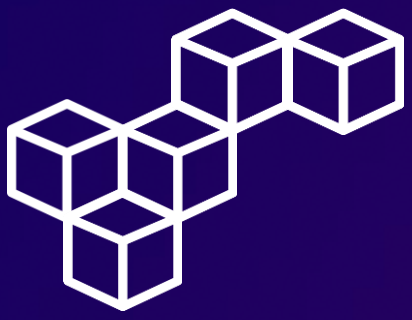
AWS re:Start

LAB

Systems Hardening

WEEK 4

aws re/start



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

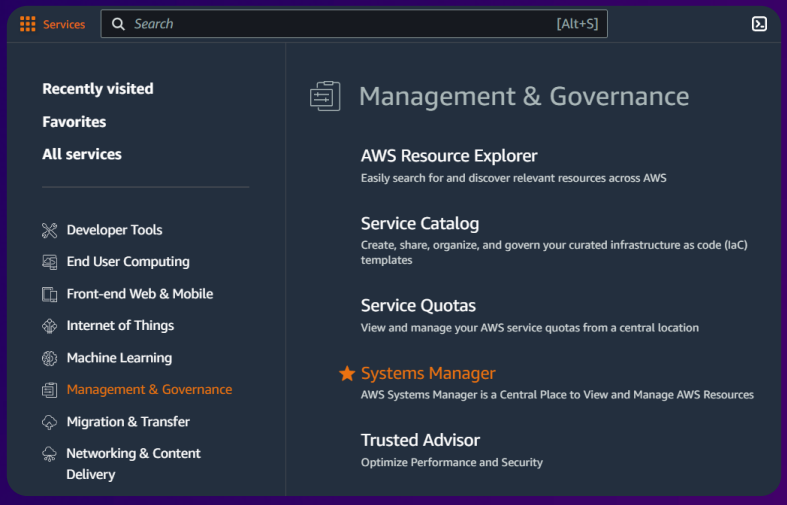
- Create a custom patch baseline
- Modify patch groups
- Configure patching
- Verify patch compliance

Task 1

Select patch baselines

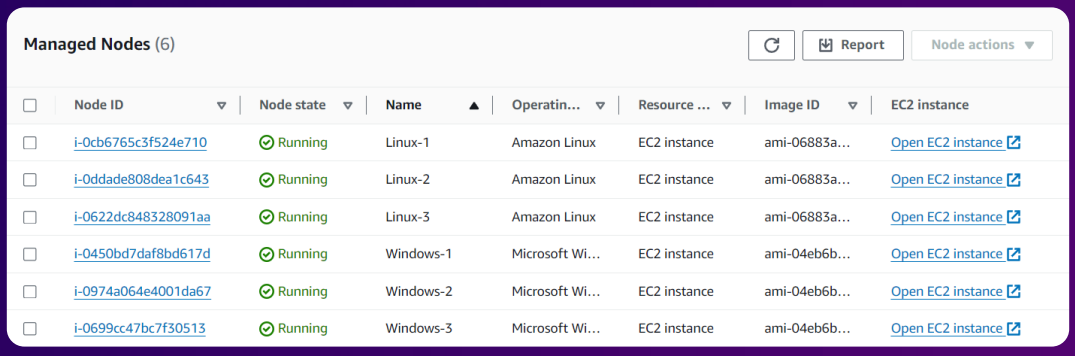
Step 1: Access the Systems Manager

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.



