.

   Para um filtro de sequência de caracteres, você pode escolher entre as seguintes opções:

   - 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 o campo Tags de recursos, você pode filtrar com base em chaves ou valores específicos.

   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 Rótulo de gravidade não é BAIXO e o Rótulo de severidade não é MÉDIO, os resultados não incluirão descobertas 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 no mesmo campo.

5. Especifique o valor do filtro. Em filtros de strings, o valor do filtro diferencia letras maiúsculas de minúsculas.
6. Escolha Aplicar.

   Para um filtro existente, você pode alterar o tipo ou o valor de correspondência do filtro. Em uma lista filtrada de descobertas, escolha o filtro. Na caixa Editar filtro, escolha o novo tipo ou valor de correspondência e, em seguida, escolha Aplicar.

Para remover um filtro, escolha o ícone x. A lista é atualizada automaticamente para refletir a alteração.

Agrupando as descobertas no Security Hub CSPM

Você pode agrupar as descobertas no CSPM do AWS Security Hub 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 correspondentes.

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.

O Security Hub CSPM pode exibir até 100 valores para um atributo selecionado. Se houver mais de 100 valores, você verá somente os 100 primeiros.

Quando você escolhe um valor de atributo, o Security Hub CSPM exibe a lista de descobertas correspondentes para esse valor.

Para agrupar as descobertas em uma lista de descobertas (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Para exibir uma lista de descobertas, execute uma das seguintes ações no painel de navegação:
   - Escolha Descobertas.
   - Escolha Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - Escolha Integrations (Integrações). Escolha Ver descobertas para obter uma integração.
3. Na lista suspensa Agrupar por, escolha o atributo a ser usado para o agrupamento.

   Para remover um atributo do agrupamento, selecione o ícone x. Quando você remove o atributo de agrupamento, a lista muda da lista de valores de atributos para uma lista de descobertas.

Definindo o status do fluxo de trabalho das descobertas no Security Hub CSPM

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 e não afeta a geração de novas descobertas. Por exemplo, se você alterar o status do fluxo de trabalho de uma descoberta para `SUPPRESSED` ou`RESOLVED`, sua alteração não impede que o Security Hub CSPM gere uma nova descoberta para o mesmo problema.

O status do fluxo de trabalho de uma descoberta pode ser um dos seguintes valores.

NOVO

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 CSPM também redefine o status do fluxo de trabalho de um `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.

NOTIFICADO

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`.

SUPRIMIDO

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`.

RESOLVIDO

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, em caso afirmativo`PASSED`, `Compliance.Status` o Security Hub CSPM define automaticamente o status do fluxo de trabalho como. `RESOLVED`

Definir o status do fluxo de trabalho das descobertas

Para alterar o status do fluxo de trabalho de uma ou mais descobertas, você pode usar o console CSPM do Security Hub ou a API CSPM do Security Hub. Se você alterar o status do fluxo de trabalho de uma descoberta, observe que pode levar alguns minutos para o Security Hub CSPM processar sua solicitação e atualizar a descoberta.

> **Tip**
>
> Você também pode alterar o status do fluxo de trabalho das descobertas automaticamente usando regras de automação. Com as regras de automação, você configura o CSPM do Security Hub para atualizar automaticamente o status do fluxo de trabalho das descobertas com base nos critérios que você especifica. Para obter mais informações, consulte Entendendo as regras de automação no Security Hub CSPM.

Para alterar o status do fluxo de trabalho de uma ou mais descobertas, escolha seu método preferido e siga as etapas.

Security Hub CSPM console

Para alterar o status do fluxo de trabalho das descobertas

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

2. No painel de navegação, siga um destes procedimentos para exibir uma tabela de descobertas:

   - Escolha Descobertas.
   - Escolha Insights. Em seguida, escolha um insight. Nos resultados do insight, escolha um resultado.
   - Escolha Integrations (Integrações). Em seguida, na seção da integração, escolha Ver descobertas.
   - Escolha padrões de segurança. Em seguida, na seção do padrão, escolha Exibir resultados. Na tabela de controles, escolha um controle para exibir as descobertas do controle.

3. Na tabela de descobertas, marque a caixa de seleção para cada descoberta cujo status do fluxo de trabalho você deseja alterar.
4. Na parte superior da página, escolha Status do fluxo de trabalho e, em seguida, escolha o novo status do fluxo de trabalho para as descobertas selecionadas.
5. Na caixa de diálogo Definir status do fluxo de trabalho, opcionalmente, insira uma nota que detalha o motivo da alteração do status do fluxo de trabalho. Em seguida, escolha Definir status.

Security Hub CSPM API

Use a operação BatchUpdateFindings. Forneça o ID da descoberta e o ARN do produto que gerou a descoberta. Você pode obter esses detalhes usando a GetFindingsoperação.

AWS CLI

Execute o comando batch-update-findings. Forneça o ID da descoberta e o ARN do produto que gerou a descoberta. Você pode obter esses detalhes executando o comando 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"
```

Enviando descobertas para uma ação CSPM personalizada do Security Hub

Você pode criar ações personalizadas do AWS Security Hub CSPM para automatizar o CSPM do Security Hub com a Amazon. EventBridge Para ações personalizadas, o tipo de evento é Security Hub Findings - Custom Action. Depois de configurar uma ação personalizada, será possível enviar descobertas para ela. Para obter mais informações e etapas detalhadas sobre como criar ações personalizadas, consulte the section called “Resposta e remediação automatizadas”.

Como enviar descobertas para uma ação personalizada (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. Para exibir uma lista de descobertas, execute um destes procedimentos:
   - No painel de navegação CSPM do Security Hub, escolha Findings.
   - No painel de navegação CSPM do Security Hub, escolha Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação CSPM do Security Hub, escolha Integrações. Escolha Ver descobertas para obter uma integração.
   - No painel de navegação CSPM do Security Hub, escolha 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 CSPM consome e agrega descobertas de produtos integrados Serviços da AWS e de terceiros. O Security Hub CSPM 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.

Esta página fornece um resumo completo do JSON para uma descoberta no AWS Security Finding Format (ASFF). O formato deriva do esquema JSON. Escolha o nome de um objeto vinculado para revisar um exemplo de descoberta desse objeto. Comparar suas descobertas de CSPM do Security Hub com os recursos e exemplos mostrados aqui pode ajudá-lo a interpretar suas descobertas.

Para obter descrições dos atributos individuais do ASFF, consulte the section called “Atributos de nível superior do ASFT obrigatórios” e. the section called “Atributos de nível superior do ASFF opcionais”

```
"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",
    "Detection": {
     "Sequence": {
      "Uid": "string",
      "Actors": [{
       "Id": "string",
       "Session": {
        "Uid": "string",
        "MfAStatus": "string",
        "CreatedTime": "string",
        "Issuer": "string"
       },
       "User": {
        "CredentialUid": "string",
        "Name": "string",
        "Type": "string",
        "Uid": "string",
        "Account": {
         "Uid": "string",
         "Name": "string"
        }
       }
      }],
      "Endpoints": [{
       "Id": "string",
       "Ip": "string",
       "Domain": "string",
       "Port": number,
       "Location": {
        "City": "string",
        "Country": "string",
        "Lat": number,
```

```
          "Lon": number
         },
         "AutonomousSystem": {
          "Name": "string",
          "Number": number
         },
         "Connection": {
          "Direction": "string"
         }
        }],
        "Signals": [{
         "Id": "string",
         "Title": "string",
         "ActorIds": ["string"],
         "Count": number,
         "FirstSeenAt": number,
         "SignalIndicators": [
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
          },
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
          }
         ],
         "LastSeenAt": number,
         "Name": "string",
         "ResourceIds": ["string"],
         "Type": "string"
        }],
        "SequenceIndicators": [
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
         },
         {
          "Key": "string",
          "Title": "string",
          "Values": ["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"
      },
      "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"
      },
      "CodeRepository": {
       "CodeSecurityIntegrationArn": "string",
       "ProjectName": "string",
       "ProviderType": "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

AWS O Security Hub CSPM oferece dois tipos de consolidação para controles:

- Visualização de controles consolidados — Com esse tipo de consolidação, cada controle tem um único identificador em todos os padrões. Além disso, no console CSPM do Security Hub, a página Controles exibe todos os controles em todos os padrões.
- Descobertas de controle consolidadas — Com esse tipo de consolidação, o Security Hub CSPM produz uma única descoberta para um controle, mesmo que o controle se aplique a vários padrões habilitados. Isso pode reduzir o ruído de localização.

Você não pode ativar ou desativar a exibição de controles consolidados. As descobertas de controle consolidadas são habilitadas por padrão se você habilitar o CSPM do Security Hub em ou após 23 de fevereiro de 2023. Caso contrário, ele será desativado por padrão. No entanto, para organizações, as descobertas de controle consolidado são habilitadas para contas de membros do CSPM do Security Hub somente se estiverem habilitadas para a conta do administrador. Para saber mais sobre as descobertas do controle consolidado, consulteGerando e atualizando descobertas de controle.

Ambos os tipos de consolidação afetam campos e valores das descobertas de controle noAWS Formato de descoberta de segurança (ASFF).

Tópicos

- Visualização de controles consolidados - Alterações no ASFF
- Descobertas de controle consolidadas - Alterações no ASFF

- Gerador IDs antes e depois, permitindo descobertas de controle consolidadas
- Como a consolidação afeta o controle IDs e os títulos
- Atualização de fluxos de trabalho para consolidação

Visualização de controles consolidados - Alterações no ASFF

O recurso de visualização de controles consolidados introduziu as seguintes alterações nos campos e valores das descobertas de controle no ASFF. Se seus fluxos de trabalho não dependerem de valores para esses campos ASFF, nenhuma ação será necessária. Se você tiver fluxos de trabalho que dependem de valores específicos para esses campos, atualize seus fluxos de trabalho para usar os valores atuais.

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor da amostra após a visualização dos controles consolidados e uma descrição da alteração
Conformidade. SecurityControlId	Não aplicável (campo novo)	EC22. 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 “:" standards/aws-foundational-security-best-practices/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 da amostra após a visualização dos controles consolidados e uma 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 CSPM arquivou as descobertas existentes.
ProductFields. ArchivalReasons:0/ ReasonCode	Não aplicável (campo novo)	"CONSOLIDATED_CONTROL_FINDINGS_UPDATE" Fornece o motivo pelo qual o Security Hub CSPM arquivou as descobertas existentes.
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.

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor da amostra após a visualização dos controles consolidados e uma descrição da alteração
Remediation.Recommendation.Text	“Para obter instruções sobre como corrigir esse problema, consulte a documentação do CSPM PCI DSS do AWS Security Hub.”	“Para obter instruções sobre como corrigir esse problema, consulte a documentação de controles CSPM 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 habilitar descobertas de controle consolidadas, poderá ser afetado pelas seguintes alterações nos campos e valores das descobertas de controle no ASFF. Essas alterações são adicionais às alterações introduzidas pelo recurso de visualização de controles consolidados. Se seus fluxos de trabalho não dependerem de valores para esses campos ASFF, nenhuma ação será necessária. Se você tiver fluxos de trabalho que dependem de valores específicos para esses campos, atualize seus fluxos de trabalho para usar os valores atuais.

> **Tip**
>
> Se você usa a solução Automated Security Response na AWS v2.0.0, observe que ela oferece suporte a descobertas de controle consolidadas. Isso significa que você pode manter seus fluxos de trabalho atuais se habilitar descobertas de controle consolidadas.

Campo do ASFF	Exemplo de valor antes de permitir descobertas consolidadas de controle	Exemplo de valor após habilitar resultados de controle consolidados e uma descrição da mudança
GeneratorId	aws-foundational-security-best-1practices/v/1.0.0/Config.	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 referencia mais informações específicas do padrão.
Id	arn: aws: hub de segurança: eu-central- 1:123456789012:6d6a26-a156-48f0-9403-115983e5a956 subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab	arn:aws:securityhub:eu-central- 1:123456789012: security-6d6a26-a156-48f0-9403-115983e5a956 control/iam.9/finding/ab Esse campo não faz mais referência a um padrão.
ProductFields.ControlId	FOTO. 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.

Campo do ASFF	Exemplo de valor antes de permitir descobertas consolidadas de controle	Exemplo de valor após habilitar resultados de controle consolidados e uma descrição da mudança
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.

Gravidade	"Severidade": {
	
	"Product": 90,
	
	"Etiqueta": "CRÍTICO",
	
	"Normalizado": 90,
	
	"Original": "CRÍTICO"
	
	}
		"Severidade": {
		
		"Etiqueta": "CRÍTICO",
		
		"Normalizado": 90,
		
		"Original": "CRÍTICO"
		
		}
		
		O Security Hub CSPM não usa mais o campo Produto para descrever a gravidade de uma descoberta.

Tipos	["Software e configuração Checks/Industry e padrões regulatórios/PCI-DSS"]	["Software e configuração Checks/Industry e padrões regulatórios"] Esse campo não faz mais referência a um padrão.

Campo do ASFF	Exemplo de valor antes de permitir descobertas consolidadas de controle	Exemplo de valor após habilitar resultados de controle consolidados e uma descrição da mudança
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 mostrará os requisitos relacionados em todos os padrões habilitados.
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::: /1.0.0 standards/aws-foundational-security-best-practices/v	Removido. Consulte `Compliance.AssociatedStandards` em vez disso.

Campo do ASFF	Exemplo de valor antes de permitir descobertas consolidadas de controle	Exemplo de valor após habilitar resultados de controle consolidados e uma descrição da mudança
ProductFields.StandardsControlArn	arn: aws: securityhub: us-east-1:123456789012:1 control/aws-foundational-security-best-practices/v/1.0.0/Config	Removido. O Security Hub CSPM gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.StandardsGuideArn	arn: aws:securityhub::: /1.2.0 ruleset/cis-aws-foundations-benchmark/v	Removido. Consulte `Compliance.AssociatedStandards` em vez disso.
ProductFields.StandardsGuideSubscriptionArn	arn: aws: hub de segurança: us-east- 2:123456789012: /1.2.0 subscription/cis-aws-foundations-benchmark/v	Removido. O Security Hub CSPM gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.StandardsSubscriptionArn	arn: aws: hub de segurança: us-east- 1:123456789012: /1.0.0 subscription/aws-foundational-security-best-practices/v	Removido. O Security Hub CSPM gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.aws/securityhub/FindingId	arn: aws: hub de segurança: us-east-1:: /751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding	arn: aws: hub de segurança: us-east-1:: /751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding Esse campo não faz mais referência a um padrão.

Os valores de campos do ASFF fornecidos pelo cliente após ativar as descobertas de controles consolidadas

Se você habilitar descobertas de controle consolidadas, o Security Hub CSPM gera uma descoberta em todos os padrões e arquiva as descobertas originais (descobertas separadas para cada padrão).

As atualizações feitas nas descobertas originais usando o console CSPM do Security Hub ou a BatchUpdateFindingsoperação não serão preservadas nas novas descobertas. Se necessário, você pode recuperar esses dados consultando as descobertas arquivadas. Para revisar as descobertas arquivadas, você pode usar a página Descobertas no console CSPM do Security Hub e definir o filtro de estado do registro como ARQUIVADO. Como alternativa, você pode usar a GetFindingsoperação da API CSPM do Security Hub.

Campo do ASFF fornecido pelo cliente	Descrição da mudança após permitir 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 (corresponde 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`.

Gerador IDs antes e depois, permitindo descobertas de controle consolidadas

A tabela a seguir lista as alterações nos valores de ID do gerador para controles quando você ativa as descobertas de controle consolidadas. Essas alterações se aplicam aos controles que o Security Hub CSPM suportou a partir de 15 de fevereiro de 2023.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
arn: aws:securityhub::: /1.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1CloudWatch.
arn: aws:securityhub::: /1.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.16
arn: aws:securityhub::: /1.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.17
arn: aws:securityhub::: /1.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.4
arn: aws:securityhub::: /1.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.9
arn: aws:securityhub::: /1.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.6
arn: aws:securityhub::: /1.16 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.2
arn: aws:securityhub::: /1.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.5
arn: aws:securityhub::: /1.20 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.18
arn: aws:securityhub::: /1.22 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
arn: aws:securityhub::: /1.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.8
arn: aws:securityhub::: /1.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.3
arn: aws:securityhub::: /1.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.11
arn: aws:securityhub::: /1.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.12
arn: aws:securityhub::: /1.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.13
arn: aws:securityhub::: /1.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.14
arn: aws:securityhub::: /1.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.15
arn: aws:securityhub::: /2.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1CloudTrail.
arn: aws:securityhub::: /2.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 4CloudTrail.
arn: aws:securityhub::: /2.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 6CloudTrail.
arn: aws:securityhub::: /2.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 5CloudTrail.
arn: aws:securityhub::: /2.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/Config.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
arn: aws:securityhub::: /2.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 7CloudTrail.
arn: aws:securityhub::: /2.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 2CloudTrail.
arn: aws:securityhub::: /2.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/KMS.4
arn: aws:securityhub::: /2.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 6EC2.
arn: aws:securityhub::: /3.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 2CloudWatch.
arn: aws:securityhub::: /3.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 3CloudWatch.
arn: aws:securityhub::: /3.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1CloudWatch.
arn: aws:securityhub::: /3.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 4CloudWatch.
arn: aws:securityhub::: /3.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 5CloudWatch.
arn: aws:securityhub::: /3.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 6CloudWatch.
arn: aws:securityhub::: /3.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 7CloudWatch.
arn: aws:securityhub::: /3.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 8CloudWatch.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
arn: aws:securityhub::: /3.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 9CloudWatch.
arn: aws:securityhub::: /3.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.0 CloudWatch
arn: aws:securityhub::: /3.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.1 CloudWatch
arn: aws:securityhub::: /3.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.2 CloudWatch
arn: aws:securityhub::: /3.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.3 CloudWatch
arn: aws:securityhub::: /3.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.4 CloudWatch
arn: aws:securityhub::: /4.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.3 EC2
arn: aws:securityhub::: /4.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 1.4 EC2
arn: aws:securityhub::: /4.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	controle de segurança/ 2EC2.
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

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
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
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	controle de segurança/ 7EC2.
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	controle de segurança/ 6EC2.
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.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
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/ 1.0 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4,11	controle de segurança/ 1.1 CloudWatch
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	controle de segurança/ 2.1 EC2
cis-aws-foundations-benchmark/v/1.4.0/5.3	controle de segurança/ 2EC2.
aws-foundational-security-best- 1practices/ v/1.0.0/Account.	security-control/Account.1
aws-foundational-security-best- 1practices/ v/1.0.0/ACM.	security-control/ACM.1
aws-foundational-security-best- 1practices/ v/1.0.0/APIGateway.	controle de segurança/ 1APIGateway.
aws-foundational-security-best- 2practices/ v/1.0.0/APIGateway.	controle de segurança/ 2APIGateway.
aws-foundational-security-best- 3practices/ v/1.0.0/APIGateway.	controle de segurança/ 3APIGateway.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 4practices/ v/1.0.0/APIGateway.	controle de segurança/ 4APIGateway.
aws-foundational-security-best- 5practices/ v/1.0.0/APIGateway.	controle de segurança/ 5APIGateway.
aws-foundational-security-best- 8practices/ v/1.0.0/APIGateway.	controle de segurança/ 8APIGateway.
aws-foundational-security-best- 9practices/ v/1.0.0/APIGateway.	controle de segurança/ 9APIGateway.
aws-foundational-security-best- 1practices/ v/1.0.0/AutoScaling.	controle de segurança/ 1AutoScaling.
aws-foundational-security-best- 2practices/ v/1.0.0/AutoScaling.	controle de segurança/ 2AutoScaling.
aws-foundational-security-best- 3practices/ v/1.0.0/AutoScaling.	controle de segurança/ 3AutoScaling.
aws-foundational-security-best- 5practices/ v/1.0.0/Autoscaling.	security-control/Autoscaling.5
aws-foundational-security-best- 6practices/ v/1.0.0/AutoScaling.	controle de segurança/ 6AutoScaling.
aws-foundational-security-best- 9practices/ v/1.0.0/AutoScaling.	controle de segurança/ 9AutoScaling.
aws-foundational-security-best- 1practices/ v/1.0.0/CloudFront.	controle de segurança/ 1CloudFront.
aws-foundational-security-best- 3practices/ v/1.0.0/CloudFront.	controle de segurança/ 3CloudFront.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 4practices/ v/1.0.0/CloudFront.	controle de segurança/ 4CloudFront.
aws-foundational-security-best- 5practices/ v/1.0.0/CloudFront.	controle de segurança/ 5CloudFront.
aws-foundational-security-best- 6practices/ v/1.0.0/CloudFront.	controle de segurança/ 6CloudFront.
aws-foundational-security-best- 7practices/ v/1.0.0/CloudFront.	controle de segurança/ 7CloudFront.
aws-foundational-security-best- 8practices/ v/1.0.0/CloudFront.	controle de segurança/ 8CloudFront.
aws-foundational-security-best- 9practices/ v/1.0.0/CloudFront.	controle de segurança/ 9CloudFront.
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 1,0	controle de segurança/ 1.0 CloudFront
aws-foundational-security-best- practices/ v/1.0.0/CloudFront 1,2	controle de segurança/ 1.2 CloudFront
aws-foundational-security-best- 1practices/ v/1.0.0/CloudTrail.	controle de segurança/ 1CloudTrail.
aws-foundational-security-best- 2practices/ v/1.0.0/CloudTrail.	controle de segurança/ 2CloudTrail.
aws-foundational-security-best- 4practices/ v/1.0.0/CloudTrail.	controle de segurança/ 4CloudTrail.
aws-foundational-security-best- 5practices/ v/1.0.0/CloudTrail.	controle de segurança/ 5CloudTrail.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 1practices/ v/1.0.0/CodeBuild.	controle de segurança/ 1CodeBuild.
aws-foundational-security-best- 2practices/ v/1.0.0/CodeBuild.	controle de segurança/ 2CodeBuild.
aws-foundational-security-best- 3practices/ v/1.0.0/CodeBuild.	controle de segurança/ 3CodeBuild.
aws-foundational-security-best- 4practices/ v/1.0.0/CodeBuild.	controle de segurança/ 4CodeBuild.
aws-foundational-security-best- 1practices/ v/1.0.0/Config.	security-control/Config.1
aws-foundational-security-best- 1practices/ v/1.0.0/DMS.	security-control/DMS.1
aws-foundational-security-best- 1practices/ v/1.0.0/DynamoDB.	security-control/DynamoDB.1
aws-foundational-security-best- 2practices/ v/1.0.0/DynamoDB.	security-control/DynamoDB.2
aws-foundational-security-best- 3practices/ v/1.0.0/DynamoDB.	security-control/DynamoDB.3
aws-foundational-security-best- practices/ v/1.0.0/EC 2,1	controle de segurança/ 1EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,3	controle de segurança/ 3EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,4	controle de segurança/ 4EC2.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- practices/ v/1.0.0/EC 2,6	controle de segurança/ 6EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,7	controle de segurança/ 7EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,8	controle de segurança/ 8EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,9	controle de segurança/ 9EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,10	controle de segurança/ 1.0 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,15	controle de segurança/ 1.5 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,16	controle de segurança/ 1.6 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,17	controle de segurança/ 1.7 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,18	controle de segurança/ 1.8 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,19	controle de segurança/ 1.9 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,2	controle de segurança/ 2EC2.
aws-foundational-security-best- practices/ v/1.0.0/EC 2,20	controle de segurança/ 2.0 EC2

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- practices/ v/1.0.0/EC 2,21	controle de segurança/ 2.1 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,23	controle de segurança/ 2.3 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,24	controle de segurança/ 2,4 EC2
aws-foundational-security-best- practices/ v/1.0.0/EC 2,25	controle de segurança/ 2.5 EC2
aws-foundational-security-best- 1practices/ v/1.0.0/ECR.	security-control/ECR.1
aws-foundational-security-best- 2practices/ v/1.0.0/ECR.	security-control/ECR.2
aws-foundational-security-best- 3practices/ v/1.0.0/ECR.	security-control/ECR.3
aws-foundational-security-best- 1practices/ v/1.0.0/ECS.	security-control/ECS.1
aws-foundational-security-best- practices/ v/1.0.0/ECS 1,0	security-control/ECS.10
aws-foundational-security-best- practices/ v/1.0.0/ECS 1,2	security-control/ECS.12
aws-foundational-security-best- 2practices/ v/1.0.0/ECS.	security-control/ECS.2
aws-foundational-security-best- 3practices/ v/1.0.0/ECS.	security-control/ECS.3

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 4practices/ v/1.0.0/ECS.	security-control/ECS.4
aws-foundational-security-best- 5practices/ v/1.0.0/ECS.	security-control/ECS.5
aws-foundational-security-best- 8practices/ v/1.0.0/ECS.	security-control/ECS.8
aws-foundational-security-best- 1practices/ v/1.0.0/EFS.	security-control/EFS.1
aws-foundational-security-best- 2practices/ v/1.0.0/EFS.	security-control/EFS.2
aws-foundational-security-best- 3practices/ v/1.0.0/EFS.	security-control/EFS.3
aws-foundational-security-best- 4practices/ v/1.0.0/EFS.	security-control/EFS.4
aws-foundational-security-best- 2practices/ v/1.0.0/EKS.	security-control/EKS.2
aws-foundational-security-best- 1practices/ v/1.0.0/ElasticBeanstalk.	controle de segurança/ 1ElasticBeanstalk.
aws-foundational-security-best- 2practices/ v/1.0.0/ElasticBeanstalk.	controle de segurança/ 2ElasticBeanstalk.
aws-foundational-security-best- practices/ v/1.0.0/ELBv 2,1	security-control/ELB.1
aws-foundational-security-best- 2practices/ v/1.0.0/ELB.	security-control/ELB.2

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 3practices/ v/1.0.0/ELB.	security-control/ELB./*
aws-foundational-security-best- 4practices/ v/1.0.0/ELB.	security-control/ELB.4
aws-foundational-security-best- 5practices/ v/1.0.0/ELB.	security-control/ELB.5
aws-foundational-security-best- 6practices/ v/1.0.0/ELB.	security-control/ELB.6
aws-foundational-security-best- 7practices/ v/1.0.0/ELB.	security-control/ELB.7
aws-foundational-security-best- 8practices/ v/1.0.0/ELB.	security-control/ELB.8
aws-foundational-security-best- 9practices/ v/1.0.0/ELB.	security-control/ELB.9
aws-foundational-security-best- practices/ v/1.0.0/ELB 1,0	security-control/ELB.10
aws-foundational-security-best- practices/ v/1.0.0/ELB 1,1	security-control/ELB.11
aws-foundational-security-best- practices/ v/1.0.0/ELB 1,2	security-control/ELB.12
aws-foundational-security-best- practices/ v/1.0.0/ELB 1,3	security-control/ELB.13
aws-foundational-security-best- practices/ v/1.0.0/ELB 1,4	security-control/ELB.14

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 1practices/ v/1.0.0/EMR.	security-control/EMR.1
aws-foundational-security-best- 1practices/ v/1.0.0/ES.	security-control/ES.1
aws-foundational-security-best- 2practices/ v/1.0.0/ES.	security-control/ES.2
aws-foundational-security-best- 3practices/ v/1.0.0/ES.	security-control/ES.3
aws-foundational-security-best- 4practices/ v/1.0.0/ES.	security-control/ES.4
aws-foundational-security-best- 5practices/ v/1.0.0/ES.	security-control/ES.5
aws-foundational-security-best- 6practices/ v/1.0.0/ES.	security-control/ES.6
aws-foundational-security-best- 7practices/ v/1.0.0/ES.	security-control/ES.7
aws-foundational-security-best- 8practices/ v/1.0.0/ES.	security-control/ES.8
aws-foundational-security-best- 1practices/ v/1.0.0/GuardDuty.	controle de segurança/ 1GuardDuty.
aws-foundational-security-best- 1practices/ v/1.0.0/IAM.	security-control/IAM.1
aws-foundational-security-best- 2practices/ v/1.0.0/IAM.	security-control/IAM.2

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- practices/ v/1.0.0/IAM 2,1	security-control/IAM.21
aws-foundational-security-best- 3practices/ v/1.0.0/IAM.	security-control/IAM.3
aws-foundational-security-best- 4practices/ v/1.0.0/IAM.	security-control/IAM.4
aws-foundational-security-best- 5practices/ v/1.0.0/IAM.	security-control/IAM.5
aws-foundational-security-best- 6practices/ v/1.0.0/IAM.	security-control/IAM.6
aws-foundational-security-best- 7practices/ v/1.0.0/IAM.	security-control/IAM.7
aws-foundational-security-best- 8practices/ v/1.0.0/IAM.	security-control/IAM.8
aws-foundational-security-best- 1practices/ v/1.0.0/Kinesis.	security-control/Kinesis.1
aws-foundational-security-best- 1practices/ v/1.0.0/KMS.	security-control/KMS.1
aws-foundational-security-best- 2practices/ v/1.0.0/KMS.	security-control/KMS.2
aws-foundational-security-best- 3practices/ v/1.0.0/KMS.	security-control/KMS.3
aws-foundational-security-best- 1practices/ v/1.0.0/Lambda.	security-control/Lambda.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 2practices/ v/1.0.0/Lambda.	security-control/Lambda.2
aws-foundational-security-best- 5practices/ v/1.0.0/Lambda.	security-control/Lambda.5
aws-foundational-security-best- 3practices/ v/1.0.0/NetworkFirewall.	controle de segurança/ 3NetworkFirewall.
aws-foundational-security-best- 4practices/ v/1.0.0/NetworkFirewall.	controle de segurança/ 4NetworkFirewall.
aws-foundational-security-best- 5practices/ v/1.0.0/NetworkFirewall.	controle de segurança/ 5NetworkFirewall.
aws-foundational-security-best- 6practices/ v/1.0.0/NetworkFirewall.	controle de segurança/ 6NetworkFirewall.
aws-foundational-security-best- 1practices/ v/1.0.0/Opensearch.	security-control/Opensearch.1
aws-foundational-security-best- 2practices/ v/1.0.0/Opensearch.	security-control/Opensearch.2
aws-foundational-security-best- 3practices/ v/1.0.0/Opensearch.	security-control/Opensearch.3
aws-foundational-security-best- 4practices/ v/1.0.0/Opensearch.	security-control/Opensearch.4
aws-foundational-security-best- 5practices/ v/1.0.0/Opensearch.	security-control/Opensearch.5
aws-foundational-security-best- 6practices/ v/1.0.0/Opensearch.	security-control/Opensearch.6

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 7practices/ v/1.0.0/Opensearch.	security-control/Opensearch.7
aws-foundational-security-best- 8practices/ v/1.0.0/Opensearch.	security-control/Opensearch.8
aws-foundational-security-best- 1practices/ v/1.0.0/RDS.	security-control/RDS.1
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,0	security-control/RDS.10
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,1	security-control/RDS.11
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,2	security-control/RDS.12
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,3	security-control/RDS.13
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,4	security-control/RDS.14
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,5	security-control/RDS.15
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,6	security-control/RDS.16
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,7	security-control/RDS.17
aws-foundational-security-best- practices/ v/1.0.0/RDS 1,9	security-control/RDS.19

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 2practices/ v/1.0.0/RDS.	security-control/RDS.2
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,0	security-control/RDS.20
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,1	security-control/RDS.21
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,2	security-control/RDS.22
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,3	security-control/RDS.23
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,4	security-control/RDS.24
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,5	security-control/RDS.25
aws-foundational-security-best- 3practices/ v/1.0.0/RDS.	security-control/RDS.3
aws-foundational-security-best- 4practices/ v/1.0.0/RDS.	security-control/RDS.4
aws-foundational-security-best- 5practices/ v/1.0.0/RDS.	security-control/RDS.5
aws-foundational-security-best- 6practices/ v/1.0.0/RDS.	security-control/RDS.6
aws-foundational-security-best- 7practices/ v/1.0.0/RDS.	security-control/RDS.7

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 8practices/ v/1.0.0/RDS.	security-control/RDS.8
aws-foundational-security-best- 9practices/ v/1.0.0/RDS.	security-control/RDS.9
aws-foundational-security-best- 1practices/ v/1.0.0/Redshift.	security-control/Redshift.1
aws-foundational-security-best- 2practices/ v/1.0.0/Redshift.	security-control/Redshift.2
aws-foundational-security-best- 3practices/ v/1.0.0/Redshift.	security-control/Redshift.3
aws-foundational-security-best- 4practices/ v/1.0.0/Redshift.	security-control/Redshift.4
aws-foundational-security-best- 6practices/ v/1.0.0/Redshift.	security-control/Redshift.6
aws-foundational-security-best- 7practices/ v/1.0.0/Redshift.	security-control/Redshift.7
aws-foundational-security-best- 8practices/ v/1.0.0/Redshift.	security-control/Redshift.8
aws-foundational-security-best- 9practices/ v/1.0.0/Redshift.	security-control/Redshift.9
aws-foundational-security-best- practices/ v/1.0.0/S 3,1	security-control/S3.1
aws-foundational-security-best- practices/ v/1.0.0/S 3,12	security-control/S3.12

