



276-[SF]-Lab - Endurecimiento de la red

Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 22/09/2023

Contacto: tomas.villaseca.c@gmail.com

Después de completar este laboratorio, podrá realizar lo siguiente:

- Configurar Amazon Inspector.
- Ejecutar una auditoría de red sin agente.
- Investigar los resultados del análisis.
- Actualizar grupos de seguridad.
- Inicie sesión en AppServer usando AWS Systems Manager Session Manager.

Entorno del laboratorio → Dos instancias EC2:

- BastionServer → Subred Pública
- AppServer → Subred Privada

Tarea 1: Ver instancias de EC2 y agregar etiquetas

BastionServer = Servidores utilizados para gestionar el acceso a una red privada desde una red externa.

- También conocidos como “Jump Boxes” o “Jump Servers”.
- Utilizados para comunicaciones de proxy o registro → SSH

Para crear un objetivo de evaluación para Amazon Inspector debe comenzar por etiquetar las instancias de EC2.

Paso 1: AWS Management Console → Services → Compute → EC2 → Instances

| Instances (2) Info | | | | |
|---|---------------|---------------------|------------------|-----------------|
| <input type="text" value="Find instance by attribute or tag (case-sensitive)"/> | | | | |
| <input type="checkbox"/> | Name ▾ | Instance ID | Instance state ▾ | Instance type ▾ |
| <input type="checkbox"/> | AppServer | i-0703968bdbfa4c883 | ✓ Running | t2.micro |
| <input type="checkbox"/> | BastionServer | i-0851addf9bf9791f2 | ✓ Running | t2.micro |

Paso 2: Seleccionar EC2 “BastionServer” → Tags → Manage Tags

| | | | |
|-------------------------------------|---------------|---------------------|-----------|
| <input checked="" type="checkbox"/> | BastionServer | i-0851addf9bf9791f2 | ✓ Running |
|-------------------------------------|---------------|---------------------|-----------|

Instance: i-0851addf9bf9791f2 (BastionServer)

| Details | Security | Networking | Storage | Status checks | Monitoring | Tags |
|---------|----------|------------|---------|---------------|------------|------|
|---------|----------|------------|---------|---------------|------------|------|

Manage tags

< 1 >

Paso 3: Add New Tag

- Key = SecurityScan
- Value = true

Manage tags [Info](#)

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key

Value - *optional*

| | | |
|---|---|--------|
| <input type="text" value="Name"/> | <input type="text" value="BastionServer"/> | Remove |
| <input type="text" value="cloudlab"/> | <input type="text" value="c89400a1935441l4814634t1w2"/> | Remove |
| <input type="text" value="SecurityScan"/> | <input type="text" value="true"/> | Remove |

Tags

Key

Value

SecurityScan

true

Se aplicó correctamente etiquetas para la instancia de BastionServer, lo que permite que el análisis de seguridad detecte y analice esta instancia.

Tarea 2: Configurar y ejecutar Amazon Inspector

Amazon Inspector = Servicio que realiza evaluaciones de seguridad automatizadas.



Amazon Inspector

- Realiza un análisis de todas las configuraciones de red en busca de vulnerabilidades de seguridad y desviaciones de las mejores prácticas de seguridad.
- Evaluación de seguridad finalizada → Lista de hallazgos de seguridad
- Lista de hallazgos de seguridad → Priorizados por nivel de gravedad, descripción detallada de cada problema de seguridad y una recomendación sobre cómo solucionarlo.


Paso 1: AWS Management Console → Services → Security, Identity, & Compliance → Amazon Inspector


Paso 2: Switch to Inspector Classic → Get Started

Inspector

×

Activate Inspector

Switch to Inspector Classic 



Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.

Get started

Paso 3: Advanced Setup

Run weekly (recommended)

Run once

Advanced setup

Cancel

Paso 4: En la sección “Define an assessment target” configurar las siguientes opciones:

- Name = Network-Audit
- Quitar la selección de la casilla “Include all EC2 instances in this AWS account and región”
- Key = SecurityScan
- Value = true
- Quitar la selección de la casilla “Install the Amazon Inspector Agent and an IAM role that allows Run Commands”.

Define an assessment target

An assessment target represents a collection of AWS resources that help you accomplish your business goals. [Learn more.](#)

Name*

All Instances ☐ Include all EC2 instances in this AWS account and region.

