

Ivan Castillo

S2: Laboratorio: Endurecimiento de sistemas Reforzamiento de sistemas con gerente de parches mediante AWS Systems Manager

Información general sobre el laboratorio

En organizaciones con cientos e incluso miles de estaciones de trabajo, puede ser logísticamente difícil mantener todo el software de sistemas operativos (SO) y de aplicaciones actualizado. En la mayoría de los casos, las actualizaciones de SO en las estaciones de trabajo se pueden aplicar automáticamente mediante la red. Sin embargo, los administradores deben tener una política de seguridad clara y un plan de referencia para asegurarse de que todas las estaciones de trabajo estén funcionando en una versión mínima del software.

En este laboratorio, usará gerente de parches, una funcionalidad de AWS Systems Manager, para crear un valor de referencia de parches. Luego, usará el valor de referencia de parches para escanear las instancias de Amazon Elastic Compute Cloud (Amazon EC2) para Linux y Windows que se crearon previamente para este laboratorio. También aprenderá cómo crear un período de mantenimiento para automatizar el proceso de escaneo y parchado.

El enfoque principal de gerente de parches es instalarlas actualizaciones relacionadas con la seguridad del SO en los nodos administrados.

OBJETIVOS

Después de completar este laboratorio, podrá realizar lo siguiente:

- Crear un valor de referencia de parche personalizado
- Modificar los grupos de parches
- Configurar la aplicación de parches
- Programar un período de mantenimiento
- Realizar un escaneo instantáneo
- Verificar la conformidad de parches

ENTORNO DEL LABORATORIO

El entorno actual tiene seis instancias de EC2: tres instancias con el SO Linux y tres con el SO Windows.



Todos los componentes de backend, como las instancias de EC2, los roles de AWS Identity and Access Management (IAM) y algunos servicios de AWS, ya están incorporados en su laboratorio.

Tarea 1: Seleccionar valores de referencia de parches

En esta tarea, seleccionará un valor de referencia de parches para aplicarlo a las instancias de EC2 de Linux. Luego, creará un valor de referencia de parches personalizado para las instancias de EC2 de servidor de Windows.

El gerente de parches proporciona valores de referencia de parches predefinidos para cada uno de los sistemas operativos que admite. Puede usar estos valores de referencia de parches como están configurados actualmente (no puede personalizarlos) o puede crear sus propios valores de referencia de parches. Puede usar valores de referencia de parches personalizados para tener un mayor control sobre cuáles parches se aprueban o rechazan para su entorno.

1. En la Consola de administración de AWS, en el cuadro de búsqueda, ingrese **Systems Manager** y selecciónelo. Esta opción lo lleva a la página de la consola de Systems Manager.
2. En el panel de navegación izquierdo, en **Node Management** (Administración de nodos), elija **Fleet Manager** (Administrador de flotas). Estas son las instancias de EC2 preconfiguradas. Hay tres instancias de Linux y tres instancias de Windows. Estas instancias de EC2 necesitan un rol de IAM específico para activar Systems Manager en las instancias, por lo que puede verlos en la sección Fleet Manager (Administrador de flotas). Esto también es parte de la preparación del laboratorio.
3. Marque la casilla situada junto a **Linux-1**. Luego, seleccione la lista desplegable **Node actions** (Acciones de nodos) y seleccione **View details** (Ver detalles). Aquí puede ver detalles acerca de la instancia específica, como **Platform type** (Tipo de plataforma), **Node type** (Tipo de nodo), **OS name** (Nombre de SO) y **IAM role** (Rol de IAM) que le permite usar Systems Manager.

General			
ID de nodo i-02ba8a4eb1b4d4cd3	Nombre Linux-1	Nombre de clave AWSLabsKeyPair-vvf3xw8fK44c4VkTiEnMNV	Recuento de parches con errores -
Tipo de plataforma Linux	Zona de disponibilidad us-west-2a	Estado del ping  Online	Recuento de parches instalados -
Tipo de origen Instancia de EC2	Nombre de equipo ip-10-0-2-112.us-west-2.compute.internal	Sistema operativo Amazon Linux	Grupo de parches -
ID de activación -	Rol de IAM -	Versión de la plataforma 2	ID de imagen ami-076e3756930a93fbb
Versión de agente 3.2.1705.0	Rol de instancia arn:aws:iam::520940006427:instance-profile/RoleForSSM	Tipo de recurso Instancia de EC2	
Arquitectura x86_64	Estado del nodo  En ejecución	ID de origen i-02ba8a4eb1b4d4cd3	
Estado de la asociación -	Dirección IP 10.0.2.112	Recuento de parches crítico no conforme -	

4. En la parte superior de la página, seleccione **AWS Systems Manager** para volver a la página de inicio de Systems Manager.
5. En el panel de navegación izquierdo, en **Node Management** (Administración de nodos), elija **Patch Manager** (Gerente de parches).
6. Seleccione el botón **View predefined patch baselines** (Ver valores de referencia de parches predefinidos).