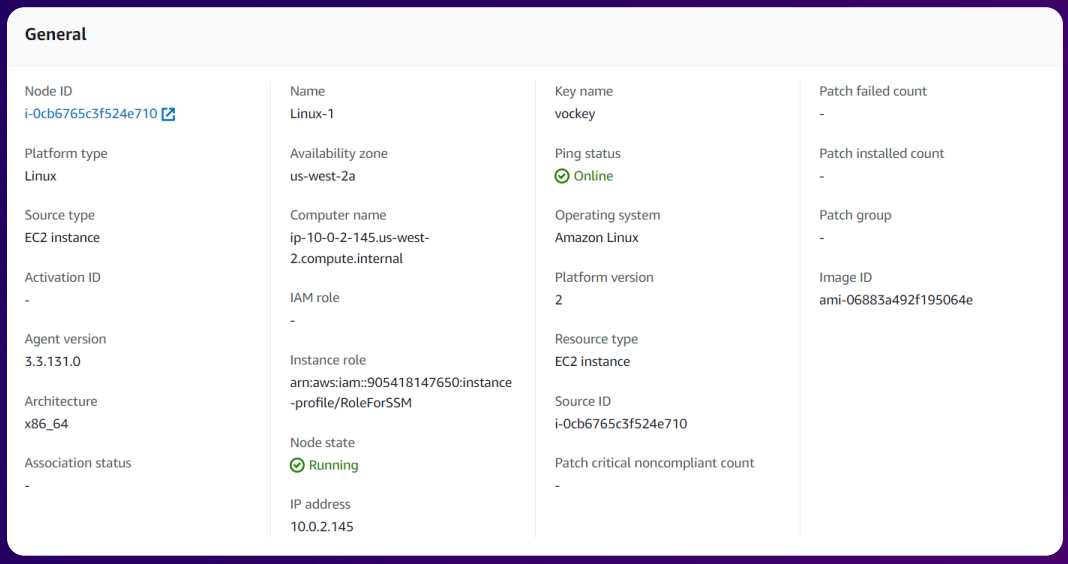
aws re/start

Task 1

Select patch baselines

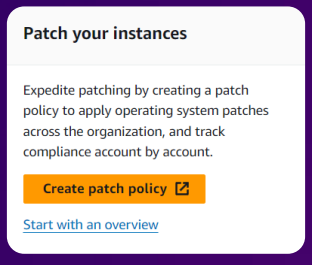
Step 3: Review node details

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



Step 4: Access the Patch Manager

Navigate to the **Patch Manager** section, and select Start with an overview.



