

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

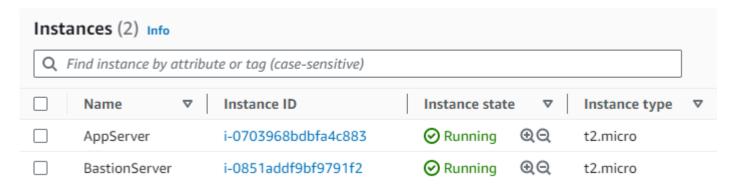
agregar etiquetas

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

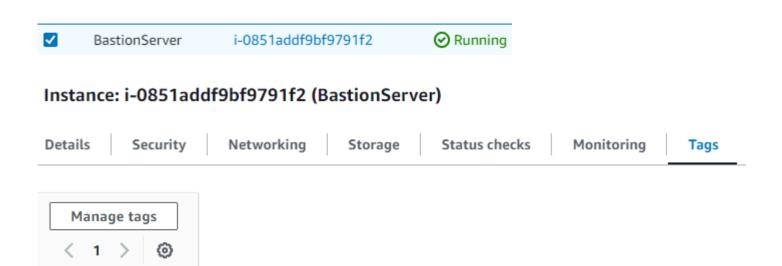
- También conocidos como "Jump Boxes" o "Jump Servers".
- Utilizados para comunicaciones de proxy o registro → SSH

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

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



Paso 2: Seleccionar EC2 "BastionServer" → Tags → Manage Tags



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 × Q Name Q BastionServer X Remove Q cloudlab Q c89400a1935441l4814634t1w2 Remove Q SecurityScan X Q true X Remove **Tags** Q 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

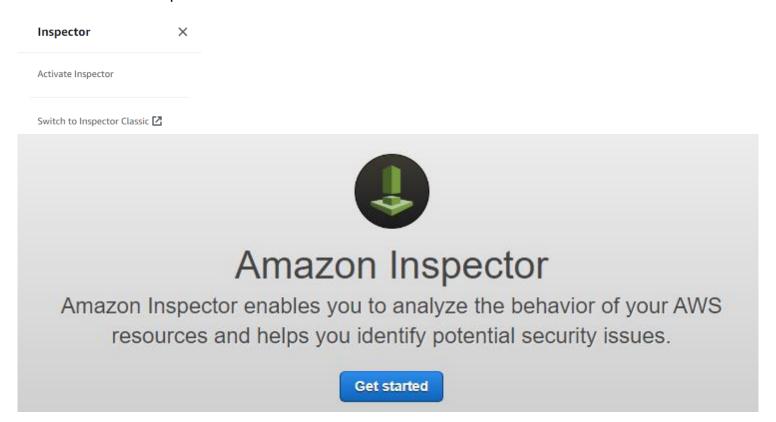
Amazon Inspector = Servicio que realiza evaluaciones de seguridad automatizadas.



- 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



Paso 3: Advanced Setup



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

- Name = Network-Audit
- Quitar la selcción 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".

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

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

- 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: ___"

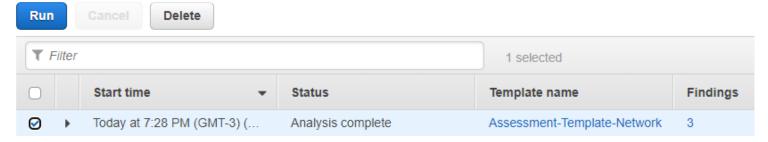
Paso 5: Seleccionar "Create"



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

Amazon Inspector - Assessment Runs

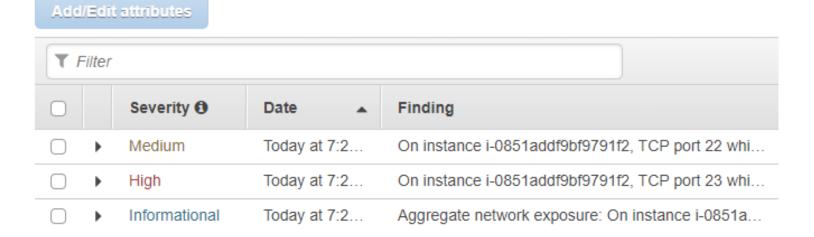
An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior as



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-



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 6 🕶	Date	Finding	Target	Template	Rules Package				
□ ▼	High	Today at 7:2	On instance i-0851addf9bf9791f2, TCP port 23 whi	Network-Audit	Assessment-Temp	Network Reachability-1.1				
Findir	Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'									
	ARN arn:aws:inspector:us-west-2:255270933105:target/0-O0I7JchO/template/0-dblICG47/run/0-5d0jOdXr/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										
On this instance, TCP port 23, which is associated with Telnet, is reachable from the internet. You can install the Internet on this port. The instance i-0851addf9bf9791f2 is located in VPC vpc-0fe19ef96b69e1301 and has an attached EN 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.

0 -	Medium	Today at 7:2	On instance i-0851addf9bf9791f2, TCP port 22 whi Network-Audit Assessment-Temp Netw					
Findi	ing for asse	essment targe	t 'Network-Audit' and template 'Assessment-Template-Network'					
		ARN	arn:aws:inspector:us-west-2:255270933105:target/0-O0I7JchO/template/0-dbIICG47/run/0-5d0jOdXr/finding/0-UDTac					
Run name Target name			Run - Assessment-Template-Network - 2023-09-22T22:26:38.452Z					
			Network-Audit					
		Template name	Assessment-Template-Network					
Start End Status Rules package AWS agent ID			Today at 7:26 PM (GMT-3) (12 minutes ago)					
			Today at 7:27 PM (GMT-3) (11 minutes ago)					
			Analysis complete					
			Network Reachability-1.1					
			i-0851addf9bf9791f2					
Finding Severity		Finding	On instance i-0851addf9bf9791f2, TCP port 22 which is associated with 'SSH' is reachable from the internet					
		Severity	Medium ❸					
		Description	On this instance, TCP port 22, which is associated with SSH, is reachable from the internet. You can install the Inspect this port. The instance i-0851addf9bf9791f2 is located in VPC vpc-0fe19ef96b69e1301 and has an attached ENI eni-C 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 hallazo de alta severidad → Selección enlace al Security Group.

