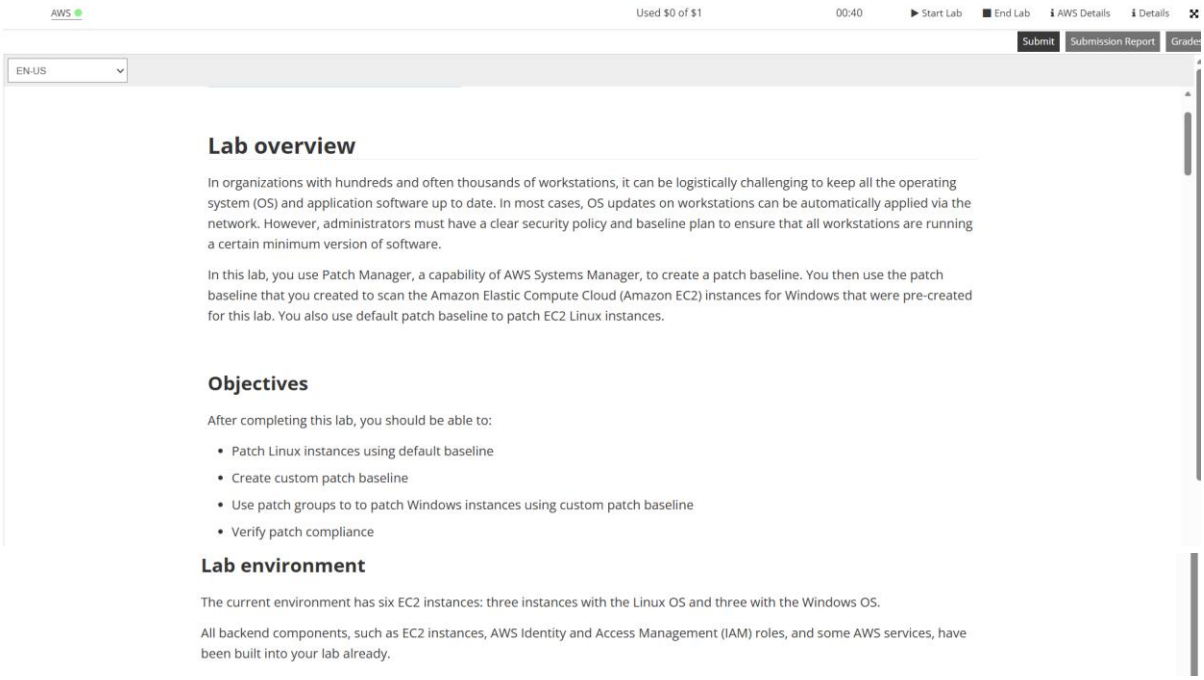
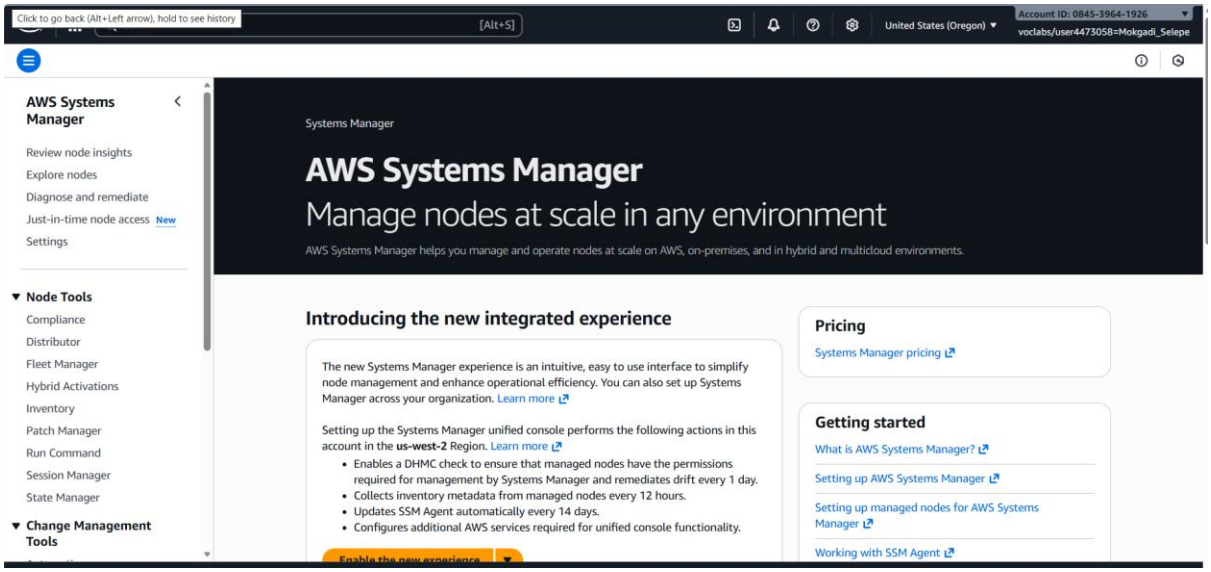
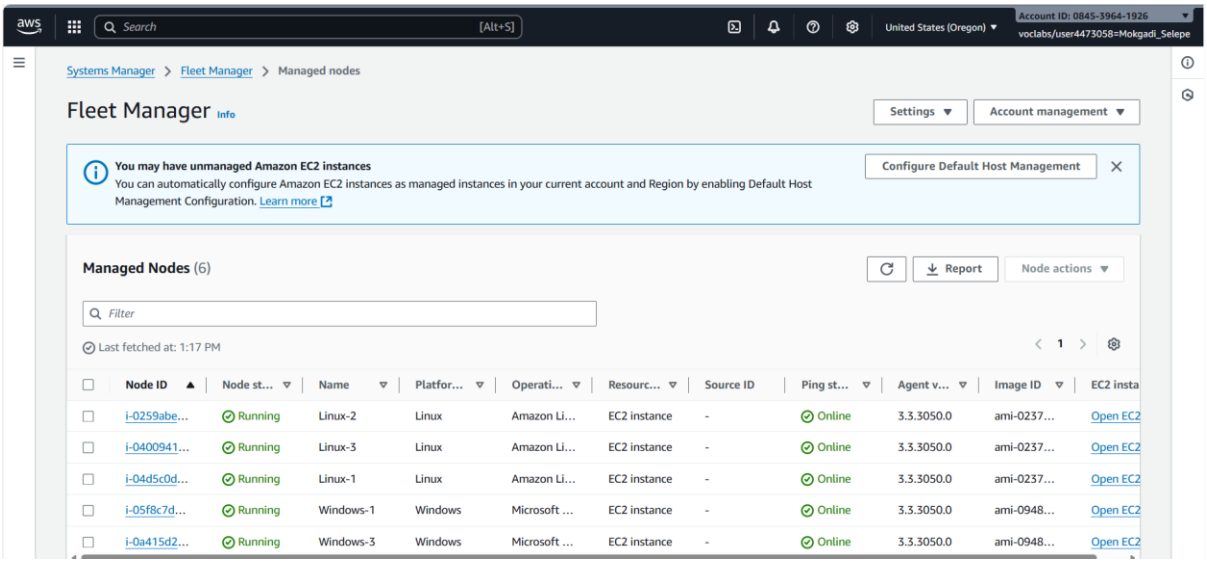
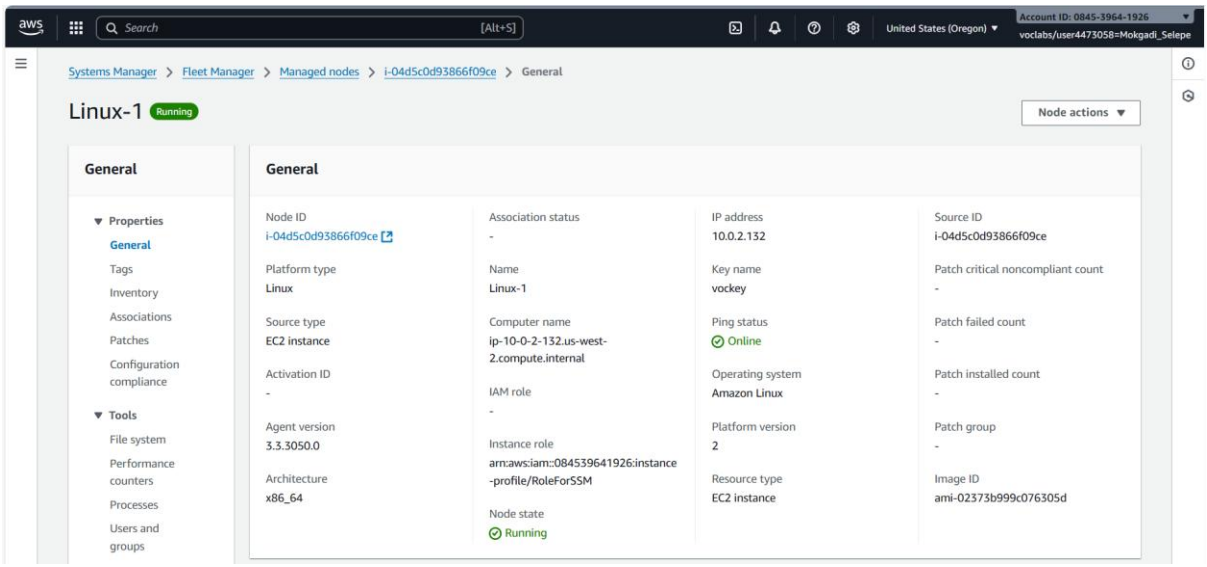
Systems Hardening with Patch Manager via AWS Systems Manager



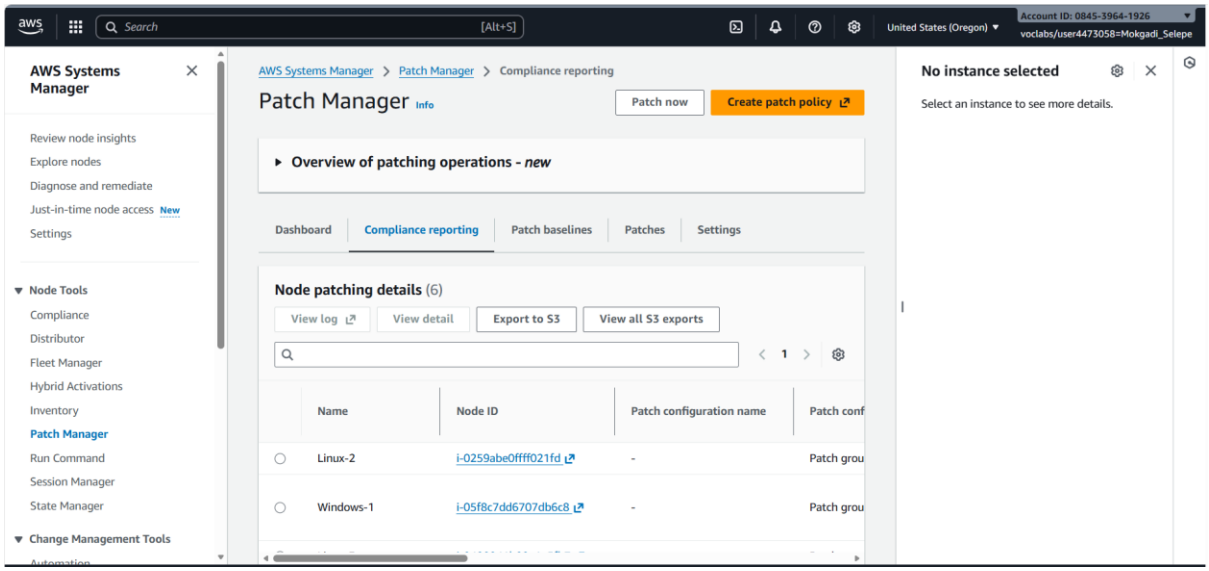
1: Patch Linux instances using default baselines

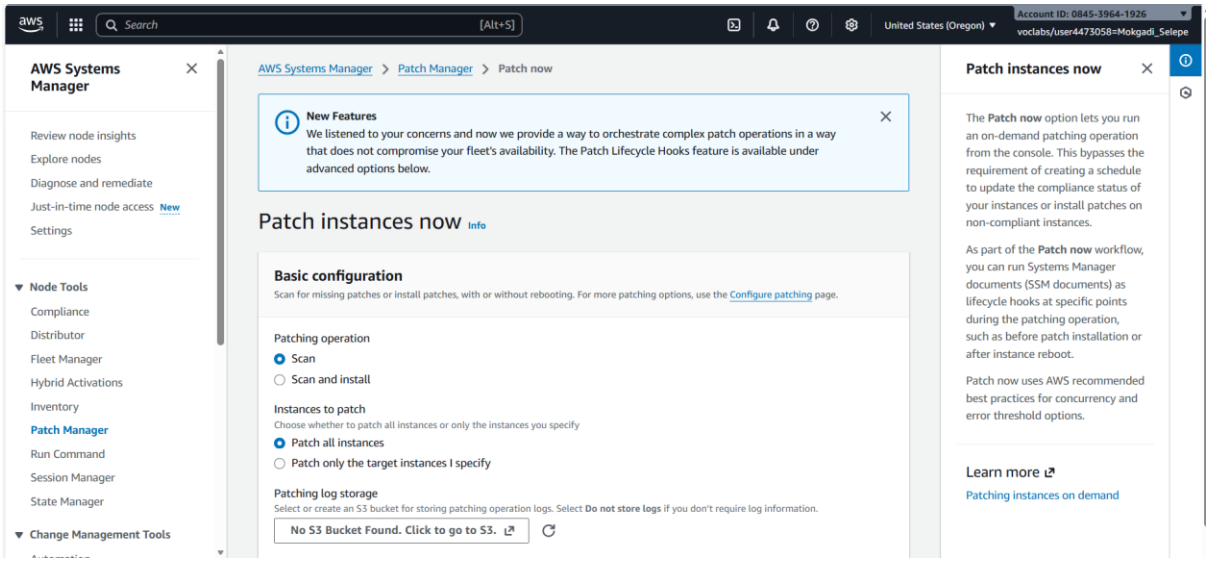


