

Ivan Castillo

SE1: Laboratorio: Endurecimiento de la red

Información general sobre el laboratorio

Asegurar una infraestructura puede ser un reto para cualquier empresa. Las empresas usan muchas herramientas para auditar redes y encontrar vulnerabilidades en los sistemas y aplicaciones. Este proceso toma mucho tiempo y esfuerzo.

En este laboratorio, usted es un nuevo ingeniero de seguridad para AnyCompany. Tiene que identificar áreas débiles de la seguridad de red de la empresa y actualizar el entorno de AnyCompany para una mejor eficiencia y optimización. Ahora usará Amazon Inspector para hacerlo.

Amazon Inspector realiza análisis de todas sus configuraciones de red, como grupos de seguridad, listas de control de acceso de red (ACL de red), tablas de ruta y gateways de Internet, juntas para inferir la accesibilidad. No necesita enviar paquetes a través de la red de nube virtual privada (VPC) o conectarse a los puertos de red de una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Es como un mapeo y reconocimiento de red sin paquetes.

Desde Amazon Inspector, usará el **paquete de accesibilidad de red** para analizar sus configuraciones de red para encontrar vulnerabilidades de seguridad en sus instancias de EC2. Los hallazgos que genera Amazon Inspector también proporcionan orientación acerca de restringir el acceso que no es seguro.

OBJETIVOS

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 una estancia del servidor de aplicación usando AWS Systems Manager Session Manager

ENTORNO DE LABORATORIO

El siguiente entorno tiene dos instancias de EC2. Una instancia es un servidor bastión llamado **BastionServer** en una subred pública. La otra instancia es un servidor de aplicación llamado **AppServer** en una subred privada.

Los servidores bastión son servidores que se usan para administrar el acceso a una red interna o privada desde una red externa. A veces se conocen como cajas de salto o servidores de salto. Dado que los servidores bastión suelen ser accesibles desde Internet, normalmente ejecutan una cantidad mínima de servicios para reducir su superficie de ataque. También se usan con frecuencia para comunicaciones de proxy y de registro, como sesiones de Secure Shell (SSH).

Todos los componentes de backend, como Amazon EC2, los roles AWS Identity and Access Management (IAM) y los servicios de Amazon Web Services (AWS), ya se incluyeron en su laboratorio.

Tarea 1: Ver instancias de EC2 y agregar etiquetas

Para crear un objetivo de evaluación para Amazon Inspector Classic para evaluar, debe comenzar por etiquetar las instancias de EC2 que desea incluir en su objetivo. En esta tarea, etiquetará la instancia de BastionServer.

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**.

1. En la Consola de administración de AWS, seleccione **Services (Servicios)** y seleccione **EC2**.
2. Si ve **New EC2 Experience** (Nueva experiencia de EC2) en la parte superior izquierda de su pantalla, confirme que **New EC2 Experience** esté seleccionado. Este laboratorio está diseñado para utilizar la nueva consola de Amazon EC2.
3. En el panel de navegación izquierdo, elija **Instances** (Instancias).

Instancias (2) Información

🔍

Buscar Instance por atributo o etiqueta (case-sensitive)












Any state

▼

Estado de la instancia = running

✕

Quitar los filtros

<input type="checkbox"/>	Name  ▼	ID de la instancia	Estado de la i... ▼	Tipo de inst... ▼	Comprobación de	Estado de la al
<input type="checkbox"/>	AppServer	i-04342a8b7248b238d	 En ejecución  	t2.micro	 2/2 comprobaci	View alarms 
<input type="checkbox"/>	BastionServer	i-00d2501c5cb30593f	 En ejecución  	t2.micro	 2/2 comprobaci	View alarms 

Se listan las instancias de EC2 de **BastionServer** y **AppServer** en ejecución.

4. Seleccione la instancia de **BastionServer**.
5. Seleccione la pestaña **Tags** (Etiquetas).
6. Seleccione **Manage Tags** (Administrar etiquetas).
7. Seleccione **Add tag** (Agregar etiqueta) y luego ingrese la siguiente información:

- Clave: **SecurityScan**
- Valor: **true**

8. Seleccione ****Save**** (Guardar).

Administrar etiquetas [Información](#)

Las etiquetas son rótulos personalizados que se asignan a un recurso de AWS. Puede utilizar etiquetas para organizar e identificar las instancias.

