Guia de implementação

Resposta de segurança automatizada na AWS

Resposta de segurança automatizada na AWS: Guia de implementação

Table of Contents

Aborde automaticamente as ameaças à segurança com ações predefinidas de resposta e remediação no AWS Security Hub

Este guia de implementação fornece uma visão geral da solução Automated Security Response on AWS, sua arquitetura e componentes de referência, considerações para planejar a implantação e etapas de configuração para implantar a solução Automated Security Response on AWS na nuvem da Amazon Web Services (AWS).

Use esta tabela de navegação para encontrar rapidamente respostas para estas perguntas:

Se você deseja...	Leia…
Conheça o custo da execução dessa solução	Custos
Entenda as considerações de segurança dessa solução	Segurança
Saiba como planejar cotas para essa solução	Cotas
Saiba quais regiões da AWS são compatíveis com essa solução	Regiões da AWS com suporte
Visualize ou baixe o CloudFormation modelo da AWS incluído nesta solução para implantar automaticamente os recursos de infraestrutura (a “pilha”) dessa solução	CloudFormation Modelos da AWS
Acessar o código-fonte e, opcionalmente, usar o AWS Cloud Development Kit (AWS CDK) para implantar a solução.	GitHub repositório

A evolução contínua da segurança exige etapas proativas para proteger os dados, o que pode tornar a reação das equipes de segurança difícil, cara e demorada. A solução Automated Security Response on AWS ajuda você a reagir rapidamente para resolver problemas de segurança

fornecendo respostas predefinidas e ações de remediação com base nos padrões de conformidade e nas melhores práticas do setor.

O Automated Security Response na AWS é uma solução da AWS que funciona com o AWS Security Hub para melhorar sua segurança e ajudar a alinhar suas cargas de trabalho às melhores práticas do pilar Well-Architected Security (0). SEC1 Essa solução torna mais fácil para os clientes do AWS Security Hub resolver descobertas de segurança comuns e melhorar sua postura de segurança na AWS.

Você pode selecionar playbooks específicos para implantar na sua conta principal do Security Hub. Cada manual contém as ações personalizadas necessárias, as funções do Identity and Access Management (IAM), EventBridge as regras da Amazon, os documentos de automação do AWS Systems Manager, as funções do AWS Lambda e as AWS Step Functions necessárias para iniciar um fluxo de trabalho de remediação em uma única conta da AWS ou em várias contas. As remediações funcionam no menu Ações no AWS Security Hub e permitem que usuários autorizados corrijam uma descoberta em todas as suas contas gerenciadas pelo AWS Security Hub com uma única ação. Por exemplo, você pode aplicar recomendações do Center for Internet Security (CIS) AWS Foundations Benchmark, um padrão de conformidade para proteger os recursos da AWS, para garantir que as senhas expirem em 90 dias e aplicar a criptografia dos registros de eventos armazenados na AWS.

> **Note**
>
> A remediação é destinada a situações emergentes que exigem ação imediata. Essa solução faz alterações para remediar descobertas somente quando iniciada por você por meio do console de gerenciamento do AWS Security Hub ou quando a remediação automatizada é habilitada usando a tabela do DynamoDB de configuração de remediação. Para reverter essas alterações, você deve colocar manualmente os recursos de volta em seu estado original.
>
> Ao remediar os recursos da AWS implantados como parte da CloudFormation pilha, esteja ciente de que isso pode causar um desvio. Quando possível, corrija os recursos da pilha modificando o código que define os recursos da pilha e atualizando a pilha. Para obter mais informações, consulte O que é deriva? no Guia do CloudFormation usuário da AWS.

O Automated Security Response na AWS inclui o manual de remediações para os padrões de segurança definidos como parte do seguinte:

- Centro de segurança na Internet (CIS) AWS Foundations Benchmark v1.2.0
- Referência do CIS AWS Foundations v1.4.0
- Referência do CIS AWS Foundations v3.0.0
- Melhores práticas de segurança da AWS Foundational (FSBP) v.1.0.0
- Padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS) v3.2.1
- Instituto Nacional de Padrões e Tecnologia (NIST) SP 800-53 Rev. 5

A solução também inclui um manual do Security Controls (SC) para o recurso consolidado de descobertas de controle do AWS Security Hub. Para obter mais informações, consulte Playbooks. Recomendamos usar o manual do SC junto com as descobertas de controle consolidadas no Security Hub.

Este guia de implementação discute considerações arquitetônicas e etapas de configuração para implantar a solução Automated Security Response on AWS na nuvem da AWS. Inclui links para CloudFormation modelos da AWS que iniciam, configuram e executam a computação, a rede, o armazenamento e outros serviços da AWS necessários para implantar essa solução na AWS, usando as melhores práticas de segurança e disponibilidade da AWS.

O guia é destinado a arquitetos, administradores e DevOps profissionais de infraestrutura de TI com experiência prática em arquitetura na nuvem da AWS.

Recursos e benefícios

O Automated Security Response na AWS fornece os seguintes recursos:

Corrija automaticamente as descobertas para controles específicos

Configure a solução para corrigir automaticamente as descobertas de controles específicos modificando a tabela do DynamoDB de configuração de remediação implantada na conta do administrador.

Gerencie remediações em várias contas e regiões a partir de um único local

A partir de uma conta de administrador do AWS Security Hub que está configurada como o destino de agregação das contas e regiões da sua organização, inicie uma remediação para uma descoberta em qualquer conta e região em que a solução esteja implantada.

Seja notificado sobre ações e resultados de remediação

Inscreva-se no tópico do Amazon SNS implantado pela solução para ser notificado quando as remediações forem iniciadas e se a correção foi bem-sucedida ou não.

Use a interface de usuário da Web para iniciar, visualizar e gerenciar remediações

Você terá a opção de ativar a interface de usuário da Web da solução ao implantar a pilha de administração, que fornecerá uma visão abrangente e fácil de usar para executar correções e visualizar todas as remediações anteriores realizadas pela solução.

Integre com sistemas de tickets como Jira ou ServiceNow

Para ajudar sua organização a reagir às correções (por exemplo, atualizar seu código de infraestrutura), essa solução pode enviar tickets para seu sistema externo de tíquetes.

Use AWSConfig correções nas partições da China GovCloud e da China

Algumas das correções incluídas na solução são repacotes de documentos de AWSConfig remediação de propriedade da AWS que estão disponíveis na partição comercial, mas não na China. GovCloud Implante essa solução para usar esses documentos nessas partições.

Estenda a solução com correções personalizadas e implementações do Playbook

A solução foi projetada para ser extensível e personalizável. Para especificar uma implementação alternativa de remediação, implante documentos de automação personalizados do AWS Systems Manager e funções do AWS IAM. Para oferecer suporte a um conjunto totalmente novo de controles que não é implementado pela solução, implante um Playbook personalizado.

Casos de uso

Imponha a conformidade com um padrão em todas as contas e regiões da sua organização

Implante o Playbook de acordo com um padrão (por exemplo, as melhores práticas de segurança da AWS Foundational) para poder usar as correções fornecidas. Inicie as correções de recursos de forma automática ou manual em qualquer conta e região em que a solução seja implantada para corrigir recursos que estão fora de conformidade.

Implemente correções ou playbooks personalizados para atender às necessidades de conformidade da sua organização

Use os componentes do Orchestrator fornecidos como uma estrutura. Crie correções personalizadas para lidar com out-of-compliance os recursos de acordo com as necessidades específicas da sua organização.

Conceitos e definições

Esta seção descreve os conceitos básicos e define a terminologia específica desta solução:

remediação, caderno de execução de remediação

Uma implementação de um conjunto de etapas que resolve uma descoberta. Por exemplo, uma correção para o controle Security Control (SC) Lambda.1 “As políticas da função Lambda devem proibir o acesso público” modificaria a política da função relevante do AWS Lambda para remover declarações que permitem acesso público.

caderno de controle

Um de um conjunto de documentos de automação do AWS Systems Manager (SSM) que o orquestrador usa para rotear uma remediação iniciada de um controle específico para o runbook de remediação correto. Por exemplo, as remediações para o SC Lambda.1 e o AWS Foundational Security Best Practices (FSBP) Lambda.1 são implementadas com o mesmo runbook de remediação. O orquestrador invoca o runbook de controle para cada controle, denominado ASR-AFSBP_Lambda.1 e ASR-SC_2.0.0_Lambda.1, respectivamente. Cada runbook de controle invoca o mesmo runbook de remediação, que nesse caso seria ASR-. RemoveLambdaPublicAccess

orquestrador

O Step Functions implantado pela solução que usa como entrada um objeto de busca do AWS Security Hub e invoca o runbook de controle correto na conta e região de destino. O orquestrador também notifica o tópico SNS da solução quando a remediação é iniciada e quando a correção é bem-sucedida ou falha.

padrão

Um grupo de controles definido por uma organização como parte de uma estrutura de conformidade. Por exemplo, um dos padrões suportados pelo AWS Security Hub e por essa solução é o AWS FSBP.

controle

Uma descrição das propriedades que um recurso deve ou não ter para estar em conformidade. Por exemplo, o controle AWS FSBP Lambda.1 afirma que as funções do AWS Lambda devem proibir o acesso público. Uma função que permite acesso público falharia nesse controle.

descobertas de controle consolidadas, controle de segurança, visualização de controles de segurança

Um recurso do AWS Security Hub que, quando ativado, exibe descobertas com seu controle consolidado, IDs em vez de IDs corresponder a um padrão específico. Por exemplo, os controles AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 e PCI-DSS v3.2.1 S3.1 são todos mapeados para o controle consolidado (SC) S3.2 “Os buckets do S3 devem proibir o acesso público de leitura”. Quando esse recurso está ativado, os runbooks SC são usados.

Administrador delegado do [Solution Web UI]

No contexto da interface de usuário da Web da solução, um administrador delegado é um usuário que foi convidado pelo administrador e tem acesso total para executar correções e visualizar o histórico de remediações. Esse usuário também pode visualizar e gerenciar outros usuários do Operador de Conta.

Operador de conta [Solution Web UI]

No contexto da interface de usuário da Web da solução, um operador de conta é um usuário convidado por um administrador ou administrador delegado para acessar a interface do usuário da Web da solução. Esse usuário está associado a uma lista de IDs de contas da AWS fornecidas em seu convite; ele só pode executar correções e visualizar o histórico de remediações no que diz respeito aos recursos dessas contas.

Para obter uma referência geral dos termos da AWS, consulte o glossário da AWS.

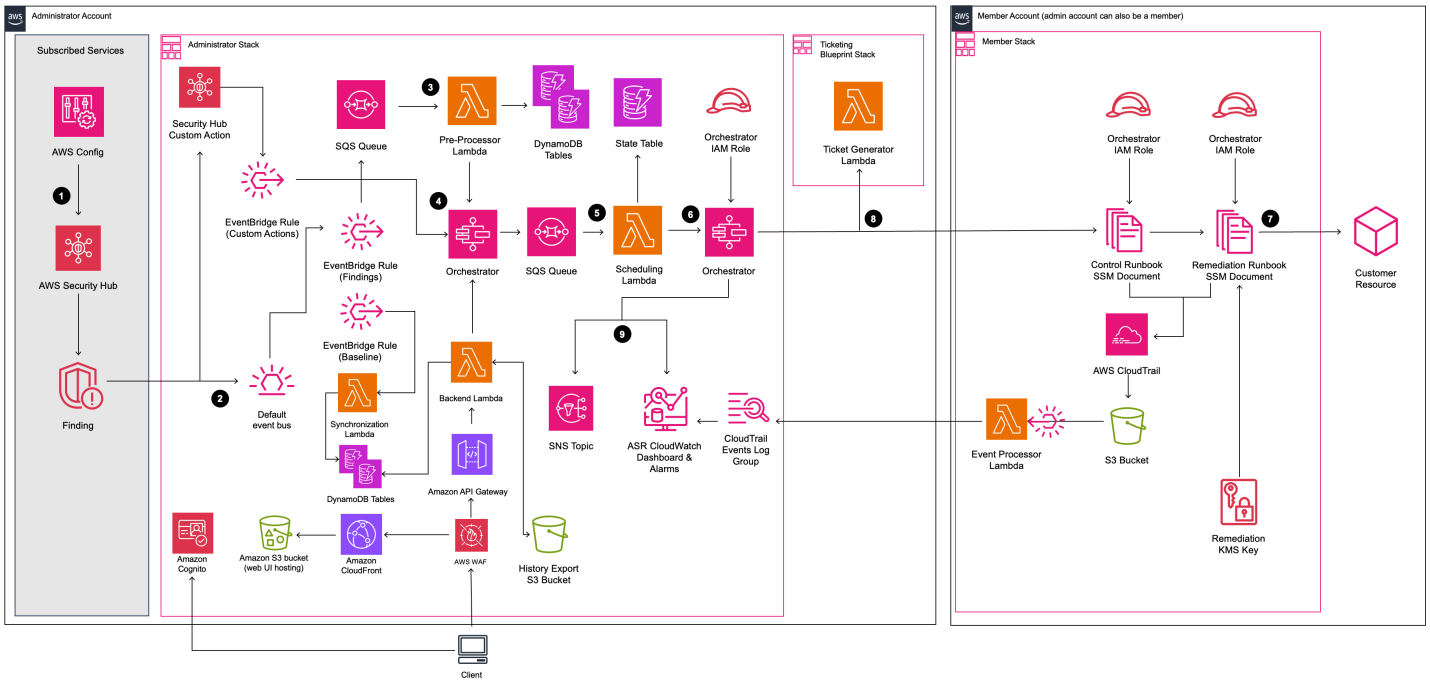
Visão geral da arquitetura

Esta seção fornece um diagrama de arquitetura de implementação de referência para os componentes implantados com essa solução.

Diagrama de arquitetura

A implantação dessa solução com os parâmetros padrão cria o seguinte ambiente na nuvem da AWS.

Resposta de segurança automatizada na arquitetura da AWS



> **Note**
>
> Os CloudFormation recursos da AWS são criados a partir de construções do AWS Cloud Development Kit (AWS CDK).

O fluxo de alto nível para os componentes da solução implantados com o CloudFormation modelo da AWS é o seguinte:

1. Detectar: o AWS Security Hub oferece aos clientes uma visão abrangente do estado de segurança da AWS. Isso os ajuda a medir seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança. Ele funciona coletando eventos e dados de outros serviços da AWS, como AWS Config, Amazon Guard Duty e AWS Firewall Manager. Esses eventos e dados são analisados de acordo com padrões de segurança, como o CIS AWS Foundations Benchmark. As exceções são declaradas como descobertas no console do AWS Security Hub. Novas descobertas são enviadas como EventBridge eventos da Amazon.
2. Ouça: EventBridge os eventos são emitidos pelo AWS Security Hub para cada descoberta criada ou modificada pelo serviço. O Automated Security Response on AWS (ASR) implanta duas EventBridge regras que escutam a localização de eventos gerados pelo AWS Security Hub:
   - EventBridge Regra de ação personalizada: escuta eventos de ações personalizadas emitidos pelo AWS Security Hub CSPM quando a ação personalizada “Remediar com ASR” é acionada por um usuário. O evento é encaminhado ao orquestrador para correção.
   - EventBridge Regra de descobertas: escuta todas as descobertas, eventos de criação ou atualização emitidos pelo AWS Security Hub e pelo AWS Security Hub CSPM. Esses eventos são encaminhados para a fila SQS do pré-processador para processamento adicional.
3. Iniciar: você pode iniciar as remediações manualmente ou configurá-las para serem executadas automaticamente. Para executar uma remediação manualmente, você pode usar a interface de usuário da Web implantada pela solução ou o recurso de ações personalizadas no AWS Security Hub CSPM. Depois de testes cuidadosos em um ambiente que não seja de produção, você também pode ativar correções automatizadas. Você pode ativar automações para remediações individuais — você não precisa ativar iniciações automáticas em todas as remediações. Para configurar as remediações para serem executadas automaticamente, consulte a página Habilitar remediações totalmente automatizadas.
4. Pré-remediação: na conta do administrador, o AWS Step Functions processa o evento de remediação e o prepara para ser agendado.
5. Cronograma: A solução invoca a função de agendamento do AWS Lambda para colocar o evento de remediação na tabela de estados do Amazon DynamoDB.
6. Orquestrar: na conta de administrador, o Step Functions usa funções entre contas do AWS Identity and Access Management (IAM). Step Functions invoca a remediação na conta do membro que contém o recurso que produziu a descoberta de segurança.
7. Remediar: um documento do AWS Systems Manager Automation na conta do membro executa a ação necessária para corrigir a descoberta no recurso de destino, como desativar o acesso público do Lambda.

Opcionalmente, você pode ativar o recurso Action Log nas pilhas de membros com o parâmetro EnableCloudTrailForASRActionLog. Esse recurso captura as ações realizadas pela solução em suas contas de membros e as exibe no CloudWatch painel da solução na Amazon.

8. (Opcional) Crie um ticket: se você usar o TicketGenFunctionNameparâmetro para ativar a emissão de tíquetes na pilha de administração, a solução invoca a função Lambda do gerador de tickets fornecida. Essa função Lambda cria um ticket em seu serviço de emissão de bilhetes após a correção ter sido executada com sucesso na conta do membro. Fornecemos pilhas para integração com o Jira e. ServiceNow
9. Notificar e registrar: o manual registra os resultados em um CloudWatch grupo de registros, envia uma notificação para um tópico do Amazon Simple Notification Service (Amazon SNS) e atualiza a descoberta do Security Hub. A solução mantém uma trilha de auditoria das ações nas notas de descoberta.

Considerações sobre o design do AWS Well-Architected

Essa solução foi projetada com as melhores práticas do AWS Well-Architected Framework, que ajuda os clientes a projetar e operar cargas de trabalho confiáveis, seguras, eficientes e econômicas na nuvem. Esta seção descreve como os princípios de design e as melhores práticas do Well-Architected Framework foram aplicados ao criar essa solução.

Excelência operacional

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- Recursos definidos como uso CloudFormation de IaC.
- Remediações implementadas com as seguintes características, sempre que possível:
  - Idempotência
  - Tratamento e emissão de relatórios de erros
  - Registro em log
  - Restaurando recursos para um estado conhecido em caso de falha

Segurança

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- IAM usado para autenticação e autorização.
- O escopo das permissões de função deve ser o mais restrito possível, embora, em muitos casos, essa solução exija permissões curinga para poder atuar em qualquer recurso.
- Para fins de segurança,

Confiabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de confiabilidade.

- O Security Hub continua criando descobertas se a causa subjacente da descoberta não for resolvida pela remediação.
- Os serviços de tecnologia sem servidor permitem que a solução seja escalada conforme necessário.

Eficiência de desempenho

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- Essa solução foi projetada para ser uma plataforma para você estender sem precisar implementar orquestração e permissões sozinho.

Otimização de custo

Esta seção descreve como arquitetamos essa solução usando os princípios e as práticas recomendadas do pilar de otimização do custo.

- Os serviços de tecnologia sem servidor permitem que você pague apenas pelo que usa.
- Use o nível gratuito para automação de SSM em todas as contas

Sustentabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de sustentabilidade.

- Os serviços de tecnologia sem servidor permitem aumentar a escala da solução verticalmente conforme necessário.

Detalhes de arquitetura

Esta seção descreve os componentes e os serviços da AWS que compõem essa solução e os detalhes da arquitetura sobre como esses componentes funcionam juntos.

Integração com o AWS Security Hub

A implantação da `automated-security-response-admin` pilha cria integração com o recurso de ação personalizada do AWS Security Hub CSPM. Quando os usuários do console CSPM do AWS Security Hub clicam em Ações > Remediar com ASR, as descobertas selecionadas são enviadas EventBridge e acionam o fluxo de trabalho de remediação.

As permissões entre contas e os runbooks do AWS Systems Manager devem ser implantados em todas as contas do AWS Security Hub (administrador e membro) usando os modelos e. `automated-security-response-member.template` `automated-security-response-member-roles.template` CloudFormation Para obter mais informações, consulte Playbooks. Esse modelo permite a remediação automática na conta de destino.

Os usuários podem configurar remediações totalmente automatizadas por controle usando o Amazon DynamoDB. Essa opção ativa a remediação totalmente automática das descobertas assim que elas são reportadas ao AWS Security Hub. Por padrão, as iniciações automáticas são desativadas. Essa opção pode ser alterada a qualquer momento após a instalação, modificando a tabela do DynamoDB de configuração de remediação.

Remediação entre contas

O Automated Security Response na AWS usa funções entre contas para trabalhar em contas primárias e secundárias usando funções entre contas. Essas funções são implantadas nas contas dos membros durante a instalação da solução. Cada remediação é atribuída a uma função individual. O processo de remediação na conta principal recebe permissão para assumir a função de remediação na conta que requer remediação. A remediação é realizada pelos runbooks do AWS Systems Manager executados na conta que requer remediação.

Manuais

Um conjunto de remediações é agrupado em um pacote chamado manual. Os playbooks são instalados, atualizados e removidos usando os modelos dessa solução. Para obter informações

sobre as correções suportadas em cada manual, consulte Guia do desenvolvedor → Manuais. Atualmente, essa solução oferece suporte aos seguintes manuais:

- Security Control, um manual alinhado ao recurso de descobertas de controle consolidadas do AWS Security Hub, publicado em 23 de fevereiro de 2023.

  > **Important**
  >
  > Quando as descobertas de controle consolidadas estão habilitadas no Security Hub, esse é o único manual que deve ser ativado na solução.

- Os benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 1.2.0, publicada em 18 de maio de 2018.
- Os benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 1.4.0, publicada em 9 de novembro de 2022.
- Os benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 3.0.0, publicados em 13 de maio de 2024.
- AWS Foundational Security Best Practices (FSBP) versão 1.0.0, publicada em março de 2021.
- Padrões de Segurança de Dados do Setor de Cartões de Pagamento (PCI-DSS) versão 3.2.1, publicada em maio de 2018.
- Instituto Nacional de Padrões e Tecnologia (NIST) versão 5.0.0, publicada em novembro de 2023.

Depois de implantar as CloudFormation pilhas da solução, os playbooks estão prontos para uso imediato — nenhuma configuração adicional é necessária para permitir correções para os padrões de segurança listados acima.

Registro em log centralizado

O Automated Security Response na AWS registra em um único grupo de CloudWatch registros, SO0111-ASR. Esses registros contêm registros detalhados da solução para solução de problemas e gerenciamento da solução.

Notificações

Essa solução usa um tópico do Amazon Simple Notification Service (Amazon SNS) para publicar os resultados da remediação. Você pode usar assinaturas deste tópico para ampliar os recursos da solução. Por exemplo, você pode enviar notificações por e-mail e atualizar os tickets de problemas.

- SO0111-ASR_Topic — Usado para enviar informações gerais e mensagens de erro relacionadas às correções executadas.
- SO0111-ASR_Alarm_Topic — Usado para notificar quando um dos alarmes da solução é acionado, indicando que a solução não está funcionando conforme o esperado.

Serviços da AWS nesta solução

A solução usa os seguintes serviços. Os serviços principais são necessários para usar a solução, e os serviços de suporte conectam os serviços principais.

Serviço da AWS	Description
Amazon EventBridge	Núcleo. EventBridge as regras são usadas para ouvir e acionar eventos emitidos pelo AWS Security Hub e pelo AWS Security Hub CSPM.
AWS IAM	Principal. Implanta várias funções para permitir correções em diferentes recursos.
AWS Lambda	Principal. Implanta várias funções lambda que serão usadas pelo orquestrador de funções step para corrigir problemas. Serve como back-end para a interface de usuário da Web da solução integrada ao API Gateway.
AWS Security Hub	Principal. Oferece aos clientes uma visão abrangente do estado de segurança da AWS.
AWS Step Functions	Principal. Implanta um orquestrador que invocará os documentos de remediação com as chamadas de API do AWS Systems Manager.

Serviço da AWS	Description
AWS Systems Manager	Principal. Implanta documentos de automação do System Manager que contêm a lógica de remediação a ser executada pela solução. Usa o Parameter Store para manter os metadados da solução e as definições de configuração.
AWS DynamoDB	Principal. Armazena a última correção executada em cada conta e região para otimizar o agendamento das remediações. Armazena descobertas geradas pelo AWS Security Hub e pelo AWS Security Hub CSPM. Armazena metadados de remediação e configuração da solução. Armazena dados para usuários que acessam a interface de usuário da Web da solução.
AWS CloudTrail	Suporte. Registra as alterações que a solução faz em seus recursos da AWS e as exibe em um CloudWatch painel.
Amazon CloudWatch	Suporte. Implanta grupos de registros que os diferentes playbooks usarão para registrar os resultados. Coleta métricas para exibir em um painel personalizado com alarmes.
Amazon Simple Notification Service	Suporte. Implanta tópicos do SNS que recebem uma notificação após a conclusão da remediação.

Serviço da AWS	Description
AWS SQS	Suporte. Auxilia no agendamento de remediaçõ es para que a solução possa executar remediações em paralelo. Armazena em buffer as execuções do Lambda usando EventSource mapeamentos Lambda.
AWS Key Management Service	Suporte. Usado para criptografar dados para remediações.
AWS Config	Suporte. Registra todos os recursos para uso com o AWS Security Hub.
Amazon S3	Suporte. Armazena o histórico de remediação exportado e os dados de registro. Hospeda a interface de usuário da Web da solução como um aplicativo de página única (SPA).
Amazon CloudFront	Suporte. Fornece a interface de usuário da Web da solução
Amazon API Gateway	Suporte. Cria a API REST da solução para oferecer suporte à interface do usuário.
AWS WAF	Suporte. Protege a interface de usuário da Web da solução.
Amazon Cognito	Suporte. Usado para autenticar e autorizar o acesso à interface de usuário da Web da solução.

Planeje a implantação

Esta seção descreve o custo, a segurança da rede, as regiões suportadas da AWS, as cotas e outras considerações antes da implantação da solução.

Custo

Você é responsável pelo custo dos serviços da AWS usados para executar essa solução.

A partir desta revisão, os custos mensais estimados são:

- Pequena implantação (10 contas, 1 região) - EUA East/N. Virginia): Approximately $14.70 for 300 remediations/month
- Implantação média (100 contas, 1 região - EUA) East/N. Virginia): Approximately $106.40 for 3,000 remediations/month
- Grande implantação (1.000 contas, 10 regiões): aproximadamente USD 7.360,00 para 30.000 remediações/mês

> **Important**
>
> Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada serviço da AWS usado nesta solução.

> **Note**
>
> Muitos serviços da AWS incluem um nível gratuito — um valor básico do serviço que os clientes podem usar gratuitamente. Os custos reais podem ser maiores ou menores do que os exemplos de preços fornecidos.

Recomendamos criar um orçamento por meio do Explorador de Custos da AWS para ajudar a gerenciar os custos. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada serviço da AWS usado nesta solução.

Tabela de custos da amostra

O custo total para executar essa solução depende dos seguintes fatores:

- O número de contas de membros do AWS Security Hub
- O número de remediações ativas invocadas automaticamente
- A frequência da remediação

Essa solução usa os seguintes componentes da AWS, que incorrem em um custo com base na sua configuração. Exemplos de preços são fornecidos para organizações de pequeno, médio e grande porte.

Serviço	Nível gratuito	Preços [USD]
AWS Systems Manager Automation — Contagem de etapas	Sem nível gratuito	Cada etapa básica é cobrada a 0,002 USD por etapa. Para automações de várias contas, todas as etapas, incluindo aquelas executadas em qualquer conta secundária, são contadas somente na conta de origem.
AWS Systems Manager Automation — Duração da etapa	Sem nível gratuito	Cada etapa `aws:executeScript` da ação é cobrada em 0,00003 USD por cada segundo.
AWS Systems Manager Automation — Armazenamento	Sem nível gratuito	0,046 USD por GB por mês
AWS Systems Manager Automation — Transferência de dados	Sem nível gratuito	0,900 USD por GB transferido (para contas cruzadas ou) out-of-Region

Serviço	Nível gratuito	Preços [USD]
AWS Security Hub CSPM — Verificações de segurança	Sem nível gratuito	Os primeiros 100.000 checks/account/Region/month custam $0,0010 por cheque Os próximos 400.000 checks/account/Region/month custam $0,0008 por cheque Mais de 500.000 checks/account/Region/month custam $0,0005 por cheque
AWS Security Hub CSPM — Encontrando eventos de ingestão	Os primeiros 10.000 events/account/Region/month são gratuitos. Encontrar eventos de ingestão associados às verificações de segurança do Security Hub.	Mais de 10.000 events/account/Region/month custam $0,00003 por evento
Amazon CloudWatch - Métricas	Métricas básicas de monitoramento (com frequência de 5 minutos) 10 Métricas de monitoramento detalhadas (com frequência de 1 minuto) 1 1 milhão de solicitações de API (não aplicável a GetMetricData, GetInsightRuleReport e GetMetricWidgetImage)	As primeiras 10.000 métricas custam 0,30 USD por mês As próximas 240.000 métricas custam 0,10 USD por mês As próximas 750.000 métricas custam 0,05 USD por mês Mais de 1.000.000 de métricas custam 0,02 USD por mês As chamadas de API custam 0,01 USD por 1.000 solicitações
Amazon CloudWatch - Painel	3 painéis para até 50 métricas por mês	$3,00 por painel por mês

Serviço	Nível gratuito	Preços [USD]
Amazon CloudWatch - Alarmes	10 métricas de alarme (não aplicáveis a alarmes de alta resolução)	A resolução padrão (60 segundos) custa 0,10 USD por métrica de alarme A alta resolução (10 segundos) custa 0,30 USD por métrica de alarme A detecção de anomalias com resolução padrão custa 0,30 USD por alarme A detecção de anomalias de alta resolução custa $0,90 por alarme O composto custa $0,50 por alarme
Amazon CloudWatch - Coleção de registros	Dados de 5 GB (ingestão, armazenamento de arquivos e dados digitalizados por consultas do Logs Insights)	0,50 USD por GB
Amazon CloudWatch - Armazenamento de registros	Dados de 5 GB (ingestão, armazenamento de arquivos e dados digitalizados por consultas do Logs Insights)	0,005 USD por GB de dados digitalizados
AWS Lambda — Solicitações	1 milhão de solicitações gratuitas por mês	0,20 USD por 1 milhão de solicitações

Serviço	Nível gratuito	Preços [USD]
AWS Lambda - Duração	400.000 GB-segundos de tempo de computação por mês	0,0000166667 USD por cada GB-segundo. O preço da duração depende da quantidade de memória que você aloca para sua função. Você pode alocar qualquer quantidade de memória para sua função entre 128 MB e 10.240 MB, em incrementos de 1 MB.
AWS Step Functions — Transições de estado	4.000 transições de estado gratuitas por mês	0,025 USD por 1.000 transições de estado posteriores
Amazon EventBridge	Todos os eventos de mudança de estado publicados pelos serviços da AWS são gratuitos	Eventos personalizados custam 1,00 USD/milhão de eventos personalizados publicados Eventos de terceiros (SaaS) custam 1,00 USD/milhão de eventos publicados Eventos entre contas custam 1,00 USD/milhão de eventos enviados entre contas
Amazon SNS	Os primeiros 1 milhão de solicitações do Amazon SNS por mês são gratuitas	0,50 USD por 1 milhão de solicitações posteriores
Amazon SQS	Os primeiros 1 milhão de solicitações do Amazon SQS por mês são gratuitas	0,40 USD por 1 milhão a 100 bilhões de solicitações posteriores

Serviço	Nível gratuito	Preços [USD]
Amazon DynamoDB	Os primeiros 25 GB de armazenamento são gratuitos	2,00 USD por 1 milhão de leituras e gravações consistentes a partir de então
AWS Key Management Service	20.000 solicitações/mês	1,00 USD por 1 chave KMS. 0,03 USD por 10.000 solicitações de API. Para chaves KMS que você gira automaticamente ou sob demanda, a primeira e a segunda rotação da chave adicionam $1/mês (rateado por hora) em custo. Observação: essa solução inclui otimizações de cache do KMS (chaves de bucket do S3, reutilização de chaves de dados SQS em 60 minutos, armazenamento em cache de 5 minutos do Secrets Manager) que reduzem as chamadas à API KMS em aproximadamente 70%.
Amazon Cognito	No nível Essentials, os primeiros 10.000 usuários ativos mensais são gratuitos. Observação: esse nível gratuito é de 50 usuários ativos mensais quando os usuários se autenticam via IdP externo (SAML/OIDC).	0,015 USD por usuário ativo mensal com mais de 10.000 usuários.