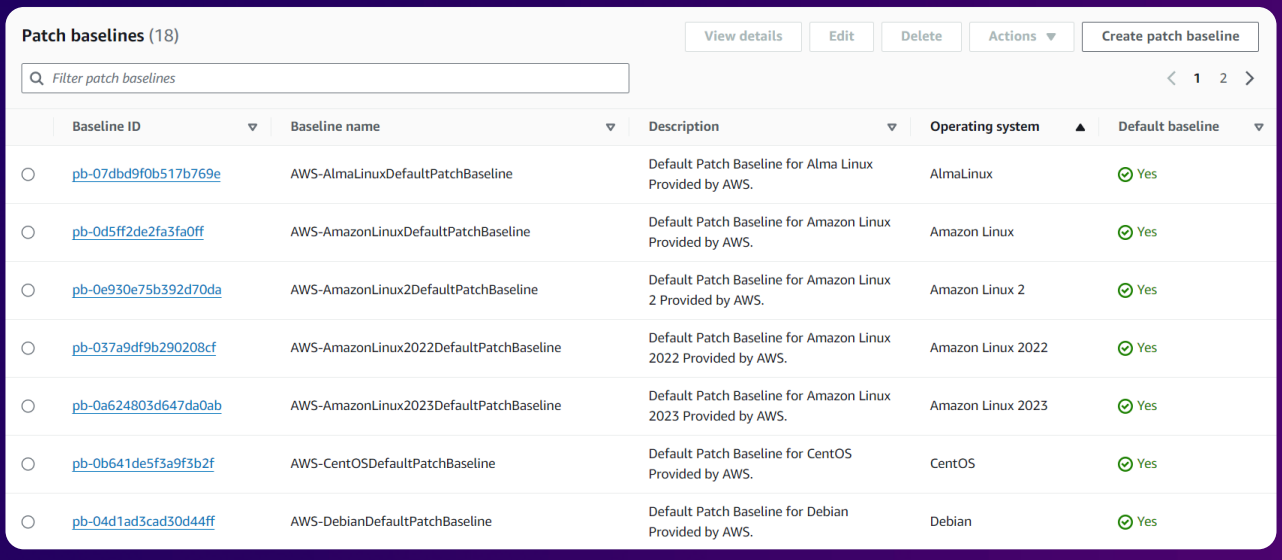
aws re/start

Task 1

Select patch baselines

Step 5: Review Patch baselines

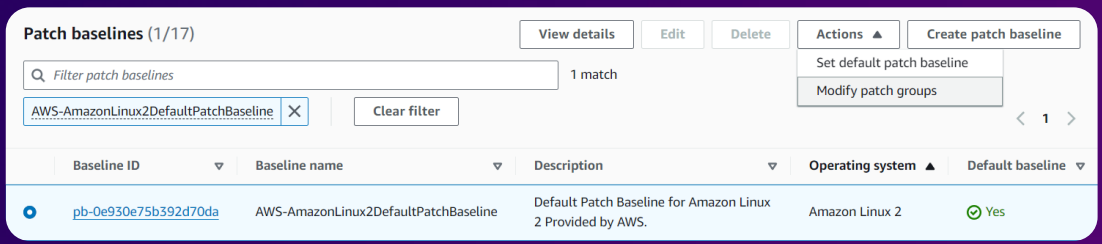
Choose the **Patch baselines** tab. This tab includes the default patch baselines that you can select.



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

Step 6: Modify patch groups

Select the AWS-AmazonLinux2DefaultPatchBaseline patch baseline and associate it with the LinuxProd patch group.



