



AWS
re:Start
LAB

Systems Hardening



WEEK 4





Overview

In organizations with hundreds and often thousands of workstations, it can be logistically challenging to keep all the operating system (OS) and application software up to date. In most cases, OS updates on workstations can be automatically applied via the network. However, administrators must have a clear security policy and baseline plan to ensure that all workstations are running a certain minimum version of software.

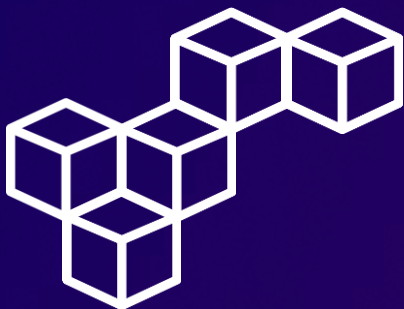
In this lab, you use Patch Manager, a capability of AWS Systems Manager, to create a patch baseline. You then use the patch baseline that you created to scan the Amazon Elastic Compute Cloud (Amazon EC2) instances for Linux and Windows that were pre-created for this lab.

The primary focus of Patch Manager is to install OS security-related updates on managed nodes.

The current environment has six EC2 instances: three instances with the Linux OS and three with the Windows OS.

Topics covered

- Create a custom patch baseline
- Modify patch groups
- Configure patching
- Verify patch compliance

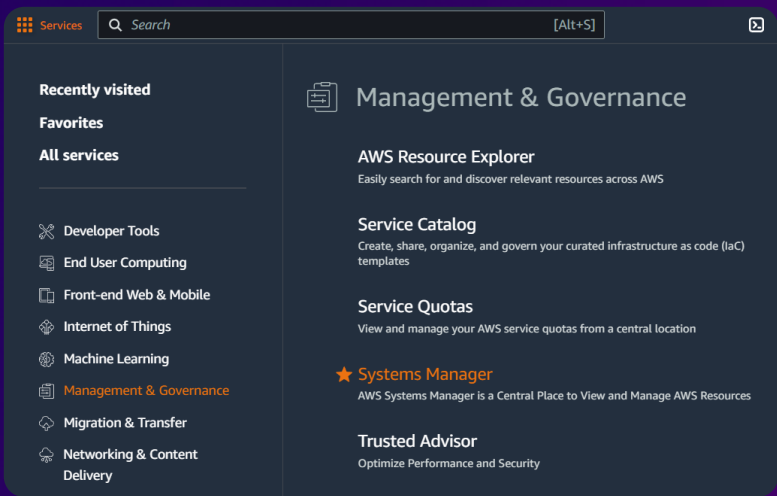


Task 1

Select patch baselines

Step 1: Access the Systems Manager

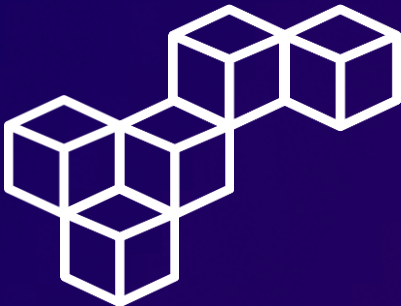
Open the AWS Management Console, and select Systems Manager.



Step 2: Review Managed Nodes

Navigate to the **Fleet Manager** section. Here are the pre-configured EC2 instances.

Managed Nodes (6)								
<input type="checkbox"/>	Node ID	Node state	Name	Operatin...	Resource ...	Image ID	EC2 instance	
<input type="checkbox"/>	i-0cb6765c3f524e710	Running	Linux-1	Amazon Linux	EC2 instance	ami-06883a...	Open EC2 instance	
<input type="checkbox"/>	i-0ddade808dea1c643	Running	Linux-2	Amazon Linux	EC2 instance	ami-06883a...	Open EC2 instance	
<input type="checkbox"/>	i-0622dc848328091aa	Running	Linux-3	Amazon Linux	EC2 instance	ami-06883a...	Open EC2 instance	
<input type="checkbox"/>	i-0450bd7daf8bd617d	Running	Windows-1	Microsoft Wi...	EC2 instance	ami-04eb6b...	Open EC2 instance	
<input type="checkbox"/>	i-0974a064e4001da67	Running	Windows-2	Microsoft Wi...	EC2 instance	ami-04eb6b...	Open EC2 instance	
<input type="checkbox"/>	i-0699cc47bc7f30513	Running	Windows-3	Microsoft Wi...	EC2 instance	ami-04eb6b...	Open EC2 instance	



Task 1

Select patch baselines

Step 3: Review node details

Select the Linux-1 managed node to view its details.

