



# ENDURECIMIENTO DE LA RED

*Laboratorio 276*



# OBJETIVOS

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

# TAREA 1: MIRAR LAS INSTANCIAS DE EC2 Y AGREGAR ETIQUETAS

- Comenzamos etiquetando las instancias de EC2, en este caso la instancia BastionServer, para permitir al escaneo de seguridad encontrar esta instancia.
- Cada etiqueta AWS consta de un par de clave y valor de su elección. Por ejemplo, puede elegir nombrar su clave Name (Nombre) y su valor MyFirstInstance.



Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

All states

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	AppServer	i-0f116b54b5a277da5	Running	t2.micro	Initializing	View alarms +	us-west-2a
<input checked="" type="checkbox"/>	BastionServer	i-08b62ba1fd34b4144	Running	t2.micro	Initializing	View alarms +	us-west-2a

i-08b62ba1fd34b4144 (BastionServer)

DetailsStatus and alarms NewMonitoringSecurityNetworkingStorageTags

▼ Instance summary Info

Instance ID

i-08b62ba1fd34b4144 (BastionServer)

IPv6 address

-

Hostname type

IP name: ip-10-0-1-58.us-west-2.compute.internal

Answer private resource DNS name

-

Auto-assigned IP address

52.27.72.171 [Public IP]

←  
Instancia BastionServer

Etiquetas

i-08b62ba1fd34b4144 (BastionServer)

DetailsStatus and alarms NewMonitoringSecurityNetworkingStorageTags

Tags

Manage tags

< 1 > ⚙

Key	Value
aws:cloudf...	c110983a2632290l6677746t1w851725211238
cloudlab	c110983a2632290l6677746t1w851725211238
Name	BastionServer
aws:cloudf...	arn:aws:cloudformation:us-west-2:851725211238:stack/c110983a2632290l6677746t1w851725211238/4e5c6010-1174-11ef-a2e6-022319217f99
aws:cloudf...	BastionServer

- Creamos un tag de nombre SecurityScan, con valor true, para la instancia BastionServer

i-08b62ba1fd34b4144 (BastionServer)

Details | Status and alarms [New](#) | Monitoring | Security | Networking | Storage | **Tags**

**Tags**

Manage tags

< 1 > ⚙

Key	Value
aws:cloudf...	c110983a2632290l6677746t1w851725211238
cloudlab	c110983a2632290l6677746t1w851725211238
Name	BastionServer
aws:cloudf...	arn:aws:cloudformation:us-west-2:851725211238:stack/c110983a2632290l6677746t1w851725211238/4e5c6010-1174-11ef-a2e6-022319217f99
aws:cloudf...	BastionServer

**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="cloudlab"/>	<input type="text" value="c110983a2632290l6677746t1w"/>	<button>Remove</button>
<input type="text" value="Name"/>	<input type="text" value="BastionServer"/>	<button>Remove</button>
<input type="text" value="SecurityScan"/>	<input type="text" value="true"/>	<button>Remove</button>