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

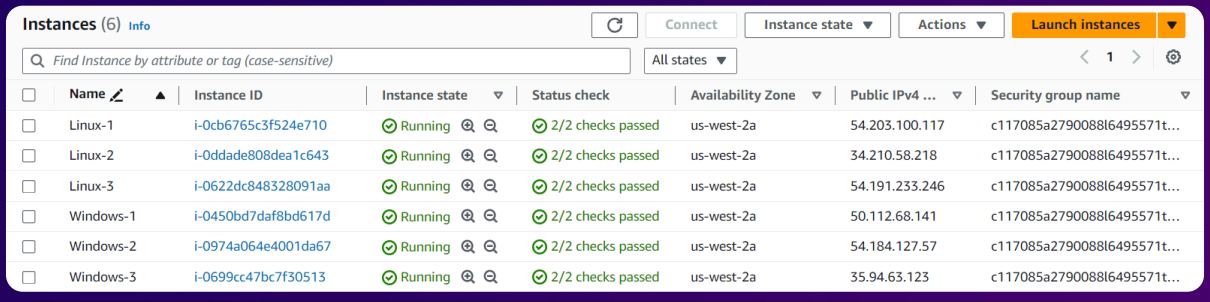
aws re/start

Task 1

Select patch baselines

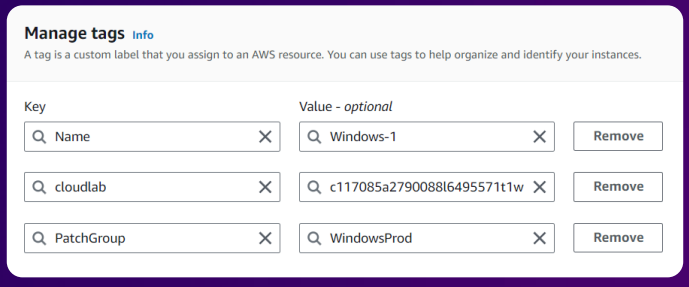
Step 7: Review running instances

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



Step 8: Tag instances

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



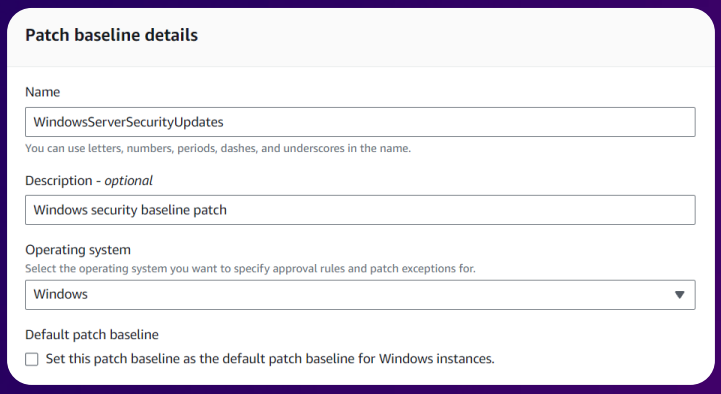
aws re/start

Task 1

Select patch baselines

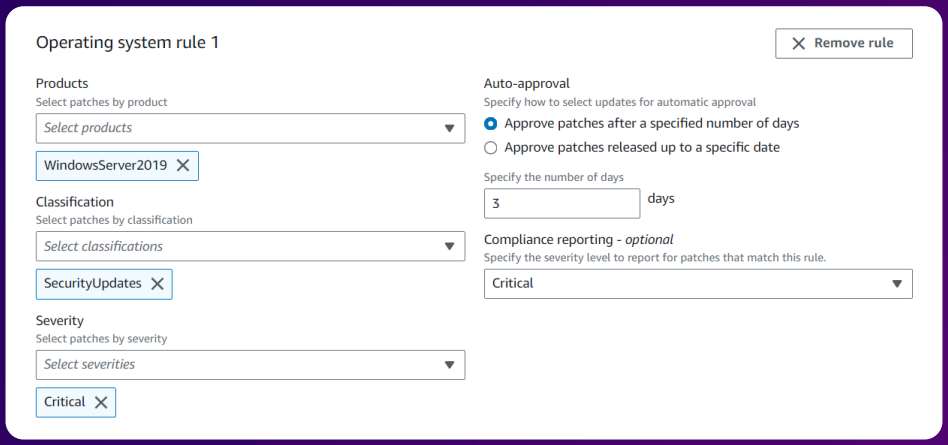
Step 9: Create a custom patch baseline

In the **Patch Manager** section, choose the **Patch baselines** tab, select Create patch baseline. In the details section, configure the following options.