Serviço	Nível gratuito	Preços [USD]
Amazon CloudFront	O nível gratuito inclui 1 TB de transferência de dados e 10.000.000 de solicitações HTTP ou HTTPS por mês.	(US/Canada/Mexico) Os primeiros 9 TB custam 0,085 USD por mês. Os próximos 40 TB custam 0,080 USD por mês. 0,0075 USD por solicitação HTTP. 0,0100 USD por solicitação HTTPS.
Amazon S3	Sem nível gratuito	Os primeiros 50 TB custam 0,023 USD por GB por mês. 0,005 USD por 1.000 solicitações PUT, COPY, POST, LIST. 0,0004 USD por 1.000 solicitações GET, SELECT e todas as outras.
Amazon API Gateway	1 milhão de chamadas de API REST nos primeiros 12 meses de uso.	$3,50 por milhão para as primeiras 333 milhões de chamadas de API.

Otimização de custos do KMS

Desde a versão 3.1.0, essa solução inclui otimizações de cache do KMS que reduzem os custos de operação criptográfica em aproximadamente 70%

- Chaves de bucket do S3: reduz as GenerateDataKey chamadas do KMS para operações de criptografia do S3
- Reutilização da chave de dados SQS: período de cache de 60 minutos para criptografia de mensagens
- Secrets Manager Caching: TTL de 5 minutos em funções Lambda

Impacto no desempenho: essas otimizações melhoram a latência em 10 a 15 ms para operações do S3 e fluxos de trabalho completos, ao mesmo tempo em que reduzem os custos, sem degradação da taxa de transferência.

Exemplos de preços (por mês)

Exemplo 1:300 remediações por mês

- 10 contas, 1 região
- 30 remediações por account/Region/month
- 500 descobertas do Security Hub processadas por account/Region/month
- UI da Web desativada
- Registro de ações desativado
- Custo total $14,70 por mês

Serviço	Suposições	Cobranças mensais [USD]
AWS Systems Manager Automation	Etapas: ~4 etapas* 300 remediações* 0,002 USD = 2,40 USD Duração: 10s * 300 remediações* 0,00003 USD = 0,09 USD	$2,49
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	0,50 USD por GB	< 0,01 US$
AWS Lambda — Solicitações	300 remediações * 7 solicitações = 2.100 solicitações 5.000 descobertas * 1 solicitação = 5.000 solicitações	$0,00142

Serviço	Suposições	Cobranças mensais [USD]
	0,20 USD/ 1.000.000 de solicitações = 0,0000002 USD por solicitação	
AWS Lambda - Duração	(512MB de memória) 4.000 ms * 300 remediações * 0,0000000083 USD = 0,00996 USD 449 ms * 5.000 descobertas * 0,0000000083 USD = 0,0186 USD	$0,029
AWS Step Functions	19 transições de estado* 300 remediações = 5.700 0,025 USD* (5.700/1.000) transições de estado = 0,14 USD	0,14 US$
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0

Serviço	Suposições	Cobranças mensais [USD]
AWS Key Management Service	1 chave* 10 contas* 1 região* $1 = $10 (Criptografar/descriptografar solicitações de API) (300 remediações * 2 solicitações) + (5.000 descobertas * 4 solicitações) = 20.600 solicitações Com o cache KMS: 20.600 * 0,30 = 6.180 solicitações 0,03 USD por 10.000 solicitações ⇒ 0,03 USD* (6.180/ 10.000) = 0,02 USD	$10,02
Amazon DynamoDB	2,00 USD* 1.000.000 de leitura e gravação = 2,00 USD (Tabela de resultados) 15 MB * 10 contas * 1 região = 150 MB (Tabela de histórico) 10 MB * 10 contas * 1 região = 100 MB 0,25 USD por GB por mês * 0,25 GB = 0,0625 USD	$2.0625
Amazon SQS	0,40 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,50 USD* (600/ 1.000.000 de notificações) = 0,0003 USD	$0,0003

Serviço	Suposições	Cobranças mensais [USD]
Amazon CloudWatch - Métricas	(Métricas aprimoradas desativadas) 0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (300 chamadas de API de métricas de colocação/ 1.000) = 0,003 USD	$2,10
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00
Amazon CloudWatch - Alarmes	(Métricas aprimoradas desativadas) 0,10 USD* 4 alarmes = 0,40 US$	$0,40
Amazon CloudWatch - X-Ray Traces	300 remediações * 7 solicitaç ões = 2.100 invocações do Lambda 5.000 descobertas * 1 solicitaç ão = 5.000 invocações Lambda 0,000005 USD por rastreame nto * 7.100 traços = 0,0355 USD	$0,0355
Total		$14,70

Exemplo 2:300 correções por mês (interface de usuário da Web ativada)

- 10 contas, 1 região
- 30 remediações por account/Region/month

- 5.000 descobertas do Security Hub processadas por account/Region/month
- UI da Web ativada
- Registro de ações desativado
- Custo total: $36,35 por mês

Serviço	Suposições	Cobranças mensais [USD]
AWS Systems Manager Automation	Etapas: ~4 etapas* 300 remediações* 0,002 USD = 2,40 USD Duração: 10s * 300 remediações* 0,00003 USD = 0,09 USD	$2,49
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	0,50 USD por GB	< 0,01 US$
AWS Lambda — Solicitações	300 remediações * 7 solicitações = 2.100 solicitações 5.000 descobertas * 1 solicitação = 5.000 solicitações 0,20 USD/ 1.000.000 de solicitações = 0,0000002 USD por solicitação	$0,00142
AWS Lambda - Duração	(512MB de memória) 4.000 ms * 300 remediações * 0,0000000083 USD = 0,00996 USD	$0,029

Serviço	Suposições	Cobranças mensais [USD]
	449 ms * 5.000 descobertas * 0,0000000083 USD = 0,0186 USD	
AWS Step Functions	19 transições de estado* 300 remediações = 5.700 0,025 USD* (5.700/1.000) transições de estado = 0,14 USD	0,14 US$
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	1 chave* 10 contas* 1 região* $1 = $10 (Criptografar/descriptografar solicitações de API) (300 remediações * 2 solicitações) + (5.000 descobertas * 4 solicitações) = 20.600 solicitações 0,03 USD por 10.000 solicitações ⇒ 0,03 USD* (20.600/10.000) = 0,06 USD	$10,06

Serviço	Suposições	Cobranças mensais [USD]
Amazon DynamoDB	2,00 USD* 1.000.000 de leitura e gravação = 2,00 USD (Tabela de resultados) 15 MB * 10 contas * 1 região = 150 MB (Tabela de histórico) 10 MB * 10 contas * 1 região = 100 MB 0,25 USD por GB por mês * 0,25 GB = 0,0625 USD	$2.0625
Amazon SQS	0,40 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,50 USD* (600/ 1.000.000 de notificações) = 0,0003 USD	$0,0003
Amazon CloudWatch - Métricas	(Métricas aprimoradas desativadas) 0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (300 chamadas de API de métricas de colocação/ 1.000) = 0,003 USD	$2,10
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00
Amazon CloudWatch - Alarmes	(Métricas aprimoradas desativadas) 0,10 USD* 4 alarmes = 0,40 US$	$0,40

Serviço	Suposições	Cobranças mensais [USD]
Amazon CloudWatch - X-Ray Traces	300 remediações * 7 solicitações = 2.100 invocações do Lambda 5.000 descobertas * 1 solicitação = 5.000 invocações Lambda 0,000005 USD por rastreamento * 7.100 traços = 0,0355 USD	$0,0355
Amazon Cognito	(Nível Essentials) 500 usuários ativos mensais	$0
Amazon CloudFront	Transferência regional de dados para a origem (por GB) = 0,020 USD Transferência regional de dados para a Internet (por GB) = 0,085 USD Solicite preços para todos os métodos HTTP (por 10.000) = 0,0075 USD	$0,1125

Serviço	Suposições	Cobranças mensais [USD]
Amazon S3	(Hospedagem de interface do usuário) 0,023 USD por GB * 0,002 GB = 0,000046 USD (Exportação de histórico) 0,023 USD por GB * 0,50 GB = 0,0125 USD 0,0004 USD por 1.000 solicitações GET	0,0125 USD
AWS WAF	1 Web ACL = 5,00 USD por mês 7 regras * 1,00 USD por regra = 7,00 USD	$12
Amazon API Gateway	3,50 USD por milhão de chamadas de API REST	$3,50
Total		$36,35

Exemplo 3:3.000 remediações por mês

- 100 contas, 1 região
- 30 remediações por account/Region/month
- 500 descobertas do Security Hub processadas por account/Region/month
- UI da Web desativada
- Registro de ações desativado
- Custo total: $106,40 por mês

Serviço	Suposições	Cobranças mensais [USD]
AWS Systems Manager Automation	Etapas: ~4 etapas* 3.000 remediações* 0,002 USD = 24,00 USD Duração: 10s * 3.000 remediações* 0,00003 USD = 0,90 USD	$24,90
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	0,50 USD por GB	< 0,01 US$
AWS Lambda — Solicitações	3.000 remediações * 7 solicitações = 2.100 solicitações 50.000 descobertas * 1 solicitação = 50.000 solicitações 0,20 USD/ 1.000.000 de solicitações = 0,0000002 USD por solicitação	$0,01
AWS Lambda - Duração	(512MB de memória) 4.000 ms * 3.000 remediações * 0,0000000083 USD = 0,0996 USD 449 ms * 50.000 descobertas * 0,0000000083 USD = 0,186 USD	0,29 US$

Serviço	Suposições	Cobranças mensais [USD]
AWS Step Functions	19 transições de estado* 3.000 remediações = 57.000 transições de estado de 0,025 USD* (57.000/1.000) = 1,425 USD	$1.425
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	1 chave * 100 contas* 1 região* $1 = $100 (Criptografar/descriptografar solicitações de API) (3.000 remediações * 2 solicitações) + (50.000 descobertas * 4 solicitações) = 206.000 solicitações Com o cache KMS: 206.000 * 0,30 = 61.800 solicitações 0,03 USD por 10.000 solicitaç ões ⇒ 0,03 USD* (61.800/ 10.000) = 0,185 USD	$100.185

Serviço	Suposições	Cobranças mensais [USD]
Amazon DynamoDB	2,00 USD* 1.000.000 de leitura e gravação = 2,00 USD (Tabela de resultados) 15 MB * 100 contas * 1 região = 1.500 MB (Tabela de histórico) 10 MB * 100 contas * 1 região = 1.000 MB 0,25 USD por GB por mês * 2,5 GB = 0,625 USD	$2.625
Amazon SQS	0,40 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,50 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	(Métricas aprimoradas desativadas) 0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (3.000/ 1.000) chamadas de API de métricas de colocação = 0,03 USD	$2,13
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00
Amazon CloudWatch - Alarmes	0,10 USD* 4 alarmes = 0,40 US$	$0,40

Serviço	Suposições	Cobranças mensais [USD]
Amazon CloudWatch - X-Ray Traces	3.000 remediações * 7 solicitações = 2.100 invocações do Lambda 50.000 descobertas * 1 solicitação = 50.000 invocações do Lambda 0,000005 USD por rastreamento * 52.100 traços = 0,2605 USD	$0.2605
Total		$106,40

Exemplo 4:30.000 remediações por mês

- 1.000 contas, 10 regiões
- 30 remediações por account/Region/month
- 500 descobertas do Security Hub processadas por account/Region/month
- UI da Web desativada
- Registro de ações desativado
- Custo total: $7.360,00 por mês

Serviço	Suposições	Cobranças mensais [USD]
AWS Systems Manager Automation	Etapas: ~4 etapas* 30.000 remediações* 0,002 USD = 240,00 USD Duração: 10s * 30.000 remediações* 0,00003 USD = 9,00 USD	$249,00

Serviço	Suposições	Cobranças mensais [USD]
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	0,50 USD por GB	< 0,01 US$
AWS Lambda — Solicitações	30.000 remediações * 7 solicitações = 210.000 solicitações 5.000.000 de descobertas * 1 solicitação = 5.000.000 de solicitações 0,20 USD/ 1.000.000 de solicitações = 0,0000002 USD por solicitação	$1.042
AWS Lambda - Duração	(512MB de memória) 4.000 ms * 30.000 remediaçõ es * 0,0000000083 USD = 0,996 USD 449 ms * 5.000.000 de descobertas * 0,0000000083 USD = 18,63 USD	$19,63
AWS Step Functions	19 transições de estado* 30.000 remediações = 570.000 transições de estado de 0,025 USD* (570.000/1.000) = 14,25 US$	$14,25

Serviço	Suposições	Cobranças mensais [USD]
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	(1 chave) $1 * 1.000 contas* 10 regiões = $10.000 (Criptografar/descriptografar solicitações de API) (30.000 remediações * 2 solicitações) + (5.000.000 de descobertas * 4 solicitações) = 20.060.000 solicitações Com o cache KMS: 20.060.000 * 0,30 = 6.018.000 solicitações 0,03 USD por 10.000 solicitações ⇒ 0,03 USD* (6.018.000/10.000) = 18,05 USD	$10.018,05
Amazon DynamoDB	$2,00 * (10.000.000 de leitura e gravação/ 1.000.000) = $20,00 (Tabela de resultados) 15 MB * 1000 contas * 10 regiões = 150 GB (Tabela de histórico) 10 MB * 1000 contas * 10 regiões = 100 GB 0,25 USD por GB por mês * 250 GB = 62,50 USD	$82,50

Serviço	Suposições	Cobranças mensais [USD]
Amazon SQS	0,40 USD* (5.060.000 solicitações/1.000.000) = 2,024 USD	$2.024
Amazon SNS	0,000005 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	(Métricas aprimoradas desativadas) 0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (30.000/1.000) chamadas de API de métricas de colocação = 0,30 USD	$2,40
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00
Amazon CloudWatch - Alarmes	(Métricas aprimoradas desativadas) 0,10 USD* 4 alarmes = 0,40 US$	$0,40
Amazon CloudWatch - X-Ray Traces	30.000 remediações * 7 solicitações = 210.000 invocações do Lambda 5.000.000 de descobertas * 1 solicitação = 5.000.000 de invocações Lambda 0,000005 USD por rastreamento * 5.210.000 traços = 26,05 USD	$26,05
Total		$7.360,00

Exemplo 5:30.000 correções por mês (interface de usuário da Web ativada)

- 1.000 contas, 10 regiões
- 30 remediações por account/Region/month
- 500 descobertas do Security Hub processadas por account/Region/month
- UI da Web ativada
- Registro de ações desativado
- Custo total: $7.380,10 por mês

Serviço	Suposições	Cobranças mensais [USD]
AWS Systems Manager Automation	Etapas: ~4 etapas* 30.000 remediações* 0,002 USD = 240,00 USD Duração: 10s * 30.000 remediações* 0,00003 USD = 9,00 USD	$249,00
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	0,50 USD por GB	< 0,01 US$
AWS Lambda — Solicitações	30.000 remediações * 7 solicitações = 210.000 solicitações 5.000.000 de descobertas * 1 solicitação = 5.000.000 de solicitações 0,20 USD/ 1.000.000 de solicitações = 0,0000002 USD por solicitação	$1.042

Serviço	Suposições	Cobranças mensais [USD]
AWS Lambda - Duração	(512MB de memória) 4.000 ms * 30.000 remediaçõ es * 0,0000000083 USD = 0,996 USD 449 ms * 5.000.000 de descobertas * 0,0000000083 USD = 18,63 USD	$19,63
AWS Step Functions	19 transições de estado* 30.000 remediações = 570.000 transições de estado de 0,025 USD* (570.000/1.000) = 14,25 US$	$14,25
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0

Serviço	Suposições	Cobranças mensais [USD]
AWS Key Management Service	(1 chave) $1 * 1.000 contas* 10 regiões = $10.000 (Criptografar/descriptografar solicitações de API) (30.000 remediações * 2 solicitações) + (5.000.000 de descobertas * 4 solicitações) = 20.060.000 solicitações Com o cache KMS: 20.060.000 * 0,30 = 6.018.000 solicitações 0,03 USD por 10.000 solicitações ⇒ 0,03 USD* (6.018.000/10.000) = 18,05 USD	$10.018,05
Amazon DynamoDB	$2,00 * (10.000.000 de leitura e gravação/ 1.000.000) = $20,00 (Tabela de resultados) 15 MB * 1000 contas * 10 regiões = 150 GB (Tabela de histórico) 10 MB * 1000 contas * 10 regiões = 100 GB 0,25 USD por GB por mês * 250 GB = 62,50 USD	$82,50
Amazon SQS	0,40 USD* (5.060.000 solicitações/1.000.000) = 2,024 USD	$2.024

Serviço	Suposições	Cobranças mensais [USD]
Amazon SNS	0,000005 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	(Métricas aprimoradas desativadas) 0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (30.000/1.000) chamadas de API de métricas de colocação = 0,30 USD	$2,40
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00
Amazon CloudWatch - Alarmes	(Métricas aprimoradas desativadas) 0,10 USD* 4 alarmes = 0,40 US$	$0,40
Amazon CloudWatch - X-Ray Traces	30.000 remediações * 7 solicitações = 210.000 invocações do Lambda 5.000.000 de descobertas * 1 solicitação = 5.000.000 de invocações Lambda 0,000005 USD por rastreamento * 5.210.000 traços = 26,05 USD	$26,05
Amazon Cognito	(Nível Essentials) 5.000 usuários ativos mensais	$0

Serviço	Suposições	Cobranças mensais [USD]
Amazon CloudFront	Transferência regional de dados para a origem (por GB) = 0,020 USD Transferência regional de dados para a Internet (por GB) = 0,085 USD Solicite preços para todos os métodos HTTP (por 10.000) = 0,0075 USD	$0,1125
Amazon S3	(Hospedagem de interface do usuário) 0,023 USD por GB * 0,002 GB = 0,000046 USD (Exportação de histórico) 0,023 USD por GB * 100 GB = 2,30 USD 0,0004 USD por 1.000 solicitações GET * 5.000 solicitações = 2,00 USD	$4,30
AWS WAF	1 Web ACL = 5,00 USD por mês 7 regras * 1,00 USD por regra = 7,00 USD	$12
Amazon API Gateway	3,50 USD por milhão de chamadas de API REST	$3,50
Total		$7.380,10

> **Important**
>
> Custos de rotação de chaves do KMS O AWS Key Management Service (KMS) alterna automaticamente as chaves gerenciadas pelo cliente uma vez por ano quando a rotação está ativada. Cada rotação tem um custo de $1,00 por chave por ano. Por exemplo, com 1.000 contas em uma única região, isso resulta em um adicional de $1000/ano (1 rotação × 1000 chaves × $1,00).

Custo adicional para recursos opcionais

Esta seção identifica os custos adicionais associados aos recursos opcionais dessa solução.

CloudWatch Métricas aprimoradas

Se você selecionar `yes` o EnableEnhancedCloudWatchMetricsparâmetro ao implantar a pilha de administração, a solução criará duas métricas personalizadas e um alarme para cada ID de controle. O custo depende do número de controles IDs que você está remediando. Na tabela a seguir, presumimos que você esteja remediando todos os 96 controles diferentes IDs por mês, para determinar o limite superior dos custos.

Serviço	Pressupostos 96 IDs control* 2 = 192 métricas personali zadas	Cobranças mensais [USD]
Amazon CloudWatch - Métricas	0,30 USD* 192 métricas personalizadas = 57,60 USD	$57,60
Amazon CloudWatch - Alarmes	0,10 USD* 96 alarmes = 9,60 US$	$9,60
Total		$67,20

CloudTrail Registro de ações

Em cada conta de membro para a qual você ativa o recurso Action Log, as soluções criam uma CloudTrail trilha para registrar todos os eventos de gerenciamento de gravação. Uma função Lambda filtra eventos não relacionados à solução. Isso significa que o custo está relacionado ao número total

de eventos de gerenciamento em sua conta, pois os eventos não relacionados à solução ainda são capturados pela trilha e processados pela função Lambda.

Para a tabela a seguir, presumimos 150.000 eventos de gerenciamento por mês na conta. O custo real depende da atividade real do evento de gerenciamento em sua conta.

Serviço	Suposições	Cobranças mensais [USD]
AWS CloudTrail	150.000 * $2,00/100.000 = $3,00	$3,00
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB por segundo 3.750 * 0,0000166667 USD = custo de tempo de computação de 0,0625 USD 0,15 * 0,20 USD = custo de solicitação de 0,03 USD 0,0625 USD + 0,03 USD = custo total do Lambda de 0,0952 USD	$0,0925
Total		$3,09 por conta de membro

Segurança

Quando você cria sistemas na infraestrutura da AWS, as responsabilidades de segurança são compartilhadas entre você e a AWS. Esse modelo compartilhado reduz sua carga operacional porque a AWS opera, gerencia e controla os componentes, incluindo o sistema operacional do host, a camada de virtualização e a segurança física das instalações nas quais os serviços operam. Para obter mais informações sobre a segurança da AWS, visite a AWS Cloud Security.

Política de segurança do API Gateway

Se você optar por ativar a interface de usuário da Web da solução, uma API REST do API Gateway será implantada junto com a CloudFormation pilha de administração, que serve como back-end para

todas as operações na interface do usuário da Web. A API REST implantada pela solução usa a política de segurança TLS padrão para o API Gateway, que é regional`TLS-1-0`. APIs

No entanto, depois de implantar a CloudFormation pilha Admin, você pode optar por personalizar a API REST da solução adicionando uma política de segurança TLS mais restritiva. Por exemplo, você pode escolher a opção de `TLS_1_2 security policy` restringir o tráfego usando TLSv1 .2 ou TLSv1 .3. Você pode encontrar a API REST da solução no console do API Gateway abaixo do nome AutomatedSecurityResponseApi.

Para escolher uma política de segurança para a API REST da solução, você deve primeiro configurar um nome de domínio personalizado. Para obter mais informações, consulte Nome de domínio personalizado para REST público APIs no API Gateway.

Para obter mais informações sobre como adicionar uma política de segurança à sua API REST, consulte Escolha uma política de segurança para seu domínio personalizado da API REST no API Gateway no guia do API Gateway.

Perfis do IAM

As funções do AWS Identity and Access Management (IAM) permitem que os clientes atribuam políticas e permissões de acesso granulares a serviços e usuários na nuvem da AWS. Essa solução cria funções do IAM que concedem às funções automatizadas da solução acesso para realizar ações de remediação dentro de um conjunto restrito de permissões específicas para cada remediação.

A função Step da conta de administrador é atribuída à função SO0111-ASR-Orchestrator-Admin . Somente essa função pode assumir o SO0111-Orchestrator-Member em cada conta de membro. Cada função de remediação permite que a função de membro seja transmitida ao serviço AWS Systems Manager para executar runbooks de remediação específicos. Os nomes das funções de remediação começam com SO0111, seguidos por uma descrição correspondente ao nome do runbook de remediação. Por exemplo, SO0111-Remove VPCDefault SecurityGroupRules é a função do runbook de remediação ASR-Remove. VPCDefault SecurityGroupRules

Regiões da AWS compatíveis

Important

A ativação de recursos opcionais na solução pode reduzir a lista de regiões com suporte para implantação. Em outras palavras, a lista abaixo se aplica somente aos componentes principais da solução. Por exemplo, se você optar por habilitar a interface de usuário da Web,

não poderá implantar a solução em GovCloud regiões, pois não CloudFront é suportada nos GovCloud (EUA), em novembro de 2025.

Nome da região	Código da região
Leste dos EUA (Ohio)	us-east-2
Leste dos EUA (Norte da Virgínia)	us-east-1
Oeste dos EUA (Norte da Califórnia)	us-west-1
Oeste dos EUA (Oregon)	us-west-2
África (Cidade do Cabo)	af-south-1
Ásia-Pacífico (Hong Kong)	ap-east-1
Ásia-Pacífico (Hyderabad)	ap-south-2
Ásia-Pacífico (Jacarta)	ap-southeast-3
Ásia-Pacífico (Melbourne)	ap-southeast-4
Ásia-Pacífico (Mumbai)	ap-south-1
Ásia-Pacífico (Osaka)	ap-northeast-3
Ásia-Pacífico (Seul)	ap-northeast-2
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Ásia-Pacífico (Tóquio)	ap-northeast-1
Canadá (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Irlanda)	eu-west-1

Nome da região	Código da região
Europa (Londres)	eu-west-2
Europa (Milão)	eu-south-1
Europa (Paris)	eu-west-3
Europa (Espanha)	eu-south-2
Europa (Estocolmo)	eu-north-1
Europa (Zurique)	eu-central-2
Oriente Médio (Barém)	me-south-1
Oriente Médio (Emirados Árabes Unidos)	me-central-1
América do Sul (São Paulo)	sa-east-1
AWS GovCloud (Leste dos EUA)	us-gov-east-1
AWS GovCloud (Oeste dos EUA)	us-gov-west-1
China (Pequim)	cn-north-1
China (Ningxia)	cn-northwest-1
Israel (Tel Aviv)	il-central-1
Oeste do Canadá (Calgary)	ca-west-1
México (Cidade do México)	mx-central-1
Ásia-Pacífico (Tailândia)	ap-southeast-7
Ásia-Pacífico (Malásia)	ap-southeast-5

> **Note**
>
> Qualquer nova região da AWS não listada pode ser suportada por meio da implantação local, mas não da implantação com um clique.

Cotas

Service quotas, ou limites, representam o máximo de recursos ou operações de serviço permitidos em uma conta AWS.

Cotas para serviços da AWS nesta solução

Verifique se você tem cota suficiente para cada um dos serviços implementados nessa solução. Para obter mais informações, consulte as cotas de serviços da AWS.

Use os links a seguir para acessar a página desse serviço. Para visualizar as cotas de serviço de todos os serviços da AWS na documentação sem trocar de página, veja as informações na página de endpoints e cotas do serviço no PDF.

CloudFormation Cotas da AWS

Sua conta da AWS tem CloudFormation cotas da AWS que você deve conhecer ao lançar a pilha nesta solução. Ao compreender essas cotas, você pode evitar erros de limitação que o impediriam de implantar essa solução com êxito. Para obter mais informações, consulte as CloudFormation cotas da AWS no Guia do CloudFormation usuário da AWS.

CloudWatch Cotas da AWS

Sua conta da AWS tem CloudWatch cotas da AWS vinculadas às políticas de CloudWatch recursos, que permitem apenas 10 políticas de recursos por região por conta. Isso não pode ser solicitado para aumentar a cota. Consulte Cotas de CloudWatch registros da AWS no Guia do usuário da AWS CloudWatch . Antes da implantação, verifique seu uso atual para garantir que você não ultrapasse esse limite ao implantar a solução.

AWS Organizations

As funções Lambda da solução fazem chamadas para a API do AWS Organizations para buscar o alias da conta atual para incluir nas mensagens publicadas no tópico SNS da solução. Isso permite

que nomes de contas legíveis por humanos sejam visíveis nas notificações da solução para fins de depuração e rastreamento.

O AWS Organizations impõe limites à frequência com que os clientes podem invocar seus endpoints de API. Se você achar que a solução está excedendo os limites definidos para sua conta, você pode desativar o recurso que busca e exibe o alias da conta.

Para fazer isso, navegue até a função Lambda chamada `SO0111-ASR-sendNotifications` localizada na região e na conta em que você implantou a pilha Admin. Em seguida, localize a variável de ambiente chamada `DISABLE_ACCOUNT_ALIAS_LOOKUP` e altere o valor de “Falso” para “Verdadeiro”. O campo de alias da conta nas notificações da solução agora será “Desconhecido”, mas isso não afetará a funcionalidade da solução.

Implantação do AWS Security Hub

A implantação e a configuração do AWS Security Hub são um pré-requisito para essa solução. Para obter mais informações sobre como configurar o AWS Security Hub CSPM, consulte Configurar o AWS Security Hub CSPM no Guia do usuário do AWS Security Hub. Essa solução também é compatível com o AWS Security Hub (versão não CSPM). Para obter mais informações sobre como configurar o AWS Security Hub, consulte Habilitando o Security Hub.

No mínimo, você deve ter um Security Hub ativo configurado em sua conta principal. Você pode implantar essa solução na mesma conta (e região da AWS) da conta principal do Security Hub. Em cada conta primária e secundária do Security Hub, você também deve implantar o modelo de membro que concede AssumeRole permissões ao AWS Step Functions da solução para executar runbooks de remediação na conta.

Empilhamento versus implantação StackSets

Um conjunto de pilhas permite criar pilhas em contas da AWS em todas as regiões da AWS usando um único modelo da AWS CloudFormation . A partir da versão 1.4, essa solução oferece suporte à implantação de conjuntos de pilhas dividindo os recursos com base em onde e como eles são implantados. Clientes com várias contas, especialmente aqueles que usam o AWS Organizations, podem se beneficiar do uso de conjuntos de pilhas para implantação em várias contas. Isso reduz o esforço necessário para instalar e manter a solução. Para obter mais informações sobre StackSets, consulte Como usar a AWS CloudFormation StackSets.

Implante a solução

> **Important**
>
> Se o recurso de descobertas de controle consolidado estiver ativado no Security Hub, ative somente o manual do Security Control (SC) ao implantar essa solução. Se o recurso não estiver ativado, habilite somente os playbooks para os padrões de segurança habilitados no Security Hub. Por padrão, as descobertas de controles consolidadas estarão ativadas se você tiver habilitado o CSPM do Security Hub a partir de 23 de fevereiro de 2023, inclusive.

Essa solução usa CloudFormation modelos e pilhas da AWS para automatizar sua implantação. Os CloudFormation modelos especificam os recursos da AWS incluídos nessa solução e suas propriedades. A CloudFormation pilha provisiona os recursos descritos nos modelos.

Para que a solução funcione, três modelos devem ser implantados. Primeiro, decida onde implantar os modelos e, em seguida, decida como implantá-los.

Essa visão geral descreverá os modelos e como decidir onde e como implantá-los. As próximas seções terão instruções mais detalhadas para implantar cada pilha como uma pilha ou. StackSet

Decidindo onde implantar cada pilha

Os três modelos serão chamados pelos seguintes nomes e conterão os seguintes recursos:

- Pilha de administração: função de etapa do orquestrador, regras de eventos e ação personalizada do Security Hub.
- Pilha de membros: documentos de automação SSM de remediação.
- Pilha de funções dos membros: funções do IAM para remediações.

A pilha de administração deve ser implantada uma vez, em uma única conta e em uma única região. Ele deve ser implantado na conta e na região que você configurou como destino de agregação das descobertas do Security Hub para sua organização. Se quiser usar o recurso Action Log para monitorar eventos de gerenciamento, você deve implantar a pilha Admin na conta de gerenciamento da sua organização ou em uma conta de administrador delegado.

A solução opera com base nas descobertas do Security Hub, portanto, não poderá operar nas descobertas de uma conta e região específicas se essa conta ou região não tiver sido configurada para agregar descobertas na conta e região do administrador do Security Hub.

> **Important**
>
> Se você estiver usando o AWS Security Hub (não CSPM), você é responsável por garantir que suas contas membros integradas ao AWS Security Hub CSPM também estejam integradas ao AWS Security Hub (não CSPM). As regiões agregadas no AWS Security Hub CSPM também devem corresponder às regiões agregadas no AWS Security Hub (não CSPM).

Por exemplo, uma organização tem contas operando em regiões `us-east-1` e`us-west-2`, com a conta `111111111111` como administrador delegado do Security Hub, na regiãous-east-1. Contas `222222222222` e `333333333333` devem ser contas de membros do Security Hub para a conta `111111111111` de administrador delegado. Todas as três contas devem ser configuradas para agregar descobertas `us-west-2` de a. `us-east-1` A pilha de administração deve ser implantada na conta`111111111111`. `us-east-1`

Para obter mais detalhes sobre como encontrar a agregação, consulte a documentação das contas de administrador delegado do Security Hub e da agregação entre regiões.