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- practices/ v/1.0.0/S 3,13	security-control/S3.13
aws-foundational-security-best- practices/ v/1.0.0/S 3,2	security-control/S3.2
aws-foundational-security-best- practices/ v/1.0.0/S 3,3	security-control/S3.3
aws-foundational-security-best- practices/ v/1.0.0/S 3,5	security-control/S3.5
aws-foundational-security-best- practices/ v/1.0.0/S 3,6	security-control/S3.6
aws-foundational-security-best- practices/ v/1.0.0/S 3,8	security-control/S3.8
aws-foundational-security-best- practices/ v/1.0.0/S 3,9	security-control/S3.9
aws-foundational-security-best- 1practices/ v/1.0.0/SageMaker.	controle de segurança/ 1SageMaker.
aws-foundational-security-best- 2practices/ v/1.0.0/SageMaker.	controle de segurança/ 2SageMaker.
aws-foundational-security-best- 3practices/ v/1.0.0/SageMaker.	controle de segurança/ 3SageMaker.
aws-foundational-security-best- 1practices/ v/1.0.0/SecretsManager.	controle de segurança/ 1SecretsManager.
aws-foundational-security-best- 2practices/ v/1.0.0/SecretsManager.	controle de segurança/ 2SecretsManager.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 3practices/ v/1.0.0/SecretsManager.	controle de segurança/ 3SecretsManager.
aws-foundational-security-best- 4practices/ v/1.0.0/SecretsManager.	controle de segurança/ 4SecretsManager.
aws-foundational-security-best- 1practices/ v/1.0.0/SQS.	security-control/SQS.1
aws-foundational-security-best- 1practices/ v/1.0.0/SSM.	security-control/SSM.1
aws-foundational-security-best- 2practices/ v/1.0.0/SSM.	security-control/SSM.2
aws-foundational-security-best- 3practices/ v/1.0.0/SSM.	security-control/SSM.3
aws-foundational-security-best- 4practices/ v/1.0.0/SSM.	security-control/SSM.4
aws-foundational-security-best- 1practices/ v/1.0.0/WAF.	security-control/WAF.1
aws-foundational-security-best- 2practices/ v/1.0.0/WAF.	security-control/WAF.2
aws-foundational-security-best- 3practices/ v/1.0.0/WAF.	security-control/WAF.3
aws-foundational-security-best- 4practices/ v/1.0.0/WAF.	security-control/WAF.4
aws-foundational-security-best- 6practices/ v/1.0.0/WAF.	security-control/WAF.6

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
aws-foundational-security-best- 7practices/ v/1.0.0/WAF.	security-control/WAF.7
aws-foundational-security-best- 8practices/ v/1.0.0/WAF.	security-control/WAF.8
aws-foundational-security-best- practices/ v/1.0.0/WAF 1,0	security-control/WAF.10
foto-. dss/v/3.2.1/PCI AutoScaling.1	controle de segurança/ 1AutoScaling.
foto-. dss/v/3.2.1/PCI CloudTrail.1	controle de segurança/ 2CloudTrail.
foto-. dss/v/3.2.1/PCI CloudTrail.2	controle de segurança/ 3CloudTrail.
foto-. dss/v/3.2.1/PCI CloudTrail.3	controle de segurança/ 4CloudTrail.
foto-. dss/v/3.2.1/PCI CloudTrail.4	controle de segurança/ 5CloudTrail.
foto-. dss/v/3.2.1/PCI CodeBuild.1	controle de segurança/ 1CodeBuild.
foto-. dss/v/3.2.1/PCI CodeBuild.2	controle de segurança/ 2CodeBuild.
pci- .Config.1 dss/v/3.2.1/PCI	security-control/Config.1
foto - dss/v/3.2.1/PCI C.W.1	controle de segurança/ 1CloudWatch.
foto - dss/v/3.2.1/PCI D.MS.1	security-control/DMS.1
foto-. dss/v/3.2.1/PCI EC2.1	controle de segurança/ 1EC2.
foto-. dss/v/3.2.1/PCI EC2.2	controle de segurança/ 2EC2.
foto-. dss/v/3.2.1/PCI EC2.4	controle de segurança/ 1.2 EC2
foto-. dss/v/3.2.1/PCI EC25.	controle de segurança/ 1.3 EC2
foto-. dss/v/3.2.1/PCI EC2.6	controle de segurança/ 6EC2.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
foto-. dss/v/3.2.1/PCI ELBv2.1	security-control/ELB.1
foto- .ES.1 dss/v/3.2.1/PCI	security-control/ES.2
foto- .ES.2 dss/v/3.2.1/PCI	security-control/ES.1
foto-. dss/v/3.2.1/PCI GuardDuty.1	controle de segurança/ 1GuardDuty.
foto - IAM.1 dss/v/3.2.1/PCI	security-control/IAM.4
foto - IAM.2 dss/v/3.2.1/PCI	security-control/IAM.2
foto - IAM.3 dss/v/3.2.1/PCI	security-control/IAM.1
foto - IAM.4 dss/v/3.2.1/PCI	security-control/IAM.6
foto - IAM.5 dss/v/3.2.1/PCI	security-control/IAM.9
foto - I.AM.6 dss/v/3.2.1/PCI	security-control/IAM.19
foto - I.AM.7 dss/v/3.2.1/PCI	security-control/IAM.8
foto - I.AM.8 dss/v/3.2.1/PCI	security-control/IAM.10
foto - dss/v/3.2.1/PCI KMS.1	security-control/KMS.4
foto- Lambda.1 dss/v/3.2.1/PCI	security-control/Lambda.1
foto- Lambda.2 dss/v/3.2.1/PCI	security-control/Lambda.3
pci- .Abrir pesquisa.1 dss/v/3.2.1/PCI	security-control/Opensearch.2
pci- .Opensearch.2 dss/v/3.2.1/PCI	security-control/Opensearch.1
foto - RDS.1 dss/v/3.2.1/PCI	security-control/RDS.1
foto- RDS.2 dss/v/3.2.1/PCI	security-control/RDS.2
foto- dss/v/3.2.1/PCI .Redshift.1	security-control/Redshift.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
pic-S.3.1 dss/v/3.2.1/PCI	security-control/S3.3
pic-S 3.2 dss/v/3.2.1/PCI	security-control/S3.2
pic-S.3.3 dss/v/3.2.1/PCI	security-control/S3.7
foto- S.3.5 dss/v/3.2.1/PCI	security-control/S3.5
foto S.3.6 dss/v/3.2.1/PCI	security-control/S3.1
foto-. dss/v/3.2.1/PCI SageMaker.1	controle de segurança/ 1SageMaker.
foto - dss/v/3.2.1/PCI S.SM.1	security-control/SSM.2
pic-.SSM.2 dss/v/3.2.1/PCI	security-control/SSM.3
pic-.SSM.3 dss/v/3.2.1/PCI	security-control/SSM.1
service-managed-aws-control- 1tower/v/1.0.0/ ACM.	security-control/ACM.1
service-managed-aws-control- 1tower/v/1.0.0/ APIGateway.	controle de segurança/ 1APIGateway.
service-managed-aws-control- 2tower/v/1.0.0/ APIGateway.	controle de segurança/ 2APIGateway.
service-managed-aws-control- 3tower/v/1.0.0/ APIGateway.	controle de segurança/ 3APIGateway.
service-managed-aws-control- 4tower/v/1.0.0/ APIGateway.	controle de segurança/ 4APIGateway.
service-managed-aws-control- 5tower/v/1.0.0/ APIGateway.	controle de segurança/ 5APIGateway.
service-managed-aws-control- 1tower/v/1.0.0/ AutoScaling.	controle de segurança/ 1AutoScaling.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 2tower/v/1.0.0/AutoScaling.	controle de segurança/ 2AutoScaling.
service-managed-aws-control- 3tower/v/1.0.0/AutoScaling.	controle de segurança/ 3AutoScaling.
service-managed-aws-control- 4tower/v/1.0.0/AutoScaling.	controle de segurança/ 4AutoScaling.
service-managed-aws-control- 5tower/v/1.0.0/Autoscaling.	security-control/Autoscaling.5
service-managed-aws-control- 6tower/v/1.0.0/AutoScaling.	controle de segurança/ 6AutoScaling.
service-managed-aws-control- 9tower/v/1.0.0/AutoScaling.	controle de segurança/ 9AutoScaling.
service-managed-aws-control- 1tower/v/1.0.0/CloudTrail.	controle de segurança/ 1CloudTrail.
service-managed-aws-control- 2tower/v/1.0.0/CloudTrail.	controle de segurança/ 2CloudTrail.
service-managed-aws-control- 4tower/v/1.0.0/CloudTrail.	controle de segurança/ 4CloudTrail.
service-managed-aws-control- 5tower/v/1.0.0/CloudTrail.	controle de segurança/ 5CloudTrail.
service-managed-aws-control- 1tower/v/1.0.0/CodeBuild.	controle de segurança/ 1CodeBuild.
service-managed-aws-control- 2tower/v/1.0.0/CodeBuild.	controle de segurança/ 2CodeBuild.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 4tower/v/1.0.0/CodeBuild.	controle de segurança/ 4CodeBuild.
service-managed-aws-control- 5tower/v/1.0.0/CodeBuild.	controle de segurança/ 5CodeBuild.
service-managed-aws-control- 1tower/v/1.0.0/DMS.	security-control/DMS.1
service-managed-aws-control- 1tower/v/1.0.0/DynamoDB.	security-control/DynamoDB.1
service-managed-aws-control- 2tower/v/1.0.0/DynamoDB.	security-control/DynamoDB.2
service-managed-aws-control- tower/v/1.0.0/EC2,1	controle de segurança/ 1EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,2	controle de segurança/ 2EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,3	controle de segurança/ 3EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,4	controle de segurança/ 4EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,6	controle de segurança/ 6EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,7	controle de segurança/ 7EC2.
service-managed-aws-control- tower/v/1.0.0/EC2,8	controle de segurança/ 8EC2.

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- tower/v/1.0.0/EC 2,9	controle de segurança/ 9EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2,10	controle de segurança/ 1.0 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,15	controle de segurança/ 1.5 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,16	controle de segurança/ 1.6 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,17	controle de segurança/ 1.7 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,18	controle de segurança/ 1.8 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,19	controle de segurança/ 1.9 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,20	controle de segurança/ 2.0 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,21	controle de segurança/ 2.1 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,22	controle de segurança/ 2.2 EC2
service-managed-aws-control- 1tower/v/1.0.0/ ECR.	security-control/ECR.1
service-managed-aws-control- 2tower/v/1.0.0/ ECR.	security-control/ECR.2

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 3tower/v/1.0.0/ ECR.	security-control/ECR.3
service-managed-aws-control- 1tower/v/1.0.0/ ECS.	security-control/ECS.1
service-managed-aws-control- 2tower/v/1.0.0/ ECS.	security-control/ECS.2
service-managed-aws-control- 3tower/v/1.0.0/ ECS.	security-control/ECS.3
service-managed-aws-control- 4tower/v/1.0.0/ ECS.	security-control/ECS.4
service-managed-aws-control- 5tower/v/1.0.0/ ECS.	security-control/ECS.5
service-managed-aws-control- 8tower/v/1.0.0/ ECS.	security-control/ECS.8
service-managed-aws-control- tower/v/1.0.0/ ECS 1,0	security-control/ECS.10
service-managed-aws-control- tower/v/1.0.0/ ECS 1,2	security-control/ECS.12
service-managed-aws-control- 1tower/v/1.0.0/ EFS.	security-control/EFS.1
service-managed-aws-control- 2tower/v/1.0.0/ EFS.	security-control/EFS.2
service-managed-aws-control- 3tower/v/1.0.0/ EFS.	security-control/EFS.3

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 4tower/v/1.0.0/EFS.	security-control/EFS.4
service-managed-aws-control- 2tower/v/1.0.0/EKS.	security-control/EKS.2
service-managed-aws-control- 2tower/v/1.0.0/ELB.	security-control/ELB.2
service-managed-aws-control- 3tower/v/1.0.0/ELB.	security-control/ELB./*
service-managed-aws-control- 4tower/v/1.0.0/ELB.	security-control/ELB.4
service-managed-aws-control- 5tower/v/1.0.0/ELB.	security-control/ELB.5
service-managed-aws-control- 6tower/v/1.0.0/ELB.	security-control/ELB.6
service-managed-aws-control- 7tower/v/1.0.0/ELB.	security-control/ELB.7
service-managed-aws-control- 8tower/v/1.0.0/ELB.	security-control/ELB.8
service-managed-aws-control- 9tower/v/1.0.0/ELB.	security-control/ELB.9
service-managed-aws-control- tower/v/1.0.0/ELB 1,0	security-control/ELB.10
service-managed-aws-control- tower/v/1.0.0/ELB 1,2	security-control/ELB.12

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- tower/v/1.0.0/ ELB 1,3	security-control/ELB.13
service-managed-aws-control- tower/v/1.0.0/ ELB 1,4	security-control/ELB.14
service-managed-aws-control- tower/v/1.0.0/ ELBv 2,1	controle de segurança/ 1ELBv2.
service-managed-aws-control- 1tower/v/1.0.0/ EMR.	security-control/EMR.1
service-managed-aws-control- 1tower/v/1.0.0/ ES.	security-control/ES.1
service-managed-aws-control- 2tower/v/1.0.0/ ES.	security-control/ES.2
service-managed-aws-control- 3tower/v/1.0.0/ ES.	security-control/ES.3
service-managed-aws-control- 4tower/v/1.0.0/ ES.	security-control/ES.4
service-managed-aws-control- 5tower/v/1.0.0/ ES.	security-control/ES.5
service-managed-aws-control- 6tower/v/1.0.0/ ES.	security-control/ES.6
service-managed-aws-control- 7tower/v/1.0.0/ ES.	security-control/ES.7
service-managed-aws-control- 8tower/v/1.0.0/ ES.	security-control/ES.8

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 1tower/v/1.0.0/ ElasticBeanstalk.	controle de segurança/ 1ElasticBeanstalk.
service-managed-aws-control- 2tower/v/1.0.0/ ElasticBeanstalk.	controle de segurança/ 2ElasticBeanstalk.
service-managed-aws-control- 1tower/v/1.0.0/ GuardDuty.	controle de segurança/ 1GuardDuty.
service-managed-aws-control- 1tower/v/1.0.0/ IAM.	security-control/IAM.1
service-managed-aws-control- 2tower/v/1.0.0/ IAM.	security-control/IAM.2
service-managed-aws-control- 3tower/v/1.0.0/ IAM.	security-control/IAM.3
service-managed-aws-control- 4tower/v/1.0.0/ IAM.	security-control/IAM.4
service-managed-aws-control- 5tower/v/1.0.0/ IAM.	security-control/IAM.5
service-managed-aws-control- 6tower/v/1.0.0/ IAM.	security-control/IAM.6
service-managed-aws-control- 7tower/v/1.0.0/ IAM.	security-control/IAM.7
service-managed-aws-control- 8tower/v/1.0.0/ IAM.	security-control/IAM.8
service-managed-aws-control- tower/v/1.0.0/ IAM 2,1	security-control/IAM.21

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 1tower/v/1.0.0/ Kinesis.	security-control/Kinesis.1
service-managed-aws-control- 1tower/v/1.0.0/ KMS.	security-control/KMS.1
service-managed-aws-control- 2tower/v/1.0.0/ KMS.	security-control/KMS.2
service-managed-aws-control- 3tower/v/1.0.0/ KMS.	security-control/KMS.3
service-managed-aws-control- 1tower/v/1.0.0/ Lambda.	security-control/Lambda.1
service-managed-aws-control- 2tower/v/1.0.0/ Lambda.	security-control/Lambda.2
service-managed-aws-control- 5tower/v/1.0.0/ Lambda.	security-control/Lambda.5
service-managed-aws-control- 3tower/v/1.0.0/ NetworkFirewall.	controle de segurança/ 3NetworkFirewall.
service-managed-aws-control- 4tower/v/1.0.0/ NetworkFirewall.	controle de segurança/ 4NetworkFirewall.
service-managed-aws-control- 5tower/v/1.0.0/ NetworkFirewall.	controle de segurança/ 5NetworkFirewall.
service-managed-aws-control- 6tower/v/1.0.0/ NetworkFirewall.	controle de segurança/ 6NetworkFirewall.
service-managed-aws-control- 1tower/v/1.0.0/ Opensearch.	security-control/Opensearch.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 2tower/v/1.0.0/ Opensearch.	security-control/Opensearch.2
service-managed-aws-control- 3tower/v/1.0.0/ Opensearch.	security-control/Opensearch.3
service-managed-aws-control- 4tower/v/1.0.0/ Opensearch.	security-control/Opensearch.4
service-managed-aws-control- 5tower/v/1.0.0/ Opensearch.	security-control/Opensearch.5
service-managed-aws-control- 6tower/v/1.0.0/ Opensearch.	security-control/Opensearch.6
service-managed-aws-control- 7tower/v/1.0.0/ Opensearch.	security-control/Opensearch.7
service-managed-aws-control- 8tower/v/1.0.0/ Opensearch.	security-control/Opensearch.8
service-managed-aws-control- 1tower/v/1.0.0/ RDS.	security-control/RDS.1
service-managed-aws-control- 2tower/v/1.0.0/ RDS.	security-control/RDS.2
service-managed-aws-control- 3tower/v/1.0.0/ RDS.	security-control/RDS.3
service-managed-aws-control- 4tower/v/1.0.0/ RDS.	security-control/RDS.4
service-managed-aws-control- 5tower/v/1.0.0/ RDS.	security-control/RDS.5

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 6tower/v/1.0.0/ RDS.	security-control/RDS.6
service-managed-aws-control- 8tower/v/1.0.0/ RDS.	security-control/RDS.8
service-managed-aws-control- 9tower/v/1.0.0/ RDS.	security-control/RDS.9
service-managed-aws-control- tower/v/1.0.0/ RDS 1,0	security-control/RDS.10
service-managed-aws-control- tower/v/1.0.0/ RDS 1,1	security-control/RDS.11
service-managed-aws-control- tower/v/1.0.0/ RDS 1,3	security-control/RDS.13
service-managed-aws-control- tower/v/1.0.0/ RDS 1,7	security-control/RDS.17
service-managed-aws-control- tower/v/1.0.0/ RDS 1,8	security-control/RDS.18
service-managed-aws-control- tower/v/1.0.0/ RDS 1,9	security-control/RDS.19
service-managed-aws-control- tower/v/1.0.0/ RDS 2,0	security-control/RDS.20
service-managed-aws-control- tower/v/1.0.0/ RDS 2,1	security-control/RDS.21
service-managed-aws-control- tower/v/1.0.0/ RDS 2,2	security-control/RDS.22

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- tower/v/1.0.0/ RDS 2,3	security-control/RDS.23
service-managed-aws-control- tower/v/1.0.0/ RDS 2,5	security-control/RDS.25
service-managed-aws-control- 1tower/v/1.0.0/ Redshift.	security-control/Redshift.1
service-managed-aws-control- 2tower/v/1.0.0/ Redshift.	security-control/Redshift.2
service-managed-aws-control- 4tower/v/1.0.0/ Redshift.	security-control/Redshift.4
service-managed-aws-control- 6tower/v/1.0.0/ Redshift.	security-control/Redshift.6
service-managed-aws-control- 7tower/v/1.0.0/ Redshift.	security-control/Redshift.7
service-managed-aws-control- 8tower/v/1.0.0/ Redshift.	security-control/Redshift.8
service-managed-aws-control- 9tower/v/1.0.0/ Redshift.	security-control/Redshift.9
service-managed-aws-control- tower/v/1.0.0/S 3,1	security-control/S3.1
service-managed-aws-control- tower/v/1.0.0/S 3,2	security-control/S3.2
service-managed-aws-control- tower/v/1.0.0/S 3,3	security-control/S3.3

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- tower/v/1.0.0/S3,5	security-control/S3.5
service-managed-aws-control- tower/v/1.0.0/S3,6	security-control/S3.6
service-managed-aws-control- tower/v/1.0.0/S3,8	security-control/S3.8
service-managed-aws-control- tower/v/1.0.0/S3,9	security-control/S3.9
service-managed-aws-control- tower/v/1.0.0/S3,12	security-control/S3.12
service-managed-aws-control- tower/v/1.0.0/S3,13	security-control/S3.13
service-managed-aws-control- 1tower/v/1.0.0/SageMaker.	controle de segurança/ 1SageMaker.
service-managed-aws-control- 1tower/v/1.0.0/SecretsManager.	controle de segurança/ 1SecretsManager.
service-managed-aws-control- 2tower/v/1.0.0/SecretsManager.	controle de segurança/ 2SecretsManager.
service-managed-aws-control- 3tower/v/1.0.0/SecretsManager.	controle de segurança/ 3SecretsManager.
service-managed-aws-control- 4tower/v/1.0.0/SecretsManager.	controle de segurança/ 4SecretsManager.
service-managed-aws-control- 1tower/v/1.0.0/SQS.	security-control/SQS.1

GeneratorID antes de permitir descobertas de controle consolidadas	GeneratorID após permitir descobertas de controle consolidadas
service-managed-aws-control- 1tower/v/1.0.0/SSM.	security-control/SSM.1
service-managed-aws-control- 2tower/v/1.0.0/SSM.	security-control/SSM.2
service-managed-aws-control- 3tower/v/1.0.0/SSM.	security-control/SSM.3
service-managed-aws-control- 4tower/v/1.0.0/SSM.	security-control/SSM.4
service-managed-aws-control- 2tower/v/1.0.0/WAF.	security-control/WAF.2
service-managed-aws-control- 3tower/v/1.0.0/WAF.	security-control/WAF.3
service-managed-aws-control- 4tower/v/1.0.0/WAF.	security-control/WAF.4

Como a consolidação afeta o controle IDs e os títulos

A visualização de controles consolidados e as descobertas de controle consolidado padronizam o controle IDs e os títulos 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.

O console CSPM do Security Hub exibe títulos de controle de segurança IDs e controle de segurança independentes de padrões, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas para sua conta. No entanto, as descobertas do CSPM do Security Hub contêm títulos de controle específicos do padrão, para PCI DSS e CIS v1.2.0, se as descobertas de controle consolidado estiverem desativadas em sua conta. Além disso, as descobertas do CSPM do Security Hub contêm o ID de controle específico do padrão e o ID de controle de segurança. Para obter exemplos de como a consolidação afeta os resultados do controle, consulteAmostras de resultados de controle.

Para controles que fazem parte do padrão AWS Control Tower gerenciado por serviços, o prefixo `CT.` é removido da ID de controle e do título nas descobertas quando as descobertas de controle consolidadas são habilitadas.

Para desativar um controle de segurança no Security Hub CSPM, você deve desativar todos os controles padrão que correspondem ao controle de segurança. A tabela a seguir mostra o mapeamento do controle IDs e dos títulos de segurança para controles IDs e títulos específicos do padrão. IDs e os títulos dos controles que pertencem ao padrão AWS Foundational Security Best Practices (FSBP) já são independentes do padrão. Para um mapeamento dos controles de acordo com os requisitos do Center for Internet Security (CIS) v3.0.0, consulte Mapeamento de controles para os requisitos do CIS em cada versão. Para executar seus próprios scripts nessa tabela, você pode baixá-la como um arquivo.csv.

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
CIS v1.2.0	1.1 Evitar o uso do "usuário raiz"	CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”
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 IAM não deve existir
CIS v1.2.0	1.13 Certifique-se que MFA esteja habilitada para a usuário raiz	[IAM.9] A MFA 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

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 IAM não devem ter políticas do IAM anexadas
CIS v1.2.0	1.2 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 v1.2.0	1.20 Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com Suporte	[IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
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 IAM não devem permitir privilégios administr ativos completos "*"
CIS v1.2.0	1.3 Certifique-se de que as credencia is não usadas por 90 dias ou mais sejam desativadas	[IAM.8] 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

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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
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 habilitada
CIS v1.2.0	2.3 Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	[CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
CIS v1.2.0	2.4 Garanta que as CloudTrail trilhas estejam integradas aos CloudWatch registros	[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs
CIS v1.2.0	2.5 Verifique AWS Config se está ativado	[Config.1] AWS Config deve estar habilitado e usar a função vinculada ao serviço para gravação de recursos

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
CIS v1.2.0	2.7 Certifique-se de que CloudTrail os registros sejam criptografados em repouso usando o KMS CMKs	[CloudTrail.2] CloudTrail deve ter a criptografia em repouso habilitada
CIS v1.2.0	2.8 Certifique-se de que a rotação para clientes criados CMKs esteja ativada	A rotação de AWS KMS teclas [KMS.4] deve estar ativada
CIS v1.2.0	2.9 Certifique-se de que o registro de fluxo de VPC esteja ativado em todos VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs
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 um filtro e um alarme de métrica de logs existam 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 um filtro e um alarme de métrica de logs existam para alterações de 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 um filtro e um alarme de métrica de logs existam para alterações em 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 um filtro e um alarme de métrica de logs existam para alterações em gateways de rede

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 um filtro e um alarme de métrica de logs existam para alterações de 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 um filtro e um alarme de métrica de logs existam 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 um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA
CIS v1.2.0	3.3 Certifique-se que um filtro e um alarme de métrica de logs existam para uso do usuário raiz	CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”
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 um filtro e um alarme de métrica de logs existam para alterações de 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 um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do
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 um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
CIS v1.2.0	3.7 Certifique-se de que exista um filtro métrico de registro e um alarme para desativação ou exclusão programada do cliente criado CMKs	[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas 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 um filtro e um alarme de métrica de logs existam para alterações de política de 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 um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do
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] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a 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] 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] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou 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	1.14 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

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 IAM 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 Suporte	[IAM.18] Certifique-se de que um perfil de suporte tenha sido criado 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 IAM não deve existir
CIS v1.4.0	1.5 Certifique-se que A MFA esteja habilitada para a conta do usuário raiz	[IAM.9] A MFA deve estar habilitada para o usuário raiz
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	CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”
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 que as solicitações usem SSL

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 habilitadas
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.
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 habilitada
CIS v1.4.0	3.4 Garanta que as CloudTrail trilhas estejam integradas aos registros CloudWatch	[CloudTrail.5] CloudTrail trilhas devem ser integradas ao 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 e usar a função vinculada ao serviço para gravação de recursos

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
CIS v1.4.0	3.7 Certifique-se de que CloudTrail os registros sejam criptografados em repouso usando o KMS CMKs	[CloudTrail.2] CloudTrail deve ter a criptografia em repouso habilitada
CIS v1.4.0	3.8 Certifique-se de que a rotação para clientes criados CMKs esteja ativada	A rotação de AWS KMS teclas [KMS.4] deve estar ativada
CIS v1.4.0	3.9 Certifique-se de que o registro de fluxo de VPC esteja ativado em todos VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todos 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 um filtro e um alarme de métrica de logs existam para alterações de política do IAM
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 um filtro e um alarme de métrica de logs existam para alterações de CloudTrail configuração do
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 um filtro e um alarme de métrica de logs existam para falhas de AWS Management Console autenticação do

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
CIS v1.4.0	4.7 Certifique-se de que exista um filtro métrico de registro e um alarme para desativação ou exclusão programada do cliente criado CMKs	[CloudWatch.7] Certifique-se de que um filtro e um alarme de métrica de logs existam para a desativação ou exclusão programada de CMKs criadas 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 um filtro e um alarme de métrica de logs existam para alterações de política de 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 um filtro e um alarme de métrica de logs existam para alterações de AWS Config configuração do
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 um filtro e um alarme de métrica de logs existam para alterações de 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 um filtro e um alarme de métrica de logs existam para alterações em listas de controle de acesso à rede (NACL)
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 um filtro e um alarme de métrica de logs existam para alterações em 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 um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 um filtro e um alarme de métrica de logs existam para alterações de VPC
CIS v1.4.0	5.1 Certifique-se de que nenhuma rede ACLs permita a entrada de 0.0.0.0/0 às portas de administração do servidor remoto	[EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
CIS v1.4.0	5.3 Verifique se o grupo de segurança padrão de cada VPC restringe todo o tráfego	[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou 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 habilitada
PCI DSS v3.2.1	FOTO. CloudTrail.2 CloudTrail deve ser ativado	[CloudTrail.3] Pelo menos uma CloudTrail trilha deve estar habilitada
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 habilitada
PCI DSS v3.2.1	FOTO. CloudTrail.4 CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs	[CloudTrail.5] CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
PCI DSS v3.2.1	FOTO. CodeBuild.1 CodeBuild GitHub ou o repositório de origem do Bitbucket deve usar URLs OAuth	[CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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 e usar a função vinculada ao serviço para gravação de recursos
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"	CloudWatchUm filtro de métrica de log e um alarme devem existir para o uso do usuário “raiz”
PCI DSS v3.2.1	PCI.DMS.1 As instâncias de replicação do Database Migration Service não devem ser públicas	[DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
PCI DSS v3.2.1	FOTO. EC2.1 Os snapshots do EBS não devem ser restauráveis publicamente	[EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente
PCI DSS v3.2.1	FOTO. EC2.2 O grupo de segurança padrão da VPC deve proibir o tráfego de entrada e saída	[EC2.2] Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída
PCI DSS v3.2.1	FOTO. EC2.4 Não utilizado EC2 EIPs deve ser removido	[EC2.12] A Amazon não utilizada EC2 EIPs deve ser removida
PCI DSS v3.2.1	FOTO. EC2.5 Grupos de segurança não devem permitir a entrada da 0.0.0.0/0 para a porta 22	[EC2.13] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 para a porta 22

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
PCI DSS v3.2.1	FOTO. EC2.6 O registro de fluxo de VPC deve ser ativado em todos VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs
PCI DSS v3.2.1	FOTO. 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 Elasticsearch 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 IAM 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 IAM 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 IAM não devem permitir privilégios administr ativos completos "*"
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.9] A MFA deve estar habilitada para o usuário raiz

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
PCI DSS v3.2.1	PCI.IAM.6 A MFA deve estar habilitada para todos os usuários do IAM	[IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
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	[IAM.8] 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 configurações fortes
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	[Lambda.1] As funções do Lambda.1 devem proibir o acesso público
PCI DSS v3.2.1	PCI.Lambda.2 As funções do Lambda devem estar em uma VPC	[Lambda.3] 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
PCI DSS v3.2.1	PCI.RDS.1 Os instantâneos do RDS devem ser privados	[RDS.1] Os instantâneos do RDS devem ser privados

Padrão	Título e ID do controle de padrão	Título e ID do controle de segurança
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 configuração PubliclyA ccessible
PCI DSS v3.2.1	PCI.Redshift.1 Os clusters do Amazon Redshift devem proibir o acesso público	[PCI.Redshift.1] Os clusters do Amazon Redshift 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 para 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 para 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 que as solicitações usem 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 habilitad as
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	Título e ID do controle de padrão	Título e ID do controle de segurança
PCI DSS v3.2.1	As instâncias PCI.SSM.1 gerenciadas EC2 pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch	[SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
PCI DSS v3.2.1	As instâncias PCI.SSM.2 gerenciadas EC2 pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL	[SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
PCI DSS v3.2.1	As instâncias PCI.SSM.3 devem EC2 ser gerenciadas por AWS Systems Manager	[SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager

Atualização de fluxos de trabalho para consolidação

Se seus fluxos de trabalho não dependem do formato específico de nenhum campo nas descobertas de controle, nenhuma ação é necessária.

Se seus fluxos de trabalho dependerem do formato específico de um ou mais campos nas descobertas de controle, conforme observado nas tabelas anteriores, você deverá atualizar seus fluxos de trabalho. Por exemplo, se você criou uma EventBridge regra da Amazon 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, que é o valor do campo desse controle. `Compliance.SecurityControlId`

Se você criou insights personalizados que usam qualquer um dos campos ou valores que foram alterados, atualize esses insights para usar os novos campos ou valores.

Atributos de nível superior do ASFT obrigatórios

Os seguintes atributos de nível superior no AWS Security Finding Format (ASFF) são necessários para todas as descobertas no Security Hub CSPM. Para obter mais informações sobre esses atributos, consulte AwsSecurityFindingna 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 ou evento capturado por uma descoberta foi criado.

Exemplo

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

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 CSPM, 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 descobertas de controle geradas pelo Security Hub CSPM, esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

Exemplo

```
"GeneratorId": "security-control/Config.1"
```

Id

O identificador específico do produto para uma descoberta. Para as descobertas de controle geradas pelo Security Hub CSPM, esse campo fornece o Amazon Resource Name (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 Amazon Resource Name (ARN) gerado pelo Security Hub CSPM que identifica de forma exclusiva um produto de descoberta de terceiros depois que o produto é registrado no Security Hub CSPM.

O formato desse campo é `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Para Serviços da AWS que sejam integrados ao Security Hub CSPM, 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. Serviços da AWS que ainda não estão integrados ao Security Hub CSPM 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

A `Resources` matriz de objetos fornece um conjunto de tipos de dados de recursos que descrevem os AWS recursos aos quais a descoberta se refere. Para obter detalhes sobre os campos que um `Resources` objeto pode conter, incluindo quais campos são obrigatórios, consulte Resourcea Referência da API do AWS Security Hub. Para obter exemplos de `Resources` objetos específicos Serviços da AWS, consulteObjeto Resources do ASFF.

