




ENDURECIMIENTO DE SISTEMAS

LABORATORIO N° 277



-ESTEBAN CAMEJO
-IGNACIO SUAREZ
-MICHELLE DEVERA
-SANTIAGO BURGUEÑO
-MANUELA RODRIGUEZ
-JUAN SANSBERRO

OBJETIVOS

- Crear un valor de referencia de parche personalizado
- Modificar los grupos de parches
- Configurar la aplicación de parches
- Verificar la conformidad de parches

TAREA 1: SELECCIONAR VALORES DE REFERENCIA DE PARCHES

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

- Ingresamos a Fleet Manager para ver todas las instancias EC2 pre-configuradas activas



Fleet Manager [Info](#)

Settings ▾

Account management ▾

Managed Nodes (6)

🔄

📄 Report

Node actions ▲

Node overview

Connect ▶

Tools ▶

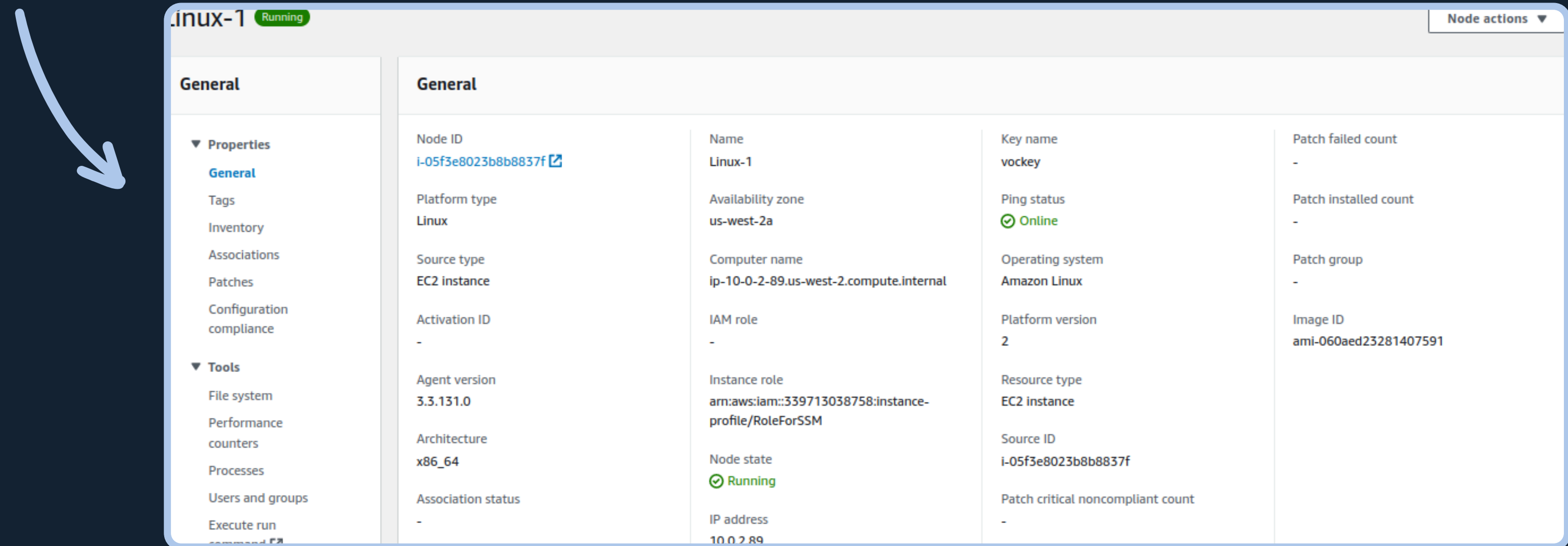
Node settings ▶

🔍 Filter

🕒 Last fetched at: 8:16 PM

<input type="checkbox"/>	Node ID ▲	Node state ▼	Name ▼	Platform t... ▼	Operating... ▼	Resource t... ▼	Source ID	Ping status ▼	Agent ver... ▼	Image ID ▼	EC2 Insta...
<input type="checkbox"/>	i-00ccb6551...	🟢 Running	Windows-1	Windows	Microsoft Wi...	EC2 instance	-	🟢 Online	3.3.131.0	ami-04eb6b...	Open EC2...
<input type="checkbox"/>	i-03d6f7db9...	🟢 Running	Linux-3	Linux	Amazon Linux	EC2 instance	-	🟢 Online	3.3.131.0	ami-060aed2...	Open EC2...
<input checked="" type="checkbox"/>	i-05f3e8023...	🟢 Running	Linux-1	Linux	Amazon Linux	EC2 instance	-	🟢 Online	3.3.131.0	ami-060aed2...	Open EC2...
<input type="checkbox"/>	i-05ff9f738c...	🟢 Running	Linux-2	Linux	Amazon Linux	EC2 instance	-	🟢 Online	3.3.131.0	ami-060aed2...	Open EC2...
<input type="checkbox"/>	i-0a99de1b3...	🟢 Running	Windows-2	Windows	Microsoft Wi...	EC2 instance	-	🟢 Online	3.3.131.0	ami-04eb6b...	Open EC2...
<input type="checkbox"/>	i-0dd846911...	🟢 Running	Windows-3	Windows	Microsoft Wi...	EC2 instance	-	🟢 Online	3.3.131.0	ami-04eb6b...	Open EC2...

- Aquí puede ver detalles acerca de la instancia Linux-1 seleccionada, tales como el Tipo de plataforma, el tipo de nodo, el nombre del SO y el rol de IAM que le permite usar Systems Manager.



The screenshot displays the AWS Systems Manager console interface for a specific instance named 'Linux-1', which is in a 'Running' state. The interface is divided into a left sidebar and a main content area. The sidebar contains a 'General' tab, which is highlighted by a blue arrow, and a 'Tools' section with various options like 'File system', 'Performance counters', and 'Processes'. The main content area shows a detailed view of the instance's properties, organized into a table-like structure with columns for different categories of information.