Clave

Valor - *opcional*

Eliminar

Agregar nueva etiqueta

Puede agregar hasta 49 etiquetas más.

Cancelar

Guardar

RESUMEN DE LA TAREA 1

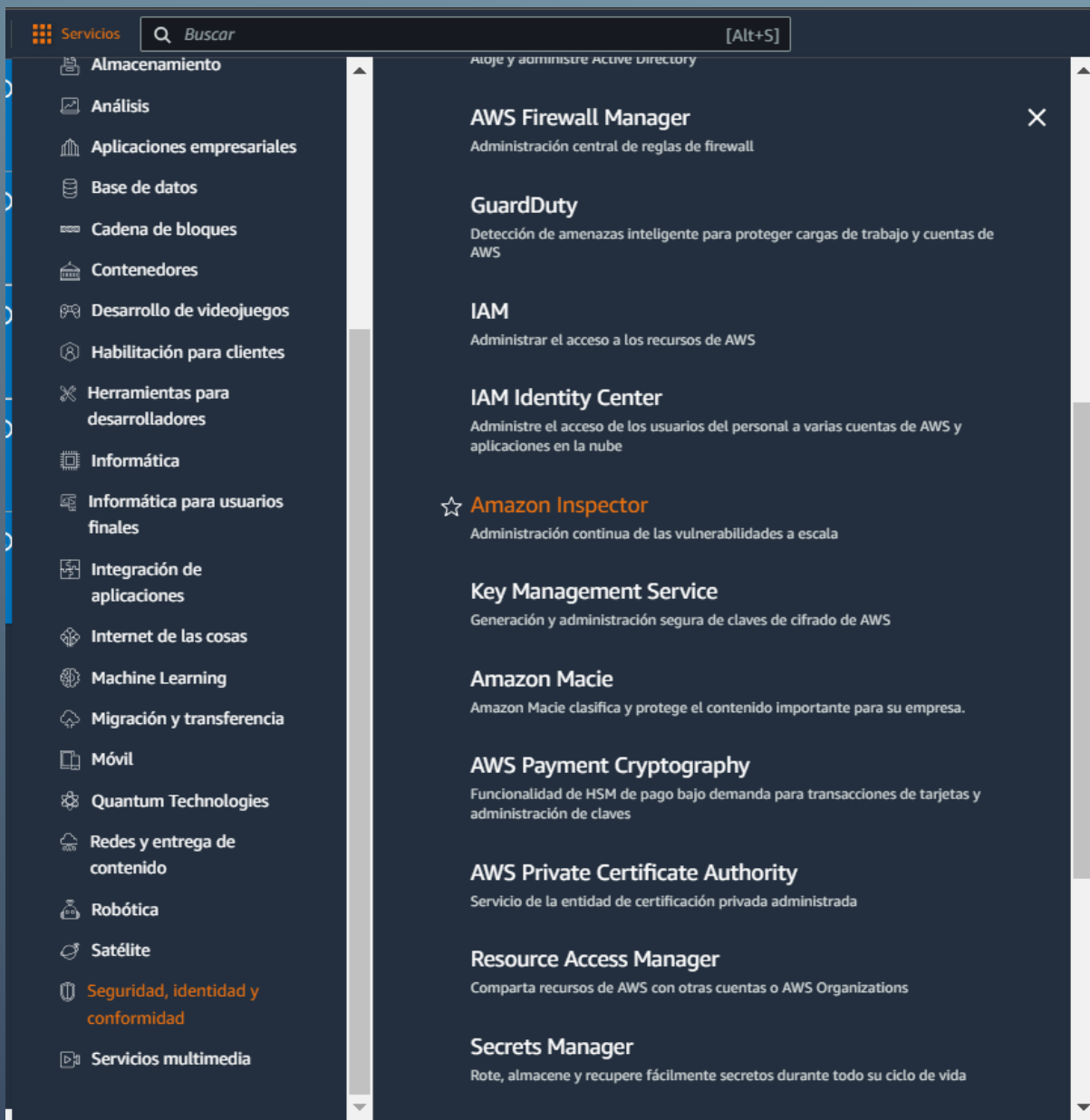
Aplicó correctamente etiquetas para la instancia de BastionServer, lo que permite que el análisis de seguridad detecte y analice esta instancia.