7. Seleccione la pestaña **Patch baselines** (Valores de referencia de parches). Esta pestaña incluye los valores de referencia de parches predeterminados que puede seleccionar.
8. En la barra de búsqueda, ingrese **AWS-AmazonLinux2DefaultPatchBaseline** y presione Intro. Luego, seleccione el botón de opción junto al valor de referencia que se indica.
9. Seleccione la lista desplegable **Actions** (Acciones) y seleccione **Modify patch groups** (Modificar grupos de parches). Puede usar el grupo de parches para asociar los nodos administrados con un valor de referencia de parches específico en gerente de parches. Los grupos de parches ayudan a asegurarse de que esté implementando los parches apropiados al conjunto de nodos correcto según las reglas de valores de referencia de parches.
10. En la sección **Modify patch groups** (Modificar grupos de parches) en **Patch groups** (Grupos de parches), ingrese **LinuxProd** y, luego, seleccione el botón **Add** (Agregar).
11. Seleccione **Close** (Cerrar).

Aplicar parches a las instancias ahora [Información](#)

Configuración básica

Analizar para buscar si faltan parches o instalar parches, con o sin reinicio. Para ver más opciones de aplicación de parches, utilice la página [Configurar la aplicación de parches](#).

Operación de aplicación de parches

- ☐ Analizar
- ☒ Analizar e instalar

Opción de reinicio

Especifique si Patch Manager debe reiniciar las instancias, o reiniciar según una programación

- ☒ Reiniciar si es necesario
- ☐ No reiniciar mis instancias
- ☐ Programar una hora de reinicio

Instancias a las que se aplicarán parches

Elija entre aplicar parches a todas las instancias o solo a las que especifique

- ☐ Aplicar parches a todas las instancias
- ☒ Aplicar parches únicamente a las instancias de destino que especifique

Selección de destino

Elija un método para seleccionar destinos.

- ☒ Especificar etiquetas de instancia
- Especifique uno o varios pares clave-valor de etiqueta para seleccionar instancias que compartan esas etiquetas.

- ☐ Elegir instancias manualmente
- Seleccione manualmente las instancias que desea registrar como destinos.

- ☐ Elegir un grupo de recursos
- Elija un grupo de recursos que incluya los recursos a los que desea dirigirse.

Especificar etiquetas de instancia

Especifique uno o varios pares clave-valor de etiqueta de instancia para identificar las instancias en las que se ejecutarán las tareas.

Clave de etiqueta

Valor de etiqueta (opcional)

Escriba una clave de etiqueta y el valor opcional aplicados a las instancias a las que desea dirigirse y, a continuación, elija **Agregar**

Resumen de ejecución de asociación

AWS-PatchNowAssociation

ID de asociación
[0a4205ac-b4f2-4945-bf73-a6dc2da936db](#)

Estado
✔ Success

Opción de reinicio
RebootIfNeeded

Summary
Success=3

ID de ejecución
[d4f99eed-ac3b-4a1d-9601-d1eaf5d3144a](#)

Operación
Install

Destinos
Instancelds: 3

Resumen de la operación de análisis/instalación



■ Pendiente ■ Omitido ■ Realizado correctamente ■ Error

Resumen de ejecución de asociación

AWS-PatchNowAssociation

ID de asociación
[0a4205ac-b4f2-4945-bf73-a6dc2da936db](#)

Estado
⌚ Pending

Opción de reinicio
RebootIfNeeded

Progress
Pending=3

ID de ejecución
[d4f99eed-ac3b-4a1d-9601-d1eaf5d3144a](#)

Operación
Install

Destinos
Instancelds: 3

Resumen de la operación de análisis/instalación



■ Pendiente ■ Omitido ■ Realizado correctamente ■ Error

TAREA 1.1: ETIQUETAR INSTANCIAS

En esta tarea, etiquetará sus instancias de Windows. Más adelante en el laboratorio, creará un grupo de parches y lo asociará con estas etiquetas.

Las instancias de Linux se preconfiguraron durante la preparación del laboratorio con etiquetas LinuxProd y no es necesario agregar más etiquetas.

12. En la Consola de administración de AWS, en la barra de búsqueda , ingrese **EC2** y selecciónelo.
13. Seleccione la casilla de verificación junto a la instancia de **Windows-1** y, luego, seleccione la pestaña **Tags** (Etiquetas).
14. Seleccione el botón **Manage tags** (Administrar etiquetas), seleccione **Add tag** (Agregar etiqueta) y configure las siguientes opciones:
 - **Key** (Clave): ingrese **Patch Group**
 - **Value** (Valor): ingrese **WindowsProd**
15. Seleccione **Save** (Guardar).
16. Repita los pasos anteriores para etiquetar las instancias de **Windows-2** y **Windows-3** con las mismas etiquetas.

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 - <i>opcional</i>	
<input type="text" value="Name"/>	<input type="text" value="Windows-1"/>	<button>Eliminar</button>
<input type="text" value="Patch Group"/>	<input type="text" value="WindowsProd"/>	<button>Eliminar</button>
<input type="text" value="Usar " windowsprod""=""/>		

Agregar nueva etiqueta

Puede agregar hasta 48 etiquetas más.

CancelarGuardar

TAREA 1.2: CREAR UN VALOR DE REFERENCIA DE PARCHE PERSONALIZADO

Luego, creará un valor de referencia de parches personalizado para las instancias de Windows. Aunque Windows tiene valores de referencia de parches predeterminados que puede usar, para este caso práctico, establecerá un valor de referencia para las actualizaciones de seguridad de Windows.

17. Vuelva a la consola de Systems Manager. En la barra de búsqueda en la parte superior, ingrese **Systems Manager** y, luego, selecciónelo.
18. En el panel de navegación izquierdo, en **Node Management** (Administración de nodos), elija **Patch Manager** (Gerente de parches).
19. En la sección **Patch your instances** (Aplicar parches a sus instancias), seleccione **View predefined patch baselines** (Ver valores de referencia de parches predefinidos).
20. Seleccione la pestaña **Patch baselines** (Valores de referencia de parches).
21. Seleccione el botón **Create patch baseline** (Crear valor de referencia de parches).
22. En **Patch baseline details** (Detalles del valor de referencia de parches), configure las opciones siguientes:

- En **Name** (Nombre), ingrese **WindowsServerSecurityUpdates**
- En **Description- optional** (Descripción- opcional), ingrese **Windows security baseline patch**
- En **Operating system** (Sistema operativo), seleccione **Windows**.
- Deje la casilla de **Default patch baseline** (Valor de referencia de parches predeterminado) sin seleccionar.

23. En la sección **Approval rules for operating systems** (Reglas de aprobación para los sistemas operativos), configure las siguientes opciones:

- **Product** (Producto): en la lista desplegable, elija **WindowsServer2019**.
- **Severity** (Severidad): esta opción indica el valor de severidad de los parches a los que se aplica la regla. Para asegurarse de que todos los paquetes de servicio estén incluidos en la regla, seleccione **Critical** (Crítico) en la lista desplegable.
- **Classification** (Clasificación): en la lista desplegable, elija **SecurityUpdates**.
- **Auto-approval** (Aprobación automática): ingrese **3** días.
- **Compliance reporting- optional** (Informe de conformidad: Opcional): en la lista desplegable, seleccione **Critical** (Crítica).

24. Seleccione **Add rule** (Agregar regla) para agregar una segunda regla a este valor de referencia de parches y configure las siguientes opciones:

- **Product** (Producto): en la lista desplegable, elija **WindowsServer2019**.
- **Severity** (Severidad): en la lista desplegable, elija **Important** (Importante).
- **Classification** (Clasificación): en la lista desplegable, elija **SecurityUpdates**.
- **Auto-approval** (Aprobación automática): ingrese **3** días.
- **Compliance reporting- optional** (Informe de conformidad: Opcional): en la lista desplegable, seleccione **High** (Alta).