General				
Node ID i-05f3e8023b8b8837f	Name Linux-1	Key name vockey	Patch failed count -	
Platform type Linux	Availability zone us-west-2a	Ping status Online	Patch installed count -	
Source type EC2 instance	Computer name ip-10-0-2-89.us-west-2.compute.internal	Operating system Amazon Linux	Patch group -	
Activation ID -	IAM role -	Platform version 2	Image ID ami-060aed23281407591	
Agent version 3.3.131.0	Instance role arn:aws:iam::339713038758:instance-profile/RoleForSSM	Resource type EC2 instance		
Architecture x86_64	Node state Running	Source ID i-05f3e8023b8b8837f		
Association status -	IP address 10.0.2.89	Patch critical noncompliant count -		

Patch baselines (1/17)

Filter patch baselines 1 match

AWS-AmazonLinux2DefaultPatchBaseline X Clear filter

View details Edit Delete Actions ▲ Create patch baseline

Set default patch baseline Modify patch groups

< 1 >

Baseline ID	Baseline name	Description	Operating system	Default baseline
pb-0e930e75b392d70da	AWS-AmazonLinux2DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	Amazon Linux 2	✔ Yes

En este paso en “Patch Baselines” buscamos la de nombre “AWS-AmazonLinux2DefaultPatchBaseline” y le modificamos el grupo de parche agregando a “LinuxProd”

Modify patch groups

Patch groups

You can create up to 25 tag values to define patch groups for this patch baseline. Tag keys are automatically named Patch Group. [Learn more](#)

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

Baseline name
AWS-AmazonLinux2DefaultPatchBaseline

Baseline description
Default Patch Baseline for Amazon Linux 2 Provided by AWS.

Patch groups

Add

Patch group values can consist of up to 256 letters, numbers, and the following characters: . _ + @ / - + :

LinuxProd X

Close

TAREA 1.1: ETIQUETAR INSTANCIAS

Manage tags

Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - optional	
<div><div>cloudlab</div><div>X</div></div>	<div><div>c110983a2632292l6678211t1w</div><div>X</div></div>	<div>Remove</div>
<div><div>Name</div><div>X</div></div>	<div><div>Windows-3</div><div>X</div></div>	<div>Remove</div>
<div><div>Patch Group</div><div>X</div></div>	<div><div>WindowsProd</div><div>X</div></div>	<div>Remove</div>

Add new tag

You can add up to 47 more tags.