Note: The limit on the maximum number of agents that can be included in an assessment run applies. [Learn more](#)

| Tags* | Key | Value | |
|-------|---------------|-------|--|
| | SecurityScan | true | |
| | Add a new key | | |

Install Agents ☐ Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

Paso 4: En la sección “Define an assessment template” configurar las siguientes opciones:

- Name = Assessment-Template-Network
- Rules packages → Solo mantener “Network Reachability-1.1”
- Duración = 15 minutos
- Quitar la selección en la casilla “Set up recurring assessment runs every: __”

Define an assessment template

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

Name*

Rules packages*

Amazon Inspector runs assessments for the assessment target against selected rules package(s). [Learn more.](#)

Duration*

The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but note that assessment ter

Assessment Schedule ☐ Set up recurring assessment runs once every days. The first run starts on create. [Learn more](#)

Paso 5: Seleccionar “Create”

[Cancel](#) [Preview](#) [Previous](#) [Create](#)

✓

SUCCESS

- Assessment run started

Success → Confirma que se inició la ejecución de la evaluación de Amazon Inspector.

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior a

[Run](#) [Cancel](#) [Delete](#)

Filter

1 selected

| <input type="checkbox"/> | Start time | Status | Template name | Findings |
|-------------------------------------|--------------------------------|-------------------|-----------------------------|----------|
| <input checked="" type="checkbox"/> | Today at 7:28 PM (GMT-3) (...) | Analysis complete | Assessment-Template-Network | 3 |

Paso 6: Una vez completado el análisis → Panel de Navegación → Findings

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a spe

[Add/Edit attributes](#)

Filter

| <input type="checkbox"/> | Severity ⓘ | Date ▲ | Finding |
|--------------------------|---------------|-----------------|---|
| <input type="checkbox"/> | Medium | Today at 7:2... | On instance i-0851addf9bf9791f2, TCP port 22 whi... |
| <input type="checkbox"/> | High | Today at 7:2... | On instance i-0851addf9bf9791f2, TCP port 23 whi... |
| <input type="checkbox"/> | Informational | Today at 7:2... | Aggregate network exposure: On instance i-0851a... |

Tarea 3: Analizar hallazgos de Amazon Inspector

Findings de la evaluación de Amazon Inspector, en este caso, muestran si sus puertos son accesibles desde internet mediante una IGW, una conexión de VPC, o una VPN mediante una Virtual Private Gateway.

Se destacan las configuraciones que permiten potenciales accesos maliciosos.


Paso 1: Expandir el Finding de severidad alta:

- AWS Agent ID = Muestra la instancia EC2 afectada.
- Description = Muestra el motivo del hallazgo.
- Recommendation = Proporciona sugerencias de corrección.

| | Severity ⓘ | Date | Finding | Target | Template | Rules Package |
|--|--|-----------------|---|---------------|--------------------|--------------------------|
| <input type="checkbox"/> | High | Today at 7:2... | On instance i-0851addf9bf9791f2, TCP port 23 whi... | Network-Audit | Assessment-Temp... | Network Reachability-1.1 |
| Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network' | | | | | | |
| ARN | arn:aws:inspector:us-west-2:255270933105:target/0-00I7JchO/template/0-dblICG47/run/0-5d0JdXr/finding/0-9ICFkPlq | | | | | |
| Run name | Run - Assessment-Template-Network - 2023-09-22T22:26:38.452Z | | | | | |
| Target name | Network-Audit | | | | | |
| Template name | Assessment-Template-Network | | | | | |
| Start | Today at 7:26 PM (GMT-3) (10 minutes ago) | | | | | |
| End | Today at 7:27 PM (GMT-3) (10 minutes ago) | | | | | |
| Status | Analysis complete | | | | | |
| Rules package | Network Reachability-1.1 | | | | | |
| AWS agent ID | i-0851addf9bf9791f2 | | | | | |
| Finding | On instance i-0851addf9bf9791f2 , TCP port 23 which is associated with 'Telnet' is reachable from the internet | | | | | |
| Severity | High ⓘ | | | | | |
| Description | On this instance, TCP port 23, which is associated with Telnet, is reachable from the internet. You can install the Inspector agent on this in on this port. The instance i-0851addf9bf9791f2 is located in VPC vpc-0fe19ef96b69e1301 and has an attached ENI eni-037d141caa4251 reachable from the internet through Security Group sg-0e94b4b70e26cede5 and IGW igw-0b310272237697444 | | | | | |
| Recommendation | You can edit the Security Group sg-0e94b4b70e26cede5 to remove access from the internet on port 23 | | | | | |

Paso 2: Expandir el Finding de severidad media:

- AWS Agent ID = Muestra la instancia EC2 afectada.
- Description = Muestra el motivo del hallazgo.
- Recommendation = Proporciona sugerencias de corrección.

