LAB

276

Refuerzo de red con Amazon Inspector y AWS Systems Manager

INEFOP

FORGE FUNDACIÓN

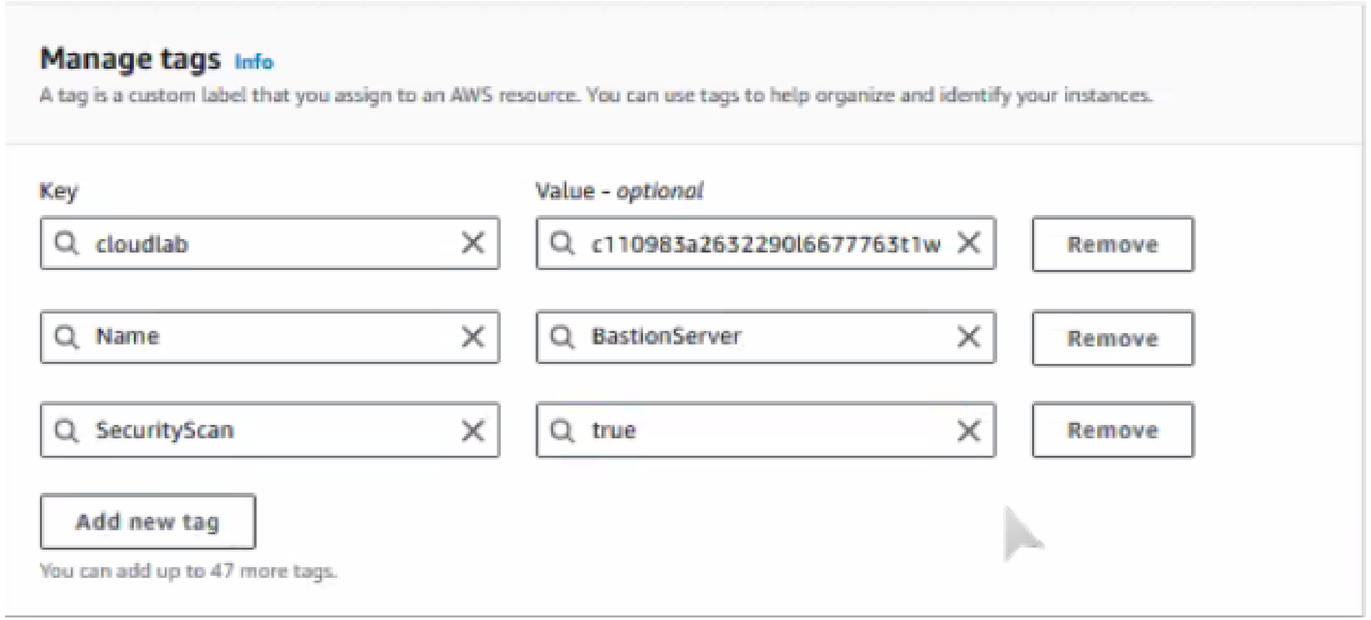
aws

Objetivos:

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

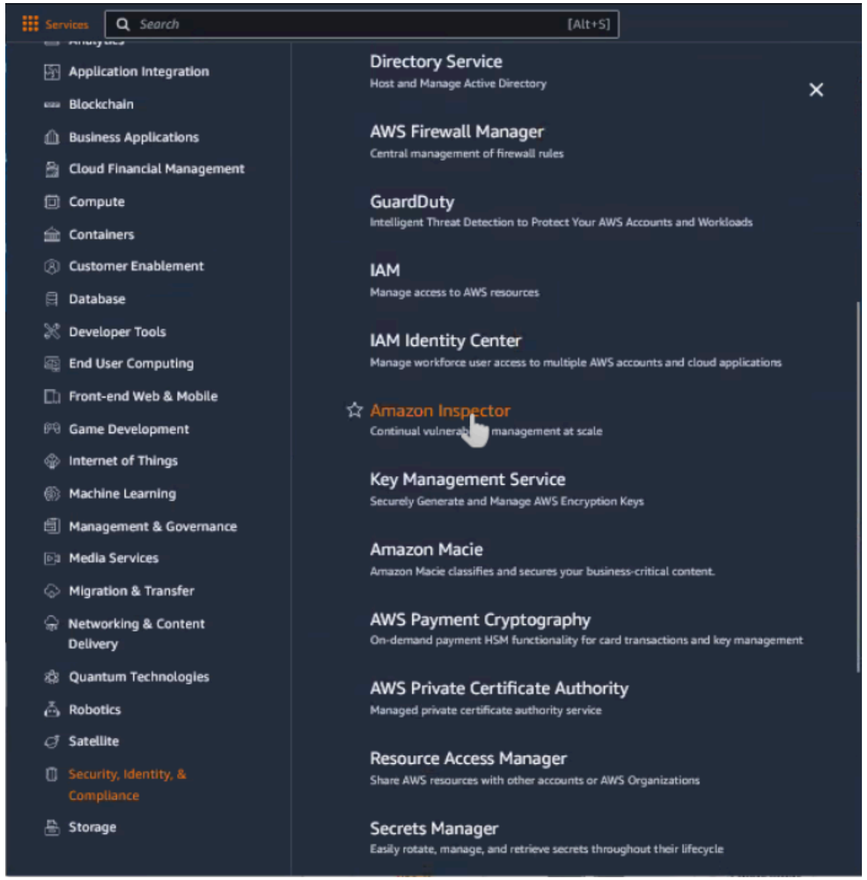
Visualizar instancia EC2 y agregar etiquetas

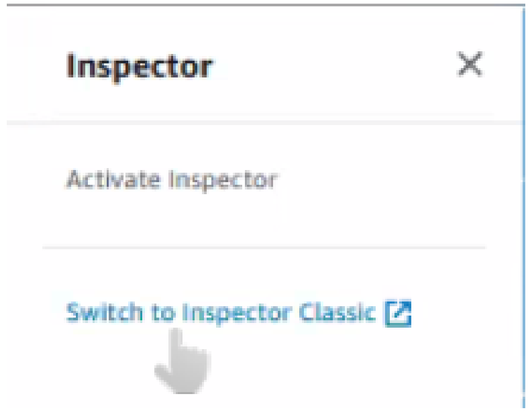
Después de ingresar a la consola de AWS seleccionamos el servicio EC2 y nos movemos a instancias en donde podremos apreciar dos instancias en ejecución **BastionServer y AppServer.** Seleccionamos **BastionServer** y bajamos a la pestaña Tags, seleccionamos administrar y agregamos una tarjeta



Configuramos y ejecutamos Amazon Inspector

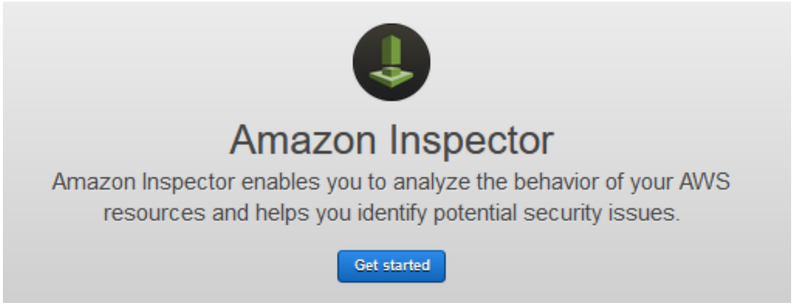
En el menú de servicios de AWS seleccionamos **Security, Identity, & Compliance,** aquí encontraremos **Amazon Inspector.** Después de ingresar abrimos el panel de navegación y seleccionamos Switch to Inspector Classic