General			
Node ID i-0cb6765c3f524e710 🔗	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-10-0-2-145.us-west-2.compute.internal	Operating system Amazon Linux	Patch group -
Activation ID -	IAM role -	Platform version 2	Image ID ami-06883a492f195064e
Agent version 3.3.131.0	Instance role arn:aws:iam::905418147650:instance-profile/RoleForSSM	Resource type EC2 instance	
Architecture x86_64	Node state 🟢 Running	Source ID i-0cb6765c3f524e710	
Association status -	IP address 10.0.2.145	Patch critical noncompliant count -	

Step 4: Access the Patch Manager

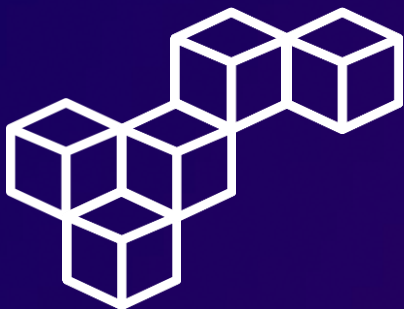
Navigate to the **Patch Manager** section, and select [Start with an overview](#).

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](#)



Task 1

Select patch baselines

Step 5: Review Patch baselines

Choose the **Patch baselines** tab. This tab includes the default patch baselines that you can select.

Patch baselines (18)

View details

Edit

Delete

Actions

Create patch baseline

Q Filter patch baselines

< 1 2 >

	Baseline ID	Baseline name	Description	Operating system	Default baseline
<input type="radio"/>	pb-07dbd9f0b517b769e	AWS-AlmaLinuxDefaultPatchBaseline	Default Patch Baseline for Alma Linux Provided by AWS.	AlmaLinux	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-0d5ff2de2fa3fa0ff	AWS-AmazonLinuxDefaultPatchBaseline	Default Patch Baseline for Amazon Linux Provided by AWS.	Amazon Linux	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-0e930e75b392d70da	AWS-AmazonLinux2DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	Amazon Linux 2	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-037a9df9b290208cf	AWS-AmazonLinux2022DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2022 Provided by AWS.	Amazon Linux 2022	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-0a624803d647da0ab	AWS-AmazonLinux2023DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2023 Provided by AWS.	Amazon Linux 2023	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-0b641de5f3a9f3b2f	AWS-CentOSDefaultPatchBaseline	Default Patch Baseline for CentOS Provided by AWS.	CentOS	<input checked="" type="checkbox"/> Yes
<input type="radio"/>	pb-04d1ad3cad30d44ff	AWS-DebianDefaultPatchBaseline	Default Patch Baseline for Debian Provided by AWS.	Debian	<input checked="" type="checkbox"/> Yes

Step 6: Modify patch groups

Select the [AWS-AmazonLinux2DefaultPatchBaseline](#) patch baseline and associate it with the LinuxProd patch group.

Patch baselines (1/17)

View details

Edit

Delete

Actions

Create patch baseline

Q Filter patch baselines

1 match

[AWS-AmazonLinux2DefaultPatchBaseline](#)

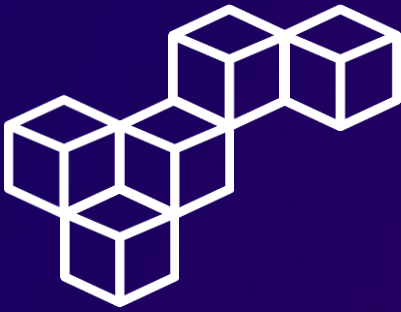
Clear filter

Set default patch baseline

Modify patch groups

< 1 >

Baseline ID	Baseline name	Description	Operating system	Default baseline
<input checked="" type="radio"/> pb-0e930e75b392d70da	AWS-AmazonLinux2DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	Amazon Linux 2	<input checked="" type="checkbox"/> Yes



Task 1

Select patch baselines

Step 7: Review running instances

In the EC2 Management Console, navigate to the **Instances** section. The six running EC2 instances are listed.

Instances (6) Info							
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>				All states ▾		< 1 > ⚙	
<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▾	Status check	Availability Zone ▾	Public IPv4 ... ▾	Security group name ▾
<input type="checkbox"/>	Linux-1	i-0cb6765c3f524e710	Running 🔍 🔍	2/2 checks passed	us-west-2a	54.203.100.117	c117085a279008816495571t...
<input type="checkbox"/>	Linux-2	i-0ddade808dea1c643	Running 🔍 🔍	2/2 checks passed	us-west-2a	34.210.58.218	c117085a279008816495571t...
<input type="checkbox"/>	Linux-3	i-0622dc848328091aa	Running 🔍 🔍	2/2 checks passed	us-west-2a	54.191.233.246	c117085a279008816495571t...
<input type="checkbox"/>	Windows-1	i-0450bd7daf8bd617d	Running 🔍 🔍	2/2 checks passed	us-west-2a	50.112.68.141	c117085a279008816495571t...
<input type="checkbox"/>	Windows-2	i-0974a064e4001da67	Running 🔍 🔍	2/2 checks passed	us-west-2a	54.184.127.57	c117085a279008816495571t...
<input type="checkbox"/>	Windows-3	i-0699cc47bc7f30513	Running 🔍 🔍	2/2 checks passed	us-west-2a	35.94.63.123	c117085a279008816495571t...

Step 8: Tag instances

Add the new tag **PatchGroup** : **WindowsProd** to the three Windows instances.

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	
<input type="text" value="Name"/>	<input type="text" value="Windows-1"/>	<input type="button" value="Remove"/>
<input type="text" value="cloudlab"/>	<input type="text" value="c117085a279008816495571t1w"/>	<input type="button" value="Remove"/>
<input type="text" value="PatchGroup"/>	<input type="text" value="WindowsProd"/>	<input type="button" value="Remove"/>



Task 1

Select patch baselines

Step 9: Create a custom patch baseline

In the **Patch Manager** section, choose the **Patch baselines** tab, select [Create patch baseline](#). In the details section, configure the following options.

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.

Step 10: Add a rule to the patch baseline

In the **Approval rules for operating systems** section, add the following rule for critical severity patches.

Operating system rule 1

X Remove rule

Products

Select patches by product

Select products

WindowsServer2019 X

Classification

Select patches by classification

Select classifications

SecurityUpdates X

Severity

Select patches by severity

Select severities

Critical X

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



Task 1

Select patch baselines

Step 11: Add a second rule to the patch baseline

In the **Approval rules for operating systems** section, add the following rule for important severity patches.

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

Step 12: Modify patch groups

Select the newly created **WindowsServerSecurityUpdates** patch baseline and associate it with the WindowsProd patch group.

Patch baselines (1/18)

View details

Edit

Delete

Actions

Create patch baseline

Set default patch baseline

Modify patch groups

Filter patch baselines

1 match

WindowsServerSecurityUpdates

Clear filter

Baseline ID	Baseline name	Description	Operating system	Default baseline
pb-09ef97bf7fb5d1d80	WindowsServerSecurityUpdates	Windows security baseline patch	Windows	No



Task 2

Configure patching

Step 1: Patch the Linux instances

Choose Scan and Install as the patching operation, specifying that Patch Manager should reboot the instances if necessary.

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

Step 2: Target selection

Specify the instance tag key-value `PatchGroup : LinuxProd` to identify the Linux instances.

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)	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

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

PatchGroup : LinuxProd

X



Task 2

Configure patching

Step 3: AWS-PatchNowAssociation

The AWS-PatchNowAssociation panel indicates that the patch installation was successful on all three Linux instances.

AWS-PatchNowAssociation

Association ID

d6d3a9c9-47ed-415b-86bd-19974cd8375b

Execution ID

087938c8-0d0f-4d4f-b229-521d1d4016fd

Status

Success

Operation

Install

Reboot option

RebootIfNeeded

Targets

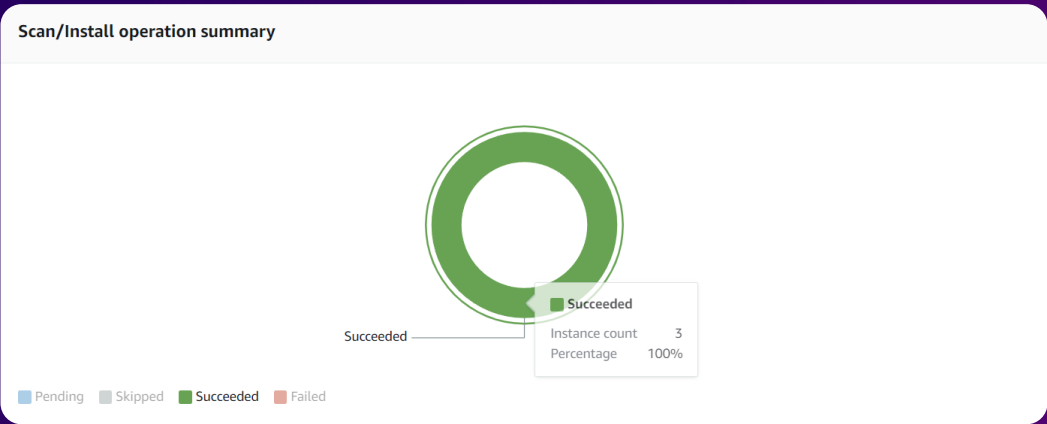
tag:PatchGroup: LinuxProd

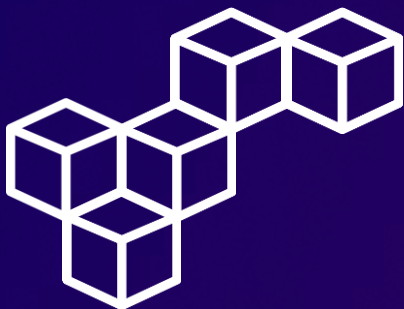
Summary

Success=3

Step 4: Scan/Install operation summary

The Scan/Install operation summary panel also confirms the "Succeeded" patch status for the affected Linux instances.





Task 2

Configure patching

Step 5: Patch the Windows Instances

Choose Scan and Install as the patching operation, specifying that Patch Manager should reboot the instances if necessary.

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

Step 6: Target selection

Specify the instance tag key-value `PatchGroup : WindowsProd` to identify the Windows instances.

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)	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

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

PatchGroup : WindowsProd X



Task 2

Configure patching

Step 7: AWS-PatchNowAssociation

The AWS-PatchNowAssociation panel indicates that the patch installation was successful. Choose the link to the [Execution ID](#).

AWS-PatchNowAssociation

Association ID d6d3a9c9-47ed-415b-86bd-19974cd8375b	Execution ID 1061e8d7-3aa0-4759-b7d2-15bdc65c92e9
Status ✔ Success	Operation Install
Reboot option RebootIfNeeded	Targets tag:PatchGroup: WindowsProd
Summary Success=3	

Step 8: Review the Run Command output

Choose the [Output](#) link for one of the Windows managed instances and review the details of the Run Command output.

▼ 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.

```
Successfully downloaded and installed the PatchBaselineOperations
PowerShell module.

Patch Summary for i-0699cc47bc7f30513

PatchGroup : WindowsProd

BaselineId : pb-09ef97bf7fb5d1d80
```

Copy

Download

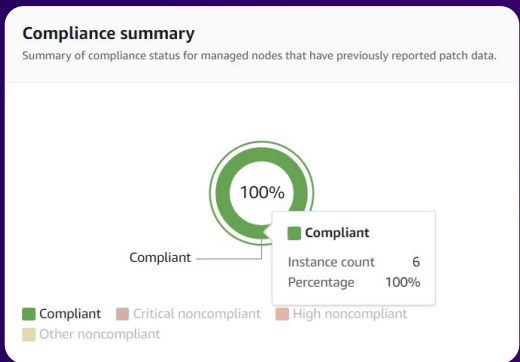


Task 2

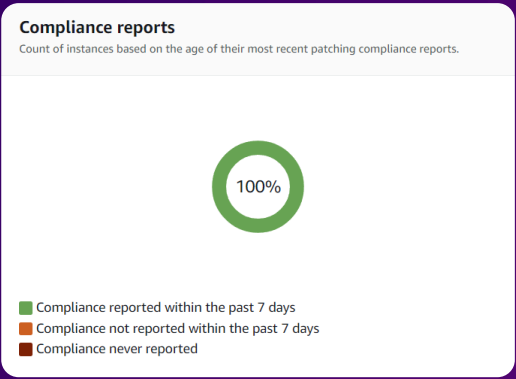
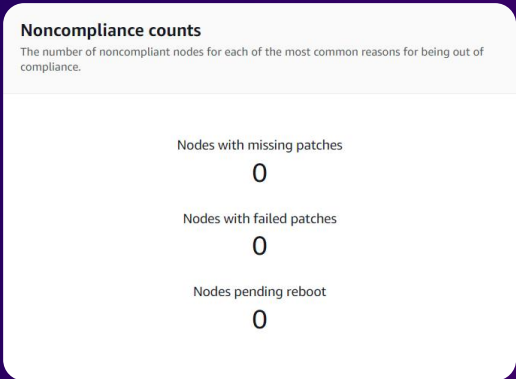
Configure patching

Step 9: Verify compliance

In the Patch Manager section, choose the Dashboard tab. The Compliance summary verifies that all Windows and Linux instances are compliant.



Still in the Dashboard tab, review the Noncompliance counts and Compliance reports.





Task 2

Configure patching

Step 10: Verify Compliant instances

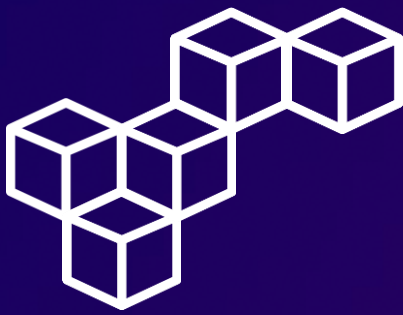
Choose the **Compliance reporting** tab. Then, review and verify the Compliant status of all Linux and Windows instances

Node patching details (6)						View log	View detail	Export to S3	View all S3 exports
	Name	Compliance status	Critical non-compliant count	Security non-compliant count	Other non-compliant count	Operating system			
<input type="radio"/>	Windows-3	✔ Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter			
<input type="radio"/>	Windows-2	✔ Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter			
<input type="radio"/>	Windows-1	✔ Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter			
<input type="radio"/>	Linux-2	✔ Compliant	0	0	0	Amazon Linux			
<input type="radio"/>	Linux-1	✔ Compliant	0	0	0	Amazon Linux			
<input type="radio"/>	Linux-3	✔ Compliant	0	0	0	Amazon Linux			

Step 11: Review applied patches

Choose the **Node ID** for one of the Windows managed nodes and observe what patches were applied to this instance.

Patches (150+)				Refresh
<input type="text" value="Search for patches"/>				< 1 2 3 4 5 6 7 8 ... > Settings
Name	Classification	Description	State	
KB4470502	SecurityUpdates	2018-12 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4470502)	Installed	
KB4470788	SecurityUpdates	2018-11 Update for Windows 10 Version 1809 for x64-based Systems (KB4470788)	Installed	
KB4480056	SecurityUpdates	2019-01 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 1809 for x64 (KB4480056)	Installed	
KB4493510	SecurityUpdates	2019-03 Servicing Stack Update for Windows 10 Version 1809 for x86-based Systems (KB4493510)	Installed	
KB4499728	SecurityUpdates	2019-05 Servicing Stack Update for Windows 10 Version 1809 for x86-based Systems (KB4499728)	Installed	
KB4504369	SecurityUpdates	2019-06 Servicing Stack Update for Windows 10 Version 1809 for ARM64-based Systems (KB4504369)	Installed	
KB4512577	SecurityUpdates	2019-09 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4512577)	Installed	



Conclusions

AWS Systems Manager

AWS Systems Manager provides a centralized platform for managing and automating operational tasks across AWS resources.

Fleet Manager

Fleet Manager within AWS Systems Manager allows efficient management of fleets of managed nodes, enabling streamlined monitoring and maintenance.

Patch Manager

Patch Manager in AWS Systems Manager automates the process of scanning for, approving, and applying patches to instances, ensuring system security and compliance.

Patch baselines

Patch baselines in AWS Systems Manager define the set of patches that should be applied to instances within a patch group, establishing a consistent patching standard.

Patch groups

Patch groups in AWS Systems Manager categorize instances based on their patching needs, allowing targeted patching operations and simplified patch management workflows.



Cristhian Becerra



[cristhian-becerra-espinoza](#)



+51 951 634 354



cristhianbecerra99@gmail.com



Lima, Peru