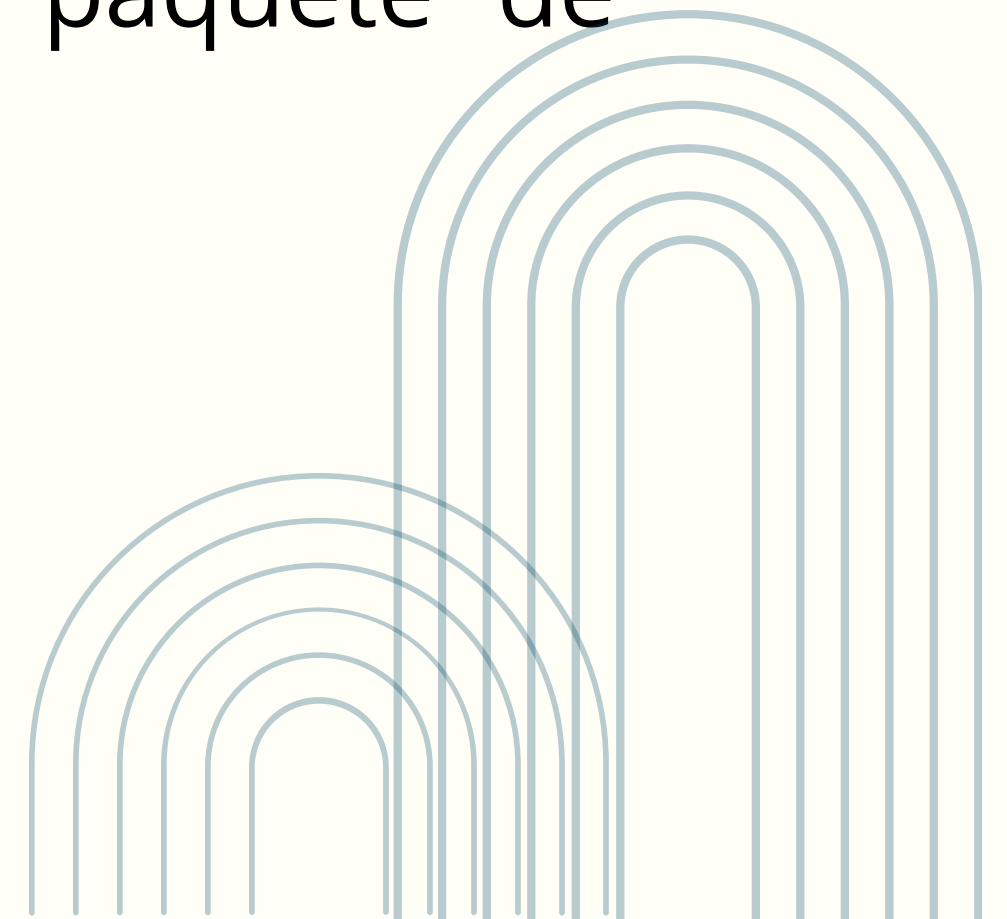
Add new tag

You can add up to 47 more tags.

Cancel Save