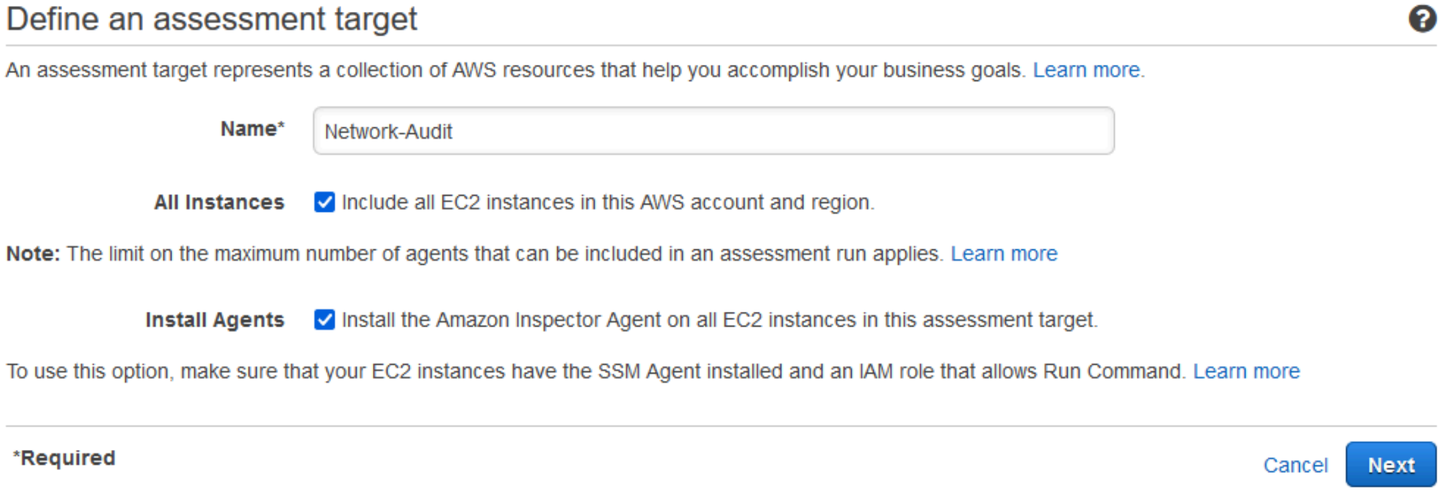




Configuramos y ejecutamos Amazon Inspector

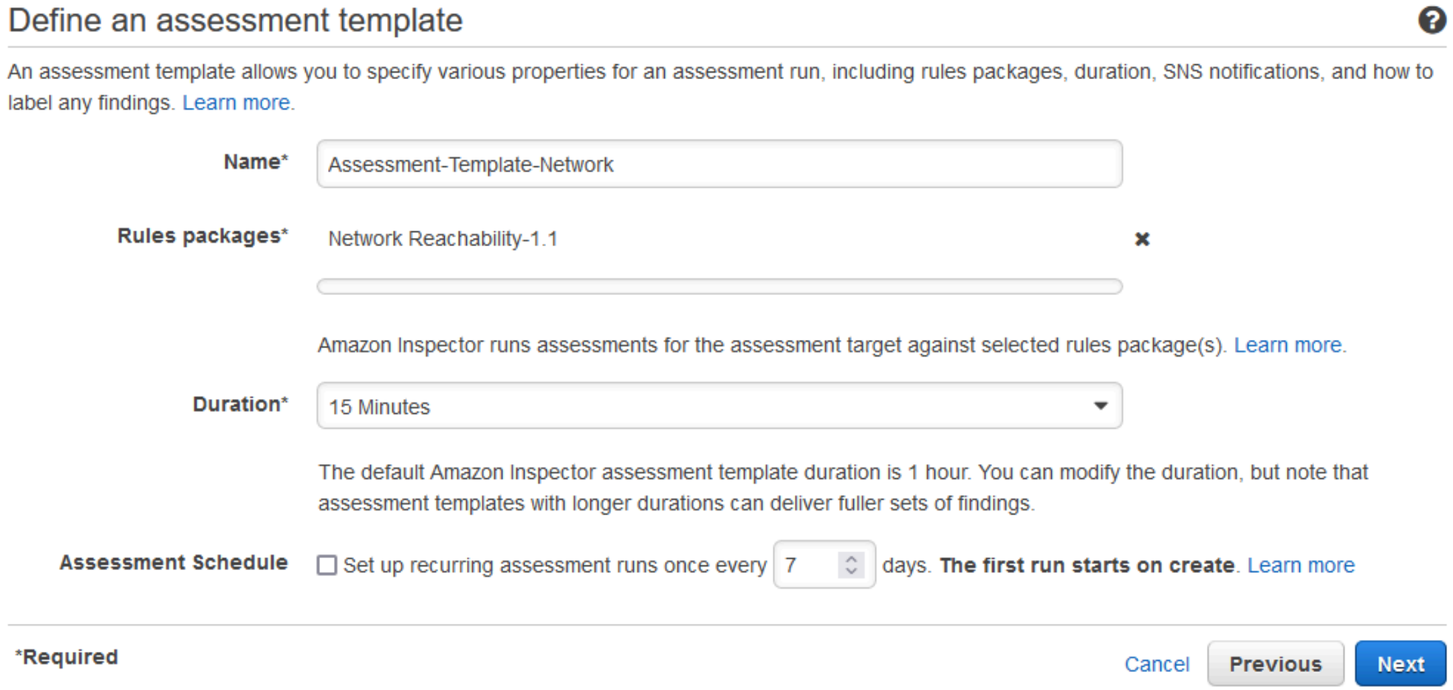
Ahora seleccionamos **Get Started** y navegamos a **Advanced setup** y configuramos **Define an assessment target** y seleccionamos next