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 a Referência `Severity`da API CSPM do 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 `Severity` objeto de nível superior para uma descoberta deve ser atualizado somente usando a `BatchUpdateFindings`API.

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 `BatchImportFindings` solicitação para uma nova descoberta fornecer apenas `Label` ou fornecer apenas`Normalized`, o CSPM do Security Hub preencherá automaticamente o valor do outro campo. Os `Original` campos `Product` e também podem ser preenchidos.

Se o `Finding.Severity` objeto de nível superior estiver presente, mas não `Finding.FindingProviderFields` estiver presente, o Security Hub CSPM cria o `FindingProviderFields.Severity` objeto e copia o todo `Finding.Severity object` nele. Isso garante que os detalhes originais fornecidos pelo provedor sejam mantidos na estrutura de `FindingProviderFields.Severity`, mesmo que o objeto de nível superior `Severity` seja sobrescrito.

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`deve ser atualizado somente usando a `BatchUpdateFindings`API.

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.

Você pode definir um caminho parcial paranamespace/category/classifier. Por exemplo, todos os tipos de descoberta a seguir são válidos:

- TTPs
- TTPs/Evasão de defesa
- TTPs/Defense Evasion/CloudTrailStopped

As categorias de táticas, técnicas e procedimentos (TTPs) na lista a seguir se alinham ao 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. No entanto, você pode classificar uma descoberta com comportamentos incomuns e tipos de TTPs descoberta.

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
  - Aplicação
  - Fluxo de rede

  - Endereço IP

  - Usuário
  - VM
  - Contêiner
  - Sem servidor
  - Processo
  - 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 `BatchUpdateFindings`operação. Você pode atualizá-lo somente usando a `BatchImportFindings`operação.

Exemplo

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Atributos de nível superior do ASFF opcionais

Os seguintes atributos de nível superior no AWS Security Finding Format (ASFF) são opcionais para descobertas no Security Hub CSPM. Para obter mais informações sobre esses atributos, consulte AwsSecurityFindingna Referência da API do AWS Security Hub.

Ação

O `Action`objeto fornece detalhes sobre uma ação que afeta ou 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 CSPM do 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 “Integrações de produtos personalizados”.

Ao usar o console CSPM do Security Hub para filtrar as descobertas pelo nome da empresa, você usa esse atributo. Ao usar a API CSPM do Security Hub para filtrar as descobertas pelo nome da empresa, você usa o `aws/securityhub/CompanyName` atributo abaixo. `ProductFields` O Security Hub CSPM não sincroniza esses dois atributos.

Exemplo

```
"CompanyName": "AWS"
```

Compliance

O objeto `Compliance` normalmente fornece detalhes sobre uma descoberta de controle, como padrões aplicáveis e o status da verificação de controle.

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 CSPM 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 “Atualizar descobertas com 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 “Atualizar descobertas com 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
```

Detecção

O `Detection` objeto fornece detalhes sobre uma sequência de ataque encontrada no Amazon GuardDuty Extended Threat Detection. GuardDuty gera uma sequência de ataque descobrindo quando vários eventos se alinham a uma atividade potencialmente suspeita. Para receber as descobertas da sequência de GuardDuty ataque no CSPM do AWS Security Hub, você deve ter GuardDuty habilitado em sua conta. Para obter mais informações, consulte Amazon GuardDuty Extended Threat Detection no Guia GuardDuty do usuário da Amazon.

Exemplo

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
```

```
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
       },
       "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "AROA987654321EXAMPLE:i-b188560f",
        "Account": {
         "Uid": "AccountId",
         "Name": "AccountName"
        }
       }
      }],
      "Endpoints": [{
       "Id": "EndpointId",
       "Ip": "203.0.113.1",
       "Domain": "example.com",
       "Port": 4040,
       "Location": {
        "City": "New York",
        "Country": "US",
        "Lat": 40.7123,
        "Lon": -74.0068
       },
       "AutonomousSystem": {
        "Name": "AnyCompany",
        "Number": 64496
       },
       "Connection": {
        "Direction": "INBOUND"
       }
      }],
      "Signals": [{
       "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
       "Title": "Someone ran a penetration test tool on your account.",
       "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
       "Count": 19,
       "FirstSeenAt": 1716916943000,
       "SignalIndicators": [
        {
         "Key": "ATTACK_TACTIC",
         "Title": "Attack Tactic",
```

```
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Data Destruction"
        ]
       },
      ],
      "LastSeenAt": 1716916944000,
      "Name": "Test:IAMUser/KaliLinux",
      "ResourceIds": [
       "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ],
      "Type": "FINDING"
     }],
     "SequenceIndicators": [
      {
       "Key": "ATTACK_TACTIC",
       "Title": "Attack Tactic",
       "Values": [
        "Discovery",
        "Exfiltration",
        "Impact"
       ]
      },
      {
       "Key": "HIGH_RISK_API",
       "Title": "High Risk Api",
       "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets"
        "s3:ListObjects"
```

```
       ]
      },
      {
       "Key": "ATTACK_TECHNIQUE",
       "Title": "Attack Technique",
       "Values": [
        "Cloud Service Discovery",
        "Data Destruction"
       ]
      }
     ]
    }
}
```

FindingProviderFields

`FindingProviderFields` inclui os seguintes atributos:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Os campos anteriores estão aninhados sob o objeto `FindingProviderFields`, mas têm análogos com o mesmo nome dos campos de nível superior do ASFF. Quando uma nova descoberta é enviada ao CSPM do Security Hub por um provedor de descoberta, o CSPM do Security Hub preenche o `FindingProviderFields` objeto automaticamente se ele estiver vazio com base nos campos de nível superior correspondentes.

A localização de provedores pode ser atualizada `FindingProviderFields` usando a `BatchImportFindings`operação da API CSPM do Security Hub. Os provedores de descobertas não podem atualizar esse objeto com `BatchUpdateFindings`.

Para obter detalhes sobre como o Security Hub CSPM lida com atualizações de `FindingProviderFields` e `BatchImportFindings` para os atributos de nível superior correspondentes, consulte. the section called “Atualizar descobertas com FindingProviderFields”

Os clientes podem atualizar os campos de nível superior usando a operação `BatchUpdateFindings`. Os clientes não podem atualizar `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 ou evento capturado por uma descoberta foi observado pela primeira vez.

Esse timestamp especifica quando o evento ou a vulnerabilidade foram observados pela primeira vez. Consequentemente, ele pode ser diferente do `CreatedAt` timestamp, que reflete quando esse registro de descoberta foi criado.

Para descobertas de controle que o Security Hub CSPM gera e atualiza, esse registro de data e hora também pode indicar quando o status de conformidade de um recurso foi alterado mais recentemente. Para outros tipos de descobertas, esse registro de data e hora deve ser imutável entre as atualizações do registro de descoberta, mas pode ser atualizado se um carimbo de data/hora mais preciso for determinado.

Exemplo

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica quando o possível problema de segurança ou evento capturado por uma descoberta foi observado mais recentemente pelo produto de descobertas de segurança.

Esse registro de data e hora especifica quando o evento ou a vulnerabilidade foram observados 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.

Você pode fornecer esse timestamp, mas isso não é obrigatório na primeira observação. Se você preencher esse campo na primeira observação, o carimbo de data/hora deverá ser igual ao carimbo de data/hora. `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, você pode 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 você pode adicionar 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"
}
```

Processo

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 CSPM recebeu uma descoberta e começou a processá-la.

Isso `CreatedAt` difere de e`UpdatedAt`, que são registros de data e hora obrigatórios relacionados à interação do provedor de busca com o problema de segurança e a descoberta. O `ProcessedAt` timestamp indica quando o Security Hub CSPM 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 CSPM 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 `Archival` são usados quando o Security Hub CSPM arquiva uma descoberta existente. Por exemplo, o Security Hub CSPM arquiva as descobertas existentes quando você desabilita um controle ou padrão e quando ativa ou desativa as 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 CSPM.

O CSPM do 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 “Integrações de produtos personalizados”.

Ao usar o console CSPM do Security Hub para filtrar as descobertas pelo nome do produto, você usa esse atributo.

Ao usar a API CSPM do Security Hub para filtrar as descobertas pelo nome do produto, você usa o `aws/securityhub/ProductName` atributo abaixo. `ProductFields`

O Security Hub CSPM 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 CSPM arquiva automaticamente as descobertas baseadas em controle se o recurso associado for excluído, se o recurso não existir ou se o controle estiver desativado.

`RecordState`é destinado a encontrar fornecedores e só pode ser atualizado usando a `BatchImportFindings`operação. Você não pode atualizá-lo usando a `BatchUpdateFindings`operação.

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 CSPM alterará automaticamente o status do fluxo de trabalho para. `NEW`

Exemplo

```
"RecordState": "ACTIVE"
```

Região

Especifica a Região da AWS partir da qual a descoberta foi gerada.

O CSPM do 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 `RelatedFindings` atributos, consulte `RelatedFinding`na Referência da API CSPM do 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" }
]
```

RiskAssessment

Exemplo

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
        "Indicators": [
            {
                "Type": "Reachability",
```

```
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            }
        ]
    }
}
```

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
 CSPM 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"
```

Objeto Resources do ASFF

No Formato AWS de descoberta de segurança (ASFF), o `Resources` objeto 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 Formato de descoberta de segurança (ASFF). Para obter exemplos de cada objeto recurso, selecione um recurso na lista a seguir.

Tópicos

- Atributos de recursos no ASFF
- Recursos da AwsAmazonMQ no ASFF
- Recursos da AwsApiGateway no ASFF
- Recursos da AwsAppSync no ASFF

- Recursos da AwsAthena no ASFF
- Recursos da AwsAutoScaling no ASFF
- Recursos da AwsBackup no ASFF
- Recursos da AwsCertificateManager no ASFF
- Recursos da AwsCloudFormation no ASFF
- Recursos da AwsCloudFront no ASFF
- Recursos da AwsCloudTrail no ASFF
- Recursos da AwsCloudWatch no ASFF
- Recursos da AwsCodeBuild no ASFF
- Recursos da AwsDms no ASFF
- Recursos da AwsDynamoDB no ASFF
- Recursos da AwsEc2 no ASFF
- Recursos da AwsEcr no ASFF
- Recursos da AwsEcs no ASFF
- Recursos da AwsEfs no ASFF
- Recursos da AwsEks no ASFF
- Recursos da AwsElasticBeanstalk no ASFF
- Recursos da AwsElasticSearch no ASFF
- Recursos da AwsElb no ASFF
- Recursos da AwsEventBridge no ASFF
- Recursos da AwsGuardDuty no ASFF
- Recursos da AwsIam no ASFF
- Recursos da AwsKinesis no ASFF
- Recursos da AwsKms no ASFF
- AwsLambda
- Recursos da AwsMsk no ASFF
- Recursos da AwsNetworkFirewall no ASFF
- Recursos da AwsOpenSearchService no ASFF
- Recursos da AwsRds no ASFF
- Recursos da AwsRedshift no ASFF

- Recursos da AwsRoute53 no ASFF
- Recursos da AwsS3 no ASFF
- Recursos da AwsSageMaker no ASFF
- Recursos da AwsSecretsManager no ASFF
- Recursos da AwsSns no ASFF
- Recursos da AwsSqs no ASFF
- Recursos da AwsSsm no ASFF
- Recursos da AwsStepFunctions no ASFF
- Recursos da AwsWaf no ASFF
- Recursos da AwsXray no ASFF
- CodeRepositoryobjeto no ASFF
- Containerobjeto no ASFF
- Otherobjeto no ASFF

Atributos de recursos no ASFF

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 objeto do tipo de recurso não inclui todos os campos que você deseja preencher. Nesse caso, use o objeto de detalhes para o tipo de recurso para preencher os campos disponíveis. Use o objeto `Other` para preencher os campos 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 objeto `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 para o tipo de recurso fornecido.

Para AWS recursos identificados pelo Amazon Resource Names (ARNs), esse é o ARN.

Para AWS recursos que faltam 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:::amzn-s3-demo-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, consulte Endpoints regionais.

Exemplo

```
"Region": "us-west-2"
```

ResourceRole

Identifica o perfil do recurso na descoberta. Um recurso é o alvo da atividade de descoberta ou o ator que realizou a atividade.

Exemplo

```
"ResourceRole": "target"
```

Tags

Esse campo fornece informações sobre a chave e o valor da tag para o recurso envolvido em uma descoberta. Você pode marcar recursos que são compatíveis com a `GetResources` operação da API de AWS Resource Groups marcação. O Security Hub chama essa operação por meio da função vinculada ao serviço e recupera as tags de recursos se o `Resource.Id` campo AWS Security Finding Format (ASFF) for preenchido com o ARN do recurso. AWS Recursos inválidos IDs são ignorados.

Você pode adicionar tags de recursos às descobertas que o Security Hub ingere, incluindo descobertas de Serviços da AWS e de produtos de terceiros integrados.

Adicionar tags informa a você se existem tags que foram associadas a um recurso quando a descoberta foi processada. Inclua o atributo `Tags` apenas para recursos que tiverem 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 de 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 as restrições que se aplicam às tags, consulte Limites e requisitos de nomenclatura das 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"
```

Recursos da AwsAmazonMQ no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsAmazonMQ` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsAmazonMQBroker

O `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 ASFF para o objeto `AwsAmazonMQBroker`. Para ver as descrições dos atributos `AwsAmazonMQBroker`, consulte AwsAmazonMQBrokerna Referência da API AWS Security Hub .

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"
        }
    ]
}
```

Recursos da AwsApiGateway no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsApiGateway` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsApiGatewayRestApi`, consulte AwsApiGatewayRestApiDetailsna Referência da API AWS Security Hub .

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` oferece informações sobre um estágio de 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 atributos `AwsApiGatewayStage`, consulte AwsApiGatewayStageDetailsna Referência da API AWS Security Hub .

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 na versão 2 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,
}
```

Recursos da AwsAppSync no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsAppSync` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 ASFF para o objeto `AwsAppSyncGraphQLApi`. Para ver as descrições dos atributos `AwsAppSyncGraphQLApi`, consulte AwsAppSyncGraphQLApina Referência da API AWS Security Hub .

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,
}
```

Recursos da AwsAthena no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsAthena` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 ASFF para o objeto `AwsAthenaWorkGroup`. Para ver as descrições dos atributos `AwsAthenaWorkGroup`, consulte AwsAthenaWorkGroupna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsAutoScaling no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsAutoScaling` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsAutoScalingAutoScalingGroup`, consulte AwsAutoScalingAutoScalingGroupDetailsna Referência da API AWS Security Hub .

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 `AwsAutoScalingLaunchConfiguration` fornece detalhes sobre a configuração de inicialização.

Veja a seguir um exemplo de `AwsAutoScalingLaunchConfiguration` descoberta no AWS Security Finding Format (ASFF).

Para ver as descrições dos atributos `AwsAutoScalingLaunchConfiguration`, consulte AwsAutoScalingLaunchConfigurationDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsBackup no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsBackup` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsBackupBackupPlan

O objeto `AwsBackupBackupPlan` fornece informações sobre um plano de backup 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 atributos `AwsBackupBackupPlan`, consulte AwsBackupBackupPlanna Referência da API AWS Security Hub .

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 cofre de backup 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 atributos `AwsBackupBackupVault`, consulte AwsBackupBackupVaultna Referência da API AWS Security Hub .

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 atributos `AwsBackupBackupVault`, consulte AwsBackupRecoveryPointna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsCertificateManager no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCertificateManager` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsCertificateManagerCertificate`, consulte AwsCertificateManagerCertificateDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsCloudFormation no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCloudFormation` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsCloudFormationStack`, consulte AwsCloudFormationStackDetailsna Referência da API AWS Security Hub .

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
}
```


Recursos da AwsCloudFront no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCloudFront` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsCloudFrontDistribution`, consulte AwsCloudFrontDistributionDetailsna Referência da API AWS Security Hub .

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": "amzn-s3-demo-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"
}
```

Recursos da AwsCloudTrail no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCloudTrail` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsCloudTrailTrail

O objeto `AwsCloudTrailTrail` fornece detalhes sobre uma trilha 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 atributos `AwsCloudTrailTrail`, consulte AwsCloudTrailTrailDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsCloudWatch no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCloudWatch` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsCloudWatchAlarm`, consulte AwsCloudWatchAlarmDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": 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"
}
```

Recursos da AwsCodeBuild no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsCodeBuild` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsCodeBuildProject`, consulte AwsCodeBuildProjectDetailsna Referência da API AWS Security Hub .

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"]
    }
```

```
}
```

Recursos da AwsDms no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsDms` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsDmsEndpoint`, consulte AwsDmsEndpointDetailsna Referência da API AWS Security Hub .

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 atributos `AwsDmsReplicationInstance`, consulte AwsDmsReplicationInstanceDetailsna Referência da API AWS Security Hub .

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 atributos `AwsDmsReplicationInstance`, consulte AwsDmsReplicationInstancena Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsDynamoDB no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsDynamoDB` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsDynamoDbTable`, consulte AwsDynamoDbTableDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsEc2 no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEc2` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 `AwsEc2Instance` objeto fornece detalhes sobre uma EC2 instância da Amazon.

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 `AwsEc2NetworkAcl` objeto contém detalhes sobre uma lista de controle EC2 de acesso à rede (ACL) da Amazon.

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 `AwsEc2NetworkInterface` objeto fornece informações sobre uma interface de EC2 rede da Amazon.

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 `AwsEc2RouteTable` objeto fornece informações sobre uma tabela de EC2 rotas da Amazon.

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 `AwsEc2SecurityGroup` objeto descreve um grupo de EC2 segurança da Amazon.

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 `AwsEc2Subnet` objeto fornece informações sobre uma sub-rede na 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 `AwsEc2TransitGateway` objeto fornece detalhes sobre um gateway de EC2 trânsito da Amazon que interconecta suas nuvens privadas virtuais (VPCs) e redes locais.

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 `AwsEc2Volume` objeto fornece detalhes sobre um EC2 volume da Amazon.

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 `AwsEc2Vpc` objeto fornece detalhes sobre uma Amazon EC2 VPC.

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 `AwsEc2VpcPeeringConnection` objeto fornece detalhes sobre a conexão de rede entre dois 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"
}
```

Recursos da AwsEcr no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEcr` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsEcrContainerImage

O objeto `AwsEcrContainerImage` fornece informações sobre uma imagem do Amazon ECR.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcrContainerImage` objeto. Para ver as descrições dos atributos `AwsEcrContainerImage`, consulte AwsEcrContainerImageDetailsna Referência da API AWS Security Hub .

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 atributos `AwsEcrRepository`, consulte AwsEcrRepositoryDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsEcrRepository": {
```

```
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

Recursos da AwsEcs no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEcs` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsEcsCluster`, consulte AwsEcsClusterDetailsna Referência da API AWS Security Hub .

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 atributos `AwsEcsContainer`, consulte AwsEcsContainerDetailsna Referência da API AWS Security Hub .

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 serviço em um cluster Amazon ECS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsService` objeto. Para ver as descrições dos atributos `AwsEcsService`, consulte AwsEcsServiceDetailsna Referência da API AWS Security Hub .

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 tarefa do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsTask` objeto. Para ver as descrições dos atributos `AwsEcsTask`, consulte AwsEcsTaskna Referência da API AWS Security Hub .

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. Uma definição de tarefa descreve as definições de contêiner e volume de uma tarefa do Amazon Elastic Container Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsTaskDefinition` objeto. Para ver as descrições dos atributos `AwsEcsTaskDefinition`, consulte AwsEcsTaskDefinitionDetailsna Referência da API AWS Security Hub .

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",
    }
```

Recursos da AwsEfs no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEfs` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsEfsAccessPoint`, consulte AwsEfsAccessPointDetailsna Referência da API AWS Security Hub .

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"
 }
}
```

Recursos da AwsEks no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEks` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsEksCluster`, consulte AwsEksClusterDetailsna Referência da API AWS Security Hub .

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": {},
  }
}
```

Recursos da AwsElasticBeanstalk no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsElasticBeanstalk` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsElasticBeanstalkEnvironment`, consulte AwsElasticBeanstalkEnvironmentDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsElasticSearch no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsElasticSearch` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsElasticSearchDomain`, consulte AwsElasticSearchDomainDetailsna Referência da API AWS Security Hub .

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"
    }
```

```
}
```

Recursos da AwsElb no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsElb` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsElbLoadBalancer`, consulte AwsElbLoadBalancerDetailsna Referência da API AWS Security Hub .

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": "amzn-s3-demo-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"
                }
```

Recursos da AwsEventBridge no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsEventBridge` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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. Registros de esquemas são contêineres que coletam e agrupam logicamente seus esquemas.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEventSchemasRegistry` objeto. Para ver as descrições dos atributos `AwsEventSchemasRegistry`, consulte AwsEventSchemasRegistryna Referência da API AWS Security Hub .

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. O endpoint pode 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 atributos `AwsEventsEndpoint`, consulte AwsEventsEndpointDetailsna Referência da API AWS Security Hub .

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. O endpoint pode 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 atributos `AwsEventsEventbus`, consulte AwsEventsEventbusDetailsna Referência da API AWS Security Hub .

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\"}}}]}"
```

Recursos da AwsGuardDuty no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsGuardDuty` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsGuardDutyDetector`, consulte AwsGuardDutyDetectorna Referência da API AWS Security Hub .

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"
```

```
        }
    }
}
```

Recursos da AwsIam no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsIam` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsIamAccessKey`, consulte AwsIamAccessKeyDetailsna Referência da API AWS Security Hub .

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 atributos `AwsIamGroup`, consulte AwsIamGroupDetailsna Referência da API AWS Security Hub .

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 atributos `AwsIamPolicy`, consulte AwsIamPolicyDetailsna Referência da API AWS Security Hub .

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

O objeto `AwsIamRole` contém informações sobre um perfil do IAM, incluindo todas as políticas do perfil.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamRole` objeto. Para ver as descrições dos atributos `AwsIamRole`, consulte AwsIamRoleDetailsna Referência da API AWS Security Hub .

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 atributos `AwsIamUser`, consulte AwsIamUserDetailsna Referência da API AWS Security Hub .

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"
        }
    ]
}
```

Recursos da AwsKinesis no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsKinesis` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsKinesisStream`, consulte AwsKinesisStreamDetailsna Referência da API AWS Security Hub .

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"
 }
}
```

Recursos da AwsKms no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsKms` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsKmsKey`, consulte AwsKmsKeyDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsLambda` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsLambdaFunction

O objeto `AwsLambdaFunction` fornece detalhes sobre a configuração de uma função do Lambda.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsLambdaFunction` objeto. Para ver as descrições dos atributos `AwsLambdaFunction`, consulte AwsLambdaFunctionDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-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 `AwsLambdaLayerVersion` fornece detalhes sobre uma versão da camada do Lambda.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsLambdaLayerVersion` objeto. Para ver as descrições dos atributos `AwsLambdaLayerVersion`, consulte AwsLambdaLayerVersionDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

Recursos da AwsMsk no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsMsk` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsMskCluster`, consulte AwsMskClusterDetailsna Referência da API AWS Security Hub .

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
        }
}
```

Recursos da AwsNetworkFirewall no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsNetworkFirewall` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsNetworkFirewallFirewall

O objeto `AwsNetworkFirewallFirewall` contém detalhes sobre um firewall do AWS Network Firewall .

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsNetworkFirewallFirewall` objeto. Para ver as descrições dos atributos `AwsNetworkFirewallFirewall`, consulte AwsNetworkFirewallFirewallDetailsna Referência da API AWS Security Hub .

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 atributos `AwsNetworkFirewallFirewallPolicy`, consulte AwsNetworkFirewallFirewallPolicyDetailsna Referência da API AWS Security Hub .

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 um grupo de regras do AWS Network Firewall . Os grupos de regras são usados para inspecionar e controlar o tráfego de rede.

Os grupos de regras sem estado se aplicam a pacotes individuais. Os grupos de regras com estado se aplicam a 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 atributos `AwsNetworkFirewallRuleGroup`, consulte AwsNetworkFirewallRuleGroupDetailsna Referência da API AWS Security Hub .

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: `IP` | `TCP` | `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` | `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | `DHCP`

- `Flags`

  Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

- `Masks`

  Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

Recursos da AwsOpenSearchService no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsOpenSearchService` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsOpenSearchServiceDomain`, consulte AwsOpenSearchServiceDomainDetailsna Referência da API AWS Security Hub .

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"
        ],
    }
}
```

Recursos da AwsRds no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsRds` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsRdsDbCluster`, consulte AwsRdsDbClusterDetailsna Referência da API AWS Security Hub .

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 atributos `AwsRdsDbClusterSnapshot`, consulte AwsRdsDbClusterSnapshotDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsRdsDbClusterSnapshot": {
    "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 `AwsRdsDbInstance` fornece detalhes sobre uma instância de banco de dados do RDS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbInstance` objeto. Para ver as descrições dos atributos `AwsRdsDbInstance`, consulte AwsRdsDbInstanceDetailsna Referência da API AWS Security Hub .

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 `AwsRdsDbSecurityGroup` contém informações sobre o Amazon Relational Database Service

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbSecurityGroup` objeto. Para ver as descrições dos atributos `AwsRdsDbSecurityGroup`, consulte AwsRdsDbSecurityGroupDetailsna Referência da API AWS Security Hub .

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 detalhes 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 atributos `AwsRdsDbSnapshot`, consulte AwsRdsDbSnapshotDetailsna Referência da API AWS Security Hub .

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 atributos `AwsRdsEventSubscription`, consulte AwsRdsEventSubscriptionDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsRedshift no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsRedshift` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsRedshiftCluster`, consulte AwsRedshiftClusterDetailsna Referência da API AWS Security Hub .

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": "amzn-s3-demo-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"
        }
    ]
}
```

Recursos da AwsRoute53 no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsRoute53` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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"
        }
    ]
}
```

Recursos da AwsS3 no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsS3` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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": "amzn-s3-demo-bucket",
        "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-123456789012",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"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 um objeto Amazon S3.

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"
}
```

Recursos da AwsSageMaker no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsSageMaker` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

AwsSageMakerNotebookInstance

O `AwsSageMakerNotebookInstance` objeto fornece informações sobre uma instância de notebook Amazon SageMaker AI, 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 atributos `AwsSageMakerNotebookInstance`, consulte AwsSageMakerNotebookInstanceDetailsna Referência da API AWS Security Hub .

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
}
```

Recursos da AwsSecretsManager no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsSecretsManager` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsSecretsManagerSecret`, consulte AwsSecretsManagerSecretDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsSns no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsSns` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsSnsTopic`, consulte AwsSnsTopicDetailsna Referência da API AWS Security Hub .

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"
}
```

Recursos da AwsSqs no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsSqs` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsSqsQueue`, consulte AwsSqsQueueDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

Recursos da AwsSsm no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsSsm` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsSsmPatchCompliance`, consulte AwsSsmPatchComplianceDetailsna Referência da API AWS Security Hub .

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"
        }
    }
}
```

Recursos da AwsStepFunctions no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsStepFunctions` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsStepFunctionStateMachine`, consulte AwsStepFunctionStateMachinena Referência da API AWS Security Hub .

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
    }
}
```

Recursos da AwsWaf no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsWaf` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsWafRateBasedRule`, consulte AwsWafRateBasedRuleDetailsna Referência da API AWS Security Hub .

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 `AwsWafRegionalRateBasedRule` contém detalhes sobre uma regra baseada em intervalos para recursos regionais. Uma regra baseada em intervalos 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 atributos `AwsWafRegionalRateBasedRule`, consulte AwsWafRegionalRateBasedRuleDetailsna Referência da API AWS Security Hub .

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. Esta regra identifica as solicitações da web que você deseja permitir, bloquear ou contabilizar.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRegionalRule` objeto. Para ver as descrições dos atributos `AwsWafRegionalRule`, consulte AwsWafRegionalRuleDetailsna Referência da API AWS Security Hub .

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 lista de controle de acesso à web (web ACL).

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRegionalRuleGroup` objeto. Para ver as descrições dos atributos `AwsWafRegionalRuleGroup`, consulte AwsWafRegionalRuleGroupDetailsna Referência da API AWS Security Hub .

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). Uma web ACL contém as regras 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 atributos `AwsApiGatewayV2Stage`, consulte AwsWafRegionalWebAclDetailsna Referência da API AWS Security Hub .

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 atributos `AwsApiGatewayV2Stage`, consulte AwsWafRuleDetailsna Referência da API AWS Security Hub .

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 atributos `AwsApiGatewayV2Stage`, consulte AwsWafRuleGroupDetailsna Referência da API AWS Security Hub .

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 atributos `AwsWafWebAcl`, consulte AwsWafWebAclDetailsna Referência da API AWS Security Hub .

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"
    }
}
```


Recursos da AwsXray no ASFF

Veja a seguir exemplos da sintaxe do AWS Security Finding Format (ASFF) para `AwsXray` recursos.

AWS Security Hub normaliza as descobertas de várias fontes no ASFF. Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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 atributos `AwsXrayEncryptionConfig`, consulte AwsXrayEncryptionConfigDetailsna Referência da API AWS Security Hub .

Exemplo

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepositoryobjeto no ASFF

O `CodeRepository` objeto fornece informações sobre um repositório de código externo que você conectou aos AWS recursos e configurou o Amazon Inspector para verificar vulnerabilidades.