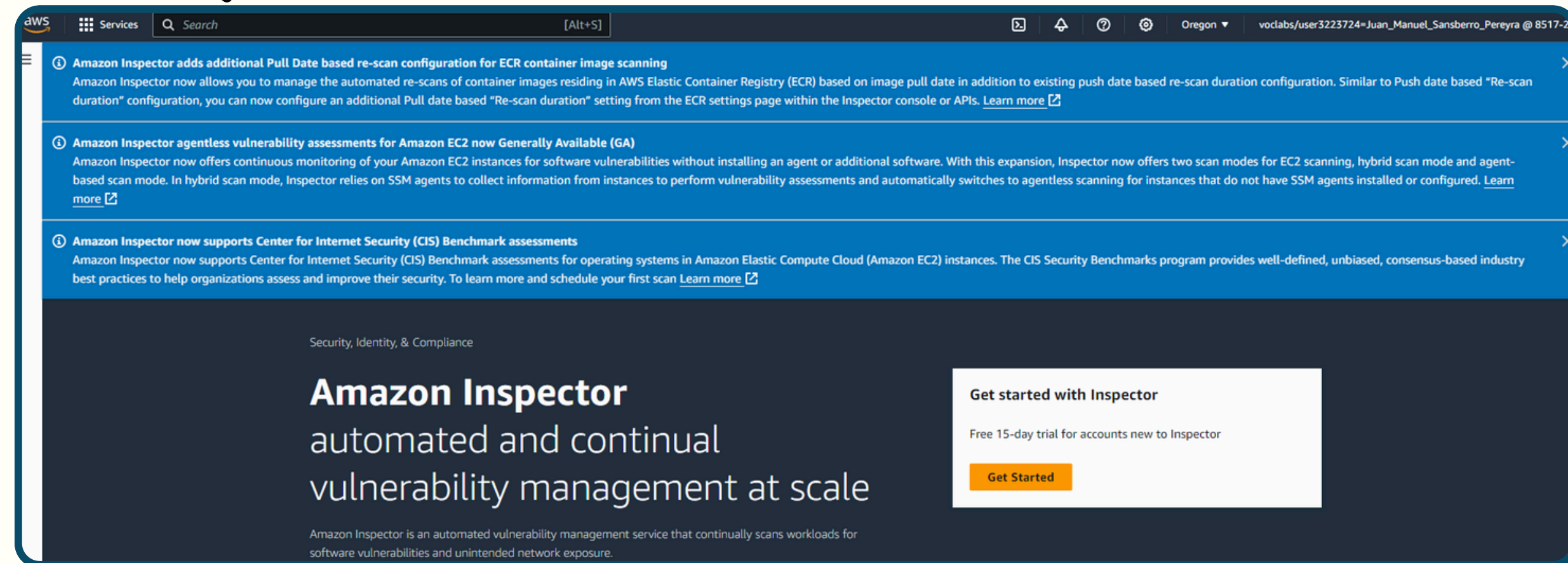
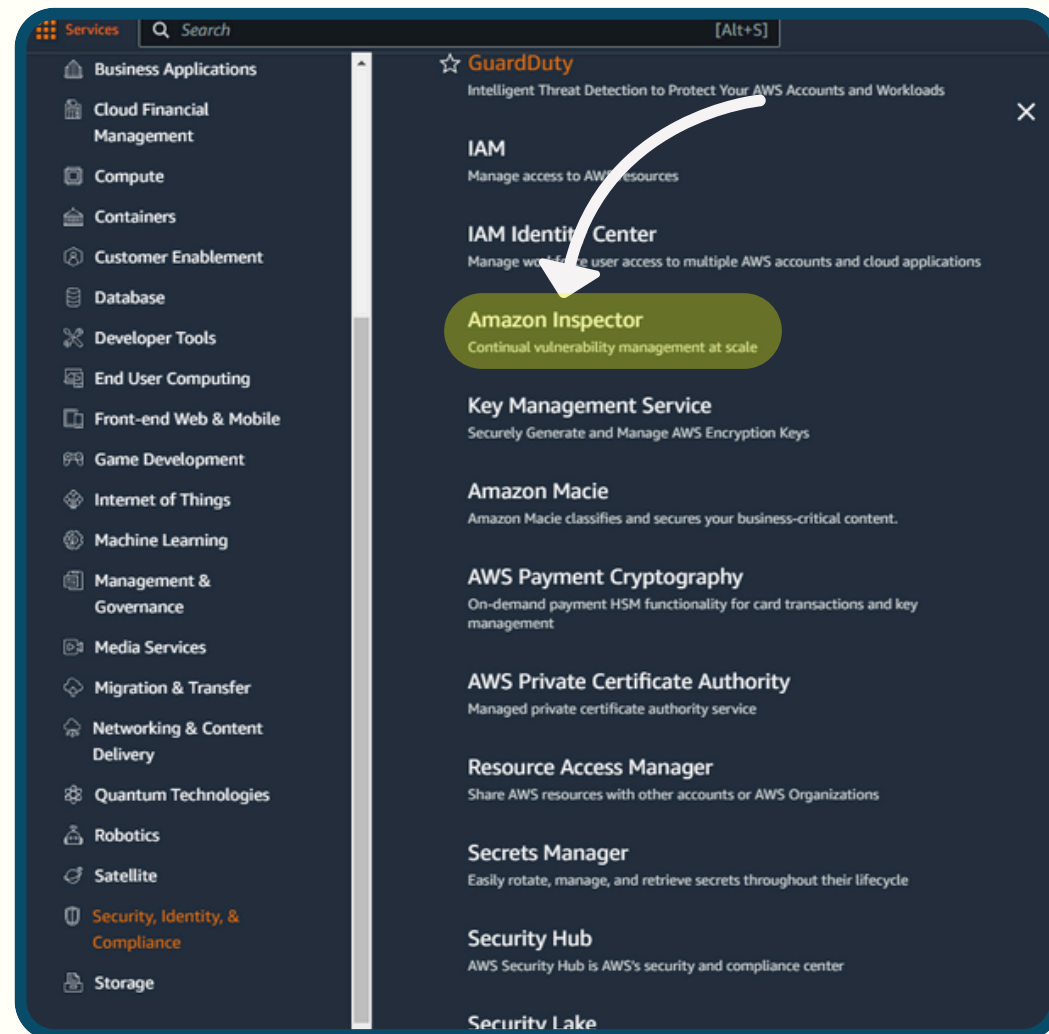
# TAREA 2: CONFIGURAR Y EJECUTAR AMAZON INSPECTOR

- En esta tarea, aprenderá a ejecutar una auditoría de red sin agente en sus instancias de EC2 usando Amazon Inspector. Para este laboratorio, usará el paquete de reglas de accesibilidad de red.

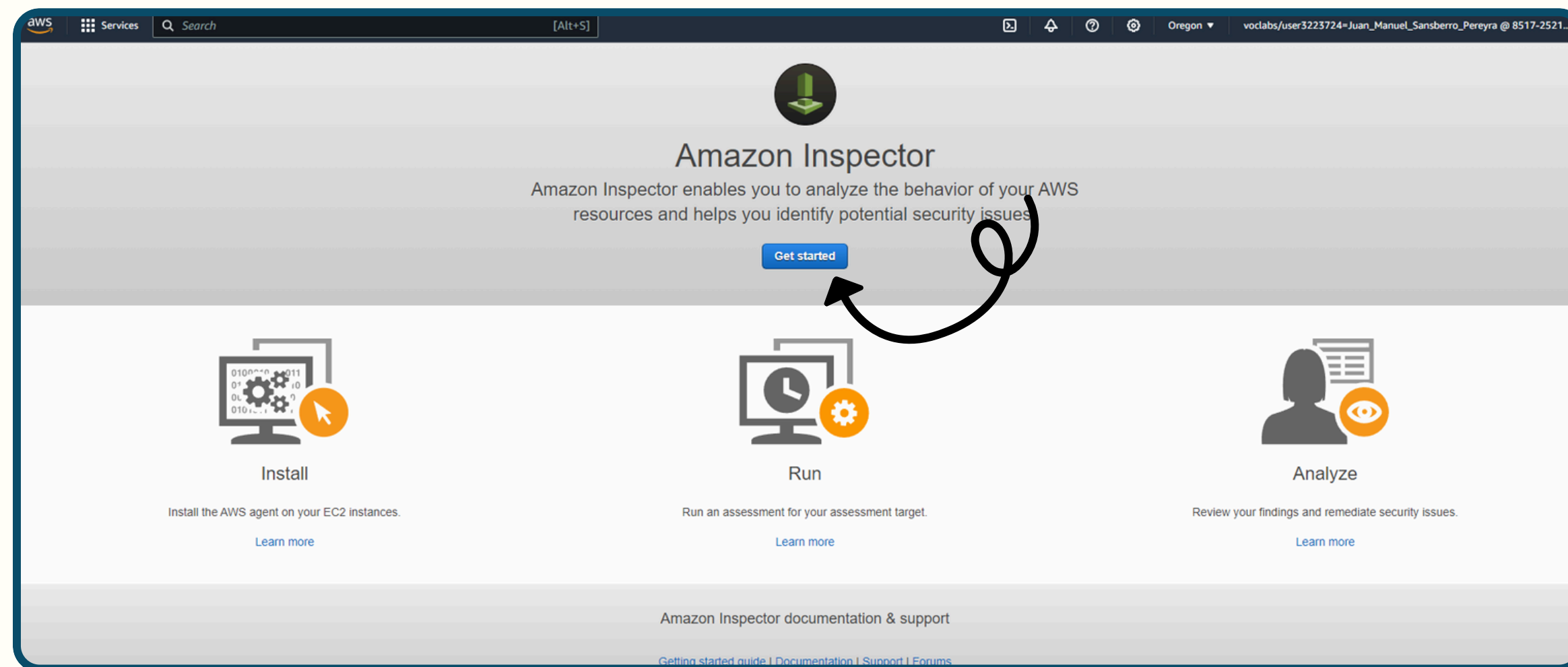
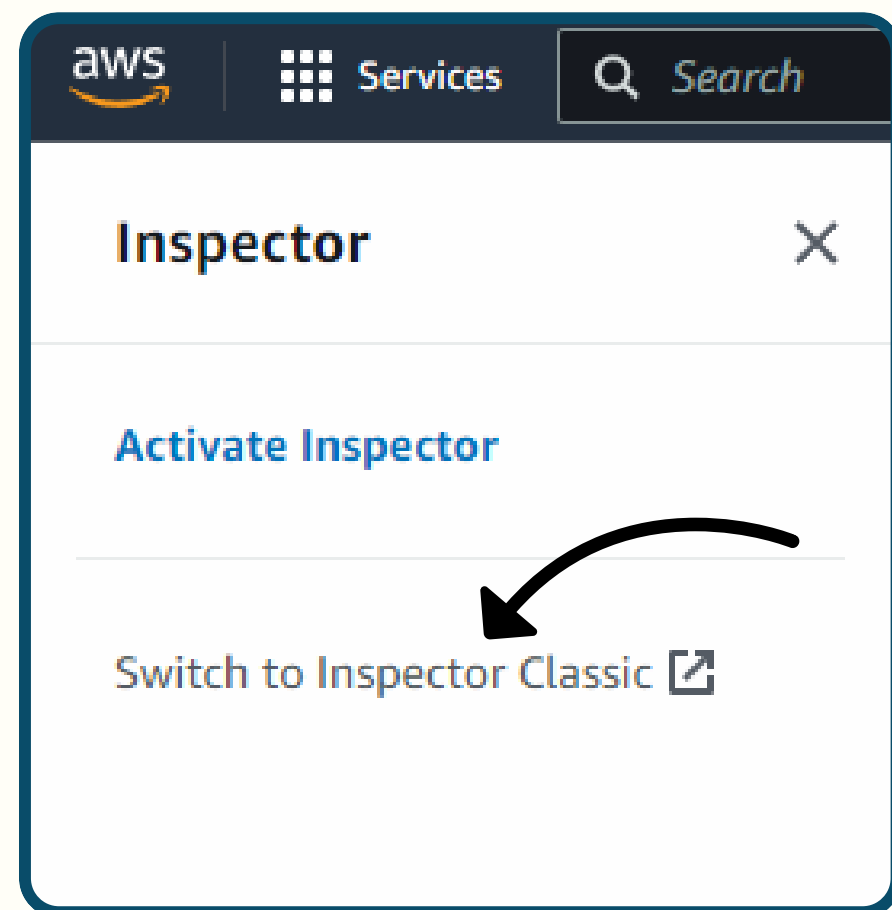




- Ingresamos a Amazon Inspector, para configurarlo, y ejecutarlo posteriormente



- Cambiamos en inspector a modo clásico, y lo iniciamos.





out Inspector Agent and how to manually install agent.  
ssed weekly, the monthly cost would be around \$120/month. [Learn more](#)

Run weekly (recommended)

Run once

Advanced setup

Seleccionamos configuración  
avanzada y lo configuramos con las  
siguientes opciones

aws Services Search [Alt+S] Oregon

## Get started with Amazon Inspector

Step 1: Define an assessment target  
Step 2: Define an assessment template  
Step 3: Review

### Define an assessment target

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

Name\* Network-Audit

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
Security Scan	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](#)

\*Required

- En este paso definimos una plantilla de evaluación y la configuramos



Get started with Amazon Inspector

**Step 1: Define an assessment target**  
**Step 2: Define an assessment template**  
Step 3: Review

### 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\***

Common Vulnerabilities and Exposures-1.1	x
CIS Operating System Security Configuration Benchmarks-1.0	x
Security Best Practices-1.0	x
Network Reachability-1.1	x

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 templates with longer durations can deliver fuller sets of findings.

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

\*Required

[Cancel](#) [Previous](#) [Next](#)

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 selected rules packages.

