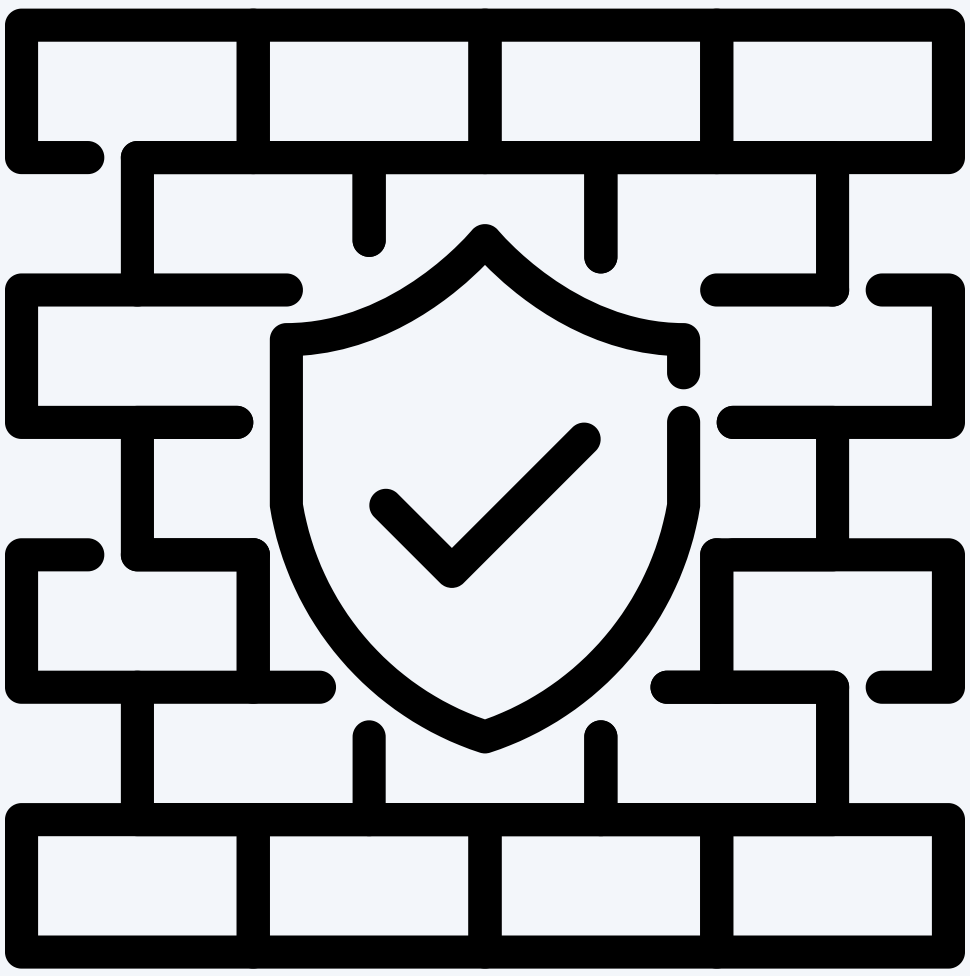
23°

Lab - AWS re/Start

Endurecimiento de red



SWIPE

Tarea 01

Protegiendo redes con Amazon Inspector y Systems Manager

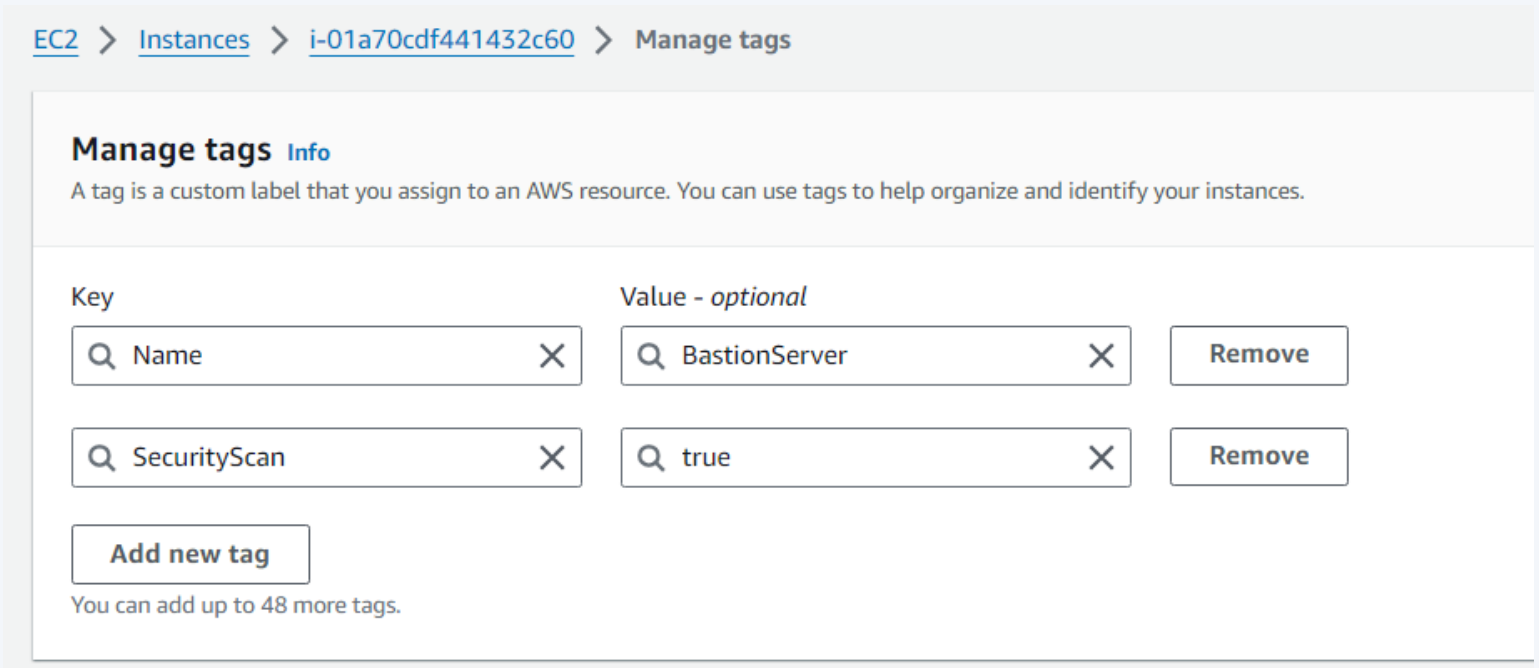
A continuación, se muestra los objetivos del laboratorio:

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

