

LAB
276

Refuerzo de red con
Amazon Inspector y
AWS Systems Manager



Objetivos:

-  Configurar Amazon Inspector.
-  Ejecutar una auditoría de red sin agentes.
-  Investigar los resultados del escaneo.
-  Actualizar grupos de seguridad.
-  Iniciar sesión en una instancia del servidor de aplicaciones mediante AWS Systems Manager Session Manager.

Visualizar instancia EC2 y agregar etiquetas

Después de ingresar a la consola de AWS seleccionamos el servicio EC2 y nos movemos a instancias en donde podremos apreciar dos instancias en ejecución **BastionServer** y **AppServer**. Seleccionamos **BastionServer** y bajamos a la pestaña Tags, seleccionamos administrar y agregamos una tarjeta

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	
cloudlab	c110983a263229016677763t1w	Remove
Name	BastionServer	Remove
SecurityScan	true	Remove

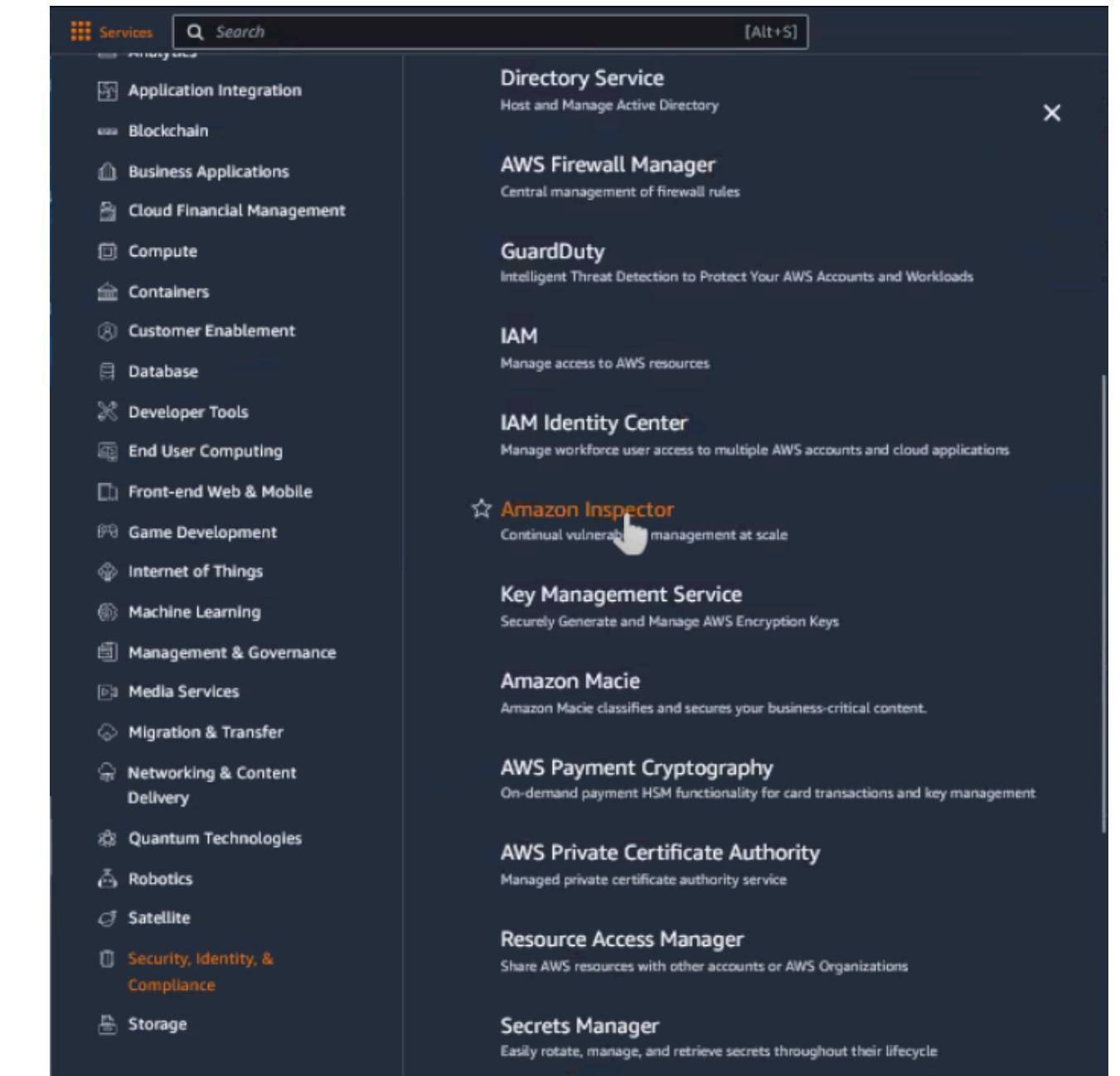
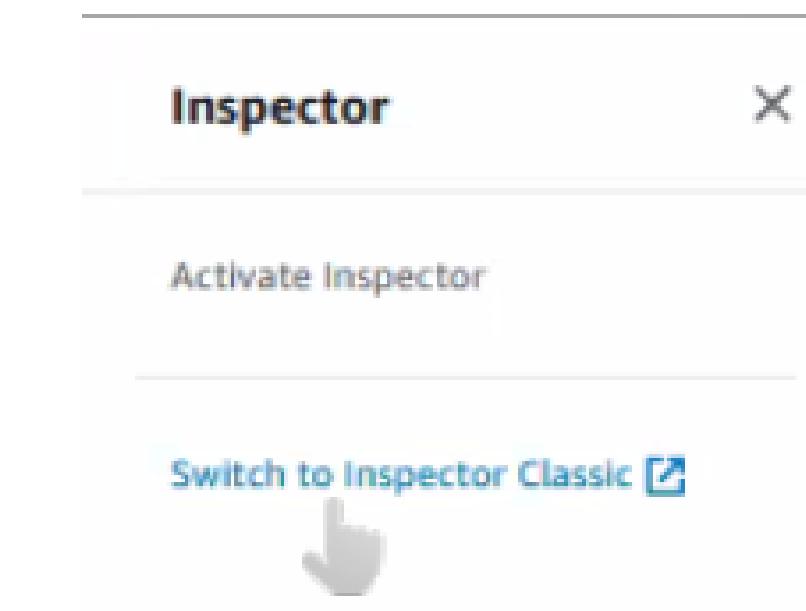
[Add new tag](#)