O exemplo a seguir mostra a sintaxe do AWS Security Finding Format (ASFF) do `CodeRepository` objeto. Para ver as descrições dos atributos `CodeRepository`, consulte CodeRepositoryDetailsna Referência da API AWS Security Hub . Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

Exemplo

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Containerobjeto no ASFF

O exemplo a seguir mostra a sintaxe do AWS Security Finding Format (ASFF) do `Container` objeto. Para ver as descrições dos atributos `Container`, consulte ContainerDetailsna Referência da API

AWS Security Hub . Para obter informações contextuais sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

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"
    }]
}
```

Otherobjeto no ASFF

No Formato AWS de descoberta de segurança (ASFF), o `Other` objeto especifica campos e valores personalizados. Para obter mais informações sobre o ASFF, consulte AWS Formato de descoberta de segurança (ASFF).

Ao usar o `Other` objeto, você pode especificar campos e valores personalizados para um recurso. Você pode usar o `Other` objeto para os seguintes casos:

- O tipo de recurso não tem um objeto `Details` correspondente. Para especificar detalhes de um recurso, use o `Other` objeto.
- O `Details` objeto do tipo de recurso não inclui todos os atributos que você deseja especificar. Nesse caso, use o `Details` objeto do tipo de recurso para especificar os atributos disponíveis. Use o `Other` objeto para especificar atributos que não estão no objeto específico do tipo`Details`.
- O tipo de recurso não é um dos tipos fornecidos. Nesse caso, `Resource.Type` defina `Other` e use o `Other` objeto para especificar 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.

Visualizando insights no Security Hub CSPM

No AWS Security Hub CSPM, um insight é uma coleção de descobertas relacionadas. Um insight pode identificar uma área de segurança específica que requer atenção e intervenção. Por exemplo, um insight pode apontar EC2 casos 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 CSPM oferece vários insights gerenciados integrados. Você não pode modificar nem excluir insights gerenciados. Para rastrear problemas de segurança exclusivos de seu AWS ambiente e uso, você pode criar insights personalizados.

A página Insights no console CSPM do AWS Security Hub 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 CSPM.
- Para exibir somente insights personalizados, escolha Insights personalizados.

Você também pode filtrar a lista de insights com base no nome do insight. Para isso, 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.

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 número de verificações de CIS reprovadas retornará resultados somente se você habilitar o padrão Center for Internet Security (CIS) AWS Foundations Benchmark.

Analisando e agindo com base em insights no CSPM do Security Hub

Para cada insight, o AWS Security Hub CSPM determina primeiro 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 visualizar e agir em relação a resultados e a descobertas.

Se você habilitar a agregação entre regiões, os resultados para insights gerenciados (quando você fez login na região de agregação) incluirão descobertas da região de agregação e das regiões vinculadas. Os resultados de insights personalizados, se o insight não for filtrado por região, incluirão descobertas da região de agregação e das regiões vinculadas (quando você fez login na região de agregação). Em outras regiões, os resultados do insight são somente para aquela região.

Para obter informações sobre agregação entre regiões, consulte the section called “Agregando dados em todas as regiões”.

Visualizar e tomar medidas em relação a resultados de insights (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.

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 a um recurso de chave de acesso do IAM, os resultados do insight incluirão ambos os recursos.

No console CSPM do Security Hub, a lista de resultados é classificada da maioria para a menor quantidade de descobertas correspondentes. O CSPM do 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 responsáveis pelas descobertas correspondentes
- Tipo de recurso – cinco principais tipos de recurso para as descobertas correspondentes
- ID do recurso — Os cinco principais recursos IDs 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 da Amazon para o tipo de `Security Hub Insight Results` evento. Para obter mais informações, consulte the section called “Resposta e remediação automatizadas”. Se você não configurou ações personalizadas, o menu Ações será desabilitado.

Security Hub CSPM console

Para visualizar e agir em relação a resultados de insights (console)

1. Abra o console CSPM 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.

Security Hub CSPM API, AWS CLI

Para visualizar e agir com base nos resultados do insight (API, AWS CLI)

Para ver os resultados do insight, use a >GetInsightResultsoperação da API CSPM do Security Hub. Se você usar o AWS CLI, execute o get-insight-resultscomando.

Para identificar o insight para o qual retornar resultados, você precisa do ARN do insight. Para obter o insight ARNs para insights personalizados, use a operação `GetInsights`da API ou o get-insight-resultscomando.

O exemplo a seguir recupera os resultados para o insight especificado. 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-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

Para obter informações sobre como criar ações personalizadas programaticamente, consulte Usando ações personalizadas para enviar descobertas e resultados de insights para EventBridge.

Visualizar e tomar medidas em relação às descobertas de um resultado de insight (console)

Em uma lista de resultados de insights no console CSPM do Security Hub, você pode exibir a lista de descobertas de cada resultado.

Como exibir e agir em relação a descobertas de insights (console)

1. Abra o console CSPM 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, você pode realizar as seguintes ações:

- Filtrando descobertas no Security Hub CSPM
- Revisar os detalhes e o histórico das descobertas
- Definindo o status do fluxo de trabalho das descobertas no Security Hub CSPM
- Enviando descobertas para uma ação CSPM personalizada do Security Hub

Insights gerenciados no Security Hub CSPM

AWS O Security Hub CSPM fornece vários insights gerenciados.

Você não pode editar nem excluir insights gerenciados pelo CSPM 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, na lista a seguir, identifica as descobertas associadas aos buckets do Amazon S3. Se uma descoberta correspondente contiver um recurso de bucket do S3 e a um recurso de chave de acesso do IAM, os resultados do insight incluirão ambos os recursos.

Atualmente, o Security Hub CSPM oferece os seguintes insights gerenciados:

1. AWS recursos com o maior número de 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 estão gerando o maior número de descobertas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Agrupado por: ID da imagem da EC2 instância

   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. EC2 instâncias envolvidas em táticas, técnicas e procedimentos conhecidos (TTPs)

   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. AWS diretores 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. AWS instâncias de recursos que não atendem aos padrões de segurança/melhores práticas

   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. AWS recursos associados à possível exfiltração de dados

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Agrupado por: ID do recurso

Filtros de descoberta:

- O tipo começa com Effects/Data Exfiltração/
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

8. AWS recursos associados ao consumo não autorizado de recursos

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. EC2 instâncias que têm 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. EC2 casos 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. EC2 instâncias que têm 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. EC2 instâncias que não atendem aos padrões de segurança/melhores práticas

    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. EC2 instâncias 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. EC2 instâncias 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 /Discovery/Recon
- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

18. AWS recursos 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. AWS recursos associados a problemas de criptomoeda

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. AWS recursos 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 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 EC2 instâncias por número 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. Top AMIs por número de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Agrupado por: ID da imagem da EC2 instância

    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 o maior número de AWS Health descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - `ProductName` igual a `Health`

34. Recursos com o maior número de AWS Config descobertas

    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`

Entendendo os insights personalizados no Security Hub CSPM

Além dos insights gerenciados do AWS Security Hub CSPM, você pode criar insights personalizados no Security Hub CSPM para rastrear problemas específicos do seu ambiente. Os insights personalizados ajudam a rastrear um subconjunto selecionado 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 AWS serviço integrado específico, pode configurar uma visão personalizada 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 pode ser 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 de insights exibirão o número de descobertas associadas a cada provedor de descobertas.
- Filtros opcionais: os filtros opcionais reduzem as descobertas correspondentes para o insight.

  Uma descoberta será incluída nos resultados do insight somente se corresponder a todos os filtros fornecidos. Por exemplo, se os filtros forem “Nome do produto é GuardDuty” e “Tipo de recurso é `AwsS3Bucket` “, as descobertas correspondentes devem corresponder a esses dois critérios.

  No entanto, o Security Hub CSPM aplica a lógica booleana OR aos filtros que usam o mesmo atributo, mas valores diferentes. Por exemplo, se os filtros forem “Nome do produto é GuardDuty” e “Nome do produto é Amazon Inspector”, uma descoberta corresponderá se foi gerada pela Amazon GuardDuty ou pelo Amazon Inspector.

Se você usar o identificador ou o tipo de recurso como atributo de agrupamento, os resultados do insight incluirão todos os recursos que estiverem 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.

Se você habilitou a agregação entre regiões e depois criou om insight personalizado, o insight se aplicará às descobertas correspondentes na região de agregação e nas regiões vinculadas. A exceção é se o insight incluir um filtro de região.

Criar um insight personalizado

No AWS Security Hub CSPM, insights personalizados podem ser usados para coletar um conjunto específico de descobertas e rastrear problemas exclusivos do seu ambiente. Para obter informações contextuais sobre insights personalizados, consulte Entendendo os insights personalizados no Security Hub CSPM.

Escolha seu método preferido e siga as etapas para criar uma visão personalizada no Security Hub CSPM

Security Hub CSPM console

Para criar um insight personalizado (console)

1. Abra o console CSPM do AWS 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. Ou escolha 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.

Security Hub CSPM API

Para criar um insight personalizado (API)

1. Para criar uma visão personalizada, use a CreateInsightoperação da API CSPM do Security Hub. Se você usar o AWS CLI, execute o create-insightcomando.
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.

O exemplo a seguir cria um insight personalizado que inclui descobertas críticas com o tipo de recurso `AwsIamRole`. 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 create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Para criar um insight personalizado (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
```

Criar um insight personalizado baseado em um insight gerenciado (apenas console)

Você não pode salvar alterações nem excluir um insight gerenciado. Você também pode usar um insight gerenciado como base para um insight personalizado. Essa é uma opção somente no console CSPM do Security Hub.

Para criar um insight personalizado baseado em um insight gerenciado (console)

1. Abra o console CSPM do AWS 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 .

Editar um insight personalizado

Você pode editar 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.

No AWS Security Hub CSPM, insights personalizados podem ser usados para coletar um conjunto específico de descobertas e rastrear problemas exclusivos do seu ambiente. Para obter informações contextuais sobre insights personalizados, consulte Entendendo os insights personalizados no Security Hub CSPM.

Para editar um insight personalizado, escolha seu método preferido e siga as instruções.

Security Hub CSPM console

Para editar um insight personalizado (console)

1. Abra o console CSPM do AWS 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 atualizar o insight existente para refletir suas alterações, escolha Atualizar ***<Insight_Name>*** e, em seguida, escolha Salvar insight.
   - Para criar um insight com as atualizações, escolha Salvar novo insight. Insira um Nome de insight e então escolha Salvar insight.

Security Hub CSPM API

Para editar um insight personalizado (API)

1. Use a `UpdateInsight`operação da API CSPM do Security Hub. Se você usar o update-insightcomando AWS CLI run the.
2. Para identificar o insight personalizado que você deseja atualizar, forneça o nome do recurso da Amazon (ARN) do insight. Para obter o ARN de um insight personalizado, execute a operação `GetInsights` ou o comando get-insights.
3. Atualizar os parâmetros `Name`, `Filters`, e `GroupByAttribute` conforme necessário.

O exemplo a seguir atualiza insight especificado. 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 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

Para editar um insight personalizado (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"
```

Excluir um insight personalizado

No AWS Security Hub CSPM, insights personalizados podem ser usados para coletar um conjunto específico de descobertas e rastrear problemas exclusivos do seu ambiente. Para obter informações contextuais sobre insights personalizados, consulte Entendendo os insights personalizados no Security Hub CSPM.

Para excluir um insight personalizado, escolha seu método preferido e siga as instruções. Você não pode excluir um insight gerenciado.

Security Hub CSPM console

Para excluir um insight personalizado (console)

1. Abra o console CSPM do AWS Security Hub 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.

Security Hub CSPM API

Para excluir um insight personalizado (API)

1. Use a `DeleteInsight`operação da API CSPM do Security Hub. Se você usar o delete-insightcomando AWS CLI run the.
2. Para identificar o insight personalizado a ser excluído, forneça o ARN do insight. Para obter o ARN de um insight personalizado, use a operação `GetInsights` ou o comando get-insights.

O exemplo a seguir exclui o insight especificado. 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 delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

Para excluir um insight personalizado (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"
```

Modificando e agindo automaticamente com base nas descobertas no Security Hub CSPM

AWS O Security Hub CSPM tem recursos que modificam e agem automaticamente com base nas descobertas com base em suas especificações.

Atualmente, o Security Hub CSPM oferece suporte 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 EventBridge regras personalizadas da Amazon que definam ações automáticas a serem tomadas em relação a descobertas e insights específicos.

As regras de automação são úteis quando você deseja atualizar automaticamente os campos de busca no Formato AWS de descoberta de segurança (ASFF). Por exemplo, você pode usar uma regra de automação para atualizar o nível de gravidade ou o status do fluxo de trabalho das descobertas de determinadas integrações de terceiros. Usar a regra de automação elimina a necessidade de atualizar manualmente o nível de gravidade ou o status do fluxo de trabalho de cada descoberta desse produto de terceiros.

EventBridge as regras são úteis quando você deseja realizar ações fora do CSPM do Security Hub com relação a descobertas específicas ou enviar descobertas específicas para ferramentas de terceiros para remediação ou investigação adicional. As regras podem ser usadas para acionar ações compatíveis, como invocar uma AWS Lambda função ou notificar um tópico do Amazon Simple Notification Service (Amazon SNS) sobre uma descoberta específica.

As regras de automação entram em vigor antes que EventBridge as regras sejam aplicadas. Ou seja, as regras de automação são acionadas e atualizam uma descoberta antes de EventBridge receber a descoberta. EventBridge as regras 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. Enquanto o Security Hub CSPM ocasionalmente atualiza títulos e descrições de controle, o controle IDs permanece o mesmo.

Tópicos

Entendendo as regras de automação no Security Hub CSPM

Você pode usar regras de automação para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. À medida que ingere as descobertas, o Security Hub CSPM pode aplicar uma variedade de ações de regras, como suprimir descobertas, alterar sua gravidade e adicionar notas. Essas ações de regra modificam as descobertas que correspondem aos critérios que você especificou.

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`.

Você pode criar e gerenciar regras de automação somente de uma conta de administrador do CSPM do Security Hub.

As regras se aplicam às novas descobertas e às descobertas atualizadas. Você pode criar uma regra personalizada do zero ou usar um modelo de regra fornecido pelo Security Hub CSPM. Você também pode começar com um modelo e modificá-lo conforme o necessário.

Definir os critérios da regra e as ações da regra

Em uma conta de administrador do Security Hub CSPM, você pode criar uma regra de automação definindo um ou mais critérios de regra e uma ou mais ações de regra. Quando uma descoberta corresponde aos critérios definidos, o Security Hub CSPM aplica as ações da regra a ela. Para obter mais informações sobre critérios e ações disponíveis, consulte Critérios de regras e ações de regras disponíveis.

Atualmente, o Security Hub CSPM suporta no máximo 100 regras de automação para cada conta de administrador.

A conta de administrador do Security Hub CSPM também pode editar, visualizar e excluir regras de automação. Uma regra se aplica as descobertas correspondentes à conta do administrador e a todas as suas contas-membro. Ao fornecer a conta do membro IDs como critério de regra, os

administradores do CSPM do Security Hub também podem usar regras de automação para atualizar ou suprimir descobertas em contas de membros específicas.

Uma regra de automação se aplica somente Região da AWS no local em que foi criada. Para aplicar uma regra em várias regiões, o administrador deve criar a regra em cada uma delas. Isso pode ser feito por meio do console CSPM do Security Hub, da API CSPM do Security Hub ou. AWS CloudFormation Você também pode usar um script de implantação multirregional.

Critérios de regras e ações de regras disponíveis

Atualmente, os seguintes campos do AWS Security Finding Format (ASFF) são aceitos como critérios para regras de automação:

Critério da regra	Operadores de filtro	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, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`ComplianceAssociatedStandardsId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`ComplianceSecurityControlId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String

Critério da regra	Operadores de filtro	Tipo de campo
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)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Critério da regra	Operadores de filtro	Tipo de campo
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
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Critério da regra	Operadores de filtro	Tipo de campo
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
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Critério da regra	Operadores de filtro	Tipo de campo
`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
`UpdatedAt`	`Start, End, DateRange`	Data (formatada como 2022-12-01T21:47:39.269Z)
`UserDefinedFields`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Mapa

Critério da regra	Operadores de filtro	Tipo de campo
`VerificationState`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`WorkflowStatus`	`Is, Is Not`	Selecionar: [`NEW`, `NOTIFIED`, `RESOLVED`, `SUPPRESSED`]

Para critérios rotulados como campos de string, o uso de diferentes operadores de filtro no mesmo campo afeta a lógica de avaliação. Para obter mais informações, consulte a Referência StringFilterda API CSPM do AWS Security Hub.

Cada critério aceita um número máximo de valores que podem ser usados para filtrar as descobertas correspondentes. Para saber os limites de cada critério, consulte AutomationRulesFindingFiltersa Referência da API CSPM do AWS Security Hub.

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 ASFF específicos, consulte a sintaxe do AWS Security Finding Format (ASFF).

> **Tip**
>
> Se você quiser que o CSPM do 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 CSPM do 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 Desativando controles no Security Hub CSPM.

Descobertas que as regras de automação avaliam

Uma regra de automação avalia descobertas novas e atualizadas que o Security Hub CSPM gera ou ingere por meio da BatchImportFindingsoperação após a criação da regra. O CSPM do 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).

As regras de automação avaliam as descobertas originais fornecidas por provedores. Os provedores podem fornecer novas descobertas e atualizar as descobertas existentes por meio da `BatchImportFindings` operação da API CSPM do Security Hub. As regras não são acionadas quando você atualiza os campos de descoberta após a criação da regra por meio da operação BatchUpdateFindings. Se você criar uma regra de automação e fizer uma atualização de `BatchUpdateFindings` que afete o mesmo campo de descoberta, a última atualização definirá o valor desse campo. Veja o seguinte exemplo:

1. Você usa `BatchUpdateFindings` para atualizar o campo `Workflow.Status` de uma descoberta de `NEW` para `NOTIFIED`.
2. Se você chamar `GetFindings`, o campo `Workflow.Status` passará a ter um valor de `NOTIFIED`.
3. Você cria uma regra de automação que altera o campo `Workflow.Status` da descoberta de `NEW` para `SUPPRESSED` (lembre-se de que as regras ignoram as atualizações feitas com `BatchUpdateFindings`).
4. O provedor de descobertas usa `BatchImportFindings` para atualizar a descoberta e alterar o campo `Workflow.Status` para `NEW`.

5. Se você chamar `GetFindings`, o campo `Workflow.Status` passará a ter um valor de `SUPPRESSED` porque a regra de automação foi aplicada e a regra foi a última ação realizada na descoberta.

Quando você cria ou edita uma regra no console CSPM do Security Hub, o console exibe uma versão beta das descobertas que correspondem aos critérios da regra. Enquanto as regras de automação avaliam as descobertas originais enviadas pelo provedor de descoberta, a versão beta do console reflete as descobertas em seu estado final, conforme elas seriam mostradas em uma resposta à operação da GetFindingsAPI (ou seja, após ações de regras ou outras atualizações serem aplicadas à descoberta).

Como funciona a ordem das regras

Ao criar regras de automação, você atribui uma ordem a cada regra. Isso determina a ordem na qual o Security Hub CSPM 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 CSPM do Security Hub, o CSPM do 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 CSPM aplica as regras subsequentes em ordem crescente.

Quando você cria uma regra por meio da API CSPM do Security Hub ou AWS CLI, o Security Hub CSPM aplica a regra com o menor valor numérico para a primeira. `RuleOrder` Em seguida, aplica regras subsequentes em ordem ascendente. Se várias descobertas tiverem o mesmo valor`RuleOrder`, o Security Hub CSPM aplica uma regra com um valor anterior para o `UpdatedAt` campo primeiro (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 CSPM`

  - `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 CSPM do Security Hub que correspondem aos critérios da Regra A. Em seguida, as ações da Regra B se aplicam às descobertas do CSPM do Security Hub com o ID de 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`.

Criar regras de automação

Uma regra de automação pode ser usada para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. Você pode criar uma regra de automação personalizada do zero ou, no console CSPM do Security Hub, usar um modelo de regra pré-preenchido. Para obter informações contextuais sobre como as regras de automação funcionam, consulte Entendendo as regras de automação no Security Hub CSPM.

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 CSPM do Security Hub, o Security Hub CSPM mostra uma versão beta das descobertas às quais sua regra se aplica. No momento, a versão beta não é suportada se seus critérios de regra incluírem um filtro CONTAINS ou NOT_CONTAINS. Você pode escolher esses filtros para os tipos de campo de mapa e segmento.

> **Important**
>
> AWS recomenda que você não inclua informações de identificação pessoal, confidenciais ou sigilosas no nome, na descrição ou em outros campos da regra.

Criar uma regra de automação personalizada

Escolha o método de sua preferência e siga as etapas a seguir para criar regras de automação personalizadas.

Console

Para criar uma regra de autorização personalizada (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação à esquerda, escolha Automação.
3. Escolha 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 compatível com os critérios selecionados, o console mostra uma versão beta 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 Criar regra.

API

Para criar uma regra de autorização personalizada (API)

1. Execute `CreateAutomationRule`a partir da conta de administrador do Security Hub CSPM. 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 CSPM aplica primeiro regras com um valor numérico menor para esse parâmetro.
5. Para o `RuleStatus` parâmetro, especifique se você deseja que o CSPM do Security Hub seja ativado 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 `Criteria` parâmetro, forneça os critérios que você deseja que o Security Hub CSPM 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 `Actions` parâmetro, forneça as ações que você deseja que o CSPM do Security Hub execute quando houver uma correspondência entre uma descoberta e seus critérios definidos. Para ver uma de ações compatíveis, consulte Critérios de regras e ações de regras disponíveis.

O AWS CLI comando de exemplo a seguir cria uma regra de automação que atualiza o status do fluxo de trabalho e a nota das descobertas correspondentes. 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 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
```

Criar uma regra de automação a partir de um modelo (console apenas)

Os modelos de regra refletem casos de uso comuns de regras de automação. Atualmente, somente o console CSPM do Security Hub oferece suporte a modelos de regras. Conclua as etapas a seguir para criar uma regra de automação a partir de um modelo no console.

Para criar uma regra de automação a partir de um modelo (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação à esquerda, escolha Automação.
3. Escolha 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 mostrará uma versão beta 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 Criar regra.

Visualizar regras de automação

Uma regra de automação pode ser usada para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. Para obter informações contextuais sobre como as regras de automação funcionam, consulte Entendendo as regras de automação no Security Hub CSPM.

Escolha seu método preferido e siga as etapas para visualizar as regras de automação existentes e os detalhes de cada regra.

Para visualizar um histórico de como as regras de automação alteraram suas descobertas, consulte Analisando os detalhes e o histórico da descoberta no Security Hub CSPM.

Console

Para visualizar regras de automação (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
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

Para visualizar regras de automação (API)

1. Para visualizar as regras de automação da sua conta, execute a `ListAutomationRules`partir da conta de administrador do CSPM do Security Hub. Essa API retorna a regra ARNs e outros metadados das suas regras. Nenhum parâmetro de entrada é necessário para essa API, mas você pode fornecer opcionalmente `MaxResults` para limitar o número de resultados e `NextToken` como parâmetro de paginação. O valor inicial de `NextToken` deveria ser `NULL`.
2. Para obter detalhes adicionais da regra, incluindo os critérios e as ações de uma regra, execute a `BatchGetAutomationRules`partir da conta de administrador do CSPM do Security Hub. Forneça as regras ARNs de automação das quais você deseja detalhes.

   O exemplo seguir recupera os detalhes das regras de automação especificadas. 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 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

Uma regra de automação pode ser usada para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. Para obter informações contextuais sobre como as regras de automação funcionam, consulte Entendendo as regras de automação no Security Hub CSPM.

Depois de criar uma regra de automação, o administrador delegado do CSPM do Security Hub pode editar a regra. Quando você edita uma regra de automação, as alterações se aplicam às descobertas novas e atualizadas que o Security Hub CSPM gera ou ingere após a edição da regra.

Escolha seu método preferido e siga as etapas para editar o conteúdo de uma regra de automação. Você pode 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 de automação.

Console

Para editar regras de automação (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
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

Para editar regras de automação (API)

1. Execute `BatchUpdateAutomationRules`a partir da conta de administrador do Security Hub CSPM.
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. Você pode editar qualquer parâmetro, exceto `RuleArn`.

O exemplo a seguir atualiza a regra de automação 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 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 de automação

Uma regra de automação pode ser usada para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. Para obter informações contextuais sobre como as regras de automação funcionam, consulte Entendendo as regras de automação no Security Hub CSPM.

Depois de criar uma regra de automação, o administrador delegado do CSPM do Security Hub pode editar a regra.

Se você quiser manter os mesmos critérios e ações da regra, mas alterar a ordem na qual o CSPM do Security Hub aplica uma regra de automação, você pode editar apenas a ordem das regras. Escolha seu método preferido e siga as etapas para editar a ordem das regras.

Para obter instruções sobre como editar os critérios ou as ações de uma regra de automação, consulte Editar regras de automação.

Console

Para editar a ordem das regras de automação (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
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 CSPM do Security Hub, o CSPM do 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

Para editar a ordem das regras de automação (API)

1. Use a `BatchUpdateAutomationRules`operação da conta de administrador do CSPM 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 CSPM aplicará uma regra com um valor anterior para o `UpdatedAt` campo primeiro (ou seja, a regra que foi editada mais recentemente se aplica por último).

Excluir ou desabilitar regras de automação

Uma regra de automação pode ser usada para atualizar automaticamente as descobertas no CSPM do AWS Security Hub. Para obter informações contextuais sobre como as regras de automação funcionam, consulte Entendendo as regras de automação no Security Hub CSPM.

Quando você exclui uma regra de automação, o Security Hub CSPM a remove da sua conta e não aplica mais a regra às descobertas. Como alternativa à exclusão, você pode desabilitar uma regra. Isso retém a regra para uso futuro, mas o Security Hub CSPM não aplicará a regra a nenhuma descoberta correspondente até que você a habilite.

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.

Console

Para excluir ou desabilitar regras de automação (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
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

Para excluir ou desabilitar regras de automação (API)

1. Use a `BatchDeleteAutomationRules`operação da conta de administrador do CSPM 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`).

O exemplo a seguir exclui a regra de automação 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 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 fornece exemplos de regras de automação para casos de uso comuns do CSPM do Security Hub. Esses exemplos correspondem aos modelos de regras que estão disponíveis no console CSPM 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`. Você pode 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 CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/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 CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
```

```
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/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 CSPM",
            "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 CSPM",
"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 CSPM da 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
```

Usando EventBridge para resposta e remediação automatizadas

Ao criar regras na Amazon EventBridge, você pode responder automaticamente às descobertas do CSPM do AWS Security Hub. O Security Hub CSPM envia descobertas como eventos EventBridge em tempo quase real. 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. Ações que podem ser automaticamente acionadas incluem:

- Invocando uma função AWS Lambda
- Invocando o comando de EC2 execução da Amazon
- Transmitir o evento Amazon Kinesis Data Streams
- Ativando uma máquina de AWS Step Functions estado
- Notificar um tópico do Amazon SNS ou 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 CSPM envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes EventBridge como EventBridge eventos. Você também pode criar ações personalizadas que permitem enviar descobertas selecionadas e resultados de insights para EventBridge.

Em seguida, você configura EventBridge as regras para responder a cada tipo de evento.

Para obter mais informações sobre o uso EventBridge, consulte o Guia EventBridge do usuário da Amazon.

> **Note**
>
> Como prática recomendada, certifique-se de que as permissões de acesso concedidas aos usuários EventBridge usem políticas de privilégios mínimos AWS Identity and Access Management (IAM) que concedam somente as permissões necessárias.
> Para obter mais informações, consulte Gerenciamento de identidade e acesso na Amazon EventBridge.

Um conjunto de modelos para resposta e remediação automatizadas entre contas também está disponível em AWS Soluções. Os modelos utilizam regras de EventBridge eventos e funções Lambda. Você implanta a solução usando AWS CloudFormation AWS Systems Manager e. A solução pode criar ações de resposta e remediação totalmente automatizadas. Ele também pode usar ações personalizadas do Security Hub CSPM 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 eventos CSPM do Security Hub em EventBridge
- EventBridge formatos de eventos para o Security Hub CSPM
- Configurando uma EventBridge regra para as descobertas do CSPM do Security Hub
- Usando ações personalizadas para enviar descobertas e resultados de insights para EventBridge

Tipos de eventos CSPM do Security Hub em EventBridge

O Security Hub CSPM usa os seguintes tipos de EventBridge eventos da Amazon para integração com. EventBridge

No EventBridge painel do Security Hub CSPM, Todos os eventos inclui todos esses tipos de eventos.

Todas as descobertas (Security Hub Findings - Imported)

O Security Hub CSPM envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes EventBridge como Security Hub Findings - Importedeventos. 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 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 the section called “Agregando dados em todas as regiões”.

Você pode definir regras EventBridge que encaminhem automaticamente as descobertas para um fluxo de trabalho de remediação, ferramenta de terceiros ou outro EventBridge alvo compatível. 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 “Configurando uma regra EventBridge ”.

Descobertas para ações personalizadas (Security Hub Findings - Custom Action)

O Security Hub CSPM também envia descobertas associadas a ações personalizadas para eventos EventBridge . Security Hub Findings - Custom Action

Isso é útil para analistas que trabalham com o console CSPM do Security Hub que desejam enviar uma descoberta específica, ou um pequeno conjunto de descobertas, para um fluxo de trabalho de resposta ou remediação. É possível selecionar uma ação personalizada para até 20 descobertas por vez. Cada descoberta é enviada EventBridge como um EventBridge evento separado.

Ao criar uma ação personalizada, você atribui a ela uma ID de ação personalizada. Você pode usar essa ID para criar uma EventBridge regra que executa uma ação específica depois de 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 CSPM do Security Hub chamada. `send_to_ticketing` Em seguida EventBridge, você cria uma regra que é acionada quando EventBridge recebe uma descoberta que inclui o ID da ação `send_to_ticketing` personalizada. A regra inclui a lógica para enviar a descoberta ao sistema de emissão de tíquetes. Em seguida, você pode selecionar as descobertas no CSPM do Security Hub e usar a ação personalizada no CSPM do Security Hub para enviar manualmente as descobertas ao seu sistema de tíquetes.

Para obter exemplos de como enviar as descobertas do CSPM do Security Hub EventBridge para processamento adicional, consulte Como integrar ações personalizadas do CSPM do AWS Security Hub com PagerDuty e Como habilitar ações personalizadas no CSPM do AWS Security Hub no blog da 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 EventBridge como Security Hub Insight Resultseventos. Os resultados do insight são os recursos que combinam com um insight. Observe que quando você envia os resultados do insight para EventBridge, você não está enviando as descobertas para 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 CSPM do 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.

EventBridge formatos de eventos para o Security Hub CSPM

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 o formato usado quando o CSPM do Security Hub envia um evento para. EventBridge

Security Hub Findings - Imported

Security Hub Findings - Importedeventos enviados do Security Hub CSPM para EventBridge usar 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 EventBridge regras que são acionadas por esses eventos, consultethe section called “Configurando uma regra EventBridge ”.

Security Hub Findings - Custom Action

Security Hub Findings - Custom Actioneventos enviados do Security Hub CSPM para EventBridge usar 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 EventBridge regras que são acionadas por esses eventos, consultethe section called “Configurando e usando ações personalizadas”.

Security Hub Insight Results

Security Hub Insight Resultseventos enviados do Security Hub CSPM para EventBridge usar 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 EventBridge regra que é acionada por esses eventos, consultethe section called “Configurando e usando ações personalizadas”.

Configurando uma EventBridge regra para as descobertas do CSPM do Security Hub

Você pode criar uma regra na Amazon EventBridge que define uma ação a ser tomada quando um Security Hub Findings - Importedevento é recebido. Security Hub Findings - Importedos eventos são acionados por atualizações `BatchUpdateFindings`das operações `BatchImportFindings`e.

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 de eventos então identifica os alvos da regra. Os alvos são as ações a serem tomadas quando EventBridge recebe um evento Security Hub Findings - Imported e a descoberta corresponde aos filtros.

As instruções fornecidas aqui usam o EventBridge console. Quando você usa o console, cria EventBridge automaticamente a política baseada em recursos necessária que permite EventBridge gravar no Amazon CloudWatch Logs.

Você também pode usar a `PutRule`operação da EventBridge API. No entanto, se você usar a EventBridge API, deverá criar a política baseada em recursos. Para obter informações sobre a política necessária, consulte Permissões de CloudWatch registros no Guia EventBridge do usuário da Amazon.

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 CSPM 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 Security Finding Format (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 em EventBridge. Se você selecionar um padrão predefinido, preenche EventBridge automaticamente e. `source` `detail-type` 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 EventBridge regra (console)

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Usando os valores a seguir, crie uma EventBridge regra que monitore a localização de eventos:
   - Para Tipo de regra, escolha Regra com 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 Fonte do evento, selecione Serviços da AWS . • Para o AWS serviço, selecione 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 EventBridge console.)	• 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"] } } }`	

- Para Tipos de destino, escolha AWS serviço e, para Selecionar um destino, escolha um destino, como um tópico ou AWS Lambda função do Amazon SNS. O destino é acionado quando é recebido um evento que corresponde ao padrão de evento definido na regra.

Para obter detalhes sobre a criação de regras, consulte Criação de EventBridge regras da Amazon que reagem a eventos no Guia EventBridge do usuário da Amazon.

Usando ações personalizadas para enviar descobertas e resultados de insights para EventBridge

Para usar as ações personalizadas do CSPM do AWS Security Hub para enviar descobertas ou resultados de insights para a Amazon EventBridge, primeiro você cria a ação personalizada no

CSPM do Security Hub. Em seguida, você pode definir regras EventBridge que se apliquem às suas ações personalizadas.

É possível criar até 50 ações personalizadas.

Se você habilitar a agregação entre regiões e gerenciar as descobertas na região de agregação, crie as ações personalizadas na região de agregação.

A regra em EventBridge usa o Amazon Resource Name (ARN) da ação personalizada.

Criar uma ação personalizada

Ao criar uma ação personalizada no CSPM do AWS Security Hub, você especifica seu nome, descrição e um identificador exclusivo.

Uma ação personalizada especifica quais ações devem ser tomadas quando um EventBridge evento corresponde a uma EventBridge regra. O CSPM do Security Hub envia cada descoberta EventBridge como um evento.

Escolha seu método preferido e siga as etapas para criar uma regra personalizada.

Console

Para criar uma ação personalizada no Security Hub CSPM (console)

1. Abra o console CSPM 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.

API

Para criar uma ação personalizada (API)

Use a operação CreateActionTarget. Se você estiver usando o AWS CLI, execute o create-action-targetcomando.

O exemplo a seguir cria uma ação personalizada para enviar descobertas para uma ferramenta de remediação. 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 create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definindo uma regra em EventBridge

Para acionar uma ação personalizada na Amazon EventBridge, você deve criar uma regra correspondente em EventBridge. A definição da regra inclui o nome do recurso da Amazon (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 EventBridge console. Quando você usa o console, cria EventBridge automaticamente a política baseada em recursos necessária que permite EventBridge gravar CloudWatch em registros.

Você também pode usar a `PutRule`operação de EventBridge API da API. No entanto, se você usar a EventBridge API, deverá criar a política baseada em recursos. Para obter detalhes sobre a política necessária, consulte Permissões de CloudWatch registros no Guia EventBridge do usuário da Amazon.

Para definir uma regra em EventBridge (EventBridge console)

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Escolha Create rule.
4. Insira um nome e uma descrição para a regra.
5. Em Barramento de Eventos, 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, escolha Rule with an event pattern.
7. Escolha Próximo.
8. Em Origem de eventos, escolha Eventos da AWS .
9. Em Padrão de evento, selecione Formulário de padrão de evento.
10. Em Fonte do evento, selecione Serviços da AWS .
11. Para o AWS serviço, 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. Escolha Ação personalizada específica ARNs e adicione um ARN de ação personalizada.

    Se a regra se aplicar a várias ações personalizadas, escolha Adicionar para adicionar mais ações personalizadas ARNs.

14. Escolha Próximo.
15. Em Adicionar destino, selecione e configure destino a ser invocado quando essa regra for correspondida.
16. Escolha Próximo.
17. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte as EventBridge tags da Amazon no Guia EventBridge do usuário da Amazon.
18. Escolha Próximo.
19. Analise os detalhes da regra e selecione Criar regra.