 **Medium** Today at 7:2... On instance i-0851addf9bf9791f2, TCP port 22 whi... Network-Audit Assessment-Temp... Netv

Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'

ARN

arn:aws:inspector:us-west-2:255270933105:target/0-00I7JchO/template/0-dblICG47/run/0-5d0jOdXr/finding/0-UDTa

Run name

Run - Assessment-Template-Network - 2023-09-22T22:26:38.452Z

Target name

Network-Audit

Template name

Assessment-Template-Network

Start

Today at 7:26 PM (GMT-3) (12 minutes ago)

End

Today at 7:27 PM (GMT-3) (11 minutes ago)

Status

Analysis complete

Rules package

Network Reachability-1.1

AWS agent ID

i-0851addf9bf9791f2

Finding

On instance [i-0851addf9bf9791f2](#), TCP port 22 which is associated with 'SSH' is reachable from the internet

Severity

Medium ⓘ

Description

On this instance, TCP port 22, which is associated with SSH, is reachable from the internet. You can install the Inspe
this port. The instance [i-0851addf9bf9791f2](#) is located in VPC [vpc-0fe19ef96b69e1301](#) and has an attached ENI [eni-0](#)
reachable from the internet through Security Group [sg-0e94b4b70e26cede5](#) and IGW [igw-0b310272237697444](#)

Recommendation

You can edit the Security Group [sg-0e94b4b70e26cede5](#) to remove access from the internet on port 22

Tarea 4: Actualizar grupos de seguridad

Paso 1: En la sección “Recommendation” en el hallazgo de alta severidad → Selección enlace al Security Group.

Recommendation You can edit the Security Group [sg-0e94b4b70e26cede5](#) to remove access from the internet on port 23

Security Groups (1/1) [Info](#)

Security group ID: [sg-0e94b4b70e26cede5](#)

| <input checked="" type="checkbox"/> | Name | Security group ID | Security group name |
|-------------------------------------|-----------------|--------------------------------------|-----------------------|
| <input checked="" type="checkbox"/> | BastionServerSG | sg-0e94b4b70e26cede5 | c89400a1935441l481... |

Paso 2: Inbound Rules → Edit Inbound rules

- Eliminar regla de entrada asociada al puerto 23 (telnet).

[Details](#)

[Inbound rules](#)

[Outbound rules](#)

[Tags](#)

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

| Security group rule ID | Type Info | Protocol Info | Port range Info | Source Info | |
|------------------------|---|-------------------------------|---------------------------------|-----------------------------|---|
| sgr-00d21300d9f2c508b | <input type="text" value="Custom TCP"/> | TCP | 23 | Custom | <input type="text" value="0.0.0.0/0"/> <input type="button" value="X"/> |
| sgr-0089f2d9802e05416 | <input type="text" value="SSH"/> | TCP | 22 | Custom | <input type="text" value="0.0.0.0/0"/> <input type="button" value="X"/> |

- Reemplazar la Source de la regla de entrada SSH: Custom → My IP

Inbound rules [Info](#)

| Security group rule ID | Type Info | Protocol Info | Port range Info | Source Info |
|------------------------|---------------------------|-------------------------------|---------------------------------|-----------------------------|
| sgr-00d21300d9f2c508b | SSH | TCP | 22 | My IP |

207.248.217.198/32 ✕

Paso 3: Analizar nuevamente el entorno con Amazon Inspector

- Panel de navegación → Assessment Templates → Run

Amazon Inspector - Assessment Templates

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS

[Create](#)
[Run](#)
[Delete](#)
[Clone](#)
[Create Assessment Events](#)

Filter 1 selected

| <input type="checkbox"/> | Name | Duration |
|-------------------------------------|-----------------------------|------------|
| <input checked="" type="checkbox"/> | Assessment-Template-Network | 15 Minutes |

Análisis Completo:

| <input type="checkbox"/> | Start time | Status | Template name | Findings |
|--------------------------|--------------------------------|-------------------|-----------------------------|----------|
| <input type="checkbox"/> | Today at 7:46 PM (GMT-3) (...) | Analysis complete | Assessment-Template-Network | 2 |

Se puede evidenciar que el Finding de severidad alta ya no aparece, pero el de severidad media sigue apareciendo.