Step 10: Add a rule to the patch baseline

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



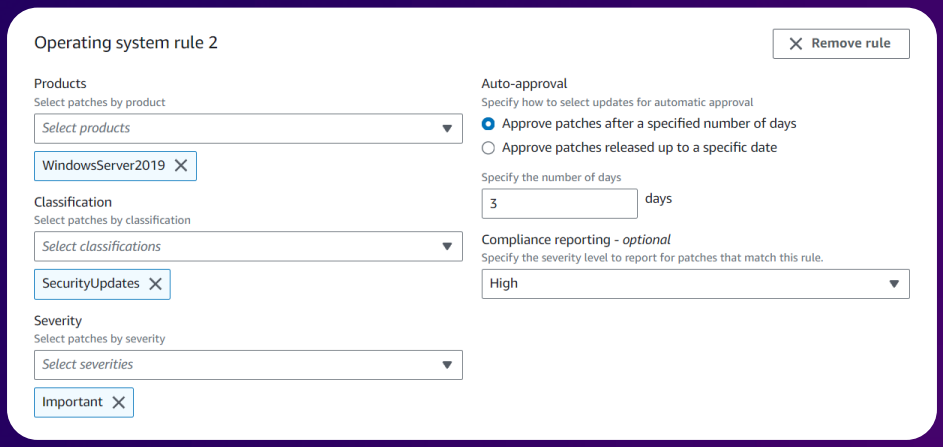
aws re/start

Task 1

Select patch baselines

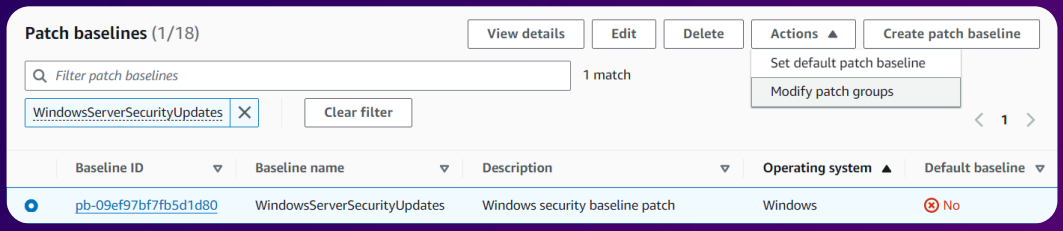
Step 11: Add a second rule to the patch baseline

