Implementation Guide

Automated Security Response on AWS

Automated Security Response on AWS: Implementation Guide

Table of Contents

Solution overview 1

Features and benefits 3

Use cases 3

Concepts and definitions 4

Architecture overview 6

Architecture diagram 6

AWS Well-Architected design considerations 7

Architecture details 10

AWS Security Hub integration 10

Cross-account remediation 10

Playbooks 10

Centralized logging 11

Notifications 11

AWS services in this solution 11

Plan your deployment 13

Cost 13

Pricing Examples (monthly) 17

Security 20

IAM roles 21

Supported AWS Regions 21

Quotas 22

Quotas for AWS services in this solution 22

AWS CloudFormation quotas 22

AWS Security Hub deployment 22

Solution updates 23

Stack vs StackSets deployment 23

Deploy the solution 24

Deciding where to deploy each stack 24

Deciding how to deploy each stack 25

Consolidated Control Findings 26

AWS CloudFormation templates 26

Admin account support 26

Member accounts 27

Member roles 28

- Automated deployment - StackSets 28
  - Prerequisites 28
  - Deployment overview 29
  - Step 1. Launch the Admin stack in the delegated Security Hub Admin account 31
  - Step 2. Install the remediation roles into each AWS Security Hub Member account 32
  - Step 3. - Launch the Member stack into each AWS Security Hub Member account and Region 33
- Automated deployment - Stacks 34
  - Prerequisites 34
  - Deployment overview 34
  - Step 1. Launch the Admin stack 35
  - Step 2. Install the remediation roles into each AWS Security Hub Member account 37
  - Step 3. Launch the Member stack 39
  - Step 4: (Optional) Adjust the available remediations 41

Monitoring this solution with Service Catalog AppRegistry 43
- Activate CloudWatch Application Insights 44
- Activate AWS Cost Explorer 45
- Activate cost allocation tags associated with the solution 45
- Confirm cost tags associated with the solution 46

Update the solution 47
- Upgrading from versions prior to v1.4 47
- Upgrading from v1.4 and later 47

Troubleshooting 48
- Solutions logs 48
- Issues and resolutions 49
- Issues with specific remediations 51

Uninstall the solution 53
- V1.0.0-V1.2.1 53
- V1.3.x 53
- V1.4.0 and later 54

Administrator guide 55
- Enabling and disabling parts of the solution 55
- Example SNS notifications 56

Use the solution 59
- Getting Started with Automated Security Response on AWS 59
  - Prepare the accounts 59

- Enable AWS Config 60
- Enable AWS security hub 60
- Enable consolidated control findings 61
- Configure cross-region finding aggregation 61
- Designate a Security Hub administrator account 62
- Create the roles for self-managed StackSets permissions 63
- Create the insecure resources that will generate example findings 63
- Create CloudWatch log groups for related controls 65

Deploy the solution to tutorial accounts 65
- Deploy the admin stack 65
- Deploy the member stack 66
- Deploy the member roles stack 67

Subscribe to the SNS topic 67

Remediate example findings 68
- Initiate the remediation 68
- Confirm that the remediation resolved the finding 68

Trace the execution of the remediation 69
- EventBridge rule 69
- Step Function execution 69
- SSM Automation 69
- CloudWatch Log Group 70

Enable fully-automated remediations 70
- Confirm that you have no resources this finding may accidentally be applied to 70
- Enable the rule 70
- Configure the resource 71
- Confirm that the remediation resolved the finding 68

Clean up 72
- Delete the example resources 72
- Delete the admin stack 72
- Delete the member stack 72
- Delete the member roles stack 73
- Delete the retained roles 73
- Schedule the retained KMS keys for deletion 74
- Delete the stacks for self-managed StackSets permissions 74

Developer guide 75

Source code 75

- Playbooks ... 75
- Adding new remediations ... 91
  - Overview ... 91
  - Step 1. Create a runbook in the member account(s) ... 92
  - Step 2. Create an IAM role in the member account(s) ... 92
  - Step 3: (Optional) Create an automatic remediation rule in the admin account ... 93
- Adding a new playbook ... 93
- AWS Systems Manager Parameter Store ... 93
- SNS topic ... 94

Reference ... 96

- Anonymized data collection ... 96
- Related resources ... 97
- Contributors ... 97

Revisions ... 99

Notices ... 103

Automatically address security threats with predefined response and remediation actions in AWS Security Hub

Publication date: *August 2020 (last update: October 2023)*

This implementation guide provides an overview of the Automated Security Response on AWS solution, its reference architecture and components, considerations for planning the deployment, configuration steps for deploying the Automated Security Response on AWS solution to the Amazon Web Services (AWS) Cloud.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	Read . . .
Know the cost for running this solution	Cost
Understand the security considerations for this solution	Security
Know how to plan for quotas for this solution	Quotas
Know which AWS Regions are supported for this solution	Supported AWS Regions
View or download the AWS CloudFormation template included in this solution to automatically deploy the infrastructure resources (the “stack”) for this solution	AWS CloudFormation templates

The continued evolution of security requires proactive steps to secure data which can make it difficult, expensive, and time-consuming for security teams to react. The Automated Security Response on AWS solution helps you quickly react to address security issues by providing predefined responses and remediation actions based on industry compliance standards and best practices.

This solution is an add-on solution that works with AWS Security Hub to provide a ready-to-deploy architecture and a library of automated playbooks. This solution makes it easier for AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS.

You can select specific playbooks to deploy in your Security Hub primary account. Each playbook contains the necessary custom actions, Identity and Access Management (IAM) roles, Amazon EventBridge rules, AWS Systems Manager automation documents, AWS Lambda functions, and AWS Step Functions needed to start a remediation workflow within a single AWS account, or across multiple accounts. Remediations work from the Actions menu in AWS Security Hub and allow authorized users to remediate a finding across all of their AWS Security Hub-managed accounts with a single action. For example, you can apply recommendations from the Center for Internet Security (CIS) AWS Foundations Benchmark, a compliance standard for securing AWS resources, to ensure passwords expire within 90 days and enforce encryption of event logs stored in AWS.

> **Note**
>
> Remediation is intended for emergent situations that require immediate action. This solution makes changes to remediate findings only when initiated by you via the AWS Security Hub Management console, or when automated remediation has been enabled using the Amazon EventBridge rule for a specific control. To revert these changes, you must manually put resources back in their original state.
> When remediating AWS resources deployed as a part of the CloudFormation stack, be aware that this might cause a drift. When possible, remediate stack resources by modifying the code that defines the stack resources and updating the stack. For more information, refer to What is drift? in the *AWS CloudFormation User Guide*.

Automated Security Response on AWS includes the playbook remediations for the security standards defined as part of the Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, and Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1. The solution also includes a Security Controls (SC) playbook for the consolidated control findings feature of AWS Security Hub. For more information, refer to Playbooks.

This implementation guide discusses architectural considerations and configuration steps for deploying the Automated Security Response on AWS solution in the AWS Cloud. It includes links to AWS CloudFormation templates that launch, configure, and run the AWS compute, network, storage, and other services required to deploy this solution on AWS, using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting in the AWS Cloud.

Features and benefits

The Automated Security Response on AWS provides the following features:

Automatically remediate findings for specific controls

Activate Amazon EventBridge rules for controls to automatically remediate findings for that control immediately after they appear in AWS Security Hub.

Manage remediations across multiple accounts and Regions from one location

From an AWS Security Hub administrator account that is configured as the aggregation destination for your organization’s accounts and Regions, initiate a remediation for a finding in any account and region in which the solution is deployed.

Get notified of remediation actions and results

Subscribe to the Amazon SNS topic deployed by the solution to be notified when remediations are initiated and whether or not the remediation was successful.

Use AWSConfigRemediations in the GovCloud and China partitions

Some of the remediations included in the solution are repackages of AWS-owned AWSConfigRemediation documents that are available in the commercial partition but not in GovCloud or China. Deploy this solution to make use of these documents in those partitions.

Extend the solution with custom remediation and Playbook implementations

The solution is designed to be extensible and customizable. To specify an alternative remediation implementation, deploy customized AWS Systems Manager automation documents and AWS IAM Roles. To support an entire new set of controls that is not implemented by the solution, deploy a custom Playbook.

Use cases

Enforce compliance to a standard across your organization’s accounts and Regions

Deploy the Playbook for a standard (e.g. AWS Foundational Security Best Practices) to be able to use the provided remediations. Automatically or manually initiate remediations for resources in any account and region in which the solution is deployed to fix resources that are out of compliance.

Deploy custom remediations or Playbooks to meet your organization's compliance needs

Use the provided Orchestrator components as a framework. Build custom remediations to address out-of-compliance resources according to your organization's specific needs.

Concepts and definitions

This section describes key concepts and defines terminology specific to this solution:

Application

A logical group of AWS resources that you want to operate as a unit.

Remediation, Remediation Runbook

An implementation of a set of steps that resolves a finding. For example, a remediation for the control Security Control (SC) Lambda.1 "Lambda function policies should prohibit public access" would modify the policy of the relevant AWS Lambda Function to remove statements that allow public access.

Control Runbook

One of a set of AWS Systems Manager (SSM) automation documents that the Orchestrator uses to route an initiated remediation for a specific control to the correct remediation runbook. For example, the remediations for SC Lambda.1 and AWS Foundational Security Best Practices (FSBP) Lambda.1 are implemented with the same remediation runbook. The Orchestrator invokes the control runbook for each control, which are named ASR-AFSBP_Lambda.1 and ASR-SC_2.0.0_Lambda.1, respectively. Each control runbook invokes the same remediation runbook, which in this case would be ASR-RemoveLambdaPublicAccess.

Orchestrator

The Step Functions deployed by the solution that takes as input a finding object from AWS Security Hub and invokes the correct control runbook in the target account and region. The Orchestrator also notifies the solution SNS Topic when the remediation is started and when the remediation succeeds or fails.

Standard

A group of controls defined by an organization as part of a compliance framework. For example, one of the standards supported by AWS Security Hub and this solution is AWS FSBP.

Control

A description of the properties that a resource should or should not have in order to be in compliance. For example, the control AWS FSBP Lambda.1 states that AWS Lambda Functions should prohibit public access. A function that allows public access would fail this control.

Consolidated Control Findings, Security Control, Security Controls View

A feature of AWS Security Hub that, when activated, displays findings with their consolidated control IDs rather than IDs that correspond to a particular standard. For example, the controls AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2, and PCI-DSS v3.2.1 S3.1 all map to the consolidated (SC) control S3.2 “S3 Buckets should prohibit public read access.” When this feature is turned on, SC runbooks are used.

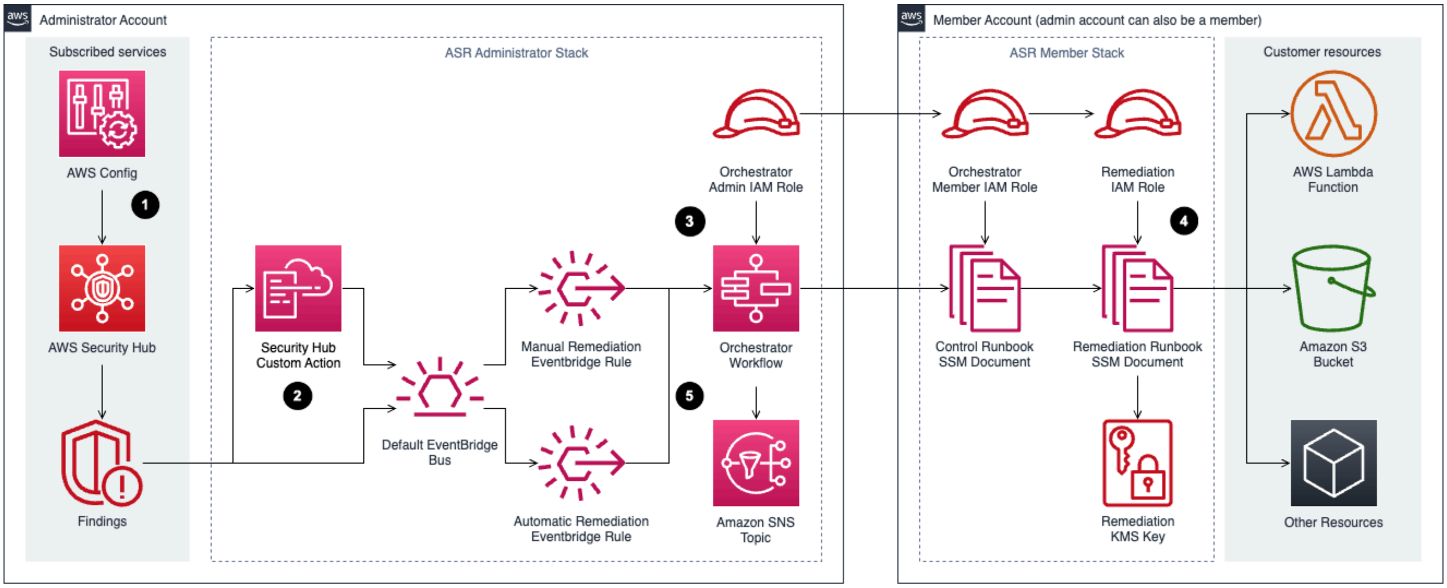
For a general reference of AWS terms, refer to the AWS glossary in the AWS General Reference.

Architecture overview

This section provides a reference implementation architecture diagram for the components deployed with this solution.

Architecture diagram

Deploying this solution with the default parameters builds the following environment in the AWS Cloud.



Automated Security Response on AWS architecture

> **Note**
>
> AWS CloudFormation resources are created from AWS Cloud Development Kit (AWS CDK) constructs.

The high-level process flow for the solution components deployed with the AWS CloudFormation template is as follows:

1. **Detect**: AWS Security Hub provides customers with a comprehensive view of their AWS security state. It helps them to measure their environment against security industry standards and best practices. It works by collecting events and data from other AWS services, such as AWS Config, Amazon Guard Duty, and AWS Firewall Manager. These events and data are analyzed against

security standards, such as CIS AWS Foundations Benchmark. Exceptions are asserted as *findings* in the AWS Security Hub console. New findings are sent as Amazon EventBridge.

