Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 22/09/2023

Contacto: tomas.villaseca.c@gmail.com

Después de completar este laboratorio, podrá realizar lo siguiente:

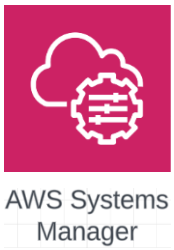
- Crear una línea de base de parches personalizada
- Modificar grupos de parches
- Configurar la aplicación de parches
- Verificar el cumplimiento de los parches (Conformidad)

Entorno del laboratorio → Seis instancias EC2

- Tres instancias Linux
- Tres instancias Windows

Tarea 1: Seleccionar valores de referencia de parches

AWS Systems Manager = Solución de administración segura para recursos de AWS y en entornos multicloud e híbridos.



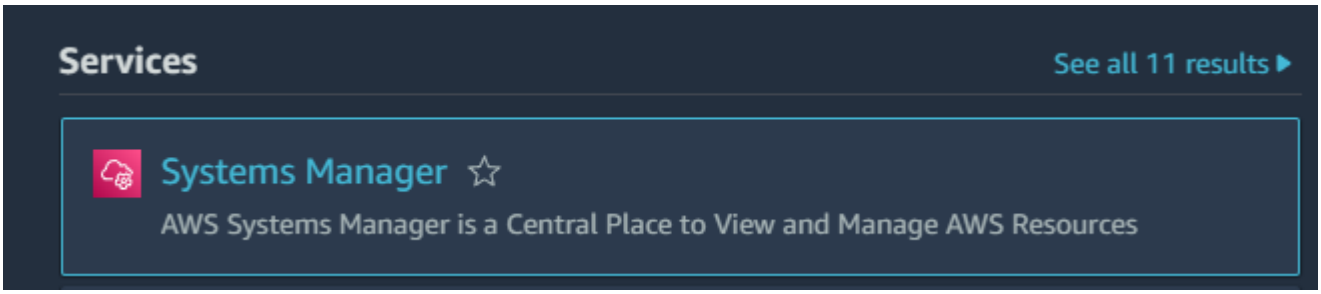
- Operations Management → Proporciona visibilidad de sus aplicaciones e infraestructura y ayuda a solucionar problemas con rapidez.
- Application Management → Implemente, administre y escale sus aplicaciones.
- Change Management → Manera controlada y auditable de realizar cambios en sus aplicaciones e infraestructura.
- Node Management → Gestione sus instancias EC2 y otros recursos on-premise.

Patch Manager = Funcionalidad de AWS Systems Manager que permite crear un baseline (valor de referencia) de parches.

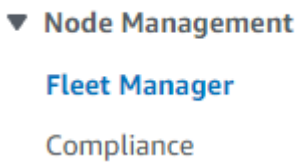
- Baseline = Valor o punto de referencia que se utiliza para comparar otros valores.
- Usar el baseline → Escanear las instancias EC2
- Instalar actualizaciones relacionadas con la seguridad del Sistema operativo de los nodos administrados.

Patch Manager ofrece baselines de parches predefinidos para cada uno de los sistemas operativos que admite.

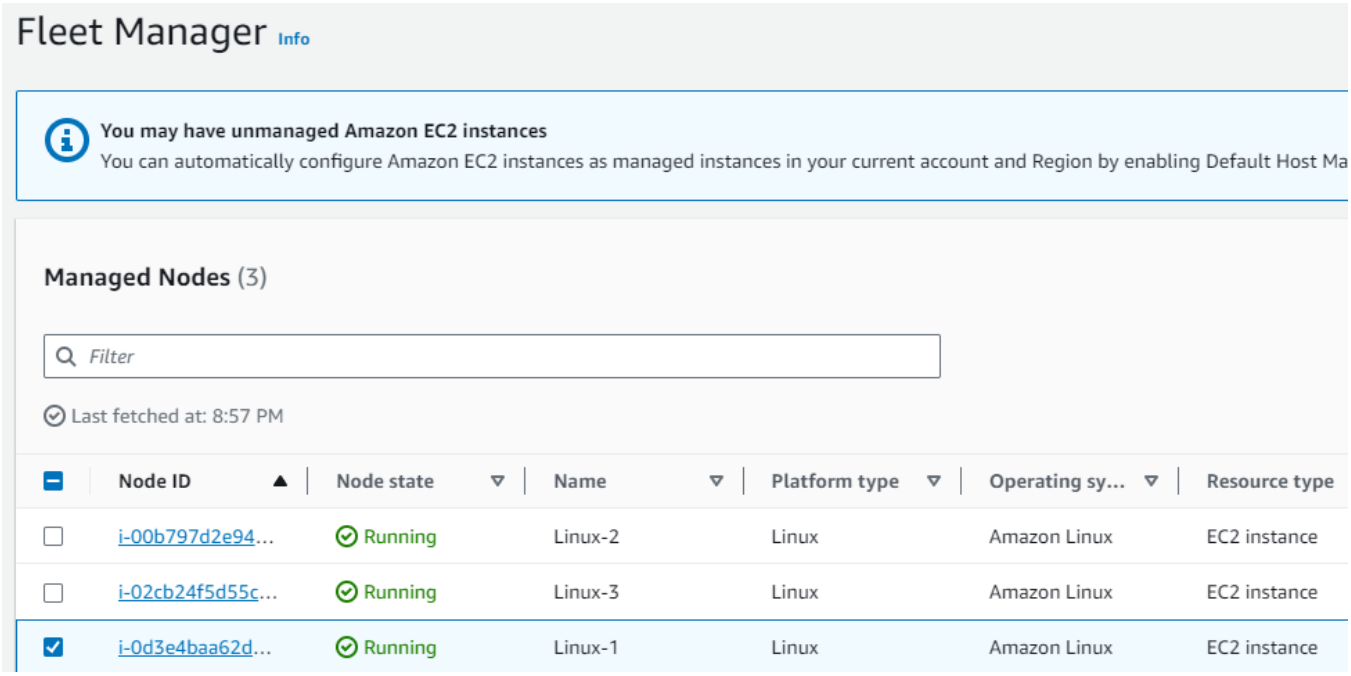
Paso 1: AWS Management Console → Busqueda → Amazon Systems Manager