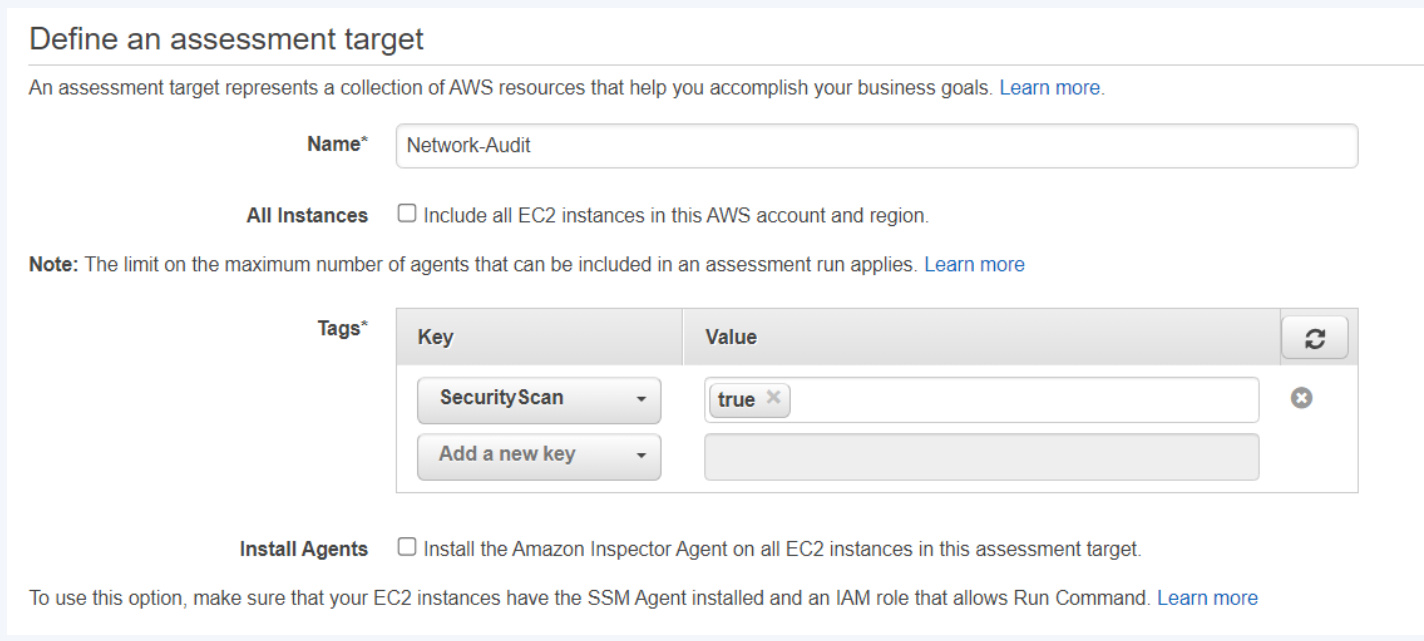
Nota. Utilizamos Amazon Inspector para analizar todas las configuraciones de red como grupos de seguridad, listas de control de acceso de red, tablas de enrutamiento, puertas de enlace de internet, pero sin la necesidad de enviar paquetes a través de la red de la VPC o conectarsea los puertos de la instancia de EC2.