2. **Initiate**: You can initiate events against findings using custom actions, which result in Amazon EventBridge Events. AWS Security Hub Custom Actions and Amazon EventBridge rules initiate Automated Security Response on AWS playbooks to address findings. One EventBridge rule is deployed to match the custom action event, and one Amazon EventBridge Event Rule is deployed for each supported control (deactivated by default) to match the real-time finding event. You can use the Security Hub Custom Action menu to initiate automated remediation, or after careful testing in a non-production environment, they can activate automated remediations. This can be activated per remediation—it is not necessary to activate automatic initiations on all remediations.
3. **Orchestrate**: Using cross-account AWS Identity and Access Management (IAM) roles, Step Functions in the admin account invokes the remediation in the member account containing the resource that produced the security finding.
4. **Remediate**: An AWS Systems Manager Automation Document in the member account performs the action required to remediate the finding on the target resource, such as disabling AWS Lambda public access.
5. **Log**: The playbook logs the results to an Amazon CloudWatch Logs group, sends a notification to an Amazon Simple Notification Service (Amazon SNS) topic, and updates the Security Hub finding. An audit trail of actions taken is maintained in the finding notes. On the Security Hub dashboard, the finding workflow status is changed from **NEW** to either **NOTIFIED** or **RESOLVED** on the Security Hub dashboard. The security finding notes are updated to reflect the remediation performed.

AWS Well-Architected design considerations

This solution was designed with best practices from the AWS Well-Architected Framework which helps customers design and operate reliable, secure, efficient, and cost-effective workloads in the cloud. This section describes how the design principles and best practices of the Well-Architected Framework were applied when building this solution.

Operational excellence

This section describes how the principles and best practices of the operational excellence pillar were applied when designing this solution.

- Resources defined as IaC using CloudFormation.

- Remediations implemented with the following characteristics, where possible:
  - Idempotency
  - Error handling and reporting
  - Logging
  - Restoring resources to a known state on failure

Security

This section describes how the principles and best practices of the security pillar were applied when designing this solution.

- IAM used for authentication and authorization.

- Role permissions scoped to be as narrow as possible, though in many cases this soloution requires wildcard permissions to be able to act on any resources.

Reliability

This section describes how the principles and best practices of the reliability pillar were applied when designing this solution.

- Security Hub continues to create findings if the underlying cause of the finding is not resolved by the remediation.
- Serverless services allow the solution to scale as needed.

Performance efficiency

This section describes how the principles and best practices of the performance efficiency pillar were applied when designing this solution.

- This solution was designed to be a platform for you to extend without having to implement orchestration and permissions yourself.

Cost Optimization

This section describes how the principles and best practices of the cost optimization pillar were applied when designing this solution.

- Serverless services allow you to pay for only what you use.
- Use the free tier for SSM automation in every account

Sustainability

This section describes how the principles and best practices of the sustainability pillar were applied when designing this solution.

- Serverless services allow you to scale up or down as needed.

Architecture details

This section describes the components and AWS services that make up this solution and the architecture details on how these components work together.

AWS Security Hub integration

Deploying the `aws-sharr-deploy` stack creates integration with AWS Security Hub's custom action feature. When AWS Security Hub console users select **Findings for remediation**, the solution routes the finding record for remediation using an AWS Step Functions.

Cross-account permissions and AWS Systems Manager runbooks must be deployed to all AWS Security Hub accounts (admin and member) using the `aws-sharr-member.template` and `aws-sharr-member-roles.template` CloudFormation templates. For more information, refer to Playbooks. This template allows automated remediation in the target account.

Users can automatically initiate automated remediations on a per-remediation basis using Amazon CloudWatch events rules. This option activates fully automatic remediation of findings as soon as they are reported to AWS Security Hub. By default, automatic initiations are turned off. This option can be changed at any time during or after installation of the playbook by turning on the CloudWatch Events rules in the AWS Security Hub admin account.

Cross-account remediation

Automated Security Response on AWS uses cross-account roles to work across primary and secondary accounts using cross-account roles. These roles are deployed to member accounts during solution installation. Each remediation is assigned an individual role. The remediation process in the primary account is granted permission to assume the remediation role in the account that requires remediation. Remediation is performed by AWS Systems Manager runbooks running in the account that requires remediation.

Playbooks

A set of remediations is grouped into a package called a *playbook*. Playbooks are installed, updated, and removed using Service Catalog. This solution currently supports the following playbook:

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0, published May 18, 2018.

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.4.0, published November 9, 2022.
- AWS Foundational Security Best Practices (FSBP) version 1.0.0, published March 2021.
- Payment Card Industry Data Security Standard (PCI-DSS), version 3.2.1, published May 2018.
- Security Control, a playbook aligned with the Consolidated Control Findings feature of AWS Security Hub, published February 23, 2023.

Centralized logging

Automated Security Response on AWS logs to a single CloudWatch Logs group, SO0111-SHARR. These logs contain detailed logging from the solution for troubleshooting and management of the solution.

Notifications

This solution uses an Amazon Simple Notification Service (Amazon SNS) topic to publish remediation results. You can use subscriptions to this topic to extend the capabilities of the solution. For example, you can send email notifications and update trouble tickets.

AWS services in this solution

The following AWS services are included in this solution:

AWS service	Description
AWS Lambda	**Core**. Deploys multiple lambda functions that will be used by the step function orchestator to remediate issues.
AWS Step Functions	**Core**. Deploys an orchestrator that will invoke the remediation documents with AWS Systems Manager API calls
AWS Systems Manager	**Core**. Deploys Systems Manager Documents (link to doc) that contain the remediation logic that will be ran.

AWS service	Description
AWS IAM	**Core**. Deploys many roles to allow remediations on different resources.
AWS Security Hub	**Core**. Provides customers with a comprehensive view of their AWS security state.
AWS EventBridge	**Core**. Deploys events that will trigger the orchestator step function when a finding is being remediated.
Amazon Simple Notification Service	**Supporting**. Deploys SNS topics that receive a notification once a remediation has been completed.
Amazon CloudWatch	**Supporting**. Deploys log groups that the different playbooks will use to log results.
AWS Service Catalog AppRegistry	**Supporting**. Deploys application for deployed stacks to track cost and usage.

Plan your deployment

This section describes the cost, network security, supported AWS Regions, quotas, and other considerations prior to deploying the solution.

Cost

You are responsible for the cost of the AWS services used to run this solution. As of this revision, the cost for running this solution with the default settings in the US East (N. Virginia) AWS Region is approximately **$3.33 for 300 remediations/month**, **$26.83 for 3,000 remediations/month**, and **$261.90 for 30,000 remediations/month**. Prices are subject to change. For full details, see the pricing page for each AWS service used in this solution.

> **Note**
>
> Many AWS Services include a Free Tier – a baseline amount of the service that customers can use at no charge. Actual costs may be more or less than the pricing examples provided.

The total cost to run this solution depends on the following factors:

- The number of AWS Security Hub member accounts
- The number of active automatically-invoked remediations
- The frequency of remediation

This solution uses the following AWS components, which incur a cost based on your configuration. Pricing examples are provided for small, medium, and large organizations.

Service	Free Tier	Pricing [USD]
AWS Systems Manager Automation - Step Count	100,000 steps per account per month	Beyond the free tier, each basic step is charged at $0.002 per step. For multi-account automations, all steps including those run in any child accounts are

Service	Free Tier	Pricing [USD]
		counted only in the originating account.
AWS Systems Manager Automation - Step Duration	5,000 seconds per month	Beyond the free tier, each `aws:executeScript` action step is charged at $0.00003 for every second after a free tier of 5,000 seconds per month.
AWS Systems Manager Automation - Storage	No free tier	$0.046 per GB per month
AWS Systems Manager Automation - Data Transfer	No free tier	$0.900 per GB transferred (for cross-account or out-of-Region)
AWS Security Hub - Security Checks	No free tier	First 100,000 checks/account/region/month costs $0.0010 per check Next 400,000 checks/account/region/month costs $0.00.0 per check Over 500,000 checks/account/region/month costs $0.0005 per check
AWS Security Hub - Finding Ingestion Events	First 10,000 events/account/region/month is free. Finding ingestion events associated with Security Hub's security checks.	Over 10,000 events/account/region/month costs $0.00003 per event

Service	Free Tier	Pricing [USD]
Amazon CloudWatch - Metrics	Basic Monitoring Metrics (at 5-minute frequency) 10 Detailed Monitoring Metrics (at 1-minute frequency) 1 Million API requests (not applicable to GetMetricData and GetMetricWidgetImage)	First 10,000 metrics costs $0.30 metric/month Next 240,000 metrics costs $0.10 metric/month Next 750,000 metrics costs $0.05 metric/month Over 1,000,000 metrics costs $0.02 metric/month
Amazon CloudWatch - Dashboard	3 Dashboards for up to 50 metrics per month	$3.00 per dashboard per month
Amazon CloudWatch - Alarms	10 Alarm metrics (not applicable to high-resolution alarms)	Standard Resolution (60 sec) costs $0.10 per alarm metric High Resolution (10 sec) costs $0.30 per alarm metric Standard Resolution Anomaly Detection costs $0.30 per alarm High Resolution Anomaly Detection costs $0.90 per alarm Composite costs $0.50 per alarm
Amazon CloudWatch - Logs Collection	5GB Data (ingestion, archive storage, and data scanned by Logs Insights queries)	$0.50 per GB

Service	Free Tier	Pricing [USD]
Amazon CloudWatch - Logs Storage	5GB Data (ingestion, archive storage, and data scanned by Logs Insights queries)	$0.005 per GB of data scanned
Amazon CloudWatch - Events	All events except custom events are included	$1.00 per million events for custom events $1.00 per million events for cross-acc ount events
AWS Lambda - Requests	1M free requests per month	$0.20 per 1M requests
AWS Lambda - Duration	400,000 GB-seconds of compute time per month	$0.0000166667 for every GB-second. The price for Duration depends on the amount of memory you allocate to your function. You can allocate any amount of memory to your function between 128MB and 10,240MB, in 1MB increment s.
AWS Step Functions - State Transitions	4,000 free state transitions per month	$0.025 per 1,000 state transitions thereafter
Amazon EventBridge	All state change events published by AWS services are free	Custom events cost $1.00/mil lion custom events published Third-party (SaaS) events cost $1.00/million events published Cross-account events cost $1.00/million cross-account events sent
Amazon SNS	First 1 million Amazon SNS requests per month are free	$0.50 per 1 million requests thereafter

Pricing Examples (monthly)

Example 1: 300 remediations per month

- 10 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $3.33 per month

Service	Assumptions	Monthly Charges [USD]
AWS Systems Manager Automation	Steps: ~4 steps * 300 remediations * $0.002 = $2.40 Duration: 10s * 300 remediations * $0.00003 = $0.09	$2.49
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	300 remediations * $0.000002 = $0.0006 $0.0006 * 0.03 = $0.000018	< $0.01
AWS Lambda - Requests	300 remediations * 6 requests = 1,800 requests $0.20 * 1,000,000 requests = $0.20	$0.20
AWS Lambda - Duration	256M: 1.875 GB sec * 300 remediations * $0.0000167 = $0.009375	< $0.01
AWS Step Functions	15 state transitions * 300 remediations = 4,500	< $0.12

Service	Assumptions	Monthly Charges [USD]
	$0.025 * (4,500/1,000) state transitions = $0.1125	
Amazon EventBridge Rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notificat ions = $0.50	$0.50
Total		**$3.33**

Example 2: 3,000 remediations per month

- 100 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $26.83 per month

Service	Assumptions	Monthly Charges [USD]
AWS Systems Manager Automation	Steps: ~4 steps * 3,000 remediations * $0.002 = $24.00 Duration: 10s * 3,000 remediations * $0.00003 = $0.90	$24.90
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	3,000 remediations * $0.000002 = $0.006 $0.006 * 0.03 = $0.00018	< $0.01
AWS Lambda - Requests	3,000 remediations * 6 requests = 18,000 requests	$0.20

Service	Assumptions	Monthly Charges [USD]
	$0.20 * 1,000,000 requests = $0.20	
AWS Lambda - Duration	256M: 1.875 GB sec * 3,000 remediations * $0.000167 = $0.09375	$0.09
AWS Step Functions	15 state transitions * 3,000 remediations = 45,000 $0.025 * (45,000/1,000) state transitions = $1.125	$1.13
Amazon EventBridge rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notificat ions = $0.50	$0.50
Total		**$26.83**

Example 3: 30,000 remediations per months

- 1000 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $261.90 per month

Service	Assumptions	Monthly Charges [USD]
AWS Systems Manager Automation	Steps: ~4 steps * 30,000 remediations * $0.002 = $240.00 Duration: 10s * 30,000 remediations * $0.00003 = $9.00	$249.00

Service	Assumptions	Monthly Charges [USD]
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	30,000 remediations * $0.000002 = $0.06 $0.06 * 0.03 = $0.0018	< $0.01
AWS Lambda - Requests	30,000 remediations * 6 requests = 180,000 requests $0.20 * 1,000,000 requests = $0.20	$0.20
AWS Lambda - Duration	256M: 1.875 GB sec * 30,000 remediations * $0.000167 = $0.9375	$0.94
AWS Step Functions	15 state transitions * 30,000 remediations = 450,000 $0.025 * (450,000/1,000) state transitions = $11.25	$11.25
Amazon EventBridge rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notificat ions = $0.50	$0.50
Total		**$261.90**

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model reduces your operational burden because AWS operates, manages, and controls the components including the host operating system, the virtualization layer, and the physical security of the facilities in which the services operate. For more information about AWS security, visit the AWS Cloud Security.

IAM roles

AWS Identity and Access Management (IAM) roles allow customers to assign granular access policies and permissions to services and users in the AWS Cloud. This solution creates IAM roles that grant the solution's automated functions access to perform remediation actions within a narrow scope set of permissions specific to each remediation.

The admin account's Step Function is assigned to the SO0111-SHARR-Orchestrator-Admin role. Only this role is allowed to assume the SO0111-Orchestrator-Member in each member account. The member role is allowed by each remediation role to pass it to the AWS Systems Manager service to run specific remediation runbooks. Remediation role names begin with SO0111 , followed by a description matching the name of the remediation runbook. For example, SO0111-RemoveVPCDefaultSecurityGroupRules is the role for theASR-RemoveVPCDefaultSecurityGroupRules remediation runbook.

Supported AWS Regions

Region name	Region name
US East (Ohio)	China (Beijing)
US East (N. Virginia)	China (Ningxia)
US West (Northern California)	Europe (Frankfurt)
US West (Oregon)	Europe (Ireland)
Africa (Cape Town)	Europe (London)
Asia Pacific (Hong Kong)	Europe (Milan)
Asia Pacific (Hyderabad)	Europe (Paris)
Asia Pacific (Jakarta)	Europe (Spain)
Asia Pacific (Mumbai)	Europe (Stockholm)
Asia Pacific (Osaka)	Europe (Zurich)

Region name	Region name
Asia Pacific (Seoul)	Middle East (Bahraim)
Asia Pacific (Singapore)	Middle East (UAE)
Asia Pacific (Sydney)	South America (Sao Paulo)
Asia Pacific (Tokyo)	AWS GovCloud (US-East)
Canada (Central)	AWS GovCloud (US-West)

Quotas

Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account.

Quotas for AWS services in this solution

Make sure you have sufficient quota for each of the services implemented in this solution. For more information, refer to AWS service quotas.