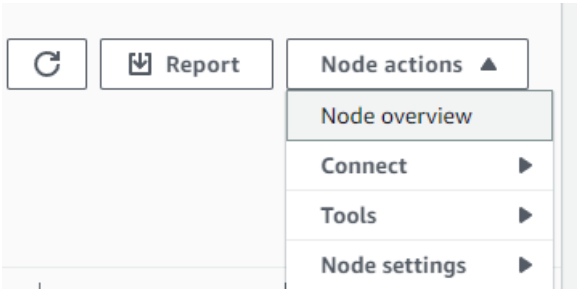


Paso 2: Panel de navegación → Node Management → Fleet Manager

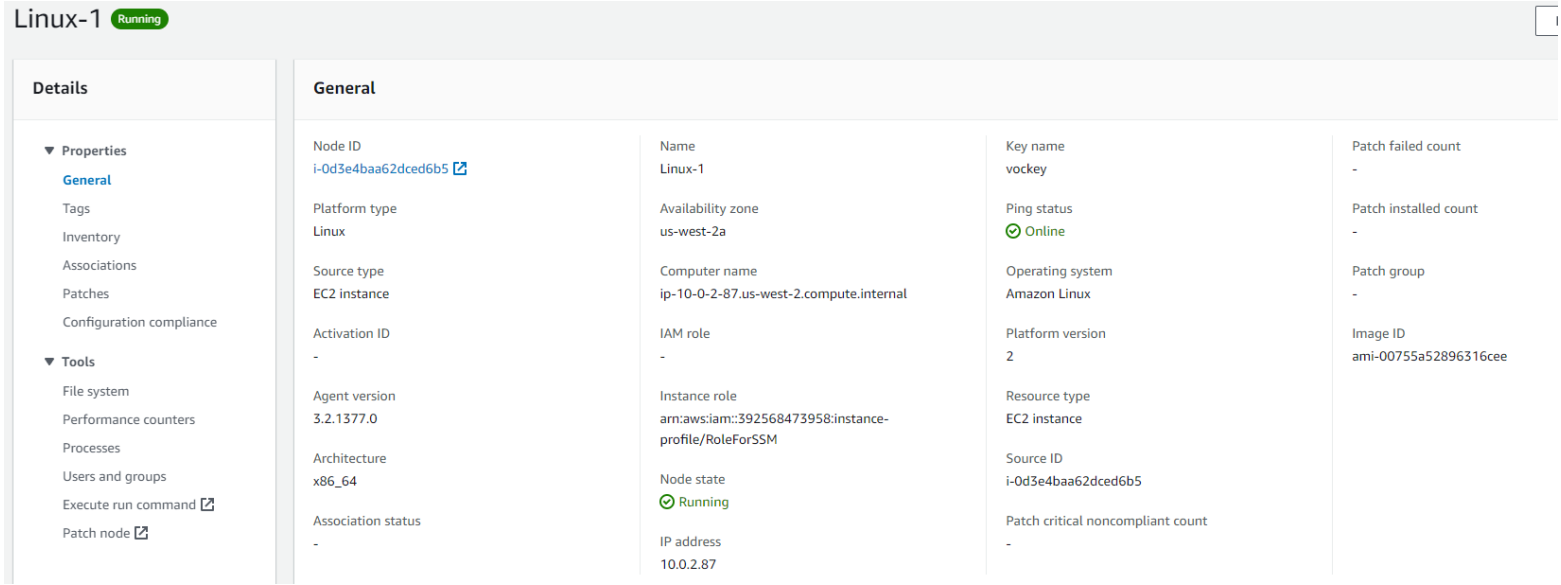


Paso 3: Fleet Manager → Linux-1 → Node Actions → Node Overview



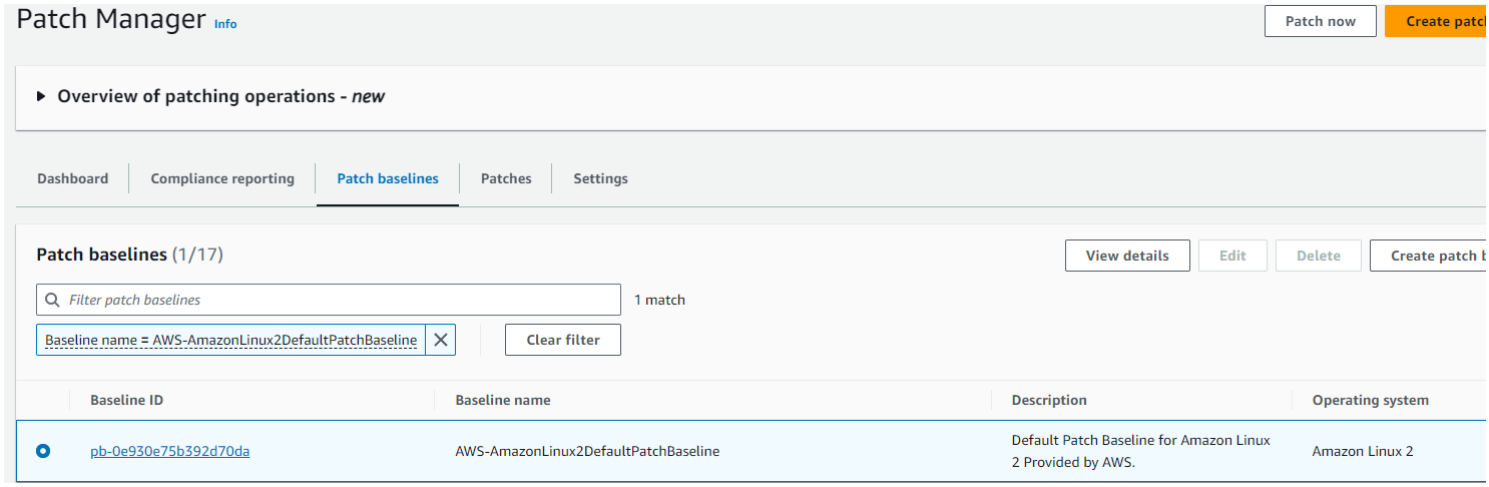


En Node Overview puede ver detalles acerca de la instancia específica, como el **Tipo de plataforma**, el **Tipo de nodo**, el **Nombre de OS** y el **Rol de IAM** que le permite usar Amazon Systems Manager.

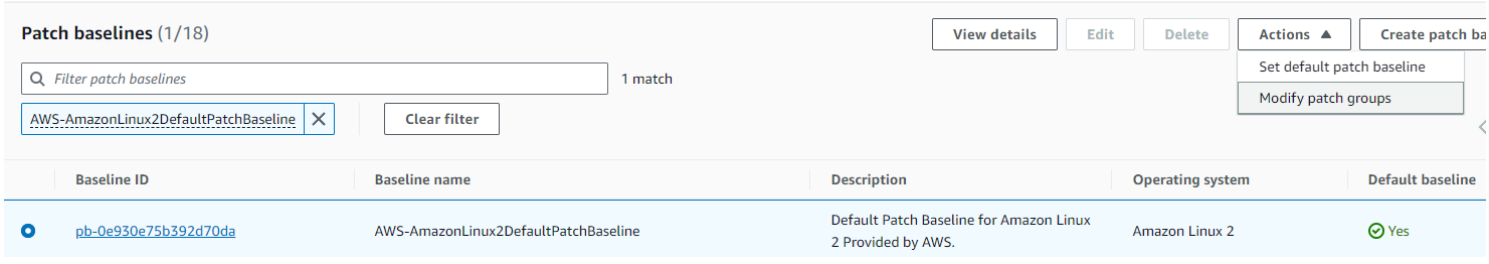


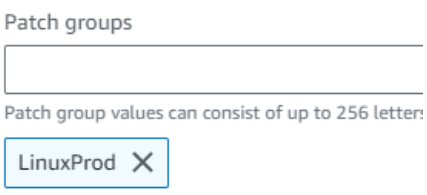
Paso 4: Node Management → Patch Manager → Start with an overview

Paso 4: Seleccionar pestaña “Patch Baselines” → Buscar `AWS-AmazonLinux2DefaultPatchBaseline`



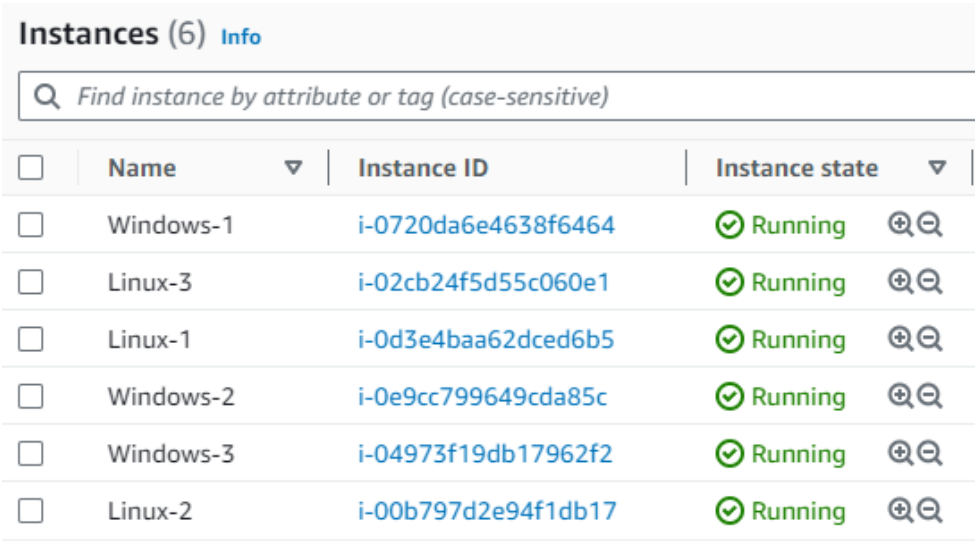
Paso 5: Action → Modify Patch Group → Patch Groups → LinuxProd → Add