Cancel

Save

Manage tags

Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - optional	
<div><div>Name</div><div>X</div></div>	<div><div>Windows-1</div><div>X</div></div>	<div>Remove</div>
<div><div>cloudlab</div><div>X</div></div>	<div><div>c110983a2632292l6678211t1w</div><div>X</div></div>	<div>Remove</div>
<div><div>Patch Group</div><div>X</div></div>	<div><div>WindowsProd</div><div>X</div></div>	<div>Remove</div>

Add new tag

You can add up to 47 more tags.

Cancel

Save

En este paso, en la pestaña "Etiquetas", agregamos una nueva etiqueta llamada "Patch Group" con el valor "WindowsProd" y repetimos este proceso para cada instancia Windows.

Manage tags

Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - optional	
<div><div>cloudlab</div><div>X</div></div>	<div><div>c110983a2632292l6678211t1w</div><div>X</div></div>	<div>Remove</div>
<div><div>Name</div><div>X</div></div>	<div><div>Windows-2</div><div>X</div></div>	<div>Remove</div>
<div><div>Patch Group</div><div>X</div></div>	<div><div>WindowsProd</div><div>X</div></div>	<div>Remove</div>

Add new tag

You can add up to 47 more tags.

Cancel

Save

TAREA 1.2: CREAR UN VALOR DE REFERENCIA DE PARCHE PERSONALIZADO

Patch baseline details

Name

WindowsServerSecurityUpdates

You can use letters, numbers, periods, dashes, and underscores in the name.

Description - optional

Windows security baseline patch

Operating system

Select the operating system you want to specify approval rules and patch exceptions for.

Windows

Default patch baseline

☐ Set this patch baseline as the default patch baseline for Windows instances.

- Crearemos un valor de referencia de parches personalizado para las instancias de Windows
- En Patch baseline details, configure las opciones siguientes:

- En la sección Approval rules for operating systems, configure las siguientes opciones:

Approval rules for operating systems

Create auto-approval rules to specify that certain types of operating system patches are approved automatically.

Operating system rule 1

 Remove rule

Products

Select patches by product

Select products

WindowsServer2019 

Classification

Select patches by classification

Select classifications

SecurityUpdates 

Severity

Select patches by severity

Select severities

Critical 

Auto-approval

Specify how to select updates for automatic approval

☒ Approve patches after a specified number of days

☐ Approve patches released up to a specific date

Specify the number of days

3

days

Compliance reporting - optional

Specify the severity level to report for patches that match this rule.

Critical

- Seleccione Add rule para agregar una segunda regla a este valor de referencia de parche y configure las siguientes opciones:



Operating system rule 2

Remove rule

Products

Select patches by product

Select products

WindowsServer2019

Classification

Select patches by classification

Select classifications

SecurityUpdates

Severity

Select patches by severity

Select severities

Important

Auto-approval

Specify how to select updates for automatic approval

☒ Approve patches after a specified number of days

☐ Approve patches released up to a specific date

Specify the number of days

3 days

Compliance reporting - optional

Specify the severity level to report for patches that match this rule.

High

Add rule

8 remaining

Patch baselines (1/18)

Filter patch baselines 1 match

WindowsServerSecurityUpdates X Clear filter

View details Edit Delete Actions ▲ Create patch baseline

Set default patch baseline

Modify patch groups

< 1 >

Baseline ID	Baseline name	Description	Operating system	Default baseline
pb-034899c0768dbb7fe	WindowsServerSecurityUpdates	Windows security baseline patch	Windows	Yes

- Ahora seleccionamos la Patch Baseline de Windows que hemos creado y la modificaremos, para así asociarlo con un grupo de parches.
- Ingresamos en Actions, luego en Modify patch groups, y en patch groups escribiremos WindowsProd y le damos en Add, y luego en Close

Patch groups

You can create up to 25 tag values to define patch groups for this patch baseline. Tag keys are automatically named Patch Group. [Learn more](#)

Baseline ID
pb-087b329b81616b3f4

Baseline name
WindowsServerSecurityUpdates

Baseline description
Windows security baseline patch

Patch groups

Add

Patch group values can consist of up to 256 letters, numbers, and the following characters: . _ + @ / - + :

WindowsProd X

Close

TAREA 2: CONFIGURAR LA APLICACIÓN DE PARCHES

Después de la configuración, *Patch Manager* 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 la programación definida (periodo de mantenimiento).

TAREA 2.1: APLICAR PARCHE A LAS INSTANCIAS DE LINUX

- Aplicamos el parche a las instancia de Linux



Basic configuration

Scan for missing patches or Install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

Patching operation

☐ Scan

☒ Scan and install

Reboot option

Specify whether Patch Manager should reboot your instances, or reboot on a schedule

☒ Reboot if needed

☐ Do not reboot my instances

☐ Schedule a reboot time

Instances to patch

Choose whether to patch all instances or only the instances you specify

☐ Patch all instances

☒ Patch only the target instances I specify

Target selection

Choose a method for selecting targets.

☒ **Specify instance tags**
Specify one or more tag key-value pairs to select instances that share those tags.

☐ **Choose instances manually**
Manually select the instances you want to register as targets.

☐ **Choose a resource group**
Choose a resource group that includes the resources you want to target.

Specify instance tags

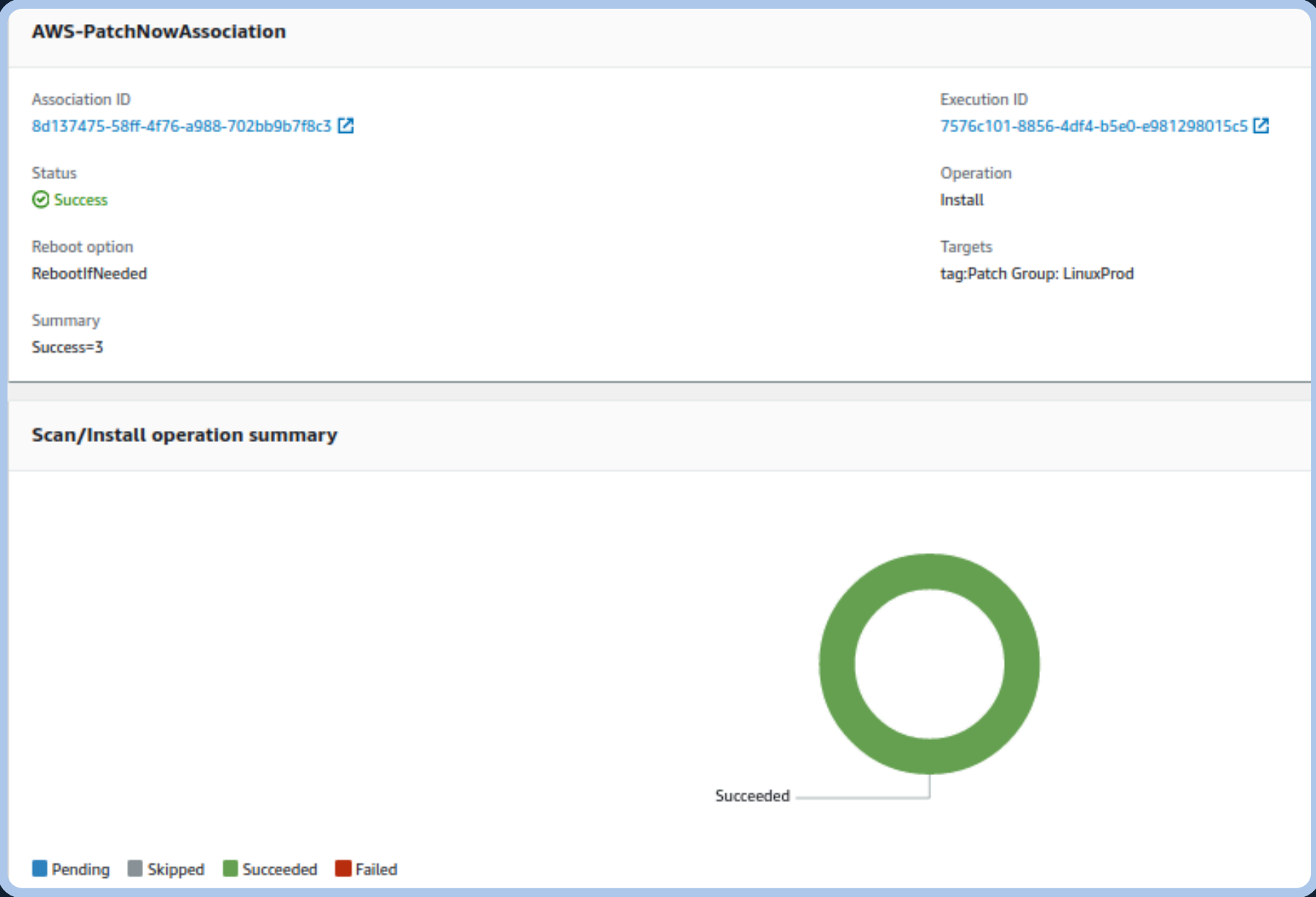
Specify one or more instance tag key-value pairs to identify the instances where the tasks will run.

Tag key

Tag value (optional)

Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Patch Group : LinuxProd X



TAREA 2.2: APLICAR PARCHE A LAS INSTANCIAS DE WINDOWS

- Aplicamos el parche a las instancia de Windows



Basic configuration

Scan for missing patches or Install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

Patching operation

☐ Scan

☒ Scan and install

Reboot option

Specify whether Patch Manager should reboot your instances, or reboot on a schedule

☒ Reboot if needed

☐ Do not reboot my instances

☐ Schedule a reboot time

Instances to patch

Choose whether to patch all instances or only the instances you specify

☐ Patch all instances

☒ Patch only the target instances I specify

Target selection

Choose a method for selecting targets.

☒ Specify instance tags

☐ Choose instances manually

☐ Choose a resource group

Specify one or more tag key-value pairs to identify the instances where the tasks will run.

Specify one or more instance tag key-value pairs to identify the instances where the tasks will run.

Tag key

Tag value (optional)

Add

Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Specify one or more tag key-value pairs to select instances that share those tags.

Manually select the instances you want to register as targets.

Choose a resource group that includes the resources you want to target.

Specify instance tags

Specify one or more instance tag key-value pairs to identify the instances where the tasks will run.

Tag key

Tag value (optional)

Add

Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Patch Group : WindowsProd X

AWS-PatchNowAssociation

Association ID	8d137475-58ff-4f76-a988-702bb9b7f8c3	Execution ID	aa0f5c50-5082-4177-926b-d441d53cd48e
Status	Success	Operation	Install
Reboot option	RebootIfNeeded	Targets	tag:Patch Group: WindowsProd
Summary	Success=3		