El puerto 22 (SSH) redujo su alcance al modificar el Source a My IP, pero técnicamente sigue “abierto” para el internet fuera de la VPC.

| <input type="checkbox"/> | Severity ⓘ | Date | Finding | Target |
|--------------------------|------------|-----------------|---|---------------|
| <input type="checkbox"/> | Medium | Today at 7:4... | On instance i-0851addf9bf9791f2, TCP port 22 whi... | Network-Audit |

Se actualizó el Security Group adjunto a BastionServer para que permita tráfico solo desde su dirección IP, en lugar de desde el Internet abierto (0.0.0.0), y eliminó el puerto 23 (Telnet) que estaba completamente abierto y ya no era necesario.

Tarea 5: Reemplace BastionServer con Systems Manager

AWS Systems Manager = Solución de administración segura para recursos de AWS y en entornos multicloud e híbridos.



AWS Systems
Manager

- Operations Management → Proporciona visibilidad de sus aplicaciones e infraestructura y ayuda a solucionar problemas con rapidez.
- Application Management → Implemente, administre y escale sus aplicaciones.
- Change Management → Manera controlada y auditable de realizar cambios en sus aplicaciones e infraestructura.
- Node Management → Gestione sus instancias EC2 y otros recursos on-premise.

Reemplazar la instancia EC2 BastionServer, que usaba principalmente SSH para conectarse a AppServer dentro de la subred privada con Amazon Systems Manager para conectarse mediante Session Manager.

Paso 1: AWS Management Console → Services → Compute → EC2 → Security Groups

| Security Groups (1/4) Info | | | |
|---|-----------------|----------------------|-----------------------|
| <input type="text" value="Filter security groups"/> | | | |
| <input type="checkbox"/> | Name | Security group ID | Security group name |
| <input type="checkbox"/> | – | sg-08f1fa8b66d46d929 | default |
| <input checked="" type="checkbox"/> | BastionServerSG | sg-0aedf85633292aa1d | c89400a1935441l481... |
| <input type="checkbox"/> | AppSG | sg-07773a5928ca3f599 | c89400a1935441l481... |
| <input type="checkbox"/> | – | sg-01086e68fd75c8333 | default |

Paso 2: Inbound Rules → Edit inbound Rules → Eliminar regla de SSH.

| Details | Inbound rules | Outbound rules | Tags |
|---------|---------------|----------------|------|
|---------|---------------|----------------|------|


Edit inbound rules

Delete

| | | | | |
|-------------------------------------|---------------|---------------------|---------|--|
| <input checked="" type="checkbox"/> | BastionServer | i-0b4bae935fa9bf023 | Running | |
|-------------------------------------|---------------|---------------------|---------|--|

Stop instance?

Instance IDs

 i-0b4bae935fa9bf023 (BastionServer)

To confirm that you want to stop the instance, choose the *Stop* button below.

Cancel

Stop

↺

Connect

Instance state ▾

Actions ▾

Launch instances ▾

< 1 >

⚙

12

Conexión a AppServer mediante Session Manager:

Session ID: user2741130=Tom__sVillaseca-0468fcaec5a5e662f

Instance ID: i-021b4cdcd0e5b9573

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$
```

Paso 5: Analizar nuevamente el entorno con Amazon Inspector

- Panel de navegación → Assessment Templates → Run

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against a baseline.

| <div>Run Cancel Delete</div> | | | | |
|-------------------------------------|--------------------------------|-------------------|-----------------------------|----------|
| Filter | | | 1 selected | |
| <input type="checkbox"/> | Start time | Status | Template name | Findings |
| <input checked="" type="checkbox"/> | Today at 8:26 PM (GMT-3) (...) | Analysis complete | Assessment-Template-Network | 0 |
| <input type="checkbox"/> | Today at 7:46 PM (GMT-3) (...) | Analysis complete | Assessment-Template-Network | 2 |

Se verifica que no hay Findings.

Se mejoró correctamente la seguridad de la red al agregar un rol IAM a AppServer y al eliminar la regla de entrada SSH dentro del grupo de seguridad de BastiónServer.

Se hizo que sea incluso más fácil conectarse usando Session Manager proporcionado por Amazon Systems Manager.

Laboratorio Completado