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



Step 12: Modify patch groups

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



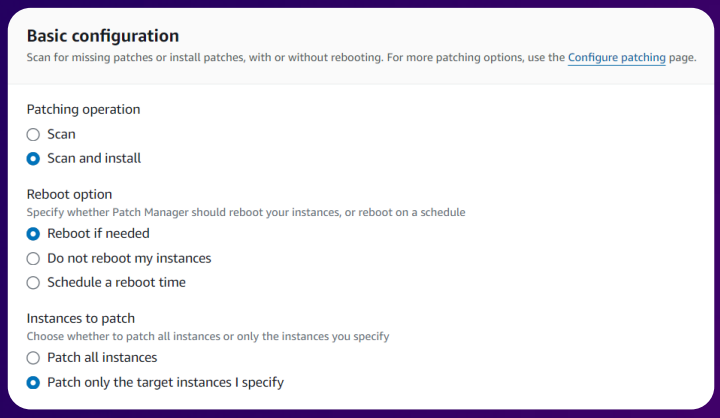
aws re/start

Task 2

Configure patching

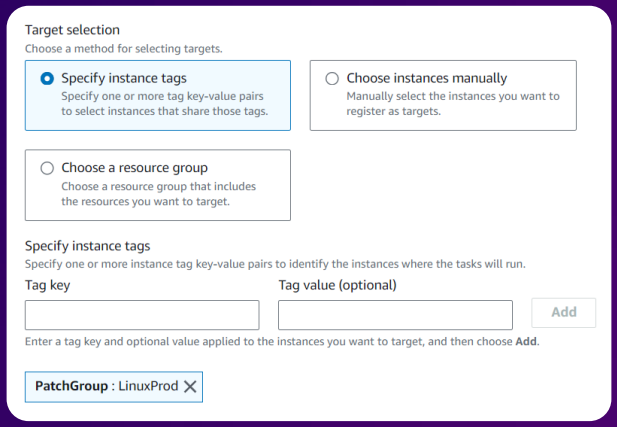
Step 1: Patch the Linux instances

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



Step 2: Target selection

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



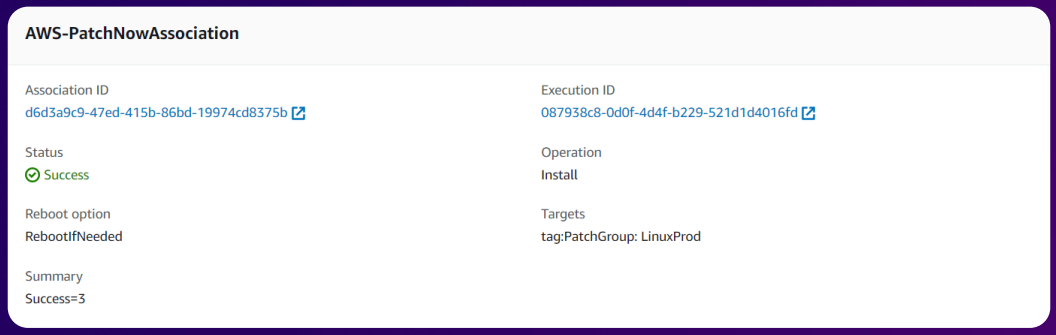
aws re/start

Task 2

Configure patching

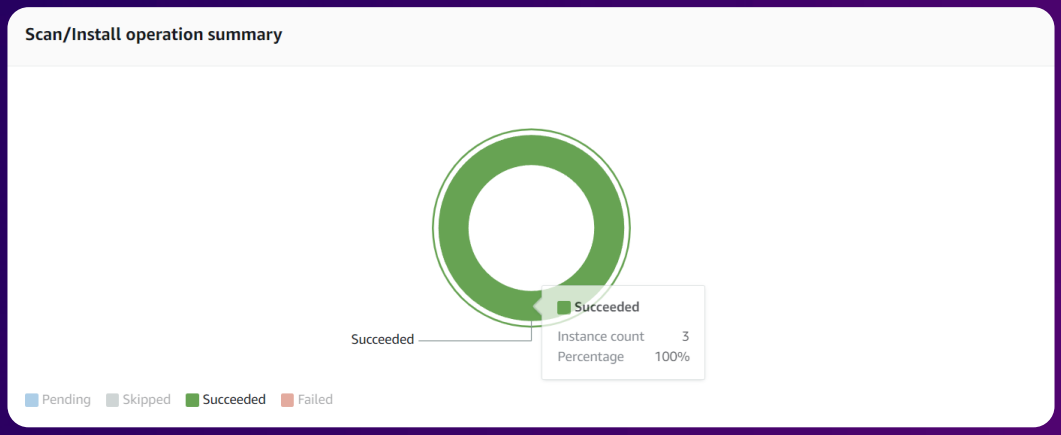
Step 3: AWS-PatchNowAssociation

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



Step 4: Scan/Install operation summary

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



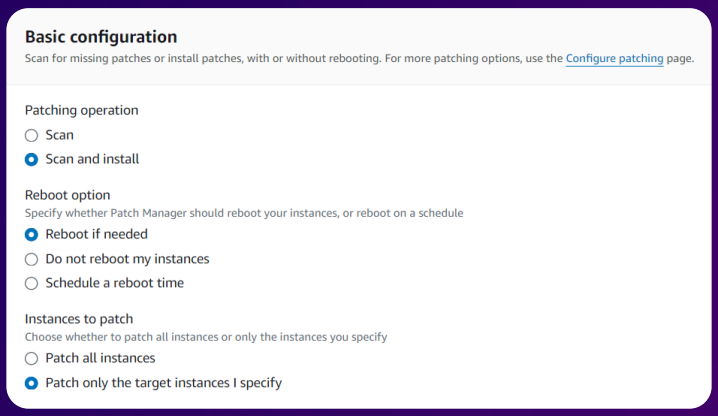
aws re/start

Task 2

Configure patching

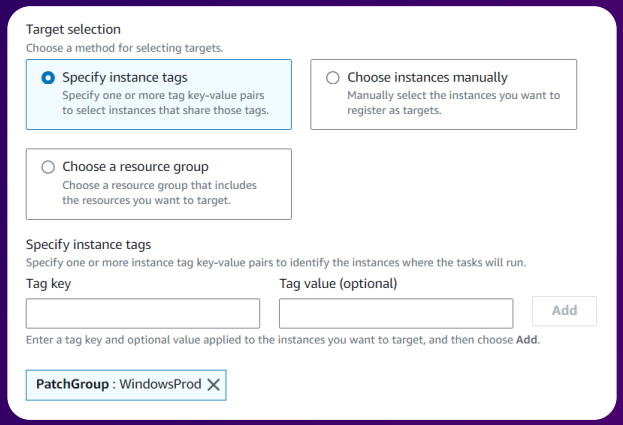
Step 5: Patch the Windows Instances

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



Step 6: Target selection

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