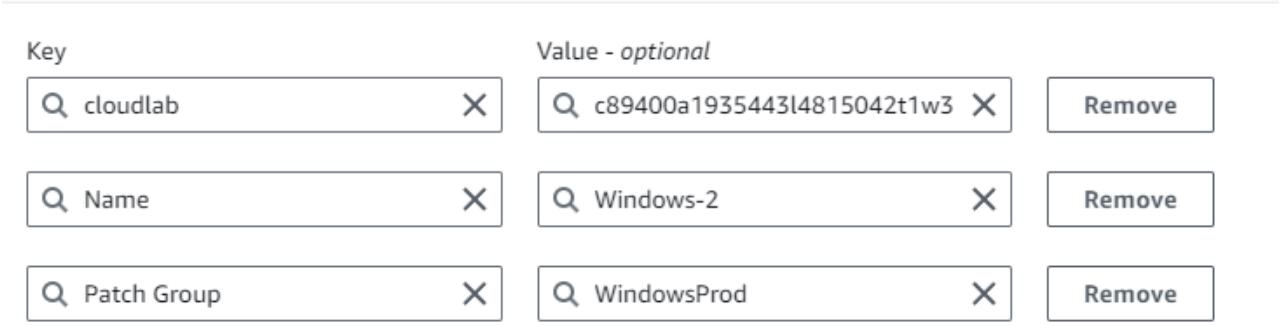
Tarea 1.1 – Etiquetar Instancias:

Paso 1: Services → Compute → EC2 → Instances



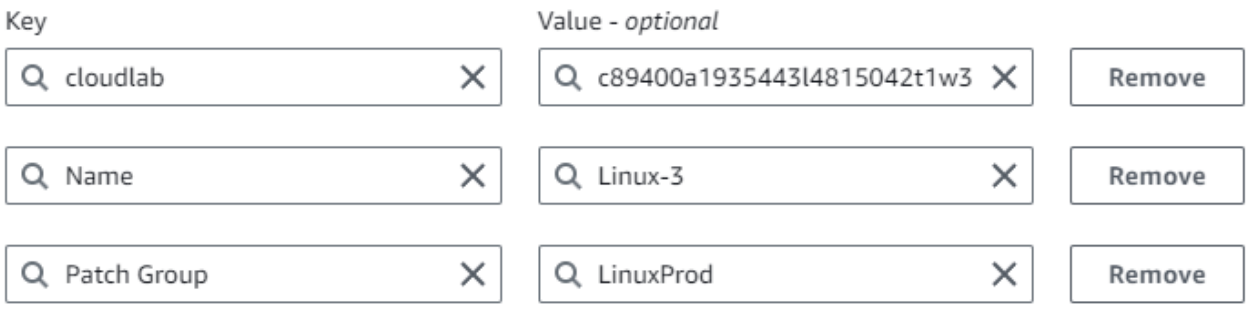
Paso 2: Pestaña "Tag" → Manage Tags → Etiquetar instancias Windows

- Key = Patch Group
- Value = WindowsProd



Paso 2: Pestaña "Tag" → Manage Tags → Etiquetar instancias Linux

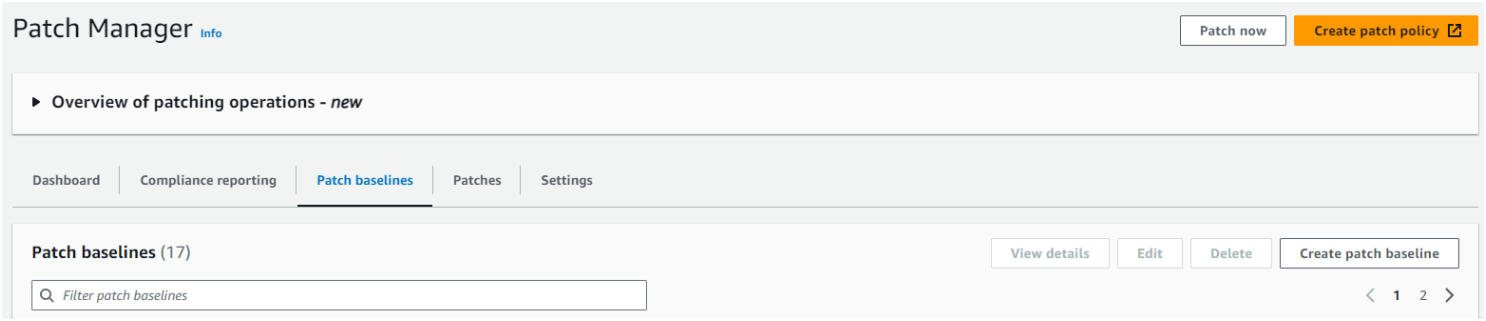
- Key = Patch Group
- Value = LinuxProd



Tarea 1.2 – Crear un Baseline de parche personalizado:

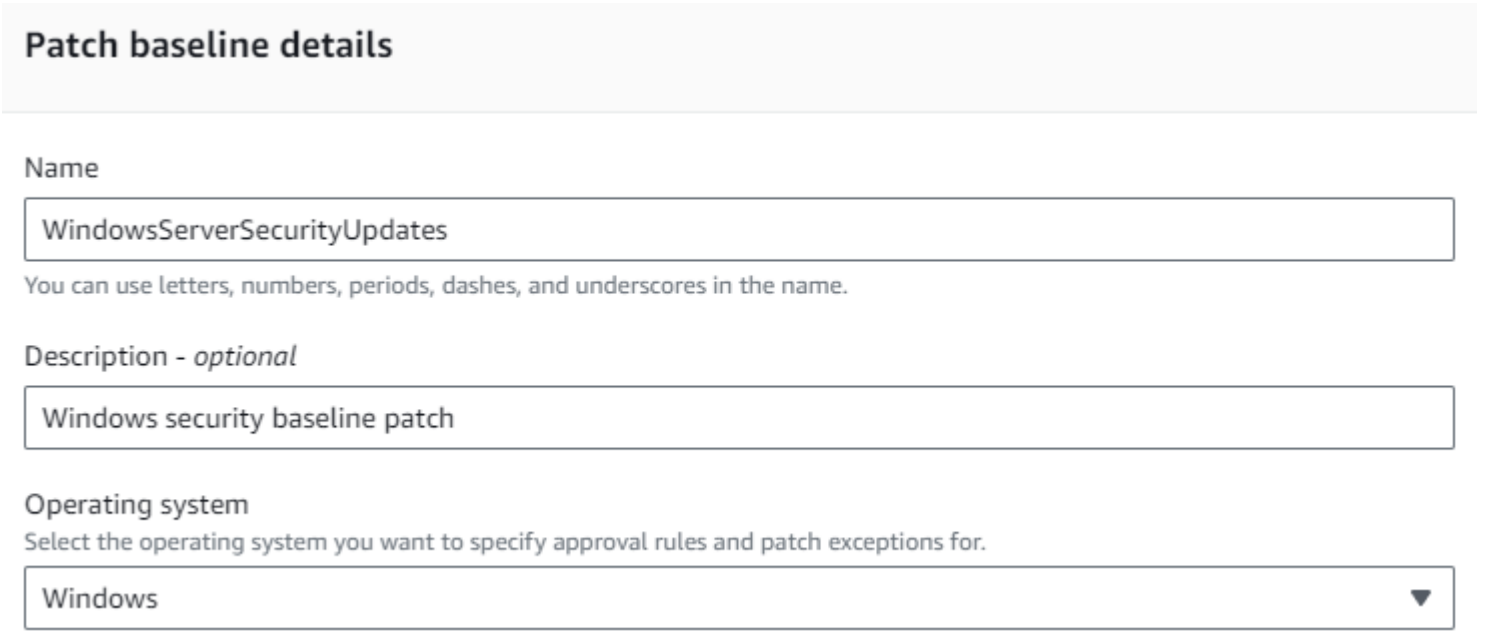
Paso 1: Amazon Systems Manager → Node Management → Patch Manager → Star with overview

- Seleccionar pestaña “Patch Baseline” → Create Patch Baseline



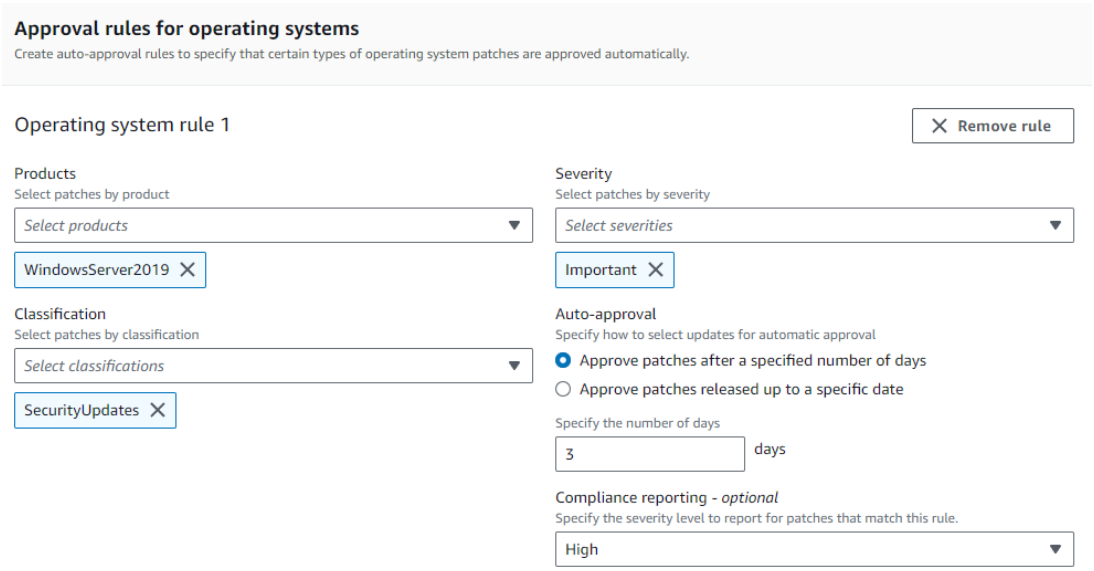
Paso 2: Configurar Baseline de parche → Details

- Name = WindowsServerSecurityUpdates
- Description = Windows security baseline patch
- Operating System = Windows
- Dejar seleccionada la casilla “Default patch baseline”



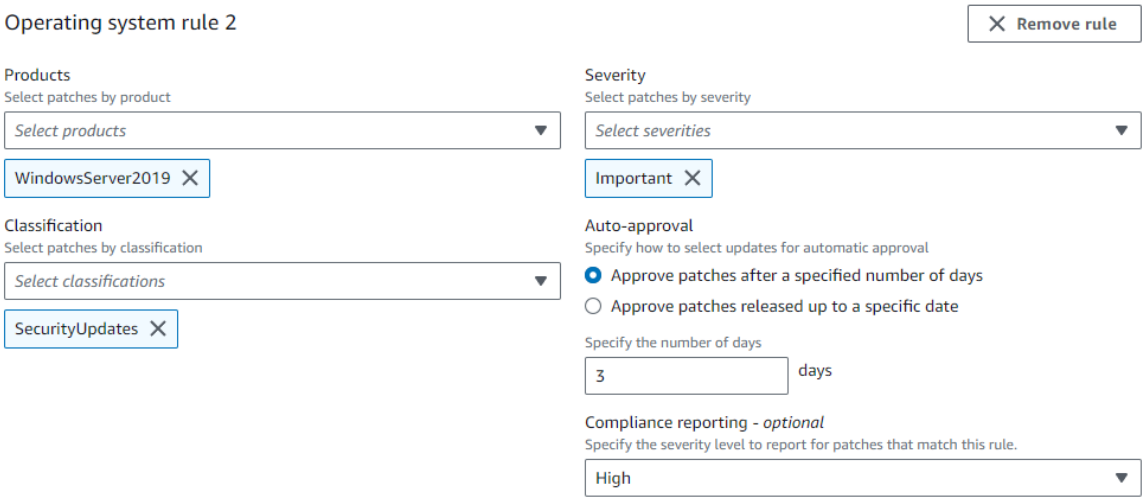
Paso 3: Configurar Baseline de parche → Approval rules for operating systems

- Products = WindowsServer2019
- Severity = Important
- Classification = SecurityUpdates
- Auto-Approval = 3 Days
- Compliance reporting = High



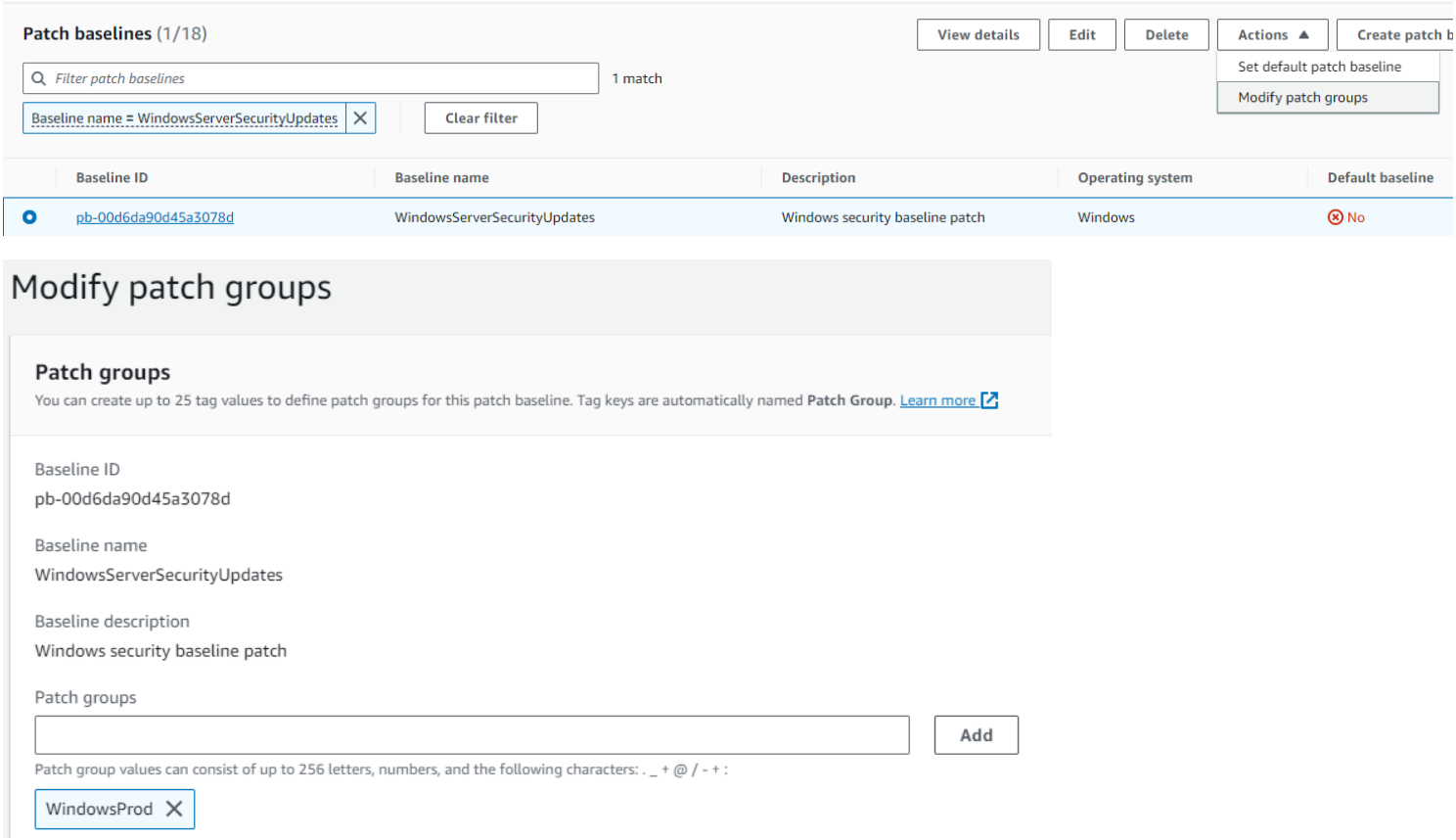
Paso 4: Configurar Baseline de parche → Add Rule → Create Patch Baseline

- Products = WindowsServer2019
- Severity = Important
- Classification = SecurityUpdates
- Auto-Approval = 3 Days
- Compliance reporting = High



Paso 5: Seleccionar pestaña “Patch Baseline” → Buscar WindowsServerSecurityUpdates

Paso 6: Action → Modify Patch Group → Patch Groups → WindowsProd → Add



En esta tarea, usó una baseline de parches predeterminado de Linux Amazon y modificó un grupo de parches para el grupo LinuxProd. Luego etiquetó sus instancias de Windows para que pudieran asociarse con el grupo de parches WindowsProd. Aprendió cómo crear un valor de referencia de parches personalizado para las instancias de Windows.

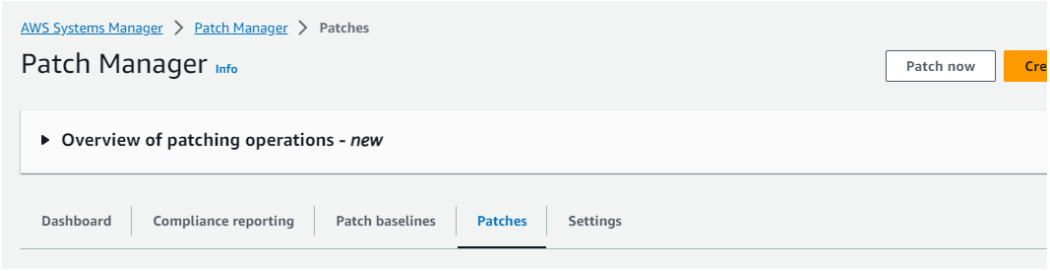
Tarea 2: Configurar la aplicación de parches

Configurar los parches para las instancias de Linux y crear un periodo de mantenimiento programado. Aplicar el parche a las instancias de Windows manualmente.

Después de realizar la configuración, Patch Manager usa el **Run Command** para llamar al documento **RunPatchBaseline** para evaluar cuáles parches se deben instalar en las instancias de destino, según el tipo de sistema operativo de cada instancia, de forma directa o durante la programación definida (periodo de mantenimiento).

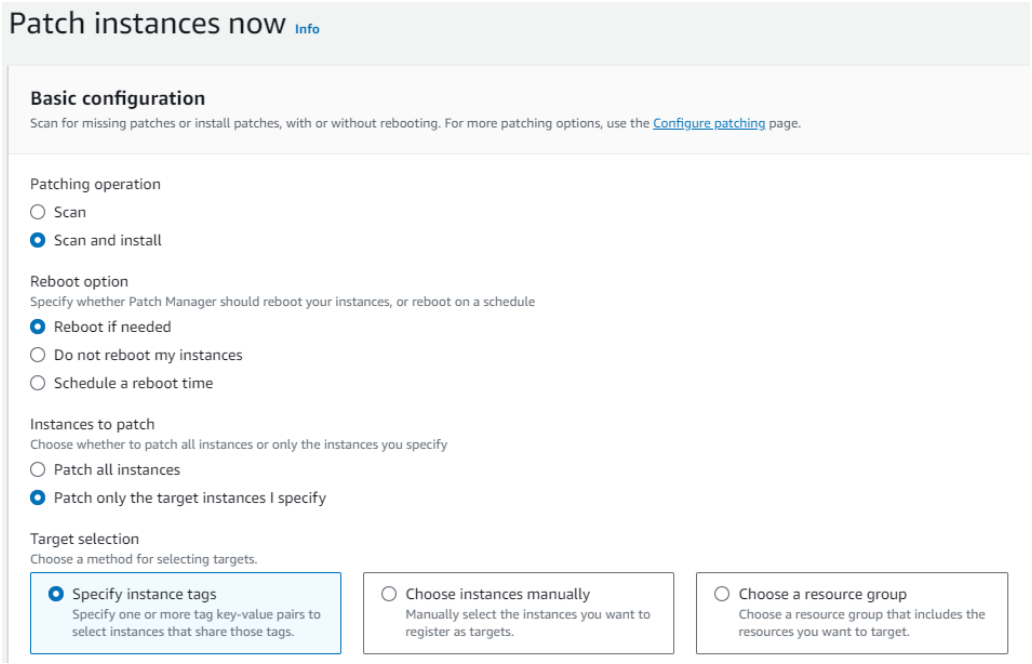
Tarea 2.1 – Parchar Instancias Linux

Paso 1: Amazon Systems Manager → Node Management → Patch Manager → Patches → Patch Now



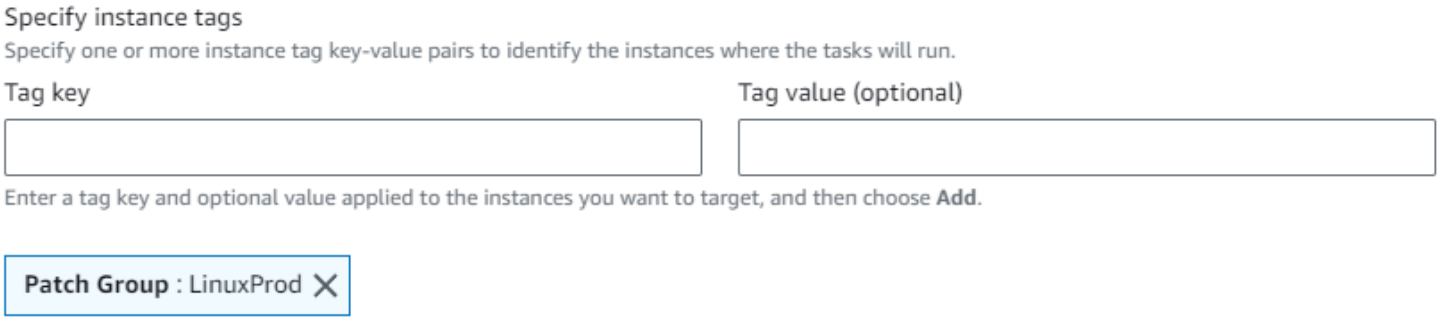
Paso 2: Patch instances now → Basic Configuration (1)

- Patching operation = Scan and install
- Reboot Option = Reboot if needed
- Instance to patch = Patch only the target instance specified



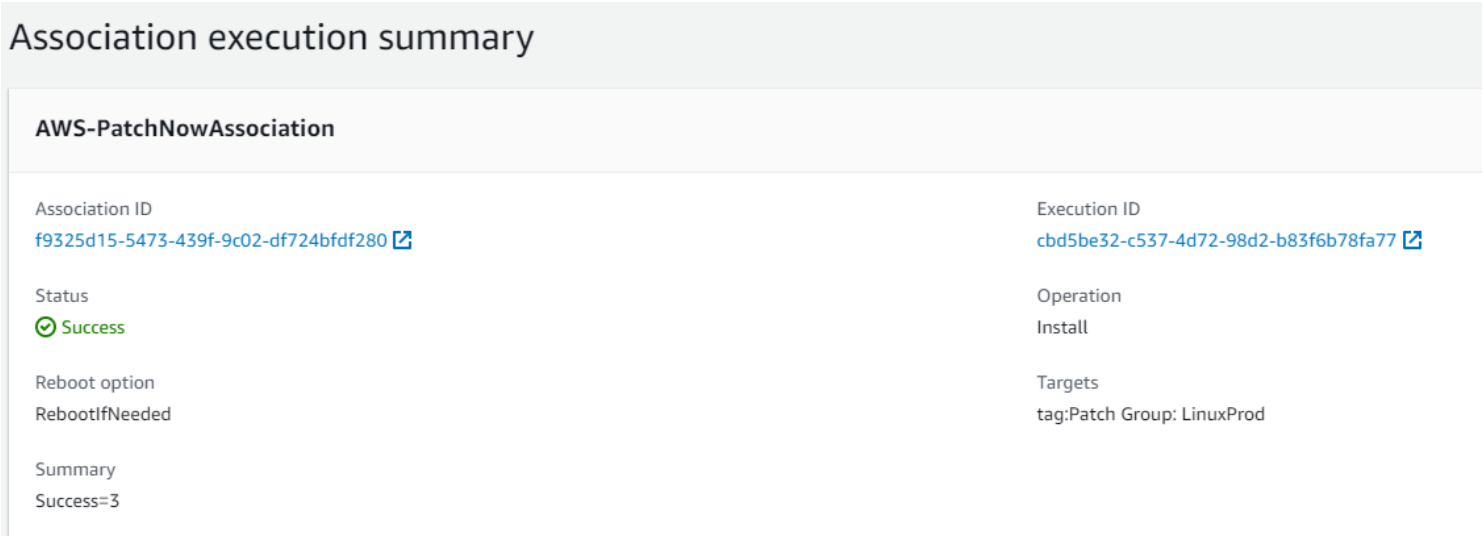
Paso 3: Patch instances now → Basic Configuration (2)

- Specify instance tags → Key = Patch Group, Value = LinuxProd. → Add

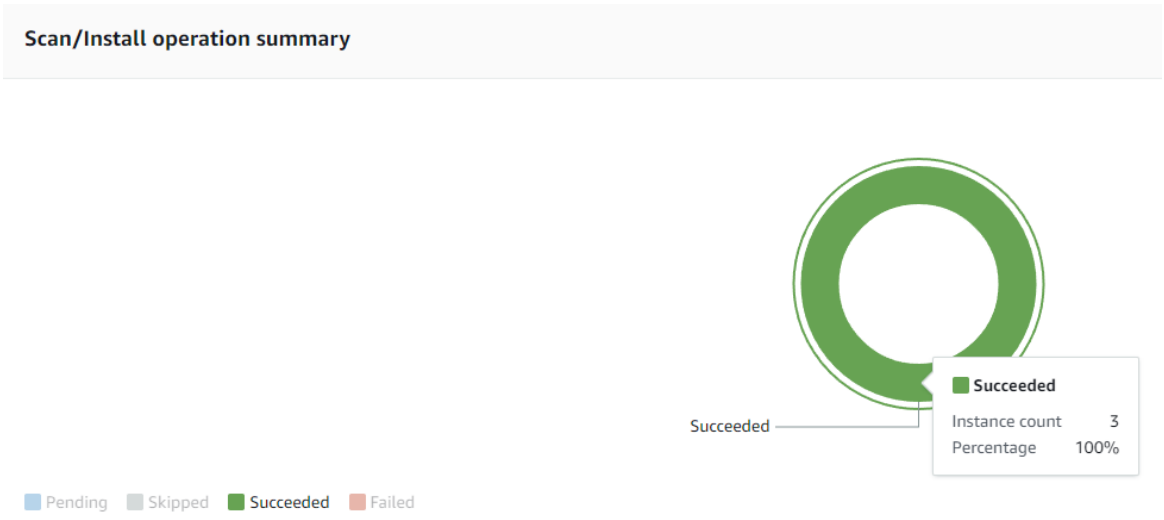


Paso 4: Seleccionar “Patch Now” → Aparece una nueva página

- Progress/Summary → Muestra que 3 instancias se verán afectadas y el progreso realizado.

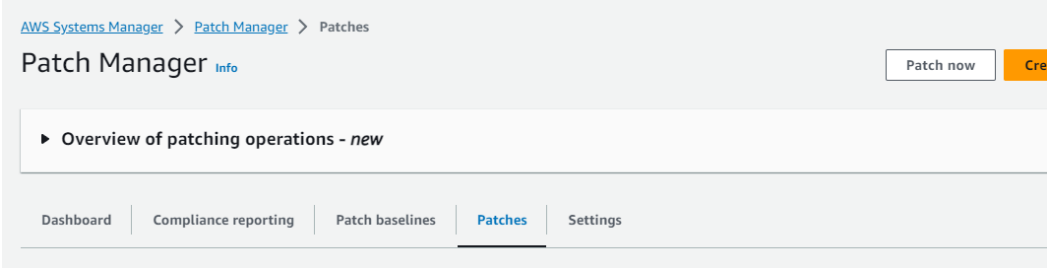


- Scan/install operation summarty → Muestra visualmente el estado de las instancias afectadas.



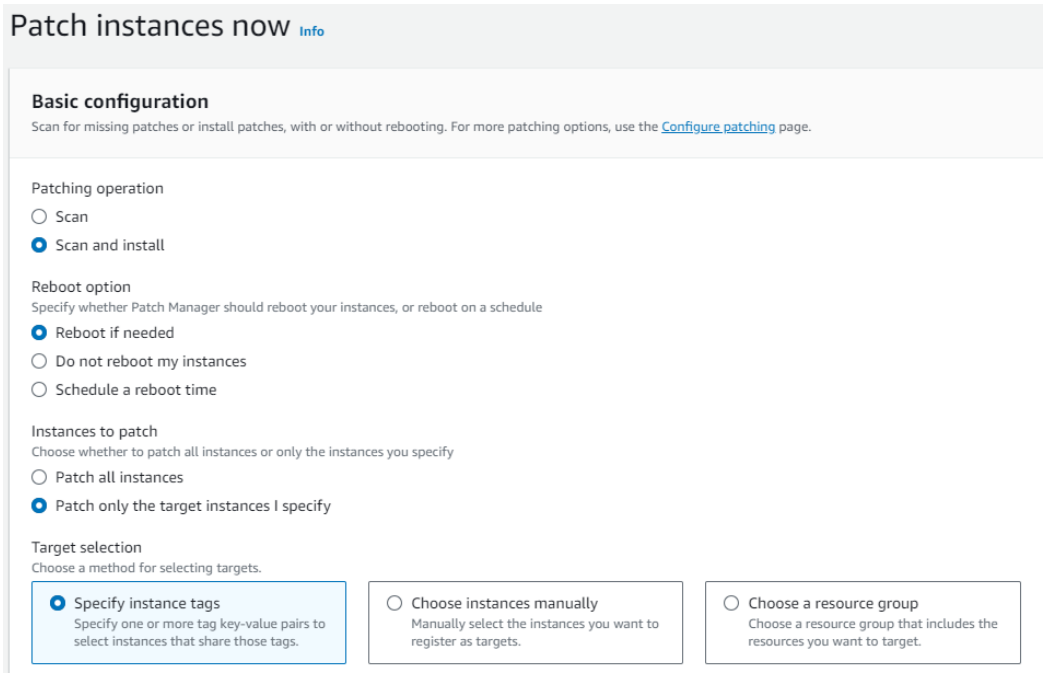
Tarea 2.2 – Parchar Instancias Windows

Paso 1: Amazon Systems Manager → Node Management → Patch Manager → Patches → Patch Now



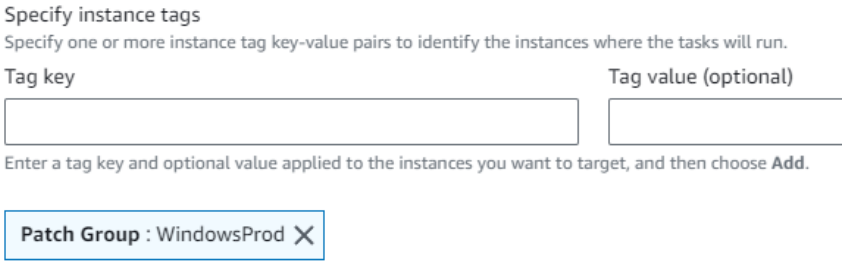
Paso 2: Patch instances now → Basic Configuration (1)

- Patching operation = Scan and install
- Reboot Option = Reboot if needed
- Instance to patch = Patch only the target instance specified

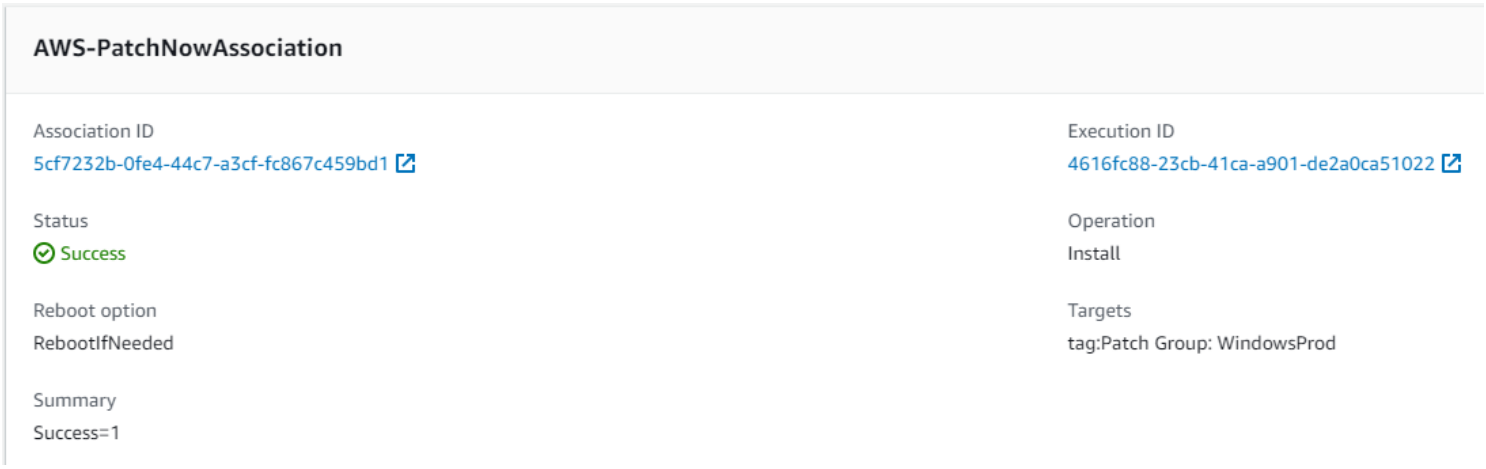


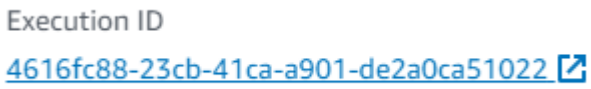
Paso 3: Patch instances now → Basic Configuration (2)

