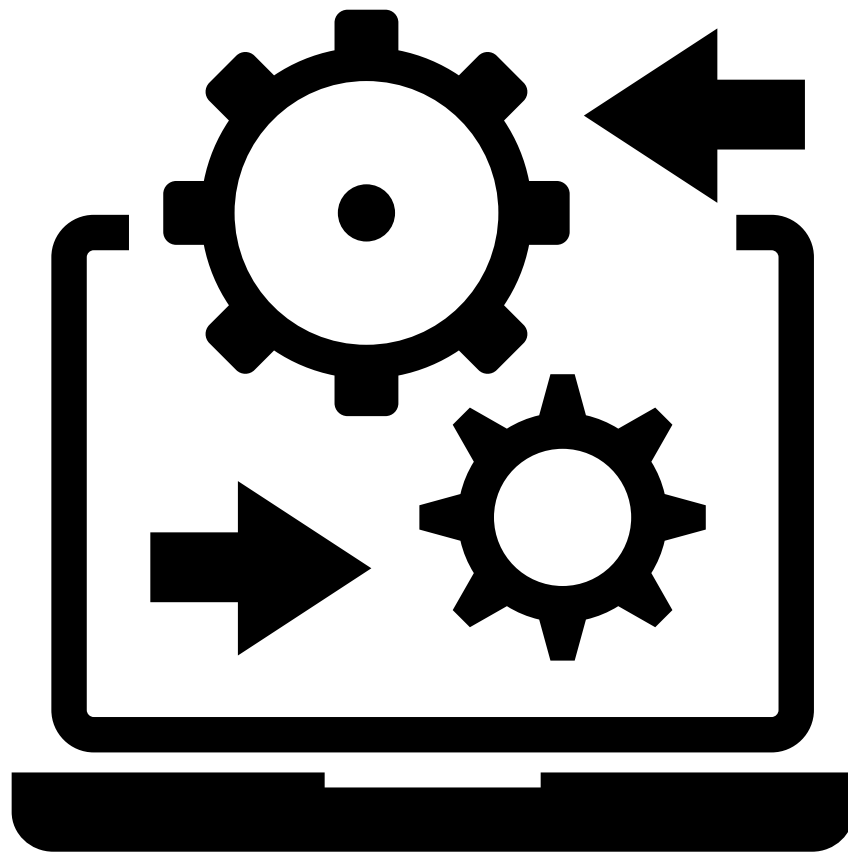




# 24°

**Lab - AWS re/Start**

**Endurecimiento de  
Sistemas**





# Protegiendo sistemas con Patch Manager

A continuación, se muestra los objetivos del laboratorio:

- Parchear instancias Linux utilizando la línea de base por defecto
- Crear una línea de base de parches personalizada
- Utilizar grupos de parches para parchear instancias Windows utilizando la línea de base de parches personalizada
- Verificar el cumplimiento de los parches

**Nota.** Utilizamos *Patch Manager*, una función de *AWS Systems Manager*, para crear una línea base de parches la cual es utilizada para analizar y parchear instancias de EC2.

# Tarea 01



Empezaremos parcheando instancias Linux utilizando las líneas base predeterminadas. Donde podremos ver mediante *Fleet Manager* cuales son las instancias que tienen el rol asignado que les permite ser administradas por *Systems Manager*, este es el rol IAM:

IAM > Roles > LabStack-783c9c4b-e126-4728-9951-0a7c5c23e5-SSMRole-FavA8Pwwl8Kg

LabStack-783c9c4b-e126-4728-9951-0a7c5c23e5-SSMRole-FavA8Pwwl8Kg [Info](#) [Delete](#)

**Summary** [Edit](#)

Creation date January 30, 2024, 01:34 (UTC-05:00)	ARN arn:aws:iam::555451576738:role/LabStack-783c9c4b-e126-4728-9951-0a7c5c23e5-SSMRole-FavA8Pwwl8Kg	Instance profile ARN arn:aws:iam::555451576738:instance-profile/RoleForSSM
Last activity -	Maximum session duration 1 hour	

[Permissions](#) | [Trust relationships](#) | [Tags](#) | [Access Advisor](#) | [Revoke sessions](#)

**Permissions policies (1)** [Info](#) [Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type: All types < 1 > [Settings](#)

<input type="checkbox"/>	Policy name <a href="#">🔗</a>	Type	Attached entities
<input type="checkbox"/>	<a href="#">AmazonSSMManagedInstanceCore</a>	AWS managed	1

Ahora, utilizaremos *Patch Manager*. Donde primero parchearemos las instancias Linux

# Tarea 01



Esta es la configuración:

Patch instances now [Info](#)

**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)  [Add](#)

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

**Patch Group** : LinuxProd [×](#)

Y después de ejecutado el parche en las tres instancias:


[AWS Systems Manager](#) > [Patch Manager](#) > Association execution summary

**Association execution summary**

**AWS-PatchNowAssociation**

Association ID 77c6a27c-b7f4-4cc5-9314-47b89fedd0f2 <a href="#">↗</a>	Execution ID 6baae306-a6f9-4efa-bccb-b168f2d6d002 <a href="#">↗</a>
Status ✔ Success	Operation Install
Reboot option RebootIfNeeded	Targets tag:Patch Group: LinuxProd
Summary Success=3	

**Scan/Install operation summary**



Succeeded

# Tarea 01



Ahora, crearemos nuestra línea base de parche personalizada para parchear las instancias Windows.

[AWS Systems Manager](#) > [Patch Manager](#) > [Patch baselines](#) > [Create patch baseline](#)

## Create patch baseline

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.

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

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

9 remaining

Remove rule

Operating system rule 2

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

# Tarea 01



Y esta *Patch Baseline*, que hemos creado se la asignamos a un grupo de parche:

[AWS Systems Manager](#) > [Patch Manager](#) > [Patch baselines](#) > [Baseline ID: pb-057126cd8ae81d185](#) > **Modify patch groups**

### 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  
pb-057126cd8ae81d185

Baseline name  
WindowsServerSecurityUpdates

Baseline description  
Windows security baseline patch

Patch groups

Patch group values can consist of up to 256 letters, numbers, and the following characters: . \_ + @ / - + :  
No patch groups attached

La configuración del parche para las instancias Windows:

**Patch instances now** [Info](#)

**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 : WindowsProd**

# Tarea 01



Y notamos que en el reporte de cumplimiento, todas las intancias van de acuerdo a la regla.

Dashboard   Compliance reporting   Patch baselines   Patches   Patch groups   Settings						
Node patching details (6)						
<div>View logView detailExport to S3View all S3 exports</div>						
<div>Q</div>						
	Name	Node ID	Patch configuration name	Patch configuration type	Compliance status	Critical compliance
<input type="radio"/>	Linux-1	<a href="#">i-0a5707aa91ac6efe1</a>	-	Patch group	Compliant	0
<input type="radio"/>	Windows-3	<a href="#">i-0857e883ad889fc44</a>	-	Patch group	Compliant	0
<input type="radio"/>	Linux-2	<a href="#">i-07f7fed82deb87f2a</a>	-	Patch group	Compliant	0
<input type="radio"/>	Windows-1	<a href="#">i-098f076e55a1faf9b</a>	-	Patch group	Compliant	0
<input type="radio"/>	Linux-3	<a href="#">i-0e22013ab2b090191</a>	-	Patch group	Compliant	0
<input type="radio"/>	Windows-2	<a href="#">i-0b3c4e4f7adc19d69</a>	-	Patch group	Compliant	0