RunCancelDelete

Filter

	Start time	Status	Template name	Findings
<input type="checkbox"/>		Preparing to start	Assessment-Template-Network	0

Assessment - Run - Assessment-Template-Network - 2024-05-13T22:14:17.881Z

ARNarn:aws:inspector:us-west-2:851725211238:target/0-sxeFndPA/template/0-RjGipH9V/run/0-cNzNI4Xm

Target nameNetwork-Audit

Template nameAssessment-Template-Network

Rules packagesCommon Vulnerabilities and Exposures-1.1  
Network Reachability-1.1  
CIS Operating System Security Configuration Benchmarks-1.0  
Security Best Practices-1.0

Duration15 Minutes

StatusPreparing to start

Findings0

Show AWS agents

Luego de crearla podremos ver una vista previa de nuestra plantilla y el estado de la misma

Run - Assessment-Template-Network - 2024-05-13T22:14:17.881Z

Last updated on May 13, 2024 7:16:16 PM (0m ago)

Filter

« < Viewing 1-2 of 2 > »

Instance	Name	Matched tags	AWS agent health	Status	Messages received
<a href="#">i-08b62ba1fd3...</a>	BastionServer	SecurityScan:true	UNKNOWN	UNKNOWN ⓘ	0
<a href="#">i-0f116b54b5a...</a>	AppServer	SecurityScan:true	UNKNOWN	UNKNOWN ⓘ	0

OK

En este paso, podemos ver nuestros hallazgos con sus diferentes niveles de severidad

aws

Services

Search

[Alt+S]

Oregon

voclabs/user3223724=Juan\_Manuel\_Sansberro\_Pereyra @ 8517-2521...

Dashboard

Assessment targets

Assessment templates

Assessment runs

Findings

Severity Filter

High

Medium

Low

Informational

Switch to Inspector V2

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Learn more](#) [Start your free trial](#)

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more](#)

Add/Edit attributes

Last updated on May 13, 2024 7:17:03 PM (0m ago)

Filter

Viewing 1-3 of 3

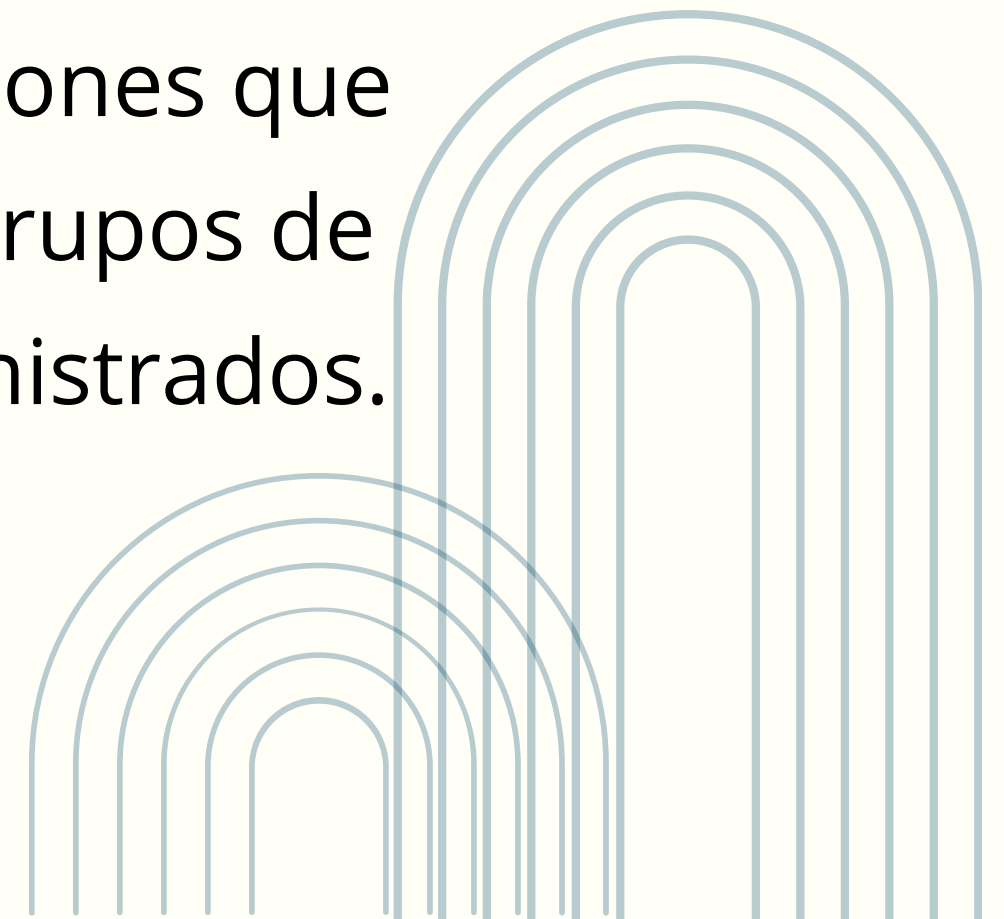
	Severity	Date	Finding	Target	Template	Rules Package
	High	Today at 7:1...	On instance i-08b62ba1fd34b4144, TCP port 23 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
	Medium	Today at 7:1...	On instance i-08b62ba1fd34b4144, TCP port 22 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
	Informational	Today at 7:1...	Aggregate network exposure: On instance i-08b62...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

Max records per page: 25

\* refresh browser to reflect change

# TAREA 3: ANALIZAR HALLAZGOS DE AMAZON INSPECTOR

- Los hallazgos que esas reglas muestran son acerca de si sus puertos son accesibles desde Internet mediante un Gateway Internet.
- Estos hallazgos también destacan las configuraciones que permiten potenciales accesos maliciosos, como grupos de seguridad, ACL y Gateways de Internet mal administrados.



Severity	Date	Finding	Target	Template	Rules Package
High	Today at 7:1...	On instance i-08b62ba1fd34b4144, TCP port 23 w...	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-2:851725211238:target/0-sxeFndPA/template/0-RjGipH9V/run/0-cNzNI4Xm/finding/0-7KVdpMFy](#)

**Run name** [Run - Assessment-Template-Network - 2024-05-13T22:14:17.881Z](#)

**Target name** [Network-Audit](#)

**Template name** [Assessment-Template-Network](#)

**Start** Today at 7:14 PM (GMT-3) (6 minutes ago)

**End** Today at 7:14 PM (GMT-3) (5 minutes ago)

**Status** Analysis complete

**Rules package** [Network Reachability-1.1](#)

**AWS agent ID** [i-08b62ba1fd34b4144](#)

**Finding** On instance [i-08b62ba1fd34b4144](#), 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 instance and re-run the assessment to check for any process listening on this port. The instance [i-08b62ba1fd34b4144](#) is located in VPC [vpc-07b44c379e712d674](#) and has an attached ENI [eni-00de29e830a96d53f](#) which uses network ACL [acl-02a2b6e7c90a66d4e](#). The port is reachable from the internet through Security Group [sg-0722ae17298706591](#) and IGW [igw-0318740bceba04827](#)

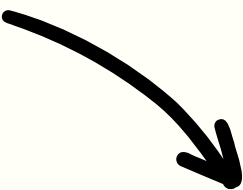
**Recommendation** You can edit the Security Group [sg-0722ae17298706591](#) to remove access from the internet on port 23

[Show Details](#)

Expandiremos el hallazgo de alta severidad. Para poder ver los siguientes detalles



Expandiremos el hallazgo de media severidad. Así podremos ver los siguientes detalles



Severity ⓘ

Date

Finding

Target

Template

Rules Package

▶ High

Today at 7:1...

On instance i-08b62ba1fd34b4144, TCP port 23 w...

Network-Audit

Assessment-Temp...

Network Reachability-1.1

▼ Medium

Today at 7:1...

On instance i-08b62ba1fd34b4144, TCP port 22 w...

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-2:851725211238:target/0-sxeFndPA/template/0-RjGipH9V/run/0-cNzNI4Xm/finding/0-btb4rWgp

Run name

Run - Assessment-Template-Network - 2024-05-13T22:14:17.881Z

Target name

Network-Audit

Template name

Assessment-Template-Network

Start

Today at 7:14 PM (GMT-3) (8 minutes ago)

End

Today at 7:14 PM (GMT-3) (8 minutes ago)

Status

Analysis complete

Rules package

Network Reachability-1.1

AWS agent ID

i-08b62ba1fd34b4144

Finding

On instance i-08b62ba1fd34b4144, 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 Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance i-08b62ba1fd34b4144 is located in VPC vpc-07b44c379e712d674 and has an attached ENI eni-00de29e830a96d53f which uses network ACL acl-02a2b6e7c90a66d4e. The port is reachable from the internet through Security Group sg-0722ae17298706591 and IGW igw-0318740bceba04827

Recommendation

You can edit the Security Group sg-0722ae17298706591 to remove access from the internet on port 22

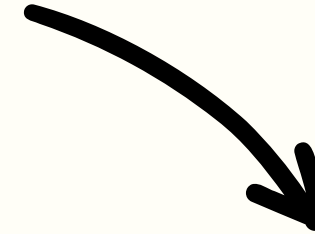


# TAREA 4: ACTUALIZAR LOS GRUPOS DE SEGURIDAD

- En esta tarea, verá algunas opciones de corrección para los hallazgos de seguridad que Amazon Inspector detectó. La primera opción muestra cómo bloquear el puerto 22 para direcciones IP específicas.
- Actualizaremos el grupo de seguridad adjunto a BastionServer para que permita tráfico solo desde su dirección IP, en lugar de desde el Internet abierto, y eliminaremos el puerto Telnet que estaba completamente abierto y ya no era necesario.



- Eliminamos el ingreso a través del protocolo Custom TCP, desde cualquier dirección IP



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 <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-0b206fcd92ed62477	SSH	TCP	22	Custom	<input type="text"/>	<input type="button" value="Delete"/>
				<input type="text" value="0.0.0.0/0"/>		
sgr-0d6368b37b94f4e71	Custom TCP	TCP	23	Custom	<input type="text"/>	<input type="button" value="Delete"/>
				<input type="text" value="0.0.0.0/0"/>		

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



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 <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	
sgr-0b206fcd92ed62477	SSH	TCP	22	Custom	<input type="text"/>
				<input type="text" value="0.0.0.0/0"/>	

- Seleccionamos como dirección IP permitida, explícitamente la perteneciente a nosotros.

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 <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>
sgr-0b206fcd92ed62477	SSH	TCP	22	My IP

[Add rule](#)

- Luego vamos al Assessment-Template-Network en el inspector y le damos a run.
- y debería salir un mensaje con un texto en
- verde que diga Success.

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

Filter 1 selected

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

Assessment Template - Assessment-Template-Network

**Name** Assessment-Template-Network

**ARN** arn:aws:inspector:us-west-2:851725211238:target/0-sxeFndPA/template/0-RjGipH9V

**Target name** Network-Audit [Preview Target](#)

**Rules packages** Common Vulnerabilities and Exposures-1.1  
Network Reachability-1.1  
CIS Operating System Security Configuration Benchmarks-1.0  
Security Best Practices-1.0

[Preview Exclusions](#)

**Duration** 15 Minutes

**SNS topics** ☒

**Assessment Events** ☒ Click below to set up recurring assessment runs once every  days, with the first run starting now. [Learn more](#)

[Add schedule](#)

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure.

[Learn more](#) [Start your free trial](#)

✓ SUCCESS

Assessment run started

## Amazon Inspector - Assessment Templates

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.](#)

Create

Run

Delete

Clone

Create Assessment Events

Filter

	Name	Duration	Target name
<input type="checkbox"/>	Assessment-Template-Network	15 Minutes	<a href="#">Network-Audit</a>

- Luego en Assessment runs, vemos como al negar el ingreso desde cualquier IP, y a través del protocolo Custom TCP, desaparece una de las vulnerabilidades.

Dashboard

Assessment targets

Assessment templates

Assessment runs

Findings

Switch to Inspector V2

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure.

[Learn more](#) [Start your free trial](#)

## 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 selected rules packages. [Learn more.](#)

Run

Cancel

Delete

Filter

Last updated on May 13, 2024 7:30:29 PM (0m ago)

«

<

Viewing 1-2 of 2

>

»

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 7:29 PM (GMT-3) (a few ...	Analysis complete	<a href="#">Assessment-Template-Network</a>	2	<a href="#">High</a>   <a href="#">Medium</a>   <a href="#">Low</a>   <a href="#">Info</a>	2	<a href="#">Download report</a>
<input type="checkbox"/>	Today at 7:14 PM (GMT-3) (16 mi...	Analysis complete	<a href="#">Assessment-Template-Network</a>	3	<a href="#">High</a>   <a href="#">Medium</a>   <a href="#">Low</a>   <a href="#">Info</a>	2	<a href="#">Download report</a>

Max records per page:

25

\* refresh browser to reflect changes

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more.](#)

[Add/Edit attributes](#)

▼ Filter

<input type="checkbox"/>	Severity ⓘ	Date ▲	Finding	Target	Template	Rules Package
<input type="checkbox"/>	Informational	Today at 7:1...	Aggregate network exposure: On instance i-08b62...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 7:1...	On instance i-08b62ba1fd34b4144, TCP port 22 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	High	Today at 7:1...	On instance i-08b62ba1fd34b4144, TCP port 23 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informational	Today at 7:3...	Aggregate network exposure: On instance i-08b62...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 7:3...	On instance i-08b62ba1fd34b4144, TCP port 22 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

- En el panel de navegación, seleccione Findings y luego Date para ordenar por los hallazgos más recientes. El hallazgo de severidad alta ya no está, pero el hallazgo de severidad media sigue ahí. Aunque el puerto 22 redujo su alcance para permitir acceso solo a su dirección IP, el puerto 22 técnicamente sigue abierto para el Internet fuera del VPC.

# TAREA 5: REEMPLAZAR BASTIONSERVER CON SYSTEMS MANAGER

- En esta tarea, se reemplazó la instancia de BastionServer, que usaba principalmente SSH para conectarse a AppServer dentro de la subred privada. En su lugar, se usará Session Manager mediante Systems Manager.
- Systems Manager es una solución de administración integral segura para entornos de nube híbrida. Systems Manager es el concentrador de operación para sus aplicaciones y recursos de AWS y consta de cuatro grupos de funciones.

Borramos la regla de entrada con protocolo SSH que tenia la instancia y guardamos los cambios.

**Edit inbound rules** [Info](#)  
Inbound rules control the incoming traffic that's allowed to reach the instance.

**Inbound rules** [Info](#)  
  

This security group has no inbound rules.

Add rule

Cancel

Preview changes

Save rules



- Ingresamos a Session Manager para poder interactuar con nuestra instancia EC2 a través de una ventana interactiva basada en Shell.

## Session Manager

 Systems Manager feature

### Specify target

Select an instance to connect to using Session Manager.