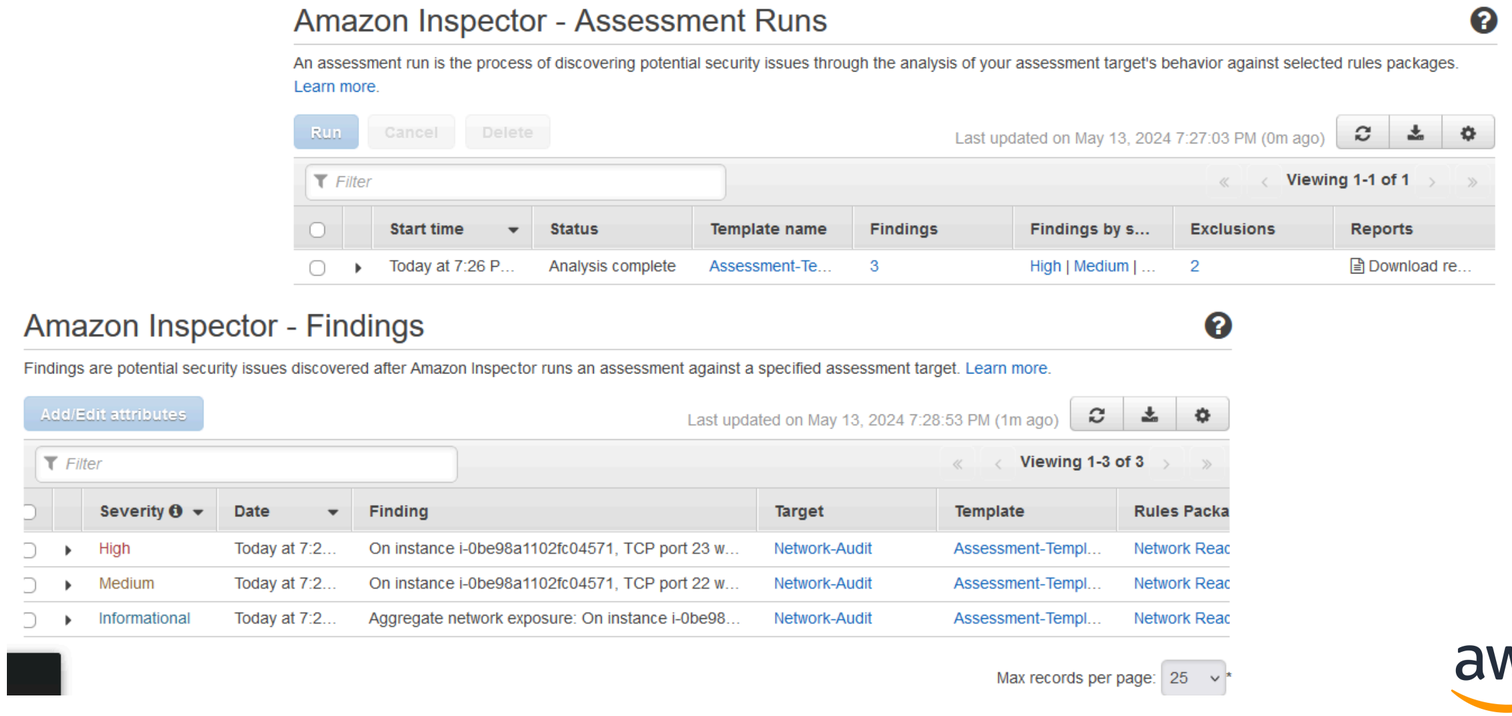
Configuramos y ejecutamos Amazon Inspector