25. Seleccione **Create patch baseline** (Crear valor de referencia de parches).

A continuación, modifique un grupo de parches para el valor de referencia de parches de Windows que acaba de crear.

26. En la sección **Patch baselines** (Valores de referencia de parches), seleccione el botón para el valor de referencia de parches **WindowsServerSecurityUpdates** que acaba de crear. **Nota:** El valor de referencia de parches que creó puede estar en la segunda página de la lista de valores de referencia.

27. Seleccione la lista desplegable **Actions** (Acciones) y, luego, seleccione **Modify patch groups** (Modificar grupos de parches).
28. En la sección **Modify patch groups** (Modificar grupos de parches), en **Patch groups** (Grupos de parches), ingrese **WindowsProd**
29. Seleccione el botón **Add** (Agregar) y, luego, seleccione **Close** (Cerrar).

Crear un punto de referencia de parches

Detalles de punto de referencia de parches

Nombre

WindowsServerSecurityUpdates

Puede utilizar letras, números, puntos, guiones y guiones bajos en el nombre.

Descripción - *opcional*

Windows security baseline patch

Sistema operativo

Seleccione el sistema operativo para el que desea especificar las reglas de aprobación y las excepciones de los parches.

Windows

Punto de referencia de parches predeterminado

☐ Establezca este punto de referencia de parches como el predeterminado para las instancias Windows.

Reglas de aprobación para sistemas operativos

Cree reglas de aprobación automática para especificar que determinados tipos de parches del sistema operativo se aprueban automáticamente.

Regla del sistema operativo 1

✕ Eliminar regla

Productos

Seleccionar parches por producto

Seleccionar productos

WindowsServer2019 ✕

Clasificación

Aprobación automática

Especificar cómo seleccionar actualizaciones para la aprobación automática

☒ Aprobar parches después de un número especificado de días

☐ Aprobar los parches publicados hasta una fecha específica

Especifique el número de días

3

días

Regla del sistema operativo 1

✕ Eliminar regla

Productos
Seleccionar parches por producto
Seleccionar productos
WindowsServer2019 ✕

Clasificación
Seleccionar parches por clasificación
Seleccionar clasificaciones
SecurityUpdates ✕

Gravedad
Seleccionar parches por gravedad
Seleccionar gravedades
Critical ✕

Aprobación automática
Especificar cómo seleccionar actualizaciones para la aprobación automática
☒ Aprobar parches después de un número especificado de días
☐ Aprobar los parches publicados hasta una fecha específica
Especifique el número de días
3 días

Informes de conformidad - *opcional*
Especifique el nivel de gravedad para informar de los parches que coincidan con esta regla.
Crítica

Regla del sistema operativo 2

✕ Eliminar regla

Productos
Seleccionar parches por producto
Seleccionar productos
WindowsServer2019 ✕

Clasificación
Seleccionar parches por clasificación
Seleccionar clasificaciones
SecurityUpdates ✕

Gravedad
Seleccionar parches por gravedad
Seleccionar gravedades
Important ✕

Aprobación automática
Especificar cómo seleccionar actualizaciones para la aprobación automática
☒ Aprobar parches después de un número especificado de días
☐ Aprobar los parches publicados hasta una fecha específica
Especifique el número de días
3 días

Informes de conformidad - *opcional*
Especifique el nivel de gravedad para informar de los parches que coincidan con esta regla.
Alta

Modificar grupos de parches

Grupos de parches

Puede crear un máximo de 25 valores de etiqueta para definir grupos de parches para esta base de referencia de revisiones. Las claves de etiqueta se denominan automáticamente **Grupo de parches**. [Más información](#)

ID de base de referencia

pb-03665e44610ac8a7a

Nombre de base de referencia

WindowsServerSecurityUpdates

Descripción de base de referencia

Windows security baseline patch

Grupos de parches

WindowsProd

Agregar

Los valores de grupo de parches pueden constar de un máximo de 256 letras, números y los siguientes caracteres: . _ + @ / - + :

No hay ningún grupo de parches asociado

Cerrar

RESUMEN DE LA TAREA 1

En esta tarea, usó un valor de referencia 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

En esta tarea, configuró los parches para las instancias de Linux y creó un periodo de mantenimiento programado. Luego, aplicó el parche a las instancias de Windows manualmente.

Después de la configuración, el gerente de parches usa **Run Command** (Comando Ejecutar) 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 el programa definido (periodo de mantenimiento).