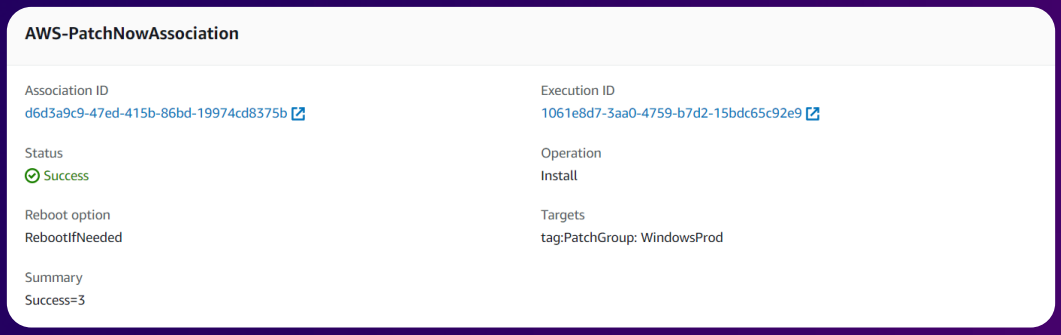
aws re/start

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.



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.

aws re/start

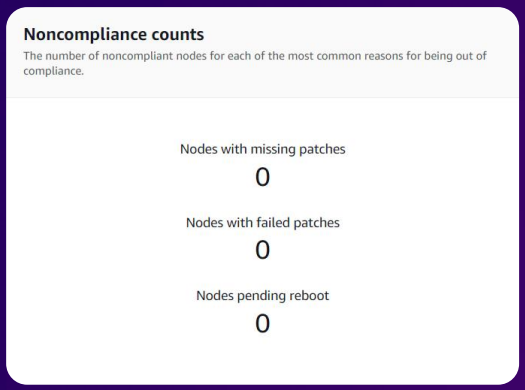
Task 2

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.



aws re/start

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

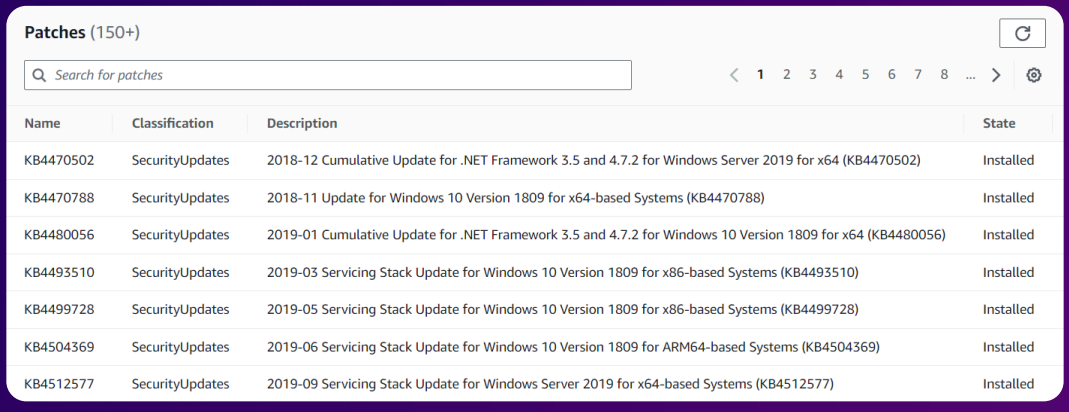
Node patching details (6)

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
○	Windows-3	Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter
○	Windows-2	Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter
○	Windows-1	Compliant	0	0	0	Microsoft Windows Server 2019 Datacenter
○	Linux-2	Compliant	0	0	0	Amazon Linux
○	Linux-1	Compliant	0	0	0	Amazon Linux
○	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.

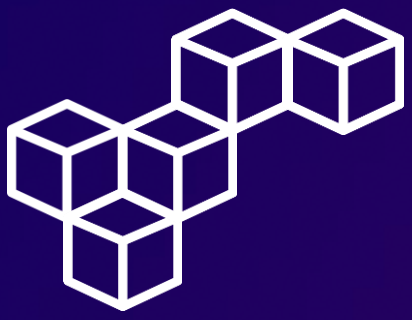


Patches (150+)

Search for patches

1 2 3 4 5 6 7 8 ...

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.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru