



Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 01/11/2023

Contacto: tomas.villaseca.c@gmail.com

AWS Solution: Automated Security Response on AWS

Referencia: https://aws.amazon.com/solutions/implementations/automated-security-response-on-aws/?nc1=h_ls



Resumen:

La solución de Respuesta Automática de Seguridad en AWS le ayuda a reaccionar rápidamente ante los problemas de seguridad proporcionando respuestas predefinidas y acciones correctivas basadas en los estándares de conformidad y las prácticas recomendadas del sector.

Esta solución es un complemento que funciona con AWS Security Hub para proporcionar una arquitectura lista para su implementación y una biblioteca de playbooks automatizados. Esta solución facilita a los clientes de AWS Security Hub la resolución de problemas de seguridad comunes y la mejora de su postura de seguridad en AWS.

Puede seleccionar Playbooks específicos para implementar en su cuenta principal de Security Hub.

Las remediaciones funcionan desde el menú Acciones de AWS Security Hub y permiten a los usuarios autorizados remediar un Finding en todas sus cuentas administradas por AWS Security Hub con una sola acción.

La remediación está pensada para situaciones emergentes que requieren una acción inmediata.

Esta solución realiza cambios para remediar Findings solo cuando:

1. Se inicia el cambio a través de la consola AWS Security Hub Management
2. Se ha habilitado la remediación automática mediante las Rules de EventBridge para un control específico.

Para revertir estos cambios, debe devolver manualmente los recursos a su estado original.

Beneficios:

Esta solución ofrece los siguientes beneficios:

Remediar automáticamente los Findings para controles específicos

- Activar las reglas de Amazon EventBridge para que los controles corrijan automáticamente las incidencias de ese control inmediatamente después de que aparezcan en AWS Security Hub.

Administrar remediaciones en varias cuentas y regiones desde una ubicación

- Desde una cuenta de administrador de AWS Security Hub que esté configurada como destino de agregación para las cuentas y regiones de su AWS Organizations, iniciar una remediación para un Finding en cualquier cuenta y región en la que esté implementada la solución.

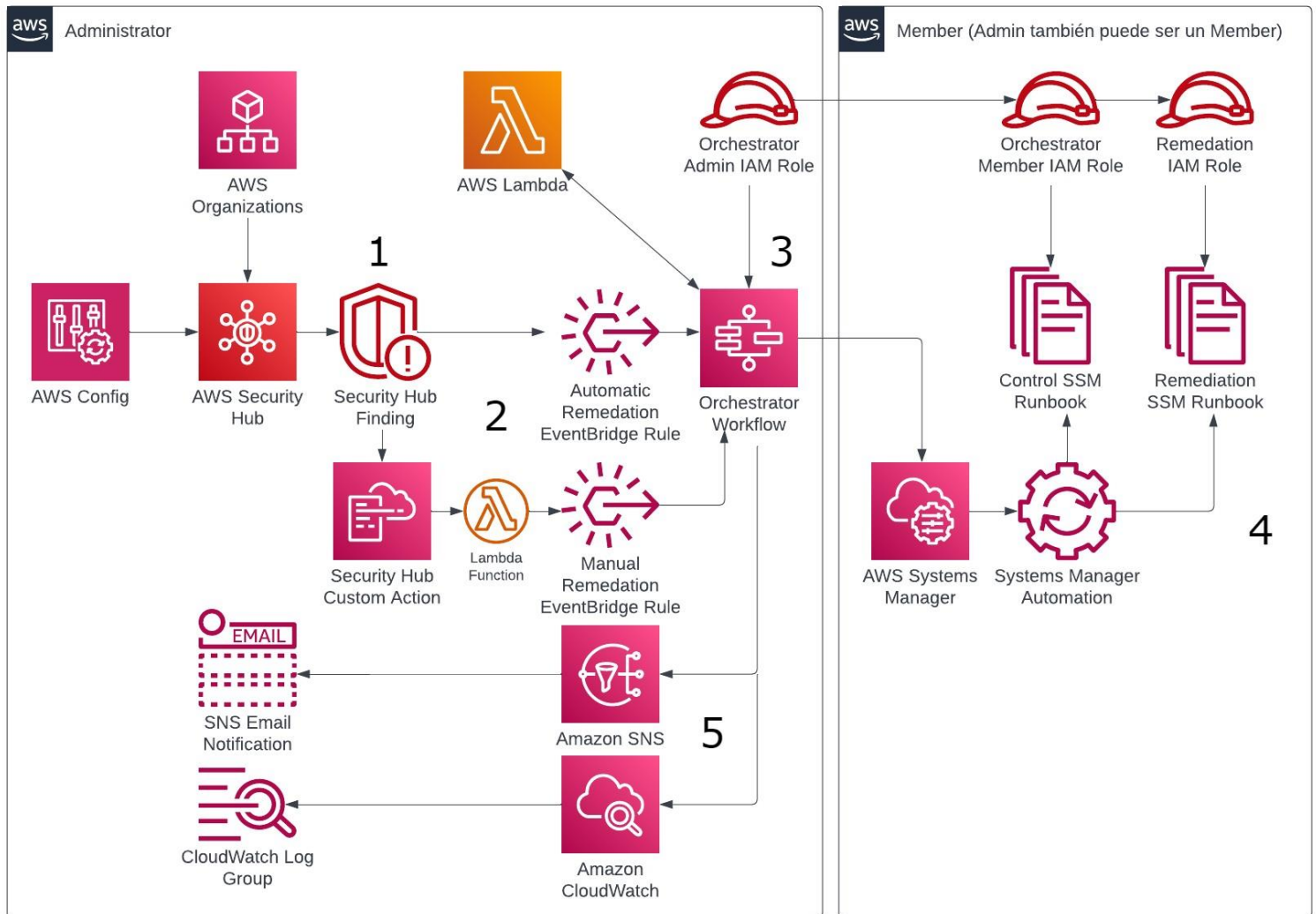
Reciba notificaciones de las acciones de remediación y los resultados

- Suscríbase al SNS topic implementado para la solución para recibir notificaciones cuando se inicien remediaciones y sobre si la remediación se ha realizado correctamente o no.

Ampliar la solución con remediaciones personalizadas e implementaciones de Playbooks

- La solución está diseñada para ser extensible y personalizable.
- Para especificar una implementación de remediación alternativa se debe implementar documentos de automatización en AWS Systems Manager y roles de IAM personalizados.
- Para admitir un nuevo conjunto completo de controles se debe implementar un Playbook personalizado.

Arquitectura de la solución:



1. Detectar:

- AWS Security Hub proporciona una visión completa del estado de seguridad de AWS.
- Ayuda a comparar su entorno con los estándares y las prácticas recomendadas del sector de seguridad.
- Funciona mediante la recopilación de eventos y datos de otros servicios (AWS Config, Amazon GuardDuty, AWS Firewall Manager, etc.)
- Eventos y datos son analizados con respecto a los estándares de seguridad (CIS AWS Foundations Benchmark, etc.)
- Las excepciones se asignan como **Findings** en la consola de AWS Security Hub.

2. Iniciar:

- Se pueden iniciar eventos contra **Findings** mediante Custom Actions que dan lugar a eventos de Amazon EventBridge.
- Las Custom Actions de AWS Security Hub y las Rules de Amazon EventBridge inician la respuesta de seguridad automatizada en los Playbooks para abordar los **Findings**.
- Se implementa una Rule de EventBridge para que coincida con el evento de acción personalizada.
- Se implementa una regla de evento de Amazon EventBridge para cada control compatible (desactivado de forma predeterminada) para que coincida con el evento en tiempo real.
- Se puede utilizar el menú de acciones personalizadas de Security Hub para iniciar la remediación automatizada, o se pueden activar las remediaciones automáticas.
- La remediación automática se puede activar para cada remediación, no es necesario activarlo en todas las remediaciones.

3. Orquestrar:

- Utilización de roles IAM entre cuentas.
- AWS Step Functions (en la cuenta del administrador) invoca la remediación en la cuenta del miembro que contiene el recurso que produjo el **Finding** de seguridad.

4. Remediar:

- Un documento de automatización de AWS Systems Manager (SSM Runbook) en la cuenta del miembro realiza la acción necesaria para remediar el **Finding** en el recurso objetivo.

5. Registrar (Log):

- El Playbook registra los resultados en un Amazon CloudWatch Logs Group.
- Se envía una notificación a un SNS Topic.
- Se actualiza el **Finding** de AWS Security Hub.
- El estado de flujo de trabajo del **Finding** cambia de **NEW** a **NOTIFIED** o **RESOLVED** en el Dashboard de AWS Security Hub.
- En las **Finding Notes** de AWS Security Hub se mantiene un rastro de auditoría de las acciones realizadas.
- Las **Finding Notes** de AWS Security Hub se actualizan para reflejar la remediación realizada.

Detalles de la Arquitectura:

En esta sección se describen los componentes y los servicios de AWS que conforman esta solución, así como los detalles de arquitectura sobre el funcionamiento conjunto de estos componentes.

Integración de AWS Security Hub:

1. Implementación del stack **aws-sharr-deploy** crea una integración con la función de Custom Action de AWS Security Hub.
 - Cuando los usuarios de la consola de AWS Security Hub seleccionan **Findings for remediation**, la solución enruta los registros de los **Findings** para remediar usando AWS Step Functions.
2. Los permisos entre cuentas y los documentos de automatización de AWS Systems Managers deben implementarse en todas las cuentas de AWS Security Hub (tanto administrador como miembros) usando el stack **aws-sharr-member.template** y **aws-sharr-member-roles**.
3. Los usuarios pueden iniciar automáticamente remediaciones automatizadas en función de cada remediación mediante reglas de eventos de Amazon CloudWatch.
 - Esta opción activa la remediación totalmente automática de las incidencias en cuanto se comunican a AWS Security Hub.
 - Por defecto, las iniciaciones automáticas están desactivadas.
 - Esta opción se puede cambiar en cualquier momento durante o después de la instalación del Playbook activando las reglas de eventos de Amazon CloudWatch en la cuenta de administrador de AWS Security Hub.

Remediación Entre cuentas:

Esta solución utiliza roles IAM entre cuentas para trabajar en cuentas principales y secundarias.

- Roles IAM son implementados en la cuenta de cada miembro durante la instalación de la solución.
- A cada remediación se le asigna un rol IAM individual.
- El proceso de remediación en la cuenta principal (administrador) recibe permisos para asumir el rol IAM de remediación en la cuenta que requiere la remediación (cuenta secundaria).
- La remediación la realizan los documentos de automatización de AWS Systems Manager (SSM Runbooks) que se ejecutan en la cuenta que requiere la remediación (cuenta secundaria).

Playbooks:

Un conjunto de remediaciones se agrupa en un paquete denominado playbook.

Los playbooks se instalan, actualizan y eliminan mediante AWS Service Catalog.

Esta solución incluye los siguientes Playbooks:

- Center for Internet Security (CIS) AWS Foundation Benchmark v1.2.0
- Center for Internet Security (CIS) AWS Foundation Benchmark v1.4.0
- AWS Foundational Security Best Practices (AFSBP) v1.0.0
- Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1
- SC 2.0.0 → Security Control Playbook alineado con la función de Consolidated Control Findings de AWS Security Hub.

Logging Centralizado:

Esta solución registra en un único CloudWatch Logs Group → SO0111-SHARR

- Logs → Contienen información de registro detallada de la solución para troubleshooting y la gestión de soluciones.

Notificaciones:

Esta solución utiliza un SNS Topic para publicar los resultados de la remediación.

- Puede utilizar las suscripciones a este SNS topic para extender las capacidades de solución.
- Ejemplo: Puede enviar notificaciones por correo y actualizar tickets de problemas.

Servicios de AWS en esta solución:

1. **AWS Lambda** → Despliega múltiples funciones lambda que serán utilizadas por AWS Step Functions para solucionar problemas.
2. **AWS Step Functions** → Implementa un orquestador que invocará los documentos de remediación con API calls de AWS Systems Manager.
3. **AWS Systems Manager** → Despliega los documentos de automatización (runbooks) que contienen la lógica de remediación que se ejecutará.
4. **AWS IAM** → Despliega roles IAM para permitir remediaciones en diferentes recursos.
5. **AWS Security Hub** → Proporciona una visión completa de su estado de seguridad en AWS.
6. **Amazon EventBridge** → Despliega eventos que activarán el orquestador de AWS Step Functions cuando se esté remediando un **Finding**.
7. **Amazon SNS** → Despliega SNS topics que reciben una notificación una vez se ha completado una remediación.
8. **Amazon CloudWatch** → Despliega Log Groups que los diferentes Playbooks utilizarán para registrar los resultados.

Costos de la solución:

El costo total de esta solución depende de los siguientes factores:

- El número de cuentas de miembros de AWS Security Hub.
- El número de remediaciones activas invocadas automáticamente.
- La frecuencia de la remediación.

El costo de ejecución esta solución con la configuración predeterminada en la región de AWS de EE.UU. Este (Virginia del Norte) se resume en la siguiente tabla con montos aproximados:

Número de remediaciones por mes	Costo (usd)
300	3.33
3000	26.83
30.000	261.90

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
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 notifications = \$0.50	\$0.50
Total		\$261.90

Implementar la solución:

Esta solución utiliza templates y stacks de AWS CloudFormation para automatizar su implementación.

- Los templates de CloudFormation especifican los recursos de AWS incluidos en esta solución y sus propiedades.
- El stack de CloudFormation aprovisiona los recursos que se describen en los templates.

Para que la solución funcione, se deben implementar tres templates:

1. **Admin Stack** → aws-sharr-deploy.template (Componentes core de la solución)
2. **Member Stack** → aws-sharr-member.template (documentos de automatización de AWS Systems Manager).
3. **Member roles stack** → aws-sharr-member-roles.template (Roles IAM para remediaciones)

Antes de implementar la solución se debe:

1. Decidir donde desplegar cada template:

- Admin Stack debe ser implementarse solamente una vez, en una sola cuenta (administrador de AWS Security Hub) y en una sola región.
- Admin Stack debe completar su implementación antes de desplegar los otros templates para que pueda crearse una relación de confianza entre la cuenta miembro y la cuenta central.
- Member Stack debe ser implementada en todas las cuentas y regiones en donde se quiera remediar Findings (esto puede incluir la cuenta del administrador).
- Member Roles Stack debe ser implementado en todas las cuentas (contiene recursos globales, por lo que no importa la región en donde sea implementado).

2. Decidir cómo desplegar cada template:

Hay 3 opciones para implementar los stacks de CloudFormation:

- CloudFormation StackSet (Self-managed permissions) → Se sugiere para Member Stack
- CloudFormation StackSet (Service-managed permissions) → Se sugiere para Member Roles Stack
- CloudFormation Stack → Se sugiere para Admin Stack

Prerrequisito para implementar la solución:

- Habilitar AWS Config
- Habilitar AWS Security Hub
- Habilitar AWS Organizations en la cuenta del administrador de AWS Security Hub.

Tarea 1: Habilitar AWS Config

AWS Config debe estar habilitado tanto en la cuenta del administrador como en la cuenta de los miembros en los que se desea tener la solución.

AWS Security Hub utiliza reglas de AWS Config para realizar la mayoría de sus comprobaciones de seguridad para los controles.

Paso 1: AWS Config → Set up AWS Config → Settings → General Settings

- Recording Strategy → Record all current and future resource types supported in this region.

Recording strategy

☒ Record all current and future resource types supported in this region

☐ Record all current and future resource types with exclusions

☐ Record specific resource types

If you select this option, when AWS Config adds support for a new regionally recorded resource type, AWS Config will record resources of that type automatically. The `AWS::RDS::GlobalCluster` resource type will be recorded in all enabled regions. If you do not want to record `AWS::RDS::GlobalCluster` in all enabled regions, choose another recording strategy.

- Seleccionar la opción “Include global resources” → Permite obtener Findings asociados con recursos globales (Ej: AWS IAM).

☒ Include globally recorded resource types

This option is a legacy field which only applies to the globally recorded IAM resource types: IAM users, groups, roles, and customer managed policies. If selected, these resources will be recorded in all enabled regions where AWS Config was supported before February 2022.

- IAM role for AWS Config → Create AWS Config service-linked role

IAM role for AWS Config

☒ Create AWS Config service-linked role

☐ Choose a role from your account

Choose an IAM role from one of your pre-existing roles and permission policies.

Paso 3: Set up AWS Config → Settings → Delivery Method

- Amazon S3 bucket → Create a bucket

Paso 4: Set up AWS Config → Rules

- Seleccionar Next (Se agregarán reglas posteriormente con CloudFormation)

Paso 5: Set up AWS Config → Review

Amazon S3 bucket

☒ Create a bucket

☐ Choose a bucket from your account

☐ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#)

S3 Bucket name (required)

config-bucket-857584943305

Prefix (optional)

/AWSLogs/857584943305/Config/
us-east-1

Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

General settings

Recording strategy

Record all current and future resource types supported in this region, excluding globally recorded resource types.

IAM role for AWS Config
AWSServiceRoleForConfig

Resource types to record

► [See list of recorded resource types](#)

Delivery method

S3 bucket name
config-bucket-857584943305


► **AWS Config rules (0)**



Cancel

Previous

Confirm

Paso 6: Verificar que IAM role y S3 bucket para AWS Config fueron creados correctamente.

	Name	AWS Region
	config-bucket-857584943305	US East (N. Virginia) us-east-1

	Role name
	AWSServiceRoleForConfig

Tarea 2: Habilitar AWS Security Hub

AWS Security Hub debe estar habilitado tanto en la cuenta del administrador como en la cuenta de los miembros en los que se desea tener la solución.

- Los miembros deben designar una cuenta de administrador de AWS Security Hub.

Paso 1: AWS Security Hub → Enable AWS Security Hub

- Security standards → Seleccionar todas las casillas.
- Enable Security Hub

Security standards

Enabling AWS Security Hub grants it permissions to conduct security checks. [Service Linked Roles \(SLRs\)](#) with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.

- ☒ Enable AWS Foundational Security Best Practices v1.0.0
- ☒ Enable CIS AWS Foundations Benchmark v1.2.0
- ☒ Enable CIS AWS Foundations Benchmark v1.4.0
- ☒ Enable NIST Special Publication 800-53 Revision 5
- ☒ Enable PCI DSS v3.2.1

Paso 2: AWS Security Hub → Settings → General → Controls

- Habilitar “Consolidated control findings”.

Controls

- ☒ Auto-enable new controls in enabled standards
- ☒ Consolidated control findings - *New*
Generates a single control finding per security check, even when a control is shared across multiple standards.

Paso 3: AWS Security Hub → Settings → Regions → Finding aggregation

- Seleccionar región principal del administrador de AWS Security Hub como “Aggregation Region”
- Vincular todas las regiones deseadas a la Aggregation Region definida.