30. En la página de la consola del **Patch Manager** (Gerente de parches), seleccione el botón **Configure patching** (Configurar la aplicación de parches).
31. En la sección **Instances to patch** (Instancias a las que aplicar parches), seleccione **Select a patch group** (Seleccionar un grupo de parches) y, luego, seleccione **LinuxProd** en la lista desplegable.
32. En **Patching schedule** (Programa de aplicación de parches), seleccione **Schedule in a new Maintenance Window** (Programar un nuevo periodo de mantenimiento) y, luego, configure las siguientes opciones:

- **How do you want to specify a Maintenance Window schedule?** (¿Cómo desea especificar un programa de periodo de mantenimiento?): seleccione **Use a CRON schedule builder** (Usar un creador de programas CRON).
- **Maintenance Window run frequency** (Frecuencia de ejecución de periodo de mantenimiento): seleccione el botón opción para **Every** (Cada). En la lista desplegable **Select** (Seleccionar), elija **Every Day** (Todos los días) e ingrese **02:00**
- **Maintenance Window duration** (Duración de periodo de mantenimiento): ingrese **1**
- **Maintenance Window name** (Nombre de periodo de mantenimiento): ingrese **Linux-Maintenance**

33. En la sección **Patching operation** (Operación de la aplicación de parches), seleccione **Scan and install** (Analizar e instalar) y seleccione el botón **Configure patching** (Configurar la aplicación de parches).

TAREA 2.1: APLICAR PARCHES A INSTANCIAS DE FORMA INSTANTÁNEA

34. En la página de la consola de **Patch Manager** (Gerente de parches), seleccione la pestaña **Patch baselines** (Valores de referencia de parches) y, luego, seleccione el botón para el valor de referencia de **WindowsServerSecurityUpdates** que creó antes.
35. Seleccione **Configure patching** (Configurar la aplicación de parches).
36. En **Configure patching** (Configurar la aplicación de parches), configure las siguientes opciones:
 - **How do you want to select instances?** (¿Cómo desea seleccionar las instancias?): seleccione **Select a patch group** (Seleccionar un grupo de parches).
 - **Patch groups** (Grupos de parches): seleccione **WindowsProd**.
 - **How do you want to specify a patching schedule?** (¿Cómo quiere especificar un programa de aplicación de parches): seleccione **Skip scheduling and patch instances now** (Omitir el programa y aplicar parches a las instancias ahora).

- **Patching operation** (Operación de la aplicación de parches): seleccione **Scan and install** (Analizar e instalar).

37. Seleccione el botón **Configure patching** (Configurar la aplicación de parches).

38. En la parte superior de la página, debería ver un anuncio verde con el mensaje **Successfully configured patching** (La aplicación de parches se configuró correctamente). Seleccione el botón **View details** (Ver detalles).

Tras bambalinas, el gerente de parches usa el **comando Run** para ejecutar el documento **AWS-RunPatchBaseline**. Ahora puede ver las instancias de Windows en progreso.

Un documento de Systems Manager (documento de SSM) define las acciones que realiza Systems Manager en sus instancias administradas.

39. Seleccione el botón de actualizar en la consola de AWS.

Espere hasta que pueda ver **Success** (Éxito) para el **Status** (Estado) de todas las instancias.

40. Seleccione el botón de opción para una de las instancias que se acaban de analizar y seleccione el botón **View output** (Ver resultado).

41. En la sección **Step 1 - Command description and status** (Paso 1: Descripción y estado del comando), expanda **Resultado**. Como lo indica **Step name** (Nombre del paso), este paso aplica los parches a las instancias de Windows (**PatchWindows**).

42. Desplácese por el resultado y busque **InstalledCount** para ver cuántos parches se instalaron.

A continuación hay otra información clave disponible en el resultado:

- PatchGroup
- BaselineId
- OperationStartTime
- OperationEndTime
- FailedCount

Aunque configuró un periodo de mantenimiento programado para el grupo de parches **LinuxProd**, es preferible aplicar los parches ahora para asegurarse.

43. En el panel de navegación izquierdo, en **Node Management** (Administración de nodos), elija **Patch Manager** (Gerente de parches).