Security Groups (1/1) Info

Q Filter security groups

Security group ID: sg-0e94b4b70e26cede5 X

Clear filters

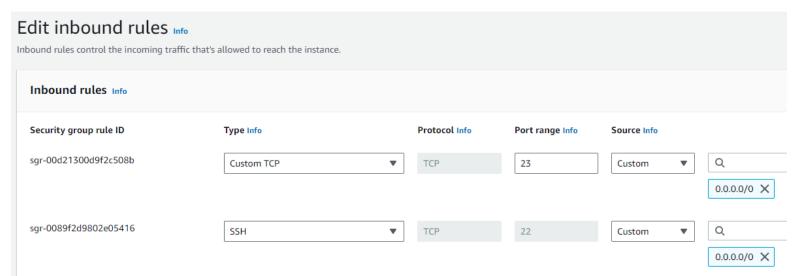
Value
Security group ID

▼ Security group ID
Security group ID

Paso 2: Inbound Rules → Edit Inbound rules

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





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

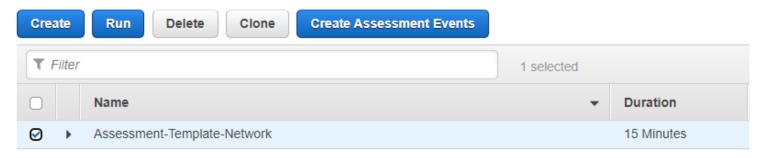


Paso 3: Analizar nuevamente el entorno con Amazon Inspector

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



Análisis Completo:



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.



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.



Manager

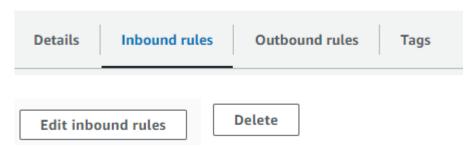
- Operations Management → Proporciona visibilidad de sus aplicaciones e infraestructura y ayuda a solucionar problemas con rapidez.
- Application Management → Implemente, administre y escale sus aplicaciones.
- Change Management → Manera controlada y auditable de realizar cambios en sus aplicaciones 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.

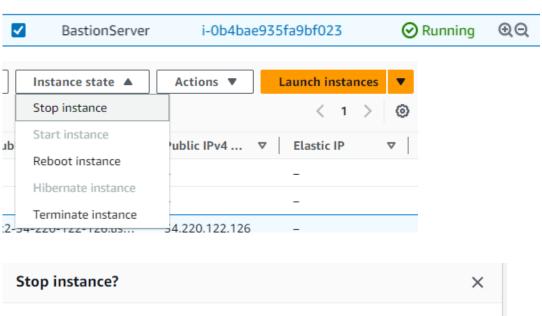
Paso 1: AWS Management Console → Services → Compute → EC2 → Security Groups

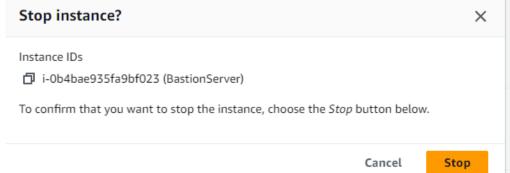
Security Groups (1/4) Info Q Filter security groups								
	_		sg-08f1fa8b66d46d929	default				
✓	BastionServerSG		sg-0aedf85633292aa1d	c89400a1935441l481				
	AppSG		sg-07773a5928ca3f599	c89400a1935441l481				
	_		sg-01086e68fd75c8333	default				

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

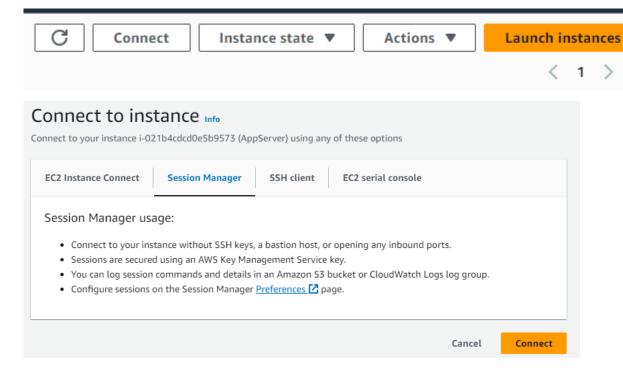


Paso 3: Instances → BastionServer → Instance State → Stop Instance





Paso 4: Instances → AppSever → Connect



Conexión a AppServer mediante Session Manager:

Session ID: user2741130=Tom_sVillaseca-0468fcaec5a5e662f

Instance ID: i-021b4cdcd0e5b9573

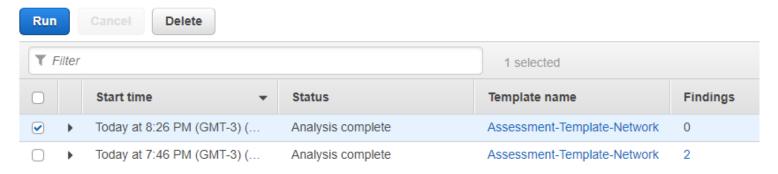


Paso 5: Analizar nuevamente el entorno con Amazon Inspector

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 aga



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.