You can add up to 47 more tags.

Configuramos y ejecutamos Amazon Inspector



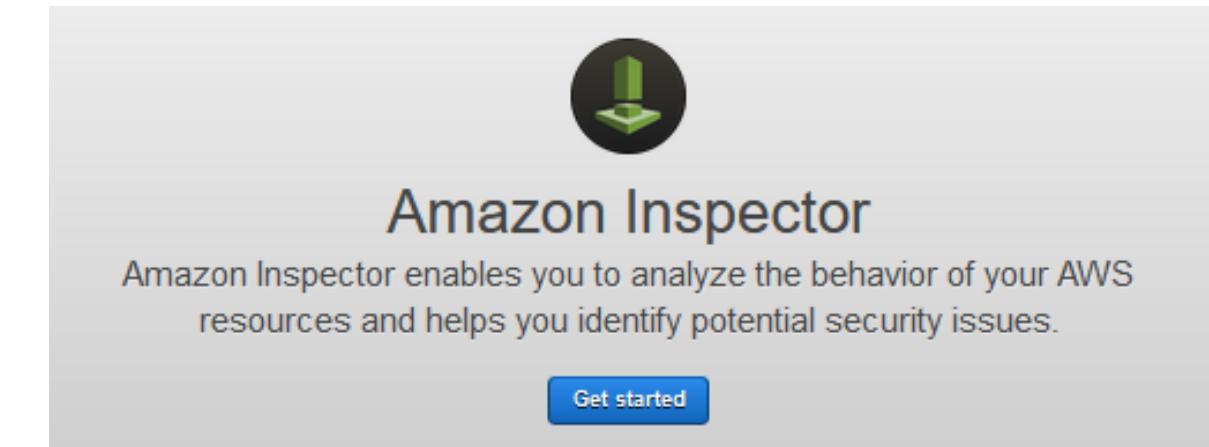
En el menú de servicios de AWS seleccionamos **Security, Identity, & Compliance**, aquí encontraremos **Amazon Inspector**. Después de ingresar abrimos el panel de navegación y seleccionamos Switch to Inspector Classic