44. Seleccione **Configure patching** (Configurar la aplicación de parches).

45. En **Configure patching** (Configurar la aplicación de parches), configure las siguientes opciones:

- **How do you want to select instances?** (¿Cómo desea seleccionar las instancias?): seleccione **Select a patch group** (Seleccionar un grupo de parches).
- **Patch groups** (Grupos de parches): seleccione **LinuxProd**.
- **How do you want to specify a patching schedule?** (Cómo quiere especificar un programa de aplicación de parches): seleccione **Skip scheduling and patch instances now** (Omitir el programa y aplicar parches a las instancias ahora).

- **Patching operation** (Operación de la aplicación de parches): seleccione **Scan and install** (Analizar e instalar).

46. Seleccione el botón **Configure patching** (Configurar la aplicación de parches).

TAREA 2.2: VERIFICACIÓN DE CONFORMIDAD

47. En el panel de navegación izquierdo, en **Node Management** (Administración de nodos), elija **Patch Manager** (Gerente de parches).
48. Seleccione la pestaña **Dashboard** (Panel). En **Compliance summary** (Resumen de conformidad), ahora debería poder ver **Compliant: 6** (En conformidad: 6), que verifica que todas las instancias de Windows y Linux están en conformidad.
49. Seleccione la pestaña **Compliance reporting** (Informes de conformidad). Este laboratorio proporciona información general de todas las instancias en ejecución de SSM. Debería poder comprobar que el **Compliance status** (Estado de conformidad) de todas las instancias de Linux y Windows es **Compliant** (En conformidad).

Modificar grupos de parches

Grupos de parches

Puede crear un máximo de 25 valores de etiqueta para definir grupos de parches para esta base de referencia de revisiones. Las claves de etiqueta se denominan automáticamente **Grupo de parches**. [Más información](#)

ID de base de referencia

arn:aws:ssm:us-west-2:280605243866:patchbaseline/pb-0e930e75b392d70da

Nombre de base de referencia

AWS-AmazonLinux2DefaultPatchBaseline

Descripción de base de referencia

Default Patch Baseline for Amazon Linux 2 Provided by AWS.

Grupos de parches

Agregar

Los valores de grupo de parches pueden constar de un máximo de 256 letras, números y los siguientes caracteres: . _ + @ / - + :

LinuxProd X

RESUMEN DE LA TAREA 2

En esta tarea, configuró los parches y creó un periodo de mantenimiento programado para el grupo LinuxProd. Ahora, esto analizará e instalará parches (si están disponibles) todos los días a las 2 AM.

Aprendió a analizar e instalar parches de forma instantánea y analizar los resultados del comando Run para ver las actualizaciones de parches. Comprobó mediante los informes de conformidad de que todas las instancias de EC2 han sido analizadas y actualizadas y están en conformidad.

Conclusión

¡Felicitaciones! Aprendió a realizar correctamente las siguientes tareas:

- Crear un valor de referencia de parche personalizado
- Modificar dos grupos de parches
- Configurar la aplicación de parches
- Programar un periodo de mantenimiento
- Llevar a cabo un análisis instantáneo y comprobar la conformidad de los parches

AWS Systems Manager > Patch Manager > Informes de conformidad

Patch Manager Información

[Aplicar parches ahora](#) [Crear política de revisión](#)

► Información general sobre las operaciones de aplicación de revisiones: *nuevo*

Panel **Informes de conformidad** Bases de referencia de revisiones Parches Grupos de parches Configuración

Detalles de revisiones en nodos (6) [Ver registro](#) [Ver detalle](#) [Exportar a S3](#) [Ver todas las exportaciones de S3](#)

	Nombre	ID de nodo	Nombre de configuración de revisión	Tipo de configuración de revisión	Estado de conformidad	Recuento de incumplimientos críticos	Recuento de incumplimientos de seguridad
<input type="radio"/>	Linux-1	i-094ae677a3150f98a	-	Patch group	Conforme	0	0
<input type="radio"/>	Windows-1	i-02febbdd43826c14d	-	Patch group	Conforme	0	0
<input type="radio"/>	Windows-3	i-0e76681175e804dd6	-	Patch group	Conforme	0	0
<input type="radio"/>	Linux-3	i-058c379f40b2dd3a6	-	Patch group	Conforme	0	0
<input type="radio"/>	Linux-2	i-07561ed7ff6e92082	-	Patch group	Conforme	0	0
<input type="radio"/>	Windows-2	i-0aa34593725408017	-	Patch group	Conforme	0	0