Tarea 01

En el entorno del lab tenemos dos instancias EC2: *BastionServer* (subred pública) y *AppServer* (subred privada). Para que Amazon Inspector pueda evaluar las instancias EC2, lo primero que debes hacer es *tagear* a aquellas que quieres como *target*.



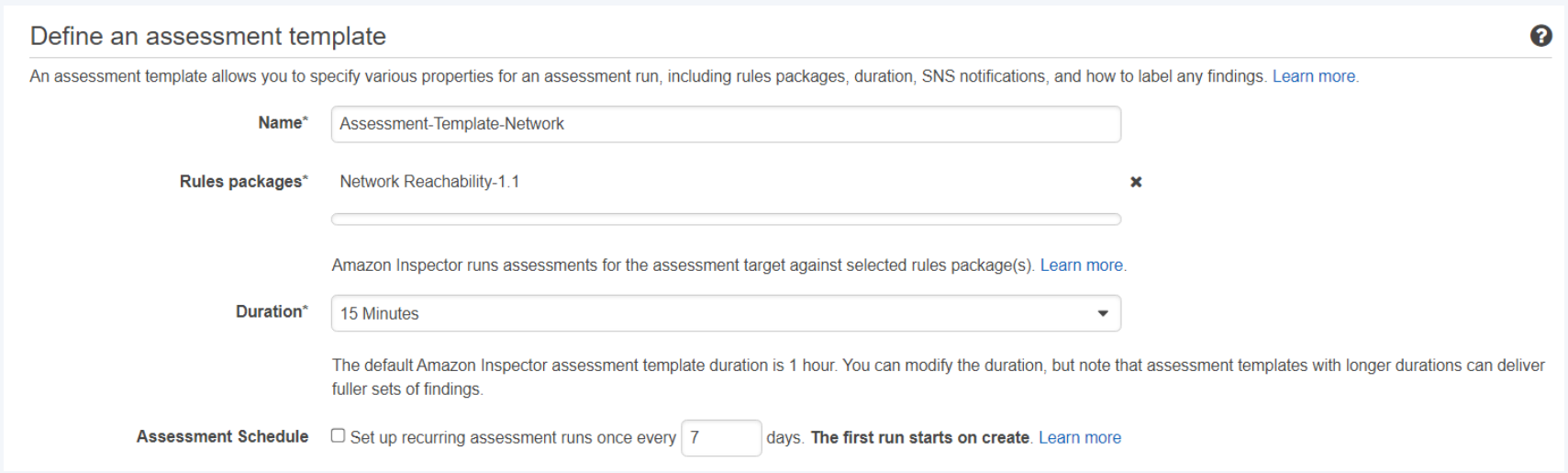
Después de esto, procedemos a configurar Amazon Inspector. Empezamos definiendo el *target de evaluación*, en este caso la instancia EC2 *BastionServer*. Esto debido a que tiene el tag *SecurityScan* en *true*.