Tarea 2: Configurar y ejecutar Amazon Inspector

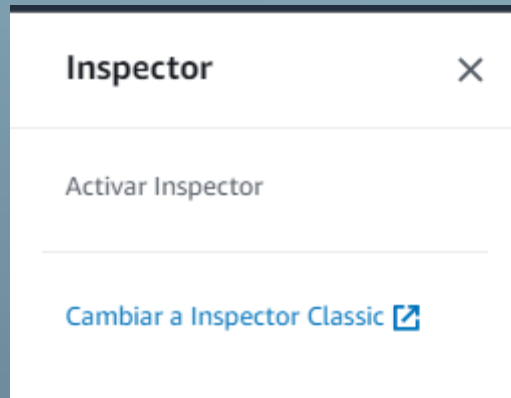
En esta tarea, aprenderá a ejecutar una auditoría de red sin agente en sus instancias de EC2 usando Amazon Inspector. Para este laboratorio, usará el paquete de reglas de accesibilidad de red.

Caso de uso: Es posible que no se puedan instalar agentes en todos los hosts en su implementación. No todos los tipos de sistemas operativos son compatibles con agentes de Amazon Inspector. Usando este método, podrá realizar auditorías de red en todos los hosts.

9. En la **Consola de administración de AWS**, luego seleccione el menú **Services** (Servicios). Luego seleccione **Security, Identity, & Compliance** (Seguridad, identidad y conformidad) y seleccione **Inspector**.



10. Para abrir el panel de navegación, seleccione a la izquierda.
11. Seleccione **Switch to Inspector Classic** (Cambiar a Inspector Classic)



12. Seleccione **Get Started** (Comenzar).



13. Seleccione **Advanced setup** (Configuración avanzada).
14. En la sección **Define an assessment target** (Definir un objetivo de evaluación), configure las siguientes opciones:

- En **Name** (Nombre), ingrese **Network-Audit**
- Cancele la selección de la casilla para **All Instances** (Todas las instancias).
- Para **Tags: Key** (Etiquetas: Clave), seleccione **SecurityScan**.
- Para **Tags: Value** (Etiquetas: Valor), seleccione **true**.
- Cancele la selección de la casilla para **Install Agents** (Instalar agentes).

Definir un objetivo de evaluación

Un objetivo de evaluación representa una colección de recursos de AWS que le ayudan a lograr sus objetivos empresariales. [Más información.](#)

Nombre*

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](#)

Etiquetas*

Clave	Valor
SecurityScan	true
Añada una clave nueva	

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](#)

15. Seleccione ****Next**** (Siguiente).

16. En la sección **Define an assessment template** (Definir una plantilla de evaluación), configure las siguientes opciones:

- En **Name** (Nombre), ingrese **Assessment-Template-Network**
- En **Rules packages** (Paquetes de reglas), deje **Network Reachability-1.1** (Accesibilidad de red: 1.1) seleccionado, pero seleccione junto a cada uno de los otros paquetes para quitarlos.
- Para **Duration** (Duración), seleccione **15 Minutes** (15 minutos).
- Cancele la selección de la casilla para **Assessment Schedule** (Cronograma de evaluaciones).

Definir una plantilla de evaluación

Una plantilla de evaluación le permite especificar diversas propiedades para una ejecución de evaluación, incluidos los paquetes de reglas, la duración, las notificaciones SNS y cómo etiquetar cualquier hallazgo. [Más información.](#)

Nombre*

Paquetes de reglas* ✕

Amazon Inspector realiza las evaluaciones del objetivo de evaluación especificadas en los paquetes de reglas seleccionados. [Más información.](#)

Duración*

La duración predeterminada de la plantilla de evaluación de Amazon Inspector es de 1 hora. Puede modificar la duración, pero tenga en cuenta que las plantillas de evaluación con duración más corta proporcionan conjuntos de hallazgos más completos.