    Quando você executa uma ação personalizada sobre descobertas ou resultados de insights em sua conta, os eventos são gerados em EventBridge.

Seleção de uma ação personalizada para descobertas e resultados de insights

Depois de criar as ações personalizadas do AWS Security Hub CSPM e EventBridge as regras da Amazon, você pode enviar descobertas e resultados de insights EventBridge para gerenciamento e processamento automáticos.

Os eventos são enviados EventBridge somente para a conta em que são visualizados. Se você visualizar uma descoberta usando uma conta de administrador, o evento será enviado para EventBridge a conta do administrador.

Para que as chamadas de AWS API sejam efetivas, as implementações do código de destino devem mudar de função para contas de membros. 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 EventBridge (console)

1. Abra o console CSPM 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 de um controle específico. Para obter mais informações, consulte Analisando os detalhes dos controles no Security Hub CSPM.
- Em Integrações, você pode navegar até uma lista de descobertas geradas por uma integração habilitada. Para obter mais informações, consulte Visualizando descobertas de uma integração CSPM do Security Hub.
- Em Insights, você pode navegar até uma lista de descobertas para um resultado de insight. Para obter mais informações, consulte Analisando e agindo com base em insights no CSPM do Security Hub.

3. Selecione as descobertas para as quais enviar EventBridge. É possível selecionar até 20 descobertas por vez.
4. Em Ações, escolha a ação personalizada que se alinha à EventBridge regra a ser aplicada.

   O CSPM do Security Hub envia um evento separado do Security Hub Findings - Custom Action para cada descoberta.

Para enviar resultados de insights para EventBridge (console)

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, escolha Insights.
3. Na página Insights, escolha o insight que inclui os resultados para os quais enviar EventBridge.
4. Selecione os resultados do insight para os quais enviar EventBridge. Você pode selecionar até 20 descobertas por vez.
5. Em Ações, escolha a ação personalizada que se alinha à EventBridge regra a ser aplicada.

Trabalhando com o painel no Security Hub CSPM

A página Resumo no console do Security Hub mostra um resumo de seus riscos, sequências de ataque e cobertura de segurança. Esta página ajuda você a identificar riscos e sequências de ataque com base em sua gravidade e na cobertura da conta para diferentes recursos de segurança. Você pode personalizar essa página adicionando e removendo diferentes widgets de segurança e definindo um critério de filtro para recuperar tipos específicos de dados.

As personalizações desta página são salvas para uso futuro. Se os usuários da sua conta personalizarem essa página, suas preferências de personalização serão salvas independentemente de suas preferências de personalização.

Se sua conta for a conta de administrador delegado de uma organização, os dados incluem descobertas para sua conta e contas de membros. Se sua conta for uma conta de membro ou uma conta independente, os dados incluirão apenas as descobertas da sua conta.

Se você configurar a agregação entre regiões no Security Hub CSPM, esta página mostra os resultados da sua agregação

> **Note**
>
> Toda vez que você abre essa página, ela é atualizada automaticamente. No entanto, as pontuações de segurança e os status de controle são atualizados a cada 24 horas.

O widget de resumo de riscos

Esse widget mostra todos os seus riscos com base na gravidade. Os riscos com maior gravidade aparecem primeiro. Os riscos são baseados em uma análise das descobertas e características do Security Hub CSPM e outros. Serviços da AWS

O widget de resumo de ameaças

Esse widget mostra todas as suas sequências de ataque com base na gravidade. As sequências de ataque com maior severidade aparecem primeiro. As sequências de ataque estão relacionadas a uma série de eventos e identificam possíveis ameaças em seu ambiente. Eles também se originam em GuardDuty.

O widget de cobertura de segurança

Widgets disponíveis para o painel Resumo

O painel de resumo inclui widgets que refletem o cenário moderno de ameaças à segurança na nuvem, orientado pelas operações e experiências de segurança dos AWS clientes. 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:

Principais sequências de ameaças

Exibe as sequências de ameaças de maior gravidade. As descobertas da sequência de ameaças, conhecidas como descobertas da sequência de ataque na Amazon GuardDuty, correlacionam vários eventos para identificar possíveis ameaças ao seu AWS ambiente. As sequências de ameaças podem incluir comportamentos de ataque em andamento ou recentes (dentro de uma janela de 24 horas) em seu ambiente, o que, por sua vez, pode levar a um maior comprometimento. Você deve ter GuardDuty o GuardDuty S3 Protection ativado para receber as descobertas da sequência de ameaças no CSPM do Security Hub.

Principais riscos

Exibe um resumo dos principais riscos em seu ambiente. A parte superior do widget mostra a contagem de riscos em cada nível de gravidade. Você pode escolher um nível de severidade para acessar a página Riscos com os riscos filtrados para o nível de severidade selecionado. Os riscos que têm mais ocorrências em seu ambiente aparecem primeiro. Esse widget ajuda você a priorizar quais riscos devem ser mitigados.

Cobertura de segurança

Resume a extensão da sua cobertura de segurança, com base nas descobertas do controle de cobertura. Os controles de cobertura verificam se um específico AWS service (Serviço da AWS) e seus recursos estão habilitados (por exemplo,[Macie.1] O Amazon Macie deve estar habilitado). Esse widget ajuda a garantir que você tenha `PASSED` descobertas sobre controles de cobertura. O console CSPM do Security Hub fornece links desse widget para ajudá-lo a ativar os recursos de segurança ausentes. Recomendamos usar a configuração central para ativar os recursos de segurança ausentes em vários Contas da AWS Regiões da AWS e. Para obter mais informações, consulte Entendendo a configuração central no Security Hub CSPM.

Padrões de segurança

Exibe sua pontuação de segurança resumida mais recente e a pontuação de segurança de cada padrão CSPM 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 Método de cálculo das pontuações de segurança. Esse widget ajuda você a entender sua postura geral de segurança.

Padrões de segurança

Exibe sua pontuação de segurança resumida mais recente e a pontuação de segurança de cada padrão CSPM 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 Método de cálculo das pontuações de segurança. 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 CSPM 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 uma Região da AWS em que o Security Hub CSPM está ativado. 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 AWS ambiente. Isso inclui ameaças como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP maliciosos.

Para visualizar esses dados, a Amazon GuardDuty deve estar habilitada. Se estiver, escolha um tipo de ameaça nesse widget para abrir o GuardDuty console 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 AWS ambiente 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 seguintes tipos de recursos: buckets do Amazon Simple Storage Service (Amazon S3), instâncias e funções do Amazon Elastic Compute Cloud (EC2Amazon). 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 AWS .

Widgets ocultos por padrão

Os widgets a seguir também estão disponíveis para o painel Resumo, mas estão ocultos por padrão:

AMIs com o maior número de descobertas

Fornece uma lista das 10 Amazon Machine Images (AMIs) que geraram a maioria das descobertas. Esses dados estarão disponíveis somente se a Amazon estiver EC2 habilitada para sua conta. Ele ajuda você a identificar quais AMIs representam possíveis riscos de segurança.

Entidades principais do IAM com mais descobertas

Fornece uma lista dos 10 usuários AWS Identity and Access Management (IAM) que geraram mais descobertas. Esse widget ajuda a realizar tarefas administrativas e de cobrança. Ele mostra quais usuários contribuem mais para o uso do CSPM 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 CSPM do Security Hub e o número de descobertas que eles geraram. Os insights identificam uma área de segurança específica que requer atenção.

Últimas descobertas das AWS integrações

Mostra o número de descobertas que você recebeu do CSPM do Security Hub integrado. Serviços da AWS 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 CSPM abre o console desse serviço.

Filtrando o painel de resumo no Security Hub CSPM

Você pode organizar o painel de resumo no console CSPM do AWS Security Hub para que ele inclua somente os dados de segurança mais relevantes para você. 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 criar essas visualizações personalizadas, 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 e widgets no painel, exceto aos dados nos widgets Insights e Padrões de segurança. Para obter uma lista dos widgets disponíveis no painel, consulte Widgets disponíveis para o painel Resumo.

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 produto AWS service (Serviço da AWS) ou de terceiros que envia descobertas para o Security Hub CSPM)
- 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 `RecordState` 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 CSPM 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 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 CSPM 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 visualização padrão do painel Resumo, sua visualização padrão será redefinida para a visualização CSPM padrão do Security Hub.

Para atualizar ou excluir um conjunto de filtros

1. Abra o console CSPM 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.

Personalizando o painel de resumo no Security Hub CSPM

Você pode personalizar o painel Summary no console CSPM do AWS Security Hub de várias maneiras. Por exemplo, você pode adicionar e remover widgets do painel. Também é possível reorganizar e redimensionar widgets no painel. Para obter uma lista dos widgets disponíveis no painel, consulte Widgets disponíveis para o painel Resumo.

Se você personalizar o painel, o Security Hub CSPM aplicará suas alterações imediatamente e salvará as novas configurações do painel. Suas alterações se aplicam à sua visualização do painel em todos Regiões da AWS os navegadores.

Para personalizar o painel Resumo

1. Abra o console CSPM 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.

Limites regionais para o Security Hub CSPM

Alguns recursos do CSPM do AWS Security Hub estão disponíveis apenas em alguns. Regiões da AWS As seções a seguir especificam esses limites regionais. Para obter uma lista completa de todas as regiões em que o CSPM do Security Hub está disponível atualmente, consulte endpoints e cotas do AWS Security Hub no. Referência geral da AWS

Restrições de agregação entre regiões

Em AWS GovCloud (US) Regions, a agregação entre regiões está disponível somente para descobertas, atualizações e insights AWS GovCloud (US) Regions . Especificamente, você pode agregar descobertas, atualizações e insights somente entre as regiões 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 pode agregar descobertas, atualizações e insights somente entre as regiões da China (Pequim) e China (Ningxia).

Você não pode usar uma região desativada por padrão como sua região de agregação. Para obter uma lista de regiões que estão desativadas por padrão, consulte Ativar ou desativar Regiões da AWS em sua conta no Guia de AWS Gerenciamento de contas referência.

Disponibilidade de integrações por região

Algumas integrações não estão disponíveis em todas Regiões da AWS. No console CSPM do Security Hub, uma integração não aparece na página Integrações se não estiver disponível na região na qual você está conectado no momento.

Integrações suportadas nas regiões da China (Pequim) e China (Ningxia)

Nas regiões da China (Pequim) e China (Ningxia), o Security Hub CSPM suporta somente as 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

Nas regiões da China (Pequim) e China (Ningxia), o Security Hub CSPM oferece suporte somente às 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 suportadas nas regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA)

Nas regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA), o Security Hub CSPM suporta somente as seguintes integrações com: Serviços da AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

Nas regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA), o CSPM do Security Hub oferece 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

O padrão AWS Control Tower gerenciado por serviços está disponível somente em Regiões da AWS que AWS Control Tower oferece suporte, inclusive. AWS GovCloud (US) Regions Para obter uma lista das regiões que AWS Control Tower atualmente oferecem suporte, consulte Como Regiões da AWS trabalhar com AWS Control Tower no Guia AWS Control Tower do usuário.

O padrão de marcação de AWS recursos não está disponível nas seguintes regiões: Ásia-Pacífico (Taipei), Ásia-Pacífico (Tailândia) e México (Central).

Outros padrões de segurança estão disponíveis em todas as regiões em que o Security Hub CSPM está disponível atualmente.

Disponibilidade de controles por região

Alguns controles CSPM do Security Hub não estão disponíveis em todas as regiões. Para obter uma lista de controles que não estão disponíveis em cada região, consulteLimites regionais nos controles CSPM do Security Hub.

No console CSPM do Security Hub, um controle não aparece na lista de controles se não estiver disponível na região na qual você está conectado no momento. A exceção é uma região de agregação. Se você definir uma região de agregação e entrar nessa região, o console mostrará os controles que estão disponíveis na região de agregação ou em uma ou mais regiões vinculadas.

Limites regionais nos controles CSPM do Security Hub

Alguns controles CSPM do AWS Security Hub não estão disponíveis em todos. Regiões da AWS Esta página especifica quais controles não estão disponíveis em regiões específicas.

No console CSPM do Security Hub, um controle não aparece na lista de controles se não estiver disponível na região na qual você está conectado no momento. A exceção é uma região de agregação. Se você definir uma região de agregação e entrar nessa região, o console mostrará os controles que estão disponíveis na região de agregação ou em uma ou mais regiões vinculadas.

Regiões da AWS

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Norte da Califórnia)
- Oeste dos EUA (Oregon)
- África (Cidade do Cabo)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)

- Ásia-Pacífico (Malásia)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Osaka)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Taipei)
- Ásia-Pacífico (Tailândia)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Oeste do Canadá (Calgary)
- China (Pequim)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milão)
- Europa (Paris)
- Europa (Espanha)
- Europa (Estocolmo)
- Europa (Zurique)
- Israel (Tel Aviv)
- México (Central)
- Oriente Médio (Bahrein)
- Oriente Médio (Emirados Árabes Unidos)
- 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 suportados na região Leste dos EUA (Norte da Virgínia).

- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH ativado
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas

Leste dos EUA (Ohio)

Os controles a seguir não são suportados na região Leste dos EUA (Ohio).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Oeste dos EUA (Norte da Califórnia)

Os controles a seguir não são suportados na região Oeste dos EUA (Norte da Califórnia).

- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado

- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados

- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Oeste dos EUA (Oregon)

Os controles a seguir não são compatíveis com a região Oeste dos EUA (Oregon).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

África (Cidade do Cabo)

Os controles a seguir não são suportados na região da África (Cidade do Cabo).

- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppRunner.1] Os serviços do App Runner devem ser marcados

- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- [ES.3] Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support

- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado

- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Hong Kong)

Os controles a seguir não são compatíveis com a região Ásia-Pacífico (Hong Kong).

- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito

- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados

- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Hyderabad)

Os controles a seguir não são suportados na região Ásia-Pacífico (Hyderabad).

- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations

- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada

- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito

- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [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
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito

- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados

- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados

- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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.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.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC

- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] 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
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas

- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Jacarta)

Os controles a seguir não são suportados na região Ásia-Pacífico (Jacarta).

- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado

- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos

- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [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
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas

- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas

- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] 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 habilitadas
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Malásia)

Os controles a seguir não são suportados na região Ásia-Pacífico (Malásia).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [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
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização

- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [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
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados

- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.1] DataSync as tarefas devem ter o registro ativado
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] 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 acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas

- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.52] gateways EC2 de trânsito devem ser marcados
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar 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 sub-redes que atribuem endereços IP públicos na inicialização
- [EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados
- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado

- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados

- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados

- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.31] Os grupos de segurança de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito
- [RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito

- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.8] 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.13] Os snapshots de cluster do Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys

- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [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 em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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

- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [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.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [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 do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados

- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Melbourne)

Os controles a seguir não são suportados na região Ásia-Pacífico (Melbourne).

- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados

- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.18] Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos

- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [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
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado

- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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

- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado

- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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.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.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
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado

- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Mumbai)

Os controles a seguir não são suportados na região Ásia-Pacífico (Mumbai).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas

- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Osaka)

Os controles a seguir não são suportados na região Ásia-Pacífico (Osaka).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem 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
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- [ELB.4] O Application Load Balancer deve ser configurado para descartar cabeçalhos http inválidos
- [ELB.6] A proteção contra exclusão dos balanceadores de carga de aplicações, gateways e redes deve estar habilitada
- [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
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [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 saúde 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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.4] A chave de acesso do usuário raiz do IAM não deve existir
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados

- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão

- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Seul)

Os controles a seguir não são suportados na região Ásia-Pacífico (Seul).

- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue

- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Singapura)

Os controles a seguir não são suportados na região Ásia-Pacífico (Cingapura).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas

- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Sydney)

Os controles a seguir não são suportados na região Ásia-Pacífico (Sydney).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados

- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Taipei)

Os controles a seguir não são suportados na região Ásia-Pacífico (Taipei).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ACM.3] Os certificados do 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
- [APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado
- [APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF

- [APIGateway.5] Os dados do cache da API REST de Gateway devem ser criptografados em repouso
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado
- [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 em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2

- [AutoScaling.10] Grupos de EC2 Auto Scaling devem ser marcados
- [Autoscaling.5] As instâncias da EC2 Amazon 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
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada

- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.1] DataSync as tarefas devem ter o registro ativado
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoB.5] As tabelas do DynamoDB devem ser marcadas
- [DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado

- [EC2.10] A Amazon EC2 deve ser configurada para usar endpoints VPC criados para o serviço Amazon EC2
- [EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.35] interfaces EC2 de rede devem ser marcadas
- [EC2.36] os gateways EC2 do cliente devem ser marcados
- [EC2.37] Os endereços IP EC2 elásticos devem ser marcados
- [EC2.38] as EC2 instâncias devem ser marcadas
- [EC2.39] gateways de EC2 internet devem ser marcados
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.41] a EC2 rede ACLs deve ser marcada
- [EC2.42] tabelas de EC2 rotas devem ser marcadas
- [EC2.43] grupos EC2 de segurança devem ser marcados
- [EC2.44] EC2 sub-redes devem ser marcadas
- [EC2.45] EC2 volumes devem ser marcados
- [EC2.46] Amazon VPCs deve ser etiquetada
- [EC2.47] Os serviços de endpoint do Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento do Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de EC2 VPN devem ser marcados

- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.52] gateways EC2 de trânsito devem ser marcados
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.172] As configurações do EC2 VPC Block Public Access devem bloquear o tráfego do gateway da Internet
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário
- [ECS.2] Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters do ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar 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 sub-redes que atribuem endereços IP públicos na inicialização

- [EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados
- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.1] Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- [ELB.7] 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
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado

- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.1] Os domínios do Elasticsearch devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- [ES.3] 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.5] Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado
- [ES.6] Os domínios do Elasticsearch devem ter pelo menos três nós de dados
- [ES.7] 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
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados

- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado

- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos

- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas

- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] 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
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.6] As funções do Lambda devem ser marcadas
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Network Firewall devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots
- [RDS.17] As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.19] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster
- [RDS.20] As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de instâncias de bancos de dados
- [RDS.21] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados
- [RDS.22] Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de segurança do banco de dados
- [RDS.23] As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.28] Os clusters de bancos de dados do RDS devem ser marcados
- [RDS.29] Os snapshots de cluster de bancos de dados do RDS devem ser marcados
- [RDS.30] As instâncias de bancos de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.32] Os snapshots de banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito
- [RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito
- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público
- [Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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 notificações de assinatura de notificações eventos do Redshift devem ser marcadas
- [Redshift.13] Os snapshots de cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes de cluster do Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch

- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [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
- [S3.22] Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas

- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [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
- [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
- [SNS.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [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 do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Tailândia)

Os controles a seguir não são suportados na região Ásia-Pacífico (Tailândia).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

- [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
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [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
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys

- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.1] DataSync as tarefas devem ter o registro ativado
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] 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 acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede

- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.52] gateways EC2 de trânsito devem ser marcados
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.172] As configurações do EC2 VPC Block Public Access devem bloquear o tráfego do gateway da Internet
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados

- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar 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 sub-redes que atribuem endereços IP públicos na inicialização
- [EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados

- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.1] GuardDuty deve ser ativado

- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados

- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster

- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio

- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.31] Os grupos de segurança de 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

- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito
- [RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito
- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público
- [Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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 notificações de assinatura de notificações eventos do Redshift devem ser marcadas
- [Redshift.13] Os snapshots de cluster do Redshift devem ser marcados

- [Redshift.14] Os grupos de sub-redes de cluster do Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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

- [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 em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [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.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos

- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [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 do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Ásia-Pacífico (Tóquio)

Os controles a seguir não são suportados na região Ásia-Pacífico (Tóquio).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Canadá (Central)

Os controles a seguir não são suportados na região do Canadá (Central).

- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados

- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Oeste do Canadá (Calgary)

Os controles a seguir não são suportados na região Oeste do Canadá (Calgary).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [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
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.1] DataSync as tarefas devem ter o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] 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 acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389

- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados

- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização
- [EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados
- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [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
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado

- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados

- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados

- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado

- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.31] Os grupos de segurança de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito

- [RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito
- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.8] 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 somente na porta do cluster de origens restritas
- [Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch

- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [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 em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas

- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [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.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra

- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

China (Pequim)

Os controles a seguir não são compatíveis com a região da China (Pequim).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] 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.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [AutoScaling.10] Grupos de EC2 Auto Scaling devem ser marcados
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados

- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso

- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve 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 EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.35] interfaces EC2 de rede devem ser marcadas
- [EC2.36] os gateways EC2 do cliente devem ser marcados

- [EC2.42] tabelas de EC2 rotas devem ser marcadas
- [EC2.46] Amazon VPCs deve ser etiquetada
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes 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

- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [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
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado

- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.21] 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] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados

- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Network Firewall devem ser marcados
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.12] A autenticação do IAM deve ser configurada para clusters 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
- [RDS.16] Os clusters de banco de dados Aurora devem ser configurados para copiar tags para DB snapshots

- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.28] Os clusters de bancos de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.32] Os snapshots de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

- [S3.22] Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [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
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

China (Ningxia)

Os controles a seguir não são suportados na região da China (Ningxia).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ACM.2] 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.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [AutoScaling.10] Grupos de EC2 Auto Scaling devem ser marcados
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados

- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados

- [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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.3] Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon 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 EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.35] interfaces EC2 de rede devem ser marcadas
- [EC2.36] os gateways EC2 do cliente devem ser marcados
- [EC2.42] tabelas de EC2 rotas devem ser marcadas
- [EC2.46] Amazon VPCs deve ser etiquetada
- [EC2.50] Os gateways de EC2 VPN devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager

- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [ECR.1] Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes 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
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [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
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada

- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.21] 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] Os perfis do IAM devem ser marcados

- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Lambda.1] As funções do Lambda.1 devem proibir o acesso público
- [Lambda.2] As funções do Lambda devem usar os tempos de execução compatíveis

- [Lambda.3] 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 do Lambda devem ser marcadas
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [Neptune.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Network Firewall devem ser marcados
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [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
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.28] Os clusters de bancos de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.32] Os snapshots de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados

- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- [Transfer.2] Os servidores do Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado

- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Europa (Frankfurt)

Os controles a seguir não são suportados na região da 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas

- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Europa (Irlanda)

Os controles a seguir não são suportados na região Europa (Irlanda).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Europa (Londres)

Os controles a seguir não são suportados na região Europa (Londres).

- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados

- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

Europa (Milão)

Os controles a seguir não são compatíveis com a região da Europa (Milão).

- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [ECR.4] Os repositórios públicos do ECR devem ser marcados

- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas

- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL

- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SSM.2] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de patch de COMPATÍVEL após a instalação de um patch
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Europa (Paris)

Os controles a seguir não são compatíveis com a região da Europa (Paris).

- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados

- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra

- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Europa (Espanha)

Os controles a seguir não são suportados na região Europa (Espanha).

- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.1] Os snapshots do Amazon EBS não devem ser restauráveis publicamente
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager

- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [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
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado

- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada

- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

- [Lambda.1] As funções do Lambda.1 devem proibir o acesso público
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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.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.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] 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
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Europa (Estocolmo)

Os controles a seguir não são suportados na região da Europa (Estocolmo).

- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados

- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito

- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas

- [IVS.3] Os canais IVS devem ser marcados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Europa (Zurique)

Os controles a seguir não são suportados na região da Europa (Zurique).

- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito

- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados

- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389

- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [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
- [ELB.2] Os balanceadores de carga clássicos com SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos

- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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.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.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado

- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Israel (Tel Aviv)

Os controles a seguir não são suportados na região de Israel (Tel Aviv).

- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas

- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados

- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito

- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS

- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- [ECR.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do 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 SSL/HTTPS ouvintes devem usar um certificado fornecido pelo AWS Certificate Manager
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados

- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] 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
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.6] Os instantâneos do cluster de banco de dados Neptune devem ser criptografados em repouso
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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.4] Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.29] Os snapshots de cluster de bancos de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.8] 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.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

México (Central)

Os controles a seguir não são suportados na região do México (Central).

- [ACM.1] Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [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
- [APIGateway.1] O registro de execução do API de Gateway, WebSocket REST e execução de API deve estar ativado
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [APIGateway.3] Os estágios da API REST de Gateway devem ter o AWS X-Ray rastreamento habilitado
- [APIGateway.4] O API Gateway deve ser associado a uma ACL da web do WAF
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados

- [Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [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
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote devem ser marcadas
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudTrail.7] Verifique se o registro de acesso ao bucket do S3 está habilitado no bucket do CloudTrail S3
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] O repositório CodeBuild de origem do Bitbucket não URLs deve 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
- [CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DataSync.1] DataSync as tarefas devem ter o registro ativado
- [DataSync.2] DataSync as tarefas devem ser marcadas

- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.1] As instâncias de replicação do Database Migration Service não devem ser públicas
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.4] 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 acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] os anexos do gateway de EC2 trânsito devem ser marcados
- [EC2.34] tabelas de rotas do gateway de EC2 trânsito devem ser marcadas
- [EC2.40] Os gateways EC2 NAT devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.52] gateways EC2 de trânsito devem ser marcados
- [EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto
- [EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR
- [EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry
- [EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2

- [EC2.171] As conexões EC2 VPN devem ter o registro ativado
- [EC2.172] As configurações do EC2 VPC Block Public Access devem bloquear o tráfego do gateway da Internet
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos

- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [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.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar 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 sub-redes que atribuem endereços IP públicos na inicialização
- [EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados
- [EFS.8] Os sistemas de arquivos do EFS devem ser criptografados em repouso
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters do EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidades do EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas

- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.3] 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.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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups

- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] GuardDuty IPSets deve ser marcado
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado
- [GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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
- [IAM.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter configurações fortes
- 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 um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os fluxos do Kinesis devem ser marcados
- [Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

- [KMS.2] As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.4] Os agentes do Amazon MQ devem ser marcados
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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

- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall devem ter a proteção contra exclusão ativada
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede 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
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.18] As instâncias do RDS devem ser implantadas em uma VPC
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.26] As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.31] Os grupos de segurança de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch
- [RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch
- [RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito
- [RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito
- [RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch
- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [PCI.Redshift.1] Os clusters do Amazon Redshift devem proibir o acesso público

- [Redshift.2] As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- [Redshift.3] Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.4] Os clusters do Amazon Redshift devem ter o registro de auditoria ativado
- [Redshift.6] O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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 notificações de assinatura de notificações eventos do Redshift devem ser marcadas
- [Redshift.13] Os snapshots de cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes de cluster do Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada somente na porta do cluster de origens restritas
- [Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão

- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [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 em log os eventos de gravação ao nível do objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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
- [SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado

- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [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.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.3] EC2 As instâncias da Amazon gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [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 do Transfer Family não devem usar o protocolo FTP para conexão de endpoints

- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro em log de ACL AWS WAF da web deve estar ativado
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Oriente Médio (Bahrein)

Os controles a seguir não são suportados na região do Oriente Médio (Bahrein).

- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.10] Os armazenamentos de dados de eventos do CloudTrail Lake devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DocumentDB.6] Os clusters do Amazon DocumentDB devem ser criptografados em trânsito
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.20] Ambos os túneis VPN para uma conexão AWS Site-to-Site VPN devem estar ativos

- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys
- [ECS.17] As definições de tarefas do ECS não devem usar o modo de rede host
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ
- [FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ
- [FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos

- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [NetworkFirewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede ativada
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.41] O RDS para instâncias de banco de dados SQL Server deve ser criptografado em trânsito
- [RDS.42] O RDS para instâncias de banco de dados MariaDB deve publicar registros em Logs CloudWatch

- [RDS.44] O RDS para instâncias de banco de dados MariaDB deve ser criptografado em trânsito
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.4] Os namespaces sem servidor do Redshift devem ser criptografados com o gerenciamento do cliente AWS KMS keys
- [RedshiftServerless.5] Os namespaces do Redshift sem servidor não devem usar o nome de usuário do administrador padrão
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [RedshiftServerless.7] Os namespaces do Redshift sem servidor não devem usar o nome do banco de dados padrão
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [SageMaker.8] instâncias de SageMaker notebook devem ser executadas em plataformas compatíveis
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [Transfer.3] Os conectores Transfer Family devem ter o registro ativado
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

Oriente Médio (Emirados Árabes Unidos)

Os controles a seguir não são suportados na região do Oriente Médio (EAU).

- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [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.4] os planos de AWS Backup relatórios devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudTrail.6] Verifique se o bucket do S3 usado para armazenar CloudTrail registros não é acessível publicamente
- [CloudWatch.16] Os grupos de CloudWatch log devem ser retidos por um período de tempo especificado
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [Detective.1] Os gráficos de comportamento do Detective devem ser marcados
- [DMS.2] Os certificados do 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.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.4] EC2 As instâncias interrompidas devem ser removidas após um período de tempo especificado
- [EC2.12] A Amazon não utilizada EC2 EIPs deve ser removida
- [EC2.14] Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.51] Os endpoints EC2 do Client VPN devem ter o registro de conexão do cliente ativado
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [EC2.180] as interfaces EC2 de rede devem ter a source/destination verificação ativada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECS.1] As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário
- [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 receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas
- [ELB.18] Os ouvintes do Application and Network Load Balancer devem usar protocolos seguros para criptografar dados em trânsito
- [ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue

- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [IAM.1] As políticas do IAM não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do IAM 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 IAM 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.8] As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.18] Certifique-se de que um perfil de suporte tenha sido criado para gerenciar incidentes com AWS Support
- [IAM.19] A MFA deve estar habilitada para todos os usuários do IAM
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.22] As credenciais de usuário do IAM não utilizadas por 45 dias devem ser removidas
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess
- [Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2
- [Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados

- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [KMS.1] As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- [KMS.2] 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.7] As funções Lambda devem ter o rastreamento ativo ativado AWS X-Ray
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.4] Os clusters MSK devem ter o acesso público desativado
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [MSK.6] Os clusters MSK devem desativar o acesso não autenticado
- 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.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança de banco de dados do RDS devem ser marcados
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.18] Os clusters do Redshift devem ter implantações Multi-AZ habilitadas
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SES.1] As listas de contatos do SES devem ser marcadas

- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SQS.1] As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas do SQS devem ser marcadas
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.1] As EC2 instâncias da Amazon devem ser gerenciadas por AWS Systems Manager
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [SSM.7] Os documentos SSM devem ter a configuração de bloqueio de compartilhamento público habilitada
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

América do Sul (São Paulo)

Os controles a seguir não são suportados na região América do Sul (São Paulo).

- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [IoT.1] perfis de AWS IoT Device Defender 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
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados

- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras

AWS GovCloud (Leste dos EUA)

Os controles a seguir não são suportados na região AWS GovCloud (Leste dos EUA).

- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [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
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados
- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados

- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Cognito.2] Os pools de identidade do Cognito não devem permitir identidades não autenticadas

- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [Connect.2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [DMS.2] Os certificados do DMS devem ser marcados
- [DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] Os endpoints do DMS devem usar SSL
- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.47] Os serviços de endpoint do Amazon VPC devem ser marcados
- [EC2.52] gateways EC2 de trânsito devem ser marcados

- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas
- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [EFS.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário

- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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 OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso
- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados

- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas
- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado

- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall 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
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [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
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.31] Os grupos de segurança de 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
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [Redshift.8] 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.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público

- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada
- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório 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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SNS.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.5] Os documentos SSM devem ser marcados
- [SSM.6] A automação de SSM deve ter o registro ativado CloudWatch
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado

- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch
- [WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso
- [WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso

AWS GovCloud (Oeste dos EUA)

Os controles a seguir não são suportados na região AWS GovCloud (Oeste dos EUA).