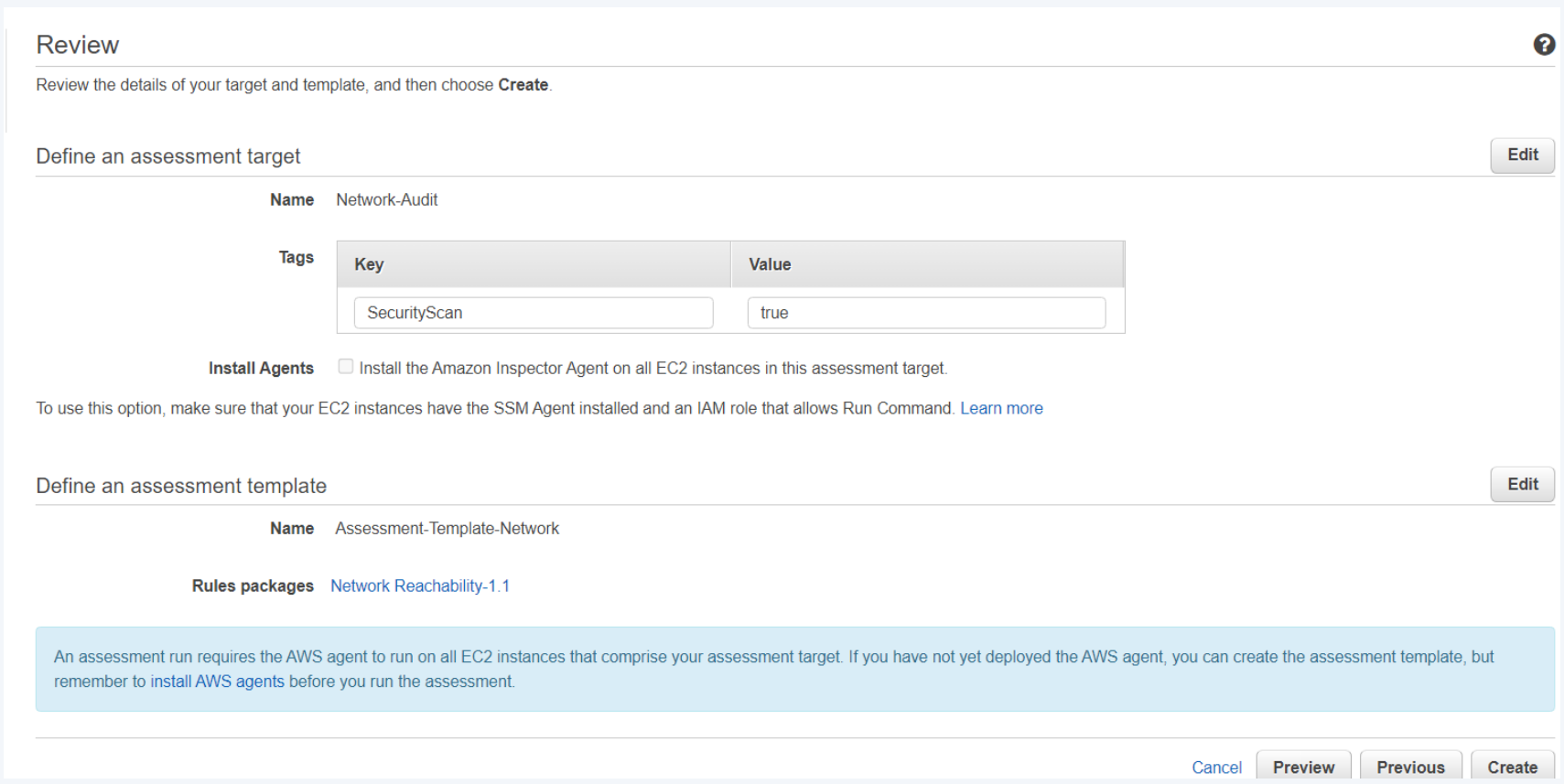
SWIPE

Tarea 01

Ahora, procedemos a definir la *Plantilla de evaluación*. En este caso solo nos concentraremos en el análisis del acceso a la red: *Network Reachability-1.1*