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

17. Seleccione ****Next**** (Siguiente).

18. Seleccione **Create** (Crear).

Debería ver una notificación que dice **SUCCESS** (Correcto), que confirma que se inició la ejecución de la evaluación. Se demora entre 3 y 5 minutos en finalizar. Mientras espera, aprenda más acerca de [Amazon Inspector](#).

Amazon Inspector - Ejecuciones de evaluación				
Una ejecución de evaluación es el proceso de descubrimiento de posibles problemas de seguridad que utiliza los paquetes de reglas seleccionados para analizar el comp				
<div><div>Ejecutar</div><div>Cancelar</div><div>Eliminar</div></div>				
<div>Filtro</div>				
<input type="checkbox"/>	Hora de inicio	Estado	Nombre de la plantilla	Hallazgos
<input type="checkbox"/>		Preparándose para comenzar	Assessment-Template-Network	0

19. Verificar el estado del análisis:

- En el panel de navegación izquierdo, elija **Assessment runs** (Ejecuciones de evaluación).
- En la sección **Amazon Inspector - Assessment Runs** (Amazon Inspector: Ejecuciones de evaluación), seleccione el en la fila para la ejecución que inició para expandirla y acceder a más opciones para su ejecución.
- Para ver el estado de la ejecución, seleccione **Show status** (Mostrar estado). Si no ve **Show status** (Mostrar estado), seleccione en la parte superior.
- Para cerrar y volver a la pantalla anterior, seleccione **Close** (Cerrar).

20. Cuando el estado cambie a **Analysis complete** (Análisis completo), seleccione **Findings** (Hallazgos) en el panel de navegación.

Amazon Inspector - Hallazgos						
Los hallazgos son posibles problemas de seguridad detectados por Amazon Inspector durante la ejecución de una evaluación del objetivo de evaluación especificado. Más información.						
Añadir Editar atributos						
<input type="text" value="Filtro"/>						
<input type="checkbox"/>	Gravedad	Fecha	Hallazgo	Objetivo	Plantilla	Paquete de reglas
<input type="checkbox"/>	Alta	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 23 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Alta	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 23 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Alta	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 23 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Media	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 22 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Media	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 22 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Media	Today at 8:4...	On instance i-00d2501c5cb30593f, TCP port 22 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informativa	Today at 8:4...	Aggregate network exposure: On instance i-00d25...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informativa	Today at 8:4...	Aggregate network exposure: On instance i-00d25...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informativa	Today at 8:4...	Aggregate network exposure: On instance i-00d25...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

RESUMEN DE LA TAREA 2

En esta tarea, creó un objetivo de evaluación (una recopilación de los recursos de AWS que desea que Amazon Inspector Classic analice). Luego creó una plantilla de evaluación (un esquema que usa para configurar su evaluación). Usó la plantilla para iniciar una ejecución de evaluación, que es el proceso de supervisión y análisis que produce un conjunto de hallazgos.

Tarea 3: Analizar hallazgos de Amazon Inspector

Los hallazgos que esas reglas generan muestran si sus puertos son accesibles desde Internet mediante un gateway de Internet (incluidas instancias detrás de equilibradores de carga de aplicación o equilibradores de carga clásicos), una interconexión de VPC o una red privada virtual (VPN) mediante un gateway virtual. Estos hallazgos también destacan las configuraciones que permiten potenciales accesos maliciosos, como grupos de seguridad, ACL y gateways de Internet mal administrados.

21. Seleccione para expandir el hallazgo de alta severidad. Debería poder ver los siguientes detalles clave:

- **AWS agent ID** (ID de agente AWS) le muestra la instancia de EC2 afectada.
- **Description** (Descripción) muestra el motivo del hallazgo. En este caso, el puerto TCP 23, que está asociado con Telnet, es accesible desde Internet.
- **Recommendation** (Recomendación) proporciona sugerencias de corrección.