A pilha de administradores deve concluir a implantação antes de implantar as pilhas de membros para que uma relação de confiança possa ser criada das contas dos membros para a conta do hub.

A pilha de membros deve ser implantada em todas as contas e regiões nas quais você deseja corrigir as descobertas. Isso pode incluir a conta de administrador delegado do Security Hub na qual você implantou anteriormente o ASR Admin Stack. Os documentos de automação devem ser executados nas contas dos membros para usar o nível gratuito da automação SSM.

Usando o exemplo anterior, se você quiser corrigir as descobertas de todas as contas e regiões, a pilha de membros deve ser implantada nas três contas (`111111111111222222222222`, e`333333333333`) e nas duas regiões (`us-east-1`e). `us-west-2`

A pilha de funções dos membros deve ser implantada em todas as contas, mas contém recursos globais (funções do IAM) que só podem ser implantados uma vez por conta. Não importa em qual região você implanta a pilha de funções de membro, então, para simplificar, sugerimos implantá-la na mesma região em que a pilha de administradores está implantada.

Usando o exemplo anterior, sugerimos implantar a pilha de funções de membro em todas as três contas (111111111111,222222222222, e333333333333) em. us-east-1

Decidindo como implantar cada pilha

As opções para implantar uma pilha são

- CloudFormation StackSet (permissões autogerenciadas)
- CloudFormation StackSet (permissões gerenciadas pelo serviço)
- CloudFormation Pilha

StackSets com permissões gerenciadas por serviços são as mais convenientes porque não exigem a implantação de suas próprias funções e podem ser implantadas automaticamente em novas contas na organização. Infelizmente, esse método não é compatível com pilhas aninhadas, que usamos tanto na pilha Admin quanto na pilha de membros. A única pilha que pode ser implantada dessa forma é a pilha de funções dos membros.

Lembre-se de que, ao implantar em toda a organização, a conta de gerenciamento da organização não é incluída. Portanto, se você quiser corrigir as descobertas na conta de gerenciamento da organização, deverá implantar nessa conta separadamente.

A pilha de membros deve ser implantada em todas as contas e regiões, mas não pode ser implantada usando StackSets permissões gerenciadas por serviços porque contém pilhas aninhadas. Por isso, sugerimos implantar essa pilha StackSets com permissões autogerenciadas.

A pilha Admin é implantada apenas uma vez, portanto, pode ser implantada como uma CloudFormation pilha simples ou StackSet com permissões autogerenciadas em uma única conta e região.

Descobertas de controle consolidadas

As contas em sua organização podem ser configuradas com o recurso consolidado de descobertas de controle do Security Hub ativado ou desativado. Consulte os resultados do controle consolidado no Guia do usuário do AWS Security Hub.

> **Important**
>
> Quando esse recurso está ativado, você deve usar a versão 2.0.0 ou posterior da solução e ativar o manual “SC” (Controle de Segurança) nas pilhas Admin e Member. Essas

pilhas implantam os documentos de automação necessários para trabalhar com controle consolidado. IDs Você não precisa implantar pilhas para padrões individuais (como o AWS FSBP) ao usar descobertas de controle consolidadas.

Implantação na China

A solução oferece suporte à implantação nas regiões da China, no entanto, você deve usar os seguintes botões de inicialização para implantação com um clique nas regiões da China, em vez dos botões de inicialização fornecidos em outras seções deste guia. O uso dos botões “Launch Solution” fornecidos nas próximas seções deste guia não funcionará se você estiver implantando em regiões da China. Você ainda pode baixar os modelos de qualquer link de bucket do S3 e implantar as pilhas fazendo o upload do arquivo de modelo.

- automated-security-response-admin.modelo:

Launch solution

- automated-security-response-member-roles.template:

Launch solution

- automated-security-response-member.modelo:

Launch solution

GovCloud Implantação (EUA)

A solução oferece suporte à implantação em regiões GovCloud (EUA), no entanto, você deve usar os seguintes botões de inicialização para implantação com um clique nas regiões GovCloud (EUA), em vez dos botões de inicialização fornecidos em outras seções deste guia. O uso dos botões “Launch Solution” fornecidos nas próximas seções deste guia não funcionará se você estiver implantando em

regiões GovCloud (EUA). Você ainda pode baixar os modelos de qualquer link de bucket do S3 e implantar as pilhas fazendo o upload do arquivo de modelo.

- automated-security-response-admin.modelo:

- automated-security-response-member-roles.template:

- automated-security-response-member.modelo:

CloudFormation Modelos da AWS

automa

security-response-admin.template - Use esse modelo para iniciar a solução Automated Security Response na AWS. O modelo instala os principais componentes da solução, uma pilha aninhada para os logs do AWS Step Functions e uma pilha aninhada para cada padrão de segurança que você escolher ativar.

Os serviços usados incluem Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 e AWS Systems Manager.

Suporte à conta de administrador

Os modelos a seguir são instalados na conta de administrador do AWS Security Hub para ativar os padrões de segurança que você deseja apoiar. Você pode escolher qual dos seguintes modelos instalar ao instalar `automated-security-response-admin.template` o.

automated-security-response-orchestrator-log.template - Cria um grupo de CloudWatch registros para a função de etapa do orquestrador.

automated-security-response-webui-nested-stack.template - Cria os recursos para oferecer suporte à interface de usuário da Web da solução.

AFSBPStack.template — Regras das melhores práticas de segurança da AWS Foundational v1.0.0.

CIS120Stack.template - benchmarks do CIS Amazon Web Services Foundations, regras v1.2.0.

CIS140Stack.template - benchmarks do CIS Amazon Web Services Foundations, regras v1.4.0.

CIS300Stack.template - benchmarks do CIS Amazon Web Services Foundations, regras v3.0.0.

PCI321Stack.template - regras do PCI-DSS v3.2.1.

NISTStack.template - Instituto Nacional de Padrões e Tecnologia (NIST), regras da v5.0.0.

SCStack.template - Regras do Security Controls v2.0.0.

Funções dos membros

automa

security-response-member-roles.template - Define as funções de remediação necessárias em cada conta membro do AWS Security Hub.

Contas-membros

automa

security-response-member.template — Use esse modelo depois de configurar a solução principal para instalar os runbooks e permissões de automação do AWS Systems Manager em cada uma das suas contas de membro do AWS Security Hub (incluindo a conta de administrador). Esse modelo permite que você escolha quais playbooks padrão de segurança instalar.

Ele `automated-security-response-member.template` instala os seguintes modelos com base em suas seleções:

automated-security-response-remediation-runbooks.template - Código de remediação comum usado por um ou mais dos padrões de segurança.

AFSBPMemberStack.template — Configurações, permissões e runbooks de remediação das melhores práticas de segurança da AWS Foundational v1.0.0.

CIS120MemberStack.template - benchmarks do CIS Amazon Web Services Foundations, configurações, permissões e runbooks de remediação da versão 1.2.0.

CIS140MemberStack.template - benchmarks do CIS Amazon Web Services Foundations, configurações, permissões e runbooks de remediação da versão 1.4.0.

CIS300MemberStack.template - benchmarks do CIS Amazon Web Services Foundations, configurações, permissões e runbooks de remediação da versão 3.0.0.

PCI321MemberStack.template - Configurações, permissões e runbooks de remediação do PCI-DSS v3.2.1.

NISTMemberStack.template - Instituto Nacional de Padrões e Tecnologia (NIST), configurações, permissões e runbooks de remediação v5.0.0.

SCMemberStack.template - Configurações de controle de segurança, permissões e runbooks de remediação.

automated-security-response-member-cloudtrail.template - Usado no recurso Action Log para rastrear e auditar atividades de serviços.

Integração do sistema de tickets

Use um dos modelos a seguir para integrar-se ao seu sistema de emissão de bilhetes.

View template

JiraBlu

- Implante se você usa o Jira como seu sistema de tíquetes.

View template

Service

- Implante se você usar ServiceNow como seu sistema de emissão de bilhetes.

Se você quiser integrar um sistema de tíquetes externo diferente, você pode usar qualquer uma dessas pilhas como modelo para entender como implementar sua própria integração personalizada.

Implantação automatizada - StackSets

> **Note**
>
> Recomendamos implantar com StackSets. No entanto, para implantações em uma única conta ou para fins de teste ou avaliação, considere a opção de implantação de pilhas.

Antes de iniciar a solução, analise a arquitetura, os componentes da solução, a segurança e as considerações de design discutidas neste guia. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em seu AWS Organizations.

Tempo de implantação: aproximadamente 30 minutos por conta, dependendo StackSet dos parâmetros.

Pré-requisitos

O AWS Organizations ajuda você a gerenciar e governar centralmente seu ambiente e seus recursos multicontas da AWS. StackSets funcionam melhor com o AWS Organizations.

Se você já implantou a versão 1.3.x ou anterior dessa solução, deverá desinstalar a solução existente. Para obter mais informações, consulte Atualizar a solução.

Antes de implantar essa solução, revise sua implantação do AWS Security Hub:

- Deve haver uma conta de administrador delegada do Security Hub em sua organização da AWS.
- O Security Hub deve ser configurado para agregar descobertas em todas as regiões. Para obter mais informações, consulte Agregando descobertas entre regiões no Guia do usuário do AWS Security Hub.
- Você deve ativar o Security Hub para sua organização em cada região em que você usa a AWS.

Esse procedimento pressupõe que você tenha várias contas usando o AWS Organizations e tenha delegado uma conta de administrador do AWS Organizations e uma conta de administrador do AWS Security Hub.

Observe que essa solução funciona com o AWS Security Hub e o AWS Security Hub CSPM.

Visão geral da implantação

> **Note**
>
> StackSets a implantação dessa solução usa uma combinação de serviços gerenciados e autogerenciados. StackSets O autogerenciado StackSets deve ser usado atualmente, pois eles usam aninhados StackSets, que ainda não são compatíveis com o gerenciamento de serviços. StackSets

Implemente o a StackSets partir de uma conta de administrador delegado em seu AWS Organizations.

Planejamento

Use o formulário a seguir para ajudar na StackSets implantação. Prepare seus dados e, em seguida, copie e cole os valores durante a implantação.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Opcional) Etapa 0: implantar a pilha de integração de tíquetes

- Se você pretende usar o recurso de emissão de tíquetes, primeiro implante a pilha de integração de tíquetes em sua conta de administrador do Security Hub.
- Copie o nome da função Lambda dessa pilha e forneça-o como entrada para a pilha de administração (consulte a Etapa 1).

Etapa 1: iniciar a pilha de administração na conta de administrador delegada do Security Hub

- Usando um modelo autogerenciado StackSet, execute o CloudFormation modelo `automated-security-response-admin.template` da AWS em sua conta de administrador do AWS Security Hub na mesma região do administrador do Security Hub. Esse modelo usa pilhas aninhadas.
- Escolha quais padrões de segurança instalar. Por padrão, somente SC é selecionado (recomendado).
- Escolha um grupo de registros existente do Orchestrator para usar. Selecione `Yes` se `SO0111-ASR- Orchestrator` já existe em uma instalação anterior.
- Escolha se deseja ativar a interface de usuário da Web da solução. Se você optar por ativar esse recurso, também deverá inserir um endereço de e-mail para receber uma função de administrador.
- Selecione suas preferências para coletar CloudWatch métricas relacionadas à integridade operacional da solução.

Para obter mais informações sobre autogerenciamento StackSets, consulte Conceder permissões autogerenciadas no Guia CloudFormation do usuário da AWS.

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

Aguarde a etapa 1 para concluir a implantação, pois o modelo na etapa 2 faz referência às funções do IAM criadas pela etapa 1.

- Usando um serviço gerenciado StackSet, execute o CloudFormation modelo da `automated-security-response-member-roles.template` AWS em uma única região em cada conta em seu AWS Organizations.
- Escolha instalar esse modelo automaticamente quando uma nova conta ingressar na organização.
- Insira o ID da conta de administrador do AWS Security Hub.
- Insira um valor para o `namespace` que será usado para evitar conflitos de nomes de recursos com uma implantação anterior ou simultânea na mesma conta. Insira uma sequência de até 9 caracteres alfanuméricos minúsculos.

Etapa 3: Inicie a pilha de membros em cada conta de membro e região do AWS Security Hub

- Usando o autogerenciamento StackSets, lance o CloudFormation modelo `automated-security-response-member.template` da AWS em todas as regiões em que você tem

recursos da AWS em todas as contas da sua organização da AWS gerenciadas pelo mesmo administrador do Security Hub.

> **Note**
>
> Até que o StackSets suporte gerenciado por serviços esteja aninhado, você deve executar essa etapa para todas as novas contas que ingressarem na organização.

- Escolha quais playbooks do Security Standard instalar.
- Forneça o nome de um grupo de CloudTrail registros (usado por algumas correções).
- Insira o ID da conta de administrador do AWS Security Hub.
- Insira um valor para o `namespace` que será usado para evitar conflitos de nomes de recursos com uma implantação anterior ou simultânea na mesma conta. Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Isso deve corresponder ao `namespace` valor que você selecionou para a pilha de funções de membro. Além disso, o valor do namespace não precisa ser exclusivo por conta de membro.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tíquetes

1. Se você pretende usar o recurso de emissão de tíquetes, inicie primeiro a respectiva pilha de integração.
2. Escolha as pilhas de integração fornecidas para o Jira ou ServiceNow use-as como um modelo para implementar sua própria integração personalizada.

   Para implantar a pilha do Jira:

   a. Insira um nome para sua pilha.

   b. Forneça o URI para sua instância do Jira.

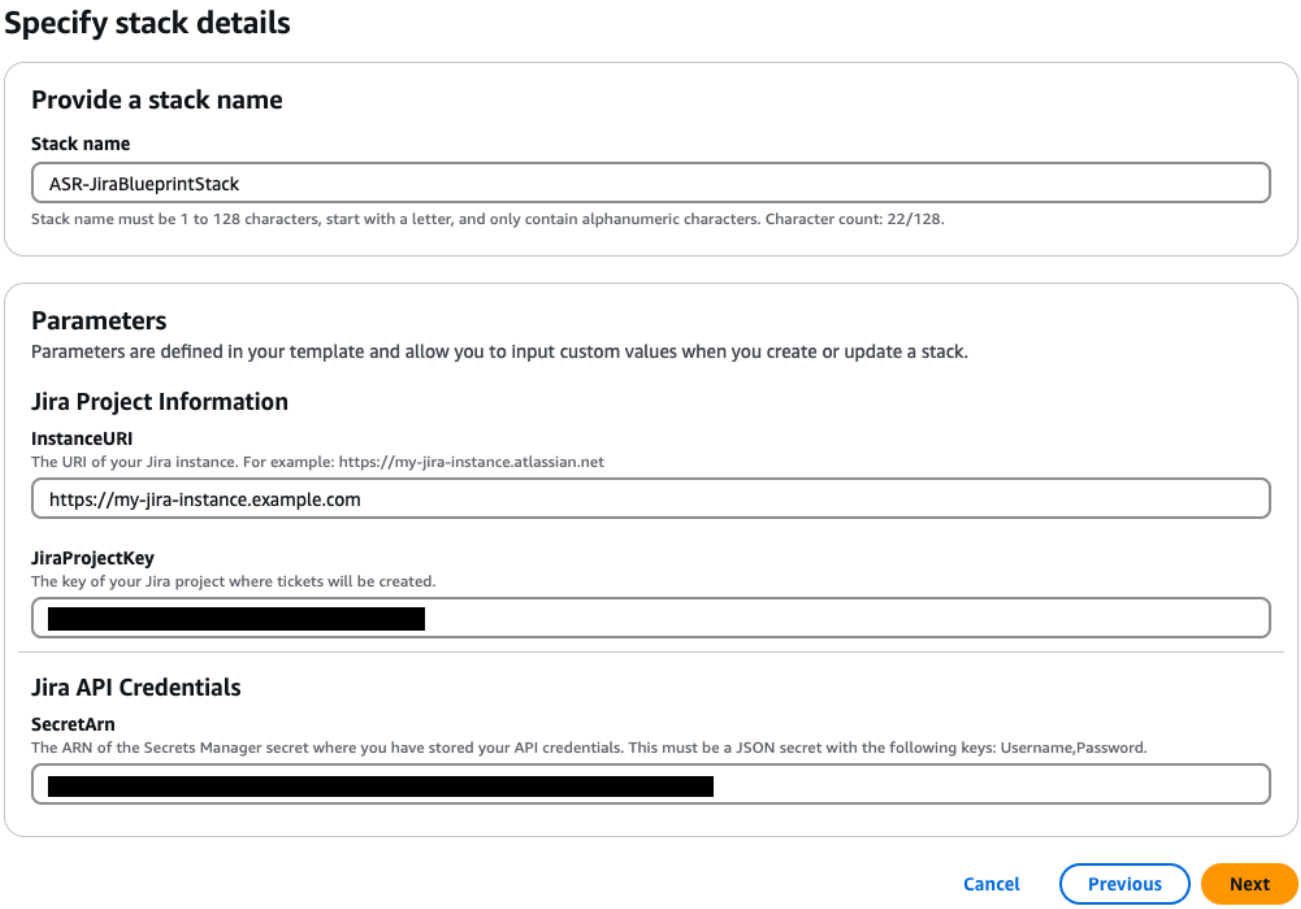
   c. Forneça a chave do projeto do Jira para o qual você deseja enviar tickets.

   d. Crie um novo segredo de valor-chave no Secrets Manager que contenha seu Jira e. `Username` `Password`

   > **Note**
   >
   > Você pode optar por usar uma chave de API do Jira no lugar de sua senha, fornecendo seu nome de usuário como `Username` e sua chave de API como o. `Password`

e. Adicione o ARN desse segredo como entrada na pilha.

Forneça um nome de pilha, informações do projeto Jira e credenciais da API Jira.



Configuração do Jira Field:

Depois de implantar a pilha do Jira, você pode personalizar os campos do ticket do Jira definindo a variável de `JIRA_FIELDS_MAPPING` ambiente na função Lambda. Essa string JSON substitui os campos padrão do ticket do Jira e deve seguir a estrutura dos campos da API do Jira.

Valores padrão quando `JIRA_FIELDS_MAPPING` está vazio ou os campos não são especificados:

- prioridade: `{"id": "3"}` (Prioridade média)
- tipo de problema: **`{"id": "10006"}`** (Tarefa)
- accountId: recuperado automaticamente usando o endpoint da API `GET /rest/api/2/myself`

Exemplo de configuração com campos personalizados:

```
{
  "reporter": {"accountId": "123456:494dcbff-1b80-482c-a89d-56ae81c145a4"},
  "priority": {"id": "1"},
  "issuetype": {"id": "10006"},
  "assignee": {"accountId": "123456:another-user-id"},
  "customfield_10001": "custom value"
}
```

Campo IDs comum do Jira:

- Prioridade IDs: 1 (mais alta), 2 (alta), 3 (média), 4 (baixa), 5 (mais baixa)
- ID do tipo de problema: varia de acordo com o projeto do Jira (por exemplo, 10006 para Task)
- ID da conta: Formato `123456:494dcbff-1b80-482c-a89d-56ae81c145a4`

Você pode encontrar seu campo IDs e sua conta do Jira IDs usando a API REST do Jira:

- `GET /rest/api/2/myself`para ID da conta
- `GET /rest/api/2/priority`para prioridade IDs
- `GET /rest/api/2/project/{projectKey}`para tipo de problema IDs

Para obter mais informações, consulte o formato POST do problema da API REST v2 do Jira.

Para implantar a ServiceNow pilha:

f. Insira um nome para sua pilha.

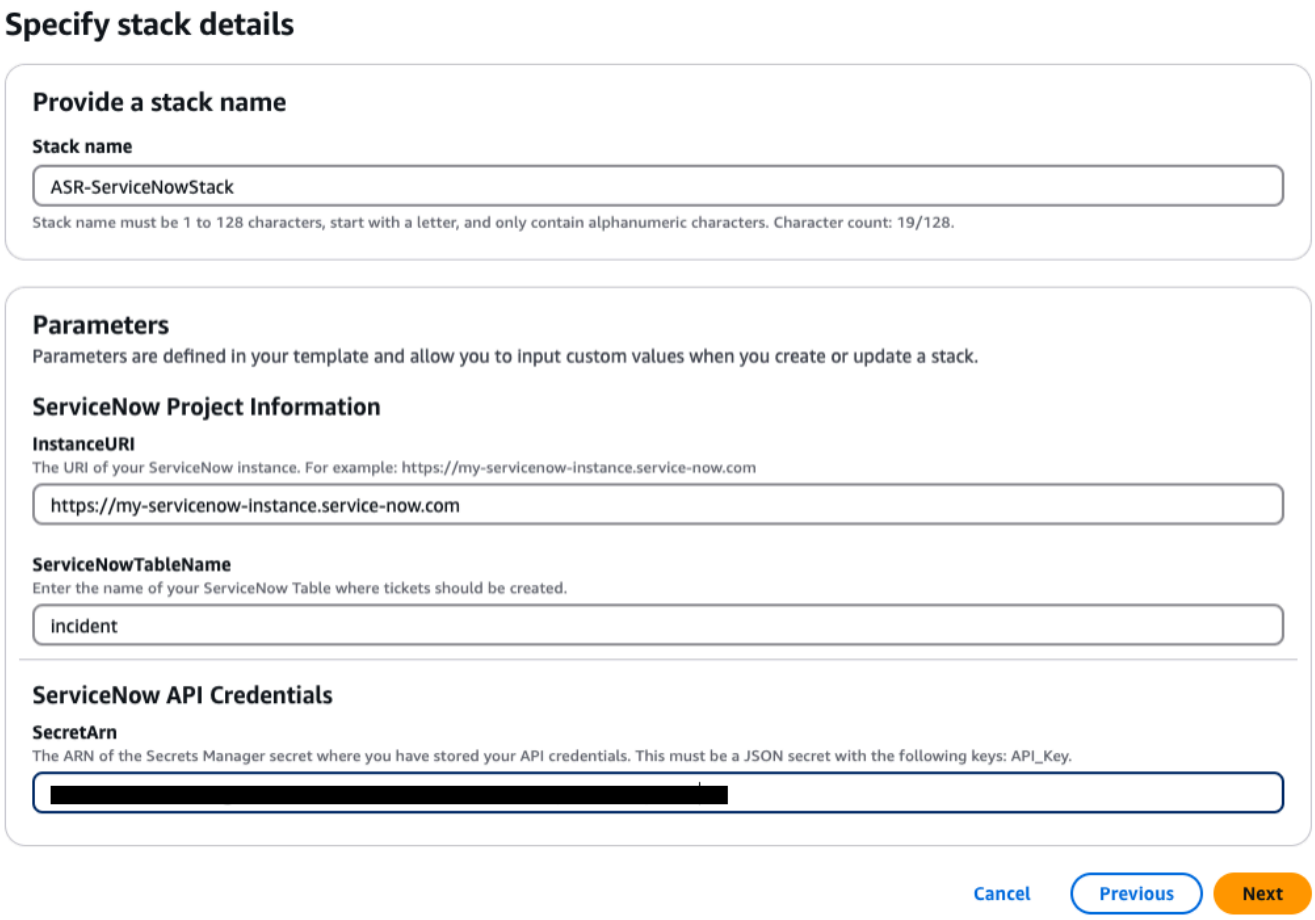
g. Forneça o URI da sua ServiceNow instância.

h. Forneça o nome ServiceNow da sua tabela.

i. Crie uma chave de API ServiceNow com permissão para modificar a tabela na qual você pretende gravar.

j. Crie um segredo no Secrets Manager com a chave `API_Key` e forneça o ARN secreto como entrada para a pilha.

Forneça um nome da pilha, informações ServiceNow do projeto e credenciais ServiceNow da API.



Para criar uma pilha de integração personalizada: inclua uma função Lambda que o orquestrador de soluções Step Functions possa chamar para cada correção. A função Lambda deve receber a entrada fornecida pelo Step Functions, construir uma carga útil de acordo com os requisitos do seu sistema de emissão de tíquetes e fazer uma solicitação ao sistema para criar o ticket.

Etapa 1: iniciar a pilha de administração na conta de administrador delegada do Security Hub

1. Inicie a pilha de administração,`automated-security-response-admin.template`, com sua conta de administrador do Security Hub. Normalmente, um por organização em uma única região. Como essa pilha usa pilhas aninhadas, você deve implantar esse modelo como autogerenciado. StackSet

Parâmetros

Parâmetro	Padrão	Description
Carregar SC Admin Stack	`yes`	Especifique se deseja instalar os componentes administr ativos para remediação automatizada dos controles SC.
Carregar pilha de administr ação do AFSBP	no	Especifique se deseja instalar os componentes administr ativos para remediação automatizada dos controles do FSBP.
Carregar pilha de CIS120 administração	no	Especifique se deseja instalar os componentes administr ativos para remediação automatizada dos CIS120 controles.
Carregar pilha de CIS140 administração	no	Especifique se deseja instalar os componentes administr ativos para remediação automatizada dos CIS140 controles.
Carregar pilha de CIS300 administração	no	Especifique se deseja instalar os componentes administr ativos para remediação automatizada dos CIS300 controles.
Carregar pilha de PC1321 administração	no	Especifique se deseja instalar os componentes administr ativos para remediação

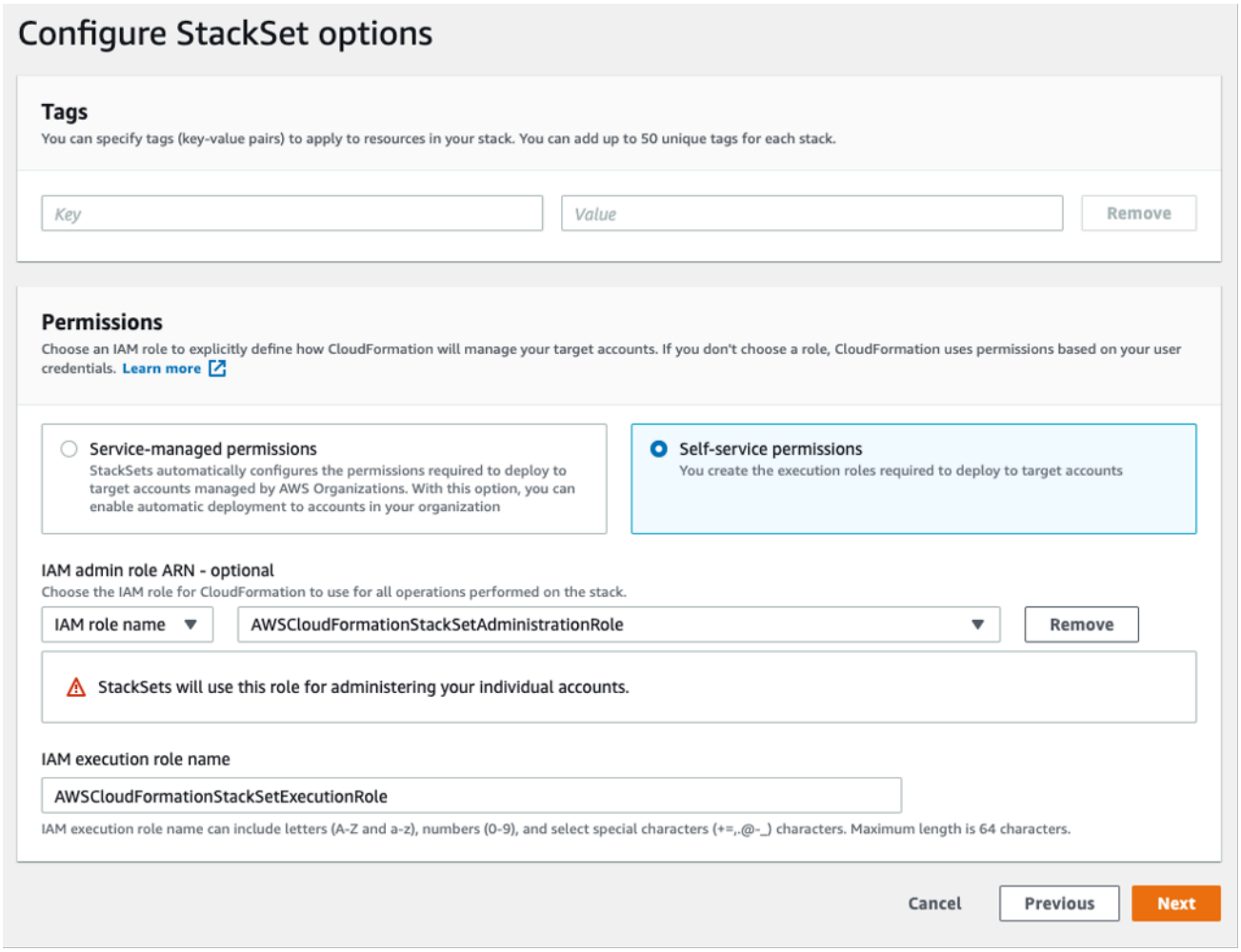
Parâmetro	Padrão	Description
		automatizada dos PC1321 controles.
Carregar o NIST Admin Stack	no	Especifique se deseja instalar os componentes administr ativos para remediação automática dos controles do NIST.
Reutilizar o grupo de registros do Orchestrator	no	Selecione se deseja ou não reutilizar um grupo de `SO0111-ASR-Orchest rator` CloudWatch registros existente. Isso simplifica a reinstalação e as atualizaç ões sem perder os dados de log de uma versão anterior. Reutilize o existente , `Orchestrator Log Group` escolha `yes` se o `Orchestrator Log Group` ainda existe de uma implantação anterior nessa conta, caso contrárionо. Se você estiver executando uma atualização de pilha de uma versão anterior à v2.3.0, escolha no

Parâmetro	Padrão	Description
ShouldDeployWebUI	`yes`	Implante os componentes da interface de usuário da Web, incluindo API Gateway, funções Lambda e CloudFront distribuição. Selecione “sim” para ativar a interface de usuário baseada na web para visualizar as descobertas e o status da remediação. Se você optar por desativar esse recurso, ainda poderá configurar remediações automatizadas e executar remediações sob demanda usando a ação personalizada CSPM do Security Hub.
AdminUserEmail	(Entrada opcional)	Endereço de e-mail do usuário administrador inicial. Esse usuário terá acesso administrativo total à interface do usuário da Web do ASR. Obrigatório somente quando a interface do usuário da Web está ativada.
Use CloudWatch métricas	`yes`	Especifique se deseja ativar CloudWatch as métricas para monitorar a solução. Isso criará um CloudWatch painel para visualizar as métricas.

Parâmetro	Padrão	Description
Use CloudWatch alarmes de métricas	`yes`	Especifique se deseja ativar os alarmes de CloudWatch métricas para a solução. Isso criará alarmes para determina das métricas coletadas pela solução.
RemediationFailureAlarmThreshold	5	Especifique o limite para a porcentagem de falhas de remediação por ID de controle. Por exemplo, se você entrar5, receberá um alarme se um ID de controle falhar em mais de 5% das remediações em um determinado dia. Esse parâmetro funciona somente se os alarmes forem criados (consulte o parâmetro Use CloudWatch Metrics Alarms).
EnableEnhancedCloudWatchMetrics	no	Seyes, cria CloudWatch métricas adicionais para rastrear todos os controles IDs individualmente no CloudWatch painel e como CloudWatch alarmes. Consulte a seção Custo para entender o custo adicional que isso acarreta.

Parâmetro	Padrão	Description
TicketGenFunctionName	(Entrada opcional)	Opcional. Deixe em branco se você não quiser integrar um sistema de bilhetagem. Caso contrário, forneça o nome da função Lambda da saída da pilha da Etapa 0, por exemplo:. `SO0111-ASR-ServiceNow-TicketGenerator`

Configurar StackSet opções



1. Para o parâmetro Números da conta, insira o ID da conta de administrador do AWS Security Hub.

2. Para o parâmetro Especificar regiões, selecione somente a região em que o administrador do Security Hub está ativado. Aguarde a conclusão dessa etapa antes de prosseguir para a Etapa 2.