Use the following links to go to the page for that service. To view the service quotas for all AWS services in the documentation without switching pages, view the information in the Service endpoints and quotas page in the PDF instead.

AWS CloudFormation quotas

Your AWS account has AWS CloudFormation quotas that you should be aware of when launching the stack in this solution. By understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, see AWS CloudFormation quotas in the in the *AWS CloudFormation User's Guide*.

AWS Security Hub deployment

AWS Security Hub deployment and configuration is a prerequisite for this solution. For more information about setting up AWS Security Hub, refer to Setting up AWS Security Hub in the *AWS Security Hub User Guide.*

At minimum, you must have a working Security Hub configured in your primary account. You can deploy this solution in the same account (and AWS Region) as the Security Hub primary account. In each Security Hub primary and secondary account, you must also deploy the member template that allows AssumeRole permissions to the solution's AWS Step Functions to run remediation runbooks in the account.

Solution updates

To upgrade this solution from v1.3.x or earlier to the latest version, you must delete the existing stack first and then reinstall the latest version of the stack. For deletion instructions, refer to Uninstall the solution. Note that any log data is retained and there is no loss of operational data. If upgrading from v1.4.x, refer to Update the solution.

Stack vs StackSets deployment

A *stack set* lets you create stacks in AWS accounts across AWS Regions by using a single AWS CloudFormation template. Starting with version 1.4, this solution supports stack set deployment by splitting resources based on where and how they are deployed. Multi-account customers, particularly those using AWS Organizations, can benefit from using stack sets for deployment across many accounts. It reduces the effort needed to install and maintain the solution. For more information about StackSets, refer to Using AWS CloudFormation StackSets.

Deploy the solution

This solution uses AWS CloudFormation templates and stacks to automate its deployment. The CloudFormation templates specify the AWS resources included in this solution and their properties. The CloudFormation stack provisions the resources that are described in the templates.

In order for the solution to function, three templates must be deployed. First, decide where to deploy the templates, then decide how to deploy them.

This overview will describe the templates and how to decide where and how to deploy them. The next sections will have more detailed instructions for deploying each stack as a Stack or StackSet.

Deciding where to deploy each stack

The three templates will be referred to by the following names and contain the following resources:

- Admin stack: orchestrator step function, event rules and Security Hub custom action.
- Member stack: remediation SSM Automation documents.
- Member roles stack: IAM roles for remediations.

The Admin stack must be deployed once, in a single account and a single Region. It must be deployed into the account and region that you have configured as the aggregation destination for Security Hub findings for your organization.

The solution operates on Security Hub findings, so it will not be able to operate on findings from a particular account and region if that account or region has not been configured to aggregate findings in the Security Hub administrator account and region.

For example, an organization has accounts operating in regions `us-east-1` and `us-west-2`, with account 111111111111 as the Security Hub delegated administrator in region `us-east-1`. Accounts 222222222222 and 333333333333 must be Security Hub member accounts for the delegated administrator account 111111111111. All three accounts must be configured to aggregate findings from `us-west-2` to `us-east-1`. The Admin stack must be deployed to account 111111111111 in `us-east-1`.

For more details on finding aggregation, consult the documentation for Security Hub delegated administrator accounts and cross-region aggregation.

The Admin stack must complete deployment first before deploying the member stacks so that a trust relationship can be created from the member accounts to the hub account.

The member stack must be deployed into every account and region in which you wish to remediate findings. This can include the Security Hub delegated administrator account in which you previously deployed the ASR Admin stack.The automation documents must execute in the member accounts in order to use the free tier for SSM Automation.

Using the previous example, if you want to remediate findings from all accounts and regions, the member stack must be deployed to all three accounts (`111111111111`, `222222222222`, and `333333333333`) and both regions (`us-east-1` and `us-west-2`).

The member roles stack must be deployed to every account, but it contains global resources (IAM roles) that can only be deployed once per account. It does not matter in which region you deploy the member roles stack, so for simplicity we suggest deploying to the same region in which the Admin stack is deployed.

In the same example as above, we suggest deploying the member roles stack to all three accounts (`111111111111`, `222222222222`, and `333333333333`) in `us-east-1`.

Deciding how to deploy each stack

The options for deploying a stack are

- CloudFormation StackSet (self-managed permissions)
- CloudFormation StackSet (service-managed permissions)
- CloudFormation Stack

StackSets with service-managed permissions are the most convenient because they do not require deploying your own roles and can automatically deploy to new accounts in the organization. Unfortunately, this method does not support nested stacks, which we use in both the Admin stack and the member stack. The only stack that can be deployed this way is the member roles stack.

Be aware that when deploying to the entire organization, the organization management account is not included, so if you want to remediate findings in the organization management account, you must deploy to this account separately.

The member stack must be deployed to every account and region but cannot be deployed using StackSets with service-managed permissions because it contains nested stacks. So we suggest deploying this stack with StackSets with self-managed permissions.

The Admin stack is only deployed once, so it can be deployed as a plain CloudFormation stack or as a StackSet with self-managed permissions in a single account and region.

Consolidated Control Findings

The accounts in your organization can be configured with the Consolidated Control Findings feature of Security Hub enabled or disabled. See the documentation for this feature. If this feature is enabled, solution deployments older than v2.0.0 will not function. Further, if this feature is enabled, you must deploy both the Admin and Member nested stacks for the "SC" or "security control" standards. This deploys the automation documents and EventBridge rules for use with the consolidated control IDs generated when this feature is enabled. There is no need to deploy the Admin or Member nested stacks for specific standards (e.g. AWS FSBP) when using this feature.

AWS CloudFormation templates

View template

aws-sharr-deploy.template - Use this template to launch the Automated Security Response on AWS solution. The template installs the core components of the solution, a nested stack for the AWS Step Functions logs, and one nested stack for each security standard you choose to activate.

Services used include Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3, and AWS Systems Manager.

Admin account support

The following templates are installed in the AWS Security Hub admin account to turn on the security standards that you want to support. You can choose which of the following templates to install when installing the `aws-sharr-deploy.template`.

aws-sharr-orchestrator-log.template - Creates a CloudWatch logs group for the Orchestrator Step Function.

AFSBPStack.template - AWS Foundational Security Best Practices v1.0.0 rules.

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

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

PCI321Stack.template - PCI-DSS v3.2.1 rules.

SCStack.template - SC v2.0.0 rules.

Member accounts

View template

aws-sharr-member.template - Use this template after you set up the core solution to install AWS Systems Manager automation runbooks and permissions in each of your AWS Security Hub member accounts (including the admin account). This template allows you to choose which security standard playbooks to install.

The `aws-sharr-member.template` installs the following templates based on your selections:

aws-sharr-remediations.template - Common remediation code used by one or more of the security standards.

AFSBPMemberStack.template - AWS Foundational Security Best Practices v1.0.0 settings, permissions, and remediation runbooks.

CIS120MemberStack.template - CIS Amazon Web Services Foundations benchmarks, version 1.2.0 settings, permissions, and remediation runbooks.

CIS140MemberStack.template - CIS Amazon Web Services Foundations benchmarks, version 1.4.0 settings, permissions, and remediation runbooks.

PCI321MemberStack.template - PCI-DSS v3.2.1 settings, permissions, and remediation runbooks.

SCMemberStack.template - Security Control settings, permissions, and remediation runbooks.

Member roles

View template

aws-sharr-member-roles.template - Defines the remediation roles needed in each AWS Security Hub member account.

Automated deployment - StackSets

> **Note**
>
> We recommend deploying with StackSets. However, for single account deployments or for testing or evaluation purposes, consider the stacks deployment option.

Before you launch the solution, review the architecture, solution components, security, and design considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the solution into your AWS Organizations.

Time to deploy: Approximately 30 minutes per account, depending upon StackSet parameters.

Prerequisites

AWS Organizations helps you centrally manage and govern your multi-account AWS environment and resources. StackSets work best with AWS Organizations.

If you have previously deployed v1.3.x or earlier of this solution, you must uninstall the existing solution. For more information, refer to Solution updates.

Before you deploy this solution, review your AWS Security Hub deployment:

- There must be a delegated Security Hub admin account in your AWS Organization.
- Security Hub should be configured to aggregate findings across Regions. For more information, refer to Aggregating findings across Regions in the AWS Security Hub User Guide.
- You should activate Security Hub for your organization in each Region where you have AWS usage.

This procedure assumes that you have multiple accounts using AWS Organizations, and have delegated an AWS Organizations admin account and an AWS Security Hub admin account.

Deployment overview

> **Note**
>
> StackSets deployment for this solution uses a combination of service-managed and self-managed StackSets. Self-Managed StackSets must be used currently as they use nested StackSets, which are not yet supported with service-managed StackSets.

Deploy the StackSets from a delegated administrator account in your AWS Organizations.

Planning

Use the following form to help with StackSets deployment. Prepare your data, then copy and paste the values during deployment.

```
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):
___________________,
___________________,
___________________,
___________________,
___________________
```

Step. 1: Launch the admin stack in the delegated Security Hub admin account

- Using a self-managed StackSet, launch the `aws-sharr-deploy.template` AWS CloudFormation template into your AWS Security Hub admin account in the same Region as your Security Hub admin. This template uses nested stacks.

- Choose which Security Standards to install. By default, all are selected (Recommended)
- Choose an existing Orchestrator log group to use. Select `Yes` if `SO0111-SHARR-Orchestrator` already exists from a previous installation.

For more information on self-managed StackSets, refer to Grant self-managed permissions in the *AWS CloudFormation User Guide*.

Step 2: Install the remediation roles into each AWS Security Hub member account

Wait for Step 1 to complete deployment, because the template in Step 2 references IAM roles created by Step 1.

- Using a service-managed StackSet, launch the `aws-sharr-member-roles.template` AWS CloudFormation template into a single Region in each account in your AWS Organizations.
- Choose to install this template automatically when a new account joins the organization.
- Enter the account ID of your AWS Security Hub admin account.

Step. 3: Launch the member stack into each AWS Security Hub member account and Region

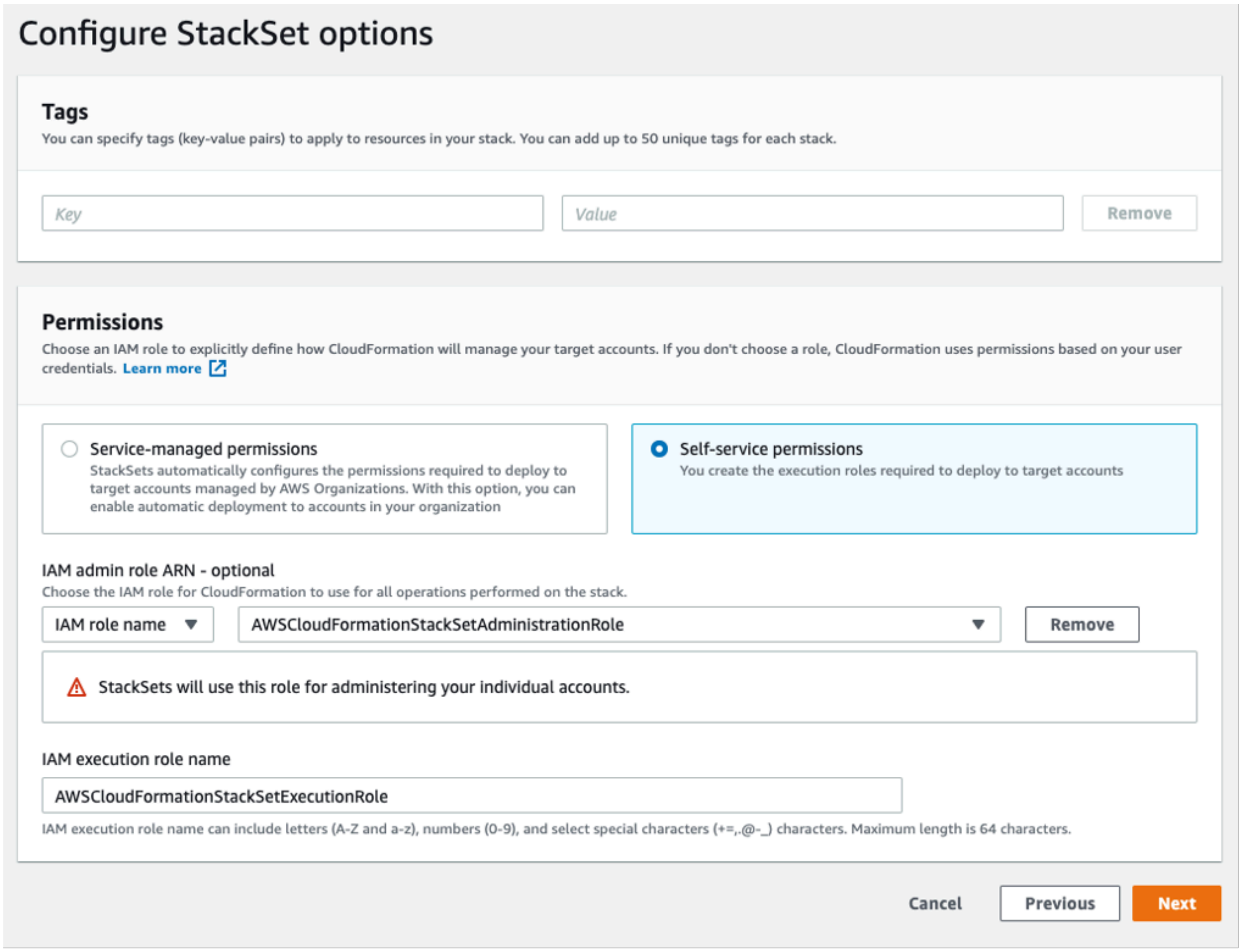
- Using self-managed StackSets, launch the `aws-sharr-member.template` AWS CloudFormation template into all Regions where you have AWS resources in every account in your AWS Organization managed by the same Security Hub admin.

> **Note**
>
> Until service-managed StackSets support nested stacks, you must do this step for any new accounts that join the organization.

- Choose which Security Standard playbooks to install.
- Provide the name of a CloudTrail logs group (used by some remediations).
- Enter the account ID of your AWS Security Hub admin account.

Step 1. Launch the admin stack in the delegated Security Hub admin account

1. Launch the admin stack, `aws-sharr-deploy.template`, with your Security Hub admin account. Typically, one per organization in a single Region. Because this stack uses nested stacks, you must deploy this template as a self-managed StackSet.

   Configure StackSet options

   Tags

   You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

   Key | Value | Remove

   Permissions

   Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

   ○ Service-managed permissions
   StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

   ● Self-service permissions
   You create the execution roles required to deploy to target accounts

   IAM admin role ARN - optional
   Choose the IAM role for CloudFormation to use for all operations performed on the stack.

   IAM role name ▼ | AWSCloudFormationStackSetAdministrationRole ▼ | Remove

   ⚠ StackSets will use this role for administering your individual accounts.

   IAM execution role name

   AWSCloudFormationStackSetExecutionRole

   IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

   Cancel | Previous | Next

   Configure StackSet options

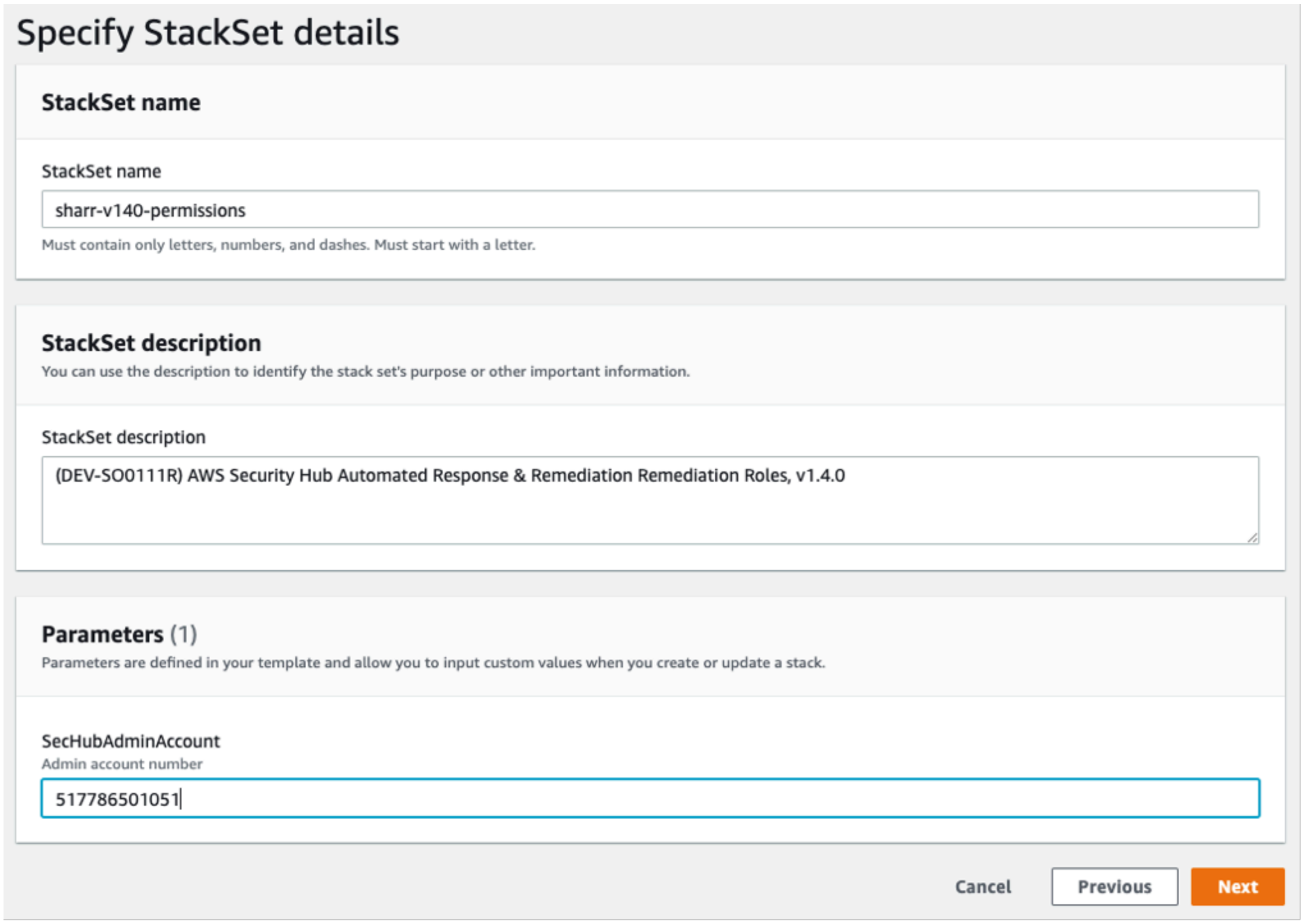
2. For the **Account numbers** parameter, enter the account ID of the AWS Security Hub admin account.

3. For the **Specify regions** parameter, select only the Region where Security Hub admin is turned on. Wait for this step to complete before going on to Step 2.

Step 2. Install the remediation roles into each AWS Security Hub member account

Use a service-managed StackSets to deploy the member roles template, `aws-sharr-member-roles.template`. This StackSet must be deployed in one Region per member account. It defines the global roles that allow cross-account API calls from the SHARR Orchestrator step function.

1. Deploy to the entire organization (typical) or to organizational units, as per your organizations policies.
2. Turn on automatic deployment so new accounts in the AWS Organizations receive these permissions.
3. For the **Specify regions** parameter, select a single Region. IAM roles are global. You can continue to Step 3 while this StackSet deploys.



Specify StackSet details

StackSet name

StackSet name

sharr-v140-permissions

Must contain only letters, numbers, and dashes. Must start with a letter.

StackSet description

You can use the description to identify the stack set's purpose or other important information.

StackSet description

(DEV-SO0111R) AWS Security Hub Automated Response & Remediation Remediation Roles, v1.4.0

Parameters (1)

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

SecHubAdminAccount

Admin account number

517786501051

Specify StackSet details

Step 3. Launch the member stack into each AWS Security Hub member account and Region

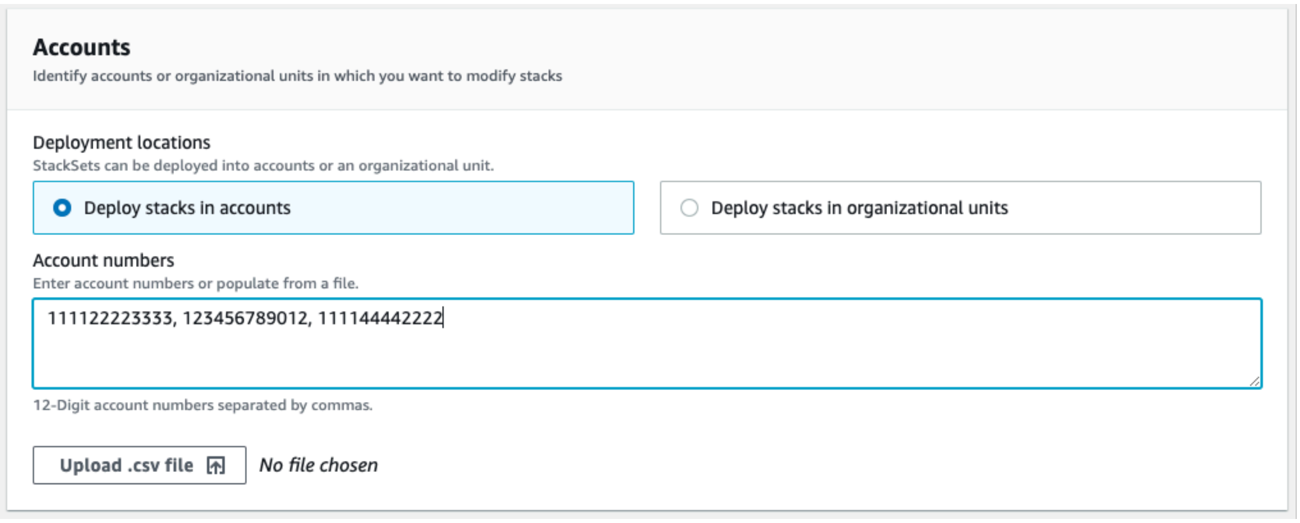
Because the member stack uses nested stacks, you must deploy as a self-managed StackSet. This does not support automatic deployment to new accounts in the AWS Organization.

Parameters

LogGroup Configuration: Choose the log group that receives CloudTrail logs. If none exists, or if the log group is different for each account, choose a convenient value. Account administrators must update the Systems Manager – Parameter Store /Solutions/SO0111/Metrics_LogGroupName parameter after creating a CloudWatch Logs Group for CloudTrail logs. This is required for remediations that create metrics alarms on API calls.

Standards: Choose the standards to load in the member account. This only installs the AWS Systems Manager runbooks – it does not enable the Security Standard.

SecHubAdminAccount: Enter the account ID of the AWS Security Hub Admin account where you installed the solution's admin template.



Accounts
Identify accounts or organizational units in which you want to modify stacks

Deployment locations
StackSets can be deployed into accounts or an organizational unit.

● Deploy stacks in accounts ○ Deploy stacks in organizational units

Account numbers
Enter account numbers or populate from a file.

111122223333, 123456789012, 111144442222

12-Digit account numbers separated by commas.

Accounts

Deployment locations: You may specify a list of account numbers or organizational units.

Specify regions: Select all of the Regions where you want to remediate findings. You can adjust Deployment options as appropriate for the number of accounts and Regions. Region Concurrency can be parallel.

Automated deployment - Stacks

Note

For multi-account customers, we strongly recommend deployment with StackSets.

Before you launch the solution, review the architecture, solution components, security, and design considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately 30 minutes

Prerequisites

Before you deploy this solution, ensure that AWS Security Hub is in the same AWS Region as your primary and secondary accounts. If you have previously deployed this solution, you must uninstall the existing solution. For more information, refer to Solution updates.

Deployment overview

Use the following steps to deploy this solution on AWS.

Step. 1 Launch the admin stack

- Launch the `aws-sharr-deploy.template` AWS CloudFormation template into your AWS Security Hub admin account.
- Choose which security standards to install.
- Choose an existing Orchestrator log group to use (select `Yes` if `SO0111-SHARR-Orchestrator` already exists from a previous installation).

Step. 2. Launch the member stack

- Specify the name of the CloudWatch Logs group to use with CIS 3.1-3.14 remediations. It must be the name of a CloudWatch Logs log group that receives CloudTrail logs.
- Choose whether to install the remediation roles. Install these roles only once per account.
- Select which playbooks to install.
- Enter the account ID of the AWS Security Hub admin account.

Step. 3 (Optional) Adjust the available remediations

- Remove any remediations on a per-member account basis. This step is optional.

Step 1. Launch the admin stack

⚠ **Important**

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy.
To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Collection of operational metrics section of this guide.

This automated AWS CloudFormation template deploys the Automated Security Response on AWS solution in the AWS Cloud. Before you launch the stack, you must enable Security Hub and complete the prerequisites.

ⓘ **Note**

You are responsible for the cost of the AWS services used while running this solution. For more details, visit to the Cost section in this guide, and refer to the pricing webpage for each AWS service used in this solution.

1. Sign in to the AWS Management Console from the account where the AWS Security Hub is currently configured, and use the button below to launch the `aws-sharr-deploy.template` AWS CloudFormation template.

   Launch solution

   You can also download the template as a starting point for your own implementation.

2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the AWS Management Console navigation bar.

   > **Note**
   >
   > This solution uses AWS Systems Manager which is currently available in specific AWS Regions only. The solution works in all of the Regions that support this service. For the most current availability by Region, refer to the AWS Regional Services List.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and then choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS limits in the *AWS Identity and Access Management User Guide*.
5. On the **Parameters** page, choose **Next**.

Parameter	Default	Description
Load AFSBP Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of FSBP controls.
Load CIS120 Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Load CIS140 Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS140 controls.
Load PC1321Admin Stack	`yes`	Specify whether to install the admin components for

Parameter	Default	Description
		automated remediation of CIS120 controls.
Load SC Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of SC controls.
Reuse Orchestrator Log Group	`no`	Select whether or not to reuse an existing `SO0111-SHARR-Orchestrator` CloudWatch Logs group. This simplifies reinstallation and upgrades without losing log data from a previous version. If you are upgrading from v1.2 or above, select `yes`.

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

Step 2. Install the remediation roles into each AWS Security Hub member account

The `aws-sharr-member-roles.template` StackSet must be deployed in only one Region per member account. It defines the global roles that allow cross-account API calls from the SHARR Orchestrator step function.

1. Sign in to the AWS Management Console for each AWS Security Hub member account (including the admin account, which is also a member). Select the button to launch the `aws-`

`sharr-member-roles.template` AWS CloudFormation template. You can also download the template as a starting point for your own implementation.

Launch solution

2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the AWS Management Console navigation bar.
3. On the **Create stack** page, verify that the correct template URL is in the Amazon S3 URL text box and then choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS limits in the AWS Identity and Access Management User Guide.
5. On the **Parameters** page, specify the following parameters and choose Next.

Parameter	Default	Description
Sec Hub Account Admin	*`<Requires input>`*	Enter the 12-digit account ID for the AWS Security Hub admin account. This value grants permissions to the admin account's solution role.

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 5 minutes. You may continue with the next step while this stack loads.

Step 3. Launch the member stack

Important

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy.

To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Collection of operational metrics section of this guide.

The `aws-sharr-member` stack must be installed into each Security Hub member account. This stack defines the runbooks for automated remediation. The admin for each member account can control what remediations are available via this stack.

1. Sign in to the AWS Management Console for each AWS Security Hub member account (including the admin account, which is also a member). Select the button to launch the `aws-sharr-member.template` AWS CloudFormation template.

   Launch solution

   You can also download the template as a starting point for your own implementation.

2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the AWS Management Console navigation bar.

   Note

   This solution uses AWS Systems Manager, which is currently available in the majority of AWS Regions. The solution works in all of the Regions that support these services. For the most current availability by Region, refer to the AWS Regional Services List.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and then choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS limits in the *AWS Identity and Access Management User Guide*.
5. On the **Parameters** page, specify the following parameters and choose **Next**.

Parameter	Default	Description
Provide the name of the LogGroup to be used to create Metric Filters and Alarms	*<Requires input>*	Specify the name of a CloudWatch Logs group where CloudTrail logs API calls. This is used for CIS 3.1-3.14 remediations.
Load AFSBP Member Stack	`yes`	Specify whether to install the admin components for automated remediation of FSBP controls.
Load CIS120 Member Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Load CIS140 Member Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS140 controls.
Load PC1321 Member Stack	`yes`	Specify whether to install the admin components for automated remediation of PC1321 controls.
Load SC Member Stack	`yes`	Specify whether to install the admin components for

Parameter	Default	Description
		automated remediation of SC controls.
Create S3 Bucket For Redshift Audit Logging	no	Select `yes` if the S3 bucket should be created for the FSBP RedShift.4 remediation. For details of the S3 bucket and the remediation, review the [Redshift.4 remediation](#) in the *AWS Security Hub User Guide*.
Sec Hub Admin Account	*<Requires input>*	Enter the 12-digit account ID for the AWS Security Hub admin account.

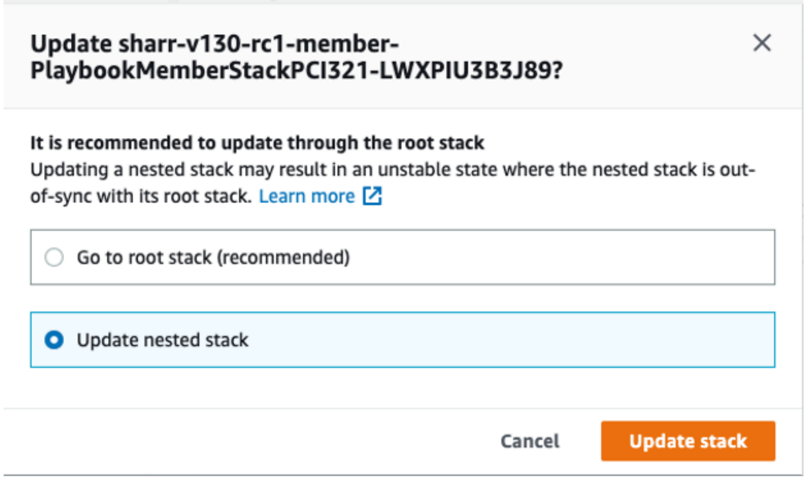
6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

Step 4: (Optional) Adjust the available remediations

If you want to remove specific remediations from a member account, you can do so by updating the nested stack for the security standard. For simplicity, the nested stack options are not propagated to the root stack.

1. Sign in to the [AWS CloudFormation console](#) and select the nested stack.
2. Choose **Update**.
3. Select **Update nested stack** and choose **Update stack**.



Update sharr-v130-rc1-member-PlaybookMemberStackPCI321-LWXPIU3B3J89?

It is recommended to update through the root stack

Updating a nested stack may result in an unstable state where the nested stack is out-of-sync with its root stack. Learn more

○ Go to root stack (recommended)

● Update nested stack

Update nested stack

4. Select **Use current template** and choose **Next**.
5. Adjust the available remediations. Change the values for desired controls to `Available` and undesired controls to `Not available`.

> **Note**
>
> Turning off a remediation removes the solutions remediation runbook for the security standard and control.

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Update stack**.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

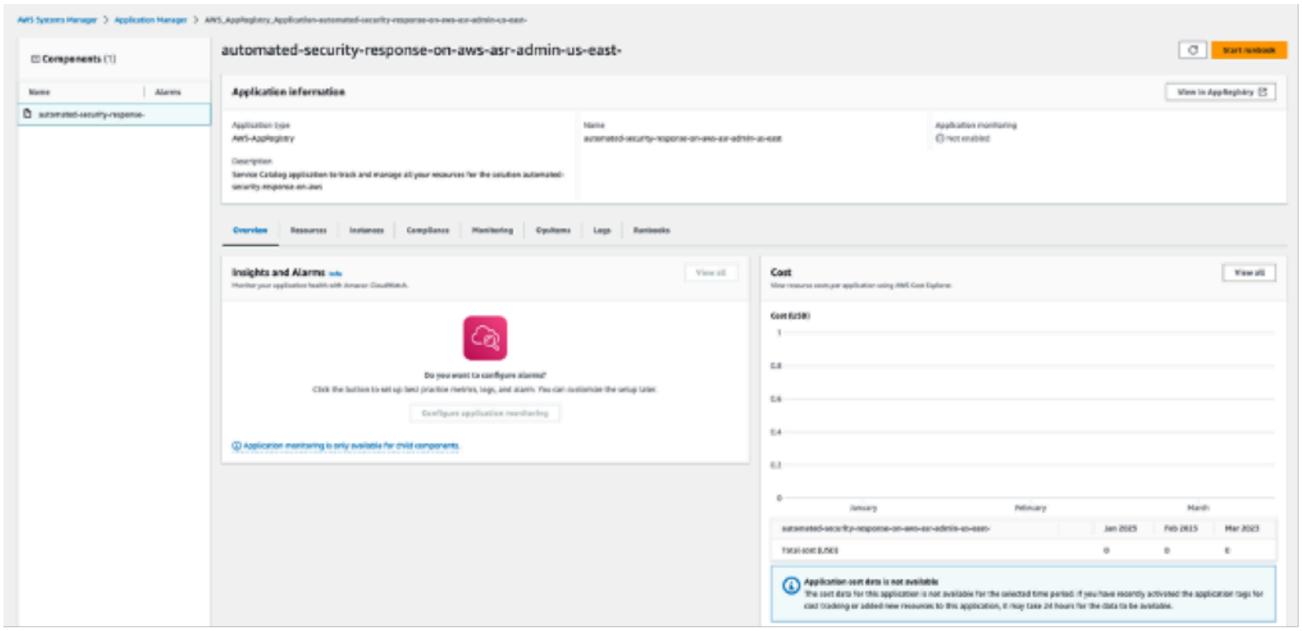
Monitoring this solution with Service Catalog AppRegistry

The Automated Security Response on AWS solution includes a Service Catalog AppRegistry resource to register the CloudFormation template and underlying resources as an application in both AWS Service Catalog AppRegistry and AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager gives you an application-level view into this solution and its resources so that you can:

- Monitor its resources, costs for the deployed resources across stacks and AWS accounts, and logs associated with this solution from a central location.
- View operations data for the resources of this solution in the context of an application, such as deployment status, CloudWatch alarms, resource configurations, and operational issues.

The following figure depicts an example of the application view for the Automated Security Response on AWS stack in Application Manager.



AWS Systems Manager > Application Manager > AWS_AppRegistry_Application-automated-security-response-on-aws-asr-admin-us-east-
Components (1)
Name
Alarms
automated-security-response-
automated-security-response-on-aws-asr-admin-us-east-
Start runbook
Application information
View in AppRegistry
Overview
Resources
Instances
Compliance
Monitoring
OpsItems
Logs
Runbooks
Insights and Alarms
Info
View all
Configure application monitoring
Cost
View all
Cost (USD)
1
0.8
0.6
0.4
0.2
0
January
February
March

Application type
AWS-AppRegistry

Name
automated-security-response-on-aws-asr-admin-us-east

Application monitoring
Not enabled

Description
Service Catalog application to track and manage all your resources for the solution automated-security-response-on-aws

Monitor your application health with Amazon CloudWatch.

Do you want to configure alarms?
Click the button to set up best practice metrics, logs, and alarms. You can customize the setup later.

Application monitoring is only available for child components.

View resource costs per application using AWS Cost Explorer.

automated-security-response-on-aws-asr-admin-us-east-	Jan 2023	Feb 2023	Mar 2023
Total cost (USD)	0	0	0

Application cost data is not available
The cost data for this application is not available for the selected time period. If you have recently activated the application tags for cost tracking or added new resources to this application, it may take 24 hours for the data to be available.

Automated Security Response on AWS in Application Manager

Note

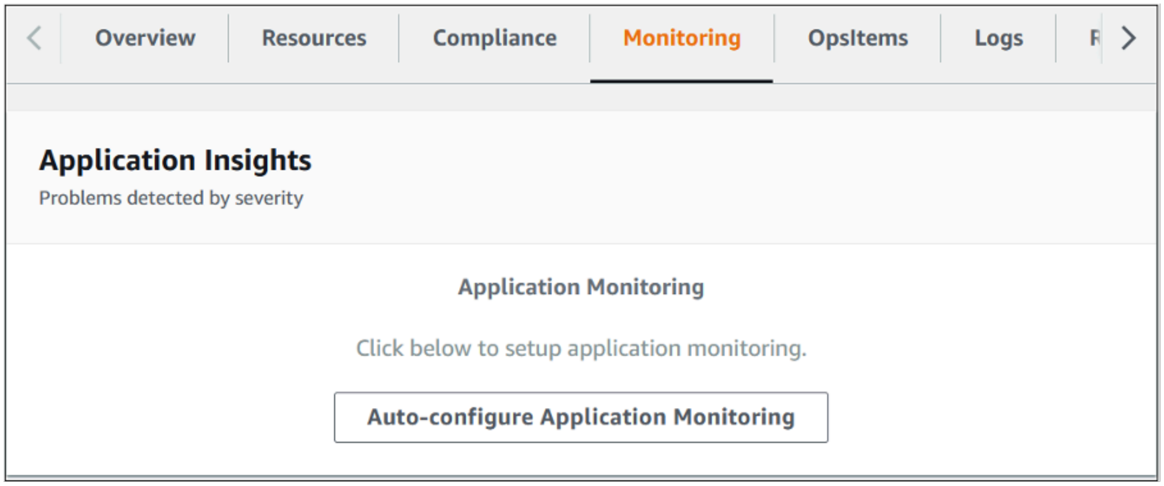
You must activate CloudWatch Application Insights, AWS Cost Explorer, and cost allocation tags associated with this solution. They are not activated by default

Activate CloudWatch Application Insights

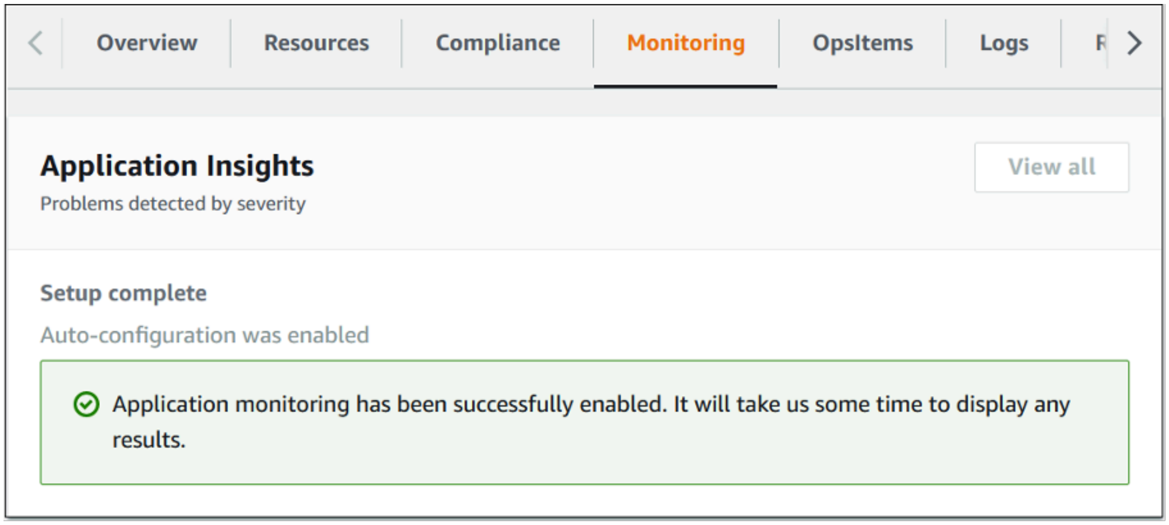
1. Open the Systems Manager console.
2. In the navigation pane, choose **Application Manager**.
3. In **Applications**, choose **AppRegistry applications**.
4. In **AppRegistry applications**, search for the application name for this solution and select it.

The next time you open Application Manager, you can find the new application for your solution in the **AppRegistry application** category.

5. In the **Components** tree, choose the application stack you want to activate.
6. In the **Monitoring** tab, in **Application Insights**, select **Auto-configure Application Monitoring**.


Overview
Resources
Compliance
Monitoring
OpsItems
Logs
R
Application Insights
Problems detected by severity
Application Monitoring
Click below to setup application monitoring.
Auto-configure Application Monitoring

Monitoring for your applications is now activated and the following status box appears:



Application Insights

Problems detected by severity

Setup complete

Auto-configuration was enabled

✓ Application monitoring has been successfully enabled. It will take us some time to display any results.

Activate AWS Cost Explorer

You can see the overview of the costs associated with the application and application components within the Application Manager console through integration with AWS Cost Explorer which must be first activated. Cost Explorer helps you manage costs by providing a view of your AWS resource costs and usage over time. To activate Cost Explorer for the solution:

1. Sign in to the AWS Cost Management console.
2. In the left navigation menu, select **Cost Explorer**.
3. On the **Welcome to Cost Explorer** page, choose **Launch Cost Explorer**.

The activation process can take up to 24 hours to complete. Once activated, you can open the Cost Explorer user interface to further analyze cost data for the solution.

Activate cost allocation tags associated with the solution

After you activate Cost Explorer, you must activate a cost allocation tag to see the costs for this solution. The cost allocation tags can only be activated from the management account for the organization. To activate cost allocation tags:

To activate cost allocation tags:

1. Sign in to the AWS Billing and Cost Management console.
2. In the navigation pane, select **Cost Allocation Tags**.

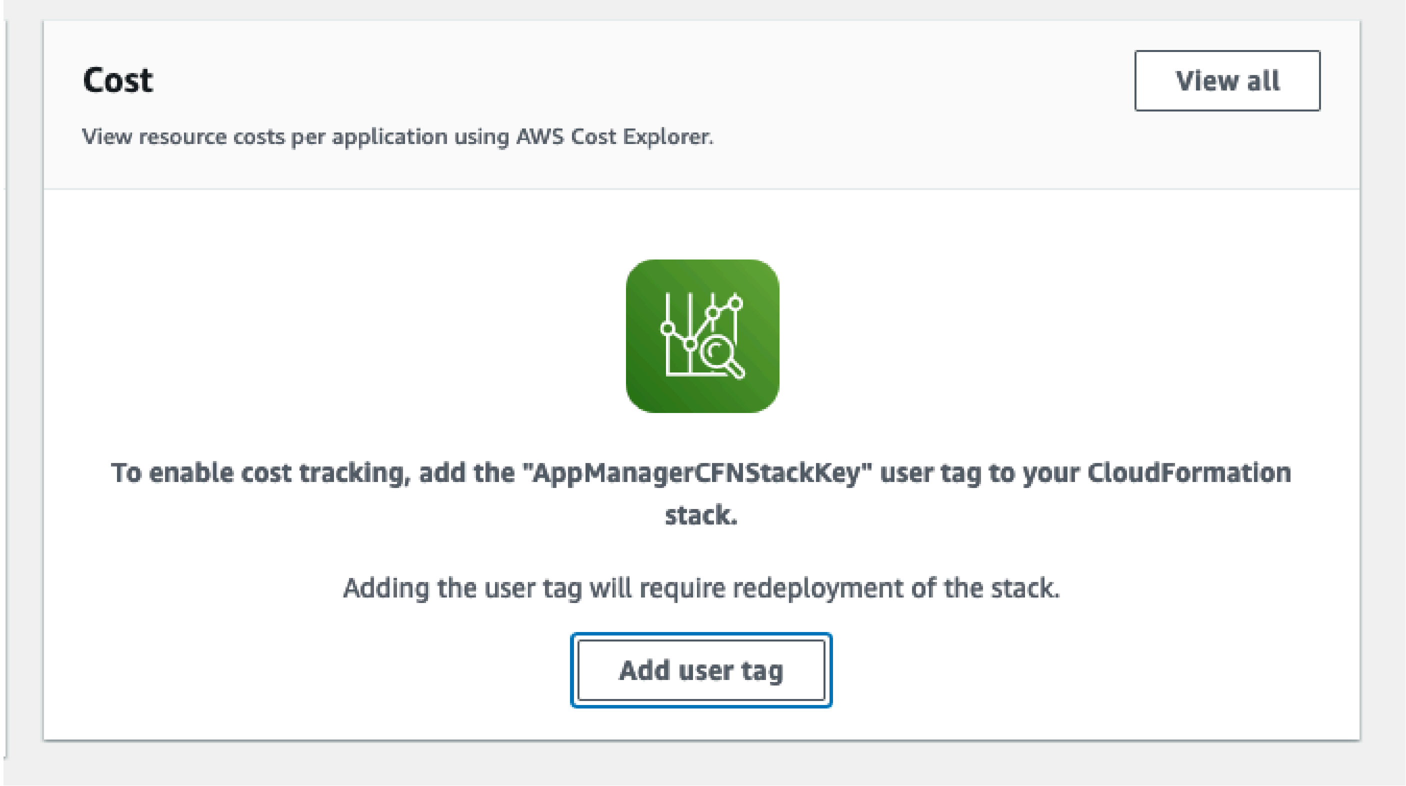
3. On the **Cost allocation tags** page, filter for the `AppManagerCFNStackKey` tag, then select the tag from the results shown.
4. Choose **Activate**

The activation process can take up to 24 hours to complete and the tag data to appear.

Confirm cost tags associated with the solution

After you activate cost allocation tags associated with the solution, you must confirm the cost allocation tags to see the costs for this solution. To confirm cost allocation tags:

1. Sign in to the Systems Manager console.
2. In the navigation pane, choose **Application Manager**.
3. In **Applications**, choose the application name for this solution and select it.
4. In the **Overview** tab, in **Cost**, select **Add user tag**.



Cost

View resource costs per application using AWS Cost Explorer.

To enable cost tracking, add the "AppManagerCFNStackKey" user tag to your CloudFormation stack.

Adding the user tag will require redeployment of the stack.

5. On the **Add user tag** page, enter `confirm`, then select **Add user tag**.

The activation process can take up to 24 hours to complete and the tag data to appear.

Update the solution

Upgrading from versions prior to v1.4

If you have previously deployed the solution prior to v1.4.x, uninstall, then install the latest version:

1. Uninstall the previously deployed solution. Refer to Uninstall the solution.
2. Launch the latest template. Refer to Automated deployment.

> **Note**
>
> If you are upgrading from v1.2.1 or earlier to v1.3.0 or later, set **Use existing Orchestrator Log Group** to No. If you are reinstalling v1.3.0 or later, you can select Yes for this option. This option allows you to continue to log to the same Log Group for the Orchestrator Step Functions.

Upgrading from v1.4 and later

If you are upgrading from v1.4.x, update all stacks or StackSets as follows:

1. Update the stack in the Security Hub admin account using the latest template.
2. In each member account, update the permissions from the latest template.
3. In each member account in all Regions where currently deployed, update the member stack from the latest template.

Troubleshooting

Solution logs

This section includes Troubleshooting information for this solution, see left navigation for topics.

This solution collects output from remediation runbooks, which run under AWS Systems Manager, and logs the result to CloudWatch Logs group `SO0111-SHARR` in the AWS Security Hub admin account. There is one stream per control per day.

The Orchestrator Step Function logs all step transitions to the `SO0111-SHARR-Orchestrator` CloudWatch Logs Group in the AWS Security Hub admin account. This log is an audit trail to record state transitions for each instance of the Step Function. There is one log stream per Step Function execution.

Both log groups are encrypted using an AWS KMS Customer-Manager Key (CMK).

The following troubleshooting information uses the `SO0111-SHARR` log group. Use this log, as well as AWS Systems Manager Automation console, Automation Executions logs, Step Function console, and Lambda logs to troubleshoot problems.

If a remediation fails, a message similar to the following will be logged to `SO0111-SHARR` in the log stream for the standard, control, and date. For example: **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)
```

The following messages provide additional detail. This output is from the SHARR runbook for the security standard and control. For example: **SHARR-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.
```

This information points you to the failure, which in this case was a child automation running in the member account. To troubleshoot this issue, you must log in to the AWS Management

Console in the member account (from the message above), go to AWS Systems Manager, navigate to **Automation**, and examine the log output for Execution ID `eecdef79-9111-4532-921a-e098549f525`.

Issues and resolutions

- **Issue:** The solution deployment fails with an error stating that the resources are already available in Amazon CloudWatch.

  Resolution: Check for an error message in the CloudFormation resources/events section indicating log groups already exist. The SHARR deployment templates allow reuse of existing log groups. Verify that you have selected reuse.
- **Issue:** I run Security Hub in multiple Regions in the same account. I want to deploy this solution in multiple Regions.

  Resolution: You must deploy the admin stack in the same account and Region as your Security Hub admin. Install the member template into each account and Region where you have a Security Hub member configured. Enable aggregation in Security Hub.
- **Issue:** Immediately after deploying, the **SO0111-SHARR-Orchestrator** is failing in the Get Automation Document State with a 502 error: *"Lambda was unable to decrypt the environment variables because KMS access was denied. Please check the function's KMS key settings. KMS Exception: UnrecognizedClientExceptionKMS Message: The security token included in the request is invalid. (Service: AWSLambda; Status Code: 502; Error Code: KMSAccessDeniedException; Request ID: …"*

  Resolution: Allow the solution about 10 minutes to stabilize before running remediations. If the problem continues, open a support ticket or GitHub issue.
- **Issue**: I attempted to remediate a finding but nothing happened.

  Resolution: Check the notes of the finding for reasons why it was not remediated. A common cause is that the finding has no automated remediation. At this time there is no way to provide direct feedback to the user when no remediation exists other than via the notes.

  Review the solution logs. Open CloudWatch Logs in the console. Find the SO0111-SHARR CloudWatch Logs Group. Sort the list so the most-recently updated streams appear first. Select the log stream for the finding you attempted to run. You should find any errors there. Some reasons for the failure could be: mismatch between finding control and remediation control, cross-account remediation (not yet supported), or that the finding has already been remediated.

If unable to determine the reason for the failure, please collect the logs and open a support ticket.

- **Issue:** After starting a remediation, the status in the Security Hub console has not updated.

  Resolution: The Security Hub console does not update automatically. Refresh the current view. The status of the finding should update.

  It might take several hours for the finding to transition from **Failed** to **Passed**. Findings are created from event data sent by other services, such as AWS Config, to AWS Security Hub. The time before a rule is reevaluated depends on the underlying service.

  If this does not resolve the issue, refer to the resolution above for *“I attempted to remediate a finding but nothing happened.”*
- **Issue**: Orchestrator step function fails in **Get Automation Document State**: *An error occurred (AccessDenied) when calling the AssumeRole operation*.

  Resolution: The member template has not been installed in the member account where SHARR is attempting to remediate a finding. Follow instructions for deployment of the member template.
- **Issue**: Config.1 runbook fails because Recorder or Delivery Channel already exists.

  Resolution: Inspect your AWS Config settings carefully to ensure Config is properly set up. The automated remediation is not able to fix existing AWS Config settings in some cases.
- **Issue**: Remediation is successful but returns the message "`No output available yet because the step is not successfully executed.`"

  Resolution: This is a known issue in this release where certain remediation runbooks do not return a response. The remediation runbooks will properly fail and signal the solution if they do not work.
- **Issue**: The resolution failed and sent a stack trace.

  Resolution: Occasionally, we miss the opportunity to handle an error condition that results in a stack trace rather than an error message. Attempt to troubleshoot the problem from the trace data. Open a support ticket if you need assistance.
- **Issue**: Removal of the v1.3.0 stack failed on the Custom Action resource.

  Resolution: Removal of the admin template may fail on the Custom Action removal. This is a known issue that will be fixed in the next release. If this occurs:

1. Sign in to AWS Security Hub management console.
2. In the admin account, go to **Settings**.
3. Select the **Custom actions** tab
4. Manually delete the entry **Remediate with SHARR**.
5. Delete the stack again.

- **Issue**: After redeploying the admin stack the step function is failing on `AssumeRole`.

  Resolution: Redeploying the admin stack breaks the trust connection between the admin role in the admin account and the member role in the member accounts. You must redeploy the member roles stack in all member accounts.

- **Issue**: CIS 3.x remediations are not showing `PASSED` after more than 24 hours.

  Resolution: This is a common occurrence if you have no subscriptions to the `SO0111-SHARR_LocalAlarmNotification` SNS topic in the member account.

Issues with specific remediations

SetSSLBucketPolicy fails with AccessDenied error

Associated controls: 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

Issue: The SetSSLBucketPolicy fails with an AccessDenied error:

An error occurred (AccessDenied) when calling the PutBucketPolicy operation: Access Denied

If the Block Public Access setting has been enabled for a bucket, attempts to put a bucket policy that includes statements that allow public access with fail with this error. This state can be reached by putting a bucket policy that contains such statements, then enabling the public access block for that bucket.

The remediation ConfigureS3BucketPublicAccessBlock (associated controls: 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) can also put a bucket into this state because it sets the public access block setting without changing the bucket policy.

The SetSSLBucketPolicy adds a statement to the bucket policy to deny requests that do not use SSL. It does not modify the other statements in the policy, so if there are statements that allow public access, the remediation will fail attempting to put the modified bucket polic that still includes those statements.

Resolution: Modify the bucket policy to remove statements that allow public access in conflict with the block public access setting on the bucket.

Uninstall the solution

Use the following procedure to uninstall the solution with the AWS Management Console.

V1.0.0-V1.2.1

For releases v1.0.0 to v1.2.1, use Service Catalog to uninstall the CIS and/or FSBP Playbooks. With v1.3.0 Service Catalog is no longer used.

1. Sign in to the AWS CloudFormation console and navigate to the Security Hub primary account.
2. Choose **Service Catalog** to terminate any provisioned playbooks, remove any security groups, roles, or users.
3. Remove the spoke `CISPermissions.template` template form the Security Hub member accounts.
4. Remove the spoke `AFSBPMemberStack.template` template form the Security Hub admin and member accounts.
5. Navigate to the Security Hub primary account, select the solution's installation stack, and then choose **Delete**.

> **Note**
>
> CloudWatch Logs group logs are retained. We recommend retaining these logs as required by your organization's log retention policy.

V1.3.x

1. Remove the `aws-sharr-member.template` from each member account.
2. Remove the `aws-sharr-admin.template` from the admin account.

> **Note**
>
> Removal of the admin template in v1.3.0 will likely fail on the Custom Action removal. This is a known issue that will be fixed in the next release. Use the following instructions to fix this issue:

1. Sign in to the AWS Security Hub management console.
2. In the admin account, go to **Settings**.
3. Select the **Custom actions** tab.
4. Manually delete the entry **Remediate with SHARR**.
5. Delete the stack again.

V1.4.0 and later

Stack deployment

1. Remove the `aws-sharr-member.template` from each member account.
2. Remove the `aws-sharr-admin.template` from the admin account.

StackSet deployment

For each StackSet, remove stacks, then remove the StackSet in the reverse order of deployment.

Note that IAM roles from the `aws-sharr-member-roles.template` are retained even if the template is removed. This is so that remediations using these roles continue to function. These SO0111-* roles can be manually removed after verifying that they are no longer in use by active remediations, such as CloudTrail to CloudWatch logging, or RDS Enhanced Monitoring.

Administrator guide

Enabling and disabling parts of the solution

As a solution administrator, you have the following controls over which functionalities of the solution are enabled.

Where the member and member roles stacks are deployed:

- The admin stack will only be able to initiate remediations (through custom action or fully automated EventBridge rules) in accounts in which the member and member roles stacks have been deployed with the admin account number given as a parameter value.
- To exempt accounts or regions from control of the solution completely, do not deploy the member or member roles stacks to those accounts or regions.

Account and region finding aggregation configuration in Security Hub:

- The admin stack will only be able to initiate remediations (through custom action or fully automated EventBridge rules) for findings which arrive in the admin account and region.
- To exempt accounts or regions from control of the solution completely, do not include those accounts or regions to send findings to the same admin account and region in which the admin stack is deployed.

Which standard nested stacks are deployed:

- The admin stack will only be able to initiate remediations (through custom action or fully automated EventBridge rules) for controls which have a control runbook deployed in the target member account and region. These are deployed by the member stack for each standard.
- The admin stack will only be able to initiate fully automated remediations using EventBridge rules for controls which have the rules deployed by the admin stack for that standard. These are deployed to the admin account.
- For simplicity, we recommend deploying standards consistently across your admin and member accounts. If you care about AWS FSBP and CIS v1.2.0, deploy those two nested admin stacks to the admin account, and deploy those two nested member stacks to each member account and region.

Which Control runbooks are deployed in each nested member stack:

- The admin stack will only be able to initiate remediations (through custom action or fully automated EventBridge rules) for controls which have a control runbook deployed in the target member account and region by the member stack for each standard.
- To exercise more fine-grained control over which controls are enabled for a particular standard, each nested stack for a standard has parameters for which control runbooks are deployed. Set the parameter for a control to the value “NOT Available” to undeploy that control runbook.

SSM Parameters for enabling and disabling standards:

- The admin stack will only be able to initiate remediations (through custom action or fully automated EventBridge rules) for standards that are enabled through the SSM Parameter deployed by the standard admin stack.
- To disable a standard, set the value for the SSM Parameter with the path “/Solutions/SO0111/<standard_name>/<standard_version>/status” to “No”.

Example SNS notifications

When a remediation is initiated

```
{
  "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"
  }
}
```

When a remediation succeeds

```
{
  "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"
  }
}
```

When a remediation fails

```
{
  "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"
  }
}
```

Use the solution

This is a tutorial that will guide you through your first deployment of ASR. It will begin with the prerequisites for deploying the solution and it will end with you remediating example findings in a member account.

Tutorial: Getting Started with Automated Security Response on AWS

This is a tutorial that will guide you through your first deployment of ASR. It will begin with the prerequisites for deploying the solution and it will end with you remediating example findings in a member account.

Prepare the accounts

In order to demonstrate the cross-account and cross-region remediation capabilities of the solution, this tutorial will use two accounts. You can also deploy the solution to a single account.

The following examples use accounts 111111111111 and 222222222222 to demonstrate the solution. 111111111111 will be the admin account and 222222222222 will be the member account. We will set up the solution to remediate findings for resources in the regions `us-east-1` and `us-west-2`.

The table below is an example to illustrate the actions we will take for each step in each account and region.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	None	None
222222222222	Member	None	None

The admin account is the account that will perform the administration actions of the solution, namely initiating remediations manually or enabling fully automated remediation with EventBridge rules. This account must also be the Security Hub delegated administrator account for all accounts in which you wish to remediate findings, but it does not need to be nor should it be the AWS Organizations administrator account for the AWS Organization to which your accounts belong.

