



277-[SF]-Lab - Endurecimiento de sistemas

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.



AWS Systems
Manager

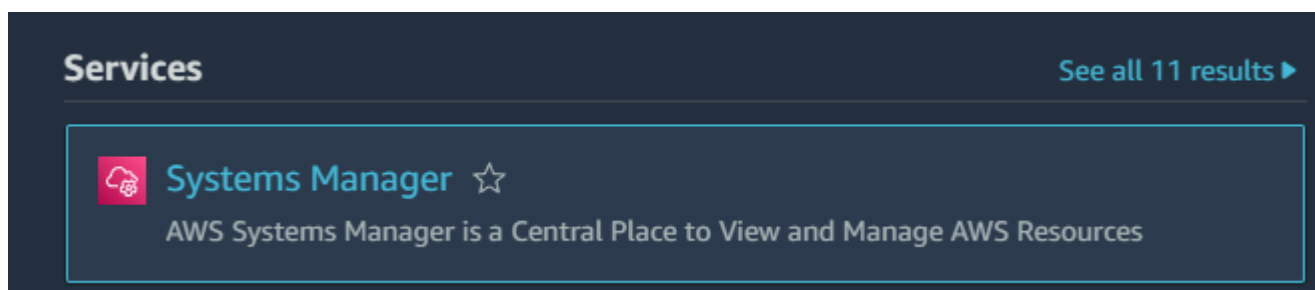
- Operations Management → Proporciona visibilidad de sus aplicaciones e infraestructura y ayuda a solucionar problemas con rapidez.
- Application Management → Implemente, administre y escale sus aplicaciones.
- Change Management → Manera controlada y auditable de realizar cambios en sus aplicaciones 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 → Búsqueda → Amazon Systems Manager



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

▼ Node Management

Fleet Manager

Compliance

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

Fleet Manager Info

You may have unmanaged Amazon EC2 instances

You can automatically configure Amazon EC2 instances as managed instances in your current account and Region by enabling Default Host Ma

Managed Nodes (3)

Q

Filter

✔

Last fetched at: 8:57 PM

<div><div></div><div></div></div>	Node ID	Node state	Name	Platform type	Operating sy...	Resource type
<div><div></div><div></div></div>	i-00b797d2e94...	<div><div>✔</div><div>Running</div></div>	Linux-2	Linux	Amazon Linux	EC2 instance
<div><div></div><div></div></div>	i-02cb24f5d55c...	<div><div>✔</div><div>Running</div></div>	Linux-3	Linux	Amazon Linux	EC2 instance
<div><div>✔</div><div></div></div>	i-0d3e4baa62d...	<div><div>✔</div><div>Running</div></div>	Linux-1	Linux	Amazon Linux	EC2 instance

↺

Report

Node actions

Node overview

Connect

Tools

Node settings

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.

Linux-1 Running

Details

▼ Properties

General

Tags

Inventory

Associations

Patches

Configuration compliance

▼ Tools

File system

Performance counters

Processes

Users and groups

Execute run command

Patch node

General

Node ID

[i-0d3e4baa62dced6b5](#)

Platform type

Linux

Source type

EC2 instance

Activation ID

-

Agent version

3.2.1377.0

Architecture

x86_64

Association status

-

Name

Linux-1

Availability zone

us-west-2a

Computer name

ip-10-0-2-87.us-west-2.compute.internal

IAM role

-

Instance role

arn:aws:iam::392568473958:instance-profile/RoleForSSM

Node state

✔

Running

IP address

10.0.2.87

Key name

vockey

Ping status

✔

Online

Operating system

Amazon Linux

Platform version

2

Resource type

EC2 instance

Source ID

i-0d3e4baa62dced6b5

Patch critical noncompliant count

-

Patch failed count

-

Patch installed count

-

Patch group

-

Image ID

ami-00755a52896316cee

3

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

Management & Governance

AWS Systems Manager Patch Manager

Manage patch compliance across the organization

Using Patch Manager, you can deploy patches simultaneously to applications and nodes across your organization. You can monitor patch compliance account by account.

Patch your instances

Expedite patching by creating a patch policy to apply operating system patches across the organization, and track compliance account by account.

[Create patch policy](#)

[Start with an overview](#)

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

Patch Manager [Info](#) Patch now Create patch

► Overview of patching operations - new

Dashboard | Compliance reporting | **Patch baselines** | Patches | Settings

Patch baselines (1/17)

1 match

Baseline name = AWS-AmazonLinux2DefaultPatchBaseline × Clear filter

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

View details Edit Delete Create patch

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

Patch baselines (1/18)

1 match

AWS-AmazonLinux2DefaultPatchBaseline × Clear filter

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

View details Edit Delete

Actions ▲

Set default patch baselineModify patch groups

Create patch ba

Patch groups

Patch group values can consist of up to 256 letter:

LinuxProd ×

Tarea 1.1 – Etiquetar Instancias:

Paso 1: Services → Compute → EC2 → Instances

Instances (6) [Info](#)

<input type="checkbox"/>	Name ▾	Instance ID	Instance state ▾
<input type="checkbox"/>	Windows-1	i-0720da6e4638f6464	Running
<input type="checkbox"/>	Linux-3	i-02cb24f5d55c060e1	Running
<input type="checkbox"/>	Linux-1	i-0d3e4baa62dced6b5	Running
<input type="checkbox"/>	Windows-2	i-0e9cc799649cda85c	Running
<input type="checkbox"/>	Windows-3	i-04973f19db17962f2	Running
<input type="checkbox"/>	Linux-2	i-00b797d2e94f1db17	Running

Paso 2: Pestaña “Tag” → Manage Tags → Etiquetar instancias Windows

- Key = Patch Group
- Value = WindowsProd

Key

X

Value - optional

X

Remove

X

X

Remove

X

X

Remove

Paso 2: Pestaña “Tag” → Manage Tags → Etiquetar instancias Linux

- Key = Patch Group
- Value = LinuxProd

Key

X

Value - optional

X

Remove

X

X

Remove

X

X

Remove

Tarea 1.2 – Crear un Baseline de parche personalizado:

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

- Seleccionar pestaña “Patch Baseline” → Create Patch Baseline

The screenshot shows the Amazon Systems Manager Patch Manager interface. At the top, there's a 'Patch Manager' header with an 'Info' link. To the right are buttons for 'Patch now' and 'Create patch policy'. Below this is a section titled 'Overview of patching operations - new'. A navigation bar contains 'Dashboard', 'Compliance reporting', 'Patch baselines' (which is selected), 'Patches', and 'Settings'. Under 'Patch baselines', there's a sub-header 'Patch baselines (17)' with a search bar containing 'Filter patch baselines'. To the right of the search bar are buttons for 'View details', 'Edit', 'Delete', and 'Create patch baseline'. At the bottom right, there are pagination controls showing '< 1 2 >'.

Paso 2: Configurar Baseline de parche → Details

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

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

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

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 ▼

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 ▼

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

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

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 ▼

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

Patch baselines (1/18)

Filter patch baselines

1 match

Baseline name = WindowsServerSecurityUpdates

Clear filter

Baseline ID	Baseline name
pb-0da7adc676d57da41	WindowsServerSecurityUpdates

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

Patch baselines (1/18)

Filter patch baselines

1 match

Baseline name = WindowsServerSecurityUpdates

Clear filter

View details

Edit

Delete

Actions

Create patch baseline

Set default patch baseline

Modify patch groups

Baseline ID	Baseline name	Description	Operating system	Default baseline
pb-00d6da90d45a3078d	WindowsServerSecurityUpdates	Windows security baseline patch	Windows	No

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-00d6da90d45a3078d

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

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.

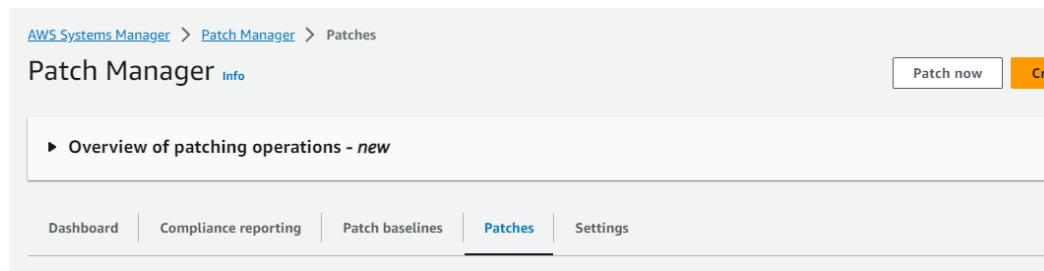
Tarea 2: Configurar la aplicación de parches

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

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.

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

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

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 ✕

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

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

Association execution summary

AWS-PatchNowAssociation

Association ID

f9325d15-5473-439f-9c02-df724bdf280 [🔗](#)

Execution ID

cbd5be32-c537-4d72-98d2-b83f6b78fa77 [🔗](#)

Status

🟢 Success

Operation

Install

Reboot option

RebootIfNeeded

Targets

tag:Patch Group: LinuxProd

Summary

Success=3

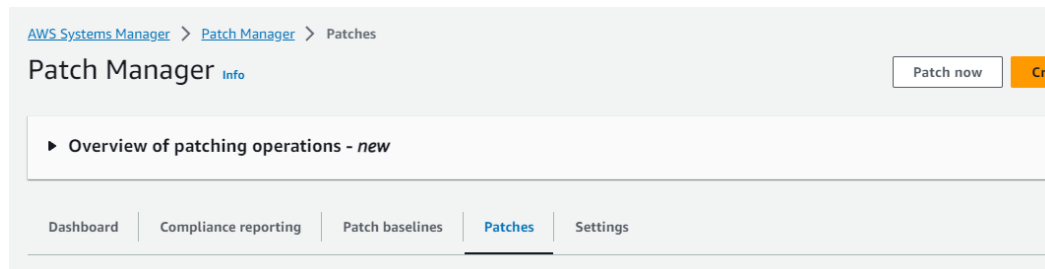
- Scan/install operation summary → Muestra visualmente el estado de las instancias afectadas.

Scan/Install operation summary



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

AWS-PatchNowAssociation

Association ID	Execution ID
5cf7232b-0fe4-44c7-a3cf-fc867c459bd1	4616fc88-23cb-41ca-a901-de2a0ca51022
Status	Operation
✔ Success	Install
Reboot option	Targets
RebootIfNeeded	tag:Patch Group: WindowsProd
Summary	
Success=1	

Execution ID

[4616fc88-23cb-41ca-a901-de2a0ca51022](#)

Paso 5: Execution ID → Output link

Execution ID: 4616fc88-23cb-41ca-a901-de2a0ca51022

Association execution targets

Resource id	Resource type	Status	Detailed status	Last execution date	Output
i-0f9d5a12650a83bb9	ManagedInstance	✔ Success	Success	Sat, 23 Sep 2023 01:15:05 GMT	Output

Expand Output Panel to observe the details:

Output on i-0f9d5a12650a83bb9

Step 1 - Command description and status

Status	Detailed status	Response code	Step name	Start time	Finish time
✔ Success	✔ Success	0	PatchWindows	Sat, 23 Sep 2023 01:14:02 GMT	Sat, 23 Sep 2023 01:15:04 GMT

▼ Output

The command output displays a maximum of 48,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.

```
Preparing to download PatchBaselineOperations PowerShell module from S3.

Downloading PatchBaselineOperations PowerShell module from https://s3.us-west-2.amazonaws.com/aws-ssm-us-west-2/patchbaselineoperations/Amazon.PatchBaselineOperations-1.45.zip to
C:\ProgramData\Amazon\SSM\InstanceData\i-0f9d5a12650a83bb9\document\orchestration\1a31efbb-a2a7-4b8f-bd69-c5abe9c2d7de\PatchWindows\Amazon.PatchBaselineOperations-1.45.zip.

Extracting PatchBaselineOperations zip file contents to temporary folder.
```

[Copy](#) [Download](#)

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

12

Tarea 2.3 – Verificar la Conformidad

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

Patch Manager [Info](#)

► Overview of patching operations - *new*

Dashboard

Compliance reporting

Patch baselines

Patches

Patch groups

Settings

Amazon EC2 instance management

Snapshot of EC2 instances in your AWS account that are and are not managed by Systems Manager.

Reporting not enabled

To view the EC2 instance snapshot, enable the Amazon EC2 OpsData source in Explorer and set up recording in AWS Config. [Learn more](#)

Enable Explorer

Compliance summary

Summary of compliance status for managed nodes that have previously reported patch data.

100%

Compliant

Compliant

Critical noncompliant

High noncompliant

Other noncompliant

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

Node patching details (6)

View log

View detail

Export to S3

Vie

Filter

	Name	Node ID	Patch configuration name	Patch configuration type	Compliance status
<input type="radio"/>	Linux-3	i-0a98f592d3c2cd9c9	-	Patch group	<input checked="" type="checkbox"/> Compliant
<input type="radio"/>	Linux-1	i-0bb92601b51c1c035	-	Patch group	<input checked="" type="checkbox"/> Compliant
<input type="radio"/>	Windows-1	i-0bf33443da931db8e	-	Patch group	<input checked="" type="checkbox"/> Compliant
<input type="radio"/>	Windows-3	i-02c343c8ce6b21665	-	Patch group	<input checked="" type="checkbox"/> Compliant
<input type="radio"/>	Linux-2	i-03d045ba79233dee0	-	Patch group	<input checked="" type="checkbox"/> Compliant
<input type="radio"/>	Windows-2	i-0f9d5a12650a83bb9	-	Patch group	<input checked="" type="checkbox"/> Compliant

13

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

Windows-2 Running

Details

▼ Properties

General

Tags

Inventory

Associations

Patches

Configuration compliance

▼ Tools

Patch summary

Patch baseline ID

[pb-04fb4ae6142167966](#)

Patch configuration name

-

Patch configuration type

Patch group

Last updated (UTC)

Sat, 23 Sep 2023 01:15:03 GMT

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

Patches (200+)

Search for patches

<

1

2

3

4

Name	Classification	Description	State	Severity
KB4470502	SecurityUpdates	2018-12 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4470502)	Installed	Important
KB4470788	SecurityUpdates	2018-11 Update for Windows 10 Version 1809 for x64-based Systems (KB4470788)	Installed	Critical
KB4480056	SecurityUpdates	2019-01 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 1809 for x64 (KB4480056)	Installed	Important
KB4493510	SecurityUpdates	2019-03 Servicing Stack Update for Windows 10 Version 1809 for x86-based Systems (KB4493510)	Installed	Critical
KB4499728	SecurityUpdates	2019-05 Servicing Stack Update for Windows 10 Version 1809 for x86-based Systems (KB4499728)	Installed	Critical

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