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

Use um serviço gerenciado StackSets para implantar o modelo de funções de membro,. `automated-security-response-member-roles.template` Isso StackSet deve ser implantado em uma região por conta de membro. Ele define as funções globais que permitem chamadas de API entre contas a partir da função de etapa do ASR Orchestrator.

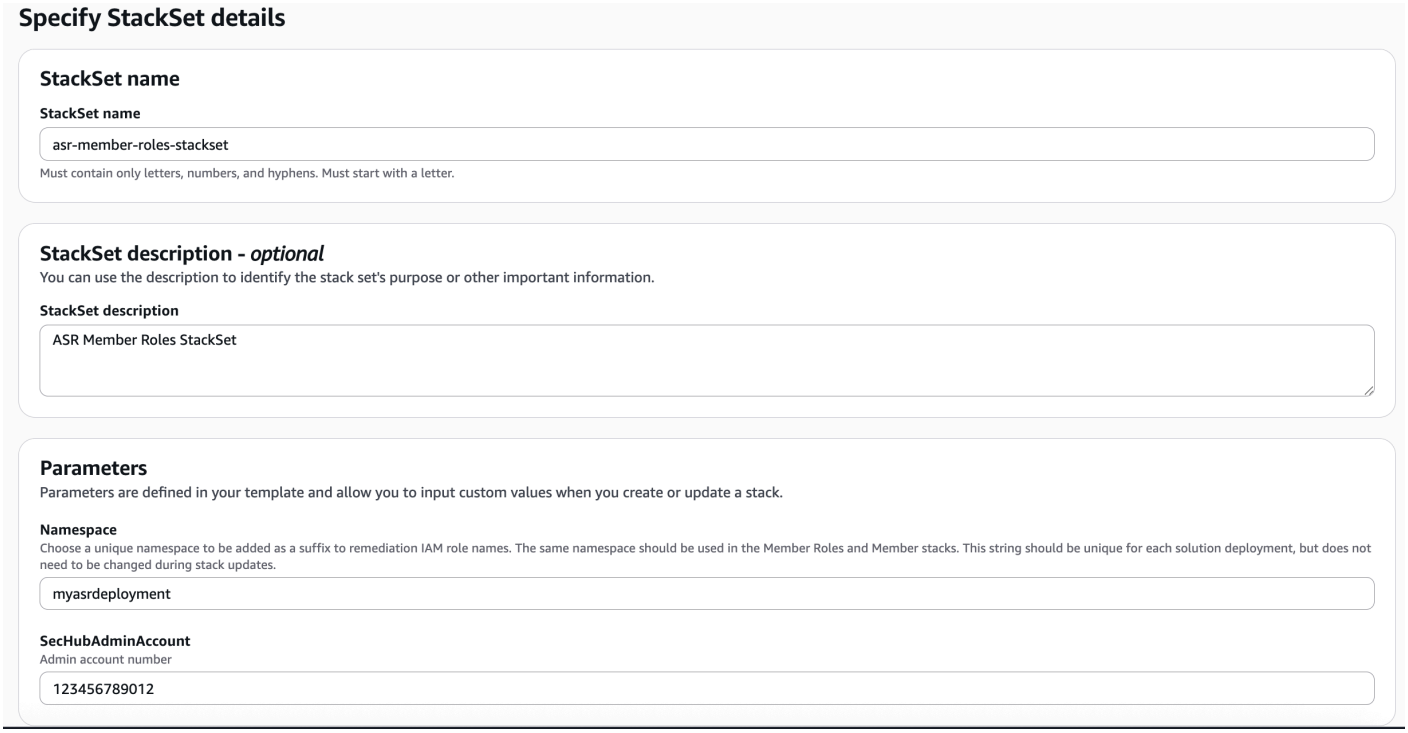
Parâmetros

Parâmetro	Padrão	Description
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Namespace exclusivo a ser adicionado como sufixo aos nomes das funções do IAM de remediaçã o. O mesmo namespace deve ser usado nas funções e pilhas de membros. Essa sequência de caracteres deve ser exclusiva para cada implantação da solução, mas não precisa ser alterada durante as atualizações da pilha. O valor do namespace não precisa ser exclusivo por conta de membro.
Administrador da conta Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de administrador do AWS Security Hub. Esse valor

Parâmetro	Padrão	Description
		concede permissões para a função de solução da conta de administrador.

1. Implante em toda a organização (típica) ou em unidades organizacionais, de acordo com as políticas de sua organização.
2. Ative a implantação automática para que novas contas no AWS Organizations recebam essas permissões.
3. Para o parâmetro Especificar regiões, selecione uma única região. As funções do IAM são globais. Você pode continuar na Etapa 3 enquanto isso é StackSet implantado.

Especifique StackSet detalhes



Etapa 3: Inicie a pilha de membros em cada conta de membro e região do AWS Security Hub

Como a pilha de membros usa pilhas aninhadas, você deve implantá-la como autogerenciada. StackSet Isso não oferece suporte à implantação automática em novas contas na organização da AWS.

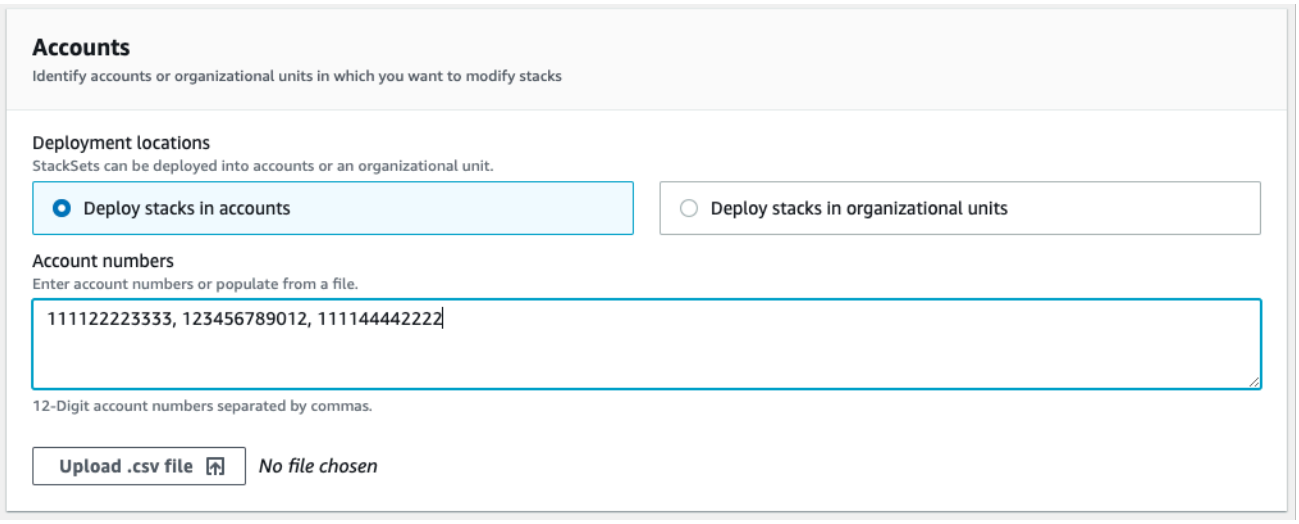
Parâmetros

Parâmetro	Padrão	Description
Forneça o nome do LogGroup a ser usado para criar filtros métricos e alarmes	`<Requires input>`	Especifique o nome de um grupo de CloudWatch registros em que CloudTrai l registra chamadas de API. Isso é usado para remediaçõ es do CIS 3.1-3.14.
Carregar pilha de membros SC	`yes`	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos controles SC.
Carregar pilha de membros do AFSBP	no	Especifique se deseja instalar os componentes membros para remediação automatiz ada dos controles do FSBP.
Carregar pilha de CIS120 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos CIS120 controles.
Carregar pilha de CIS140 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos CIS140 controles.

Parâmetro	Padrão	Description
Carregar pilha de CIS300 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatizada dos CIS300 controles.
Carregar pilha de PC1321 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatizada dos PC1321 controles.
Carregar pilha de membros do NIST	no	Especifique se deseja instalar os componentes membros para remediação automatizada dos controles do NIST.
Crie um bucket do S3 para o registro de auditoria do Redshift	no	Selecione `yes` se o bucket do S3 deve ser criado para a remediação do FSBP 4.4. RedShift Para obter detalhes sobre o bucket S3 e a remediação, consulte a remediação do Redshift.4 no Guia do usuário do AWS Security Hub.
Conta de administrador do Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de administrador do AWS Security Hub.

Parâmetro	Padrão	Description
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Essa string se torna parte dos nomes das funções do IAM e do bucket do Action Log S3. Use o mesmo valor para implantação de pilha de membros e implantação de pilha de funções de membros. A string deve ser exclusiva para cada implantação da solução, mas não precisa ser alterada durante as atualizações da pilha.
EnableCloudTrailForASRActionLog (Log)	no	Selecione `yes` se você deseja monitorar os eventos de gerenciamento conduzidos pela solução no CloudWatch painel. A solução cria uma CloudTrail trilha em cada conta de membro seleciona da`yes`. Você deve implantar a solução em uma organização da AWS para habilitar esse recurso. Além disso, você só pode ativar esse recurso em uma única região dentro da mesma conta. Consulte a seção Custo para entender o custo adicional que isso acarreta.

Contas



Locais de implantação: você pode especificar uma lista de números de contas ou unidades organizacionais.

Especifique regiões: selecione todas as regiões nas quais você deseja corrigir as descobertas. Você pode ajustar as opções de implantação conforme apropriado para o número de contas e regiões. A simultaneidade de regiões pode ser paralela.

Implantação automatizada - Stacks

> **Note**
>
> Para clientes com várias contas, é altamente recomendável implantar com StackSets.

Antes de iniciar a solução, analise a arquitetura, os componentes da solução, a segurança e as considerações de design discutidas neste guia. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em sua conta.

Tempo de implantação: Aproximadamente 30 minutos

Pré-requisitos

Antes de implantar essa solução, certifique-se de que o AWS Security Hub esteja na mesma região da AWS que suas contas primária e secundária. Se você já implantou essa solução, deverá desinstalar a solução existente. Para obter mais informações, consulte Atualizar a solução.

Visão geral da implantação

Use as etapas a seguir para implantar essa solução na AWS.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tíquetes

- Se você pretende usar o recurso de emissão de tíquetes, primeiro implante a pilha de integração de tíquetes em sua conta de administrador do Security Hub.
- Copie o nome da função Lambda dessa pilha e forneça-o como entrada para a pilha de administração (consulte a Etapa 1).

Etapa 1: iniciar a pilha de administração

- Inicie o CloudFormation modelo `automated-security-response-admin.template` da AWS em sua conta de administrador do AWS Security Hub.
- Escolha quais padrões de segurança instalar.
- Escolha um grupo de registros existente do Orchestrator para usar (selecione `Yes` se `SO0111-ASR-Orchestrator` já existe em uma instalação anterior).

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

- Lance o CloudFormation modelo `automated-security-response-member-roles.template` da AWS em uma região por conta de membro.
- Insira o IG da conta de 12 dígitos para a conta de administrador do AWS Security Hub.

Etapa 3: iniciar a pilha de membros

- Especifique o nome do grupo de CloudWatch registros a ser usado com as remediações do CIS 3.1-3.14. Ele deve ser o nome de um grupo de CloudWatch registros de registros que recebe CloudTrail registros.
- Escolha se deseja instalar as funções de remediação. Instale essas funções somente uma vez por conta.
- Selecione quais playbooks instalar.
- Insira o ID da conta de administrador do AWS Security Hub.

Etapa 4: (Opcional) Ajustar as remediações disponíveis

- Remova todas as correções por conta de membro. Esta etapa é opcional.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tíquetes

1. Se você pretende usar o recurso de emissão de tíquetes, inicie primeiro a respectiva pilha de integração.
2. Escolha as pilhas de integração fornecidas para o Jira ou ServiceNow use-as como um modelo para implementar sua própria integração personalizada.

   Para implantar a pilha do Jira:

   a. Insira um nome para sua pilha.

   b. Forneça o URI para sua instância do Jira.

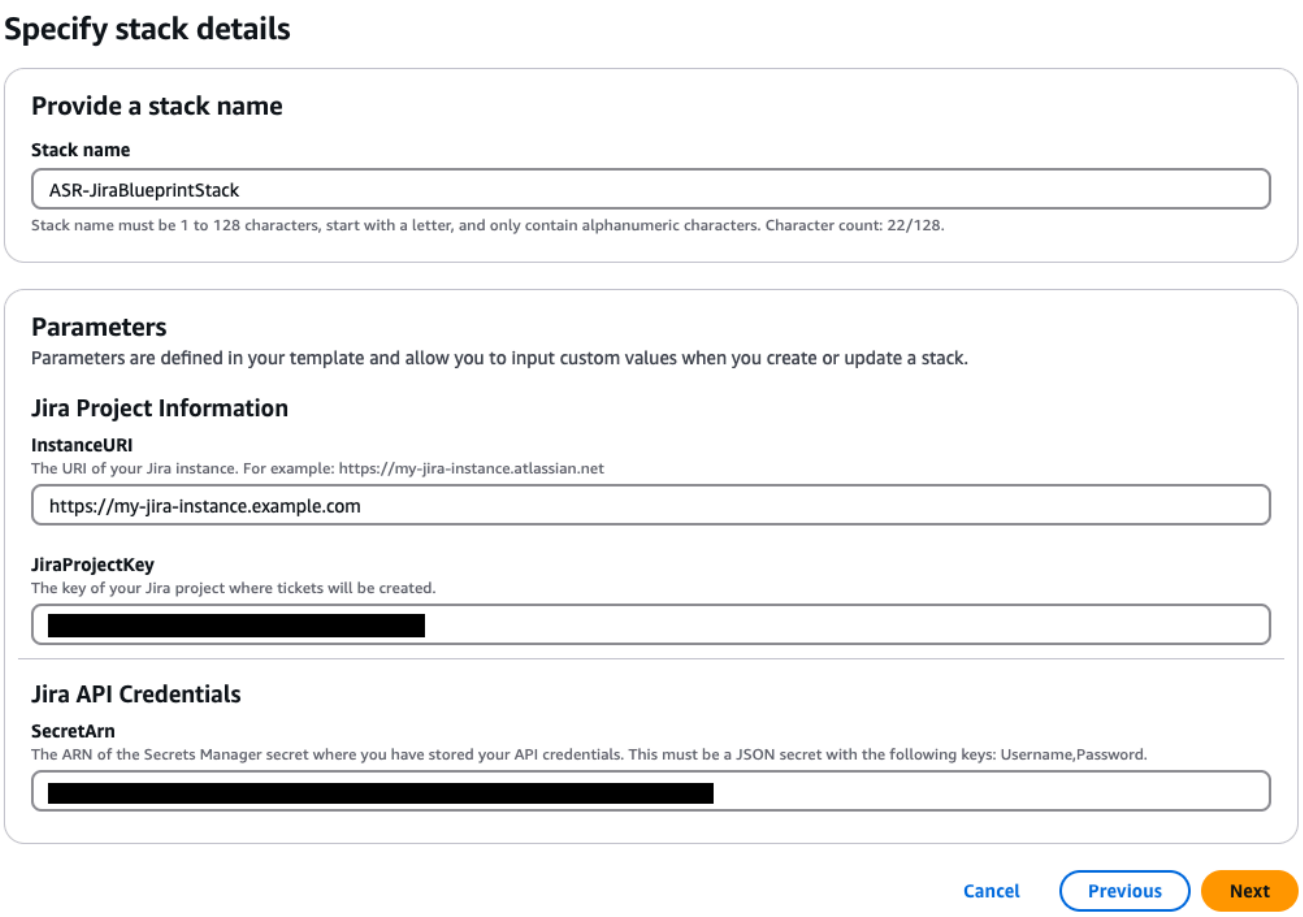
   c. Forneça a chave do projeto do Jira para o qual você deseja enviar tickets.

   d. Crie um novo segredo de valor-chave no Secrets Manager que contenha seu Jira e. `Username` `Password`

   > **Note**
   >
   > Você pode optar por usar uma chave de API do Jira no lugar de sua senha, fornecendo seu nome de usuário como `Username` e sua chave de API como o. `Password`

   e. Adicione o ARN desse segredo como entrada na pilha.

   “Forneça um nome de pilha, informações do projeto Jira e credenciais da API do Jira.



Configuração do Jira Field:

Para obter informações sobre como personalizar os campos de ticket do Jira, consulte a seção Configuração de campo do Jira na Etapa 0 da implantação. StackSet

Para implantar a ServiceNow pilha:

f. Insira um nome para sua pilha.

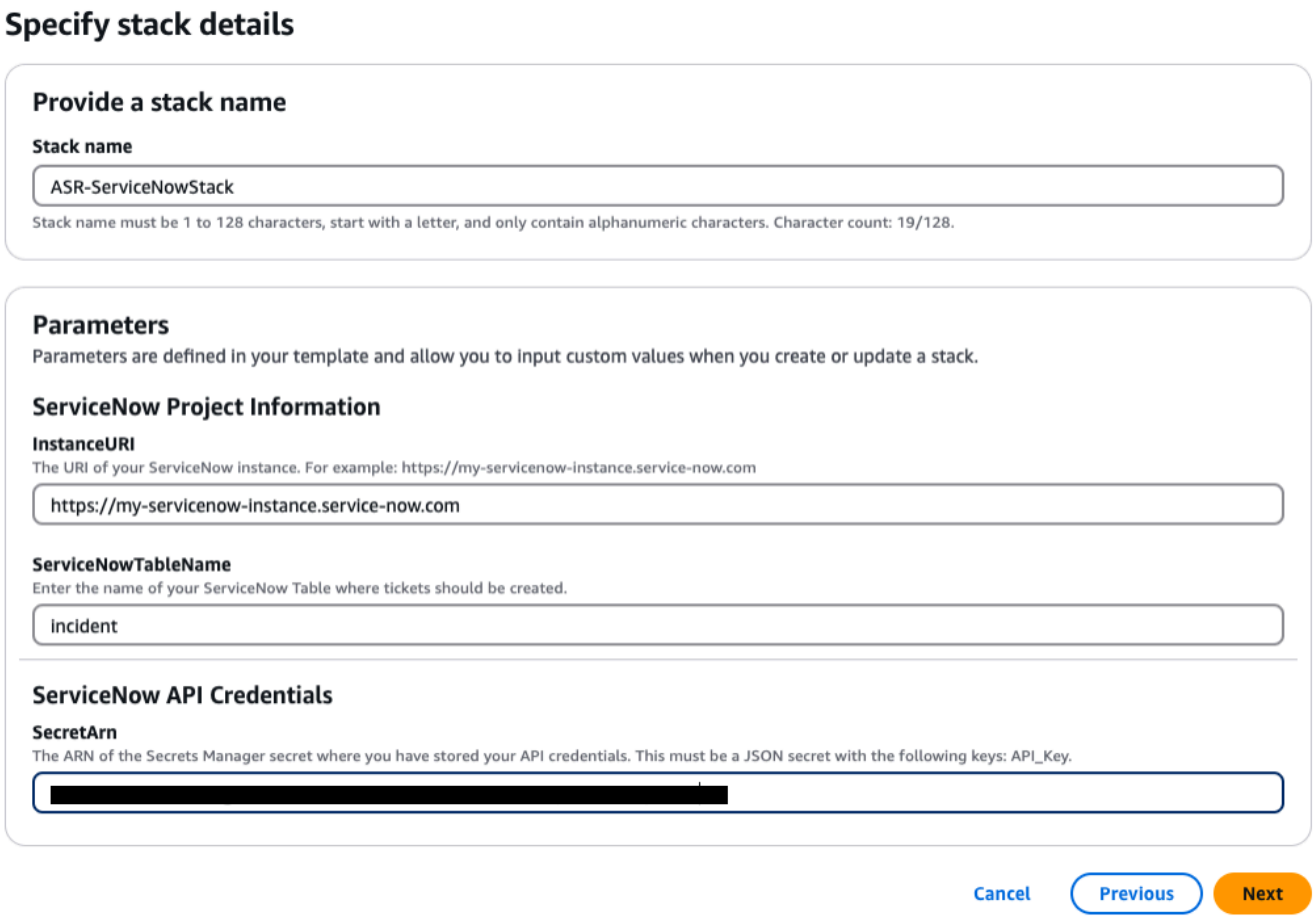
g. Forneça o URI da sua ServiceNow instância.

h. Forneça o nome ServiceNow da sua tabela.

i. Crie uma chave de API ServiceNow com permissão para modificar a tabela na qual você pretende gravar.

j. Crie um segredo no Secrets Manager com a chave `API_Key` e forneça o ARN secreto como entrada para a pilha.

Forneça um nome da pilha, informações ServiceNow do projeto e credenciais ServiceNow da API.



Para criar uma pilha de integração personalizada: inclua uma função Lambda que o orquestrador de soluções Step Functions possa chamar para cada correção. A função Lambda deve receber a entrada fornecida pelo Step Functions, construir uma carga útil de acordo com os requisitos do seu sistema de emissão de tíquetes e fazer uma solicitação ao sistema para criar o ticket.

Etapa 1: iniciar a pilha de administração

> **Important**
>
> Essa solução inclui coleta de dados. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. A AWS possui os dados coletados por meio dessa pesquisa. A coleta de dados está sujeita ao Aviso de Privacidade da AWS.

Esse CloudFormation modelo automatizado da AWS implanta a solução Automated Security Response on AWS na nuvem da AWS. Antes de iniciar a pilha, você deve habilitar o Security Hub e preencher os pré-requisitos.

> **Note**
>
> Você é responsável pelo custo dos serviços da AWS usados ao executar essa solução. Para obter mais detalhes, visite a seção Custo neste guia e consulte a página de preços de cada serviço da AWS usado nesta solução.

1. Faça login no AWS Management Console a partir da conta em que o AWS Security Hub está atualmente configurado e use o botão abaixo para iniciar o CloudFormation modelo `automated-security-response-admin.template` da AWS.

   Também é possível fazer download do modelo para usá-lo como ponto de partida para a sua própria implantação.
2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma região diferente da AWS, use o seletor de regiões na barra de navegação do AWS Management Console.

   > **Note**
   >
   > Essa solução usa o AWS Systems Manager, que atualmente está disponível somente em regiões específicas da AWS. A solução funciona em todas as regiões que oferecem suporte a esse serviço. Para obter a disponibilidade mais atual por região, consulte a Lista de serviços regionais da AWS.
3. Na página Criar pilha, verifique se o URL do modelo correto está na caixa de texto URL do Amazon S3 e escolha Avançar.
4. Na página Especificar detalhes da pilha, atribua um nome para a sua pilha de soluções. Para obter informações sobre limitações de nomes de caracteres, consulte os limites do IAM e do STS no Guia do usuário do AWS Identity and Access Management.
5. Na página Parâmetros, escolha Avançar.

Parâmetro	Padrão	Description
Carregar SC Admin Stack	`yes`	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos controles SC.
Carregar pilha de administração do AFSBP	no	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos controles do FSBP.
Carregar pilha de CIS120 administração	no	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos CIS120 controles.
Carregar pilha de CIS140 administração	no	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos CIS140 controles.
Carregar pilha de CIS300 administração	no	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos CIS300 controles.
Carregar pilha de PC1321 administração	no	Especifique se deseja instalar os componentes administrativos para remediação automatizada dos PC1321 controles.

Parâmetro	Padrão	Description
Carregar o NIST Admin Stack	no	Especifique se deseja instalar os componentes administrativos para remediação automática dos controles do NIST.
Reutilizar o grupo de registros do Orchestrator	no	Selecione se deseja ou não reutilizar um grupo de `SO0111-ASR-Orchestrator` CloudWatch registros existente. Isso simplifica a reinstalação e as atualizações sem perder os dados de log de uma versão anterior. Reutilize o existente, `Orchestrator Log Group` escolha `yes` se o `Orchestrator Log Group` ainda existe de uma implantação anterior nessa conta, caso contrário. Se você estiver executando uma atualização de pilha de uma versão anterior à v2.3.0, escolha no
ShouldDeployWebUI	`yes`	Implante os componentes da interface de usuário da Web, incluindo API Gateway, funções Lambda e CloudFront distribuição. Selecione “sim” para ativar o painel baseado na web para visualizar as descobertas e o status da remediação.

Parâmetro	Padrão	Description
AdminUserEmail	(Entrada opcional)	Endereço de e-mail do usuário administrador inicial. Esse usuário terá acesso administrativo total à interface do usuário da Web do ASR. Obrigatório somente quando a interface do usuário da Web está ativada.
Use CloudWatch métricas	`yes`	Especifique se deseja ativar CloudWatch as métricas para monitorar a solução. Isso criará um CloudWatch painel para visualizar as métricas.
Use CloudWatch alarmes de métricas	`yes`	Especifique se deseja ativar os alarmes de CloudWatc h métricas para a solução. Isso criará alarmes para determinadas métricas coletadas pela solução.

Parâmetro	Padrão	Description
RemediationFailure AlarmThreshold	5	Especifique o limite para a porcentagem de falhas de remediação por ID de controle. Por exemplo, se você entrar5, receberá um alarme se um ID de controle falhar em mais de 5% das remediações em um determinado dia. Esse parâmetro funciona somente se os alarmes forem criados (consulte o parâmetro Use CloudWatch Metrics Alarms).
EnableEnhancedClou dWatchMetrics	no	Seyes, cria CloudWatch métricas adicionais para rastrear todos os controles IDs individualmente no CloudWatch painel e como CloudWatch alarmes. Consulte a seção Custo para entender o custo adicional que isso acarreta.

Parâmetro	Padrão	Description
TicketGenFunctionName	(Entrada opcional)	Opcional. Deixe em branco se você não quiser integrar um sistema de bilhetagem. Caso contrário, forneça o nome da função Lambda da saída da pilha da Etapa 0, por exemplo:. `SO0111-ASR-ServiceNow-TicketGenerator`

> **Note**
>
> Você deve ativar manualmente as correções automáticas na conta do administrador após implantar ou atualizar as pilhas da CloudFormation solução.

1. Na página Configurar opções de pilha, selecione Avançar.
2. Na página Revisar, verifique e confirme as configurações. Marque a caixa de seleção confirmando que o modelo criará recursos do AWS Identity and Access Management (IAM).
3. Selecione Create stack (Criar pilha) para implantar a pilha.

Você pode ver o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status CREATE_COMPLETE em aproximadamente 15 minutos.

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

O `automated-security-response-member-roles.template` StackSet deve ser implantado em apenas uma região por conta de membro. Ele define as funções globais que permitem chamadas de API entre contas a partir da função de etapa do ASR Orchestrator.

1. Faça login no Console de Gerenciamento da AWS para cada conta de membro do AWS Security Hub (incluindo a conta de administrador, que também é membro). Selecione o botão para iniciar o CloudFormation modelo `automated-security-response-member-roles.template` da

AWS. Também é possível fazer download do modelo para usá-lo como ponto de partida para a sua própria implantação.

2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma região diferente da AWS, use o seletor de regiões na barra de navegação do AWS Management Console.
3. Na página Criar pilha, verifique se o URL do modelo correto está na caixa de texto URL do Amazon S3 e escolha Avançar.
4. Na página Especificar detalhes da pilha, atribua um nome para a sua pilha de soluções. Para obter informações sobre limitações de nomes de caracteres, consulte os limites do IAM e do STS no Guia do usuário do AWS Identity and Access Management.
5. Na página Parâmetros, especifique os parâmetros a seguir e escolha Avançar.

Parâmetro	Padrão	Description
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Namespace exclusivo a ser adicionado como sufixo aos nomes das funções do IAM de remediação. O mesmo namespace deve ser usado nas funções e pilhas de membros. Essa sequência de caracteres deve ser exclusiva para cada implantação da solução, mas não precisa ser alterada durante as atualizações da pilha. O valor do namespace não precisa ser exclusivo por conta de membro.

Parâmetro	Padrão	Description
Administrador da conta Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de administrador do AWS Security Hub. Esse valor concede permissões para a função de solução da conta de administrador.

6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa de seleção confirmando que o modelo criará recursos do AWS Identity and Access Management (IAM).
8. Selecione Create stack (Criar pilha) para implantar a pilha.

   Você pode ver o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status CREATE_COMPLETE em cerca de 5 minutos. Você pode continuar com a próxima etapa enquanto essa pilha é carregada.

Etapa 3: iniciar a pilha de membros

> **Important**
>
> Essa solução inclui coleta de dados. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. A AWS possui os dados coletados por meio dessa pesquisa. A coleta de dados está sujeita à Política de Privacidade da AWS.

A `automated-security-response-member` pilha deve ser instalada em cada conta de membro do Security Hub. Essa pilha define os runbooks para remediação automatizada. O administrador da conta de cada membro pode controlar quais remediações estão disponíveis por meio dessa pilha.

1. Faça login no Console de Gerenciamento da AWS para cada conta de membro do AWS Security Hub (incluindo a conta de administrador, que também é membro). Selecione o botão para iniciar o CloudFormation modelo `automated-security-response-member.template` da AWS.

Launch solution

Você também pode baixar o modelo como ponto de partida para sua própria implementação. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma região diferente da AWS, use o seletor de regiões na barra de navegação do AWS Management Console.

+

> **Note**
>
> Essa solução usa o AWS Systems Manager, que atualmente está disponível na maioria das regiões da AWS. A solução funciona em todas as regiões que oferecem suporte a esses serviços. Para obter a disponibilidade mais atual por região, consulte a Lista de serviços regionais da AWS.

1. Na página Criar pilha, verifique se o URL do modelo correto está na caixa de texto URL do Amazon S3 e escolha Avançar.
2. Na página Especificar detalhes da pilha, atribua um nome para a sua pilha de soluções. Para obter informações sobre limitações de nomes de caracteres, consulte os limites do IAM e do STS no Guia do usuário do AWS Identity and Access Management.
3. Na página Parâmetros, especifique os parâmetros a seguir e escolha Avançar.

Parâmetro	Padrão	Description
Forneça o nome do LogGroup a ser usado para criar filtros métricos e alarmes	`<Requires input>`	Especifique o nome de um grupo de CloudWatch registros em que CloudTrail registra chamadas de API. Isso é usado para remediações do CIS 3.1-3.14.
Carregar pilha de membros SC	`yes`	Especifique se deseja instalar os componentes do membro

Parâmetro	Padrão	Description
		para remediação automatiz ada dos controles SC.
Carregar pilha de membros do AFSBP	no	Especifique se deseja instalar os componentes membros para remediação automatiz ada dos controles do FSBP.
Carregar pilha de CIS120 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos CIS120 controles.
Carregar pilha de CIS140 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos CIS140 controles.
Carregar pilha de CIS300 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos CIS300 controles.
Carregar pilha de PC1321 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatiz ada dos PC1321 controles.
Carregar pilha de membros do NIST	no	Especifique se deseja instalar os componentes membros para remediação automatiz ada dos controles do NIST.

Parâmetro	Padrão	Description
Crie um bucket do S3 para o registro de auditoria do Redshift	no	Selecione `yes` se o bucket do S3 deve ser criado para a remediação do FSBP 4.4. RedShift Para obter detalhes sobre o bucket S3 e a remediação, consulte a remediação do Redshift.4 no Guia do usuário do AWS Security Hub.
Conta de administrador do Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de administrador do AWS Security Hub.
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Essa string se torna parte dos nomes das funções do IAM e do bucket do Action Log S3. Use o mesmo valor para implantação de pilha de membros e implantação de pilha de funções de membros. A string deve ser exclusiva para cada implantação da solução, mas não precisa ser alterada durante as atualizações da pilha.