Telnet es una herramienta de emulación de terminal basada en texto que es parte del conjunto de protocolos de TCP/IP. Permite que un sistema se conecte a un host remoto para realizar comandos como si estuviera en la consola del equipo remoto.

Estado	Recopilando datos
Paquete de reglas	Network Reachability-1.1
ID de agente de AWS	i-00d2501c5cb30593f
Hallazgo	On instance i-00d2501c5cb30593f, TCP port 23 which is associated with 'Telnet' is reachable from the internet
Gravedad	High ③
Descripción	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-00d2501c5cb30593f is located in VPC vpc-066b067066942fa10 and has an attached ENI eni-9a749e43f4039800f which uses network ACL acl-02f3935241837ab2e. The port is reachable from the internet through Security Group sg-067e53b6a125c1078 and IGW igw-08778763ba88aae3
Recomendación	You can edit the Security Group sg-067e53b6a125c1078 to remove access from the internet on port 23

22. Seleccione para expandir los hallazgos de severidad media y analizar los detalles.

- Para los hallazgos de severidad media, el puerto TCP 22, que está asociada con SSH, es accesible desde Internet.

SSH, como la herramienta Telnet, le brinda a un usuario la capacidad de iniciar sesión en una máquina remota y realizar comandos como si estuvieran en la consola de ese sistema. Telnet, sin embargo, no es seguro, ya que sus datos no están cifrados cuando se comunican. SSH proporciona un túnel seguro y cifrado para acceder a otro sistema de forma remota.

Estado	Recopilando datos
Paquete de reglas	Network Reachability-1.1
ID de agente de AWS	i-00d2501c5cb30593f
Hallazgo	On instance i-00d2501c5cb30593f , TCP port 22 which is associated with 'SSH' is reachable from the internet
Gravedad	Medium ⓘ
Descripción	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-00d2501c5cb30593f is located in VPC vpc-066b067066942fa10 and has an attached ENI eni-0a749e43f4039800f which uses network ACL acl-02f3935241837ab2e . The port is reachable from the internet through Security Group sg-067e53b6a125c1078 and IGW igw-087787f63ba88aae3
Recomendación	You can edit the Security Group sg-067e53b6a125c1078 to remove access from the internet on port 22

Tarea 4: Actualizar 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.

23. Seleccione para expandir los detalles del hallazgo de alta severidad.
24. En la sección **Recommendation** (Recomendación), seleccione el enlace para el grupo de seguridad. Los enlaces deben ser similares al siguiente ejemplo: **sg-0b2dc685cd6e6e706**. Cuando el enlace se abra, podrá ver que el grupo de seguridad **BastionServerSG** que está adjunto al **BastionServer** que produjo hallazgos dentro de Amazon Inspector.
25. Elija la pestaña **Inbound rules** (Reglas de entrada). Estas son las reglas de entrada actuales para este grupo de seguridad. También son los hallazgos de alto y medio nivel que Amazon Inspector detectó.
26. Seleccione **Edit inbound rules** (Editar las reglas de entrada).

Grupos de seguridad (1/1) Información

Find resources by attribute or tag

Security group ID = sg-067e53b6a125c1078 X Clear filters

<input checked="" type="checkbox"/>	Name	Security group ID	Nombre del grupo de seguridad	ID de la VPC	Descripción
<input checked="" type="checkbox"/>	BastionServerSG	sg-067e53b6a125c1078	LabStack-37ece71c-2d18-43aa-badc-...	vpc-066b067066942fa10	security group

sg-067e53b6a125c1078 - LabStack-37ece71c-2d18-43aa-badc-7e1a03f5f73d-tY7pYoHsNrTdsdGw33M1ji-0-BastionSG-10V433PBM95QA