Enable AWS Config

Review the following documentation:

- AWS Config documentation
- AWS Config pricing
- Enabling AWS Config

Enable AWS Config in both accounts and both regions. This will incur charges.

⚠ **Important**

Ensure that you select the option to "Include global resources (e.g., AWS IAM resources)." If you do not select this option when enabling AWS Config, you will not see findings related to global resources (e.g. AWS IAM resources)

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Enable AWS Config	Enable AWS Config
222222222222	Member	Enable AWS Config	Enable AWS Config

Enable AWS security hub

Review the following documentation:

- AWS Security Hub documentation
- AWS Security Hub pricing
- Enabling AWS Security Hub

Enable AWS Security Hub in both accounts and both regions. This will incur charges.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Enable AWS Security hub	Enable AWS Security hub
222222222222	Member	Enable AWS Security hub	Enable AWS Security hub

Enable consolidated control findings

Review the following documentation:

- Generating and updating control findings

For the purposes of this tutorial, we will demonstrate the usage of the solution with the consolidated control findings feature of AWS Security Hub enabled, which is the recommended configuration. In partitions which do not support this feature as of the time of writing, you will need to deploy the standard-specific playbooks rather than SC (Security Control).

Enable consolidated control findings in both accounts and both regions.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Enable Consolidated control findings	Enable Consolidated control findings
222222222222	Member	Enable Consolidated control findings	Enable Consolidated control findings

It may take some time for findings to be generated with the new feature. You can proceed with the tutorial, but you will be unable to to remediate findings generated without the new feature. Findings generated with the new feature can be identified by the `GeneratorId` field value `security-control/<control_id>`.

Configure cross-region finding aggregation

Review the following documentation:

- Cross-Region aggregation
- Enabling cross-Region aggregation

Configure finding aggregation from **us-west-2** to **us-east-1** in both accounts.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Configure aggregati on from us-west-2	None
222222222222	Member	Configure aggregati on from us-west-2	None

It may take some time for findings to propagate to the aggregation region. You can proceed with the tutorial, but you will be unable to remediate findings from other regions until they begin to appear in the aggregation region.

Designate a Security Hub administrator account

Review the following documentation:

- Managing accounts in AWS Security Hub
- Managing organization member accounts
- Managing member accounts by invitation

In the proceeding example, we will use the manual invitation method. For a set of production accounts, we recommend managing Security Hub delegated adminstration through AWS Organizations.

From the AWS Security Hub console in the admin account (111111111111), invite the member account (222222222222) to accept the admin account as a Security Hub delegated administrator. From the member account, accept the invitation.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Invite the member account	None
222222222222	Member	Accept the invitation	None

It may take some time for findings to propagate to the admin account. You can proceed with the tutorial, but you will be unable to remediate findings from member accounts until they begin to appear in the admin account.

Create the roles for self-managed StackSets permissions

Review the following documentation:

- AWS CloudFormation StackSets
- Grant self-managed permissions

We will be deploying CloudFormation stacks to multiple accounts, so we will use StackSets. We cannot use service-managed permissions because the admin stack and the member stack have nested stacks, which aren't supported by the service, so we must use self-managed permissions.

Deploy the stacks for basic permissions for StackSet operations. For production accounts, you may wish to narrow the permissions according to the "advanced permissions options" documentation.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Deploy the StackSet administrator role stack	None
222222222222	Member	Deploy the StackSet execution role stack	None

Create the insecure resources that will generate example findings

Review the following documentation:

- Security Hub controls reference
- AWS Lambda controls

The following example resource with an insecure configuration in order to demonstrate a remediation. The example control is Lambda.1: Lambda function policies should prohibit public access.

⚠ **Important**

We will be intentionally creating a resource with an insecure configuration. Please review the nature of the control and evaluate the risk of creating such a resource in your environment for yourself. Be aware of any tooling your organization may have for detecting and reporting such resources and request an exception if appropriate. If the example control we have selected is inappropriate for you, select another control that the solution supports.

In the second region of the member account, navigate to the AWS Lambda console and create a function in the latest Python runtime. Under Configuration -> Permissions, add a policy statement to allow invoking the function from the URL with no authentication.

Confirm on the console page that the function allows public access. After the solution remediates this issue, compare the permissions to confirm that the public access has been revoked.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	None	None
222222222222	Member	None	Create a Lambda function with an insecure configura tion

It may take some time for AWS Config to detect the insecure configuration. You can proceed with the tutorial, but you will be unable to remediate the finding until Config detects it.

Create CloudWatch log groups for related controls

Review the following documentation:

- Monitoring CloudTrail Log Files with Amazon CloudWatch Logs
- CloudTrail controls

Various CloudTrail controls supported by the solution require there to be a CloudWatch Log group that is the destination of a multi-region CloudTrail. In the following example, we will create a placeholder log group. For production accounts, you should properly configure CloudTrail integration with CloudWatch Logs.

Create a log group in each account and region with the same name, for example: `asr-log-group`.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Create a log group	Create a log group
222222222222	Member	Create a log group	Create a log group

Deploy the solution to tutorial accounts

Gather the three Amazon S3 URLs for the admin, member, and member roles stack.

Deploy the admin stack

View template

aws-sharr-deploy.template

In the admin account, navigate to the CloudFormation console and deploy the admin stack into the Security Hub finding aggregation region.

Choose No for the value of all parameters for loading nested admin stacks except for the "SC" or "Security Control" stack. This stack contains the resources for the consolidated control findings that we have configured in our accounts.

Choose No for reusing the orchestrator log group unless you have deployed this solution in this account and region before.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Deploy the admin stack	None
222222222222	Member	None	None

Wait until the admin stack completes deployment before continuing so a trust relationship can be created from the member accounts to the admin account.

Deploy the member stack

View template

aws-sharr-member.template

In the admin account, navigate to the CloudFormation StackSets console and deploy the member stack to each account and region. Use the StackSets admin and execution roles created in this tutorial.

Enter the name of the log group you created as the value for the parameter for the log group name.

Choose No for the value of all parameters for loading nested member stacks except for the "SC" or "security control" stack. This stack contains the resources for the consolidated control findings that we have configured in our accounts.

Enter the ID of the admin account as the value for the parameter for the admin account number. In our example, this is 111111111111.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Deploy the member StackSet / Confirm	Confirm member stack deployed

Account	Purpose	Action in us-east-1	Action in us-west-2
		member stack deployed	
222222222222	Member	Confirm member stack deployed	Confirm member stack deployed

Deploy the member roles stack

View template

aws-sharr-member-roles.template

In the admin account, navigate to the CloudFormation StackSets console and deploy the member stack to each account. Use the StackSets admin and execution roles created in this tutorial. Enter the ID of the admin account as the value for the parameter for the admin account number. In our example, this is 111111111111.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Deploy the member StackSet / Confirm member stack deployed	None
222222222222	Member	Confirm member stack deployed	None

You can proceed, but you will be unable to remediate findings until CloudFormation StackSets finishes deploying.

Subscribe to the SNS topic

In the admin account, subscribe to the Amazon SNS topic created by the admin stack. This will notify you when remediations are initiated and when the succeed or fail.

Remediate example findings

In the admin account, navigate to the Security Hub console and locate the finding for the resource with an insecure configuration that you created as part of this tutorial.

This can be done in several ways:

1. In partitions which support the consolidated control findings feature, a page labeled "Controls" allows you to locate the finding by the consolidated control ID.
2. In the "Security standards" page, you can locate the control according to which standard it belongs to.
3. You can view all findings on the "Findings" page and search by attribute.

The consolidated control ID for the public Lambda Function we created is Lambda.1.

Initiate the remediation

Select the checkbox to the left of the finding related to the resource we created. In the "Actions" drop-down menu, select "Remediate with ASR". You will see a notification that the finding was sent to Amazon EventBridge.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Initiate the remediation	None
222222222222	Member	None	None

Confirm that the remediation resolved the finding

You should receive two SNS notifications. The first will indicate that a remediation has been initiated, and the second will indicate that the remediation succeeded. After receiving the second notification, navigate to the Lambda console in the member account and confirm that the public access has been revoked.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	None	None
222222222222	Member	None	Confirm that the remediation succeeded

Trace the execution of the remediation

To understand better how the solution works, you can trace the execution of the remediation.

EventBridge rule

In the admin account, locate an EventBridge rule named "**Remediate_with_SHARR_CustomAction"**. This rule matches the finding you sent from Security Hub and sends it to the orchestrator Step Function.

Step Function execution

In the admin account, locate a Step Function named "**SO0111-SHARR-Orchestrator**". This step function calls the SSM Automation document in the target account and region. You can trace the execution of the remediation in the execution history of this Step Function.

SSM Automation

In the member account, navigate to the SSM Automation console. You will find two executions of a document named "ASR-SC_2.0.0_Lambda.1" and one execution of a document named "ASR-RemoveLambdaPublicAccess".

The first execution is from the orchestrator step function in the target account. The second execution occurs in the target region, which may not be the region from which the finding originated. The final execution is the remediation that revokes the public access policy from the Lambda Function.

CloudWatch Log Group

In the admin account, navigate to the CloudWatch Logs console and locate a Log Group named "**SO0111-SHARR**". This log group is the destination for high-level logs from the orchestrator Step Function.

Enable fully-automated remediations

The other mode of operation for the solution is to automatically remediate findings as they arrive in Security Hub.

Confirm that you have no resources this finding may accidentally be applied to

Enabling automatic remediations will initiate remediations on all resources matching the control you enable (Lambda.1).

> ⚠ **Important**
>
> Confirm that you want all public Lambda Functions within the scope of the solution to have this permission revoked. Fully-automated remediations will not be limited in scope to the Function you created. The solution will remediate this control if it is detected in any of the accounts and regions in which it is installed.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Confirm no desired public Functions	Confirm no desired public Functions
222222222222	Member	Confirm no desired public Functions	Confirm no desired public Functions

Enable the rule

In the Admin account, locate an EventBridge rule named **SC_2.0.0_Lambda.1_AutoTrigger** and enable it.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Enable the automated remediati on rules	None
222222222222	Member	None	None

Configure the resource

In the member account, re-configure the Lambda Function to allow public access.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	None	None
222222222222	Member	None	Configure the Lambda Function to allow public access

Confirm that the remediation resolved the finding

It may take some time for Config to detect the insecure configuration again. You should receive two SNS notifications. The first will indicate that a remediation has been initiated. The second will indicate that the remediation succeeded. After receiving the second notification, navigate to the Lambda console in the member account and confirm that the public access has been revoked.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Enable the automated remediati on rules	None
222222222222	Member	None	Confirm that the remediation succeeded

Clean up

Delete the example resources

In the member account, delete the example Lambda function you created.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	None	None
222222222222	Member	None	Delete the example Lambda Function

Delete the admin stack

In the admin account, delete the admin stack.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Delete the admin stack	None
222222222222	Member	None	None

Delete the member stack

In the Admin account, delete the member StackSet.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Delete the member StackSet Confirm member stack deleted	Confirm member stack deleted

Account	Purpose	Action in us-east-1	Action in us-west-2
222222222222	Member	Confirm member stack deleted	Confirm member stack deleted

Delete the member roles stack

In the Admin account, delete the member roles StackSet.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Delete the member roles StackSet Confirm rmember roles stack deleted	None
222222222222	Member	Confirm member roles stack deleted	None

Delete the retained roles

In each account, delete the retained IAM roles.

Important: These roles are retained for remediations which require a role in order for the remediation to continue functioning (e.g. VPC flow logging). Confirm that you do not require the continued function of any of these roles before deleting them.

Delete any roles prefixed with **SO0111-.**

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Delete retained roles	None
222222222222	Member	Delete retained roles	None

Schedule the retained KMS keys for deletion

The admin and member stacks both create and retain a KMS key. You will incur charges if you keep these keys.

These keys are retained in order to give you access to any resources encrypted by the solution. Confirm that you do not require them before scheduling them for deletion.

Identify the keys deployed by the solution using the aliases created by the solution or from the CloudFormation history. Schedule them for deletion.

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Identify and schedule admin key for deletion Identify and schedule member key for deletion	Identify and schedule member key for deletion
222222222222	Member	Identify and schedule member key for deletion	Identify and schedule member key for deletion

Delete the stacks for self-managed StackSets permissions

Delete the stacks created to allow for self-managed StackSets permissions

Account	Purpose	Action in us-east-1	Action in us-west-2
111111111111	Admin	Delete the StackSet administrator role stack	None
222222222222	Member	Delete the StackSet execution role stack	None

Developer guide

This section provides the source code for the solution and additional customizations.

Source code

Visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.

Playbooks

This solution includes the playbook remediations for the security standards defined as part of the Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, and Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1. If you have consolidated control findings enabled, then those controls are supported in all standards. If not, then the playbooks are supported for the previously listed standards.