Finding aggregation

View findings across multiple Regions by setting an aggregation Region and then linking other Regions to it. [Learn more](#) 

Aggregation Region

US East (N. Virginia) - us-east-1

Linked Regions (27)

Paso 4: AWS Organizations → Create an organization

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Q Search by name, email, account ID or OU ID.

Hierarchy

List

Organizational structure

Account created/joined date

▼

Root

r-2jh6

TomasVC93

management account

Joined 2023/10/16

857584943305

|

tomas.villaseca.c@gmail.com

Paso 5: AWS Organizations → Services → Integrated Services

- Habilitar Security Hub → Permite al administrador agregar miembros de la organización como miembros de SecurityHub

Security Hub

AWS Security Hub provides you with a comprehensive view of the security state of your AWS resources. Security Hub collects security data from across AWS accounts and services, and helps you analyze your security trends to identify and prioritize the security issues across your AWS environment.

Access enabled

Paso 6: AWS Security Hub → Settings → General → Delegated Administrator

- Designar desde la cuenta que administra AWS Organizacions la cuenta de administrador de AWS Security Hub.
- Ingresar account ID de la cuenta del administrador
- La cuenta de administrador de Security Hub tiene acceso a todas las cuentas de la organización y determina que cuentas de la organización habilitar como cuentas miembros de Security Hub.

Delegated Administrator

Info

Delegate permission to manage Security Hub for this organization.

Account ID

857584943305

Organization ID

o-qg014y4ffyy

i

You have authorized an account to supervise Security Hub in your organization on your behalf. You can revoke or change this designation at any time.

Paso 7: AWS Security Hub → Settings → Custom Actions

- Remediate with ASR → Se encontrará disponible una vez sea implementado el Member Stack.

Action name	Description
<div><div></div>Remediate with ASR</div>	Submit the finding to AWS Security Hub Automated Response and Remediation

Tarea 3: Crear los roles IAM para permisos de Self-Managed StackSets

AWS CloudFormation StackSets extiende la capacidad de los stacks habilitando la creación, actualización, o eliminación de stacks en varias cuentas y regiones de AWS con una sola operación.

- Mediante una cuenta de administrador puede definir y administrar templates de CloudFormation y utilizar el template como base para aprovisionar stacks en cuentas destino seleccionadas en regiones especificadas.
- Self-Managed StackSets solo es necesario para implementar el Member Stack a las cuentas.
- Tanto la cuenta del administrador como la cuenta miembro objetivo deben contar con el rol IAM necesario para permitir el aprovisionamiento mediante self-managed StackSets.
- Los dos roles IAM necesarios se pueden implementar con templates de CloudFormation.

Tarea 3.1 – Implementar AWSCloudFormationStackSetAdministration

Paso 1: CloudFormation → Stacks → Create Stack → With new resources (standard)

- Prepare template → Template ready

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

- Specify template → Upload a template file
- Choose file → AWSCloudFormationStackSetAdministrationRole.yml

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.


Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

AWSCloudFormationStackSetAdministrationRole.yml

JSON or YAML formatted file

Paso 2: Create Stack → Specify stack details

- Stack name = AWSCloudFormationStackSetAdministrationRole

Stack name

AWSCloudFormationStackSetAdministrationRole


Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Paso 3: Create Stack → Configure stack options → Default

Paso 4: Create Stack → Review → Capabilities

- Seleccionar todas las casillas

Capabilities



The following resource(s) require capabilities: [AWS::IAM::Role]


This template contains Identity and Access Management (IAM) resources. Check that you want to create
Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Paso 5: Create Stack → Submit


- Esperar que el stack sea completado.

Stacks




AWSCloudFormationStackSetAdministrationRole

2023-11-03 00:17:31 UTC-0300


 CREATE_IN_PROGRESS

Stacks



AWSCloudFormationStackSetAdministrationRole

2023-11-03 00:17:31 UTC-0300

 CREATE_COMPLETE

Paso 6: AWS IAM → Roles → Buscar → AWSCloudFormationStackSetAdministrationRole

<input checked="" type="checkbox"/>	Role name	Trusted entities
<input checked="" type="checkbox"/>	AWSCloudFormationStackSetAdministrationRole	AWS Service: cloudformation

Tarea 3.2 – Implementar `AWSCloudFormationStackSetExecutionRole`

Paso 1: CloudFormation → Stacks → Create Stack → With new resources (standard)

- Prepare template → Template ready

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

- Specify template → Upload a template file
- Choose file → `AWSCloudFormationStackSetExecutionRole.yml`

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.


Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

`AWSCloudFormationStackSetExecutionRole.yml`

JSON or YAML formatted file

Paso 2: Create Stack → Specify stack details

- Stack name = `AWSCloudFormationStackSetExecutionRole`

Stack name

`AWSCloudFormationStackSetExecutionRole`

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

- Parameters → `AdministratorAccountId = 857584943305`

Parameters

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

AdministratorAccountId

AWS Account Id of the administrator account (the account in which StackSets will be created).


`857584943305`

Paso 3: Create Stack → Configure stack options → Default

Paso 4: Create Stack → Review → Capabilities

- Seleccionar todas las casillas

Capabilities





The following resource(s) require capabilities: [AWS::IAM::Role]



This template contains Identity and Access Management (IAM) resources. Check that you want to create IAM resources. Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Paso 5: Create Stack → Submit

- Esperar que el stack sea completado.

Stacks	
	<div><div>AWSCloudFormationStackSetExecutionRole</div><div>2023-11-03 00:26:47 UTC-0300</div><div> CREATE_IN_PROGRESS</div></div>

Stacks	
	<div><div>AWSCloudFormationStackSetExecutionRole</div><div>2023-11-03 00:26:47 UTC-0300</div><div> CREATE_COMPLETE</div></div>

Paso 6: AWS IAM → Roles → Buscar → AWSCloudFormationStackSetExecutionRole

<input checked="" type="checkbox"/>	Role name	Trusted entities
<input checked="" type="checkbox"/>	AWSCloudFormationStackSetExecutionRole	Account: 857584943305

Tarea 4: Implementar Stacks de la solución

Tarea 4.1 – Implementar Admin Stack

Paso 1: CloudFormation → Stacks → Create Stack → With new resources (standard)

- Prepare template → Template ready

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

- Specify template → Upload a template file
- Choose file → aws-sharr-deploy.template

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.


Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

aws-sharr-deploy.template

JSON or YAML formatted file

Paso 2: Create Stack → Specify stack details

- Stack name = AWSCloudFormationStackSetExecutionRole

Stack name

AdminStack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

- Parameters → Security Standard Playbooks → Default.

Security Standard Playbooks

LoadAFSBPAdminStack

Load CloudWatch Event Rules for AFSBP?

yes

LoadCIS120AdminStack

Load CloudWatch Event Rules for CIS120?

yes

LoadCIS140AdminStack

Load CloudWatch Event Rules for CIS140?

yes

LoadPCI321AdminStack

Load CloudWatch Event Rules for PCI321?

yes

LoadSCAdminStack

Load CloudWatch Event Rules for SC?

yes

ReuseOrchestratorLogGroup

Reuse existing Orchestrator Log Group? Choose "yes" if the log group already exists, else "no"

no

Paso 3: Create Stack → Configure stack options → Default

Paso 4: Create Stack → Review → Capabilities

- Seleccionar todas las casillas

Capabilities



The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the documentation for more information.

- ☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.
- ☒ I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND

Paso 5: Create Stack → Submit

- Esperar que el stack sea completado.

AdminStack



2023-11-02 00:50:36 UTC-0300

CREATE_COMPLETE

Tarea 4.2 – Implementar Member Stack

Paso 1: CloudFormation → StackSets → Create StackSet → Choose a template

- Permissions → Self-service permissions

☒ Self-service permissions

You create the IAM roles required to deploy to target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials.


- IAM Admin role → AWSCloudFormationStackSetAdministratorRole
- IAM execution role name → AWSCloudFormationStackSetExecutionRole

IAM admin role ARN - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name ▼

AWSCloudFormationStackSetAdministrationRole

 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.

- Prepare template → Template ready

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

- Specify Template → Upload template file
- Choose file → aws-sharr-member.template

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

aws-sharr-member.template

JSON or YAML formatted file

Paso 2: Create StackSet → Specify StackSet details

- StackSet name = MemberStack

StackSet name

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

- Parameters → LogGroup Configuration = SO0111-SHARR-Orchestrator

LogGroup Configuration

Provide the name of the LogGroup to be used to create Metric Filters and Alarms

Name of the log group to be used to create metric filters and cloudwatch alarms. You must use a Log Group that is the logging destination of a multi-region CloudTrail

- Parameters → Playbooks → Default
- Parameters → Playbooks → SecHubAdminAccount = 857584943305

Playbooks

LoadAFSBPMemberStack

Load Playbook member stack for AFSBP?

SecHubAdminAccount

Admin account number

LoadCIS120MemberStack

Load Playbook member stack for CIS120?

LoadCIS140MemberStack

Load Playbook member stack for CIS140?

LoadPCI321MemberStack

Load Playbook member stack for PCI321?

LoadSCMemberStack

Load Playbook member stack for SC?

CreateS3BucketForRedshiftAuditLogging

Create S3 Bucket For Redshift Cluster Audit Logging.

Paso 3: Create StackSet → Configure StackSet options → Default

Paso 4: Create StackSet → Set deployment options

- Add stacks to stack set → Deploy new stacks

☒ Deploy new stacks

☐ Import stacks to stack set

- Accounts → Deployment locations → Deploy stacks in accounts
- Account numbers → Escribir los Account ID de las cuentas objetivo del stack en formato csv.

Deployment locations

StackSets can be deployed into accounts or all accounts in an organizational unit.

☒ Deploy stacks in accounts

☐ Deploy stack to all accounts in an organizational unit

Account numbers


Enter account numbers or populate from a file.

857584943305

12-digit account numbers separated by commas.

- Specify regions → Agregar regiones objetivo en donde se aplicará el stack.

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the stack set and stack set instances involved. [Learn more](#) 

US East (N. Virginia)
us-east-1



- Deployment options → Default

Deployment options

Maximum concurrent accounts - optional

Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation

Number



1

Failure tolerance - optional

Number of accounts, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation fails in more than the specified number of accounts, the operation is stopped.

Number



0

Region concurrency

Choose to deploy StackSets into regions sequentially or in parallel.

☒ Sequential


Deploy StackSets operations into one region at a time, specified by the region deployment order.

☐ Parallel

Deploy StackSets operations into all specified regions in parallel.

Paso 5: Create StackSet → Review → Capabilities → Seleccionar todas las Casillas

Capabilities



The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the following capabilities:


☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

☒ I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND


Paso 6: Create StackSet → Submit

- Esperar que el stack sea completado.

MemberStack



2023-11-02 01:33:26 UTC-0300

 CREATE_COMPLETE

Tarea 4.3 – Implementar Member Roles Stack (Admin)

Para aplicar el stack en la cuenta del administrador se debe hacer con CloudFormation Stack.

Paso 1: CloudFormation → Stacks → Create Stack → With new resources (standard)

- Prepare template → Template ready

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

- Specify template → Upload a template file
- Choose file → aws-sharr-member-roles.template

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.


Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

aws-sharr-member-roles.template

JSON or YAML formatted file

Paso 2: Create Stack → Specify stack details

- Stack name = MemberRolesStack

Stack name

MemberRolesStack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

- Parameters → SecHubAdminAccount = 857584943305

Parameters

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

SecHubAdminAccount

Admin account number

857584943305

Paso 3: Create Stack → Configure stack options → Default

Paso 4: Create Stack → Review → Capabilities

- Seleccionar todas las casillas

Capabilities



The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to c
Check that the custom names are unique within your AWS account. [Learn more](#)



I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Paso 5: Create Stack → Submit

- Esperar que el stack sea completado.

MemberRolesStack



2023-11-02 01:29:31 UTC-0300



CREATE_COMPLETE

Tarea 4.4 – Implementar Member Roles Stack (Miembros)

Para aplicar el stack en la cuenta de los miembros, lo más eficiente es usar service-managed permissions (es posible porque Member Roles Stack no es un Nested Stack).

Paso 1: CloudFormation → StackSets → Create StackSet → Choose a template

- Permissions → Service-managed permissions

- ☒ **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.

- Specify template → Upload a template file
- Choose file → aws-sharr-member-roles.template

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.


Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

 Choose file

aws-sharr-member-roles.template

JSON or YAML formatted file

Paso 2: Create StackSet → Specify StackSet details

- StackSet name = MemberRolesStack

StackSet name

MemberRolesStack

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

- Parameters → SecHubAdminAccount = 857584943305

Parameters

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

SecHubAdminAccount

Admin account number

857584943305

Paso 3: Create StackSet → Configure StackSet options → Default

Paso 4: Create StackSet → Set deployment options

- Add stack to stack set → Deploy new stack

☒ Deploy new stacks

☐ Import stacks to stack set

- Deployment targets → Deploy to organization

Deployment targets

StackSets deploys stack instances to all accounts in the target organization or organizational units (OUs). If you add a parent OU as a target, StackSets also adds any child OUs as targets.

☒ Deploy to organization

☐ Deploy to organizational units (OUs)

- Auto-deployment options → Automatic deployment → Deactivated

Auto-deployment options

Automatic deployment
With automatic deployment enabled, if an account is added to an OU, StackSets automatically deploys additional stack instances to this account.

- ☐ Activated
- ☒ Deactivated

- Specify regions → Agregar regiones objetivo en donde se aplicará el stack.

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the stack set and stack set instances involved. [Learn more](#)

US East (N. Virginia)
us-east-1

- Deployment options → Default

Deployment options

Maximum concurrent accounts - optional
Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation

Number

▼

1

Failure tolerance - optional
Number of account, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation fails in more than the specified number of accounts, CloudFormation stops the operation in that region.

Number

▼

0


Region concurrency
Choose to deploy StackSets into regions sequentially or in parallel.

☒ Sequential
Deploy StackSets operations into one region at a time, specified by the region deployment order.

☐ Parallel
Deploy StackSets operations into all specified regions in parallel.

Paso 5: Create StackSet → Review → Capabilities → Seleccionar todas las Casillas.

Capabilities


 **The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources. Check that you want to
Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Paso 6: Create StackSet → Submit

- Esperar que stack sea completado.

	StackSet name	StackSet ID	Permission model
	MemberRolesStack	MemberRolesStack:6ca24735-0438-49f9-9f9b-eee51240e1cf	SERVICE_MANAGED

Tarea 5 – Habilitar CloudTrail y crear un CloudWatch Log Group de destino

Varios controles de CloudTrail soportados por la solución requieren que haya un CloudWatch Log Group que sea el destino de un Multi-Region CloudTrail.

Crear un CloudWatch Log Group en cada cuenta y región con el mismo nombre (Ej: asr-log-group).

Paso 1: CloudTrail → Trails → Seleccionar un Trail → CloudWatch Logs → Edit

- CloudWatch Logs → Enabled
- Log group name → New = asr-log-group
- Role name → New = default

CloudWatch Logs - optional

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)

☒ Enabled

☐ New

☒ Existing

Log group name

asr-log-group

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

☐ New

☒ Existing

Role name

CloudTrailASRCloudWatchLogGroupRole

Tarea 6 – Suscribirse al SNS Topic de la solución

Paso 1: Amazon SNS → Topics → SO0111-SHARR Topic → Create subscription

- Protocol → Email
- Endpoint = tomas.villaseca.c@gmail.com

Topic ARN

Q

arn:aws:sns:us-east-1:857584943305:SO0111-SHARR_Topic

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

tomas.villaseca.c@gmail.com

Paso 2: Revisar correo → Confirm subscription



SHARR Playbook Topic (SO0111)

para mí ▾

🌐 inglés ▾ > español ▾ [Traducir mensaje](#)

You have chosen to subscribe to the topic:

arn:aws:sns:us-east-1:857584943305:SO0111-SHARR_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-1:857584943305:SO0111-SHARR_Topic:d1213a35-5e72-4d14-a45b-5a3ed32c0d2c

If it was not your intention to subscribe, [click here to unsubscribe](#).

ID	Endpoint	Status
d1213a35-5e72-4d14-a45b-5a3ed32c0d2c	tomas.villaseca.c@gmail.com	Confirmed

Tarea 7 – Probar la solución

Tarea 7.1 – Crear un recurso inseguro que generará un Finding

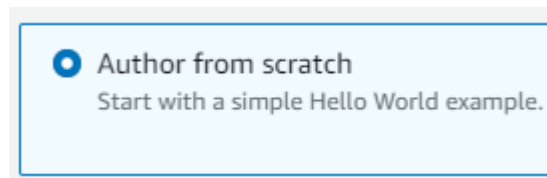
Se creará un Lambda con una configuración insegura para probar la solución.

El control de ejemplo es:

- **Lambda.1** → Las políticas de la función Lambda deben prohibir el acceso público.

Paso 1: AWS Lambda → Create function → Basic information

- Author from scratch



- Function name = InsecureLambda

Function name

Enter a name that describes the purpose of your function.

InsecureLambda

Use only letters, numbers, hyphens, or underscores with no spaces.

- Runtime → Python 3.11

Runtime [Info](#)

Choose the language to use to write your function.

Python 3.11

- Architecture → x86_64

Architecture [Info](#)

Choose the instruction set architecture you want for your function code.

☒ x86_64

☐ arm64

Paso 2: AWS Lambda → Functions → InsecureLambda → Configuration → Function URL

- Auth type → NONE

Auth type

Choose the auth type for your function URL. [Learn more](#)


☐ AWS_IAM

Only authenticated IAM users and roles can make requests to your function URL.

☒ NONE

Lambda won't perform IAM authentication on requests to your function URL. The URL endpoint will be public unless you implement your own authorization logic in your function.

Function URL permissions

-  When you choose auth type **NONE**, Lambda automatically creates the following resource-based policy and attaches it to your function. This policy makes your function public to anyone with the function URL. You can edit the policy later. To limit access to authenticated IAM users and roles, choose auth type **AWS_IAM**.

▼ View policy statement


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "StatementId": "FunctionURLAllowPublicAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "lambda:InvokeFunctionUrl",
      "Resource": "arn:aws:lambda:us-east-1:857584943305:function:InsecureLambda",
      "Condition": {
        "StringEquals": {
          "lambda:FunctionUrlAuthType": "NONE"
        }
      }
    }
  ]
}
```

Paso 3: AWS Lambda → Functions → InsecureLambda → Configuration → Permissions

Resource-based policy statements (1) [Info](#)


A resource-based policy lets you grant permissions to other AWS accounts or services on a per-resource basis.


 Find policy statements

Statement ID	Principal	
 FunctionURLAllowPublicAccess	*	-

Se verifica que se agregó la política para permitir acceso público.

Paso 4: AWS Security Hub → Findings → Buscar Finding generado

<input checked="" type="checkbox"/>	Severity ▾	Workflow status ▾	Record State ▾	Region ▾	Account Id ▾
<input checked="" type="checkbox"/>	 CRITICAL	NEW	ACTIVE	us-east-1	857584943305

Company	Product ▾	Title ▾	Resource	Compliance Status ▾
AWS	Security Hub	Lambda function policies should prohibit public access	Lambda Function InsecureLambda	 FAILED

Paso 5: Iniciar la remediación del Finding

- Actions → Remediate with ASR

Actions ▲

Workflow status ▾

Remediate with ASR

- Aparece una notificación que indica que el Finding fue enviado a Amazon EventBridge

 Successfully started action: Remediate with ASR (Description: Submit the finding to AWS Security Hub Automated Response and Remediation)

Paso 6: Confirmar la remediación resolvió el Finding.

- Se reciben dos notificaciones de SNS
- Notificación 1 → Indica que la remediación fue iniciada

SHARR Playbook Topic (SO0111)

para mí ▾

```
{
  "severity": "INFO",
  "message": "36973519-5351-4afe-a516-fb663873879f: Remediation queued for SC control Lambda.1 in account 857584943305",
  "finding": {
    "finding_id": "bec42663-7150-46f1-b3bd-7bfe6987b071",
    "finding_description": "This control checks whether the AWS Lambda function policy attached to the Lambda resource prohibits public access.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "Lambda.1",
    "title": "Lambda function policies should prohibit public access",
    "region": "us-east-1",
    "account": "857584943305",
    "finding_arn": "arn:aws:securityhub:us-east-1:857584943305:security-control/Lambda.1/finding/bec42663-7150-46f1-b3bd-7bfe6987b071"
```


- Notificación 2 → Indica que la remediación fue exitosa.

SHARR Playbook Topic (SO0111)

para mí ▼

```
{
  "severity": "INFO",
  "message": "36973519-5351-4afe-a516-fb663873879f: Remediation succeeded for SC control Lambda.1 in account 857584943305:"
```

- AWS Lambda → Functions → InsecureLambda → Configuration → Function URL

 Your function URL auth type is NONE, but is missing permissions required for public access. To allow unauthenticated requests, choose the **Permissions** tab and create a resource-based policy that grants **lambda:invokeFunctionUrl** permissions to all principals (*). Alternatively, you can update your function URL auth type to AWS_IAM to use IAM authentication.

- AWS Lambda → Functions → InsecureLambda → Configuration → Permissions

Resource-based policy statements [Info](#)

A resource-based policy lets you grant permissions to other AWS accounts or services on a per-resource basis.

Statement ID



Principal



PrincipalOrgID

No policy statements


Add permissions

Se verifica que la política para permitir acceso público fue eliminada, es decir, el Finding fue remediado.

Tarea 8 – Rastrear la ejecución de la remediación

Tarea 8.1 – EventBridge Rule

Paso 1: Amazon EventBridge → Rules → Remediate_with_SHARR_CustomAction

<input checked="" type="checkbox"/>	Name	Status	Type
<input checked="" type="checkbox"/>	Remediate_with_SHARR_CustomAction	 Enabled	Standard

- La Rule “Remediate_with_SHARR_CustomAction” se encuentra habilitada por default, lo que permite remediar los Findings a través de Security Hub (como se muestra en la Tarea 7).

Esta EventBridge Rule coincide con el Finding enviado desde Security Hub y la envía al Orquestrator Step Function SO0111-SHARR-Orchestrator.

Targets

Details	Target Name	Type
▼	SO0111-SHARR-Orchestrator 🔗	Step Functions state machine

Input to target: Matched event

Event pattern [Info](#)

```
1 {
2   "detail-type": ["Security Hub Findings - Custom Action"],
3   "resources": ["arn:aws:securityhub:us-east-1:857584943305:action/custom/ASRRemediation"],
4   "source": ["aws.securityhub"],
5   "detail": {
6     "findings": {
7       "Compliance": {
8         "Status": ["FAILED", "WARNING"]
9       }
10    }
11  }
12 }
```

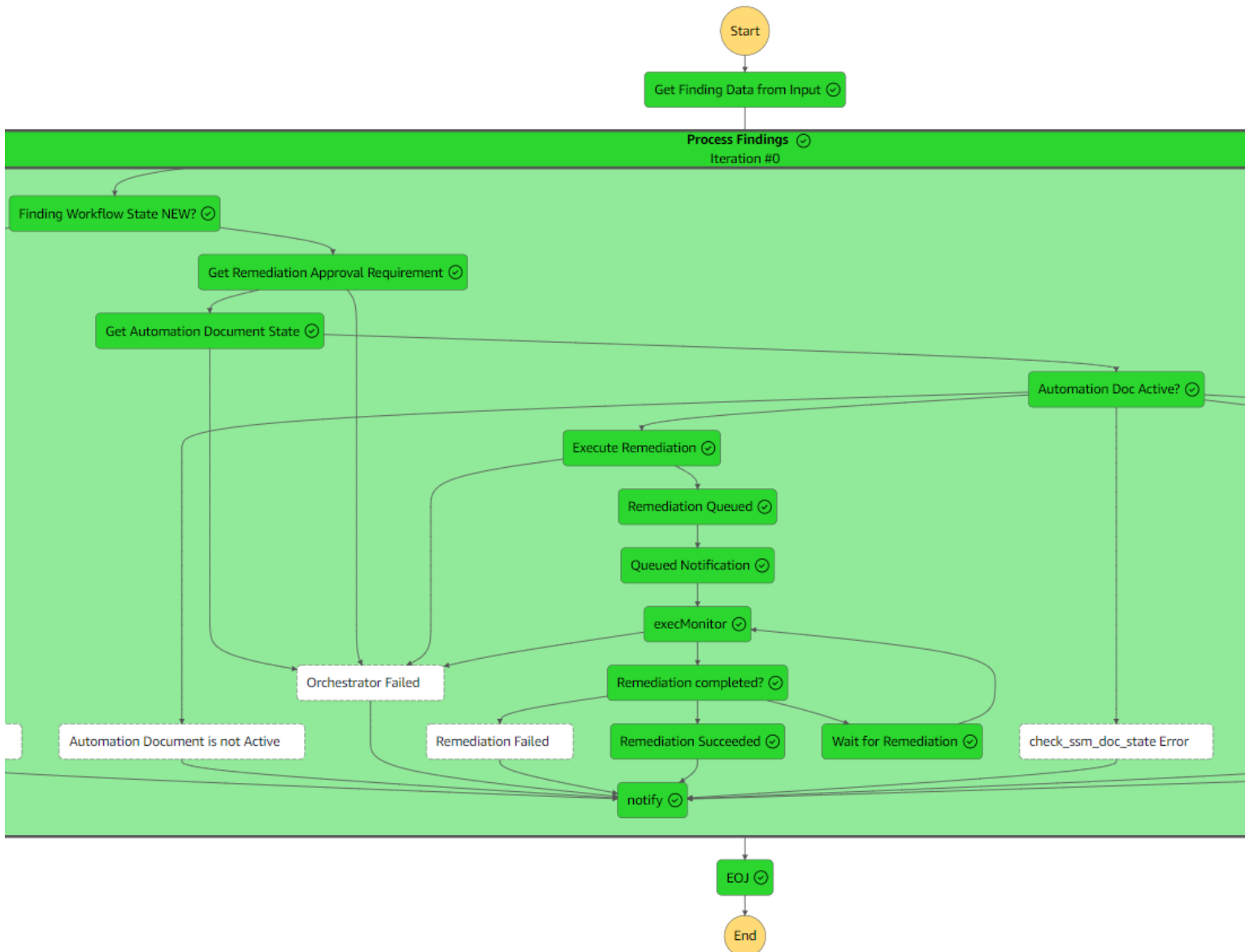
Tarea 8.2 – Ejecución de Step Function

Paso 1: AWS Step Function → State machines → SO0111-SHARR-Orchestrator

Name
SO0111-SHARR-Orchestrator

- El orquestrador de Step Function llama al documento de automatización de AWS Systems Manager (SSM) en la cuenta y región de destino.
- SO0111-SHARR-Orchestrator → Executions (Se puede revisar el historial de ejecuciones).



Executions (1/1)	
<input type="text" value="Filter executions by property or value"/>	
Name	Status
2988ed3e-0fd4-e9d5-9b09-254167c503...	Succeeded



Tarea 8.3 – Automatización de Systems Manager

Paso 1: AWS Systems Manager → Change Management → Automation

- Executions (se pueden revisar el historial de todas las automatizaciones ejecutadas).

	Execution ID	Runbook name	Status
	36973519-5351-4afe-a516-fb663873879f	ASR-SC_2.0.0_Lambda.1	 Success

- Seleccionar la ejecución → Execution details: ASR-SC_2.0.0_Lambda.1

Execution status

Overall status

Success

Failed

0

All executed steps

3

Cancelled

0

Succeeded

3

TimedOut

0

Executed steps (3)

Find Steps

Step ID	Step #	Step name	Action	Status
f8dfb72f-0dd1-470f-a2ac-53e76832ed61	1	ParseInput	aws:executeScript	<div><div></div></div> Success
d6e7c019-0d81-4945-999a-a25d762b278e	2	Remediation	aws:executeAutomation	<div><div></div></div> Success
8e72ebd6-27e9-493b-baf6-a0131bd44413	3	UpdateFinding	aws:executeAwsApi	<div><div></div></div> Success

Tarea 8.4 – CloudWatch Log Group

Paso 1: CloudWatch → Logs → Log Groups → SO0111-SHARR-Orchestrator

<input checked="" type="checkbox"/>	SO0111-SHARR-Orchestrator
-------------------------------------	---------------------------

- Log streams

<input checked="" type="checkbox"/>	Log stream
<input checked="" type="checkbox"/>	states/SO0111-SHARR-Orchestrator/2023-11-03-05/031b4af5

Paso 2: CloudWatch → Logs → Log Groups → SO0111-SHARR

☒ SO0111-SHARR

- Log streams

☒ Log stream

☒ SC-LAMBDA.1-2023-11-03

☒ SHARR-2023-11-03

Tarea 9 – Habilitar la remediación totalmente automática (Opcional)

El modo de funcionamiento de la solución consiste en remediar automáticamente los Findings a medida que llegan a Security Hub (como se evidenció en la Tarea 7).

El otro modo consiste en activar la remediación automática los Findings, en donde se iniciarán remediaciones en todos los recursos que coincidan con el control que se haya activado.

Paso 1: Amazon EventBridge → Buses → Rules

- Seleccionar la Rule que se desea activar → Enable

☒ SC_2.0.0_Lambda.1_AutoTrigger ⊖ Disabled

- Habilitar la Rule permite que sea remediada de manera totalmente automática.

Enable rule ✕

Are you sure you want to enable rule SC_2.0.0_Lambda.1_AutoTrigger?

Cancel

Enable

✔ Rule SC_2.0.0_Lambda.1_AutoTrigger was updated successfully

☒ SC_2.0.0_Lambda.1_AutoTrigger ✔ Enabled

Tarea 10 – Remediaciones personalizadas (Opcional)

La solución está diseñada para ser extensible y personalizable.

Para especificar una implementación de remediación alternativa se debe implementar documentos de automatización en AWS Systems Manager y roles de IAM personalizados.

Para admitir un nuevo conjunto completo de controles se debe implementar un Playbook personalizado.

Los SSM Runbooks deben seguir el siguiente estándar de nombre:

- ASR-<standard>-<version>-<control>
- Standard → CIS, AFSBP, PCI, or SC.
- Version → La versión del standard.
- Control → El ID del control que será remediado.
- Ejemplo: ASR-SC-2.0.0-Lambda.1

Runbook name

ASR-SC_2.0.0_Lambda.1

El IAM role asociado al SSM Runbook debe seguir el siguiente estándar de nombre:

- SO0111-Remediate-<standard>-<version>-<control>
- Ejemplo: SO0111-Remediate-SC-2.0.0-Lambda.1

Para habilitar la remediación automática se debe crear un EventBus Rule asociado:

El EventBus Rule debe seguir el siguiente estándar de nombre:

- <standard>_<version>_<control>_AutoTrigger
- Ejemplo: SC_2.0.0_Lambda.1_AutoTrigger



SC_2.0.0_Lambda.1_AutoTrigger