Configuramos y ejecutamos Amazon Inspector

Ahora seleccionamos **Get Started** y navegamos a **Advanced setup** y configuramos **Define an assessment target** y seleccionamos next



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](#)

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

Cancel

Next



Configuramos y ejecutamos Amazon Inspector

Ahora seleccionamos **Define an assessment template** y la configuramos. Al terminar le damos next y luego **Create**

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* 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**

Configuramos y ejecutamos Amazon Inspector

Verificamos el estado de análisis y en el panel de navegación izquierdo seleccionamos **Assessment runs**, expandimos y accedemos a más opciones para la ejecución. Luego, para ver el estado de la ejecución seleccionamos **Show status** y para cerrar seleccionamos **Close**. Cuando el estado cambie a **Analysis complete** seleccionamos **Findings**.

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	Last updated on May 13, 2024 7:27:03 PM (0m ago)	Filter	Viewing 1-1 of 1	
Start time	Status	Template name	Findings	Findings by s...	Exclusions	Reports
Today at 7:26 P...	Analysis complete	Assessment-Te...	3	High Medium ...	2	Download re...

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 7:28:53 PM (1m ago)	Filter	Viewing 1-3 of 3		
Severity	Date	Finding	Target	Template	Rules Packa
High	Today at 7:2...	On instance i-0be98a1102fc04571, TCP port 23 w...	Network-Audit	Assessment-Templ...	Network Reac
Medium	Today at 7:2...	On instance i-0be98a1102fc04571, TCP port 22 w...	Network-Audit	Assessment-Templ...	Network Reac
Informational	Today at 7:2...	Aggregate network exposure: On instance i-0be98...	Network-Audit	Assessment-Templ...	Network Reac



Analizar los hallazgos de Amazon Inspector

Expandimos los detalles para ver los hallazgos de alta gravedad, deberían verse de los siguientes detalles clave:

AWS agent ID [i-0be98a1102fc04571](#)

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-0be98a1102fc04571](#) is located in VPC [vpc-02de6bdc523e98a17](#) and has an attached ENI [eni-0d6245adad7825e37](#) which uses network ACL [acl-0ce9f2dae15411e7a](#). The port is reachable from the internet through Security Group [sg-0b4010be6c68aa931](#) and IGW [igw-0350797d7a29a2f4e](#)

Recommendation You can edit the Security Group [sg-0b4010be6c68aa931](#) to remove access from the internet on port 23

Actualizar grupos de seguridad

Expandimos nuevamente la pestaña para ver los hallazgos de alta gravedad y dentro de la sección “**Recommendation**” seleccionamos el link al grupo de seguridad. Dentro de éste, seleccionamos la pestaña **Inbound Rules** y las editamos.

- Para el port 23, seleccionamos **Delete**.

The screenshot shows the AWS Management Console interface for security groups. At the top, there's a search bar and a filter for 'Security group ID = sg-0b4010be6c68aa931'. Below the search bar, there's a table with columns: Name, Security group ID, Security group name, VPC ID, and Description. One row is visible for 'BastionServerSG' with the ID 'sg-0b4010be6c68aa931', name 'c110983a2632290l6677763t1w2111...', VPC ID 'vpc-02de6bdc523e98a17', and description 'security group'.

- Para la regla SSH, removeremos el inbound IP por defecto y seleccionamos nuestra IP (**Source: My IP**) y guardamos.