Scan/Install operation summary

Succeeded

Pending

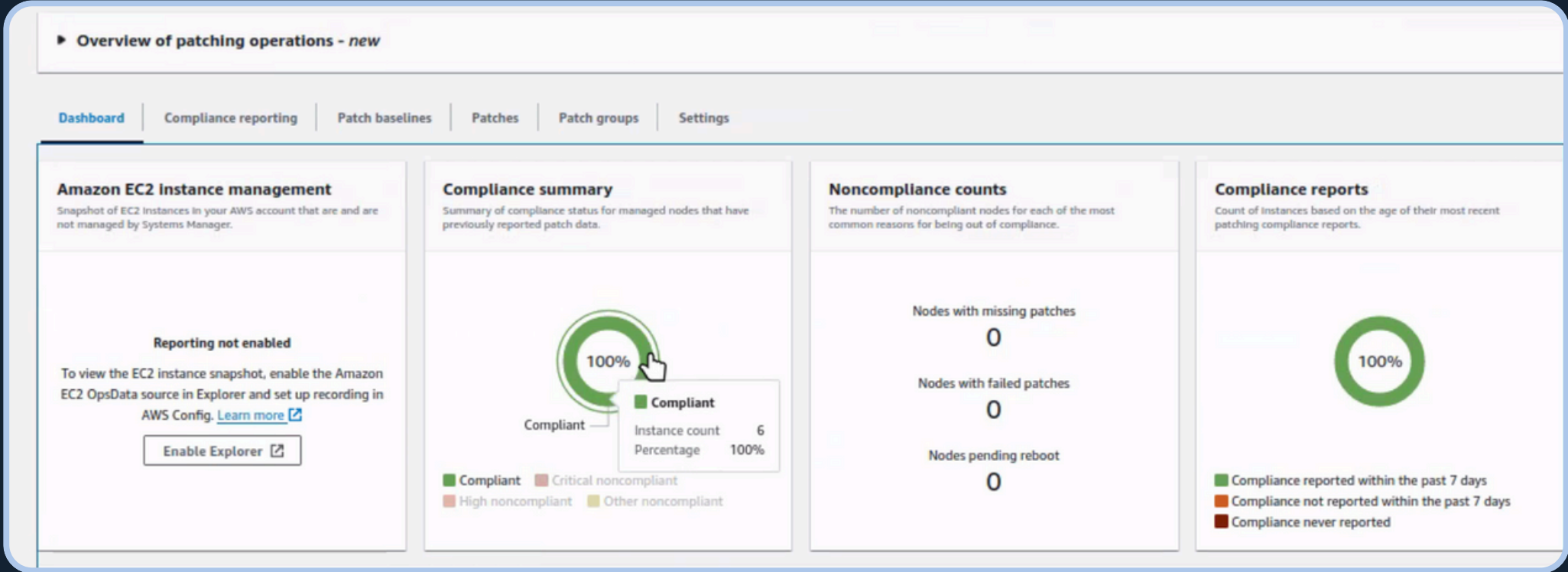
Skipped

Succeeded

Failed

TAREA 2.3: VERIFICAR CUMPLIMIENTO

- Confirmamos que todas las instancias cumplen con el último parche disponible



	Name	Node ID	Patch configuration name	Patch configuration type	Compliance status	Critical non-compliant count	Security non-compliant count	Other non-compliant count	Last operation date
<input type="radio"/>	Linux-3	i-03d6f7db9aa40de71	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:39:41 PM
<input type="radio"/>	Linux-2	i-05ff9f738c3e55240	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:39:12 PM
<input type="radio"/>	Windows-2	i-0a99de1b32e6bfb73	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:44:25 PM
<input type="radio"/>	Windows-1	i-00ccb6551ec3d1e88	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:45:47 PM
<input type="radio"/>	Linux-1	i-05f3e8023b8b8837f	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:40:10 PM
<input type="radio"/>	Windows-3	i-0dd846911819779c7	-	Patch group	✔ Compliant	0	0	0	2024-05-13 8:45:16 PM

- Lista de parches de una instancia



Windows-1

Running

Node actions

General

▼ Properties

General

Tags

Inventory

Associations

Patches

Configuration compliance

▼ Tools

File system

Performance counters

Processes

Users and groups

Windows event logs

Windows registry

EBS volumes [New](#)

Execute run command

Patch node

Patch summary

Patch baseline ID

[pb-087b329b81616b3f4](#)

Updates installed

27

Patch configuration name

-

Updates with errors

0

Patch configuration type

Patch group

Updates needed

0

Last updated (UTC)

Mon, 13 May 2024 23:45:47 GMT

Patches (50+)

Search for patches

< 1 2 3 4 5 ... >

Name	Classification	Description	State	Severity	CVE Ids	Installed Time
KB4470502	SecurityUpdates	2018-12 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4470502)	Installed	Important	-	Tue Dec 11 2018 21:00:00 GMT-0300 (Uru
KB4470788	SecurityUpdates	2018-11 Update for Windows Server 2019 for x64-based Systems (KB4470788)	Installed	Critical	-	Tue Dec 11 2018 21:00:00 GMT-0300 (Uru
KB4480056	SecurityUpdates	2019-01 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4480056)	Installed	Important	-	Tue Jan 08 2019 21:00:00 GMT-0300 (Uru
KB4493510	SecurityUpdates	2019-03 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4493510)	Installed	Critical	-	Sat Apr 20 2019 21:00:00 GMT-0300 (Uru
KB4499728	SecurityUpdates	2019-05 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4499728)	Installed	Critical	-	Tue May 14 2019 21:00:00 GMT-0300 (Uru

CONCLUSIONES

- CREAMOS UN VALOR DE REFERENCIA DE PARCHE PERSONALIZADO.
- MODIFICAMOS DOS GRUPOS DE PARCHES.
- CONFIGURAMOS LA APLICACIÓN DE LOS PARCHES.
- LLEVAMOS A CABO UN ANÁLISIS INSTANTÁNEO Y COMPROBAMOS EL CUMPLIMIENTO DE LOS PARCHES



¡GRACIAS!