#### Reason

Reason for session – *optional*

The reason for connecting to the instance. This value is included in the details of the event created by AWS CloudTrail when you start the session.

This value can have up to 256 characters.

#### Target instances

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input checked="" type="radio"/>	AppServer	i-0f116b54b5a277da5	3.3.131.0	 running	us-west-2a	Amazon Linux

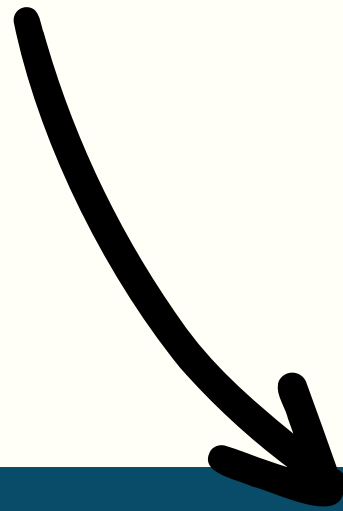
Start session

Cancel

Next

- Seleccione la casilla junto a AppServer, y luego seleccione Start session, así nos conectaremos a AppServer directamente

Vemos que podemos interactuar  
correctamente mediante comandos Shell,  
con nuestra instancia EC2



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

- Realizamos un último chequeo de seguridad con Amazon Inspector, y vemos como todas las vulnerabilidades previamente detectadas han desaparecido al borrar las reglas de ingreso a través del protocolo SSH.

### 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 selected rules packages. [Learn more.](#)

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

Filter

<input type="checkbox"/>	Start time	Status
<input checked="" type="checkbox"/>	▶ Today at 7:29 PM (GMT-3) (9 min...	Analysis complete
<input type="checkbox"/>	▶ Today at 7:14 PM (GMT-3) (24 mi...	Analysis complete

### 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 selected rules packages. [Learn more.](#)

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

Filter

<input type="checkbox"/>	Start time	Status	Template name	Findings	Findings by severity
<input type="checkbox"/>	▶ Today at 7:39 PM (GMT-3) (a few ...	Collecting data	<a href="#">Assessment-Template-Network</a>	0	
<input type="checkbox"/>	▶ Today at 7:29 PM (GMT-3) (10 mi...	Analysis complete	<a href="#">Assessment-Template-Network</a>	2	<a href="#">High</a>   <a href="#">Medium</a>   <a href="#">Low</a>   <a href="#">Info</a>
<input type="checkbox"/>	▶ Today at 7:14 PM (GMT-3) (25 mi...	Analysis complete	<a href="#">Assessment-Template-Network</a>	3	<a href="#">High</a>   <a href="#">Medium</a>   <a href="#">Low</a>   <a href="#">Info</a>

Ingresamos al último chequeo de seguridad en detalles, y vemos como se han eliminado todas las advertencia de seguridad.

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 selected rules packages. [Learn more.](#)

RunCancelDelete

Last updated on May 13, 2024 7:39:24 PM (0m ago)

Filter

«<Viewing 1-3 of 3>»

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 7:39 PM (GMT-3) (a few ...	Collecting data	<a href="#">Assessment-Template-Network</a>	0		1	

Assessment - Run - Assessment-Template-Network - 2024-05-13T22:39:21.966Z

ARN

arn:aws:inspector:us-west-2:851725211238:target/0-sxeFndPA/template/0-RjGipH9V/run/0-mCu2qveX

Start

Today at 7:39 PM (GMT-3) (a few seconds ago)

Target name

[Network-Audit](#)

Template name

[Assessment-Template-Network](#)

Rules packages

[Common Vulnerabilities and Exposures-1.1](#)

[Network Reachability-1.1](#)

[CIS Operating System Security Configuration Benchmarks-1.0](#)

[Security Best Practices-1.0](#)

Duration

15 Minutes

Status

Collecting data

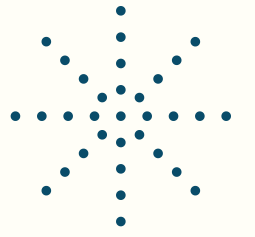
Findings

0

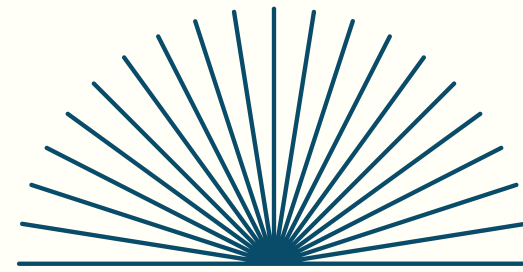
Show AWS agents

Show status

# CONCLUSIONES



- Configuramos satisfactoriamente Amazon Inspector.
- Ejecutamos una auditoría de red sin agente.
- Investigamos los resultados del análisis.
- Actualizamos los grupos de seguridad.
- Iniciamos sesión en un servidor de aplicación usando Session Manager



# Gracias por su atención

Ignacio Suarez, Michelle Devera, Manuela Rodríguez, Juan Sansberro,  
Esteban Camejo, Santiago Burgueño