- Specify instance tags → Key = Patch Group, Value = WindowsProd → Add

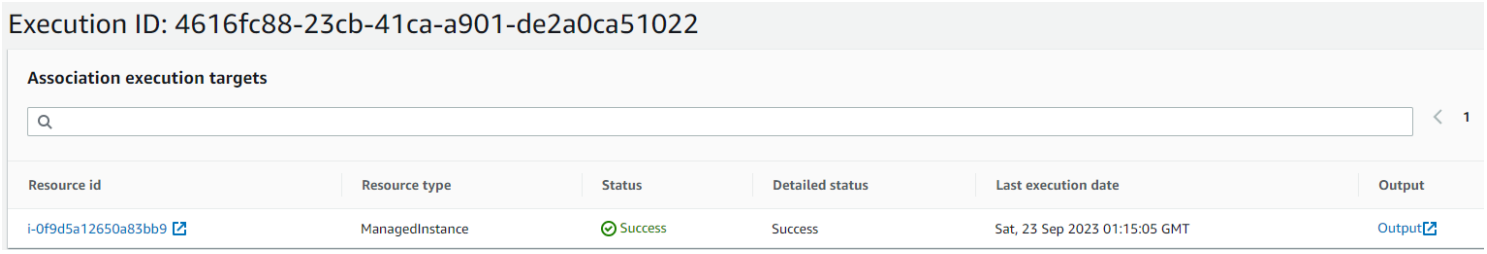


Paso 4: Seleccionar “Patch Now” → Aparece una nueva página → Execution ID Link

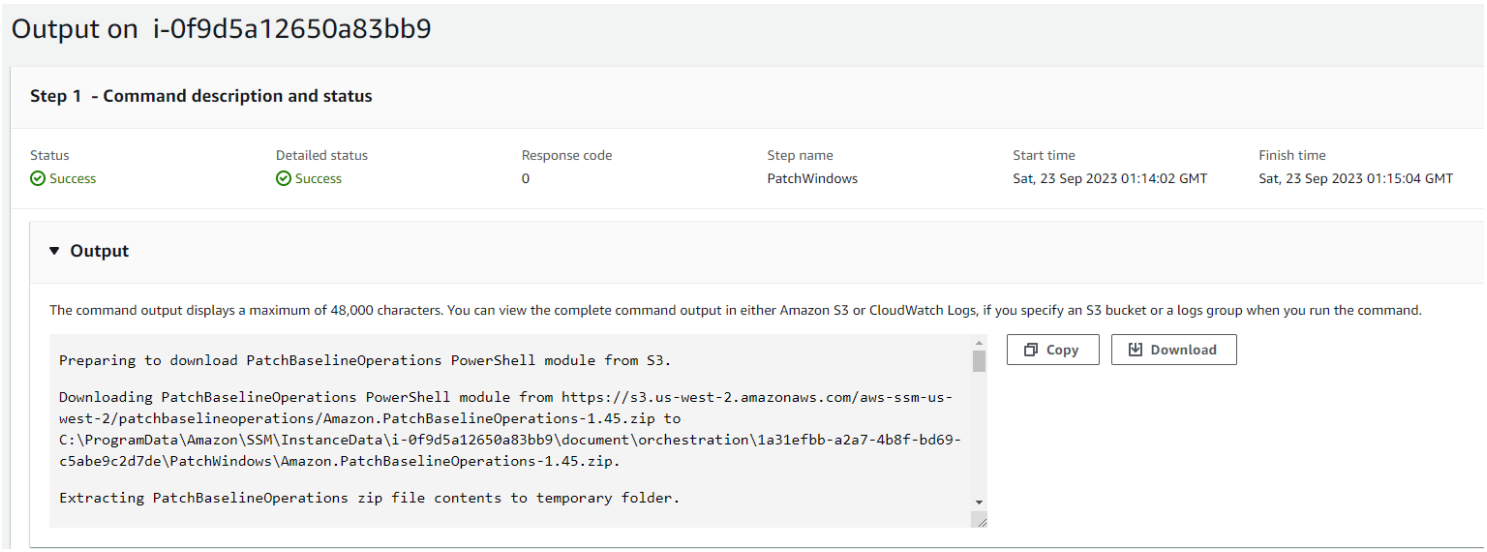




Paso 5: Execution ID → Output link



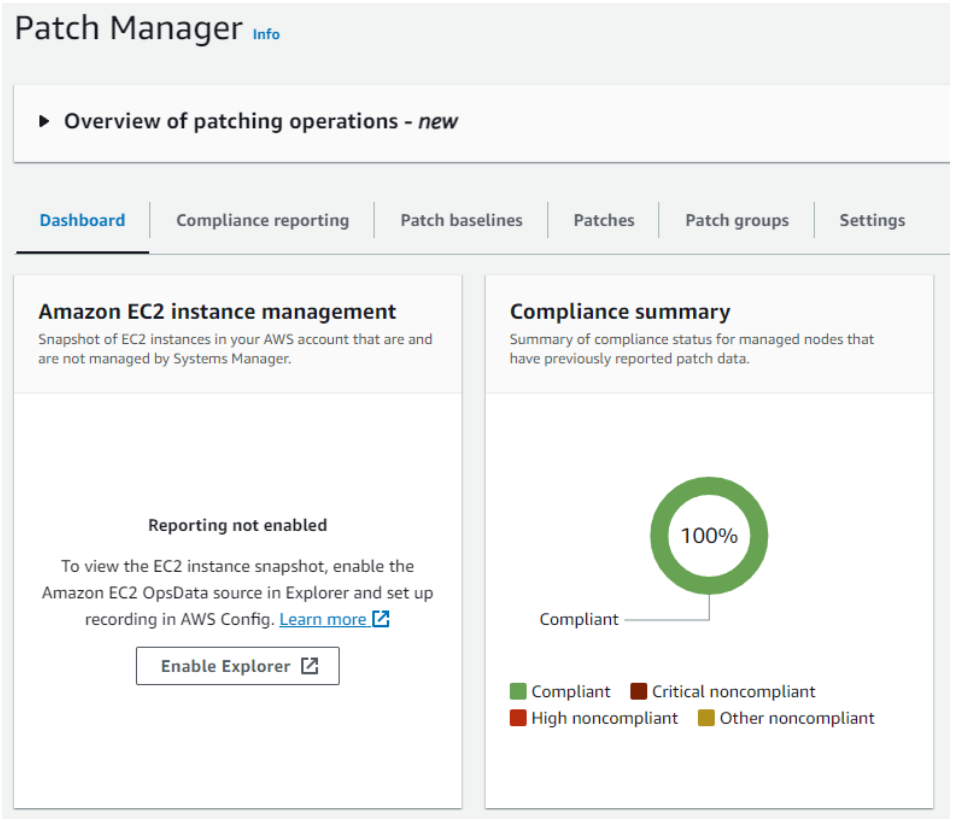
Expand Output Panel to observe the details:



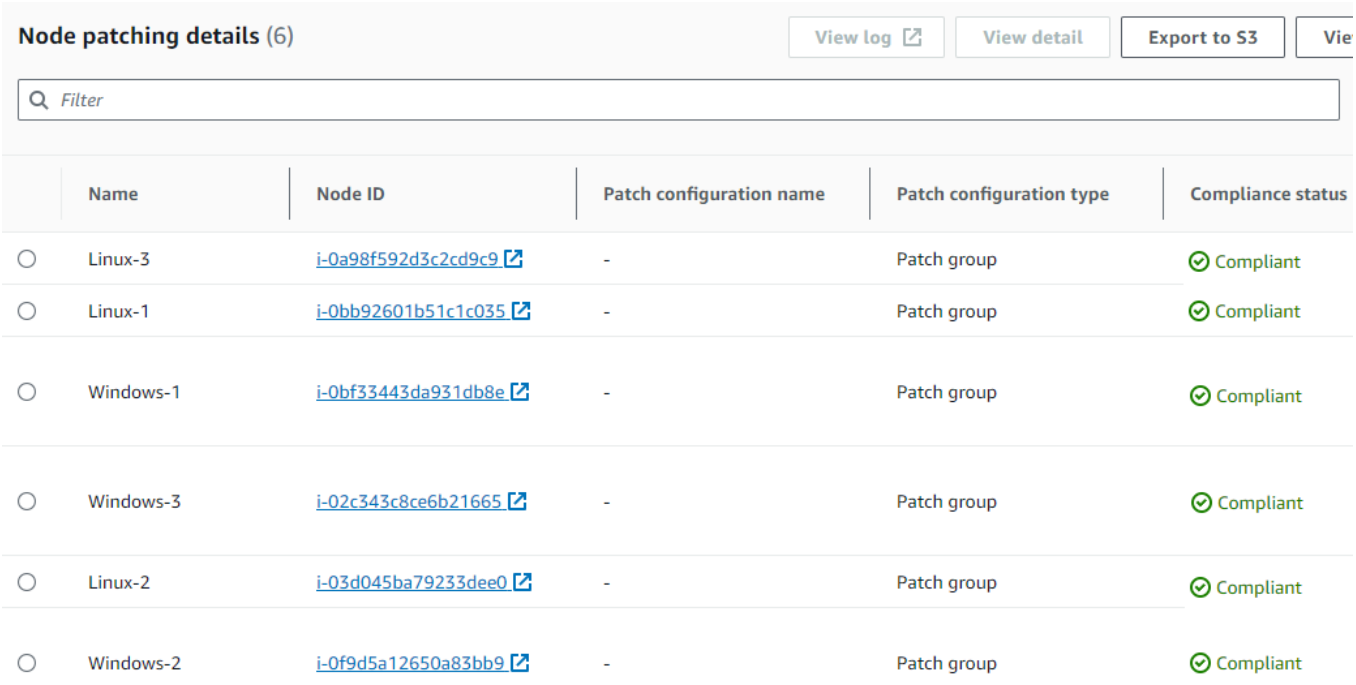
Patch Manager utiliza el **Run Command** para ejecutar el parche.

Tarea 2.3 – Verificar la Conformidad

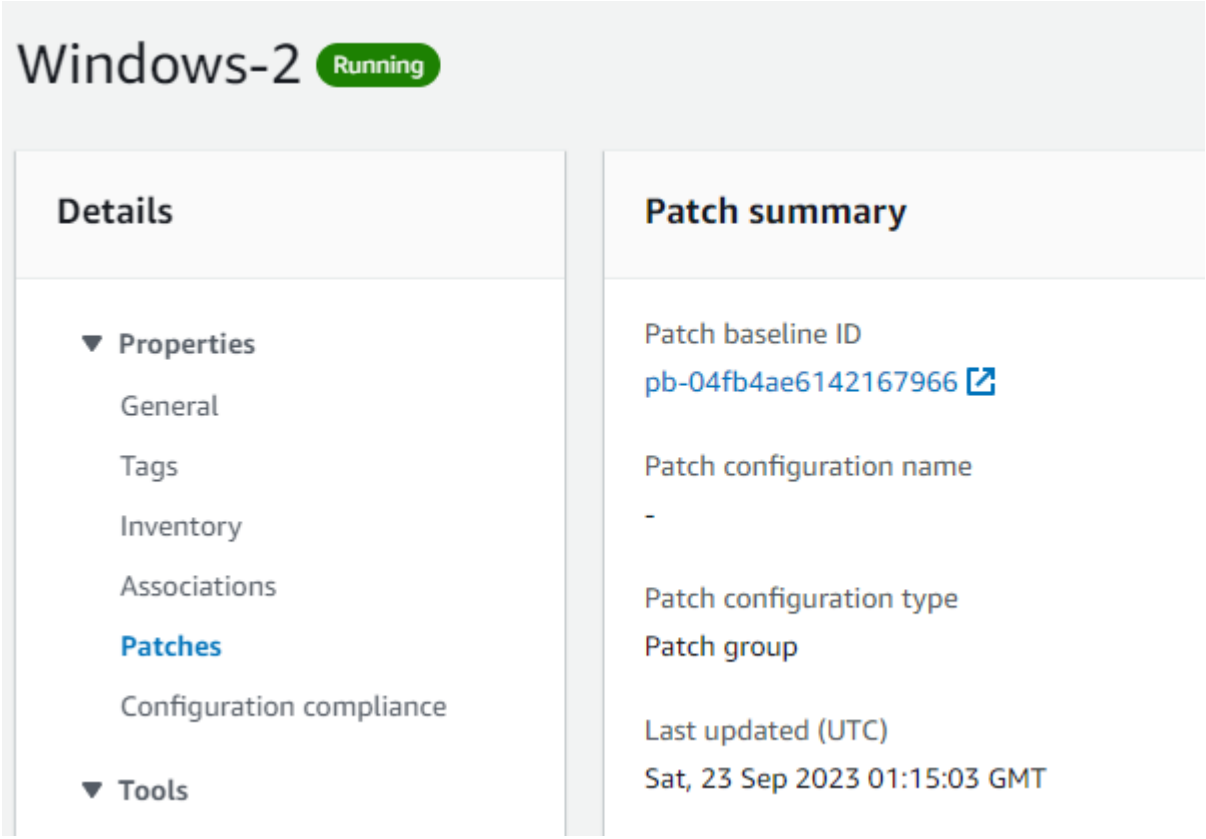
Paso 1: Amazon Systems Manager → Node Management → Patch Manager → Compliance Summary



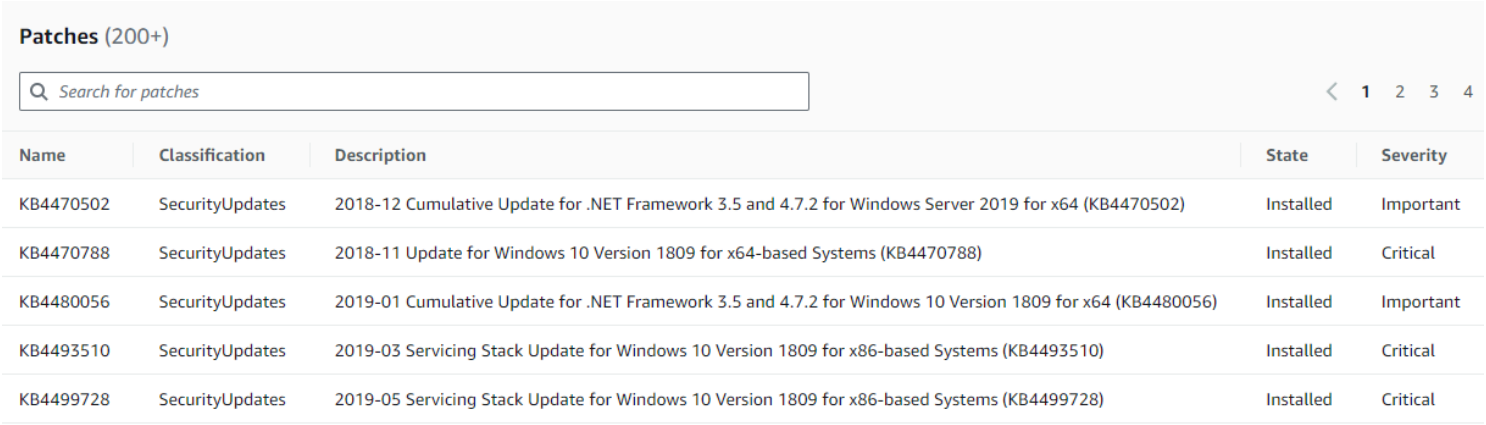
Paso 2: Seleccionar pestaña “Compliance Reporting” → Node Patching Details



Paso 3: Node Patchin Details → Node ID Link (En este caso Windows-2)



- Se pueden revisar todos los parches que se le han aplicado a la instancia.



Se configuró la aplicación de parches y las instancias parcheadas tanto en el grupo LinuxProd como en el grupo WindowsProd.

Aprendió a escanear e instalar parches instantáneamente y a analizar la salida del comando Ejecutar para ver las actualizaciones de parches. Verificó mediante informes de conformidad que todas las instancias EC2 se han analizado y actualizado y que son conformes.

Laboratorio Completado