- [ACM.2] Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [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
- [APIGateway.2] Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- [APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização
- [APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [Amplify.1] Os aplicativos Amplify devem ser marcados

- [Amplify.2] As ramificações do Amplify devem ser marcadas
- [AppConfig.1] os AWS AppConfig aplicativos devem ser marcados
- [AppConfig.2] perfis AWS AppConfig de configuração devem ser marcados
- [AppConfig.3] AWS AppConfig ambientes devem ser marcados
- [AppConfig.4] associações AWS AppConfig de extensão devem ser marcadas
- [AppFlow.1] Os AppFlow fluxos da Amazon devem ser marcados
- [AppRunner.1] Os serviços do App Runner devem ser marcados
- [AppRunner.2] Os conectores VPC do App Runner devem ser marcados
- [AppSync.1] Os caches de AWS AppSync API devem ser criptografados em repouso
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] AWS AppSync APIs GraphQL deve ser marcado
- [AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API
- [AppSync.6] Os caches de AWS AppSync API devem ser criptografados em trânsito
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento em grupo do Auto Scaling devem EC2 configurar as instâncias para exigir o Instance Metadata Service versão 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 da Amazon EC2
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Batch.1] As filas de trabalhos em lote devem ser marcadas
- [Batch.2] As políticas de agendamento em lote devem ser marcadas
- [Batch.3] Ambientes de computação em lote devem ser marcados
- [Batch.4] As propriedades dos recursos de computação em ambientes de computação gerenciados em lote 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
- [CloudFront.15] CloudFront as distribuições devem usar a política de segurança TLS recomendada
- [CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [CodeGuruProfiler.1] Os grupos de CodeGuru criação de perfil do Profiler devem ser marcados
- [CodeGuruReviewer.1] As associações do repositório do CodeGuru revisor devem ser marcadas
- [Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão
- [Connect.1] Os tipos de objetos do Amazon Connect Customer Profiles devem ser marcados
- [DataSync.2] DataSync as tarefas devem ser marcadas
- [DMS.2] Os certificados do DMS devem ser marcados
- [DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- [DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado
- [DMS.9] Os endpoints do DMS devem usar SSL

- [DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- [DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- [DocumentDB.3] 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
- [DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.3] Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito
- [EC2.21] A rede não ACLs deve permitir a entrada de 0.0.0.0/0 para a porta 22 ou a porta 3389
- [EC2.22] Grupos de EC2 segurança não utilizados da Amazon devem ser removidos
- [EC2.23] O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de anexos de VPC
- [EC2.24] Os tipos de instância EC2 paravirtual da Amazon não devem ser usados
- [EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.38] as EC2 instâncias devem ser marcadas
- [EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts
- [EC2.60] VPCs deve ser configurado com um endpoint de interface para o Systems Manager Incident Manager
- [EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2
- [EC2.173] As solicitações do EC2 Spot Fleet com parâmetros de inicialização devem habilitar a criptografia para volumes anexados do EBS
- [EC2.174] Os conjuntos de opções EC2 DHCP devem ser marcados
- [EC2.175] modelos de EC2 lançamento devem ser marcados
- [EC2.176] as listas de EC2 prefixos devem ser marcadas

- [EC2.177] sessões de espelhos EC2 de tráfego devem ser marcadas
- [EC2.178] filtros de espelhos EC2 de trânsito devem ser marcados
- [EC2.179] alvos de espelhos EC2 de tráfego devem ser marcados
- [ECR.1] 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.3] Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECS.3] As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- [ECS.4] Os contêineres ECS devem ser executados sem privilégios
- [ECS.5] Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- [ECS.8] Os segredos não devem ser passados como variáveis de ambiente do contêiner
- [ECS.9] As definições de tarefas do ECS devem ter uma configuração de registro em log
- [ECS.10] Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- [ECS.12] Os clusters do ECS devem usar Container Insights
- [EFS.3] Os pontos de acesso do EFS devem executar um diretório raiz
- [EFS.4] Os pontos de acesso do EFS devem executar uma identidade de usuário
- [EKS.2] Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELB.10] O Classic Load Balancer deve abranger várias zonas de disponibilidade
- [ELB.12] O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.13] Balanceadores de carga de aplicações, redes e gateways devem abranger 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 OSS) devem ter backups automáticos habilitados
- [ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas
- [ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado
- [ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso
- [ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores devem ter o Redis OSS AUTH 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 saúde 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
- [EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso
- [EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [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
- [FraudDetector.1] Os tipos de entidade do Amazon Fraud Detector devem ser marcados
- [FraudDetector.2] Os rótulos do Amazon Fraud Detector devem ser marcados
- [FraudDetector.3] Os resultados do Amazon Fraud Detector devem ser marcados
- [FraudDetector.4] As variáveis do Amazon Fraud Detector devem ser marcadas
- [FSx.1] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes
- [FSx.2] FSx para sistemas de arquivos Lustre, devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados

- [GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado
- [GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado
- [GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada
- [GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado
- [GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado
- [GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.9] A MFA deve estar habilitada para o usuário raiz
- [IAM.21] As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.24] Os perfis do IAM devem ser marcados
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado
- [Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada
- [Io TEvents .1] As entradas de AWS IoT Events devem ser marcadas
- [Io TEvents .2] Os modelos de detectores de eventos de AWS IoT devem ser marcados
- [Io TEvents .3] Os modelos de alarme AWS do IoT Events devem ser marcados
- [Io TSite Wise.1] Os modelos de ativos de AWS IoT devem ser SiteWise marcados
- [Io TSite Wise.2] Os painéis de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.3] Os gateways de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.4] Os portais de AWS SiteWise IoT devem ser marcados
- [Io TSite Wise.5] Projetos de AWS SiteWise IoT devem ser marcados
- [Io TTwin Maker.1] Os trabalhos de sincronização de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.2] Os espaços de trabalho de AWS IoT devem ser TwinMaker marcados
- [Io TTwin Maker.3] As cenas de AWS TwinMaker IoT devem ser marcadas
- [Io TTwin Maker.4] As entidades de AWS TwinMaker IoT devem ser marcadas
- [Io TWireless .1] Os grupos multicast AWS do IoT Wireless devem ser marcados
- [Io TWireless .2] Os perfis do serviço AWS IoT Wireless devem ser marcados
- [Io TWireless .3] As tarefas do AWS IoT FUOTA devem ser marcadas

- [IVS.1] Os pares de teclas de reprodução do IVS devem ser marcados
- [IVS.2] As configurações de gravação IVS devem ser marcadas
- [IVS.3] Os canais IVS devem ser marcados
- [Keyspaces.1] Os espaços chave do Amazon Keyspaces devem ser marcados
- [Kinesis.1] Os fluxos do Kinesis devem ser criptografados em repouso
- [KMS.5] As chaves do KMS não devem estar acessíveis ao público
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar habilitado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve estar habilitada
- [MQ.3] Os agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada
- [MQ.5] Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- [MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- [MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- [MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito
- [MSK.5] Os conectores MSK devem ter o registro ativado
- [Neptune.1] 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.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados
- [Neptune.6] Os instantâneos do cluster 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
- [Neptune.8] Os clusters de banco de dados do 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 em log do Network Firewall deve ser habilitado
- [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 pacotes fragmentados.
- [NetworkFirewall.6] O grupo de regras do Firewall de Rede sem estado não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Network Firewall 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
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [PCA.2] As autoridades de certificação de CA AWS privadas devem ser marcadas
- [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
- [RDS.24] Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.25] As instâncias de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

- [RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- [RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [RDS.45] Os clusters de banco de dados Aurora MySQL devem ter o registro de auditoria ativado
- [Redshift.7] Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.8] 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.13] Os snapshots de cluster do Redshift devem ser marcados
- [Redshift.17] Os grupos de parâmetros do cluster do Redshift devem ser marcados
- [RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC
- [RedshiftServerless.2] Conexões com grupos de trabalho sem servidor do Redshift devem ser obrigatórias para usar SSL
- [RedshiftServerless.3] Os grupos de trabalho sem servidor do Redshift devem proibir o acesso público
- [RedshiftServerless.6] Os namespaces sem servidor do Redshift devem exportar registros para Logs CloudWatch
- [Route53.1] As verificações de integridade do Route 53 devem ser marcadas
- [Route53.2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.10] Os buckets de uso geral do S3 com versionamento habilitado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos habilitadas
- [S3.12] não ACLs deve ser usado 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
- [S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada

- [S3.24] Os pontos de acesso multirregionais do S3 devem ter as configurações de bloqueio do acesso público habilitadas
- [S3.25] Os buckets de diretório S3 devem ter configurações de ciclo de vida
- [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.5] SageMaker os modelos devem ter o isolamento de rede ativado
- [SageMaker.6] as configurações da imagem SageMaker do aplicativo devem ser marcadas
- [SageMaker.7] SageMaker as imagens devem ser marcadas
- [SNS.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público
- [SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público
- [SSM.4] Os documentos SSM não devem ser públicos
- [SSM.5] Os documentos SSM devem ser marcados
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- [Transfer.4] Os contratos da Transfer Family devem ser marcados
- [Transfer.5] Os certificados Transfer Family devem ser marcados
- [Transfer.6] Os conectores Transfer Family devem ser marcados
- [Transfer.7] Os perfis do Transfer Family devem ser marcados
- [WAF.1] O registro em log AWS WAF Classic Global Web ACL deve estar ativado
- [WAF.2] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras AWS WAF Classic Regional devem ter pelo menos uma regra
- [WAF.4] A web do AWS WAF Classic Regional ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras AWS WAF Classic Regional devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras AWS WAF Classic global devem ter pelo menos uma regra
- [WAF.8] A web AWS WAF Classic global ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.10] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras
- [WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch

Criando recursos CSPM do Security Hub com CloudFormation

AWS O Security Hub CSPM se integra ao 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 CSPM 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.

CSPM e modelos do Security Hub AWS CloudFormation

Para provisionar e configurar recursos para o CSPM do Security Hub e serviços relacionados, você deve entender como os AWS CloudFormation modelos 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 CSPM do Security Hub:

- Habilitando o CSPM do Security Hub
- Designando o administrador delegado do CSPM do Security Hub para uma organização
- Especifique a forma como sua organização está configurada no Security Hub CSPM
- Habilitar um padrão de segurança
- Habilitar a agregação entre regiões
- Criar uma política de configuração central e associá-la às contas, à unidade organizacional (OUs) ou à raiz
- Criar um insight personalizado
- Criar uma regra de automação
- Personalização de parâmetros de controle

- Assinar uma integração de produtos de terceiros

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para recursos, consulte a referência do tipo de recurso CSPM do AWS Security Hub no Guia do Usuário.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

Assinando os anúncios do CSPM do Security Hub com o Amazon SNS

Esta seção fornece informações sobre a assinatura dos anúncios do CSPM do AWS Security Hub com o Amazon Simple Notification Service (Amazon SNS) para receber notificações sobre o CSPM do 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 CSPM do Security Hub.
- `UPCOMING_STANDARDS_CONTROLS`— Os controles ou padrões CSPM especificados 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 CSPM está disponível em um novo. Região da AWS
- `NEW_STANDARDS_CONTROLS`— Novos controles ou padrões CSPM do Security Hub foram adicionados.
- `UPDATED_STANDARDS_CONTROLS`— Os controles ou padrões CSPM existentes do Security Hub foram atualizados.

- `RETIRED_STANDARDS_CONTROLS`— Os controles ou padrões CSPM existentes do Security Hub foram retirados.
- `UPDATED_ASFF`— A sintaxe, os campos ou os valores do AWS Security Finding Format (ASFF) foram atualizados.
- `NEW_INTEGRATION`— Novas integrações com outros AWS serviços ou produtos de terceiros estão disponíveis.
- `NEW_FEATURE`— Novos recursos do Security Hub CSPM estão disponíveis.
- `UPDATED_FEATURE`— Os recursos existentes do CSPM do Security Hub foram atualizados.

As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS. Você pode assinar os anúncios do CSPM do Security Hub em tudo em que o CSPM do Security Regiões da AWS 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 CSPM do Security Hub envia anúncios do Amazon SNS sobre atualizações do serviço CSPM do Security Hub para qualquer assinante. Conta da AWS Para receber notificações sobre as descobertas do CSPM do Security Hub, consulte. Analisando os detalhes e o histórico da descoberta no Security Hub CSPM

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 Como inscrever uma fila em um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Queue Service.

Você também pode usar uma AWS Lambda função para invocar eventos ao receber notificações. Para obter mais informações, incluindo um exemplo de código de função, consulte Tutorial: Usando AWS Lambda com o Amazon Simple Notification Service no Guia do AWS Lambda desenvolvedor.

Os tópicos do Amazon SNS ARNs 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 (Norte da Virgínia)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
Oeste dos EUA (Norte da Califórnia)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
Oeste dos EUA (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
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`

Região da AWS	Tópico ARN do Amazon SNS
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`
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`
Europa (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
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`
Europe (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
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 (Bahrein)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
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 CSPM do Security Hub.

Para obter informações sobre o custo da assinatura dos anúncios do CSPM do Security Hub, consulte os preços do Amazon SNS.

Assinando os anúncios do CSPM do Security Hub (console)

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/ v3/home.
2. Na lista Região, escolha a região na qual você deseja assinar os anúncios do CSPM do Security Hub. Este exemplo usa a região `us-west-2`.
3. No painel de navegação, escolha Subscriptions (Assinaturas) e, depois, 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, escolha como você deseja receber os anúncios do CSPM 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 CSPM 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 CSPM 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 CSPM do Security Hub para novos controles (protocolo de e-mail)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM 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 CSPM to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

Exemplo: anúncio do CSPM do Security Hub para novos controles (protocolo Email-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 CSPM 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 CSPM 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"
}
```

Desativando o CSPM do Security Hub

Você pode desativar o CSPM do AWS Security Hub usando o console CSPM do Security Hub ou a API do Security Hub. Se você desabilitar o CSPM do Security Hub, poderá ativá-lo novamente mais tarde.

Se sua organização usa a configuração central, o administrador delegado do CSPM do Security Hub pode criar políticas de configuração que desabilitem o CSPM do Security Hub para contas e unidades organizacionais específicas () e OUs mantenham o CSPM do Security Hub ativado para outras pessoas. As políticas de configuração afetam a região de origem e todas as regiões vinculadas. Para obter mais informações, consulte Entendendo a configuração central no Security Hub CSPM.

Se você desabilitar o CSPM do Security Hub para uma conta, ocorrerá o seguinte:

- Todos os padrões e controles do Security Hub CSPM estão desativados para a conta.
- O CSPM do Security Hub interrompe a geração, a atualização e a ingestão de descobertas para a conta.
- Depois de 30 dias, o Security Hub CSPM exclui permanentemente todas as descobertas arquivadas existentes da conta. As descobertas não podem ser recuperadas usando o Security Hub CSPM.
- Após 90 dias, o Security Hub CSPM exclui permanentemente todas as descobertas ativas existentes da conta. As descobertas não podem ser recuperadas usando o Security Hub CSPM.
- Depois de 90 dias, o Security Hub CSPM exclui permanentemente todos os insights existentes e as configurações de CSPM do Security Hub para a conta. Os dados e as configurações não podem ser recuperados.

Para reter as descobertas existentes, você pode exportá-las para um bucket do S3 antes de desativar o CSPM do Security Hub. Você pode fazer isso usando uma ação personalizada com uma

EventBridge regra da Amazon. Para obter mais informações, consulte Usando EventBridge para resposta e remediação automatizadas.

Se você reativar o CSPM do Security Hub dentro de 90 dias após desativá-lo para uma conta, você recuperará o acesso às descobertas ativas existentes, bem como aos insights e às configurações do CSPM do Security Hub para a conta. Se você reativar o CSPM do Security Hub em 30 dias, também recuperará o acesso às descobertas arquivadas existentes da conta. No entanto, as descobertas existentes podem ser imprecisas porque refletirão o estado do seu AWS ambiente quando você desativou o CSPM do Security Hub. Além disso, à medida que você reativa padrões e controles individuais, o CSPM do Security Hub pode inicialmente gerar descobertas duplicadas para AWS recursos específicos, dependendo dos padrões e controles que você habilitar. Por esses motivos, recomendamos que você faça o seguinte:

- Altere o status do fluxo de trabalho de todas as descobertas existentes para `RESOLVED` antes de desativar o CSPM do Security Hub. Para obter mais informações, consulte Definir o status do fluxo de trabalho das descobertas.
- Desative todos os padrões pelo menos seis dias antes de desativar o CSPM do Security Hub. Em seguida, o Security Hub CSPM arquiva todas as descobertas existentes com base no melhor esforço, normalmente dentro de três a cinco dias. Para obter mais informações, consulte Desabilitar um padrão.

Você não pode desativar o CSPM do Security Hub nos seguintes casos:

- Sua conta é a conta delegada do administrador CSPM do Security Hub para uma organização. Se você usar a configuração central, não poderá associar uma política de configuração que desabilite o CSPM do Security Hub para a conta do administrador delegado. A associação pode ser bem-sucedida para outras contas, mas o Security Hub CSPM não aplica a política à conta do administrador delegado.
- Sua conta é uma conta de administrador do CSPM do Security Hub por convite, e você tem contas de membros. Antes de desativar o CSPM do Security Hub, você deve desassociar todas as suas contas de membros. Para saber como, consulte the section called “Desassociar contas de membro”.

Antes que o proprietário de uma conta membro possa desativar o CSPM do Security Hub, a conta deve se desassociar de sua conta de administrador. Para uma conta de organização, somente a conta de administrador pode desassociar uma conta de membro. Para obter mais informações, consulte the section called “Desassociação de contas-membro da organização”. Para uma conta

convidada manualmente, a conta do administrador ou a conta do membro podem desassociar a conta. Para ter mais informações, consulte the section called “Desassociar contas de membro” ou the section called “Desassociar de uma conta de administrador”. A dissociação não é necessária se você usar a configuração central porque o administrador do CSPM do Security Hub pode criar uma política que desabilita o CSPM do Security Hub para contas de membros específicas.

Quando você desativa o CSPM do Security Hub para uma conta, ela é desativada somente na atual. Região da AWS No entanto, se você usar a configuração central para desativar o CSPM do Security Hub para contas específicas, ela será desativada na região de origem e em todas as regiões vinculadas.

Para desativar o CSPM do Security Hub, escolha seu método preferido e siga as etapas.

Security Hub CSPM console

Siga estas etapas para desativar o CSPM do Security Hub usando o console.

Para desativar o CSPM do Security Hub

1. Abra o console CSPM do AWS Security Hub em. https://console.aws.amazon.com/securityhub/
2. No painel de navegação, em Configurações, selecione Geral.
3. Na seção Desativar CSPM do Security Hub, escolha Desativar CSPM do Security Hub.
4. Quando solicitada a confirmação, escolha Desativar CSPM do Security Hub.

Security Hub API

Para desativar o CSPM do Security Hub programaticamente, use a DisableSecurityHuboperação da API do Security Hub AWS . Ou, se você estiver usando o AWS CLI, execute o disable-security-hubcomando. Por exemplo, o comando a seguir desativa o CSPM do Security Hub no atual: Região da AWS

```
$ aws securityhub disable-security-hub
```

Segurança em AWS Security Hub

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

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Security Hub, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda 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. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Security Hub.

Tópicos

Proteção de dados em AWS Security Hub

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Security Hub. Conforme descrito neste modelo, AWS é responsável por proteger a

infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o 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 Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Security Hub ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse 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 o 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 a solicitar as permissões corretas ao administrador. Se não for possível acessar um recurso no Security Hub, consulte Solução de problemas AWS Security Hub de identidade e acesso.

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. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Security Hub, consulte Como o 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 AWS Security Hub.

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login 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 designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer 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 e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar 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 IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM 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. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil 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, é possível 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 por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o 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 perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas 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 especificado 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 recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

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

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas 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 Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- 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 recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

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

Como o Security Hub funciona com o IAM

Antes de usar o AWS Identity and Access Management (IAM) para gerenciar o acesso AWS Security Hub, saiba quais recursos do IAM estão disponíveis para uso com o Security Hub.

Recursos do IAM que você pode usar com AWS Security Hub

Recurso do IAM	Conformidade com o Security Hub
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos 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

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 do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

O Security Hub é compatível com políticas baseadas em identidade. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade para o AWS Security Hub.

Políticas baseadas em recursos para o Security Hub

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços 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 especificado 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 recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM 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 de políticas para o Security Hub

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

As ações de políticas do Security Hub usam o seguinte prefixo antes da ação:

```
securityhub:
```

Por exemplo, para conceder a um usuário permissão para habilitar o Security Hub, que é uma ação que corresponde à operação de API `EnableSecurityHub` do Security Hub, inclua a ação `securityhub:EnableSecurityHub` 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 declaração, separe-as com vírgulas. Por exemplo:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Também é possível 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 operação `DescribeStandardsControl` para ter acesso a `BatchGetSecurityControls`, `BatchGetStandardsControlAssociations` e `ListStandardsControlAssociations`.

O usuário deve ter acesso à operação `UpdateStandardsControls` para ter acesso a `BatchUpdateStandardsControlAssociations` e `UpdateSecurityControl`.

Para obter uma lista das ações do Security Hub, consulte Ações definidas pelo AWS Security Hub na Referência de autorização do serviço. Para obter exemplos de políticas que especificam ações do Security Hub, consulte Exemplos de políticas baseadas em identidade para o AWS Security Hub.

Recursos de política para o Security Hub

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

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

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

O Security Hub define os seguintes tipos de recursos:

- Hub
- Produto
- Agregador de descobertas, também conhecido como agregador entre regiões
- Regra de automação
- Política de configuração

Você pode especificar esses tipos de recursos nas políticas usando ARNs.

Para obter uma lista dos tipos de recursos do Security Hub e a sintaxe de ARNs para cada um, consulte Tipos de recursos definidos pelo AWS Security Hub na Referência de autorização do serviço. Para saber quais ações você pode especificar para cada tipo de recurso, consulte Ações definidas pelo AWS Security Hub na Referência de autorização do serviço. Para obter exemplos de políticas que especificam os recursos, consulte Exemplos de políticas baseadas em identidade para o AWS Security Hub.

Chaves de condição de política do Security Hub

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

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

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

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para obter uma lista de chaves de condição do Security Hub, consulte Chaves de condição do AWS Security Hub na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo AWS Security Hub. Para obter exemplos de políticas que usam chaves de condição, consulte Exemplos de políticas baseadas em identidade para o AWS Security Hub.

Listas de controle de acesso (ACLs) no Security Hub

Suportes ACLs: Não

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

O Security Hub não oferece suporte ACLs, o que significa que você não pode anexar uma ACL a um recurso do Security Hub.

Controle de acesso por atributo (ABAC) com o Security Hub

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as 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. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

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

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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 a esses recursos fornecendo informações de tag no elemento `Condition` de uma política.

Para obter mais informações sobre os recursos de marcação do Security Hub, consulte Marcar recursos do 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 AWS Security Hub.

Usar credenciais de segurança temporárias com o Security Hub

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "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 funções, consulte Alternar para um perfil do IAM (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 obter 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 é compatível com o uso de credenciais temporárias.

Sessões de acesso direto para o Security Hub

Compatibilidade com o recurso de 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 Sessões de acesso direto.

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 um perfil vinculado ao serviço para executar ações para você. Para obter detalhes sobre esse perfil, consulte Funções vinculadas a serviços para AWS Security Hub.

Perfis de serviço do Security Hub

O Security Hub não assume nem usa perfis de serviço. Para realizar ações para você, o Security Hub usa um perfil vinculado ao serviço. Para obter detalhes sobre esse perfil, consulte Funções vinculadas a serviços para AWS Security Hub.

> **Warning**
>
> Alterar as permissões em um perfil de serviço pode criar problemas operacionais no uso do Security Hub. Edite os perfis de serviço somente quando o Security Hub orientar você a fazer isso.

Perfis vinculados ao serviço do Security Hub

Compatibilidade com perfis vinculados a serviços: sim

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

O Security Hub usa um perfil vinculado ao serviço para realizar ações para você. Para obter detalhes sobre esse perfil, consulte Funções vinculadas a serviços para AWS Security Hub.

Exemplos de políticas baseadas em identidade para o AWS Security Hub

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Security Hub. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. 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 política

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 sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se

elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

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

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do Security Hub

Para acessar o AWS Security Hub console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Security Hub em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à 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 Adição de permissões a um usuário no Guia do usuário do IAM.

JSON

```
{
```

```
    "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 criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: permitir que os usuários criem e gerenciem uma política de configuração

Este exemplo mostra como você pode criar uma política do IAM que permite que um usuário crie, visualize, atualize e exclua políticas de configuração. Este exemplo de política também permite que o usuário inicie, interrompa e visualize as associações da política. Para que essa política do IAM funcione, o usuário deve ser o administrador delegado do Security Hub para uma organização.

JSON

```
{
    "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 revisem descobertas

Este exemplo mostra como você poderia criar uma política do IAM que permita que um usuário visualize as descobertas do Security Hub.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: permitir que os usuários criem e gerenciem regras de automação

Esse exemplo mostra como você pode criar uma política do IAM que permite que um usuário crie, visualize, atualize e exclua regras de automação do Security. Para que essa política do IAM funcione, o usuário deve ser o administrador delegado do Security Hub. Para limitar as permissões, por exemplo, para permitir que um usuário apenas visualize as regras de automação, você pode remover as permissões de criar, atualizar e excluir.

JSON

```
{
    "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 a serviços para AWS Security Hub

AWS Security Hub usa uma função vinculada ao serviço AWS Identity and Access Management (IAM) chamada. `AWSServiceRoleForSecurityHub` Um perfil vinculado ao serviço é um perfil do IAM que é vinculado 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 de sua função vinculada ao serviço e, a menos que seja definido de outra forma, 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 revisar os detalhes da função vinculada ao serviço, você pode usar o console do Security Hub. No painel de navegação, escolha Geral em Configurações. Em seguida, na seção Permissões do serviço, escolha Exibir permissões do serviço.

Você pode excluir a função vinculada ao serviço do Security Hub somente depois de desativar o Security Hub em todas as regiões em que ela está ativada. Isso protege seus recursos do Security Hub, porque não é possível remover inadvertidamente as permissões para acessá-los.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com o IAM no Guia do usuário do IAM e localize os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para revisar a documentação da função vinculada a esse serviço.

Tópicos

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 AWS Security Hub para acessar seus recursos. Essa função vinculada ao serviço permite que o Security Hub execute tarefas como receber descobertas de outras pessoas Serviços da AWS e configurar a AWS Config infraestrutura necessária para executar verificações de segurança dos controles. O perfil vinculado ao serviço `AWSServiceRoleForSecurityHub` confia no serviço `securityhub.amazonaws.com` para presumir o perfil.

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 política a seguir à identidade do IAM.

JSON

```
{
    "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 `AWSServiceRoleForSecurityHub` vinculada ao serviço é criada automaticamente quando você ativa o Security Hub pela primeira vez ou ativa o Security Hub em uma região onde não a habilitou anteriormente. Você também pode criar a função `AWSServiceRoleForSecurityHub` vinculada ao serviço manualmente usando o console do IAM, a CLI do IAM ou a API do IAM. Para mais informações sobre a criação da função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

> **Important**
>
> A função vinculada ao serviço criada para uma conta de administrador do Security Hub não se aplica às contas associadas de membros do Security Hub.

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 um perfil vinculado ao 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 uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não terá uma entidade não utilizada e não monitorada ativamente ou mantida.

Quando você desativa o Security Hub, o Security Hub não exclui automaticamente a função `AWSServiceRoleForSecurityHub` vinculada ao serviço para você. Se você habilitar o Security Hub novamente, o serviço poderá começar a usar a função vinculada ao serviço existente novamente. Se você não precisar mais usar o Security Hub, poderá excluir manualmente a função vinculada ao serviço.

> **Important**
>
> Antes de excluir a função `AWSServiceRoleForSecurityHub` vinculada ao serviço, você deve primeiro desativar o Security Hub em todas as regiões em que ela está ativada. Para obter mais informações, consulte Desativando o CSPM do Security Hub. Se o Security Hub não estiver desabilitado quando você tentar excluir a função vinculada ao serviço, haverá falha na exclusão.

Para excluir a função `AWSServiceRoleForSecurityHub` vinculada ao serviço, você pode usar o console do IAM, a CLI do IAM ou a API do IAM. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

AWS políticas gerenciadas para o 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 estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que

atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSSecurityHubFullAccess

É possível anexar a política `AWSSecurityHubFullAccess` às identidades do IAM.

Essa política concede permissões administrativas que permitem ao principal acesso total a todas as ações do CSPM do Security Hub. Essa política deve ser anexada a um diretor antes que ele habilite o CSPM do Security Hub manualmente para sua conta. Por exemplo, entidades principais com essas permissões podem visualizar e atualizar o status das descobertas. Eles também podem configurar insights personalizados, ativar integrações e ativar e desativar padrões e controles. As entidades principais de uma conta de administrador também podem gerenciar contas de membro.

Detalhes de permissões

Esta política inclui as seguintes permissões:

- `securityhub`— Permite que os diretores tenham acesso total a todas as ações do CSPM do Security Hub.
- `guardduty`— Permite que os diretores obtenham informações sobre o status da conta na Amazon GuardDuty.
- `iam`— Permite que os diretores criem uma função vinculada a serviços para o Security Hub CSPM e o Security Hub.
- `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.

Para revisar as permissões dessa política, consulte o Guia AWSSecurityHubFullAccessde referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSSecurityHubReadOnlyAccess

É possível anexar a política `AWSSecurityHubReadOnlyAccess` às identidades do IAM.

Essa política concede permissões somente para leitura que permitem que os usuários visualizem informações no CSPM do Security Hub. Os diretores com essa política anexada não podem fazer

nenhuma atualização no CSPM do 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 de 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`.

Para revisar as permissões dessa política, consulte o Guia AWSSecurityHubReadOnlyAccessde referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSSecurityHubOrganizationsAccess

É possível anexar a política `AWSSecurityHubOrganizationsAccess` às identidades do IAM.

Essa política concede permissões administrativas para habilitar e gerenciar o Security Hub e o Security Hub CSPM para uma organização em. AWS Organizations As permissões para essa política permitem que a conta de gerenciamento da organização designe a conta de administrador delegado para o Security Hub e o Security Hub CSPM. Eles também permitem que a conta do administrador delegado habilite as contas da organização como contas de membros.

Essa política só fornece permissões para AWS Organizations. A conta de gerenciamento da organização e a conta de administrador delegado também exigem permissões para ações associadas. Essas permissões podem ser concedidas usando a política gerenciada do `AWSSecurityHubFullAccess`.

Detalhes de 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:ListParents`— Lista as unidades raiz ou organizacionais (OUs) que servem como mãe imediata da OU ou conta secundária especificada.
- `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:ListPolicies`— Recupera a lista de todas as políticas em uma organização de um tipo especificado.
- `organizations:ListPoliciesForTarget`— Lista as políticas que estão diretamente vinculadas à raiz, unidade organizacional (OU) ou conta de destino especificada.
- `organizations:ListTargetsForPolicy`— Lista todas as raízes, unidades organizacionais (OUs) e contas às quais a política especificada está anexada.
- `organizations:EnableAWSServiceAccess`— Permite que os diretores possibilitem a integração com Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permite que os diretores designem a conta de administrador delegada.
- `organizations:DeregisterDelegatedAdministrator`— Permite que os diretores removam a conta de administrador delegado.
- `organizations:DescribePolicy`— Recupera informações sobre uma política.
- `organizations:DescribeEffectivePolicy`— Retorna o conteúdo da política efetiva para o tipo de política e conta especificados.
- `organizations:CreatePolicy`— Cria uma política de um tipo específico que você pode anexar a uma raiz, a uma unidade organizacional (OU) ou a uma AWS conta individual.

- `organizations:UpdatePolicy`— Atualiza uma política existente com um novo nome, descrição ou conteúdo.
- `organizations:DeletePolicy`— Exclui a política especificada da sua organização.
- `organizations:AttachPolicy`— Anexa uma política a uma raiz, a uma unidade organizacional (OU) ou a uma conta individual.
- `organizations:DetachPolicy`— Separa uma política de uma raiz, unidade organizacional (OU) ou conta de destino.
- `organizations:EnablePolicyType`— Habilita um tipo de política em uma raiz.
- `organizations:DisablePolicyType`— Desativa um tipo de política organizacional em uma raiz.
- `organizations:TagResource`— Adiciona uma ou mais tags a um recurso especificado.
- `organizations:UntagResource`— Remove todas as tags com as chaves especificadas de um recurso especificado.
- `organizations:ListTagsForResource`— Lista as tags anexadas a um recurso especificado.

Para revisar as permissões dessa política, consulte o Guia AWSSecurityHubOrganizationsAccessde referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSSecurityHubServiceRolePolicy

Não é possível anexar a `AWSSecurityHubServiceRolePolicy` às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o CSPM do Security Hub execute ações em seu nome. Para obter mais informações, consulte the section called “Perfis vinculados a serviço”.

Essa política concede permissões administrativas que permitem que a função vinculada ao serviço execute tarefas como executar verificações de segurança para controles CSPM do Security Hub.

Detalhes de permissões

Esta política inclui as seguintes permissões:

- `cloudtrail`— Recupere informações sobre CloudTrail trilhas.
- `cloudwatch`— Recupere os CloudWatch alarmes atuais.
- `logs`— Recupere filtros métricos para 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`— Recupere e gere relatórios de credenciais para contas.
- `organizations` – Recuperar as informações da conta e da unidade organizacional (OU) de uma organização.
- `securityhub`— recupere informações sobre como o serviço, os padrões e os controles do Security Hub CSPM estão configurados.
- `tag` – Recuperar informações sobre tags de recursos.

Para revisar as permissões dessa política, consulte o Guia AWSSecurityHubServiceRolePolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSSecurityHubV2ServiceRolePolicy

> **Note**
>
> O Security Hub está em versão prévia e está sujeito a alterações.

Essa política permite que o Security Hub gerencie AWS Config regras e recursos do Security Hub para sua organização e em seu nome. Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível anexar essa política às suas identidades do IAM. Para obter mais informações, consulte the section called “Perfis vinculados a serviço”.

Detalhes de permissões

Esta política inclui as seguintes permissões:

- `config`— Gerencie gravadores de configuração vinculados a serviços para recursos do Security Hub.
- `iam`— Crie a função vinculada ao serviço para. AWS Config
- `organizations` – Recuperar as informações da conta e da unidade organizacional (OU) de uma organização.
- `securityhub`— Gerenciar a configuração do Security Hub.
- `tag` – Recuperar informações sobre tags de recursos.

Para revisar as permissões dessa política, consulte o Guia AWSSecurityHubV2ServiceRolePolicyde referência de políticas AWS gerenciadas.

Atualizações do Security Hub para políticas AWS gerenciadas

A tabela a seguir fornece detalhes sobre as atualizações das políticas AWS gerenciadas do AWS Security Hub e do Security Hub CSPM desde que esse serviço começou a rastrear essas alterações. Para alertas automáticos sobre atualizações das políticas, assine o feed RSS na página de histórico de documentos do Security Hub.

Alteração	Descrição	Data
AWSSecurityHubOrganizationsAccess: atualizar para uma política existente	O Security Hub adicionou novas permissões à política. As permissões permitem que o gerenciamento da organização habilite e gerencie o Security Hub e o CSPM do Security Hub para uma organização.	17 de junho de 2025
AWSSecurityHubFullAccess: atualização para uma política existente	O CSPM do Security Hub adicionou novas permissões que permitem que os diretores criem uma função vinculada ao serviço para o Security Hub.	17 de junho de 2025
AWSSecurityHubV2ServiceRolePolicy — Nova política	O Security Hub adicionou uma nova política para permitir que o Security Hub gerencie AWS Config regras e recursos do Security Hub para a organização de um cliente e em nome do cliente. O Security Hub	17 de junho de 2025

Alteração	Descrição	Data
	está em versão prévia e está sujeito a alterações.	
AWSSecurityHubFullAccess— Atualização de uma política existente	O Security Hub CSPM 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 CSPM atualizou essa política gerenciada adicionando um `Sid` campo.	22 de fevereiro de 2024
AWSSecurityHubFullAccess— Atualização de uma política existente	O Security Hub CSPM 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 CSPM atualizou a política para conceder permissões adicionais para permitir acesso somente de leitura à funcionalidade do administrador delegado. AWS Organizations Isso inclui detalhes como raiz, unidades organizacionais (OUs), contas, estrutura organizacional e acesso ao serviço.	16 de novembro de 2023

Alteração	Descrição	Data
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub CSPM adicionou as `UpdateSecurityControl` permissões `sBatchGetSecurityControls` ,`DisassociateFromAdministratorAccount` , 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 CSPM adicionou a `tag:GetResources` permissão para ler tags de recursos relacionadas às descobertas.	7 de novembro de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub CSPM adicionou a `BatchGetStandardsControlAssociations` permissão para obter informações sobre o status de ativação de um controle em um padrão.	27 de setembro de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub CSPM adicionou novas permissões para obter AWS Organizations dados, ler e atualizar as configurações do Security Hub CSPM, incluindo padrões e controles.	20 de setembro de 2023

Alteração	Descrição	Data
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O CSPM do Security Hub moveu a `config:DescribeConfigRuleEvaluationStatus` permissão 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 CSPM do Security Hub moveu a `config:PutEvaluations` permissão 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 CSPM adicionou uma nova permissão para permitir que a função vinculada ao serviço forneça resultados de avaliação a. AWS Config	29 de junho de 2021
AWSSecurityHubServiceRolePolicy— Adicionado à lista de políticas gerenciadas	Foram adicionadas informações sobre a política gerenciada AWSSecurityHubServiceRolePolicy, que é usada pela função vinculada ao serviço CSPM do Security Hub.	11 de junho de 2021

Alteração	Descrição	Data
AWSSecurityHubOrganizationsAccess— Nova política	O Security Hub CSPM adicionou uma nova política que concede as permissões necessárias para a integração do Security Hub CSPM com o Organizations.	15 de março de 2021
O Security Hub CSPM começou a rastrear as alterações	O Security Hub CSPM começou a monitorar as mudanças em suas políticas AWS gerenciadas.	15 de março de 2021

Solução de problemas AWS Security Hub de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Security Hub um 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 pessoas fora da minha acessem meus Conta da AWS recursos do Security Hub

Não tenho autorização para executar uma ação no Security Hub

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário `mateojackson` tenta usar o console para ver detalhes sobre um*`widget`*, mas não tem `securityhub:`*`GetWidget`* 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 uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro 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 precisar de ajuda, entre em contato com seu AWS administrador. 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 pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identidade da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de ferramentas AWS SDKs e ferramentas.
IAM	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando

Qual usuário precisa de acesso programático?	Para	Por
		credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para 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 em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em 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 Criando 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 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 Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Security Hub

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

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

Validação de conformidade AWS Security Hub

Para saber se um AWS service (Serviço da AWS) está no escopo de programas específicos de conformidade, consulte Serviços da AWS no escopo por programa de conformidade Serviços da AWS de conformidade e selecione o programa de conformidade do seu interesse. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. AWS A fornece os seguintes recursos para ajudar com a conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos os Serviços da AWS estão qualificados pela HIPAA.
- AWS Recursos de de conformidade da: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- AWS Guias de conformidade do cliente da: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO).
- Avaliar recursos com regras no Guia do AWS Config desenvolvedor da: o AWS Config serviço avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty - Este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados, monitorando seu ambiente em busca de atividades suspeitas e mal-intencionadas. GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu AWS uso da para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no AWS Security Hub

A infraestrutura AWS global é construída em torno Regiões da AWS de 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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

Segurança da infraestrutura em AWS Security Hub

Como serviço gerenciado, AWS Security Hub é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Security Hub pela rede. Os clientes devem oferecer compatibilidade com:

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

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

AWS Security Hub e endpoints VPC 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 o Security Hub APIs sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com o Security Hub. APIs 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 obter mais informações, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia da Amazon Virtual Private Cloud.

Considerações sobre os endpoints da VPC do Security Hub

Antes de configurar um VPC endpoint de interface para o Security Hub, revise os pré-requisitos e outras informações no Guia da Amazon Virtual Private Cloud.

O Security Hub é compatível com chamadas para todas as ações de API da sua VPC.

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 a (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Criar um VPC endpoint no Guia da Amazon Virtual Private Cloud.

Crie um endpoint da VPC para o Security Hub usando o seguinte nome de serviço:

`com.amazonaws.`*`region`*`.securityhub`

Onde *`region`* está o código da região aplicável Região da AWS.

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 a região Leste dos EUA (Norte da Virgínia).

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 realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para obter mais informações, consulte Controle o acesso aos endpoints da VPC usando políticas de endpoint no Guia da Amazon Virtual Private Cloud.

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 de VPC, consulte Compartilhe suas sub-redes de VPC com outras contas no Guia da Amazon Virtual Private Cloud.

Registrando chamadas da API do Security Hub com CloudTrail

AWS O Security Hub CSPM é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Security Hub CSPM. CloudTrail captura chamadas de API para o CSPM do Security Hub como eventos. As chamadas capturadas incluem chamadas do console CSPM do Security Hub e chamadas de código para as operações da API CSPM do Security Hub. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Security Hub CSPM. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações CloudTrail coletadas, você pode determinar a solicitação que foi feita ao Security Hub CSPM, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

Informações do CSPM do Security Hub em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade de evento suportada ocorre no CSPM do Security Hub, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua conta, incluindo eventos do Security Hub CSPM, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões do AWS . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail

- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

O Security Hub CSPM suporta o registro de todas as ações da API CSPM do Security Hub como eventos em registros. CloudTrail Para ver uma lista das operações CSPM do Security Hub, consulte a Referência da API CSPM do Security Hub.

Quando a atividade das ações a seguir é registrada CloudTrail, o valor de `responseElements` é definido como. `null` Isso garante que informações confidenciais não sejam incluídas nos CloudTrail registros.

- `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 o seguinte:

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

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Exemplo: entradas do arquivo de log CSPM do Security Hub

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra 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 Visualizando insights no Security Hub CSPM.

```
{
    "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 Security Hub

Uma tag é um rótulo opcional que você pode definir e atribuir aos AWS recursos, incluindo certos tipos de recursos CSPM do AWS Security Hub. As tags podem ajudá-lo 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.

Você pode adicionar tags aos seguintes tipos de recursos CSPM do Security Hub:

- Regras de automação
- Políticas de configuração
- Recurso do `Hub`

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 uma etiqueta 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 OUs e.

Ao definir e atribuir tags aos recursos CSPM do AWS Security Hub, lembre-se do seguinte:

- Cada recurso pode ter um máximo de 50 tags.
- Em todos os recursos, cada chave de etiqueta deve ser exclusiva e pode ter apenas um valor de tag.
- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Como práticas recomendadas, recomendamos definir uma estratégia para letras maiúsculas em tags e implementá-las de forma consistente em todos os seus 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 `aws:` prefixo é reservado para uso por AWS. Você não pode usá-lo em nenhuma chave ou valor de tag que você definir. Além disso, você não pode alterar ou remover chaves de tag ou valores 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 você Conta da AWS e somente no local Região da AWS em que você as atribui.
- Se você atribuir tags a um recurso usando o CSPM do Security Hub, as tags serão aplicadas somente ao recurso armazenado diretamente no CSPM do Security Hub no aplicável. Região da AWS Eles não são aplicados a nenhum recurso de suporte associado que o Security Hub CSPM crie, use ou mantenha 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 CSPM do Security Hub para a região especificada. Elas não são aplicadas aos seus buckets do S3. Para também atribuir tags a um recurso associado, você pode usar AWS Resource Groups ou AWS service (Serviço da AWS) aquele que armazena o recurso, por exemplo, Amazon S3 para um bucket do S3. A atribuição de tags aos recursos associados pode ajudá-lo a identificar recursos de suporte para seus recursos de CSPM 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. As tags podem ser acessadas por muitos Serviços da AWS, inclusive Gerenciamento de Faturamento e Custos da AWS. As tags não devem ser usadas para dados confidenciais.

Para adicionar e gerenciar tags para recursos CSPM do Security Hub, você pode usar o console CSPM do Security Hub, a API CSPM do Security Hub ou a API Tagging. AWS Resource Groups Com o Security Hub CSPM, você pode adicionar tags a um recurso ao criar o recurso. Você também pode adicionar e gerenciar tags para recursos individuais existentes. Com o Resource Groups, você pode adicionar e gerenciar tags em massa para vários recursos existentes, abrangendo vários Serviços da AWS, incluindo o Security Hub CSPM.

Para obter dicas adicionais de marcação e melhores práticas, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

Utilizar tags nas políticas do IAM

Depois de começar a atribuir tags aos recursos, defina permissões de recurso baseadas em tags em políticas do AWS Identity and Access Management (IAM). Ao usar tags dessa forma, você pode implementar um controle granular de quais usuários e funções em sua empresa Conta da AWS têm permissão para criar e marcar recursos e quais usuários e funções têm permissão para adicionar, editar e remover tags de forma mais geral. Para controlar o acesso com base em tags, você pode usar chaves de condição relacionadas à tag no elemento Condição das políticas do IAM.

Por exemplo, você pode criar uma política do IAM que permita que um usuário tenha acesso total a todos os recursos CSPM do AWS Security Hub, se a `Owner` tag do recurso especificar seu nome de usuário:

JSON

```
{
    "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 você pode 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 Controle do acesso a AWS recursos usando tags no Guia do usuário do IAM.

Adicionar tags aos recursos CSPM do Security Hub

Uma tag é um rótulo que você pode definir e atribuir aos AWS recursos, incluindo certos tipos de recursos CSPM do AWS Security Hub. Ao usar tags, você pode identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, propriedade, ambiente ou outros critérios. Por exemplo, você pode usar tags para aplicar políticas, alocar custos, distinguir entre versões de recursos ou identificar recursos que suportam determinados requisitos de conformidade ou fluxos de trabalho.

Você pode adicionar tags aos seguintes tipos de recursos CSPM do Security Hub:

- Regras de automação
- Políticas de configuração
- Recurso do Hub

Um recurso pode ter até 50 tags. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Uma chave de tag é uma etiqueta 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. Para obter mais informações sobre os requisitos e as opções de marcação, consulte Fundamentos das tags.

Para adicionar tags a um recurso CSPM do Security Hub, você pode usar o console CSPM do Security Hub ou a API CSPM do Security Hub. Porém, o console não é compatível com a adição de tags ao recurso Hub.

Depois de adicionar tags, você pode editar a tag e alterar a chave ou o valor da tag.

Para adicionar ou editar tags para vários recursos CSPM do Security Hub ao mesmo tempo, use as operações de marcação da AWS Resource Groups API de marcação.

> **Important**
>
> Adicionar tags a um recurso pode afetar o acesso a ele. Antes de adicionar uma tag a um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar tags para controlar o acesso aos recursos.

Console

Para adicionar tags a um recurso CSPM do Security Hub (console)

Quando você cria uma regra de automação ou uma política de configuração, o console CSPM 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 CSPM API

Para adicionar tags a um recurso CSPM (API) do Security Hub

Para criar um recurso e adicionar uma ou mais tags a ele programaticamente, use a operação apropriada para o tipo de recurso que deseja criar:

- Para criar uma política de configuração e adicionar uma ou mais tags a ela, invoque a CreateConfigurationPolicyAPI ou, se estiver usando a AWS CLI, execute o create-configuration-policycomando.
- Para criar uma regra de automação e adicionar uma ou mais tags a ela, invoque a CreateAutomationRuleAPI ou, se estiver usando a AWS CLI, execute o create-automation-rulecomando.
- Para habilitar o CSPM do Security Hub e adicionar uma ou mais tags ao seu `Hub` recurso, invoque a EnableSecurityHubAPI ou, se estiver usando o 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 associado.

Para adicionar uma ou mais tags a um recurso existente, use a TagResourceoperação da API CSPM do Security Hub ou, se estiver usando o AWS CLI, execute o comando tag-resource. Na solicitação, especifique o nome do recurso da Amazon (ARN) ao qual a tag será adicionada. 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 AWS CLI comando a seguir adiciona uma chave de `Environment` tag com um valor de `Prod` tag 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 '{"Environment":"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 '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Para cada objeto em uma matriz `tags`, os argumentos `key` e `value` são obrigatórios. No entanto, o valor do argumento `value` pode ser um segmento vazio. Se você não quiser associar um valor de tag a uma chave de tag, não especifique um valor para o argumento `value`. Por exemplo, o comando a seguir adiciona uma chave de tag `0wner` sem valor associado:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Se uma operação de marcação for bem-sucedida, o Security Hub CSPM retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub CSPM retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Editando tags para recursos CSPM do Security Hub

À medida que seu ambiente ou requisitos mudam com o tempo, você pode avaliar as tags existentes para seus recursos CSPM do AWS Security Hub e alterá-las conforme necessário. Uma tag é

um rótulo que você define e atribui a um ou mais recursos da AWS , incluindo certos tipos de recursos do Macie. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Uma chave de tag é uma etiqueta 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.

As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Por exemplo, você pode usar tags para aplicar políticas, alocar custos, distinguir entre versões de recursos ou identificar recursos que suportam determinados requisitos de conformidade ou fluxos de trabalho.

Você pode adicionar tags aos seguintes tipos de recursos CSPM do Security Hub:

- Regras de automação
- Políticas de configuração
- Recurso do Hub

Para editar chaves de tag ou valores de tag para um recurso CSPM do Security Hub, você pode usar a API CSPM do Security Hub. Atualmente, o console CSPM do Security Hub não oferece suporte à edição de tags.

> **Important**
>
> Editar as tags de um recurso pode afetar o acesso a ele. Antes de editar uma tag para um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar tags para controlar o acesso aos recursos.

Security Hub CSPM API

Para editar tags para um recurso CSPM (API) do Security Hub

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 de tag, um valor de tag ou ambos. Para editar uma chave de tag, remova a tag atual e adicione uma nova.

Para editar ou remover somente o valor da tag associado a uma chave de tag, substitua o valor existente usando a TagResourceoperação da API CSPM 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 AWS CLI comando a seguir altera o valor da tag de `Prod` `Test` para para a chave de `Environment` tag atribuída à regra de automação 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 tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"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 tag de uma chave de tag, 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 '{"Owner":""}'
```

Se a operação for bem-sucedida, o Security Hub CSPM retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub CSPM retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Revisão de tags para recursos de CSPM do Security Hub

Depois de adicionar ou editar tags para os recursos CSPM do AWS Security Hub, você pode ver quais chaves e valores de tag um recurso tem atualmente. Uma tag é um rótulo que você define

e atribui a um ou mais recursos da AWS , incluindo certos tipos de recursos do Macie. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Uma chave de tag é uma etiqueta 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.

As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Por exemplo, você pode usar tags para aplicar políticas, alocar custos, distinguir entre versões de recursos ou identificar recursos que suportam determinados requisitos de conformidade ou fluxos de trabalho.

Você pode adicionar tags aos seguintes tipos de recursos CSPM do Security Hub:

- Regras de automação
- Políticas de configuração
- Recurso do Hub

Você pode revisar as tags de uma regra de automação CSPM ou política de configuração do Security Hub usando o console CSPM do Security Hub ou a API CSPM do Security Hub. O console não aceita a revisão de tags para o recurso Hub. Programaticamente, você pode revisar as tags de qualquer recurso.

Para revisar as tags de vários recursos CSPM do Security Hub ao mesmo tempo, use as operações de marcação da AWS Resource Groups API de marcação.

Console

Para revisar as tags de um recurso CSPM do Security Hub (console)

1. Usando as credenciais do administrador do CSPM do Security Hub, abra o console do CSPM 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 CSPM API

Para revisar as tags de um recurso CSPM (API) do Security Hub

Para recuperar e revisar as tags de um recurso existente, invoque a ListTagsForResourceAPI. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN).

Se você estiver usando o AWS CLI, execute o list-tags-for-resourcecomando e use o `resource-arn` parâmetro 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 for bem-sucedida, o Security Hub CSPM retornará uma matriz. `tags` Cada objeto na matriz especifica uma tag (tanto a chave quanto o valor) que está atualmente atribuída ao recurso. Por exemplo:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Em que `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 recuperar uma lista de todos os recursos CSPM do Security Hub que têm tags e todas as tags atribuídas a cada um desses recursos, use a GetResourcesoperação da API de marcação. 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 `resource-type-filters` parâmetro 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 CSPM do Security Hub que tem tags. Cada objeto especifica o ARN de um recurso CSPM do Security Hub e as chaves e valores de tag atribuídos ao recurso.

Removendo tags dos recursos CSPM do Security Hub

Se você adicionar tags a um recurso CSPM do AWS Security Hub, poderá remover posteriormente uma ou mais delas. Uma tag é um rótulo que você define e atribui aos AWS recursos, incluindo certos tipos de recursos CSPM do Security Hub. Você pode adicionar, editar e remover tags dos seguintes tipos de recursos CSPM do Security Hub: regras de automação, políticas de configuração e o Hub recurso.

Para remover tags de um recurso CSPM individual do AWS Security Hub, você pode usar a API CSPM do Security Hub. Atualmente, o console CSPM do Security Hub não oferece suporte à remoção de tags.

Para remover tags de vários recursos CSPM do Security Hub ao mesmo tempo, use as operações de marcação da AWS Resource Groups API de marcação.

> **Important**
>
> Remover tags de um recurso pode afetar o acesso a ele. Antes de remover uma tag, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Security Hub CSPM API

Para remover tags de um recurso CSPM (API) do Security Hub

Para remover uma ou mais tags de um recurso programaticamente, use a UntagResourceoperação da API CSPM do Security Hub. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) que terá a tag removida. 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 um E comercial (&), por exemplo, `tagKeys=`*`key1`*`&tagKeys=`*`key2`*. Para remover somente um valor específico (e não a chave) de um recurso, edite a tag em vez de removê-la.

Se você estiver usando o 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 que terá a tag removida. 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 CSPM retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub CSPM retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Cotas para o Security Hub

Você Conta da AWS tem certas cotas padrão, anteriormente chamadas de limites, para cada uma. 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 AWS Security Hub 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. 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 de Quotas de Serviço, use o formulário de aumento do limite de serviço AWS Support Center Console no para solicitar um aumento na cota.

Cotas máximas

Para obter uma lista de cotas que se aplicam aos recursos do AWS Security Hub, consulte endpoints e cotas do AWS Security Hub no. Referência geral da AWS

Cotas de tarifa

Para ver uma lista de cotas que se aplicam às operações da API do AWS Security Hub, consulte a Referência da API do AWS Security Hub.

Se você configurar a agregação entre regiões no CSPM do Security Hub, uma chamada para `BatchImportFindings` e `BatchUpdateFindings` impacta 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.

Histórico de documentos do Guia do Usuário do AWS Security Hub

A tabela a seguir descreve as mudanças importantes na documentação desde a última versão do AWS Security Hub e do Security Hub CSPM. Para lançamentos de novos controles de segurança do CSPM, a data especifica quando os controles começam a estar disponíveis no suporte. Regiões da AWS Pode levar de 1 a 2 semanas para que os controles estejam disponíveis em todas as regiões suportadas.

Para receber notificações sobre atualizações no Guia do Usuário do AWS Security Hub, você pode assinar um feed RSS.

Alteração	Descrição	Data
Atualizações nos padrões e controles de segurança	Devido às limitações do Amazon Redshift, planejamos retirar os controles Redshift.9 e RedshiftServerless.7 e removê-los de todos os padrões aplicáveis em 15 de setembro de 2025. Atualmente, esses controles se aplicam ao padrão AWS Foundational Security Best Practices (FSBP) e ao padrão NIST SP 800-53 Rev. 5. O controle Redshift.9 também se aplica ao padrão gerenciado por serviços.AWS Control Tower	15 de agosto de 2025
Novo objeto de detalhes do recurso no ASFF	O AWS Security Finding Format (ASFF) agora inclui um objeto `CodeRepository` de recurso. Esse objeto fornece detalhes sobre um repositório de código externo	1.º de agosto de 2025

	que você conectou aos AWS recursos e configuro u o Amazon Inspector para verificar vulnerabilidades.	
Disponibilidade regional	O Security Hub CSPM agora está disponível na região Ásia-Pacífico (Taipei). Para obter uma lista completa de Regiões da AWS onde o CSPM do Security Hub está disponível atualmente, consulte endpoints e cotas do AWS Security Hub no. Referência geral da AWS	23 de julho de 2025
Nova integração de terceiros	Dynatraceé uma nova integração de terceiros que pode receber descobertas do CSPM do Security Hub.	18 de julho de 2025

Novos controles de segurança	O Security Hub CSPM lançou 13 novos controles. A maioria dos controles é compatível com o padrão AWS Foundational Security Best Practices (FSBP). Alguns dos controles suportam os requisitos do NIST SP 800-53 Rev. 5. • Para o padrão AWS FSBP, os controles aplicáveis são: CloudFront.15, IDs Cognito.2, EC2 .180, ELB.18, MSK.4, MSK.5, MSK.6, RDS.45, Redshift.18, S3.25, SSM.6 e SSM.7. • Para o NIST SP 800-53 Rev. 5, os controles aplicáveis são: IDs Lambda.7 e RDS.45.	15 de julho de 2025

Atualizações na geração de resultados de controle	Para ajudá-lo a monitorar as mudanças de conformidade, o Security Hub CSPM agora atualiza as descobertas de controle existentes, em vez de gerar novas descobert as, quando há alteraçõe s no status de conformid ade de recursos individuais. Isso significa que você pode usar os dados fornecidos por descobertas individuais para rastrear alterações de conformidade de recursos específicos em relação a controles específicos.	3 de julho de 2025
Atualizações nos padrões e controles de segurança	Removemos o controle IAM.13 do padrão PCI DSS v4.0.1. Também removemos o controle IAM.17 do padrão NIST SP 800-171 Revisão 2. Os padrões não exigem explicitamente as verificaç ões que esses controles fornecem. Também atualizam os os detalhes dos requisitos relacionados a esses padrões para determinados controles que verificam as políticas de senha do IAM: IAM.7 e IAM.10 a IAM.17.	30 de junho de 2025

Atualizações para encontrar retenção	O Security Hub CSPM agora armazena as descobertas arquivadas por 30 dias em vez de 90 dias, o que pode reduzir o ruído das descobertas. Para retenção de longo prazo, você pode exportar descobertas para um bucket do S3 usando uma ação personalizada com uma regra da Amazon. EventBridge	20 de junho de 2025
Atualizações nas políticas gerenciadas existentes	O Security Hub CSPM adicionou uma nova permissão à política AWS gerenciada chamada. `AWSSecurityHubOrganizationsAccess` A permissão permite que o gerenciamento da organização habilite e gerencie o Security Hub e o CSPM do Security Hub dentro de uma organização. O Security Hub CSPM também adicionou uma nova permissão à política AWS gerenciada chamada. `AWSSecurityHubFullAccess` A permissão permite que os diretores criem uma função vinculada ao serviço para o Security Hub.	18 de junho de 2025

Versão prévia pública e uma nova política gerenciada para o Security Hub	Versão prévia pública do AWS Security Hub e do Guia do Usuário do AWS Security Hub. Esta versão inclui uma nova política AWS gerenciada,`AWSSecurityHubV2ServiceRolePolicy` . A política permite que o Security Hub gerencie AWS Config regras e recursos do Security Hub na organização de um cliente e em nome do cliente. O Security Hub está em versão prévia e está sujeito a alterações.	17 de junho de 2025
Atualizações nos padrões e controles de segurança	Removemos o controle IAM.10 do padrão PCI DSS v4.0.1. Esse controle verifica se as políticas de senha da conta para usuários do IAM atendem aos requisitos mínimos, incluindo um tamanho mínimo de senha de 7 caracteres. O PCI DSS v4.0.1 agora exige que as senhas tenham no mínimo 8 caracteres. O controle IAM.10 continua sendo aplicado ao padrão PCI DSS v3.2.1, que tem requisitos de senha diferentes.	30 de maio de 2025

Novo padrão de segurança	O Security Hub CSPM agora fornece um padrão de segurança que se alinha à estrutura de conformidade e cibersegurança do NIST SP 800-171 Revisão 2. Esse novo padrão inclui mais de 60 controles de segurança existentes. Os controles realizam verificações automatizadas que avaliam determinados recursos Serviços da AWS e recursos quanto à conformidade com um subconjunto dos requisitos definidos pela estrutura.	29 de maio de 2025
Atualizações nos controles de segurança	Ao todo, o Security Hub CSPM reverteu a liberação do seguinte controle Regiões da AWS: [RDS.46] As instâncias de banco de dados do RDS não devem ser implantadas em sub-redes públicas com rotas para gateways da Internet. Anteriormente, esse controle era compatível com o padrão AWS Foundational Security Best Practices (FSBP).	8 de maio de 2025

Novos controles de segurança	O Security Hub CSPM lançou 9 novos controles. A maioria dos controles é compatível com o padrão AWS Foundational Security Best Practices (FSBP). Alguns dos controles suportam os requisitos do NIST SP 800-53 Rev. 5. • Para o padrão AWS FSBP, IDs os controles aplicáveis são: DocumentDB.6, RDS.44, RedshiftServerless .2, .3, .5, .6 e RedshiftServerless .7. RedshiftServerless RedshiftServerless RedshiftServerless • Para o NIST SP 800-53 Rev. 5, IDs os controles aplicáveis são: CloudTrail.10, RedshiftServerless .4 e .7. RedshiftServerless	7 de maio de 2025

Novos controles de segurança	O Security Hub CSPM lançou 24 novos controles. A maioria dos controles é compatível com o padrão AWS Foundational Security Best Practices (FSBP) ou AWS Resource Tagging. Alguns dos controles suportam os requisitos do NIST SP 800-53 Rev. 5. • Para o padrão AWS FSBP, IDs os controles aplicáveis são: EC2.173, RDS.41, RDS.42 e .8. SageMaker • Para o padrão AWS Resource Tagging, IDs os controles aplicáveis são: Amplify.1, Amplify.2, Batch.4, .2, .174, EC2 .175, .176, .177, .178, DataSyncEC2.179, Redshift.17, EC2 .6, .7, SSM.5, Transfer.4, EC2Transfer.5, EC2 EC2 SageMaker SageMaker https://docs.aws.amazon.com/securityhub/latest/userguide/transfer-controls.html#transfer-6Transferir.6 e Transfer.7. • Para o NIST SP 800-53 Rev. 5, os controles aplicáveis são: IDs ECS.17 e RDS.42.	16 de abril de 2025

Novos controles de segurança	O Security Hub CSPM lançou quatro novos controles para o padrão AWS Foundational Security Best Practices. Os controles são: • the section called “[FSx.3] FSx para sistemas de arquivos OpenZFS devem ser configurados para implantação Multi-AZ” • the section called “[FSx.4] FSx para sistemas de arquivos NetApp ONTAP, deve ser configurado para implantação Multi-AZ” • the section called “[FSx.5] FSx para Windows File Server, os sistemas de arquivos devem ser configurados para implantação Multi-AZ” • the section called “[RedshiftServerless.1] Os grupos de trabalho do Amazon Redshift sem servidor deverão usar o roteamento aprimorado da VPC”	18 de março de 2025

Atualizações nos padrões e controles de segurança	Removemos o controle de segurança RDS.18 do padrão AWS Foundational Security Best Practices e automatiz amos as verificações dos requisitos do NIST SP 800-53 Rev. 5. Como a rede Amazon EC2 -Classic foi descontin uada, as instâncias do Amazon Relational Database Service (Amazon RDS) não podem mais ser implantadas fora de uma VPC. O controle continua fazendo parte do padrão AWS Control Tower gerenciado por serviços.	07 de março de 2025
Atualizações nas descobertas de controle	O Security Hub CSPM agora gera `WARNING` descobertas para um controle ativado se a gravação de recursos não estiver ativada AWS Config para o tipo de recurso que o controle verifica. Isso pode ajudá-lo a identificar e resolver possíveis lacunas de configura ção em suas verificações de controle de segurança.	25 de fevereiro de 2025

Novos controles de segurança	O Security Hub CSPM lançou 11 novos controles. Os controles são: • the section called “[Connect .2] As instâncias do Amazon Connect devem ter CloudWatch o registro ativado” • the section called “[ECR.5] Os repositórios ECR devem ser criptografados com gerenciamento de clientes AWS KMS keys” • the section called “[ELB.17] Os balanceadores de carga de aplicativos e redes com ouvintes devem usar as políticas de segurança recomendadas” • the section called “[Glue.4] Os trabalhos do AWS Glue Spark devem ser executados em versões compatíveis do AWS Glue” • the section called “[GuardDuty.11] O monitoramento GuardDuty de tempo de execução deve estar ativado” • the section called “[GuardDuty.12] O monitoramento de tempo de execução GuardDuty do ECS deve estar ativado”	24 de fevereiro de 2025

- the section called “[GuardDuty.13] O monitoramento GuardDuty EC2 de tempo de execução deve estar ativado”
- the section called “[Network Firewall.10] Os firewalls do Network Firewall devem ter a proteção contra alterações de sub-rede ativada”
- the section called “[RDS.40] O RDS para instâncias de banco de dados SQL Server deve publicar registros em Logs CloudWatch ”
- the section called “[SQS.3] As políticas de acesso à fila do SQS não devem permitir acesso público”
- the section called “[Transfer.3] Os conectores Transfer Family devem ter o registro ativado”

Novos controles de segurança	O Security Hub CSPM lançou 37 novos controles para o AWS Resource Tagging Standard. O Security Hub CSPM também lançou os seguintes novos controles: • the section called “[EMR.3] As configurações de segurança do Amazon EMR devem ser criptografadas em repouso” • the section called “[EMR.4] As configurações de segurança do Amazon EMR devem ser criptografadas em trânsito” • the section called “[SageMaker.5] SageMaker os modelos devem ter o isolamento de rede ativado”	22 de janeiro de 2025
Novo controle de segurança	O Security Hub CSPM lançou EC2.172 As configurações de bloqueio de acesso público de EC2 VPC devem bloquear o tráfego do gateway de Internet.	15 de janeiro de 2025

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis. • the section called “[Cognito.1] Os grupos de usuários do Cognito devem ter a proteção contra ameaças ativada com o modo de fiscalização de funções completas para autenticação padrão” • the section called “[RDS.38] O RDS para instâncias de banco de dados PostgreSQL deve ser criptografado em trânsito” • the section called “[RDS.39] O RDS para instâncias de banco de dados MySQL deve ser criptografado em trânsito” • the section called “[Redshift.16] Os grupos de sub-redes do cluster do Redshift devem ter sub-redes de várias zonas de disponibilidade”	17 de dezembro de 2024

O Security Hub CSPM é compatível com PCI DSS v4.0.1	O Security Hub CSPM agora suporta a versão 4.0.1 do Payment Card Industry Data Security Standard (PCI DSS). Para obter mais informações sobre o padrão e os controles que se aplicam a ele, consulte PCI DSS no Security Hub CSPM.	11 de dezembro de 2024
O Security Hub CSPM recebe descobertas da sequência de GuardDuty ataque	O Security Hub CSPM agora recebe descobertas da sequência de ataque do Amazon GuardDuty Extended Threat Detection. Os detalhes da busca da sequência de ataque estão disponíveis no objeto Detecção do Formato de Busca de AWS Segurança (ASFF).	1.º de dezembro de 2024
O Security Hub CSPM é compatível com o novo Região da AWS	O Security Hub CSPM agora está disponível na região Ásia-Pacífico (Malásia). Alguns controles de segurança têm limitações regionais. Para obter uma lista dos controles que não estão disponíveis nessa região, consulte Limites regionais nos controles CSPM do Security Hub.	22 de novembro de 2024

Alterações no Config.1	O Security Hub CSPM aumentou a severidade do controle Config.1 de `MEDIUM` para `CRITICAL` e adicionou novos códigos de status e motivos de status para falhas nas descobertas do Config.1. Para obter mais informaçõ es sobre as alterações, consulte a entrada de 20 de novembro de 2024 no Registro de alterações dos controles CSPM do Security Hub.	20 de novembro de 2024

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis. Esses controles fazem parte das Melhores Práticas AWS de Segurança Fundamental e do NIST SP 800-53 Rev. 5, e avaliam se uma nuvem privada virtual (VPC) que você gerencia tem uma interface VPC endpoint para um recurso ou. AWS service (Serviço da AWS) AWS • the section called “[EC2.55] VPCs deve ser configurado com um endpoint de interface para a API ECR” • the section called “[EC2.56] VPCs deve ser configurado com um endpoint de interface para Docker Registry” • the section called “[EC2.57] VPCs deve ser configurado com um endpoint de interface para Systems Manager” • the section called “[EC2.58] VPCs deve ser configurado com um endpoint de interface para Systems Manager Incident Manager Contacts” • the section called “[EC2.60] VPCs deve ser configura	15 de novembro de 2024

	do com um endpoint de interface para o Systems Manager Incident Manager”	
Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis. • the section called “[AppSync .1] Os caches de AWS AppSync API devem ser criptografados em repouso” • the section called “[AppSync .6] Os caches de AWS AppSync API devem ser criptografados em trânsito” • the section called “[EC2.170] os modelos de EC2 lançamento devem usar o Instance Metadata Service versão 2 () IMDSv2” • the section called “[EC2.171] As conexões EC2 VPN devem ter o registro ativado” • the section called “[EFS.8] Os sistemas de arquivos do EFS devem ser criptogra fados em repouso” • the section called “[KMS.5] As chaves do KMS não devem estar acessíveis ao público” • the section called “[SNS.4] As políticas de acesso a tópicos do SNS não devem permitir o acesso público”	18 de outubro de 2024

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis. • the section called “[ECS.16] Os conjuntos de tarefas do ECS não devem atribuir automaticamente endereços IP públicos” • the section called “[GuardDuty.7] O Monitoramento de Runtime do GuardDuty EKS deve estar habilitado” • the section called “[Kinesis.3] Os fluxos do Kinesis devem ter um período de retenção de dados adequado” • the section called “[MSK.3] Os conectores da MSK Connect devem ser criptografados em trânsito” • the section called “[RDS.36] O RDS para instâncias de banco de dados PostgreSQL deve publicar registros em Logs CloudWatch ” • the section called “[RDS.37] Os clusters de banco de dados Aurora PostgreSQL devem publicar registros no Logs CloudWatch ” • the section called “[S3.24] Os pontos de acesso multirregionais do S3 devem	3 de outubro de 2024

ter as configurações de bloqueio do acesso público habilitadas”

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis. • the section called “[Athena.4] Os grupos de trabalho do Athena devem ter o registro em log habilitado” • the section called “[CodeBuild.7] as exportações CodeBuild do grupo de relatórios devem ser criptografadas em repouso” • the section called “[DataSync.1] DataSync as tarefas devem ter o registro ativado” • the section called “[EFS.7] Os sistemas de arquivos do EFS devem ter backups automáticos habilitados” • Glue.2 (retirado) • the section called “[Glue.3] As transformações AWS Glue de aprendizado de máquina devem ser criptografadas em repouso” • the section called “[WorkSpaces.1] os volumes WorkSpaces do usuário devem ser criptografados em repouso” • the section called “[WorkSpaces.2] os volumes WorkSpaces raiz devem ser criptografados em repouso”	30 de agosto de 2024

Novo painel de descobertas	O novo painel de descobertas no console CSPM do Security Hub ajuda você a agir rapidamente sobre as descobertas, analisar os detalhes dos recursos e o histórico de descobertas e encontrar outras informações pertinentes sobre uma descoberta.	16 de agosto de 2024
Atualização do controle Config.1	O controle Config.1 verifica se AWS Config está ativado, usa a função vinculada ao serviço e registra os recursos dos controles habilitados. O Security Hub CSPM adicionou um parâmetro de controle personalizado chamado. `includeConfigServiceLinkedRoleCheck` Definindo esse parâmetro como `false`, você pode optar por não verificar se o AWS Config usa o perfil vinculado ao serviço.	15 de agosto de 2024
Designar uma região inicial sem regiões vinculadas	Agora você pode criar um agregador de busca e estabelecer uma região de origem sem vincular nenhuma Regiões da AWS à região de origem. Isso permite que você habilite a configuração central sem especificar as regiões vinculadas.	25 de julho de 2024

Selecionar os controles disponíveis em mais regiões	Os controles a seguir agora estão disponíveis adicional mente Regiões da AWS, incluindo Leste dos EUA (Norte da Virgínia) e Leste dos EUA (Ohio). • 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado” • the section called “[DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado” • the section called “[DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito” • the section called “[EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes	15 de julho de 2024

que atribuem endereços IP públicos na inicialização”

- the section called “[EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes”
- the section called “[FSx.2] FSx para sistemas de arquivos 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 agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada”
- 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 somente na porta do cluster 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 do Transfer Family não devem usar o protocolo FTP para conexão de endpoints”

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis: • the section called “[GuardDuty.5] O Monitoramento de GuardDuty Logs de Auditoria do EKS deve estar habilitado” • the section called “[GuardDuty.6] A Proteção do GuardDuty Lambda deve estar habilitada” • the section called “[GuardDuty.8] O formulário de proteção contra GuardDuty malware EC2 deve estar ativado” • the section called “[GuardDuty.9] A proteção do GuardDuty RDS deve estar habilitada” • the section called “[GuardDuty.10] A proteção do GuardDuty S3 deve estar habilitada” • the section called “[Inspector.1] O escaneamento do Amazon Inspector deve estar ativado EC2 ” • the section called “[Inspector.2] A varredura do ECR do Amazon Inspector deve estar habilitada”	11 de julho de 2024

- the section called “[Inspector.3] A varredura de código do Lambda do Amazon Inspector deve estar habilitada”
- the section called “[Inspector.4] A varredura padrão do Lambda do Amazon Inspector deve estar habilitada”

Lançamento do CIS AWS Foundations Benchmark v3.0.0	O Security Hub CSPM lançou o Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0. O lançamento inclui os seguintes controles novos, bem como mapeamentos para vários controles existentes. • the section called “[EC2.53] grupos de EC2 segurança não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor” • the section called “[EC2.54] grupos EC2 de segurança não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto” • the section called “[IAM.26] SSL/TLS Certificados expirados gerenciados no IAM devem ser removidos” • the section called “[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloud ShellFullAccess ” • the section called “[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve ser habilitado”	13 de maio de 2024

- the section called “[S3.22] Os buckets de uso geral do S3 devem registrar em log os eventos de gravação ao nível do objeto”
- the section called “[S3.23] Os buckets de uso geral do S3 devem registrar em log os eventos de leitura ao nível do objeto”

Novos controles de segurança	Os seguintes novos controles CSPM 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 do DMS para o MongoDB devem ter um mecanismo de autenticação habilitado” • the section called “[DMS.12] Os endpoints do DMS para o Redis OSS devem ter o TLS habitado” • the section called “[DynamoDB.7] Os clusters do acelerador do DynamoDB devem ser criptografados em trânsito” • the section called “[EFS.6] Os destinos de montagem do EFS não devem ser associados a sub-redes que atribuem endereços IP públicos na inicialização”	3 de maio de 2024

- the section called “[EKS.3] Os clusters do EKS devem usar segredos criptografados do Kubernetes”
- the section called “[FSx.2] FSx para sistemas de arquivos 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 agentes do Amazon MQ devem ter a atualização automática de versões secundárias habilitada”
- 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 somente na porta do cluster 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 do 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 CSPM agora está disponível ao público em geral, junto com novos controles que se aplicam ao padrão.	30 de abril de 2024
Atualização de política gerenciada existente	O Security Hub CSPM atualizou a política AWS gerenciada nomeada `AmazonSecurityHubFullAccess` para obter detalhes de preços Serviços da AWS e produtos.	24 de abril de 2024
Configuração de parâmetros de controles no contexto	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 CSPM do Security Hub.	29 de março de 2024

Atualização de política gerenciada existente	O Security Hub CSPM 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 habilitada já está disponível. Para ver os limites regionais desse controle, consulte Disponibilidade de controles por região.	19 de fevereiro de 2024
Security Hub CSPM disponível no Oeste do Canadá (Calgary)	O Security Hub CSPM agora está disponível no Oeste do Canadá (Calgary). Todos os recursos do CSPM 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 CSPM 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 EC2 do Client VPN devem ter o registro de conexão do cliente ativado” • 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] FSx para sistemas de arquivos OpenZFS, devem ser configurados para copiar tags para backups e volumes”	14 de dezembro de 2023

- the section called “[Macie.1] O Amazon Macie deve estar habilitado”
- 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 em log do Network Firewall deve ser habilitado”
- 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 CSPM adicionou os novos campos `AwsAccountName` de descoberta e `ApplicationName` ao AWS Security Finding Format (ASFF). `ApplicationArn`	27 de novembro de 2023
Aprimoramentos no painel Resumo	Agora você pode acessar mais widgets do painel na página Resumo do console CSPM 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 CSPM do Security Hub pode configurar o CSPM, os padrões e os controles do Security Hub em várias contas organizacionais, unidades organizacionais () OUs e regiões.	27 de novembro de 2023

Atualizações da política gerenciada	O Security Hub CSPM adicionou novas permissões à política `AWSSecurityHubServiceRolePolicy` gerenciada que permitem que o CSPM do Security Hub leia e atualize propriedades de controle de segurança personalizáveis.	26 de novembro de 2023
Parâmetros de controle personalizados	Agora você pode personalizar os valores dos parâmetros para determinados controles CSPM 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 CSPM atualizou `AWSSecurityHubFullAccess` e `AWSSecurityHubOrganizationsAccess` gerenciou as políticas que permitem que você use, respectivamente, os recursos do Security Hub CSPM 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 CSPM existentes do Security Hub foram adicionados ao Service-Managed Standard:. AWS Control Tower • ACM.2 • AppSync5. • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC22.3 • 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 CSPM do Security Hub adicionou uma nova permissão de marcação à política `AWSSecurityHubServiceRolePolicy` gerenciada que permite que o CSPM do Security Hub leia as tags de recursos relacionadas às descobertas.	7 de novembro de 2023

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis: • the section called “[AppSync.5] O AWS AppSync APIs GraphQL não deve ser autenticado com chaves de API” • the section called “[DMS.6] As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada” • the section called “[DMS.7] As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado” • the section called “[DMS.8] As tarefas de replicação do DMS para o banco de dados de origem devem ter o registro em log ativado” • the section called “[DMS.9] Os endpoints do DMS devem usar SSL” • the section called “[DocumentDB.3] Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos”	10 de outubro de 2023

- the section called “[DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch ”
- the section called “[DocumentDB.5] Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada”
- the section called “[ECS.9] 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 “[MSK.1] Os clusters MSK devem ser criptografados em trânsito entre os nós do agente”
- the section called “[MQ.5] Os agentes do ActiveMQ

devem usar o modo de implantação ativo/em espera”

- the section called “[MQ.6] Os agentes do RabbitMQ devem usar o modo de implantação de cluster”
- the section called “[Network Firewall.9] Os firewalls do Network Firewall 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 “[RDS.35] Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada”
- the section called “[Route53 .2] As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS”
- the section called “[WAF.12] AWS WAF As regras do devem ter as métricas habilitadas CloudWatch ”

Atualizações na política gerenciada	O Security Hub CSPM adicionou novas ações do Organizations à política `AWSSecurityHubServiceRolePolicy` gerenciada que permitem que o CSPM do Security Hub recupere informações da conta e da unidade organizacional (OU). Também adicionamos novas ações do CSPM do Security Hub que permitem que o CSPM do 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 CSPM existentes do Security Hub foram adicionados ao Service-Managed Standard:. AWS Control Tower • the section called “[Athena.1] Os grupos de trabalho do Athena devem ser criptografados em repouso” • the section called “[DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso” • the section called “[DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado” • the section called “[Neptune.1] 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 “[Neptune.3] Os instantâneos do cluster de banco de dados	26 de setembro de 2023

do Neptune não devem ser públicos”

- the section called “[Neptune .4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada”
- the section called “[Neptune .5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados”
- the section called “[Neptune .6] Os instantâneos do cluster 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 “[Neptune .8] Os clusters de banco de dados do Neptune devem ser configurados para copiar tags para instantâneos”
- the section called “[RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso”

Visualização de controles consolidados e descobertas de controle consolidadas 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 CSPM 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 CSPM 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 CSPM disponível na região de Israel (Tel Aviv)	O Security Hub CSPM agora está disponível em Israel (Tel Aviv). Todos os recursos do CSPM 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 CSPM do Security Hub estão disponíveis: • the section called “[Athena.1] Os grupos de trabalho do Athena devem ser criptografados em repouso” • the section called “[DocumentDB.1] Os clusters do Amazon DocumentDB devem ser criptografados em repouso” • the section called “[DocumentDB.2] Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado” • the section called “[Neptune.1] 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 “[Neptune.3] Os instantâneos do cluster de banco de dados do Neptune não devem ser públicos”	28 de julho de 2023

- the section called “[Neptune .4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada”
- the section called “[Neptune .5] Os clusters de banco de dados do Neptune devem ter backups automatizados habilitados”
- the section called “[Neptune .6] Os instantâneos do cluster 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 “[Neptune .8] Os clusters de banco de dados do Neptune devem ser configurados para copiar tags para instantâneos”
- the section called “[RDS.27] Os clusters de banco de dados do RDS 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 CSPM agora oferece regras de automação que atualizam automaticamente as descobertas com base nos critérios que você especifica.	13 de junho de 2023
Novas integrações de terceiros	Snyké uma nova integração de terceiros que envia descobertas para o CSPM do Security Hub.	12 de junho de 2023

Controles de segurança existentes adicionados ao Service-Managed Standard: AWS Control Tower	Os seguintes controles CSPM 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 “[APIGateway.8] As rotas do API de Gateway devem especificar um tipo de autorização” • the section called “[APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway” • the section called “[CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados” • the section called “[EC2.25] Os modelos de EC2 lançamento da Amazon não devem atribuir interfaces públicas IPs às 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] A AWS WAF web ACLs deve ter pelo menos uma regra ou grupo de regras”

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis: • the section called “[ACM.2] 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 CSPM disponível na Ásia-Pacífico (Melbourne)	O Security Hub CSPM agora está disponível na Ásia-Pacífico (Melbourne). Todos os recursos do CSPM 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 CSPM agora pode rastrear o histórico de uma descoberta nos últimos 90 dias.	4 de maio de 2023

Novos controles de segurança	Os seguintes novos controles CSPM do Security Hub estão disponíveis: • the section called “[EKS.1] 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 Bloqueio de Objetos habilitado”	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 consolidadas de controle.	24 de março de 2023
Security Hub CSPM disponível em novo Regiões da AWS	O Security Hub CSPM agora está disponível na 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 CSPM atualizou uma permissão existente na política `AWSSecurityHubServiceRolePolicy` gerenciada.	17 de março de 2023

Novos controles de segurança para o padrão NIST 800-53	O Security Hub CSPM 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] Os CloudWatch alarmes devem ter ações especificadas configuradas” • the section called “[CloudWatch.16] Os grupos de CloudWatch log devem ser retidos por um período de tempo especificado” • the section called “[CloudWatch.17] as ações CloudWatch de alarme devem ser ativadas” • the section called “[DynamoDB.4] 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”	3 de março de 2023

	• EC2.29 — EC2 as instâncias devem ser lançadas em uma VPC (desativada) • the section called “[RDS.26] 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 versionamento habilitado” • the section called “[WAF.11] O registro em log 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 CSPM agora suporta o 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 CSPM 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 CSPM do Security Hub estão disponíveis. Alguns controles têm limitações regionais. • the section called “[ElastiCache.1] Os clusters ElastiCache (Redis OSS) devem ter backups automáticos habilitados” • the section called “[ElastiCache.2] os ElastiCache clusters devem ter atualizações automáticas de versões secundárias habilitadas” • the section called “[ElastiCache.3] os grupos de ElastiCache replicação devem ter o failover automático ativado” • the section called “[ElastiCache.4] os grupos de ElastiCache replicação devem ser criptografados em repouso” • the section called “[ElastiCache.5] os grupos de ElastiCache replicação devem ser criptografados em trânsito” • the section called “[ElastiCache.6] ElastiCache (Redis OSS) grupos de replicação de versões anteriores	16 de fevereiro de 2023

	devem ter o Redis OSS AUTH ativado” • the section called “[ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão”	
Novos campos do ASFF	O Security Hub CSPM foi adicionado. 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 CSPM 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 você pode ver os detalhes da vulnerabilidade no console CSPM do Security Hub para ver as descobertas que o Amazon Inspector envia para o CSPM do Security Hub.	14 de janeiro de 2023
O Security Hub CSPM está disponível no Oriente Médio (EAU)	O Security Hub CSPM agora está disponível no Oriente Médio (EAU). Alguns controles têm limites regionais.	12 de janeiro de 2023

Adicionada a integração de terceiros com o MetricStream	O Security Hub CSPM agora oferece suporte a uma integração de terceiros MetricStream em todas as regiões, exceto na China e. AWS GovCloud (US)	11 de janeiro de 2023
Aumento do limite da conta organizacional	O Security Hub CSPM agora suporta até 11.000 contas de membros para cada conta de administrador do Security Hub CSPM por região.	27 de dezembro de 2022
ElasticBeanstalk.3 Revertido	O CSPM do Security Hub reverteu o controle [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros do padrão FSBP em todas as regiões. CloudWatch	21 de dezembro de 2022
O Security Hub CSPM adiciona novos controles de segurança	Os novos controles CSPM do Security Hub estão disponíveis para clientes que habilitaram o padrão FSBP. Alguns controles têm limitações regionais.	15 de dezembro de 2022
Orientações sobre os próximos atributos	O Security Hub CSPM planeja lançar dois novos recursos: visualização de controles consolidados 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 CSPM do Security Hub ao receber as descobert as do CSPM do Security Hub.	29 de novembro de 2022
Support for Service-Managed Standard: AWS Control Tower	O Security Hub CSPM 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 CSPM 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 CSPM do Security Hub em todas as regiões disponíveis, 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 CSPM do Security Hub em todas as regiões disponíve is.	17 de novembro de 2022

Support para o CIS AWS Foundations Benchmark v1.4.0	O Security Hub CSPM 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 CSPM em AWS GovCloud (US)	Agora você pode assinar os anúncios do CSPM do Security Hub com o Amazon Simple Notification Service (Amazon AWS GovCloud SNS) em (Leste dos EUA) e (Oeste dos EUA AWS GovCloud) para receber notificações sobre o CSPM do Security Hub.	3 de outubro de 2022
AWS O Security Hub CSPM adiciona um novo controle de segurança	O novo controle CSPM do Security Hub AutoScaling.9 está disponível para clientes que habilitaram o padrão FSBP. Os controles podem ter limitações regionais.	1º de setembro de 2022
Assine os anúncios do Security Hub CSPM	Agora você pode assinar os anúncios do CSPM do Security Hub com o Amazon Simple Notification Service (Amazon SNS) para receber notificações sobre o CSPM do Security Hub.	29 de agosto de 2022

Expansão da região para agregação entre regiões	A agregação entre regiões já está disponível para descobertas, 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 CSPM do Security Hub e JFrog é uma integração de terceiros que envia as descobertas para o CSPM do Security Hub.	26 de julho de 2022
EC2.27 está aposentado	O CSPM do Security Hub foi descontinuado EC2. 27 - EC2 As instâncias em execução não devem 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 CSPM 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 Foundational Security Best Practices (FSBP). AWS	19 de julho de 2022

AWS O Security Hub CSPM adiciona novos controles de segurança	Os novos controles CSPM do Security Hub estão disponíveis para clientes que habilitaram o padrão FSBP. Alguns controles têm limitações regionais.	22 de junho de 2022
AWS O Security Hub CSPM oferece suporte a uma nova região	O Security Hub CSPM agora 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 CSPM e AWS Config	Os usuários do Security Hub CSPM podem ver os resultados das avaliações de AWS Config regras como descobertas no CSPM do 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 CSPM 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 5 novos controles ao padrão AWS Foundational Security Best Practices.	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 AWS Foundational Security Best Practices.	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 CloudFront e ao padrão Foundational Security Best AWS Practices. Também foram adicionados os 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 adicionada com AWS Health	AWS Health usa mensagens de service-to-service eventos para enviar descobertas ao CSPM do Security Hub.	19 de janeiro de 2022
Integração adicionada com AWS Trusted Advisor	Trusted Advisor envia os resultados de suas verificações para o Security Hub CSPM como descobertas do CSPM do Security Hub. O Security Hub CSPM 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` . Adição de `MetadataOptions` a `AwsAutoScalingLaunchConfiguration` . Adição de `BucketVersioningConfiguration` a `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 CSPM está integrado com a nova versão do Amazon Inspector , bem como com o Amazon Inspector Classic. O Amazon Inspector envia descobertas para o Security Hub CSPM.	29 de novembro de 2021
Alterou a severidade de EC2 1,9	A severidade de EC2 .19 (grupos de segurança não devem permitir acesso irrestrito a portas com alto risco) é alterada de Alta para Crítica.	17 de novembro de 2021
Nova integração com o Sonrai Dig	O Security Hub CSPM agora oferece uma integração com o. Sonrai Dig Sonrai Digmonitora ambientes de nuvem para identificar riscos de segurança . Sonrai Digenvia as descobertas para o Security Hub CSPM.	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 CSPM 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 1.9	EC2.19 agora também verifica se os grupos de segurança não permitem acesso irrestrito às seguintes portas: 3000 (estruturas de desenvolvimento web Go, Node.js e Ruby), 5000 (estruturas de desenvolvimento web Python), 8088 (porta HTTP antiga) 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 descobertas do Security Hub CSPM.	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
Alterou a severidade de EC2 1,9	A severidade de [EC2.19] Os grupos de segurança não devem permitir que o acesso irrestrito às portas com alto risco seja alterada de Médio para Alto.	30 de setembro de 2021

A integração com agora AWS Organizations é suportada nas regiões da China	A integração do Security Hub CSPM com Organizations agora é suportada na China (Pequim) e na 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 CSPM agora oferece uma integração com o. HackerOne Vulnerability Intelligence A integração envia as descobertas para o Security Hub CSPM.	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 CSPM 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 CSPM está retirando o controle [Lambda.4] As funções do Lambda devem ter uma fila de mensagens mortas configurada. Quando um controle é retirado, ele não é mais exibido no console e o Security Hub CSPM não executa verificações nele.	31 de agosto de 2021
Desativando o PCI. EC23. controle	O Security Hub CSPM está retirando o controle [PCI]. EC2.3] Grupos de EC2 segurança não utilizados devem ser removidos. Quando um controle é retirado, ele não é mais exibido no console e o Security Hub CSPM não executa verificações nele.	27 de agosto de 2021
Alteração na forma como o Security Hub CSPM envia descobertas para ações personalizadas	Quando você envia descobert as para uma ação personali zada, o Security Hub CSPM agora envia cada descobert a em um evento separado Security Hub Findings - Custom Action.	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 CSPM do Security Hub não pôde realizar uma verificação em um tempo de execução Lambda personalizado.	20 de agosto de 2021
AWS Firewall Manager integração agora suportada nas regiões da China	A integração do Security Hub CSPM com o Firewall Manager agora é suportada na China (Pequim) e na China (Ningxia).	19 de agosto de 2021
Novas integrações com Caveonix Cloud e Forcepoint Cloud Security Gateway	O Security Hub CSPM agora oferece integrações com e. Caveonix Cloud Forcepoint Cloud Security Gateway Ambas as integrações enviam descobertas para o Security Hub CSPM.	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 (EC2.19), Amazon ECS EC2 (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 a ES.8), Amazon RDS (RDS.16 a RDS.23), Amazon Redshift (Redshift.4) e Amazon SQS (SQS.23) 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 (CloudFront.5 e CloudFront .6), Amazon (EC2.17 e EC2 .18), Amazon ECS EC2 (ECS.1), Amazon Service (ES.4), (IAM.21), OpenSearch Amazon RDS (RDS.15) AWS Identity and Access Management 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
Foi adicionada a integração com o Amazon Q Developer em aplicativos de bate-papo	Foi adicionada a integração com o Amazon Q Developer em aplicativos de bate-papo. O Security Hub CSPM envia descobertas para o Amazon Q Developer em aplicativos de bate-papo.	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. Atualizou o objeto da EC2 instância 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 CSPM 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 CSPM	Foram adicionadas informaçõ es sobre como o Security Hub CSPM lida com contas suspensas em. 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 CSPM. O Cyber Investigator da NETSCOUT envia as descobertas para o Security Hub CSPM.	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 CSPM 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 CSPM do 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 Payment Card Industry Data Security Standard (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 CSPM.	14 de maio de 2021

Controles adicionados ao padrão AWS Foundational Security Best Practices	Foram adicionados novos controles para Amazon API Gateway (APIGateway.2 e APIGateway .3), AWS CloudTrail (CloudTrail.4 e .5), Amazon (CloudTrailEC2.15 e EC2 .16), EC2 (ElasticB eanstalk.1 e ElasticBe anstalk .2), (AWS Lambda Lambda.4), Amazon RDS AWS Elastic Beanstalk (RDS.12 — RDS.14), Amazon Redshift (Redshift.7), (.3 e .4) e (WAF.1). 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.Guard Duty.1` foi alterada de Média para Alta. Um parâmetro `databaseE ngines` 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 a EC2 rede Amazon ACLs, EC2 sub-redes e AWS Elastic Beanstalk ambientes da Amazon.	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 CSPM 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 CSPM agora suporta uma integração com o Systems Manager Explorer e. OpsCenter A integração recebe descobertas do Security Hub CSPM e atualiza essas descobertas no Security Hub CSPM.	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 CSPM 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 CSPM e na API do Security Hub.	22 de abril de 2021

Atualizado APIGateway 1.1 para substituir HTTP por Websocket	O título, a descrição e a correção foram atualizados para APIGateway .1. 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 o CSPM 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
O Security Hub CSPM foi lançado na Ásia-Pacífico (Osaka)	O Security Hub CSPM agora 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 CSPM.	23 de março de 2021
Fazendo a transição para o gerenciamento AWS Organizations de contas	Para clientes que já têm uma conta de administrador com contas-membro, foram adicionadas novas informações sobre como mudar do gerenciamento de contas por convite para o gerenciamento de contas usando o 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 Organizations as permissões necessárias para a conta de gerenciamento da organização e para a conta delegada de administrador do CSPM 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 o SecureCloud banco de dados	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 CSPM.	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), OpenSearc h Amazon Service (ES.2 e ES.3), Elastic Load Balancing (ELB.6) e () (KMS.3). AWS Key Management Service A WS 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 Antivirus para Amazon S3 envia os resultados da verificação de vírus para o Security Hub CSPM como descobertas.	27 de janeiro de 2021
Atualizado o processo de cálculo da pontuação de segurança para as contas de administrador	Para uma conta de administr ador, o Security Hub CSPM usa um processo separado para calcular a pontuação de segurança. O novo processo garante que a pontuação inclua os controles que estão habilitados para as contas-me mbros, mas desabilitados 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 CSPM redefine 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, ou`FAILED`. `WARNING` `NOT_AVAILABLE` 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 `ProductFields` objeto no Formato de descoberta de AWS segurança (ASFF).	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 de CSPM do Security Hub é recebida. As atualizaç ões desses incidentes ou problemas resultam em atualizações das descobertas no CSPM do Security Hub.	11 de dezembro de 2020
Nova integração com o AWS Audit Manager	O Security Hub CSPM agora oferece uma integração com o AWS Audit Manager. A integração permite que o Audit Manager receba descobert as baseadas em controle do Security Hub CSPM.	8 de dezembro de 2020
Nova integração com o Aqua Security Kube-bench	O Security Hub CSPM adicionou uma integração com o Aqua Security Kube-bench. A integração envia as descobertas para o Security Hub CSPM.	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 CSPM agora está integrado com AWS Organizations	Agora, os clientes podem gerenciar as contas de membros usando a configuração de conta do Organizations. A conta de gerenciamento da organização designa a conta de administrador do CSPM do Security Hub, que determina quais contas da organização devem ser habilitadas no CSPM do 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 CSPM agora oferece suporte a integrações com cloudtamer.io, 3, Prowler e Kubernetes Security. CORESec StackRox A 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 CSPM agora está integrado ao. ThreatModeler 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
O Security Hub CSPM foi lançado na China (Pequim) e na China (Ningxia)	O Security Hub CSPM agora está disponível nas regiões da 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.	1.º de outubro de 2020
Novas integrações com as séries VM da Blue Hexagon for AWS, Alcide KAudit e Palo Alto Networks.	O Security Hub CSPM 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 descobertas para o Security Hub CSPM. A série VM recebe descobertas do Security Hub CSPM.	30 de setembro de 2020
Objetos de detalhes de recursos novos e atualizados no ASFF	Foram adicionados novos objetos `Resources.Details` para `AwsApiGatewayRestApi`, `AwsApiGatewayStage`, `AwsApiGatewayV2Api`, `AwsApiGatewayV2Stage`, `AwsCertificateManagerCertificate`, `AwsElbLoadBalancer`, `AwsIamGroup` e `AwsRedshiftCluster`. Detalhes adicionados aos objetos `AwsCloudFrontDistribution`, `AwsIamRole` e `AwsIamAccessKey`.	30 de setembro de 2020

Novo atributo `ResourceRole` 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 CSPM. O Patch Manager envia as descobertas ao CSPM do Security Hub quando as instâncias da frota de um cliente não estão em conformidade com o 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 de membros	Por padrão, as contas-membros agora têm o mesmo acesso a `BatchUpdateFindings` que 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 CSPM do 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, você pode filtrar utilizando a opção não é para localizar as descobertas para as quais o valor do campo não é igual ao valor do filtro. Você pode 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 CSPM agora está integrado ao RSA Archer. O RSA Archer recebe descobertas do Security Hub CSPM.	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

Atualizado como o Security Hub CSPM 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
Atualizou a forma como o Security Hub CSPM calcula a pontuação de segurança de um padrão	Ao calcular a pontuação de segurança de um padrão, o Security Hub CSPM 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. EC25., PCI. EC26., PCI. ELBV21., 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, .6, S3.5 e EC2 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.	1.º de julho de 2020
Novos `Resource.Details` objetos no ASFF para grupos EC2 , volumes e volumes do Auto Scaling EC2 VPCs	Os objetos `AwsAutoSc alingAutoScalingGr oup` , `AWSEc2Volume` e `AwsEc2Vpc` foram adicionad os a `Resource.Details` .	1.º 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.	1.º de julho de 2020
Solucionar as descobertas automaticamente quando `Compliance.Status` for `PASSED`	Para descobertas de controles , se `Compliance.Status` houver`PASSED`, o Security Hub CSPM será automatic amente definido `Workflow.Status` como. `RESOLVED`	24 de junho de 2020
AWS Command Line Interface exemplos	AWS CLI Sintaxe e exemplos adicionados para várias tarefas CSPM do Security Hub. Inclui a ativação do CSPM do Security Hub, o gerenciamento de insights, o gerenciamento de padrões e controles, o gerenciamento de integrações de produtos e a desativação do CSPM 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 CSPM. 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)	Foi adicionado o padrão de segurança Security Hub CSPM para o Payment Card Industry Data Security Standard (PCI DSS). Quando esse padrão está habilitado, o Security Hub CSPM executa verificações automatizadas em relação aos 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 desabilitar 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 nos conceitos de CSPM do Security Hub	Algumas descrições foram atualizadas e novos termos foram adicionados aos conceitos de CSPM do Security Hub.	21 de setembro de 2019
AWS Versão de disponibilidade geral do Security Hub CSPM	Atualizações de conteúdo para refletir as melhorias feitas no CSPM do Security Hub durante o período beta.	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 CSPM do AWS Security Hub.	15 de abril de 2019
versão beta do AWS Security Hub CSPM	Publicou a versão beta do Guia do Usuário do AWS Security Hub CSPM.	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.