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



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.**



Analizar los hallazgos de Amazon Inspector

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

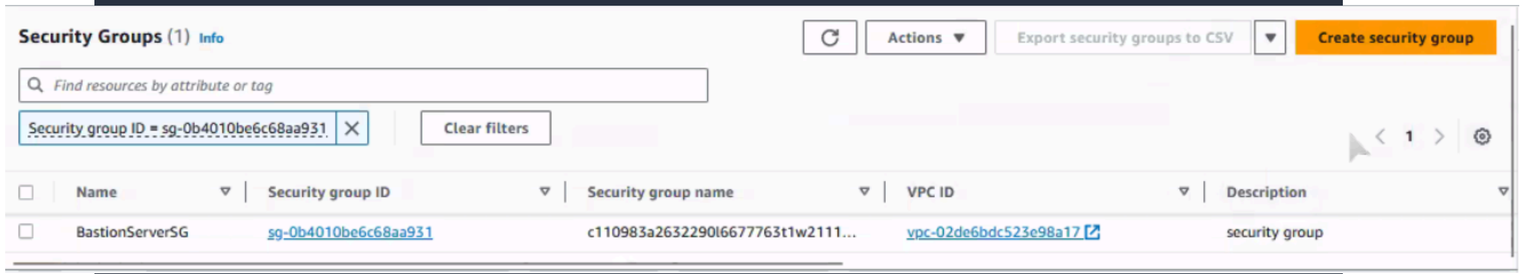
AWS agent ID	i-0be98a1102fc04571

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

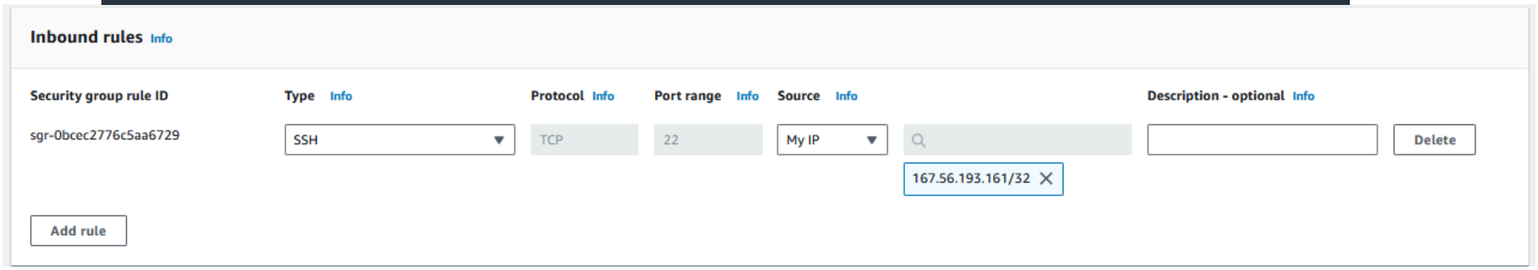
Actualizar grupos de seguridad

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**.