For details on a specific remediation, refer to the Systems Manager automation document with the name deployed by the solution in your account. Go to the AWS Systems Manager console, then in the navigation pane choose **Documents**.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	Security control ID
ASR-EnableAutoScalingGroupELBHealthCheck Auto Scaling groups associated with a load balancer should use load balancer health checks	Autoscaling.1		Autoscaling.1		Autoscaling.1

ASR-CreateCloudTrailMultiRegionTrail CloudTrail should be activated and configured with at least one multi-Region trail	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1
ASR-EnableCloudTrailEncryption CloudTrail should have encryption at rest activated	CloudTrail.2	2.7	CloudTrail.1	3.7	CloudTrail.2
ASR-EnableCloudTrailLogFileValidation Ensure CloudTrail log file validation is activated	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4
ASR-EnableCloudTrailToCloudWatchLogging Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs	CloudTrail.5	2.4	CloudTrail.4	3.4	CloudTrail.5

ASR-ReplaceCodeBuildClearTextCredentials CodeBuild project environment variables should not contain clear text credentials	CodeBuild.2		CodeBuild.2		CodeBuild.2
ASR-EnableAWSConfig Ensure AWS Config is activated	Config.1	2.5	Config.1	3.5	Config.1
ASR-MakeEBSSnapshotsPrivate Amazon EBS snapshots should not be publicly restorable	EC2.1		EC2.1		EC2.1
ASR-RemoveVPCDefaultSecurityGroupRules VPC default security group should prohibit inbound and outbound traffic	EC2.2	4.3	EC2.2	5.3	EC2.2

ASR-EnableVPCFlowLogs VPC flow logging should be enabled in all VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6
ASR-EnableEbsEncryptionByDefault EBS default encryption should be activated	EC2.7				EC2.7
ASR-RevokeUnrotatedKeys Users' access keys should be rotated every 90 days or less	IAM.3	1.4		1.14	IAM.3
ASR-SetIAMPasswordPolicy IAM default password policy	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7
ASR-RevokeUnusedIAMUserCredentials User credentials should be turned off if not used within 90 days	IAM.8	1.3	IAM.7		IAM.8

ASR-RevokeUnusedIAMUserCredentials User credentials should be turned off if not used within 45 days				1.12	IAM.22
ASR-RemoveLambdaPublicAccess Lambda functions should prohibit public access	Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotPrivate RDS snapshots should prohibit public access	RDS.1		RDS.1		RDS.1
ASR-DisablePublicAccessToRDSInstance RDS DB Instances should prohibit public access	RDS.2		RDS.2		RDS.2

ASR-EncryptRDSSnapshot RDS cluster snapshots and database snapshots should be encrypted at rest	RDS.4				RDS.4
ASR-EnableMultiAZOnRDSInstance RDS DB instances should be configured with multiple Availability Zones	RDS.5				RDS.5
ASR-EnableEnhancedMonitoringOnRDSInstance Enhanced monitoring should be configured for RDS DB instances and clusters	RDS.6				RDS.6
ASR-EnableRDSClusterDeletionProtection RDS clusters should have deletion protection activated	RDS.7				RDS.7

ASR-EnableRDSInstanceDeletionProtection RDS DB instances should have deletion protection activated	RDS.8				RDS.8
ASR-EnableMinorVersionUpgradeOnRDSDBInstance RDS automatic minor version upgrades should be activated	RDS.13				RDS.13
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDS DB clusters should be configured to copy tags to snapshots	RDS.16				RDS.16
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift clusters should prohibit public access	Redshift.1		Redshift.1		Redshift.1

ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift clusters should have automatic snapshots activated	Redshift.3				Redshift.3
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift clusters should have audit logging activated	Redshift.4				Redshift.4
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift should have automatic upgrades to major versions activated	Redshift.6				Redshift.6
ASR-ConfigureS3PublicAccessBlock S3 Block Public Access setting should be activated	S3.1		S3.6	2.1.5.1	S3.1

ASR-ConfigureS3BucketPublicAccessBlock S3 buckets should prohibit public read access	S3.2		S3.2	2.1.5.2	S3.2
ASR-EnableDefaultEncryptionS3 S3 buckets should have server-side encryption activated	S3.4		S3.4	2.1.1	S3.4
ASR-SetSSLBucketPolicy S3 buckets should require requests to use SSL	S3.5		S3.5	2.1.2	S3.5
ASR-S3BlockDenylist Amazon S3 permissions granted to other AWS accounts in bucket policies should be restricted	S3.6				S3.6

ASR-ConfigureS3BucketPublicAccessBlock S3 Block Public Access setting should be activated at the bucket level	S3.8				S3.8
ASR-ConfigureS3BucketPublicAccessBlock Ensure the S3 bucket CloudTrail logs to is not publicly accessible		2.3			CloudTrail.6
ASR-CreateAccessLoggingBucket Ensure S3 bucket access logging is activated on the CloudTrail S3 bucket		2.6			CloudTrail.7
ASR-EnableKeyRotation Ensure rotation for customer-created CMKs is activated		2.8	KMS.1	3.8	KMS.4

ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for unauthorized API calls		3.1		4.1	CloudWatch.1
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA		3.2		4.2	CloudWatch.2
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for usage of the "root" user		3.3	CW.1	4.3	CloudWatch.3
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for IAM policy changes		3.4		4.4	CloudWatch.4

ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for CloudTrail configuration changes		3.5		4.5	CloudWatch.5
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Management Console authentication failures		3.6		4.6	CloudWatch.6
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs		3.7		4.7	CloudWatch.7

ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for S3 bucket policy changes		3.8		4.8	CloudWatch.8
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Config configuration changes		3.9		4.9	CloudWatch.9
Ensure a log metric filter and alarm exist for AWS Config configuration changes					
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for security group changes		3.10		4.10	CloudWatch.10

ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)		3.11		4.11	CloudWatch.11
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for changes to network gateways		3.12		4.12	CloudWatch.12
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for route table changes		3.13		4.13	CloudWatch.13
ASR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for VPC changes		3.14		4.14	CloudWatch.14

AWS-DisablePublicAccessForSecurityGroup Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		4.1	EC2.5		EC2.13
AWS-DisablePublicAccessForSecurityGroup Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389		4.2			EC2.14
ASR-ConfigureSNSTopicForStack CloudFormation stacks should be integrated with Simple Notification Service (SNS)	CloudFormation.1				CloudFormation.1
ASR-CreateIAMSupportRole Ensure a support role has been created to manage incidents with AWS Support		1.20	1,17	1,17	IAM.18

ASR-DisablePublicIPAutoAssign Amazon EC2 subnets should not automatically assign public IP addresses	EC2.15				EC2.15
ASR-EnableCloudTrailLogFileValidation CloudTrail log file validation should be enabled	CloudTrail.4	2.2	CloudTrail.4	3.2	CloudTrail.4
ASR-EnableEncryptionForSNSTopic SNS topics should be encrypted at-rest using AWS KMS	SNS.1				SNS.1
ASR-EnableDeliveryStatusLoggingForSNSTopic Logging of delivery status should be enabled for notification messages sent to a topic	SNS.2				SNS.2

ASR-EnableEncryptionForSQSQueue Amazon SQS queues should be encrypted at rest	SQS.1				SQS.1
ASR-EnableVPCFlowLogs VPC flow logging should be enabled in all VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6
ASR-MakeRDSSnapshotPrivate RDS snapshot should be private	RDS.1		RDS.1		RDS.1

Adding new remediations

Adding a new remediation to an existing playbook does not require modification to the solution itself.

Note

The instructions that follow leverage resources installed by the solution as a starting point. By convention, most solution resource names contain **SHARR** and/or **SO0111** to make it easy to locate and identify them.

Overview

Automated Security Response on AWS runbooks must follow the following standard naming:

```
ASR-<standard>-<version>-<control>
```

Standard: The abbreviation for the security standard. This must match standards supported by SHARR. It must be one of “CIS”, “AFSBP”, “PCI”, or "SC".

Version: The version of the standard. Again, this must match the version supported by SHARR and the version in the finding data.

Control: The control ID of the control to be remediated. This must match the finding data.

1. Create a runbook in the member account(s).
2. Create an IAM role in the member account(s).
3. (Optional) Create an automatic remediation rule in the admin account.

Step 1. Create a runbook in the member account(s)

1. Sign in to the AWS Systems Manager console and obtain an example of the finding JSON.
2. Create an automation runbook that remediates the finding. In the **Owned by me** tab, use any of the `ASR-` documents under the **Documents** tab as a starting point.
3. The AWS Step Functions in the admin account will run your runbook. Your runbook must specify the remediation role in order to be passed when calling the runbook.

Step 2. Create an IAM role in the member account(s)

1. Sign in to the AWS Identity and Access Management console.
2. Obtain an example from the IAM **SO0111** roles and create a new role. The role name must start with `SO0111-Remediate-<standard>-<version>-<control>`. For example, if adding CIS v1.2.0 control 5.6 the role must be `SO0111-Remediate-CIS-1.2.0-5.6`.
3. Using the example, create a properly scoped role that allows only the necessary API calls to perform remediation.

At this point, your remediation is active and available for automated remediation from the SHARR Custom Action in AWS Security Hub.

Step 3: (Optional) Create an automatic remediation rule in the admin account

Automatic (not "automated") remediation is the immediate execution of the remediation as soon as the finding is received by AWS Security Hub. Carefully consider the risks before using this option.

1. View an example rule for the same security standard in CloudWatch Events. The naming standard for rules is `standard_control_`**`AutoTrigger`**.
2. Copy the event pattern from the example to be used.
3. Change the `GeneratorId` value to match the `GeneratorId` in your Finding JSON.
4. Save and activate the rule.

Adding a new playbook

Download the Automated Security Response on AWS solution playbooks and deployment source code from the GitHub repository.

The AWS CloudFormation resources are created from AWS CDK components, and the resources contain the playbook template code that you can use to create and configure new playbooks. For more information about setting up your project and customizing your playbooks, refer to the README.md file in GitHub.

AWS Systems Manager Parameter Store

Automated Security Response on AWS uses AWS Systems Manager Parameter Store for storage of operational data. The following parameters are stored in Parameter Store:

Name	Value	Use
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS key that will encrypt data for FSBP remediations	Encryption of customer data, such as CloudTrail logs, as part of remediations
`/Solutions/SO0111/CMK_ARN`	AWS KMS key that SHARR will use to encrypt data	Encryption of solution data

Name	Value	Use
/Solutions/SO0111/SNS_Topic_ARN	ARN of the Amazon SNS topic for the solution	Notification of remediation events
/Solutions/SO0111/SNS_Topic_Config.1	SNS topic for AWS Config updates	Config.1 remediation
/Solutions/SO0111/sendAnonymousMetrics	Yes	Anonymized metrics collection
/Solutions/SO0111/version	Solution version	
/Solutions/SO0111/ *<security standard long name>*/*<version>* / status	enabled	Indicates whether the standard is active in the solution. A standard can be disabled for automated remediation by changing this to disabled
/Solutions/SO0111/ *<security standard long name>*/shortname	String	Short name for the security standard. For example: 'CIS', 'AFSBP', 'PCI'
/Solutions/SO0111/ *<security standard long name>*/*<version>* /*<control>* /remap	String	When one control uses the same remediation as another, these parameters accomplish the remap

Amazon SNS topic

Automated Security Response on AWS creates an Amazon SNS topic, SO0111-SHARR_Topic. This topic is used to post updates about remediation progress. Following are the three possible notifications sent to this topic.

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in account <account_ID>
```

This is the completion message. It indicates that the remediation completed without error; however, the definitive test for successful remediation is the AWS Config check and/or manual validation.

Reference

This section includes information about an optional feature for collecting unique metrics for this solution, pointers to related resources, and a list of builders who contributed to this solution.

Anonymized data collection

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When enabled, the following information is collected and sent to AWS:

- **Solution ID** - The AWS solution identifier
- **Unique ID (UUID)** - Randomly generated, unique identifier for each AWS Security Hub Response and Remediation deployment
- **Timestamp** - Data collection timestamp
- **Instance Data** - Information about this stack deployment
- **Status** - Deployment status (passed or failed solution) or (passed or failed remediation)
- **Error message** - The generic error message in the status field
- **Generator_id** - Security Hub rule information
- **Type** - Remediation type and name
- **productArn** - The Region where Security Hub is deployed
- **finding_triggered_by** - The type of remediation performed (custom action or automated trigger)

AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

1. Download the AWS CloudFormation template to your local hard drive.
2. Open the AWS CloudFormation template with a text editor.
3. Modify the AWS CloudFormation template mapping section from:

```
Mappings:
  Solution:
    Data:
      SendAnonymousUsageData: 'Yes'
```

to:

```
Mappings:
  Solution:
    Data:
      SendAnonymousUsageData: 'No'
```

4. Sign in to the AWS CloudFormation console.
5. Select **Create stack**.
6. On the **Create stack** page, **Specify template section**, select **Upload a template file**.
7. Under **Upload a template file**, choose **Choose file** and select the edited template from your local drive.
8. Choose **Next** and follow the steps in Launch the stack in the Automated Deployment section of this guide.

Related resources

- Automated Response and Remediation with AWS Security Hub
- CIS Amazon Web Services Foundations benchmarks, version 1.2.0
- AWS Foundational Security Best Practices standard
- Payment Card Industry Data Security Standard (PCI DSS)

Contributors

The following individuals contributed to this document:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar

- Max Granat
- Tim Mekari

Revisions

Date	Change
August 2020	Initial release
October 2020	Added additional troubleshooting information to Appendix C.
November 2020	Added deployment instructions for China regions; updated solution deployment instructions for the Security Hub admin account; for more information, refer to the CHANGELOG.md file in the GitHub repository.
April 2021	Release v1.2.0: Added new playbook architect ure and new FSBP remediations. For more information, refer to the CHANGELOG.md file in the GitHub repository.
May 2021	Release v1.2.1: Bugfix for an issue affecting EC2.2 and EC2.7. For more information, refer to the CHANGELOG.md file in the GitHub repository.
August 2021	Release v1.3.0: Added PCI DSS v3.2.1 Playbook. Added 17 new remediations to CIS v1.2.0. Added four new remediations to FSBP. Converted CIS to use new playbook architecture based on SSM runbooks. Added instructions to extend existing Playbooks with customer-defined remediations. For more information, refer to the CHANGELOG.md file in the GitHub repository.
September 2021	Release v1.3.1: `CreateLogMetricFilterAndAlarm.py` changed to make

Date	Change
	Actions active, add SNS notification to `SO0111-SHARR-LocalAlarmNotification` . Changed CIS 2.8 remediation to match new finding data format. For more information, refer to the CHANGELOG.md file in the GitHub repository.
November 2021	Release v1.3.2: Bug fixes for CIS v1.2.0 controls 3.1 - 3.14. For more information, refer to the CHANGELOG.md file in the GitHub repository.
December 2021	Release v1.4.0: The solution can now be deployed using StackSets. Cross-Region remediation is now supported in addition to cross-account. Member account IAM roles are now retained when the stack is removed. For more information, refer to the CHANGELOG.md file in the GitHub repository.
January 2022	Release v1.4.1: Bug fixes. For more information, refer to the CHANGELOG.md file in the GitHub repository.
January 2022	Release v1.4.2: Bug fixes. For more information, refer to the CHANGELOG.md file in the GitHub repository.
June 2022	Release v1.5.0: Additional remediations. For more information, refer to the CHANGELOG.md file in the GitHub repository.

Date	Change
December 2022	Release 1.5.1 Changes to switch SSM document creation from Custom Resource Lambda to `CfnDocument` . Prefix for the SSM document names are updated to start with ASR instead of SHARR. For more information, refer to the CHANGELOG.md file in the GitHub repository.
March 2023	Release 2.0.0: Added support for security controls and CIS v1.4.0 standards, five new remediations to FSBP standards, one new remediation to CIS v1.2.0 standards, the service catalog AppRegistry integration, and additional protections to avoid deployment failure due to SSM document throttling. For more information, refer to the CHANGELOG .md file in the GitHub repository.
April 2023	Release 2.0.1: Mitigated impact caused by new default settings for S3 Object Ownership (ACLs disabled) for all new S3 buckets. For more information, refer to the CHANGELOG .md file in the GitHub repository.
May 2023	Updated Well-Architected definitions, added guidance on where to deploy each stack, additional Troubleshooting edition of issues with specific remediation, and updated code examples in SNS notification.
July 2023	Updated the architecture diagram and the solution components in the workflow.

Date	Change
October 2023	Release 2.0.2: Updated package versions to resolve security vulnerabilities. For more information, refer to the CHANGELOG.md file in the GitHub repository.
November 2023	Documentation update: Added Confirm cost tags associated with the solution to the Monitoring the solution with AWS Service Catalog AppRegistry section.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.