Detalles Reglas de entrada Reglas de salida Etiquetas

27. Para la regla de entrada asociada con el rango de puertos **23**, seleccione **Delete** (Eliminar). Telnet puerto 23 es vulnerable a ataques de seguridad y el protocolo SSH le ayuda a superar muchos de los problemas de seguridad de Telnet. SSH es actualmente el único protocolo importante que accede a los dispositivos de red y servidores mediante Internet.
28. Para la regla **SSH**, quite la dirección IP de entrada actual de **0.0.0.0/0** seleccionando la **X** a su lado para actualizar el recurso. La dirección IP 0.0.0.0/0 para reglas de entrada significa que el puerto 22 es accesible para cualquier persona en Internet. Puede ajustar las reglas de entrada para que solo su dirección IP pueda acceder al puerto 22. Aunque esta opción es mucho más segura, sigue teniendo vulnerabilidades. Por ejemplo, alguien puede acceder al equipo que está asociado con esa dirección IP y obtener acceso.
29. Para **Source** (Fuente), seleccione la lista desplegable **Custom** (Personalizada) y luego seleccione **My IP** (Mi IP).
30. Seleccione ****Save rules**** (Guardar reglas).

Editar reglas de entrada Información

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>
sgr-0774409c4e0b78301	SSH	TCP	22	Mi IP

Agregar regla

VOLVER A ANALIZAR EL ENTORNO

31. Navegue hasta la pestaña del navegador que tiene Amazon Inspector abierto. En el panel de navegación izquierdo, seleccione **Assessment templates** (Plantillas de evaluación).
32. Seleccione la casilla junto a **Assessment-Template-Network** (Plantilla de evaluación: Red) y seleccione **Run** (Ejecutar).

Este paso ejecuta el mismo análisis anterior en el laboratorio y produce hallazgos desde las actualizaciones del grupo de seguridad. **Nota** El análisis tarda aproximadamente 30 a 60 segundos en completarse.

33. En el panel de navegación izquierdo, seleccione **Assessment runs** (Ejecuciones de evaluación) y actualice cada 10 a 15 segundos hasta que **Status** (Estado) cambie a **Analysis complete** (Análisis completo).
34. En el panel de navegación izquierdo, seleccione **Findings** (Hallazgos) y luego seleccione **Date** (Fecha) 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.

Amazon Inspector - Hallazgos

Los hallazgos son posibles problemas de seguridad detectados por Amazon Inspector durante la ejecución de una evaluación de

Añadir/Editar atributos

▼ Filtro

<input type="checkbox"/>	Gravedad ⓘ▼	Fecha ▼	Hallazgo	Objetivo
<input type="checkbox"/>	▶ Media	Today at 9:1...	On instance i-034a96d9041c719a6, TCP port 22 w...	Network-Audit
<input type="checkbox"/>	▶ Informativa	Today at 9:1...	Aggregate network exposure: On instance i-034a9...	Network-Audit

RESUMEN DE LA TAREA 4

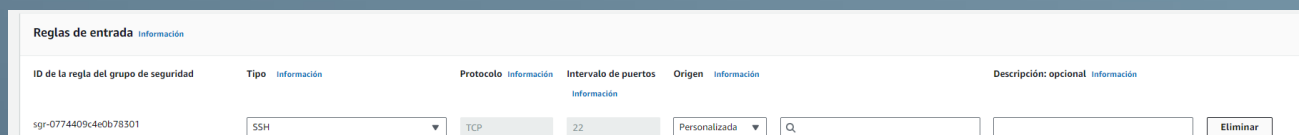
En esta tarea, actualizó el grupo de seguridad adjunto a BastionServer para que permita tráfico solo desde su dirección IP, en lugar de desde el Internet abierto, y eliminó el puerto Telnet que estaba completamente abierto y ya no era necesario.

Tarea 5: Reemplace BastionServer con Systems Manager

En esta tarea, reemplazó la instancia de BastionServer, que usaba principalmente SSH para conectarse a AppServer dentro de la subred privada. En su lugar, usted usa 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.

35. En Consola de administración de AWS, seleccione **Services (Servicios)** y seleccione **EC2**.
36. En el panel de navegación izquierdo, elija **Security Groups** (Grupos de seguridad).
37. Seleccione **Security group ID** (ID de grupo de seguridad) para **BastionServerSG**.
38. Seleccione **Edit inbound rules** (Editar las reglas de entrada).
39. Seleccione **Delete** (Eliminar) y luego seleccione **Save rules** (Guardar reglas) para eliminar la regla de entrada de SSH.



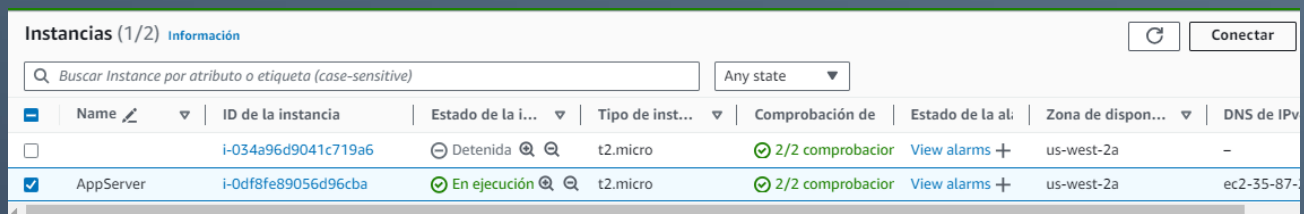
ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional
sgr-0774409c4e0b78301	SSH	TCP	22	Personalizada	

40. En el panel de navegación izquierdo, elija **Instances** (Instancias).
41. Seleccione la casilla de **BastionServer**. Seleccione la lista desplegable **Instance state** (Estado de la instancia) y, a continuación, elija **Stop instance** (Detener instancia).
42. En el cuadro de diálogo de confirmación, seleccione **Stop** (Detener).

A continuación, conéctese a AppServer directamente usando Session Manager.

Con **Session Manager**, puede acceder de forma rápida y segura a sus instancias 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.

43. Seleccione la casilla junto a **AppServer**, y luego seleccione **Connect** (Conectar). Ahora está conectado directamente a **AppServer**.



	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al:	Zona de dispon...	DNS de IPv
<input type="checkbox"/>		i-034a96d9041c719a6	Detenida	t2.micro	2/2 comprobador	View alarms +	us-west-2a	-
<input checked="" type="checkbox"/>	AppServer	i-0df8fe89056d96cba	En ejecución	t2.micro	2/2 comprobador	View alarms +	us-west-2a	ec2-35-87-

44. Ingrese los siguientes comandos Linux para cambiar el directorio y ver el directorio de trabajo actual de AppServer.

```
cd ~  
pwd
```

El resultado debería verse de la siguiente manera: `/home/ssm-user`

ID de sesión: 37ece71c-2d18-43aa-badc-7e1a03f5f73d-097f82b824321b957

ID de instancia: i-0df8fe89056d96cba

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

ANÁLISIS FINAL DEL ENTORNO

45. Vaya a la pestaña del navegador que tiene **Amazon Inspector** abierto.
46. En el panel de navegación izquierdo, elija **Assessment runs** (Ejecuciones de evaluación).
47. Seleccione la casilla para la evaluación ejecutada anteriormente y luego seleccione **Run** (Ejecutar).
48. Espere que **Status** (Estado) muestre **Analysis complete** (Análisis completo) y seleccione para expandir los detalles de la ejecución de evaluación más reciente.
49. Compruebe que no haya ningún **Hallazgo**.

Amazon Inspector - Hallazgos

Los hallazgos son posibles problemas de seguridad detectados por Amazon Inspector durante la ejecución de una evaluación del objetivo.

Añadir/Editar atributos

Filtro



Gravedad ⓘ ▼

Fecha ▼

Hallazgo

Objetivo

RESUMEN DE LA TAREA 5

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 Bastión e hizo que sea incluso más fácil conectarse usando Session Manager, proporcionado por System Manager.

Conclusión

¡Felicitaciones! Aprendió a realizar correctamente las siguientes tareas:

- Configurar Amazon Inspector
- Ejecutar una auditoría de red sin agente
- Investigar los resultados del análisis
- Actualizar grupos de seguridad
- Iniciar sesión en un servidor de aplicación usando Session