The screenshot shows the 'Inbound rules' section for the 'BastionServerSG' security group. It has a table with columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. One rule is listed: 'sgr-0bcec2776c5aa6729' with Type 'SSH', Protocol 'TCP', Port range '22', Source 'My IP', and Description '167.56.193.161/32'. Below the table is a button labeled 'Add rule'.



Last updated on May 13, 2024 7:38:58 PM (0m ago)

Viewing

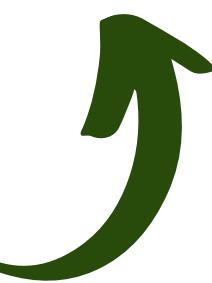
Run Delete Clone Create Assessment Events

Name	Duration	Target name	Last run
Assessment-Template-Network	15 Minutes	Network-Audit	Analysis complete

Volvimos a correr el mismo proceso de amazon inspector, debería salir **Analysis complete**.

En **high-severity** desapareció, pero en **medium-severity** permanece.
Aunque el **puerto 22** se redujo para permitir el acceso solo a su dirección IP, el **puerto 22** sigue técnicamente abierto a Internet fuera de la VPC.

Para resumir esto último, se actualizó el grupo de seguridad adjunto a BastionServer para que permita el tráfico solo desde su dirección IP en lugar de Internet abierto y se eliminó el puerto Telnet abierto ya que no es necesario.



Reemplazar BastionServer con Systems Manager

En la consola elegimos en servicio EC2 y seleccionamos **Security Groups**. Seleccionamos **Security group ID** para **BastionServerSG**. Luego seleccionamos **Edit inbound rules** y elegimos **Delete** y luego **Save rules** para eliminar la regla de entrada de SSH.

The screenshot shows the 'Connect to instance' page for an EC2 instance. At the top, there are four tabs: 'EC2 Instance Connect' (selected), 'Session Manager', 'SSH client', and 'EC2 serial console'. A yellow warning box is present, stating: 'Port 22 (SSH) is not authorized. Port 22 (SSH) is currently not authorized by your security group. To use EC2 Instance Connect, you must authorize port 22 for the EC2 Instance Connect service IP addresses in your Region: 18.237.140.160/29.' Below the tabs, the 'Instance ID' is listed as 'i-020560a7797accfc5 (AppServer)'. Under 'Connection Type', the 'Connect using EC2 Instance Connect' option is selected. Other connection options shown are 'Public IP address' (35.89.133.119) and 'Username' (ec2-user). The URL in the browser is 'EC2 > Instances > i-020560a7797accfc5 > Connect to instance'. On the right side, another 'Connect to instance' page is shown with the 'Session Manager' tab selected. It includes a section titled 'Session Manager usage:' with the following bullet points:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager Preferences [page](#).

Regresamos y seleccionamos la instancia BastionServer y la detenemos. Ahora nos conectamos a AppServer directamente usando Session Manager

Utilizamos un Shell interactivo para verificar los últimos pasos

Accedemos de forma rápida y segura a la instancia de EC2 mediante un **shell interactivo basado en navegador** de un solo clic o mediante AWS Command Line Interface (AWS CLI) sin la necesidad de abrir puertos entrantes, mantener hosts de bastión o administrar claves SSH.

```
sh-4.2$ cd ~  
sh-4.2$ pwd  
/home/ssh-user  
sh-4.2$ █
```



Escaneo final del entorno

	Start time	Status	Template name	Findings
	Today at 8:18 PM (GMT-3)	Analysis complete	Assessment-Template-N...	0

Para concluir, ha mejorado con éxito la seguridad de la red al agregar una función de **IAM** al **AppServer** y eliminar la regla de entrada SSH dentro del grupo de seguridad de **Bastion**, al tiempo que facilita aún más la conexión mediante el **Session Manager** proporcionado por **Systems Manager**.



AIC

Gracias por ver!

Agustín Rodríguez, Sony Etcheverry,
Tatiana Rosa, Fidel Fernández
Gabriel Porley, Felipe Barceló