Así quedaría la configuración del análisis con Inspector:



SWIPE

Tarea 01

Después de que el análisis ha sido completado, podemos ver los *resultados(findings)*. A continuación, se muestran los resultados de *severidad alta (High Severity)*

Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'

ARN	arn:aws:inspector:us-west-2:252526466788:target/0-bmjxAaNq/template/0-kGgPs5ad/run/0-uQjbMGza/finding/0-iAmrizLX
Run name	Run - Assessment-Template-Network - 2024-01-30T05:33:40.090Z
Target name	Network-Audit
Template name	Assessment-Template-Network
Start	Today at 12:33 AM (GMT-5) (7 minutes ago)
End	Today at 12:34 AM (GMT-5) (6 minutes ago)
Status	Analysis complete
Rules package	Network Reachability-1.1
AWS agent ID	i-01a70cdf441432c60
Finding	On instance i-01a70cdf441432c60, 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-01a70cdf441432c60 is located in VPC vpc-09674d9f767dfd16c and has an attached ENI eni-008c7c6941b6a33f0 which uses network ACL acl-0f035762742c3181f. The port is reachable from the internet through Security Group sg-0c8cf9a42fcae9257 and IGW igw-038f0a0c68036d31d
Recommendation	You can edit the Security Group sg-0c8cf9a42fcae9257 to remove access from the internet on port 23

Y el de *severidad media:*

Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'

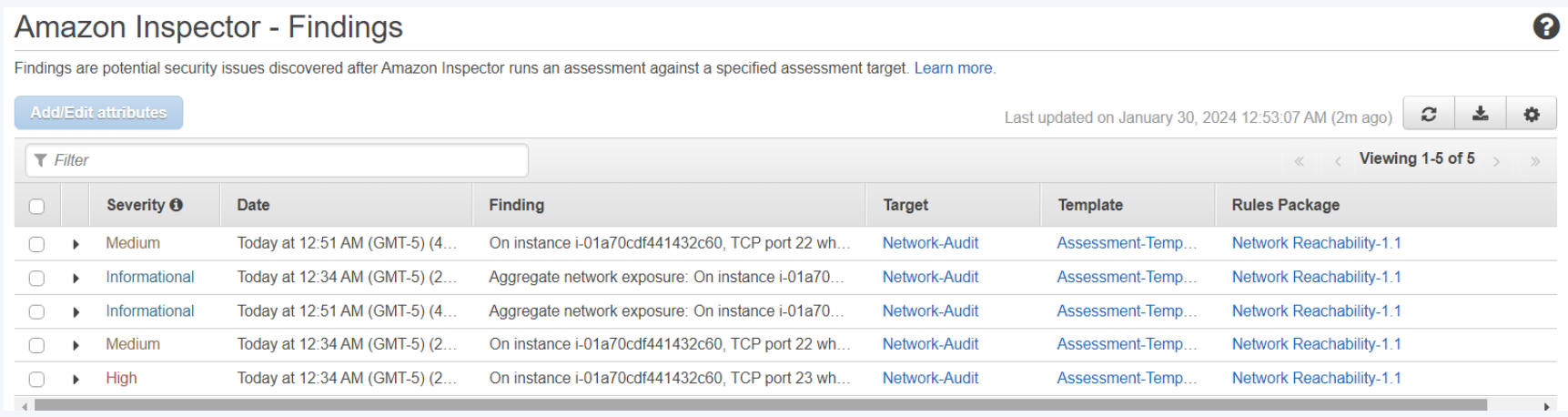
ARN	arn:aws:inspector:us-west-2:252526466788:target/0-bmjxAaNq/template/0-kGgPs5ad/run/0-uQjbMGza/finding/0-KQ9xUhj5
Run name	Run - Assessment-Template-Network - 2024-01-30T05:33:40.090Z
Target name	Network-Audit
Template name	Assessment-Template-Network
Start	Today at 12:33 AM (GMT-5) (8 minutes ago)
End	Today at 12:34 AM (GMT-5) (7 minutes ago)
Status	Analysis complete
Rules package	Network Reachability-1.1
AWS agent ID	i-01a70cdf441432c60
Finding	On instance i-01a70cdf441432c60, 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-01a70cdf441432c60 is located in VPC vpc-09674d9f767dfd16c and has an attached ENI eni-008c7c6941b6a33f0 which uses network ACL acl-0f035762742c3181f. The port is reachable from the internet through Security Group sg-0c8cf9a42fcae9257 and IGW igw-038f0a0c68036d31d
Recommendation	You can edit the Security Group sg-0c8cf9a42fcae9257 to remove access from the internet on port 22

SWIPE

Tarea 01

Vamos a hacer las respectivas correcciones en las reglas de entrada en los puertos 22 y 23 del grupo de seguridad de la instancia. Esto debido a que *Telnet* es vulnerable a ataques de seguridad y el hecho de cualquier dirección IP pueda conectarse a nuestra instancia EC2 via el puerto 22 es inseguro, por lo que solo permitiremos la conexión a nuestra instacia si es que el origen es nuestra dirección IP.

Esto hace que el resultado de severidad alta sea superado, sin embargo, el de severidad media persiste puesto que el puerto 22 está tecnicamente abierto al internet fuera de la VPC.

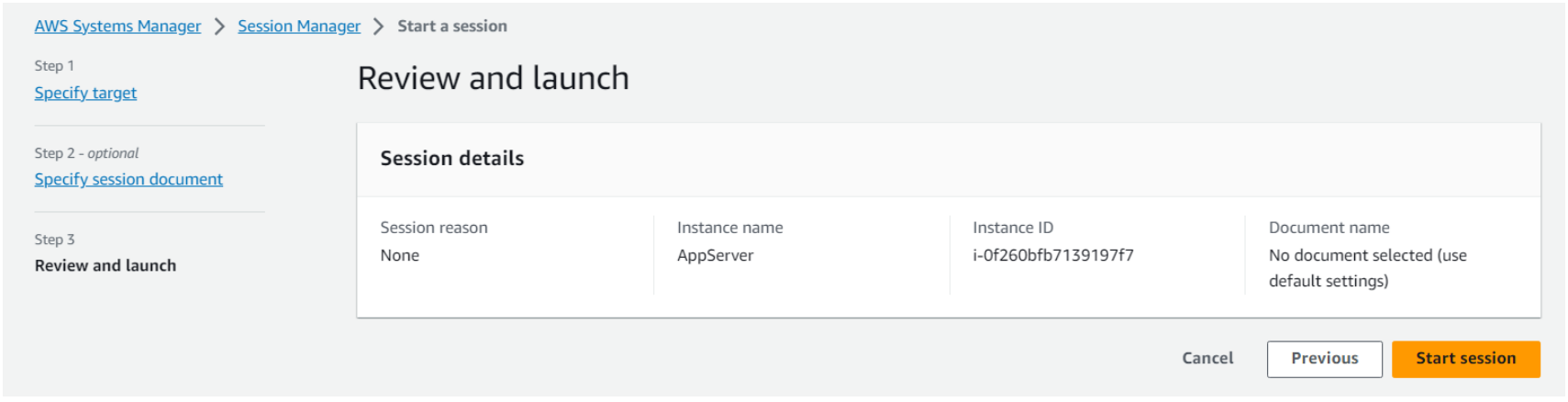


SWIPE

Tarea 01

Ahora, procedemos a reemplazar nuestra instancia *BastionServer*, que es utilizada para conectarse a la instancia *AppServer* que se encuentra dentro de una subred privada, por **Systems Manager**. El cual es una solución de administración integral segura para entornos de nube híbrida.

Con **Sessions Manager**, podemos conectarnos de manera segura y rápida a nuestras instancias EC2, sin la necesidad de abrir puertos de entrada o administrar claves SSH.



Notamos que la conexión fue exitosa:

SWIPE