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



Run | Delete | Clone | Create Assessment Events

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

1 selected

Viewing

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

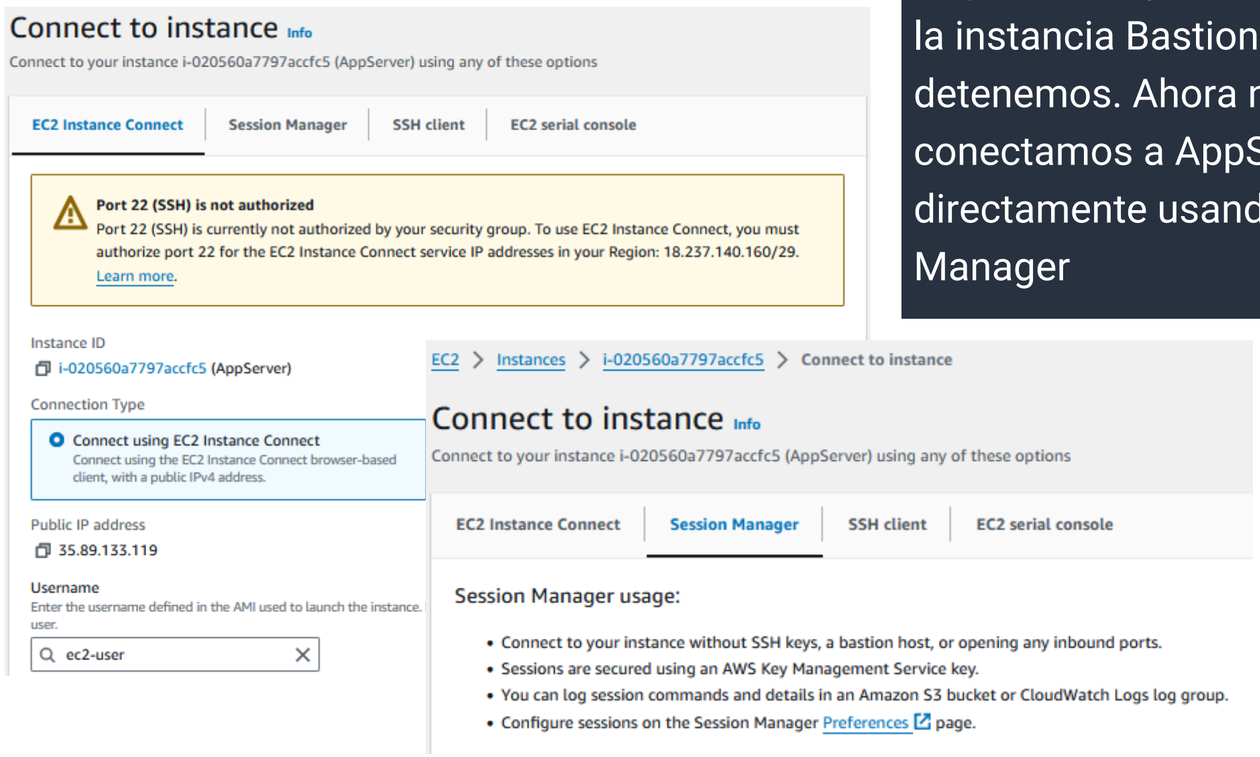
Volvimos a correr el mismo proceso de amazon inspector, debería salir **Analysis complete**.
En **high-severity** desapareció, pero en medium-severity permanece.
Aunque el **puerto 22** se redujo para permitir el acceso solo a su dirección IP, el **puerto 22** sigue técnicamente abierto a Internet fuera 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

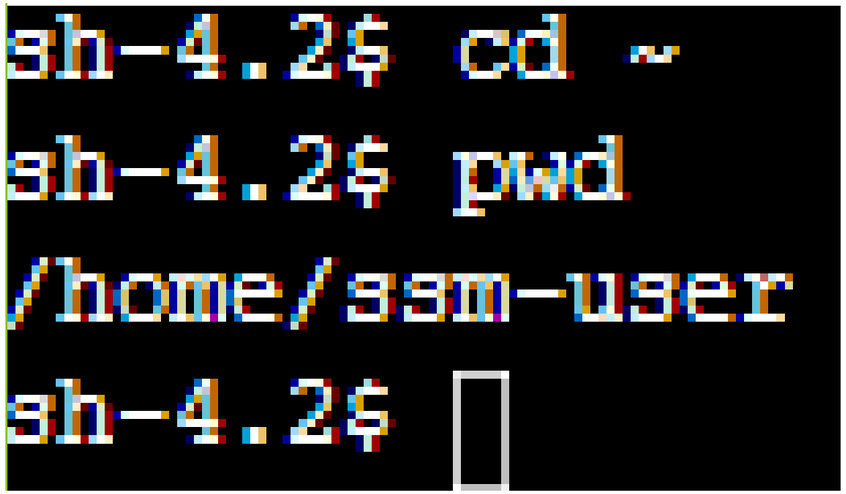
En la consola elegimos en servicio EC2 y seleccionamos **Security Groups**. Seleccionamos **Security group ID** para **BastionServerSG**. Luego seleccionamos **Edit inbound rules** y elegimos **Delete** y luego **Save rules** para eliminar la regla de entrada de SSH.

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.



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**.

Gracias por ver!

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