Parâmetro	Padrão	Description
EnableCloudTrailFo rASRActionLog (Log)	no	Selecione `yes` se você deseja monitorar os eventos de gerenciamento conduzido s pela solução no CloudWatc h painel. A solução cria uma CloudTrail trilha em cada conta de membro seleciona da `yes`. Você deve implantar a solução em uma organizaç ão da AWS para habilitar esse recurso. Além disso, você só pode ativar esse recurso em uma única região dentro da mesma conta. Consulte a seção Custo para entender o custo adicional que isso acarreta.

4. Na página Configurar opções de pilha, selecione Avançar.
5. Na página Revisar, verifique e confirme as configurações. Marque a caixa de seleção confirmando que o modelo criará recursos do AWS Identity and Access Management (IAM).
6. Selecione Create stack (Criar pilha) para implantar a pilha.

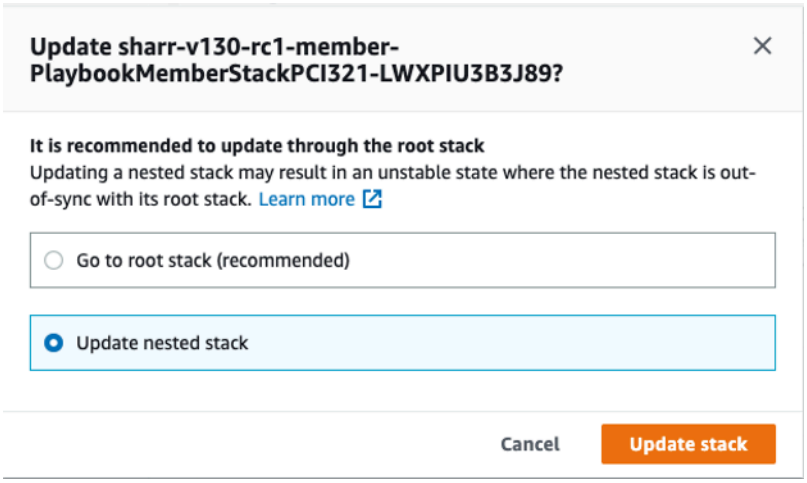
Você pode ver o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status CREATE_COMPLETE em aproximadamente 15 minutos.

Etapa 4: (Opcional) Ajustar as remediações disponíveis

Se quiser remover correções específicas da conta de um membro, você pode fazer isso atualizando a pilha aninhada de acordo com o padrão de segurança. Para simplificar, as opções de pilha aninhada não são propagadas para a pilha raiz.

1. Faça login no CloudFormation console da AWS e selecione a pilha aninhada.
2. Selecione Atualizar.
3. Selecione Atualizar pilha aninhada e escolha Atualizar pilha.

Atualizar pilha aninhada



4. Selecione Usar modelo atual e escolha Avançar.
5. Ajuste as remediações disponíveis. Altere os valores dos controles desejados para `Available` e dos controles indesejados para`Not available`.

> **Note**
>
> Desativar uma remediação remove o runbook de remediação de soluções para o padrão e controle de segurança.

6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa de seleção confirmando que o modelo criará recursos do AWS Identity and Access Management (IAM).
8. Escolha Atualizar pilha.

Você pode ver o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status CREATE_COMPLETE em aproximadamente 15 minutos.

Implantação da Control Tower (CT)

O guia Customizations for AWS Control Tower (cFCT) é para administradores, DevOps profissionais, fornecedores independentes de software, arquitetos de infraestrutura de TI e integradores de sistemas que desejam personalizar e ampliar seus ambientes da AWS Control Tower para suas empresas e clientes. Ele fornece informações sobre a personalização e a extensão do ambiente do AWS Control Tower com o pacote de personalização do CfCT.

Tempo de implantação: Aproximadamente 30 minutos

Pré-requisitos

Antes de implantar essa solução, certifique-se de que ela seja destinada aos administradores do AWS Control Tower.

Quando você estiver pronto para configurar sua landing zone usando o console do AWS Control Tower ou APIs siga estas etapas:

Para começar a usar o AWS Control Tower, consulte: Getting Started with AWS Control Tower

Para saber como personalizar sua zona de pouso, consulte: Personalizando sua zona de pouso

Para iniciar e implantar sua zona de pouso, consulte: Guia de implantação da zona de pouso

Visão geral da implantação

Use as etapas a seguir para implantar essa solução na AWS.

Etapa 1: criar e implantar o bucket S3

> **Note**
>
> Configuração do bucket S3 — somente para ADMIN. Essa é uma etapa de configuração única e não deve ser repetida pelos usuários finais. Os buckets do S3 armazenam o pacote de implantação, incluindo o CloudFormation modelo da AWS e o código Lambda necessários para a execução do ASR. Esses recursos são implantados usando CfCt ou StackSet.

1. Configurar o bucket S3

Configure o bucket do S3 que será usado para armazenar e servir seus pacotes de implantação.

2. Configurar o ambiente do

Prepare as variáveis de ambiente, as credenciais e as ferramentas necessárias para o processo de criação e implantação.

3. Configurar políticas de bucket do S3

Defina e aplique as políticas de bucket apropriadas para controlar o acesso e as permissões.

4. Prepare a construção

Compile, empacote ou prepare seu aplicativo ou ativos para implantação.

5. Implantar pacotes no S3

Faça o upload dos artefatos de construção preparados para o bucket S3 designado.

Etapa 2: implantação de pilhas no AWS Control Tower

1. Crie um manifesto de construção para componentes do ASR

Defina um manifesto de construção que liste todos os componentes do ASR, suas versões, dependências e instruções de construção.

2. Atualize o CodePipeline

Modifique a CodePipeline configuração da AWS para incluir as novas etapas de construção, artefatos ou estágios necessários para a implantação dos componentes do ASR.

Etapa 1: criar e implantar no bucket S3

As soluções da AWS usam dois buckets: um bucket para acesso global aos modelos, que é acessado via HTTPS, e buckets regionais para acessar ativos dentro da região, como o código Lambda.

1. Configurar o bucket S3

Escolha um nome de bucket exclusivo, por exemplo, asr-staging. Defina duas variáveis de ambiente em seu terminal, uma deve ser o nome base do bucket com -reference como sufixo e a outra com a região de implantação pretendida como sufixo:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Configuração do ambiente

Na sua conta da AWS, crie dois buckets com esses nomes, por exemplo, asr-staging-reference e asr-staging-us-east -1. (O bucket de referência conterá os CloudFormation modelos, o bucket

regional conterá todos os outros ativos, como o pacote de código lambda.) Seus buckets devem ser criptografados e impedir o acesso público

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Ao criar seus buckets, certifique-se de que eles não estejam acessíveis ao público. Use nomes de bucket aleatórios. Desative o acesso público. Use a criptografia KMS. E verifique a propriedade do bucket antes de fazer o upload.

3. Configuração da política de buckets do S3

Atualize a política de bucket do S3 $TEMPLATE_BUCKET_NAME para incluir permissões para o ID da conta de execução. PutObject Atribua essa permissão a uma função do IAM na conta de execução que está autorizada a gravar no bucket. Essa configuração permite que você evite criar o bucket na conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "org-id"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
```

```
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::account-id:role/iam-role-name"
                }
            }
        }
    ]
}
```

Altere a política de bucket do S3 do ativo para incluir permissões. Atribua essa permissão a uma função do IAM na conta de execução que está autorizada a gravar no bucket. Repita essa configuração para cada bucket de ativos regional (por exemplo, asr-staging-us-east asr-staging-eu-west -1, -1 etc.), permitindo implantações em várias regiões sem precisar criar os buckets na conta de gerenciamento.

4. Preparação da construção

- Pré-requisitos:
  - AWS CLI v2
  - Python 3.11+ com pip
  - AWS CDK 2.171.1+
  - Node.js 20+ com npm
  - Poesia v2 com plugin para exportar
- Clone do Git https://github.com/aws-solutions/automated-security-response-on-aws.git

Primeiro, certifique-se de ter executado npm install na pasta de origem.

Em seguida, na pasta de implantação em seu repositório clonado, execute build-s3-dist.sh, passando o nome raiz do seu bucket (ex. mybucket) e a versão que você está criando (por exemplo, v1.0.0). Recomendamos usar uma versão semver com base na versão baixada de GitHub (ex. GitHub: v1.0.0, sua compilação: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
```

```
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Implante pacotes no S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Etapa 2: implantação de pilhas no AWS Control Tower

1. Crie um manifesto para componentes do ASR

Depois de implantar artefatos ASR nos buckets do S3, atualize o manifesto do pipeline do Control Tower para fazer referência à nova versão e, em seguida, acione a execução do pipeline, consulte: implantação da torre de controle

> **Important**
>
> Para garantir a implantação correta da solução ASR, consulte a documentação oficial da AWS para obter informações detalhadas sobre a visão geral dos CloudFormation modelos e a descrição dos parâmetros. Links de informações abaixo: Guia de visão geral dos parâmetros dos CloudFormation modelos

O manifesto dos componentes do ASR tem a seguinte aparência:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: ShouldDeployWebUI
```

```
        parameter_value: "yes"
      - parameter_key: AdminUserEmail
        parameter_value: "<YOUR EMAIL ADDRESS>"
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>
```

```
- name:  <MEMBER STACK NAME>
  resource_file: s3://<MEMBER TEMPLATE BUCKET path>
  parameters:
    - parameter_key: SecHubAdminAccount
      parameter_value: <ADMIN_ACCOUNT_NAME>
    - parameter_key: LoadCIS120MemberStack
      parameter_value: "no"
    - parameter_key: LoadNIST80053MemberStack
      parameter_value: "no"
    - parameter_key: Namespace
      parameter_value: <NAMESPACE>
    - parameter_key: CreateS3BucketForRedshiftAuditLogging
      parameter_value: "no"
    - parameter_key: LoadAFSBPMemberStack
      parameter_value: "no"
    - parameter_key: LoadSCMemberStack
      parameter_value: "yes"
    - parameter_key: LoadPCI321MemberStack
      parameter_value: "no"
    - parameter_key: LoadCIS140MemberStack
      parameter_value: "no"
    - parameter_key: EnableCloudTrailForASRActionLog
      parameter_value: "no"
    - parameter_key: LogGroupName
      parameter_value: <LOG_GROUP_NAME>
    - parameter_key: LoadCIS300MemberStack
      parameter_value: "no"
  deploy_method: stack_set
  deployment_targets:
   accounts: # :type: list
      - <ACCOUNT_NAME> # and/or
      - <ACCOUNT_NUMBER>
  organizational_units:
    - <ORG UNIT>
  regions: # :type: list
    - <REGION_NAME>
```

2. Atualização do pipeline de código

Adicione um arquivo de manifesto a custom-control-tower-configuration um.zip e execute uma CodePipeline, consulte: visão geral do pipeline de código

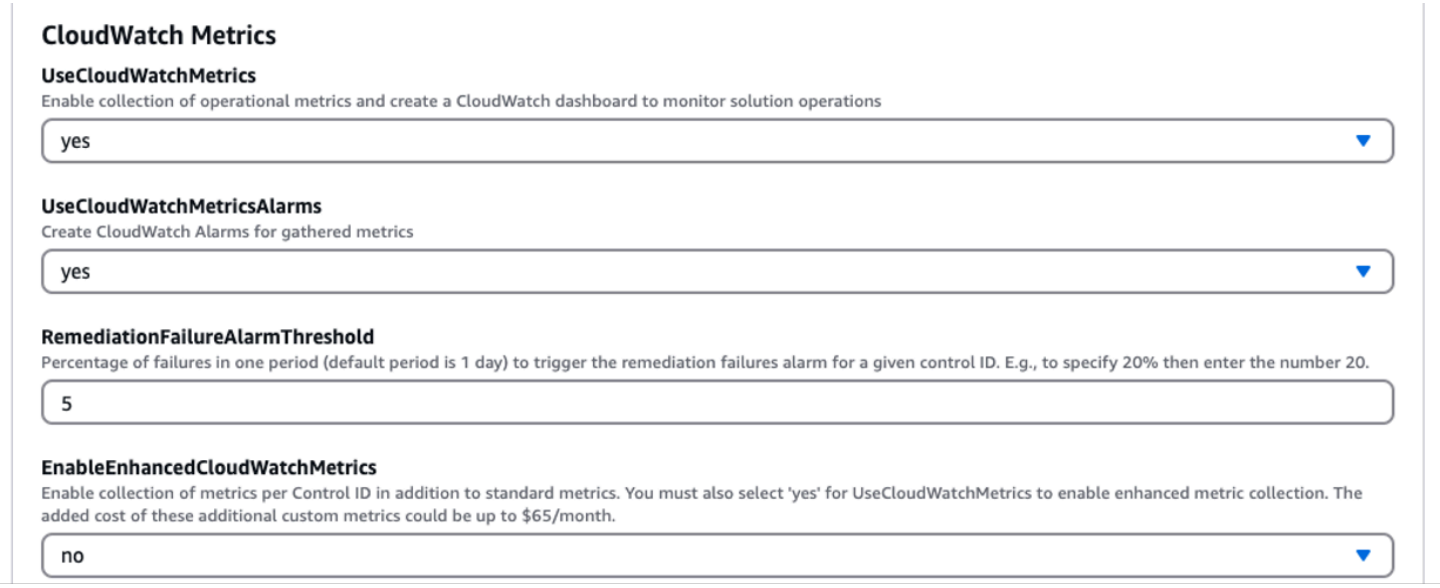
Monitore as operações da solução com um CloudWatch painel da Amazon

Essa solução inclui métricas e alarmes personalizados exibidos em um CloudWatch painel da Amazon.

O CloudWatch painel e os alarmes monitoram as operações da solução e alertam quando há um possível problema.

Ativando CloudWatch métricas, alarmes e painel

Há quatro parâmetros CloudFormation de modelo para CloudWatch funcionalidade.



1. UseCloudWatchMetrics- Definir isso para `yes` permitir a coleta de métricas operacionais e cria um CloudWatch painel para visualizar essas métricas.
2. UseCloudWatchAlarms- Definir isso para `yes` ativar os alarmes padrão da solução.
3. RemediationFailureAlarmThreshold- A porcentagem de falhas nas correções em um período para acionar um alarme.
4. EnableEnhancedCloudWatchMetrics- Defina esse parâmetro `yes` para coletar métricas individuais por ID de controle. Por padrão, esse parâmetro é definido como`no`, de forma que somente as métricas sobre o número total de remediações em todo o controle IDs sejam coletadas. Métricas e alarmes individuais por ID de controle incorrem em custos adicionais.

Usando o CloudWatch painel

Para visualizar o painel:

1. Navegue até Amazon CloudWatch e depois Dashboards.
2. Selecione o painel chamado “ASR-Remediation-Metrics-Dashboard”.

O CloudWatch painel contém as seguintes seções:

1. Total de remediações bem-sucedidas - fornece uma visão sobre o número de descobertas do Security Hub que foram corrigidas com sucesso pela solução.
2. Falhas de remediação - Mostra quantas correções falharam, no total e em porcentagem, e a causa da falha. Um grande número de falhas pode sugerir um problema técnico com a solução que talvez você precise investigar com mais detalhes.
3. Sucesso/falha da correção por ID de controle - Se você ativou as Métricas aprimoradas no momento da implantação, esta seção lista os resultados da remediação por ID de controle. Quando a seção Falhas de Remediação mostra uma alta taxa de falhas em geral, esta seção mostra se as falhas estão distribuídas em vários controles IDs ou se apenas determinados controles IDs estão falhando.
4. Runbook Assume Role Failures - Mostra o número de falhas que ocorreram devido a tentativas de remediação em contas que não têm a função de membro da solução instalada. Falhas repetidas por tentativas automatizadas de remediação devido à falta de funções causam custos desnecessários. Reduza isso instalando a pilha de funções de membro nas contas em questão, desativando todas as EventBridge regras criadas pela solução ou desassociando a conta no Security Hub.
5. Ações de gerenciamento de trilhas do Cloud pelo ASR - lista as ações de gerenciamento da solução em todas as contas de membros nas quais você ativou os registros de ação com o parâmetro EnableCloudTrailForASRActionLog no momento da implantação. Quando você observa mudanças inesperadas de recursos em qualquer uma das suas contas da AWS, esse widget pode ajudá-lo a entender se os recursos foram modificados pela solução.

O CloudWatch painel também vem com alarmes predefinidos que alertam sobre erros operacionais comuns.

1. Execuções do State Machine > 1000 em um período de 24 horas.

   a. Um grande aumento nas execuções de remediação pode indicar que uma regra de evento está sendo iniciada com mais frequência do que o pretendido.

   b. O limite pode ser alterado usando o CloudFormation parâmetro.

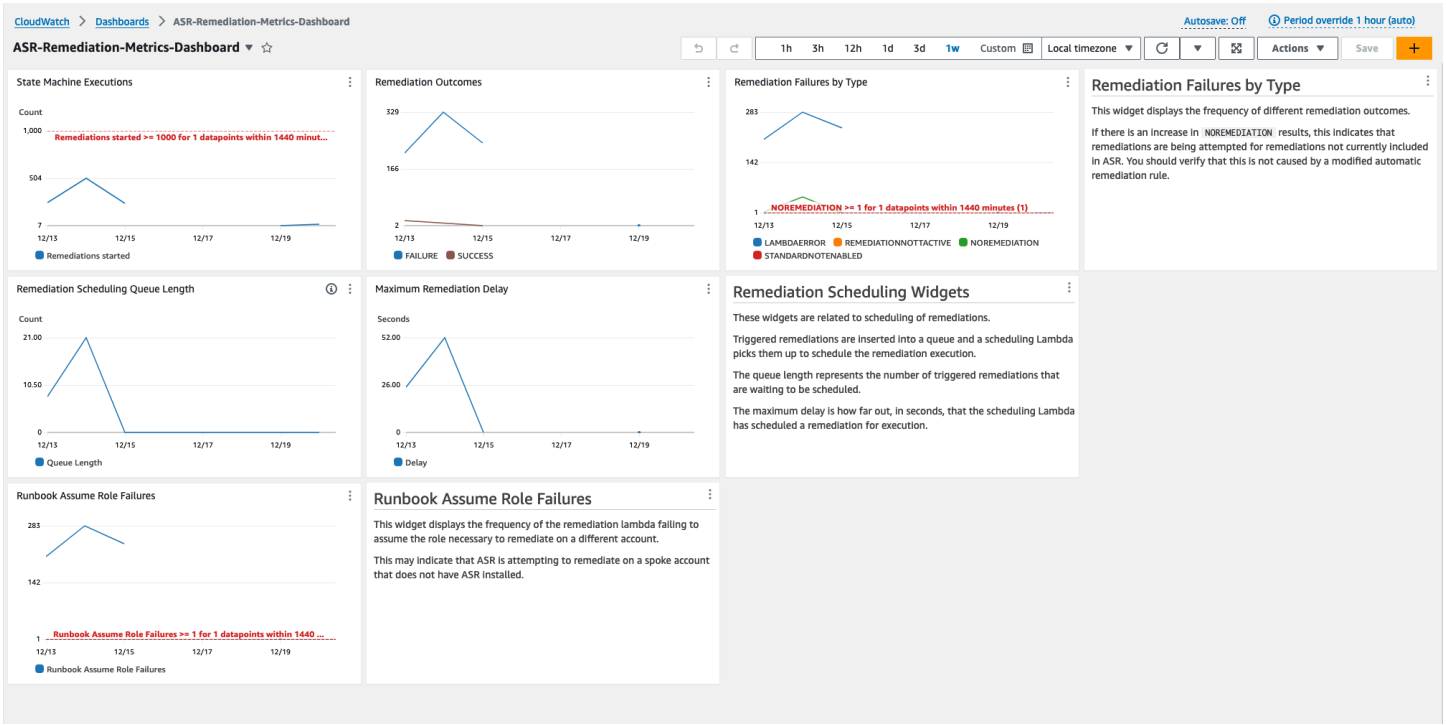
2. Falhas de remediação por tipo = NOREMEDIAÇÃO > 0

   a. As remediações estão sendo tentadas para remediações que não estão incluídas no ASR. Isso pode indicar que uma regra de evento foi modificada para incluir mais do que as remediações pretendidas.

3. Falhas de função do Runbook Assume > 0

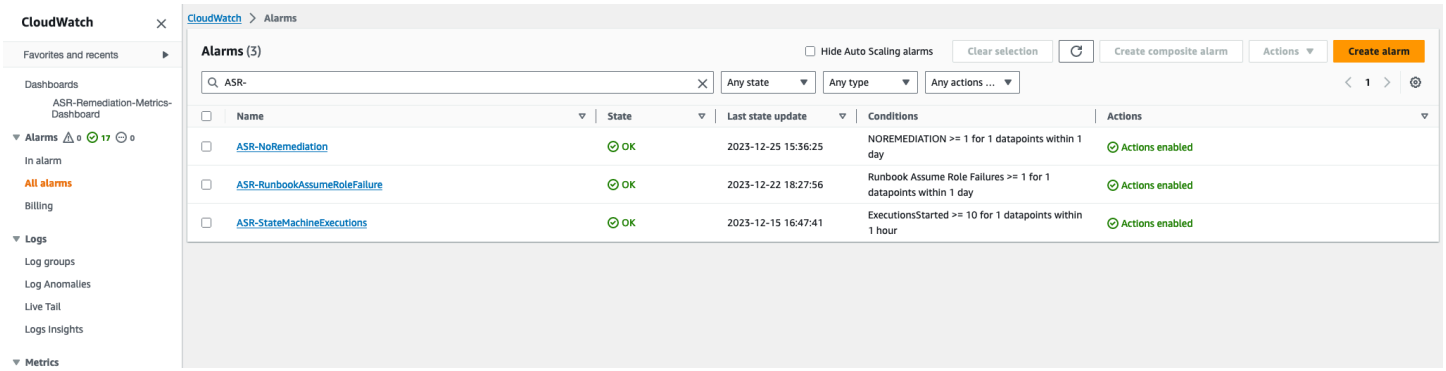
   a. As correções estão sendo tentadas em contas ou regiões que não têm a solução implantada adequadamente. Isso pode indicar que uma regra de evento foi modificada para incluir mais contas do que o pretendido.

Todos os limites de alarme podem ser modificados para atender às necessidades individuais de implantação.

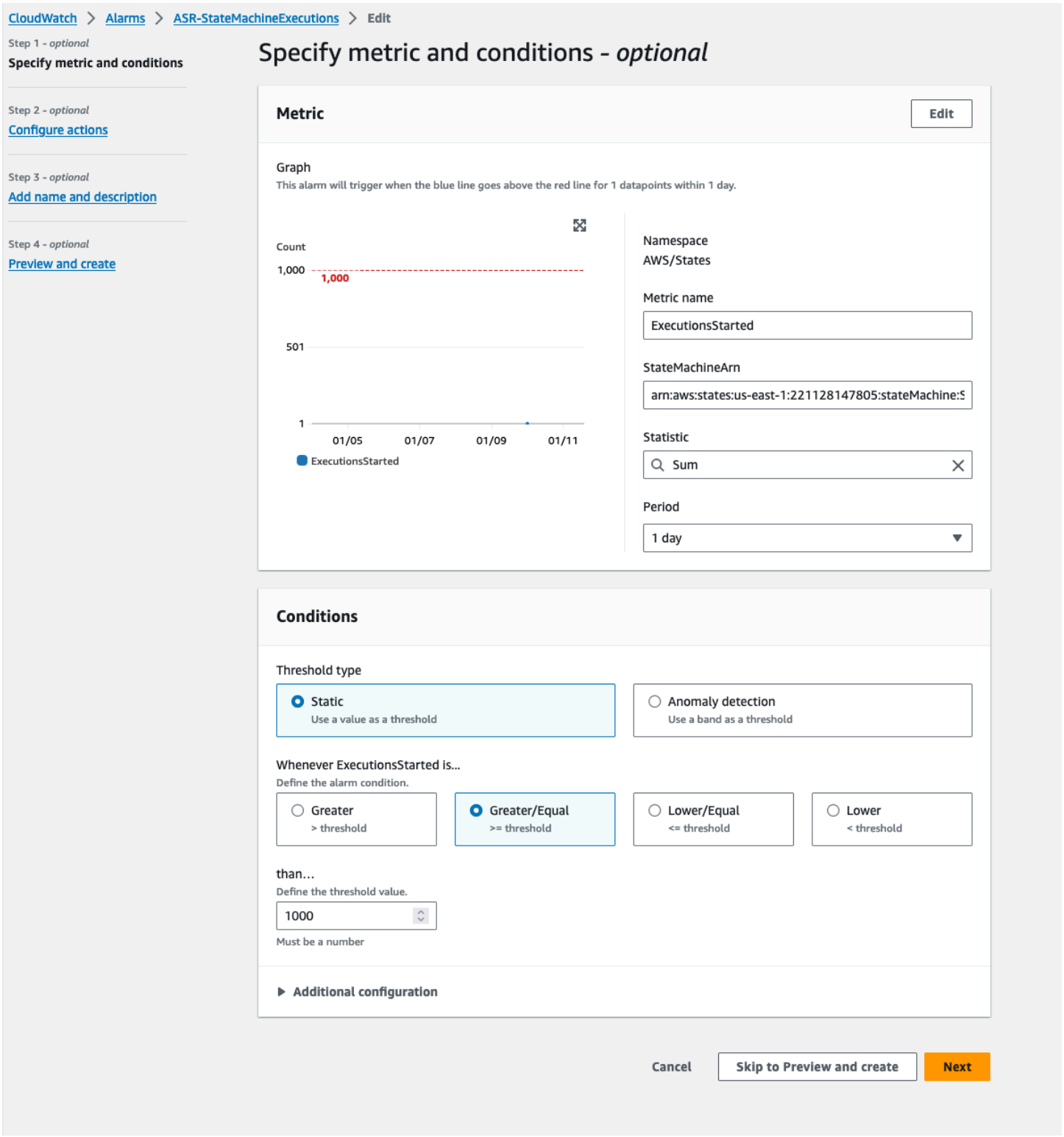


Modificando os limites de alarme

1. Navegue até Amazon CloudWatch → Alarmes → Todos os alarmes.
2. Escolha o Alarme que você gostaria de modificar e selecione Ações → Editar.



1. Altere o limite para o valor desejado e salve.



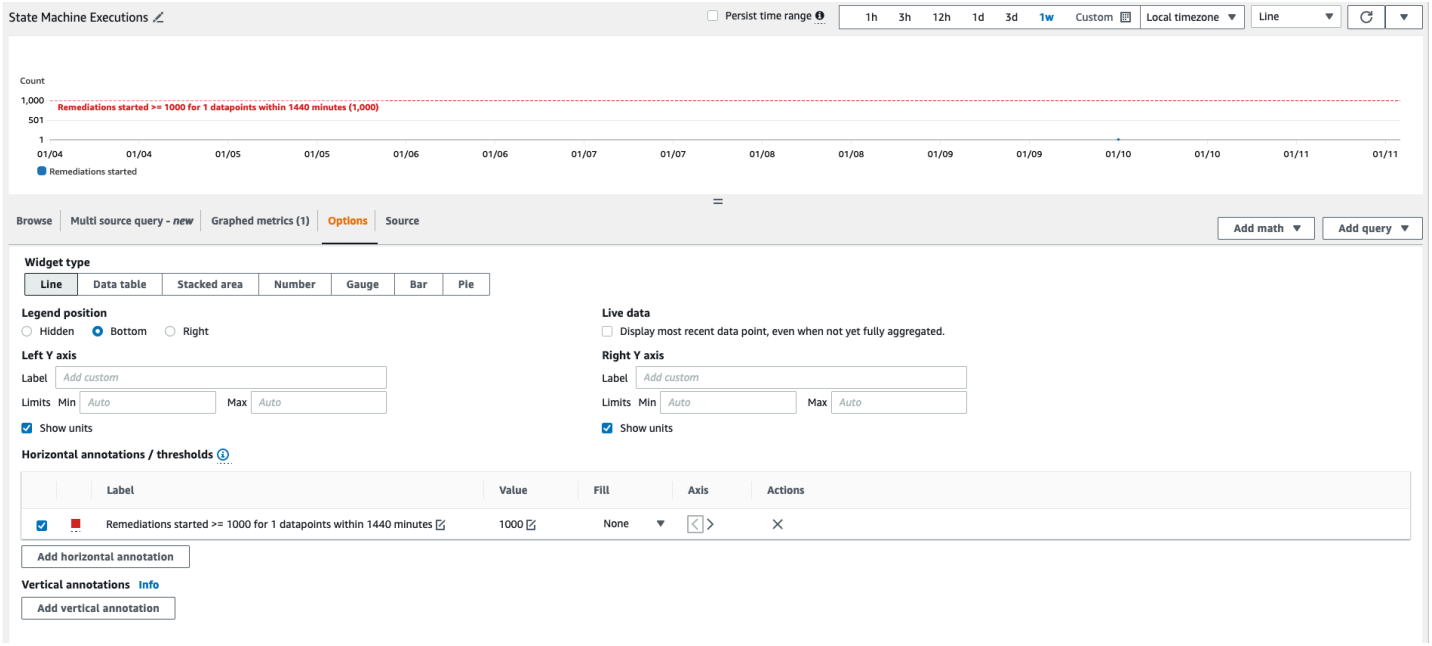
1. Navegue até o CloudWatch painel para modificar os gráficos de acordo com as novas configurações.

   a. Selecione as reticências no canto superior direito do widget correspondente.

b. Selecione Editar.

c. Vá para a guia Opções.

d. Modifique a anotação do alarme para corresponder às novas configurações.



Inscrever-se para receber notificações de alarme

Na conta de administrador, assine o tópico do Amazon SNS criado pela pilha de administradores, SO0111-ASR_Alarm_Topic. Isso o notificará quando um alarme entrar no estado ALARM.

Atualizar a solução

Important

- Ao atualizar a solução, as regras automatizadas de remediação talvez precisem ser reativadas manualmente na conta do administrador. Consulte Habilitar remediações totalmente automatizadas.
- Se você estiver usando o `Reuse Orchestrator Log Group` parâmetro para reter registros, verifique se ele está definido adequadamente durante a atualização da pilha para evitar a recriação do grupo de registros ou a perda das configurações de retenção de registros. Consulte Implantar a solução. Se você estiver executando uma atualização de pilha para a v2.3.0+ a partir de uma versão anterior, escolha “não”

Atualização de versões anteriores à v1.4

Se você já implantou a solução antes da v1.4.x, desinstale e instale a versão mais recente:

1. Desinstale a solução implantada anteriormente. Consulte Desinstalar a solução.
2. Inicie o modelo mais recente. Consulte Implantar a solução.

Note

Se você estiver atualizando da v1.2.1 ou anterior para a v1.3.0 ou posterior, defina Usar grupo de registros do orquestrador existente como. No Se você estiver reinstalando a v1.3.0 ou posterior, poderá selecionar essa opçãoYes. Essa opção permite que você continue fazendo login no mesmo grupo de registros do Orchestrator Step Functions.

Atualizando da versão 1.4 e versões posteriores

Se você estiver atualizando a partir da v1.4.x, atualize todas as pilhas da seguinte forma: StackSets

1. Atualize a pilha na conta de administrador do Security Hub usando o modelo mais recente.
2. Em cada conta de membro, atualize as permissões do modelo mais recente.

3. Em cada conta de membro em todas as regiões em que está implantada atualmente, atualize a pilha de membros a partir do modelo mais recente.
4. Se a interface do usuário da Web estiver ativada e você tiver atualizado parâmetros como`TicketGenFunctionName`, invalide o CloudFront cache para refletir as alterações imediatamente:

```
aws cloudfront create-invalidation \
  --distribution-id <distribution-id> \
  --paths "/aws-exports.json"
```

Atualizando a partir da v2.0.x

Se você estiver atualizando da v2.0.x, atualize para a v2.1.2 ou posterior. A atualização para v2.1.0 - v2.1.1 falhará. CloudFormation

Atualizando a partir da versão 2.1.4 ou anterior

Se você estiver atualizando da v2.1.4 ou anterior, deverá atualizar para a v2.3.0 antes de atualizar para qualquer versão superior à v2.3.0. Caso contrário, a operação de atualização da pilha falhará. Como alternativa, você pode excluir e reimplantar as pilhas da solução em vez de realizar uma atualização da pilha.

Solução de problemas

A resolução de problemas conhecidos fornece instruções para mitigar erros conhecidos. Se essas instruções não resolverem seu problema, o Contact AWS Support fornece instruções para abrir um caso do AWS Support para essa solução.

Registros da solução

Esta seção inclui informações sobre solução de problemas dessa solução. Consulte a navegação à esquerda para ver os tópicos.

Essa solução coleta resultados de runbooks de remediação, que são executados sob o AWS Systems Manager, e registra o resultado `S00111-ASR` no grupo CloudWatch Logs na conta de administrador do AWS Security Hub. Há um stream por controle por dia.

O Orchestrator Step Functions registra todas as transições de etapas no Grupo `S00111-ASR-Orchestrator` CloudWatch Logs na conta de administrador do AWS Security Hub. Esse log é uma trilha de auditoria para registrar as transições de estado para cada instância do Step Functions. Há um fluxo de log por execução do Step Functions.

Ambos os grupos de log são criptografados usando uma chave de gerente de cliente (CMK) do AWS KMS.

As informações de solução de problemas a seguir usam o grupo de `S00111-ASR` registros. Use esse log, bem como o console do AWS Systems Manager Automation, os registros do Automation Executions, o console Step Function e os logs do Lambda para solucionar problemas.

Se uma correção falhar, uma mensagem semelhante à seguinte será registrada `S00111-ASR` no fluxo de log para o padrão, o controle e a data. Por exemplo: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

As mensagens a seguir fornecem detalhes adicionais. Essa saída é do manual de execução do ASR para o padrão e controle de segurança. Por exemplo: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Essas informações apontam para a falha, que nesse caso foi uma automação infantil em execução na conta do membro. Para solucionar esse problema, você deve fazer login no AWS Management Console na conta do membro (da mensagem acima), acessar o AWS Systems Manager, navegar até Automation e examinar a saída do log para o ID `eecdef79-9111-4532-921a-e098549f525` de Execução.

Resolução de problemas conhecidos

- Problema: A implantação da solução falha com um erro informando que os recursos já estão disponíveis na Amazon CloudWatch.

  Resolução: verifique se há uma mensagem de erro na seção CloudFormation recursos/eventos indicando que grupos de registros já existem. Os modelos de implantação do ASR permitem a reutilização de grupos de registros existentes. Verifique se você selecionou a reutilização.

- Problema: a solução falha ao ser implantada com um erro em uma pilha aninhada do manual em que uma EventBridge regra não é criada

  Resolução: você provavelmente atingiu a cota de EventBridge regras com o número de manuais implantados. Você pode evitar isso usando as descobertas de controle consolidadas no Security Hub combinadas com o manual do SC nesta solução, implantando somente os manuais dos padrões usados ou solicitando um aumento na cota de regras. EventBridge

- Problema: eu executo o Security Hub em várias regiões na mesma conta. Quero implantar essa solução em várias regiões.

  Resolução: implante a pilha administrativa na mesma conta e região do administrador do Security Hub. Instale o modelo de membro em cada conta e região em que você tem um membro do Security Hub configurado. Ative a agregação no Security Hub.

- Problema: imediatamente após a implantação, o SO0111-ASR-Orchestrator está falhando no estado do documento Get Automation com um erro 502: “`O Lambda não conseguiu descriptografar as variáveis de ambiente porque o acesso ao KMS foi negado. Verifique as configurações da tecla KMS da função. Exceção KMS: Mensagem UnrecognizedClientException KMS: o token de segurança incluído na solicitação é inválido. (Serviço: AWSLambda; Código de status: 502; Código de erro: KMSAccessDeniedException; ID da solicitação:... `”

Resolução: aguarde a estabilização da solução por cerca de 10 minutos antes de executar as correções. Se o problema persistir, abra um ticket de suporte ou GitHub problema.

- Problema: tentei corrigir uma descoberta, mas nada aconteceu.

  Resolução: Verifique as notas da descoberta para saber os motivos pelos quais ela não foi corrigida. Uma causa comum é que a descoberta não tem remediação automática. No momento, não há como fornecer feedback direto ao usuário quando não existe nenhuma correção além das notas. Analise os registros da solução. Abra CloudWatch Logs no console. Encontre o grupo SO0111 de CloudWatch registros -ASR. Classifique a lista para que os streams atualizados mais recentemente apareçam primeiro. Selecione o fluxo de log para a descoberta que você tentou executar. Você deve encontrar algum erro lá. Alguns motivos para a falha podem ser: incompatibilidade entre o controle de descoberta e o controle de remediação, remediação entre contas (ainda não suportada) ou o fato de a descoberta já ter sido corrigida. Se não conseguir determinar o motivo da falha, colete os registros e abra um ticket de suporte.

- Problema: depois de iniciar uma correção, o status no console do Security Hub não foi atualizado.

  Resolução: o console do Security Hub não é atualizado automaticamente. Atualize a exibição atual. O status da descoberta deve ser atualizado. Pode levar várias horas para que a descoberta passe de Falha para Aprovada. As descobertas são criadas a partir de dados de eventos enviados por outros serviços, como o AWS Config, para o AWS Security Hub. O tempo até que uma regra seja reavaliada depende do serviço subjacente. Se isso não resolver o problema, consulte a resolução anterior para “`Eu tentei corrigir uma descoberta, mas nada aconteceu. `”

- Problema: a função de etapa do orquestrador falha em Obter estado do documento de automação: ocorreu um erro (AccessDenied) ao chamar a AssumeRole operação.

  Resolução: O modelo de membro não foi instalado na conta do membro em que o ASR está tentando corrigir uma descoberta. Siga as instruções para a implantação do modelo de membro.

- Problema: o runbook do Config.1 falha porque o gravador ou o canal de entrega já existe.

  Resolução: inspecione suas configurações do AWS Config com cuidado para garantir que o Config esteja configurado corretamente. A remediação automatizada não é capaz de corrigir as configurações existentes do AWS Config em alguns casos.

- Problema: a correção foi bem-sucedida, mas retorna a mensagem `"No output available yet because the step is not successfully executed."`

Resolução: Esse é um problema conhecido nesta versão em que determinados runbooks de correção não retornam uma resposta. Os runbooks de remediação falharão adequadamente e sinalizarão a solução se não funcionarem.

- Problema: a resolução falhou e enviou um rastreamento de pilha.

  Resolução: ocasionalmente, perdemos a oportunidade de lidar com uma condição de erro que resulta em um rastreamento de pilha em vez de uma mensagem de erro. Tente solucionar o problema a partir dos dados de rastreamento. Abra um ticket de suporte se precisar de ajuda.

- Problema: a remoção da pilha v1.3.0 falhou no recurso de ação personalizada.

  Resolução: a remoção do modelo administrativo pode falhar na remoção da Ação Personalizada. Esse é um problema conhecido que será corrigido na próxima versão. Se isso ocorrer:

  a. Faça login no console de gerenciamento do AWS Security Hub.
  b. Na conta de administrador, acesse Configurações.
  c. Selecione a guia Ações personalizadas
  d. Exclua manualmente a entrada Remediate with ASR.
  e. Exclua a pilha novamente.

- Problema: depois de reimplantar a pilha de administração, a função step está falhando. `AssumeRole`

  Resolução: a reimplantação da pilha de administração quebra a conexão de confiança entre a função de administrador na conta de administrador e a função de membro nas contas de membros. Você deve reimplantar a pilha de funções dos membros em todas as contas dos membros.

- Problema: as correções do CIS 3.x não aparecem `PASSED` após mais de 24 horas.

  Resolução: Essa é uma ocorrência comum se você não tiver assinaturas do tópico do `SO0111-ASR_LocalAlarmNotification` SNS na conta do membro.

Problemas com correções específicas

A definição SSLBucket de política falha com AccessDenied erro

Controles associados: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

Problema: a SSLBucket política definida falha com um AccessDenied erro:

Ocorreu um erro (AccessDenied) ao chamar a PutBucketPolicy operação: Acesso negado

Se a configuração Bloquear acesso público tiver sido ativada para um bucket, as tentativas de colocar uma política de bucket que inclua instruções que permitam o acesso público falharão com esse erro. Esse estado pode ser alcançado colocando uma política de bucket que contenha essas declarações e, em seguida, habilitando o bloco de acesso público para esse bucket.

O ConfigureS3 de remediação BucketPublicAccessBlock (controles associados: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) também pode colocar um bucket nesse estado porque define a configuração do bloco de acesso público sem alterar a política do bucket.

O Set SSLBucket Policy adiciona uma declaração à política do bucket para negar solicitações que não usam SSL. Ela não modifica as outras declarações na política, portanto, se houver declarações que permitam o acesso público, a remediação falhará ao tentar colocar a política de bucket modificada que ainda inclua essas declarações.

Resolução: modifique a política do bucket para remover declarações que permitem acesso público em conflito com a configuração de bloqueio de acesso público no bucket.

O PuTs3 falha BucketPolicyDeny

Controles associados: AWS FSBP v1.0.0 S3.6, (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2

Problema: O PuTs3 BucketPolicyDeny com o seguinte erro:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Se os principais de todas as políticas no intervalo de destino forem “*”, a solução não poderá adicionar a política de negação ao intervalo de destino, pois isso bloquearia todas as ações do intervalo de todos os principais.

Resolução: modifique a política do bucket para permitir ações em contas específicas em vez de usar os principais “*” e restrinja as ações negadas.

Como desativar a solução

No caso de um incidente, você pode achar que precisa desativar a solução sem remover nenhuma infraestrutura. Esses cenários detalham como desativar diferentes componentes na solução.

Cenário 1: desabilitar a remediação automática para um único controle

1. Na conta de administrador, navegue até o CloudFormation console da AWS.
2. Localize a pilha Admin e visualize sua guia Saídas.
3. Copie o valor da `RemediationConfigurationDynamoDBTable` saída.
4. Navegue até o console do DynamoDB e abra a tabela de configuração de remediação.
5. Selecione Explore Table Items (Explorar itens da tabela).
6. Em Digitalizar ou consultar itens, selecione Consulta.
7. Insira o ID do controle (por exemplo,`Lambda.1`) no campo Chave de partição: ID do controle e clique em Executar.
8. Selecione o item devolvido e clique em Ações > Editar item.
9. Altere o valor do `automatedRemediationEnabled` atributo para False.
10. Clique em Salvar e fechar.

Cenário 2: desabilitar a correção automática para todos os controles

1. Siga as etapas 1 a 5 do Cenário 1 para acessar os itens da tabela de Configuração de Remediação.
2. Em Digitalizar ou consultar itens, selecione Digitalizar para ver todos os controles.
3. Para cada controle `automatedRemediationEnabled` definido como Verdadeiro, selecione o item e clique em Ações > Editar item.
4. Altere o valor do `automatedRemediationEnabled` atributo para False e clique em Salvar e fechar.
5. Repita o procedimento para todos os controles que você deseja desativar.

Cenário 3: desabilitar a correção manual para uma conta

1. Navegue até o console do EventBridge .
2. Selecione Regras na barra lateral.
3. Selecione o barramento de eventos padrão e pesquise por`Remediate_with_ASR_CustomAction`.
4. Selecione a regra e clique no botão Desativar.

Entrar em contato com o AWS Support

Se você tem o AWS Business Support+, o AWS Enterprise Support ou o Unified Operations, você pode usar o AWS Support Center para obter assistência especializada com essa solução. As seções a seguir dão instruções.

Criar caso

1. Faça login na Central de suporte.
2. Escolha Criar caso.

Como podemos ajudar?

1. Escolha Técnico.
2. Em Serviço, selecione Soluções.
3. Em Categoria, selecione Outras soluções.
4. Em Severidade, selecione a opção que melhor corresponda ao seu caso de uso.
5. Quando você insere o Serviço, a Categoria e a Gravidade, a interface preenche links para perguntas comuns de solução de problemas. Se você não conseguir resolver sua pergunta com esses links, escolha Próxima etapa: mais informações.

Mais informações

1. Em Assunto, insira um texto resumindo sua pergunta ou problema.
2. Para Descrição, descreva o problema em detalhes, incluindo o nome dessa solução e a versão que você está usando, como este exemplo: Automated Security Response on AWS vX.Y.Z.
3. Selecione Anexar arquivos.
4. Anexe as informações de que o suporte precisa para processar a solicitação.

Ajude-nos a resolver seu caso com mais rapidez

1. Insira as informações solicitadas.
2. Escolha Próxima etapa: solucione ou entre em contato conosco.

Solucione ou entre em contato conosco

1. Analise as soluções Solucionar agora.
2. Se você não conseguir resolver seu problema com essas soluções, escolha Fale conosco, insira as informações solicitadas e escolha Enviar.

Desinstalar a solução

Use o procedimento a seguir para desinstalar a solução com o AWS Management Console.

V1.0.0-V1.2.1

Para as versões v1.0.0 a v1.2.1, use o Service Catalog para desinstalar os playbooks do CIS FSBP. and/or Com a v1.3.0, o Service Catalog não é mais usado.

1. Faça login no CloudFormation console da AWS e navegue até a conta principal do Security Hub.
2. Escolha Service Catalog para encerrar qualquer manual provisionado, remover grupos de segurança, funções ou usuários.
3. Remova o `CISPermissions.template` modelo spoke das contas dos membros do Security Hub.
4. Remova o `AFSBPMemberStack.template` modelo spoke das contas de administrador e membro do Security Hub.
5. Navegue até a conta principal do Security Hub, selecione a pilha de instalação da solução e escolha Excluir.

> **Note**
>
> CloudWatch Os registros do grupo de registros são mantidos. Recomendamos reter esses registros conforme exigido pela política de retenção de registros da sua organização.

V1.3.x

1. Remova o `automated-security-response-member.template` da conta de cada membro.
2. Remova o `automated-security-response-admin.template` da conta de administrador.

> **Note**
>
> A remoção do modelo administrativo na v1.3.0 provavelmente falhará na remoção da Ação Personalizada. Esse é um problema conhecido que será corrigido na próxima versão. Use as instruções a seguir para corrigir esse problema:

1. Faça login no console de gerenciamento do AWS Security Hub.
2. Na conta de administrador, acesse Configurações.
3. Selecione a guia Ações personalizadas.
4. Exclua manualmente a entrada Remediate with ASR.
5. Exclua a pilha novamente.

V1.4.0 e versões posteriores

Implantação do Stack

1. Remova o `automated-security-response-member.template` da conta de cada membro.
2. Remova o `automated-security-response-admin.template` da conta de administrador.

StackSet implantação

Para cada uma StackSet, remova as pilhas e, em seguida, remova-as StackSet na ordem inversa da implantação.

Observe que as funções do IAM do `automated-security-response-member-roles.template` são mantidas mesmo que o modelo seja removido. Isso é para que as remediações usando essas funções continuem funcionando. Essas funções SO0111-* podem ser removidas manualmente após a verificação de que não estão mais em uso por meio de remediações ativas, como CloudWatch registro ou monitoramento aprimorado do CloudTrail RDS.

Guia do administrador

Ativando e desativando partes da solução

Como administrador da solução, você tem os seguintes controles sobre quais funcionalidades da solução estão habilitadas.

Onde as pilhas de membros e funções de membros são implantadas:

- A pilha administrativa só poderá iniciar correções (por meio de ação personalizada ou totalmente automatizada) em contas nas quais as pilhas de funções de membro e membro tenham sido implantadas com o número da conta do administrador fornecido como um valor de parâmetro.
- Para isentar completamente as contas ou regiões do controle da solução, não implante as pilhas de membros ou funções de membros nessas contas ou regiões.

Configuração de agregação de localização de conta e região no Security Hub:

- A pilha administrativa só poderá iniciar correções (por meio de ação personalizada ou totalmente automatizada) para descobertas que chegarem à conta do administrador e à região.
- Para isentar completamente as contas ou regiões do controle da solução, não inclua essas contas ou regiões para enviar descobertas para a mesma conta de administrador e região em que a pilha administrativa está implantada.

Quais pilhas aninhadas padrão são implantadas:

- A pilha de administração só poderá iniciar correções (por meio de ação personalizada ou totalmente automatizada) para controles que tenham um runbook de controle implantado na conta e região do membro de destino. Eles são implantados pela pilha de membros para cada padrão.
- A pilha administrativa só poderá iniciar remediações totalmente automatizadas para controles habilitados na tabela de configuração de remediação do DynamoDB. Essa tabela é implantada na conta do administrador.
- Para simplificar, recomendamos a implantação consistente de padrões em suas contas de administrador e membro. Se você se preocupa com o AWS FSBP e o CIS v1.2.0, implante essas duas pilhas de administração aninhadas na conta de administrador e implante essas duas pilhas de membros aninhadas em cada conta membro e região.

Quais runbooks de controle são implantados em cada pilha de membros aninhada:

- A pilha de administração só poderá iniciar remediações (por meio de ação personalizada ou totalmente automatizada) para controles que tenham um runbook de controle implantado na conta do membro alvo e na região pela pilha de membros para cada padrão.
- Para exercer um controle mais refinado sobre quais controles estão habilitados para um determinado padrão, cada pilha aninhada de um padrão tem parâmetros para os quais os runbooks de controle são implantados. Defina o parâmetro de um controle com o valor “NÃO disponível” para desimplantar esse runbook de controle.

Parâmetros SSM para ativar e desativar padrões:

- A pilha de administração só poderá iniciar correções (por meio de ação personalizada ou totalmente automatizada) para padrões habilitados por meio do parâmetro SSM implantado pela pilha de administração padrão.
- <standard_name><standard_version>Para desativar um padrão, defina o valor do Parâmetro SSM com o caminho “/Solutions/SO0111///status" como “Não”.

Acesso à interface de usuário da Web da solução:

- Quando a pilha de administração for implantada, você receberá um e-mail com credenciais temporárias para entrar na interface de usuário da Web usando o endereço de e-mail fornecido durante a implantação.
- Usando a página Convidar usuários, administradores e administradores delegados podem convidar usuários adicionais para acessar a interface de usuário da Web e delegar acesso à solução.
- Usando a página Exibir usuários, administradores e administradores delegados podem visualizar e gerenciar usuários existentes.
- Para saber mais sobre permissões e como usar a interface de usuário da Web da solução, consulte the section called “Interface do usuário da Web” o.

Exemplo de notificações de SNS

Quando uma remediação é iniciada

```
{
```

```
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando uma remediação é bem-sucedida

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando uma remediação falha

```
{
```

```
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Tutorial

Este é um tutorial que o guiará em sua primeira implantação do ASR. Começará com os pré-requisitos para a implantação da solução e terminará com você corrigindo exemplos de descobertas em uma conta de membro.

Tutorial: Introdução ao Automated Security Response na AWS

Este é um tutorial que o guiará em sua primeira implantação. Começará com os pré-requisitos para a implantação da solução e terminará com você corrigindo exemplos de descobertas em uma conta de membro.

Prepare as contas

Para demonstrar os recursos de remediação entre contas e regiões da solução, este tutorial usará duas contas. Você também pode implantar a solução em uma única conta.

Os exemplos a seguir usam contas `111111111111` e demonstram `222222222222` a solução. `111111111111`será a conta do administrador e `222222222222` será a conta do membro. Vamos configurar a solução para remediar as descobertas de recursos nas regiões `us-east-1` e. `us-west-2`

A tabela abaixo é um exemplo para ilustrar as ações que tomaremos em cada etapa em cada conta e região.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
`111111111111`	Administrador	Nenhum	Nenhum
`222222222222`	Membro	Nenhum	Nenhum

A conta de administrador é a conta que executará as ações administrativas da solução, ou seja, iniciar as remediações manualmente ou ativar a remediação totalmente automatizada usando a tabela do DynamoDB de configuração de remediação. Essa conta também deve ser a conta de administrador delegado do Security Hub para todas as contas nas quais você deseja corrigir descobertas, mas não precisa ser nem deve ser a conta de administrador do AWS Organizations para a organização da AWS à qual suas contas pertencem.

Habilitar o AWS Config

Analise a seguinte documentação:

- Documentação do AWS Config
- Definição de preço do AWS Config
- Habilitando o AWS Config

Habilite o AWS Config em ambas as contas e em ambas as regiões. Isso incorrerá em cobranças.

> **Important**
>
> Certifique-se de selecionar a opção “Incluir recursos globais (por exemplo, recursos do AWS IAM)”. Se você não selecionar essa opção ao ativar o AWS Config, você não verá descobertas relacionadas a recursos globais (por exemplo, recursos do AWS IAM)

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Habilitar o AWS Config	Habilitar o AWS Config
222222222222	Membro	Habilitar o AWS Config	Habilitar o AWS Config

Habilite o hub de segurança da AWS

Analise a seguinte documentação:

- Documentação do AWS Security Hub
- Preços do AWS Security Hub
- Habilitando o AWS Security Hub

Habilite o AWS Security Hub em ambas as contas e em ambas as regiões. Isso incorrerá em cobranças.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Habilite o AWS Security Hub	Habilite o AWS Security Hub
222222222222	Membro	Habilite o AWS Security Hub	Habilite o AWS Security Hub

Possibilite descobertas consolidadas de controle

Analise a seguinte documentação:

- Gerando e atualizando descobertas de controle

Para os fins deste tutorial, demonstraremos o uso da solução com o recurso consolidado de descobertas de controle do AWS Security Hub ativado, que é a configuração recomendada. Em partições que não oferecem suporte a esse recurso no momento em que este artigo foi escrito, você precisará implantar os manuais específicos do padrão em vez do SC (Controle de Segurança).

Possibilite descobertas de controle consolidadas em ambas as contas e em ambas as regiões.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Possibilite descobertas consolidadas de controle	Possibilite descobertas consolidadas de controle
222222222222	Membro	Possibilite descobertas consolidadas de controle	Possibilite descobertas consolidadas de controle

Pode levar algum tempo para que as descobertas sejam geradas com o novo recurso. Você pode continuar com o tutorial, mas não conseguirá corrigir as descobertas geradas sem o novo recurso. As descobertas geradas com o novo recurso podem ser identificadas pelo valor do `GeneratorId` campo`security-control/<control_id>`.

Configurar a agregação de localização entre regiões

Analise a seguinte documentação:

- Agregação entre regiões
- Habilitando a agregação entre regiões

Configure a agregação de localização de us-west-2 a us-east-1 em ambas as contas.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Configurar a agregação de us-west-2	Nenhum
222222222222	Membro	Configurar a agregação de us-west-2	Nenhum

Pode levar algum tempo para que as descobertas se propaguem para a região de agregação. Você pode continuar com o tutorial, mas não poderá corrigir descobertas de outras regiões até que elas comecem a aparecer na região de agregação.

Designar uma conta de administrador do Security Hub

Analise a seguinte documentação:

- Gerenciamento de contas no AWS Security Hub
- Gerenciando contas de membros da organização
- Gerenciando contas de membros por convite

No exemplo a seguir, usaremos o método de convite manual. Para um conjunto de contas de produção, recomendamos gerenciar a administração delegada do Security Hub por meio do AWS Organizations.

No console do AWS Security Hub na conta de administrador (111111111111), convide a conta membro (222222222222) para aceitar a conta de administrador como administrador delegado do Security Hub. Na conta do membro, aceite o convite.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Convide a conta do membro	Nenhum
222222222222	Membro	Aceite o convite	Nenhum

Pode levar algum tempo para que as descobertas se propaguem para a conta do administrador. Você pode continuar com o tutorial, mas não poderá corrigir as descobertas das contas dos membros até que elas comecem a aparecer na conta do administrador.

Crie as funções para permissões autogerenciadas StackSets

Analise a seguinte documentação:

- AWS CloudFormation StackSets
- Conceda permissões autogerenciadas

Vamos implantar CloudFormation pilhas em várias contas, então usaremos. StackSets Não podemos usar permissões gerenciadas pelo serviço porque a pilha de administradores e a pilha de membros têm pilhas aninhadas, que não são suportadas pelo serviço, portanto, devemos usar permissões autogerenciadas.

Implante as pilhas para obter permissões básicas para StackSet operações. Para contas de produção, talvez você queira restringir as permissões de acordo com a documentação de “opções de permissões avançadas”.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar a pilha de funções de StackSet administrador	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
		Implante a pilha StackSet de funções de execução	
222222222222	Membro	Implante a pilha StackSet de funções de execução	Nenhum

Crie os recursos inseguros que gerarão exemplos de descobertas

Analise a seguinte documentação:

- Referência de controles do Security Hub
- Controles do AWS Lambda

O exemplo a seguir é um recurso com uma configuração insegura para demonstrar uma remediação. O exemplo de controle é o Lambda.1: As políticas da função Lambda devem proibir o acesso público.

> **Important**
>
> Estaremos criando intencionalmente um recurso com uma configuração insegura. Analise a natureza do controle e avalie por si mesmo o risco de criar esse recurso em seu ambiente. Esteja ciente de qualquer ferramenta que sua organização possa ter para detectar e relatar esses recursos e solicite uma exceção, se apropriado. Se o controle de exemplo que selecionamos não for adequado para você, selecione outro controle compatível com a solução.

Na segunda região da conta do membro, navegue até o console do AWS Lambda e crie uma função no tempo de execução mais recente do Python. Em Configuração → Permissões, adicione uma declaração de política para permitir a invocação da função a partir da URL sem autenticação.

Confirme na página do console se a função permite acesso público. Depois que a solução corrigir esse problema, compare as permissões para confirmar que o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Crie uma função Lambda com uma configuração insegura

Pode levar algum tempo para que o AWS Config detecte a configuração insegura. Você pode continuar com o tutorial, mas não conseguirá corrigir a descoberta até que o Config a detecte.

Crie grupos de CloudWatch registros para controles relacionados

Analise a seguinte documentação:

- Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs
- CloudTrail controles

Vários CloudTrail controles suportados pela solução exigem que haja um grupo de CloudWatch registros que seja o destino de uma multirregião CloudTrail. No exemplo a seguir, criaremos um grupo de registros de espaço reservado. Para contas de produção, você deve configurar adequadamente a CloudTrail integração com o CloudWatch Logs.

Crie um grupo de registros em cada conta e região com o mesmo nome, por exemplo:`asr-log-group`.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Criar um grupo de logs	Criar um grupo de logs
222222222222	Membro	Criar um grupo de logs	Criar um grupo de logs

Implemente a solução em contas de tutoriais

Reúna os três Amazon S3 URLs para a pilha de funções de administrador, membro e membro.

Implante a pilha de administração

View template

automa

security-response-admin.modelo

Na conta de administrador, navegue até o CloudFormation console e implante a pilha administrativa na região de agregação de localização do Security Hub.

Escolha No o valor de todos os parâmetros para carregar pilhas administrativas aninhadas, exceto a pilha “SC” ou “Security Control”. Essa pilha contém os recursos para as descobertas de controle consolidadas que configuramos em nossas contas.

Opte No por reutilizar o grupo de registros do orquestrador, a menos que você tenha implantado essa solução nessa conta e região antes.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implante a pilha de administração	Nenhum
222222222222	Membro	Nenhum	Nenhum

Espere até que a pilha administrativa conclua a implantação antes de continuar para que uma relação de confiança possa ser criada das contas dos membros para a conta do administrador.

Implante a pilha de membros

View template

automa

security-response-member.modelo

Na conta de administrador, navegue até o CloudFormation StackSets console e implante a pilha de membros em cada conta e região. Use as funções de StackSets administração e execução criadas neste tutorial.

Insira o nome do grupo de registros que você criou como o valor do parâmetro para o nome do grupo de registros.

Escolha No o valor de todos os parâmetros para carregar pilhas de membros aninhadas, exceto a pilha “SC” ou “controle de segurança”. Essa pilha contém os recursos para as descobertas de controle consolidadas que configuramos em nossas contas.

Insira o ID da conta do administrador como o valor do parâmetro para o número da conta do administrador. Em nosso exemplo, isso é111111111111.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar o membro StackSet //Confirmar a pilha de membros implantada	Confirme se a pilha de membros foi implantada
222222222222	Membro	Confirme se a pilha de membros foi implantada	Confirme se a pilha de membros foi implantada

Implante a pilha de funções de membros

automated-security-response-memberbotão de modelo -roles.template -roles.template automated-security-response-member

Na conta de administrador, navegue até o CloudFormation StackSets console e implante a pilha de membros em cada conta. Use as funções de StackSets administração e execução criadas neste tutorial. Insira o ID da conta do administrador como o valor do parâmetro para o número da conta do administrador. Em nosso exemplo, isso é111111111111.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar o membro StackSet //Confirmar a pilha de membros implantada	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
222222222222	Membro	Confirme se a pilha de membros foi implantada	Nenhum

Você pode continuar, mas não poderá corrigir as descobertas até que a implantação seja CloudFormation StackSets concluída.

Inscreva-se no tópico do SNS

Atualizações de remediação

Tópico - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-east-1-221128147805-SO0111-ASR-tópico} [SO0111-ASR_Topic]

Na conta de administrador, assine o tópico do Amazon SNS criado pela pilha de administradores. Isso o notificará quando as remediações forem iniciadas e quando elas forem bem-sucedidas ou falharem.

Alarmes

Tópico - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-east-1-221128147805-SO0111-ASR-Alarm-topic} [SO0111-ASR_Alarm_topic]

Na conta de administrador, assine o tópico do Amazon SNS criado pela pilha de administradores. Isso o notificará quando os alarmes métricos forem iniciados.

Corrija exemplos de descobertas

Important

Este exemplo requer o uso do console CSPM do Security Hub. Atualmente, o console do Security Hub (não CSPM) não oferece suporte a correções manuais por meio de ações personalizadas. Para corrigir as descobertas sem usar o console CSPM do Security Hub, consulte a seção Remediar usando a interface de usuário da Web.

Na conta de administrador, navegue até o console CSPM do Security Hub e localize a descoberta do recurso com uma configuração insegura que você criou como parte deste tutorial.

Isso pode ser feito de diversas formas:

1. Em partições que suportam o recurso de descobertas de controle consolidado, uma página chamada “Controles” permite localizar a descoberta pelo ID de controle consolidado.
2. Na página “Padrões de segurança”, você pode localizar o controle de acordo com o padrão ao qual ele pertence.
3. Você pode ver todas as descobertas na página “Descobertas” e pesquisar por atributo.

O ID de controle consolidado para a função pública do Lambda que criamos é Lambda.1.

Inicie a remediação

Marque a caixa de seleção à esquerda da descoberta relacionada ao recurso que criamos. No menu suspenso “Ações”, selecione “Remediar com ASR”. Você verá uma notificação de que a descoberta foi enviada para a Amazon EventBridge.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Inicie a remediação	Nenhum
222222222222	Membro	Nenhum	Nenhum

Confirme se a remediação resolveu a descoberta

Você deve receber duas notificações do SNS. O primeiro indicará que uma remediação foi iniciada e o segundo indicará que a remediação foi bem-sucedida. Depois de receber a segunda notificação, navegue até o console Lambda na conta do membro e confirme se o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
222222222222	Membro	Nenhum	Confirme se a correção foi bem-sucedida

Corrija usando a interface de usuário da Web

Como alternativa, você pode usar a interface de usuário da Web da solução para corrigir as descobertas do AWS Security Hub e visualizar as remediações anteriores.

> **Note**
>
> Você deve definir o `ShouldDeployWebUI` parâmetro como “sim” ao implantar a pilha Admin para usar a interface de usuário da Web da solução.

Faça login na interface de usuário da Web

Depois de implantar a solução, você receberá um e-mail com credenciais temporárias e um link para a interface de usuário da Web da solução em no-reply@verificationemail.com. Isso será enviado para o endereço de e-mail que você forneceu ao implantar a pilha de administração.

Localize o e-mail, copie as credenciais temporárias e clique no link da interface do usuário da Web. Esse link o levará diretamente à página de login, onde você inserirá suas credenciais temporárias e definirá uma nova senha.

Localize a descoberta do Lambda.1

Depois de fazer login, você verá a página Descobertas. Esta página exibe todas as descobertas do Security Hub em sua conta de administrador do Security Hub que são suportadas para remediação, incluindo descobertas de contas de membros integradas ao AWS Security Hub.

Na página Descobertas, use a barra de pesquisa para filtrar o Resource ID inserindo o ARN da função Lambda que você criou como parte deste tutorial e realizando uma pesquisa usando o operador “=”. Isso exibirá todas as descobertas do AWS Security Hub suportadas pela solução para a função Lambda que você criou.

Para encontrar a `Lambda.1` descoberta gerada neste tutorial, aplique outro filtro em Tipo de descoberta. Clique na barra de pesquisa, selecione Tipo de busca e selecione o operador “=”. Se as descobertas de controle consolidadas estiverem habilitadas em seu ambiente, insira`security-control/Lambda.1`. Caso contrário, escolha um padrão de segurança que suporte o controle Lambda.1 e insira a ID do gerador, por exemplo. `aws-foundational-security-best-practices/v/1.0.0/Lambda.1`

Depois de aplicar os filtros Resource ID e Finding Type, você verá somente a descoberta Lambda.1 gerada pelo AWS Security Hub para seu recurso de teste listado na tabela.

> **Note**
>
> Pode levar algum tempo para que o AWS Security Hub gere a descoberta Lambda.1 para o recurso que você criou. Se você não ver a descoberta depois de aplicar os dois filtros, aguarde de 5 a 10 minutos e pesquise a descoberta novamente.

Inicie a remediação

Selecione a descoberta que você localizou na etapa anterior e clique em Ações > Remediar. Isso iniciará uma remediação para a descoberta que você selecionou.

Você pode ver o progresso dessa remediação na página Histórico de Execução. Depois de esperar alguns minutos, atualize a página Histórico de Execução clicando no ícone de atualização no canto superior direito e você verá que o Status mudou de `In progress` para. `Success`

Confirme se a remediação resolveu a descoberta

Quando a descoberta for marcada como `Resolved` pelo AWS Security Hub, ela será automaticamente removida da página Descobertas na interface de usuário da Web.

Para verificar se a correção resolveu a descoberta, navegue até o console Lambda na conta do membro e confirme se o acesso público foi revogado.

> **Note**
>
> Algumas descobertas ainda podem aparecer na página Descobertas, mesmo com um status de remediação de`Success`. Isso ocorre porque o AWS Security Hub leva até 24 horas para marcar uma descoberta como resolvida após a atualização do recurso. Você pode suprimir

descobertas que não deseja mais ver na página Descobertas selecionando a descoberta e clicando em Ações > Suprimir.

Rastreie a execução da remediação

Para entender melhor como a solução funciona, você pode rastrear a execução da remediação.

EventBridge regra

Na conta do administrador, localize uma EventBridge regra chamada CustomActionRemediate_with_ASR_. Essa regra corresponde à descoberta que você enviou do Security Hub e a envia para o Orchestrator Step Functions.

Execução de Step Functions

Na conta de administrador, localize o AWS Step Functions chamado "SO0111-ASR-Orchestrator". Essa função de etapa chama o documento de automação SSM na conta e região de destino. Você pode rastrear a execução da remediação no histórico de execução desse AWS Step Functions.

Automação SSM

Na conta do membro, navegue até o console do SSM Automation. Você encontrará duas execuções de um documento chamado "ASR-SC_2.0.0_Lambda.1" e uma execução de um documento chamado "ASR-". RemoveLambdaPublicAccess

A primeira execução é da função de etapa do orquestrador na conta de destino. A segunda execução ocorre na região alvo, que pode não ser a região da qual a descoberta se originou. A execução final é a remediação que revoga a política de acesso público da Função Lambda.

CloudWatch Grupo de registros

Na conta de administrador, navegue até o console de CloudWatch registros e localize um grupo de registros chamado "SO0111-ASR". Esse grupo de registros é o destino dos registros de alto nível do Orchestrator Step Functions.

Permita remediações totalmente automatizadas

O outro modo de operação da solução é corrigir automaticamente as descobertas à medida que elas chegam ao Security Hub.

> **Important**
>
> Antes de ativar correções totalmente automatizadas, certifique-se de que a solução esteja configurada nas contas e regiões em que você está em conformidade com a solução fazendo alterações automatizadas. Se você quiser restringir o escopo das remediações automatizadas da solução, consulte a seção abaixo sobre como filtrar remediações totalmente automatizadas.

Exemplo: habilite remediações totalmente automatizadas para o Lambda.1

A ativação de remediações automáticas iniciará as remediações em todos os recursos correspondentes ao controle que você habilita (Lambda.1).

> **Important**
>
> Confirme que você deseja que todas as Funções Lambda públicas dentro do escopo da solução tenham essa permissão revogada. As remediações totalmente automatizadas não serão limitadas em escopo à Função que você criou. A solução remediará esse controle se ele for detectado em qualquer uma das contas e regiões nas quais está instalado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Confirme se não há funções públicas desejadas	Confirme se não há funções públicas desejadas
222222222222	Membro	Confirme se não há funções públicas desejadas	Confirme se não há funções públicas desejadas

Localize a tabela de configuração de remediação do DynamoDB

Na conta Admin, veja `Outputs` a pilha do Admin no CloudFormation console. Você verá uma saída intituladaRemediationConfigurationDynamoDBTable.

Esse é o nome da tabela do DynamoDB de Configuração de Remediação, que controla as configurações de remediação automatizada para a solução. Copie o valor dessa saída e localize a tabela correspondente do DynamoDB no console do DynamoDB.

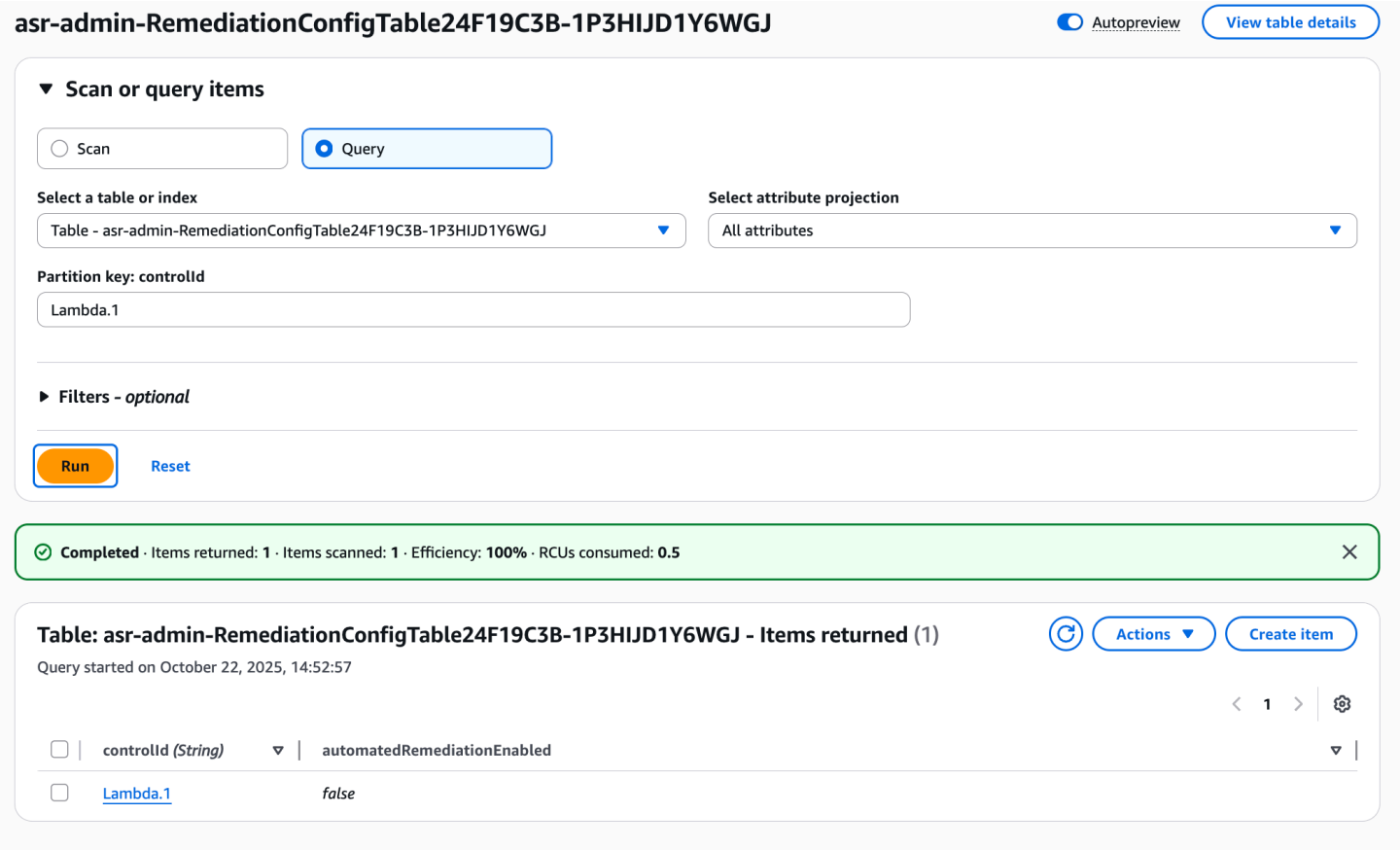
Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Localize a tabela do DynamoDB de configuração de remediação.	Nenhum
222222222222	Membro	Nenhum	Nenhum

Modificar a tabela de configuração de remediação

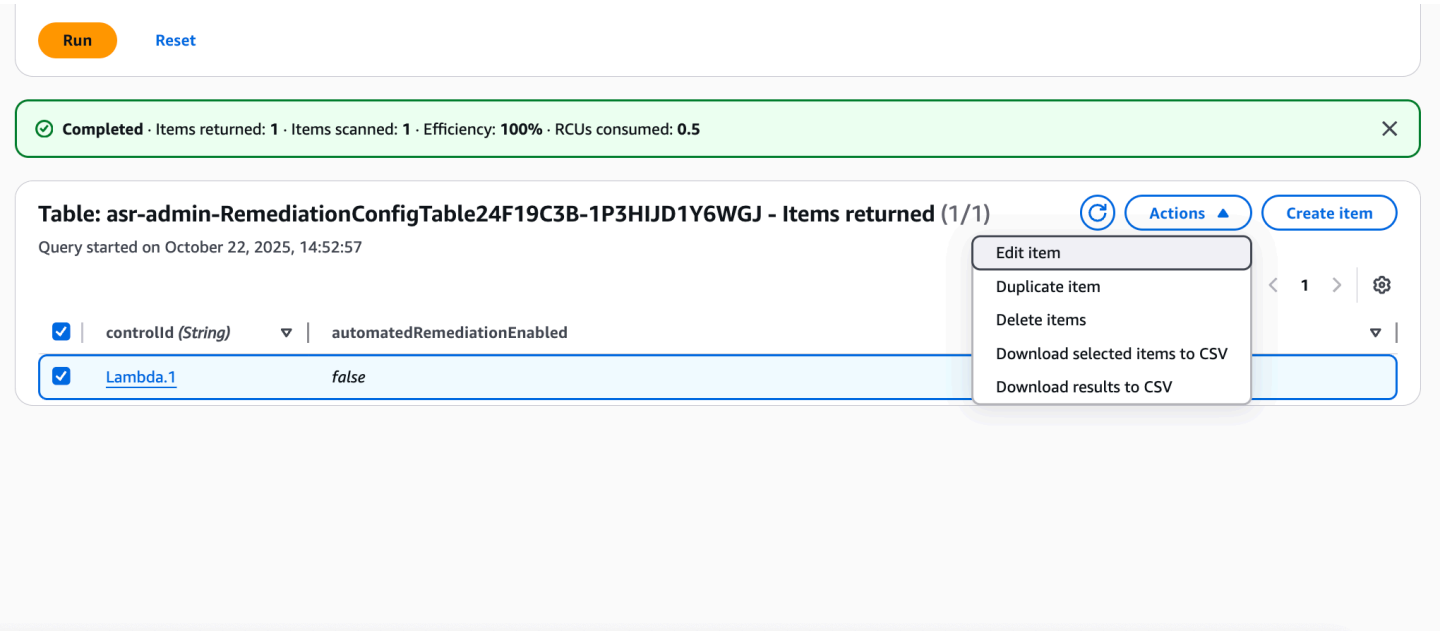
No console do DynamoDB em que você localizou a tabela de configuração de remediação, selecione Explorar itens da tabela.

Cada item na tabela corresponde a um controle do Security Hub suportado pela solução. Cada item tem um `automatedRemediationEnabled` atributo que pode ser modificado para permitir correções totalmente automatizadas para o controle associado.

Para habilitar o Lambda.1, em Digitalizar ou consultar itens, selecione Consulta. Em Chave de partição: ControlID, digite `Lambda.1` e clique em Executar. Você verá um único item retornado correspondente ao controle Lambda.1.



Agora, selecione o `Lambda.1` item e clique em Ações > Editar item.



Por fim, altere o valor do `automatedRemediationEnabled` atributo para Verdadeiro. Clique em Salvar e fechar.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Modifique a tabela do DynamoDB de configuração de remediação.	Nenhum
222222222222	Membro	Nenhum	Nenhum

Configurar o recurso

Na conta do membro, reconfigure a Função Lambda para permitir o acesso público.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Configurar a função Lambda para permitir o acesso público

Confirme se a remediação resolveu a descoberta

Pode levar algum tempo para que o Config detecte a configuração insegura novamente. Você deve receber duas notificações do SNS. O primeiro indicará que uma remediação foi iniciada. O segundo indicará que a remediação foi bem-sucedida. Depois de receber a segunda notificação, navegue até o console Lambda na conta do membro e confirme se o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Confirme se a correção foi bem-sucedida

(Opcional) Configurar a filtragem para remediações totalmente automatizadas

Se você quiser limitar o escopo no qual a solução executa correções, você pode aplicar filtros. Esses filtros se aplicarão somente a remediações totalmente automatizadas e não afetarão as remediações invocadas manualmente.

A solução oferece filtragem nas seguintes dimensões:

1. IDs da conta
2. Unidades organizacionais (OUs)
3. Tags de recursos

Cada dimensão é configurável modificando os parâmetros do Systems Manager implantados pela solução correspondente à determinada dimensão. Todos os parâmetros de filtragem no Parameter Store podem estar localizados na conta Admin abaixo do `/ASR/Filters/` caminho.

Cada dimensão tem dois parâmetros para configuração, um para o valor do filtro e outro para o modo de filtro. Por exemplo, a dimensão Account Ids tem dois parâmetros chamados `/ASR/Filters/AccountFilters` `/ASR/Filters/AccountFilterMode` e. Ambos devem ser modificados para configurar a filtragem em IDs de conta.

Por exemplo, para limitar a execução de remediações totalmente automatizadas somente em contas 111111111111222222222222, você alteraria o valor de para “111111111111, **`/ASR/Filters/AccountFilters`** 222222222222". Em seguida, altere o valor de `/ASR/Filters/AccountFilterMode` para “Incluir”. A solução então ignorará todas as descobertas geradas para contas que não sejam 111111111111 ou 2222222222.

Cada parâmetro de filtro usa uma lista de valores delimitada por vírgula para filtrar, e cada parâmetro de “modo” pode ser definido como Incluir, Excluir ou Desativado.

Limpeza

Exclua os recursos de exemplo

Na conta do membro, exclua o exemplo de função Lambda que você criou.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Exclua o exemplo da função Lambda

Exclua a pilha de administração

Na conta de administrador, exclua a pilha de administração.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Exclua a pilha de administração	Nenhum
222222222222	Membro	Nenhum	Nenhum

Excluir a pilha de membros

Na conta de administrador, exclua o membro StackSet.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir o membro StackSet Confirme se a pilha de membros foi excluída	Confirme se a pilha de membros foi excluída
222222222222	Membro	Confirme se a pilha de membros foi excluída	Confirme se a pilha de membros foi excluída

Exclua a pilha de funções dos membros

Na conta de administrador, exclua as funções dos membros StackSet.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Exclua as funções dos membros StackSet Confirme se a pilha de funções de lembrete foi excluída	Nenhum
222222222222	Membro	Confirme se a pilha de funções dos membros foi excluída	Nenhum

Excluir as funções retidas

Em cada conta, exclua as funções retidas do IAM.

Importante: essas funções são mantidas para remediações que exigem uma função para que a remediação continue funcionando (por exemplo, registro de fluxo de VPC). Confirme que você não precisa da função contínua de nenhuma dessas funções antes de excluí-las.

Exclua todas as funções prefixadas com SO0111-.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir funções retidas	Nenhum
222222222222	Membro	Excluir funções retidas	Nenhum

Programe as chaves KMS retidas para exclusão

As pilhas de administradores e membros criam e retêm uma chave KMS. Você incorrerá em cobranças se guardar essas chaves.

Essas chaves são retidas para que você tenha acesso a quaisquer recursos criptografados pela solução. Confirme que você não precisa deles antes de programá-los para exclusão.

Identifique as chaves implantadas pela solução usando os aliases criados pela solução ou a partir do CloudFormation histórico. Agende-os para exclusão.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Identifique e agende a chave do administrador para exclusão Identifique e agende a chave do membro para exclusão	Identifique e agende a chave do membro para exclusão
222222222222	Membro	Identifique e agende a chave do membro para exclusão	Identifique e agende a chave do membro para exclusão

Exclua as pilhas para obter permissões StackSets autogerenciadas

Exclua as pilhas criadas para permitir permissões StackSets autogerenciadas

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir a pilha de funções de StackSet administrador	Nenhum
222222222222	Membro	Excluir a pilha StackSet de funções de execução	Nenhum

Guia do desenvolvedor

Esta seção fornece o código-fonte da solução e personalizações adicionais.

Código-fonte

Visite nosso GitHub repositório para baixar os modelos e scripts dessa solução e compartilhar suas personalizações com outras pessoas.

Manuais

Essa solução inclui o manual de remediações para os padrões de segurança definidos como parte do Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 e National Institute of Standards and Tecnologia (NIST).

Se você tiver as descobertas de controle consolidadas habilitadas, esses controles serão suportados em todos os padrões. Se esse recurso estiver ativado, somente o manual do SC precisará ser implantado. Caso contrário, os manuais são compatíveis com os padrões listados anteriormente.

> **Important**
>
> Somente implante os manuais de acordo com os padrões habilitados para evitar atingir as cotas de serviço.

Para obter detalhes sobre uma remediação específica, consulte o documento de automação do Systems Manager com o nome implantado pela solução em sua conta. Acesse o console do AWS Systems Manager e, no painel de navegação, escolha Documents.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Total de remediações	63	34	29	33	65	19	90
ASR-Verificação EnableAutoScalingGroup ELBHealth Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do balanceador de carga	Escalonamento automático.1		Escalonamento automático.1		Escalonamento automático.1		Escalonamento automático.1
ASR-Configure					Escalonamento		Escalonamento

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
AutoScali ngLaunchC onfigToRe quire IMDSv2 As configura ções de lançament o em grupo do Auto Scaling devem configura r as EC2 instância s para exigir o Instance Metadata Service versão 2 () IMDSv2					automátic o.3		automátic o.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateCloudTrailMultiRegionTrail CloudTrail deve ser ativada e configurada com pelo menos uma trilha multirregional	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail deve ter a criptografia em repouso ativada	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableLogFileValidation Certifique-se de que a validação do arquivo de CloudTrail log esteja ativada	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableClo udTrailTo CloudWatc hLogging Garanta que as CloudTrai l trilhas estejam integrada s com o Amazon CloudWatc h Logs	CloudTrai l5.	2.4	CloudTrai l4.	3.4	CloudTrai l5.		CloudTrai l5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O ASR configura 3 BucketLogging Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3		2.6		3.6		3.4	CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild as variáveis de ambiente do projeto não devem conter credenciais de texto não criptografado	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR AWSConfig Certifiqu e-se de que o AWS Config esteja ativado	Config.1	2,5	Config.1	3.5	Config.1	3.3	Config.1
ASR-Make EBSSnapsl ots Privado Os snapshots do Amazon EBS não devem ser restauráv eis publicame nte	EC21.		EC21.		EC21.		EC21.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-Remove VPCDefaul t SecurityG roupRules O grupo de segurança padrão da VPC deve proibir o tráfego de entrada e saída	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Registros habilitados para ASR VPCFlow O registro de fluxo de VPC deve ser ativado em todos VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnableEbsEncryptionByDefault A criptografia padrão do EBS deve ser ativada	EC27.	2.2.1			EC27.	2.2.1	EC27.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-RevokeUnrotatedKeys As chaves de acesso dos usuários devem ser trocadas a cada 90 dias ou menos	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
Política ASR-SetIAMPassword Política de senha padrão do IAM	IAM.7	1,5-1,11	IAM.8	1.8	IAM.7	1.8	IAM.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-Credencias RevokeUnused IAMUser As credencias do usuário devem ser desativadas se não forem usadas dentro de 90 dias	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CredentialsRevokeUnusedIAMUser As credenciais do usuário devem ser desativadas se não forem usadas dentro de 45 dias				1.12		1.12	IAM.22

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-RemoveLambdaPublicAccess As funções Lambda devem proibir o acesso público	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotPrivado Os instantâneos do RDS devem proibir o acesso público	RDS.1		RDS.1		RDS.1		RDS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-DisablePublicAccessToRDSInstance As instâncias de banco de dados do RDS devem proibir o acesso público	RDS.2		RDS 2		RDS 2	2.3.3	RDS 2

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Criptogra fia ASR RDSSnaps ot Os snapshots do cluster do RDS e os snapshots do banco de dados devem ser criptogra fados em repouso	RDS.4				RDS.4		RDS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableMulti AZOnRDSInstance As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade	RDS.5				RDS.5		RDS.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableEnhancedMonitoringOnRDSInstance O monitoramento aprimorado deve ser configurado para instâncias e clusters de banco de dados do RDS	RDS.6				RDS.6		RDS.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR RDSCluster DeletionProtection Os clusters do RDS devem ter a proteção contra exclusão ativada	RDS.7				RDS.7		RDS.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR RDSInstance DeletionProtection As instâncias de banco de dados do RDS devem ter a proteção de exclusão ativada	RDS.8				RDS.8		RDS.8

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableMin orVersion UpgradeOr RDSDBInst ance As atualizaç ões automátic as de versões secundári as do RDS devem ser ativadas	RDS.13				RDS. 13	2.3.2	RDS.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableCopyTagsToSnapshotOnRDSCluster Os clusters de banco de dados do RDS devem ser configurados para copiar tags para instantâneos	RDS.16				RDS.16		RDS.16

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-DisablePublicAccessToRedshiftCluster Os clusters do Amazon Redshift devem proibir o acesso público	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableAut omaticSna pshotsOnR edshiftCl uster Os clusters do Amazon Redshift devem ter snapshots automátic os ativados	Redshift. 3				Redshift. 3		Redshift. 3

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableRedshiftClusterAuditLogging Os clusters do Amazon Redshift devem ter o registro de auditoria ativado	Redshift. 4				Redshift. 4		Redshift. 4

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableAut omaticVer sionUpgra deOnRedsh iftCluster O Amazon Redshift deve ter as atualizaç ões automátic as para as versões principais ativadas	Redshift. 6				Redshift. 6		Redshift. 6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O ASR configura 3 PublicAccessBlock A configuração do S3 Block Public Access deve ser ativada	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
O ASR configura 3 BucketPublicAccessBlock Os buckets do S3 devem proibir o acesso público à leitura	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O ASR configura 3 BucketPublicAccessBlock Os buckets do S3 devem proibir o acesso público à gravação		S3.3					S3.3
ASR-S3 EnableDefaultEncryption Os buckets S3 devem ter a criptografia do lado do servidor ativada	S3.4		S3.4	2.1.1	S3.4		S3.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Política ASR-Set SSLBucket Os buckets S3 devem exigir solicitações para usar SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-S3 BlockDenylist As permissões do Amazon S3 concedidas a outras contas da AWS em políticas de bucket devem ser restritas	3.6				S3.6		S3.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
A configuração do S3 Block Public Access deve ser ativada no nível do bucket	S3.8				S3.8		S3.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O ASR configura 3 BucketPublicAccessBlock Certifique-se de que os CloudTrail registros do bucket do S3 não estejam acessíveis publicamente		2.3					CloudTrail.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateAccessLoggingBucket Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3		2.6					CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableKeyRotation Garanta que a rotação criada pelo cliente CMKs esteja ativada		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas		3.1		4.1			Cloudwatch.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de log e um alarme para login no AWS Management Console sem MFA		3.2		4.2			Cloudwatch.2

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLog MetricFil terAndAla rm Certifiqu e-se de que exista um filtro métrico de log e um alarme para uso do usuário “root”		3.3	VACA.1	4.3			Cloudwatc h.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações de política do IAM		3.4		4.4			Cloudwatch.4

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLog MetricFil terAndAla rm Certifiqu e-se de que exista um filtro métrico de registro e um alarme para alteraçõe s CloudTrai l de configura ção		3.5		4.5			Cloudwatc h.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de log e um alarme para falhas de autenticação do AWS Management Console		3.6		4.6			Cloudwatch.6

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLog MetricFil terAndAla rm Certifiqu e-se de que exista um filtro métrico de registro e um alarme para desativaç ão ou exclusão programad a do cliente criado CMKs		3.7		4.7			Cloudwatc h.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3		3.8		4.8			Cloudwatch.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de log e um alarme para as alterações de configuração do AWS Config		3.9		4,9			Cloudwatch.9

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações do grupo de segurança		3.10		4.10			Cloudwatch.10

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLog MetricFil terAndAla rm Verificar se existe um alarme e um filtro de métrica de log para alteraçõe s em listas de controle de acesso à rede (NACL)		3.11		4.11			Cloudwatc h.11

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede		3.12		4.12			Cloudwatch.12

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas		3.13		4.13			Cloudwatch.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações de VPC		3,14		4.14			Cloudwatch.14

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
AWS-DisablePublicAccessForSecurityGroup Certifique-se de nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 22		4.1	EC25.		EC21.3		EC21.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
AWS-DisablePublicAccessForSecurityGroup 4.2 Certifique-se de que nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 3389		4.2			EC21.4		EC21.4
Configuração ASR SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
Função ASR-CreateIAMSupport		1,20		1.17		1.17	IAM.18

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-DisablePu blic IPAuto Atribuir EC2 As sub-redes da Amazon não devem atribuir automatic amente endereços IP públicos	EC21.5				EC21.5		EC21.5
ASR-EnableClo udTrailLo gFileVali dation	CloudTrai l4.	2.2	CloudTrai l3.	3.2			CloudTrai l4.
ASR-EnableEnc ryptionFo r SNSTopic	SNS.1				SNS.1		SNS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableDeliveryStatusLoggingForSNSTopic O registro do status de entrega deve ser ativado para mensagens de notificação enviadas para um tópico	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionFor SQSQueue	SQS.1				SQS.1		SQS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O instantâneo RDS RDSSnapshot privado do ASR-Make deve ser privado	RDS.1		RDS.1				RDS.1
Bloco ASR SSMDocument PublicAccess Os documentos SSM não devem ser públicos	SSM.4				SSM.4		SSM.4

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableClo udFrontDe faultRoot Object CloudFron t as distribui ções devem ter um objeto raiz padrão configura do	CloudFron t1.				CloudFron t1.		CloudFron t1.
ASR-SetCloudF rontOrigi nDomain CloudFron t distribui ções não devem apontar para origens inexisten tes do S3	CloudFron t1.2				CloudFron t1.2		CloudFron t1.2

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-RemoveCo eBuildPri vilegedMo de CodeBuild os ambientes do projeto devem ter uma configura ção AWS de registro	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Instância de encerrame nto do ASR EC2 EC2 As instância s interromp idas devem ser removidas após um período de tempo especific ado	EC24.				EC24.		EC24.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR IMDSV2 OnInstance EC2 as instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2	EC28.				EC28.	5.6	EC28.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-RevokeUnauthorizedInboudRules Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas	EC21.8				EC21.8		EC21.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
INSIRA O TÍTULO AQUI Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	EC21.9				EC21.9		EC21.9

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Desabilit ar ASR TGWAuto AcceptSha redAttach ments O Amazon EC2 Transit Gateways não deve aceitar automatic amente solicitaç ões de anexos de VPC	EC22.3				EC22.3		EC22.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnablePrivateRepositoryScanning Os repositórios privados do ECR devem ter a digitalização de imagens configurada	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty deve ser habilitado	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
O ASR configura 3 BucketLogging O registro em log de acesso ao servidor para bucket do S3 deve estar habilitado	S3.9				S3.9		S3.9

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableBucketEventNotifications Os buckets do S3 devem ter as notificações de eventos ativadas	S3.11				S3.11		S3.11
Conjuntos ASR 3 Lifecycle Policy Os buckets do S3 devem ter políticas de ciclo de vida configuradas	S3.13				S3.13		S3.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableAutoSecretRotation Os segredos do Secrets Manager devem ter a alternância automática ativada	SecretsManager1.				SecretsManager1.		SecretsManager1.
ASR-RemoveUnsedSecret Remover segredos do Secrets Manager não utilizados	SecretsManager3.				SecretsManager3.		SecretsManager3.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-UpdateSecretRotationPeriod Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias	SecretsManager4.				SecretsManager4.		SecretsManager4.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR APIGateway CacheDataEncryption Os dados do cache da API REST de Gateway devem ser criptografados em repouso					APIGateway5.		APIGateway5.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-SetLogGro upRetenti onDays CloudWatc h os grupos de registros devem ser mantidos por um período de tempo especific ado					CloudWatc h1.6		CloudWatc h1.6

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-AttachSer vice VPCEndpo nt A Amazon EC2 deve ser configura da para usar endpoints VPC que são criados para o serviço Amazon EC2	EC2.10				EC2.10		EC2.10
ASR-TagGuardD utyResour ce GuardDuty os filtros devem ser marcados							GuardDuty 2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-TagGuardDutyResource GuardDuty detectores devem ser marcados							GuardDuty 4.
SSMPermissionsASR-Anexar a EC2 EC2 As instâncias da Amazon devem ser gerenciadas pelo Systems Manager	SSM.1		SSM.3				SSM.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2 As instâncias da Amazon lançadas usando as configurações de lançamento em grupo do Auto Scaling não devem ter endereços IP públicos					Autoscaling.5		Autoscaling.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Habilitar ASR APIGateway Execution Logs	APIGateway1.						APIGateway1.
ASR-EnableMacie O Amazon Macie deve ser habilitado	Macie.1				Macie.1		Macie.1

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableAth enaWorkGr oupLoggin g Os grupos de trabalho do Athena devem ter o registro em log habilitado	Athena.4						Athena.4

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-Enfor ce LAB HTTPSFor O Applicati on Load Balancer deve ser configura do para redirecio nar todas as solicitaç ões HTTP para HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Limite ASR ECSRootFilesystemAccess Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz	ECS.5				ECS.5		ECS.5

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableElastiCacheBackups ElastiCache Os clusters (Redis OSS) devem ter backups automáticos habilitados	ElastiCache1.				ElastiCache1.		ElastiCache1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableElastiCacheVersionUpgrades ElastiCache os clusters devem ter atualizações automáticas de versões secundárias habilitadas	ElastiCache2.				ElastiCache2.		ElastiCache2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache os grupos de replicação devem ter o failover automático ativado	ElastiCache3.				ElastiCache3.		ElastiCache3.

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
Escalabil idade ASR Configure Dynamo DBAuto As tabelas do DynamoDB devem escalar automatic amente a capacidad e de acordo com a demanda	DynamoDB 1				DynamoDB 1		DynamoDB. 1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID do controle de segurança
ASR-Recurso TagDynamoDBTable As tabelas do DynamoDB devem ser marcadas							DynamoDB.5
Proteção ASR EnableDynamo DBDeletion As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada					DynamoDB.6		DynamoDB.6

Adicionando novas remediações

As correções podem ser adicionadas manualmente, atualizando os arquivos apropriados do manual, ou programaticamente, estendendo a solução por meio de construções de CDK, dependendo do fluxo de trabalho de sua preferência.

> **Note**
>
> As instruções a seguir utilizam os recursos instalados pela solução como ponto de partida. Por convenção, a maioria dos nomes de recursos da solução contém ASR and/or SO0111 para facilitar sua localização e identificação.

Visão geral do fluxo de trabalho manual

Os runbooks do Automated Security Response on AWS devem seguir a seguinte nomenclatura padrão:

ASR- *<standard>* - - *<version>* *<control>*

Padrão: a abreviatura do padrão de segurança. Isso deve corresponder aos padrões suportados pelo ASR. Deve ser “CIS”, “AFSBP”, “PCI”, “NIST” ou “SC”.

Versão: A versão do padrão. Novamente, isso deve corresponder à versão suportada pelo ASR e à versão nos dados de busca.

Controle: O ID de controle do controle a ser remediado. Isso deve corresponder aos dados de descoberta.

1. Crie um runbook na (s) conta (s) do membro.
2. Crie uma função do IAM na (s) conta (s) do membro.
3. (Opcional) Crie uma regra de remediação automática na conta do administrador.

Etapa 1. Crie um runbook na (s) conta (s) do membro

1. Faça login no console do AWS Systems Manager e obtenha um exemplo da descoberta de JSON.
2. Crie um runbook de automação que corrija a descoberta. Na guia Propriedade minha, use qualquer um dos `ASR-` documentos na guia Documentos como ponto de partida.

3. O AWS Step Functions na conta de administrador executará seu runbook. Seu runbook deve especificar a função de remediação para ser aprovado ao chamar o runbook.

Etapa 2. Crie uma função do IAM na (s) conta (s) do membro

1. Faça login no console do AWS Identity and Access Management.
2. Obtenha um exemplo das funções do IAM SO0111 e crie uma nova função. O nome da função deve começar com SO0111-remediate- - -. *<standard> <version> <control>* Por exemplo, se adicionar o controle 5.6 do CIS v1.2.0, a função deverá ser. `S00111-Remediate-CIS-1.2.0-5.6`
3. Usando o exemplo, crie uma função com escopo adequado que permita que somente as chamadas de API necessárias realizem a correção.

Neste momento, sua remediação está ativa e disponível para remediação automatizada a partir da ASR Custom Action no AWS Security Hub.

Etapa 3: (Opcional) Crie uma regra de remediação automática na conta do administrador

A remediação automática (não “automatizada”) é a execução imediata da remediação assim que a descoberta é recebida pelo AWS Security Hub. Considere cuidadosamente os riscos antes de usar essa opção.

1. Veja um exemplo de regra para o mesmo padrão de segurança em CloudWatch Eventos. O padrão de nomenclatura para regras `éstandard_control_*AutoTrigger*`.
2. Copie o padrão de evento do exemplo a ser usado.
3. Altere o `GeneratorId` valor para corresponder ao `GeneratorId` em seu Finding JSON.
4. Salve e ative a regra.

Visão geral do fluxo de trabalho do CDK

Em resumo, os seguintes arquivos no repositório ASR serão modificados ou adicionados. Neste exemplo, uma nova remediação para ElastiCache .2 foi adicionada aos manuais do SC e do AFSBP.

> **Note**
>
> Todas as novas remediações devem ser adicionadas ao manual do SC, pois ele consolida todas as remediações disponíveis no ASR. Se você pretende implantar somente um conjunto específico de manuais (por exemplo, AFSBP), você pode: (1) adicionar a correção somente aos manuais pretendidos ou (2) adicionar a correção a todos os manuais para os quais ela existe no Padrão do Security Hub correspondente, além do manual do SC. A segunda opção é recomendada para flexibilidade.

Neste exemplo, ElastiCache .2 está incluído nos seguintes padrões do Security Hub:

- AFSBP
- 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

Como, por padrão, o ASR implementa apenas manuais para AFSBP e NIST.800-53, adicionaremos essa nova correção a esses manuais, além do SC.

Modifique

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[nome padrão] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[nome padrão] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediações.ts
- source/test/regex_registry.ts

Adicionar

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts

- source/playbooks/SC/ssmdocs/descriptions/ElastiCache2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> O nome escolhido para o runbook pode ser qualquer string, desde que seja consistente com o restante das alterações feitas.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ 2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Etapas de desenvolvimento

1. Crie o Runbook de Remediação.
2. Crie os Control Runbooks.
3. Integre cada manual de controle com um manual.
4. Crie a função do IAM de remediação e integre o runbook de remediação
5. Atualizar testes unitários

Etapa 1: Criar o Runbook de Remediação

Este é o documento SSM usado para remediar recursos. Ele deve incluir o `AutomationAssumeRole` parâmetro, que é a função do IAM com permissões para executar a correção. Visualize o arquivo existente `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` como referência ao criar novos runbooks de remediação.

Todos os novos runbooks devem ser adicionados ao `source/remediation_runbooks/` diretório.

Etapa 2: Criar os Runbooks de Controle

Um runbook de controle é um runbook específico de um manual que analisa os dados de busca de um determinado padrão e executa o manual de execução de remediação apropriado. Como estamos adicionando a remediação ElastiCache .2 aos manuais SC, AFSBP e NIST8 0053, precisamos criar um novo manual de controle para cada um. Os seguintes arquivos são criados:

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ 2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

<CONTROL.ID>A nomeação desses arquivos é importante e deve seguir o formato <PLAYBOOK_NAME>_ .ts/yaml

Alguns manuais no ASR oferecem suporte aos runbooks de controle do IaC TypeScript, enquanto outros devem ser escritos em YAML bruto. Consulte as remediações existentes no respectivo manual como exemplos. Neste exemplo, abordaremos o manual do SC, que usa IaC.

No manual do SC, seu novo runbook de controle deve exportar uma classe que se estenda ControlRunbookDocument e corresponda ao nome do seu runbook de remediação. Veja o exemplo abaixo:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`é o ID de controle da remediação que você está adicionando, conforme definido na exibição de controles consolidados no Security Hub.
- `remediationName`é o nome que você escolheu para o seu runbook de remediação.
- `scope`é o escopo do recurso que você está remediando, indicando se ele existe globalmente ou em uma região específica.

- `resourceIdRegex`é o regex usado para capturar o ID do recurso que você gostaria de passar para o runbook de remediação como parâmetro. Somente um grupo deve ser capturado, todos os outros grupos não devem ser capturadores. Se você quiser passar o ARN inteiro, omita esse campo.
- `resourceIdName`é o nome que você gostaria de definir para o ID do recurso capturado usando`resourceIdRegex`. Ele deve corresponder ao nome do parâmetro do ID do recurso em seu runbook de remediação.
- `updateDescription`é a string que você gostaria de atribuir à seção “notas” da descoberta no Security Hub quando a correção for bem-sucedida.

Você também deve exportar uma função chamada `createControlRunbook` que retorna uma nova instância da sua classe. Para ElastiCache 1.2, isso se parece com:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

onde `controlId` está o ID de controle, conforme definido no Padrão de Segurança associado ao manual sob o qual você está operando.

Se o controle do Security Hub tiver parâmetros que você gostaria de passar para o seu runbook de remediação, você poderá passá-los adicionando substituições aos seguintes métodos: -`getExtraSteps`: define valores padrão para cada parâmetro implementado para o controle no Security Hub

> **Note**
>
> Cada parâmetro do Security Hub deve receber um valor padrão

- `getInputParamsStepOutput`: define as saídas para a GetInputParams etapa do runbook de controle
- Cada saída tem um `name`e`outputType`, `selector` e. `selector`Deve ser o mesmo seletor usado na substituição do `getExtraSteps` método.

- `getRemediationParams`: define os parâmetros passados para o runbook de remediação, obtidos nas saídas da GetInputParams etapa.

Para ver um exemplo, navegue até o `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts` arquivo.

Etapa 3: Integrar cada manual de controle com um manual

Para cada runbook de controle criado na etapa anterior, agora você deve integrá-lo às definições de infraestrutura no manual associado. Siga as etapas abaixo para cada runbook de controle.

> **Important**
>
> Se você criou o runbook de controle usando YAML bruto em vez de IaC datilografado, vá para a próxima seção.

Em */<playbook_name>/*`control_runbooks-construct.ts` Importar seu arquivo de runbook de controle recém-criado, como:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Em seguida, vá para a matriz para

```
const controlRunbooksRecord: Record<string, any>
```

E adicione uma nova entrada mapeando o ID de controle (específico do manual) para o `createControlRunbook` método que você criou:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Adicione o ID de controle específico do manual à lista de remediações, conforme abaixo: *<playbook_name>*`\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

O `versionAdded` campo deve ser a versão mais recente da solução. Se a adição da remediação violar o limite de tamanho do modelo, aumente o. `versionAdded` Você pode ajustar o número de remediações incluídas na pilha de cada membro do manual. `solution_env.sh`

Etapa 4: criar a função do IAM de remediação e integrar o runbook de remediação

Cada remediação tem sua própria função do IAM com permissões personalizadas necessárias para executar o runbook de remediação. Além disso, o `RunbookFactory.createRemediationRunbook` método precisa ser invocado para adicionar o runbook de remediação que você criou na Etapa 1 aos modelos da solução. CloudFormation

No`remediation-runook-stack.ts`, cada remediação tem seu próprio bloco de código na `RemediationRunbookStack` classe. O bloco de código a seguir mostra a criação de uma nova função do IAM e a integração do runbook de remediação para a remediação ElastiCache .2:

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
```

```
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Etapa 5: atualizar os testes unitários

Recomendamos atualizar e executar os testes de unidade após adicionar uma nova correção.

Primeiro, você deve adicionar quaisquer novas expressões regulares (que ainda não tenham sido adicionadas) ao `source/test/regex_registry.ts` arquivo. Esse arquivo impõe testes para cada nova expressão regular incluída nos runbooks da solução. Veja a `addElastiCacheClusterTestCases` função como exemplo, que é usada para testar expressões regulares usadas em ElastiCache remediações.

Por fim, você precisará atualizar os instantâneos de cada pilha. Os instantâneos são definições de CloudFormation modelo com controle de versão que são usadas para rastrear as alterações feitas na infraestrutura do ASR. Você pode atualizar esses arquivos de instantâneo executando o seguinte comando no `deployment` diretório:

```
./run-unit-tests.sh update
```

Agora você está pronto para implantar sua nova remediação! Navegue até a seção Criar e implantar abaixo para obter instruções sobre como criar e implantar a solução com suas novas alterações.

Adicionar um novo manual

Baixe os manuais da solução Automated Security Response on AWS e o código-fonte de implantação do Automated Security Response on AWS do GitHub repositório.

Os CloudFormation recursos da AWS são criados a partir de componentes do AWS CDK, e os recursos contêm o código do modelo de manual que você pode usar para criar e configurar novos manuais. Para obter mais informações sobre como configurar seu projeto e personalizar seus playbooks, consulte o arquivo README.md em. GitHub

AWS Systems Manager Parameter Store

O Automated Security Response na AWS usa o AWS Systems Manager Parameter Store para armazenamento de dados operacionais. Os seguintes parâmetros são armazenados no Parameter Store:

Nome	Valor	Use
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Chave do AWS KMS que criptografará dados para remediações do FSBP	Criptografia dos dados do cliente, como CloudTrail registros, como parte das correções
`/Solutions/SO0111/CMK_ARN`	Chave do AWS KMS que o ASR usará para criptografar dados	Criptografia dos dados da solução
`/Solutions/SO0111/SNS_Topic_ARN`	ARN do tópico Amazon SNS para a solução	Notificação de eventos de remediação
`/Solutions/SO0111/SNS_Topic_Config.1`	Tópico do SNS para atualizaç ões do AWS Config	Remediação do Config.1
`/Solutions/SO0111/version`	Versão da solução	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /status	`enabled`	Indica se o padrão está ativo na solução. Um padrão pode ser desativado para remediação automatizada alterando-o para `disabled`
`/Solutions/SO0111/`*`<security standard long name>`*`/`nome curto	`String`	Nome curto para o padrão de segurança. Por exemplo:`CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security`	`String`	Quando um controle usa a mesma remediação que outro,

Nome	Valor	Use
standard long name><version> /*<control>* /remapear		esses parâmetros realizam o remapeamento
/ASR/Filters/AccountFilterMode	Incluir, excluir ou desativar	Controla o comportamento de filtragem de ID da conta para remediações totalmente automatizadas
/ASR/Filters/AccountFilters	Lista delimitada por vírgula da conta da AWS IDs	Lista de contas da AWS IDs para as quais a solução deve filtrar as remediações automatizadas.
/ASR/Filters/OUFilterMode	Incluir, excluir ou desativar	Controla o comportamento de filtragem das Unidades Organizacionais (OUs) para remediações totalmente automatizadas
/ASR/Filters/OUFilters	Lista delimitada por vírgula de IDs de unidades organizacionais	Lista das quais OUs a solução deve filtrar as remediações automatizadas.
/ASR/Filters/TagFilterMode	Incluir, excluir ou desativar	Controla o comportamento de filtragem do Resource Tag para remediações totalmente automatizadas
/ASR/Filters/TagFilters	Lista delimitada por vírgula de chaves de tag de recursos	Lista de chaves de tag de recursos para as quais a solução deve filtrar as remediações automatizadas.

Tópico do Amazon SNS - Progresso da remediação

O Automated Security Response na AWS cria um tópico do Amazon SNS, SO0111-ASR_Topic. Este tópico é usado para publicar atualizações sobre o progresso da remediação. A seguir estão as três possíveis notificações enviadas para esse tópico.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Essa é a mensagem de conclusão. Isso indica que a remediação foi concluída sem erros; no entanto, o teste definitivo para uma remediação bem-sucedida é a validação manual da verificação do AWS Config. and/or

Filtrando uma assinatura de tópico do SNS

Políticas de filtro de assinatura do Amazon SNS:

1. Navegue até a assinatura do tópico do SNS.
2. Em Política de filtro de assinatura, selecione “Editar”.
3. Expanda “Política de filtro de assinatura” e alterne a opção “Política de filtro de assinatura” para ativar os filtros.
4. Selecione o escopo “Corpo da mensagem”.
5. Adicione sua política ao editor JSON.
6. Salve as alterações.

Exemplo de políticas:

Filtrar por conta

```
{
"finding": {
```

```
"account": [
"111111111111",
"222222222222"
]
}
```

Filtrar por erros

```
{
"severity": ["ERROR"]
}
```

Filtrar por controles

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Tópico do Amazon SNS - Alarmes CloudWatch

Essa solução cria um tópico do Amazon SNS,. `SO0111-ASR_Alarm_Topic` Este tópico é usado para publicar alertas de alarme.

Os detalhes de todos os alarmes que entrarem no estado ALARME serão enviados para este tópico.

Inicie o Runbook on Config Findings

Essa solução pode iniciar runbooks com base em descobertas personalizadas do AWS Config. Para fazer isso, você precisará:

1. Encontre o nome da regra do AWS Config que você gostaria de corrigir. Isso pode ser encontrado no AWS Config ou na descoberta que o Security Hub gera para essa regra.
2. Navegue até o AWS Systems Manager Parameter Store e selecione Create Parameter.
3. O nome da sua regra deve ser `/Solutions/SO0111/` [.replaceable] `Rule name from Step 1`
4. O valor deve ser formatado da seguinte forma:

```
{
```

```
"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

1. RunbookName é um campo obrigatório e será o runbook executado quando você corrigir essa regra de Config. RunbookRole é a função que o orquestrador assumirá ao executar essa função. Não é um campo obrigatório e, se deixado de fora, o orquestrador usará como padrão a função de membro da conta.
2. Depois que isso estiver pronto, você poderá corrigir sua regra de Config usando a ação personalizada “Remediar com ASR” encontrada no Security Hub.

Interface do usuário da Web

A interface de usuário da Web da solução permite que os usuários corrijam as descobertas do AWS Security Hub com um clique, visualizem e baixem as remediações anteriores e deleguem acesso à solução.

A interface de usuário da Web não é necessária para usar a solução; como alternativa, você pode configurar remediações totalmente automatizadas para evitar a necessidade de execução manual ou aproveitar o console CSPM do AWS Security Hub para iniciar as remediações usando a ação personalizada Remediate with ASR.

> **Note**
>
> Você deve definir o `ShouldDeployWebUI` parâmetro como “sim” ao implantar a pilha Admin para usar a interface de usuário da Web da solução.

Como funciona

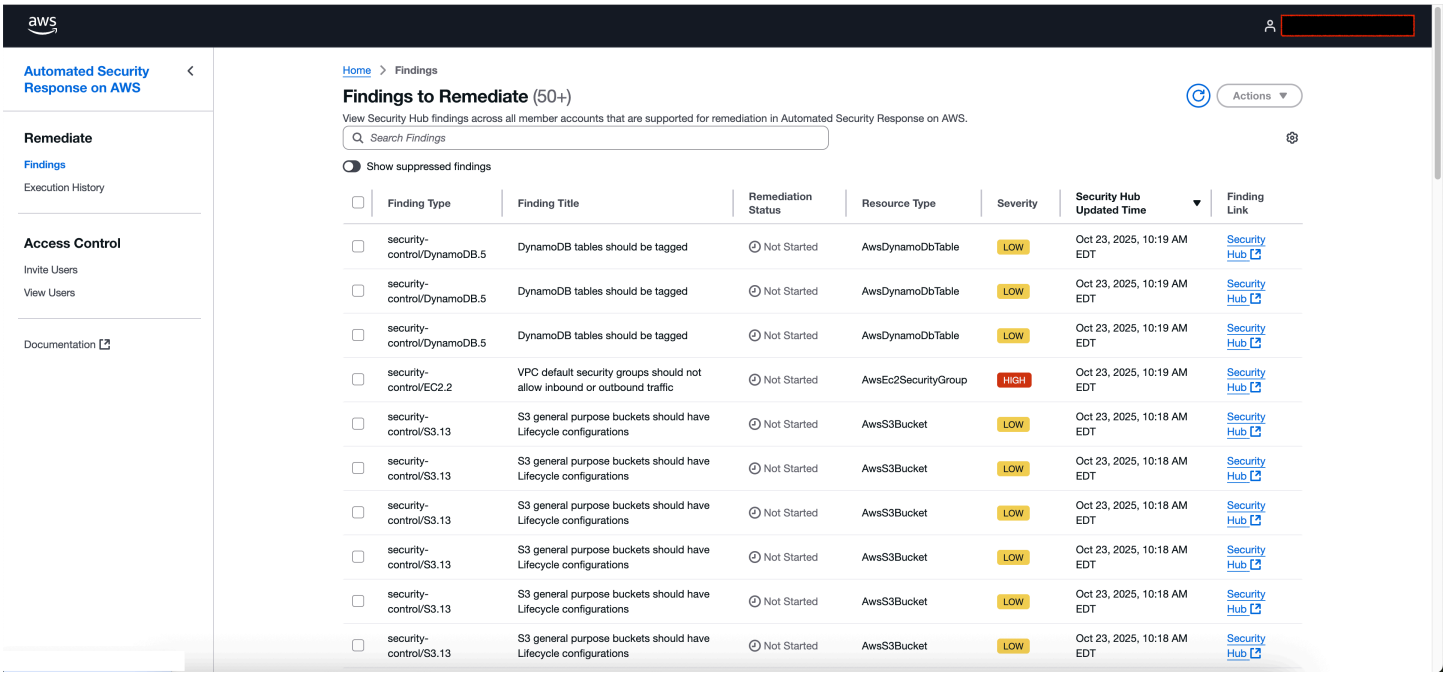
A interface de usuário da web da solução é um aplicativo web de página única hospedado em sua conta pelo Amazon S3 e distribuído pela Amazon. CloudFront A solução também implanta uma API REST usando o API Gateway para dar suporte às operações na interface de usuário da Web.

Quando a pilha de administração é implantada, as funções Lambda da solução começam a carregar todas as descobertas do AWS Security Hub suportadas pela solução que estão presentes em sua

conta de administrador no DynamoDB. Quando isso for concluído, as descobertas apresentadas na interface do usuário da Web são mantidas sincronizadas com o Security Hub quase em tempo real, graças às EventBridge regras implantadas pela solução.

Toda semana, as funções Lambda da solução são acionadas para atualizar a tabela do DynamoDB que armazena as descobertas do AWS Security Hub exibidas na interface do usuário da Web. Isso garante que os dados obsoletos sejam limpos e que nossas tabelas do DynamoDB sejam mantidas. up-to-date Se você quiser configurar essa linha de base para ser executada com mais ou menos frequência, modifique a EventBridge regra chamada `SO0111-ASR-SynchronizationFindingsLambdaWeeklyRule` localizada na sua conta de administrador na mesma região em que você implantou a solução.

Execute correções diretamente na interface do usuário da Web



Na página Descobertas, usuários administradores ou administradores delegados podem ver todas as descobertas do AWS Security Hub suportadas pela solução para remediação. Isso inclui descobertas de contas de membros do Security Hub integradas à conta principal do Security Hub. Se a solução também for implantada na região de agregação, as descobertas em qualquer região integrada também serão exibidas. Para ver a lista de descobertas suportadas pela solução, consulte a seção de manuais.

Os usuários do operador de conta só poderão visualizar as descobertas originadas nas contas da AWS às quais eles têm acesso, conforme definido no convite. Além disso, eles só poderão executar correções para recursos nas contas às quais estão associados.

Para executar correções, selecione qualquer número de itens na tabela e clique em Ações > Remediar. Você também pode suprimir descobertas clicando em Ações > Suprimir, o que oculta as descobertas selecionadas da visualização padrão. Você pode visualizar descobertas suprimidas a qualquer momento clicando no botão Mostrar descobertas suprimidas.

Depois de iniciar a remediação de uma descoberta, você pode clicar na coluna Status da Remediação enquanto a remediação está **`In Progress`** ou deve ser levada diretamente **`Failed`** para aquela remediação na página Histórico de Execução.

Filtrar descobertas e remediações disponíveis

Nas páginas Descobertas e Histórico de Execução, você pode filtrar os dados exibidos na tabela por qualquer uma das colunas presentes em cada tabela respectiva.

Por exemplo, na página Findings, você pode filtrar por Finding Type para pesquisar tipos específicos de descobertas do AWS Security Hub (por exemplo, Lambda.1 ou Athena.4) clicando na barra de pesquisa e selecionando Finding Type.

> **Note**
>
> Os valores preenchidos automaticamente na barra de pesquisa não representam uma lista abrangente dos dados disponíveis. Os valores sugeridos para cada critério de pesquisa representam apenas os dados atualmente buscados e exibidos na interface do usuário.

Você também pode combinar vários atributos em uma única pesquisa. Por exemplo, você pode aplicar o Tipo de descoberta e o ID do recurso em sua pesquisa para realizar uma `AND` consulta lógica. Além disso, você pode aplicar vários dos mesmos critérios de filtro para realizar uma `OR` pesquisa lógica, como Finding Type = Lambda.1 e Finding Type = Athena.4. Os mesmos princípios se aplicam à página Histórico de Execução

Autenticação e autorização na interface de usuário da Web

A interface de usuário da Web da solução é protegida pela autenticação fornecida pelo Amazon Cognito. Quando a solução é implantada, um grupo de usuários do Cognito, um cliente do aplicativo Cognito e um domínio do grupo de usuários do Cognito são provisionados e configurados junto com a interface do usuário da Web. O endereço de e-mail fornecido como parâmetro para a pilha Admin recebe credenciais temporárias e recebe acesso de administrador à interface do usuário da Web.

Há três tipos de permissão que definem o acesso de um usuário à interface do usuário da Web:

Tipo de permissão	Nível de acesso	Caso de uso
Administrador	Controle total na interface do usuário da Web; pode visualizar todas as descobertas e remediações, executar qualquer remediação e invite/view qualquer usuário.	Atribuído somente ao usuário que implantou a pilha de administração quando ele fornece seu endereço de e-mail durante a CloudFormation implantação.
Administrador delegado	Controle elevado na interface do usuário da Web; pode visualizar todas as descobertas e remediações, executar qualquer remediação e os usuários do operador de invite/view conta. Não é possível convidar ou visualizar administradores e administradores delegados na interface do usuário da Web.	O usuário administrador pode delegar acesso à solução convidando usuários administradores delegados, que poderão executar e gerenciar quaisquer correções.
Operador de conta	Controle limitado na interface do usuário da Web; restrito a visualizar e corrigir descobertas somente nas contas às quais estão associadas mediante convite. Não é possível convidar ou ver usuários adicionais.	Day-to-day usuários que deveriam ter acesso limitado para executar correções em um subconjunto de contas integradas. Os administradores ou administradores delegados são responsáveis por convidar esses usuários e definir seu escopo.

Todos os usuários devem ser convidados por um administrador ou administrador delegado antes de poderem entrar na interface de usuário da Web. Para convidar usuários adicionais, um administrador ou administrador delegado pode inserir seu endereço de e-mail e nível de permissão na página Convidar usuários da interface do usuário da Web.

Administradores e administradores delegados também podem visualizar, gerenciar e excluir usuários existentes. Para ver uma lista de todos os usuários, navegue até a página Exibir usuários.

Para gerenciar um usuário existente, selecione o usuário na tabela e clique em Gerenciar usuário. Em seguida, você pode excluir o usuário clicando em Excluir usuário. Se o usuário for um operador de conta, você poderá modificar a lista de contas da AWS às IDs quais ele tem acesso no contexto da solução. Atualmente, não há suporte para alterar o tipo de permissão de um usuário existente.

Observe que os administradores delegados só podem visualizar e gerenciar usuários do Operador de Conta.

Integração com o externo IdPs

Você pode personalizar o mecanismo de autenticação fornecido pela solução para permitir que os usuários façam login usando seu próprio provedor de identidade OIDC ou SAML, como Okta ou Microsoft Entra ID. As etapas a seguir para integração com o externo IdPs exigem acesso à conta da AWS em que a pilha de administração está implantada.

> **Important**
>
> Os usuários ainda devem ser convidados antes de fazer login usando qualquer IdP externo configurado para trabalhar com a solução. Além disso, o endereço de e-mail vinculado ao perfil do IdP deve corresponder ao e-mail fornecido no convite.

Etapa 1 - Localize o grupo de usuários da solução

No console do Amazon Cognito, localize o grupo de usuários da solução chamado SO0111-ASR -. UserPool

Clique no nome do grupo de usuários SO0111-ASR- UserPool para acessar a página de visão geral. A partir daí, selecione Provedores sociais e externos na barra de navegação.

Etapa 2 - Adicione seu provedor de identidade

Na página Provedores sociais e externos, clique no botão Adicionar provedor de identidade no canto superior direito.

Selecione OIDC ou SAML, dependendo do seu provedor de identidade.

Depois de selecionar seu tipo de provedor, você será solicitado a inserir informações sobre seu provedor de identidade.

Preencha os seguintes campos para provedores de SAML:

1. Nome do provedor: um nome amigável para seu provedor
2. Login com SAML iniciado pelo IdP: Selecione `Require SP-initiated SAML assertions - Recommended`
3. Fonte do documento de metadados: Selecionar `Upload metadata document`
4. Documento de metadados: faça o upload do documento de metadados SAML fornecido pelo seu IdP.
5. Em Mapear atributos entre seu provedor de SAML e seu grupo de usuários, clique em Adicionar outro atributo. Para o atributo do grupo de usuários, `email` selecione no menu suspenso. Para o atributo SAML, insira o nome completo do atributo em que o endereço de e-mail do usuário está armazenado no seu provedor de identidade SAML. Por exemplo, `.http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
6. Clique em Adicionar provedor de identidade para salvar suas alterações.

Preencha os seguintes campos para fornecedores do OIDC:

1. Nome do provedor: um nome amigável para seu provedor
2. ID do cliente: insira o ID do cliente fornecido pelo seu provedor de identidade do OpenID Connect.
3. Segredo do cliente: insira o segredo do cliente fornecido pelo provedor de identidade do OpenID Connect.
4. Escopos autorizados: Enter `openid profile email`
5. Método de solicitação de atributo: selecione `GET` ou `POST` com base na configuração do seu provedor de identidade.
6. Método de configuração: selecione `Auto fill through issuer URL` e insira o URL do emissor do seu provedor OIDC. Como alternativa, insira os valores manualmente.
7. Em Mapear atributos entre seu provedor do OpenID Connect e seu grupo de usuários, clique em Adicionar outro atributo. Para o atributo do grupo de usuários, `email` selecione no menu suspenso. Para o atributo OpenID Connect, insira o nome completo do atributo em que o endereço de e-mail do usuário está armazenado no seu provedor de identidade OIDC. Por exemplo, `.email`
8. Clique em Adicionar provedor de identidade para salvar suas alterações.

> **Important**
>
> Você deve adicionar um mapeamento de atributos para o atributo `email` do grupo de usuários, mesmo que o nome do atributo do seu provedor de identidade também sejaemail.

Etapa 3 - Adicione seu provedor ao App Client da solução

Navegue até a página App Clients e selecione o cliente chamado SO0111-ASR-Webui -. UserPoolClient

Clique na guia Páginas de login e, em Configuração de páginas de login gerenciadas, clique em Editar.

No campo Provedores de identidade, adicione o provedor de identidade que você criou na etapa anterior. Clique em Salvar alterações

Etapa 4 - Configurar seu provedor de identidade

Para permitir que seu provedor de identidade redirecione para a interface de usuário da Web da solução após o login, você deve incluir na lista de permissões o seguinte URLs na configuração do IdP.

Dependendo do tipo do seu provedor, liste um dos seguintes retornos de chamada URLs:

1. URL de retorno de chamada do SAML: https://so0111-asr - *<your-aws-account-id>* .auth. *<aws-region>*.amazoncognito. com/saml2/idpresponse
2. URL de retorno de chamada do OIDC: https://so0111-asr - .auth. *<your-aws-account-id>* *<aws-region>*.amazoncognito. com/oauth2/idpresponse

Você deve <your-aws-account-id> substituir pelo ID da conta da AWS em que você implantou a pilha de administração e <aws-region> pela região em que você implantou a pilha de administração.

Etapa 4 - Verifique sua integração

Navegue até a página de login da Web UI. Confirme se seu provedor de identidade personalizado está visível na página de login.

Para testar a integração, convide um novo usuário usando a página Convidar usuários. Em seguida, certifique-se de que o usuário possa se autenticar clicando em seu provedor de identidade personalizado na página de login da interface do usuário da Web.

Observe que o perfil do usuário em seu IdP personalizado deve estar vinculado ao mesmo endereço de e-mail fornecido no convite. Em outras palavras, o endereço de e-mail nas reivindicações do seu provedor deve corresponder ao convite.

Referência

Esta seção inclui informações sobre um recurso opcional para coleta de dados, indicadores para recursos relacionados e uma lista dos criadores que contribuíram para essa solução.

Coleta de dados

Essa solução envia métricas operacionais para a AWS (os “Dados”) sobre o uso dessa solução. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. A coleta desses dados pela AWS está sujeita ao Aviso de Privacidade da AWS.

Recursos relacionados

- Resposta e remediação automatizadas com o AWS Security Hub
- Benchmarks do CIS Amazon Web Services Foundations, versão 1.2.0
- Padrão de práticas recomendadas de segurança básica da AWS
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- Instituto Nacional de Padrões e Tecnologia (NIST) SP 800-53 Rev. 5

Colaboradores

As pessoas a seguir contribuíram na elaboração deste documento:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky

- Josh Moss
- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain
- Manish Jangid
- André Stephen
- Peter DeVries
- Mukta Dadariya

Revisões

Data de publicação: agosto de 2020 (última atualização: janeiro de 2025)

Visite o CHANGELOG.md em nosso GitHub repositório para acompanhar melhorias e correções específicas da versão.

Avisos

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) serve apenas para fins informativos, (b) representa as ofertas e práticas atuais de produtos da AWS, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia da AWS e de suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e obrigações da AWS para com seus clientes são controladas pelos contratos da AWS, e este documento não faz parte nem modifica nenhum acordo entre a AWS e seus clientes.

O Automated Security Response na AWS é licenciado de acordo com os termos da Licença Apache Versão 2.0, disponível na The Apache Software Foundation.

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.