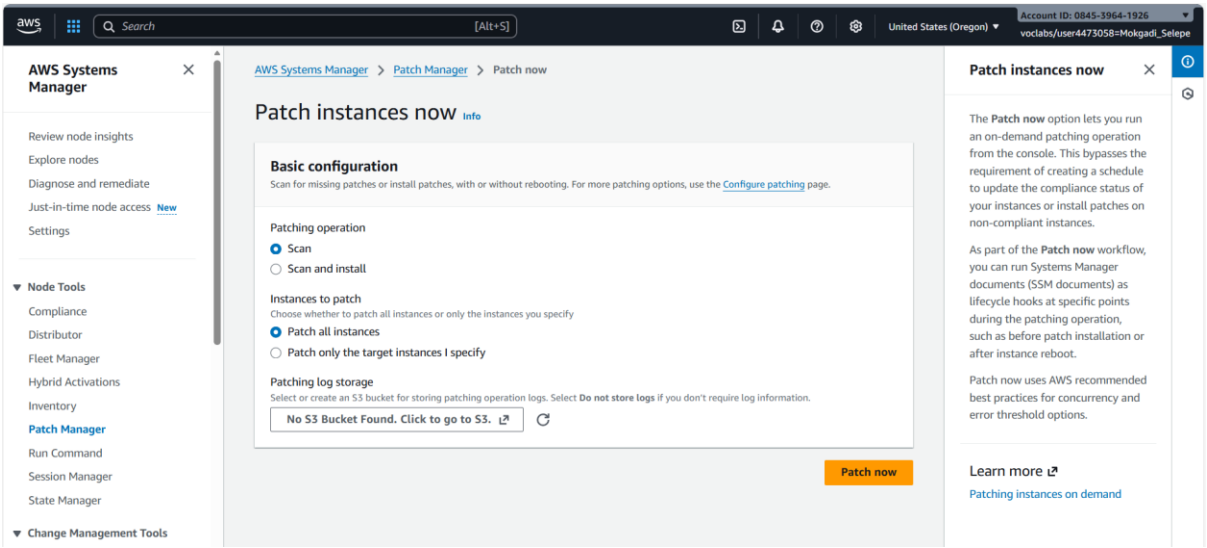

Systems Manager > Fleet Manager > Managed nodes
Fleet Manager Info
Settings
Account management
You may have unmanaged Amazon EC2 instances
You can automatically configure Amazon EC2 instances as managed instances in your current account and Region by enabling Default Host Management Configuration. Learn more
Configure Default Host Management
Managed Nodes (6)
Report
Node actions
Filter
Last fetched at: 1:17 PM
Node ID
Node st...
Name
Platfor...
Operati...
Resourc...
Source ID
Ping st...
Agent v...
Image ID
EC2 insta
i-0259abe... Running Linux-2 Linux Amazon Li... EC2 instance - Online 3.3.3050.0 ami-0237... Open EC2
i-0400941... Running Linux-3 Linux Amazon Li... EC2 instance - Online 3.3.3050.0 ami-0237... Open EC2
i-04d5c0d... Running Linux-1 Linux Amazon Li... EC2 instance - Online 3.3.3050.0 ami-0237... Open EC2
i-05f8c7d... Running Windows-1 Windows Microsoft ... EC2 instance - Online 3.3.3050.0 ami-0948... Open EC2
i-0a415d2... Running Windows-3 Windows Microsoft ... EC2 instance - Online 3.3.3050.0 ami-0948... Open EC2

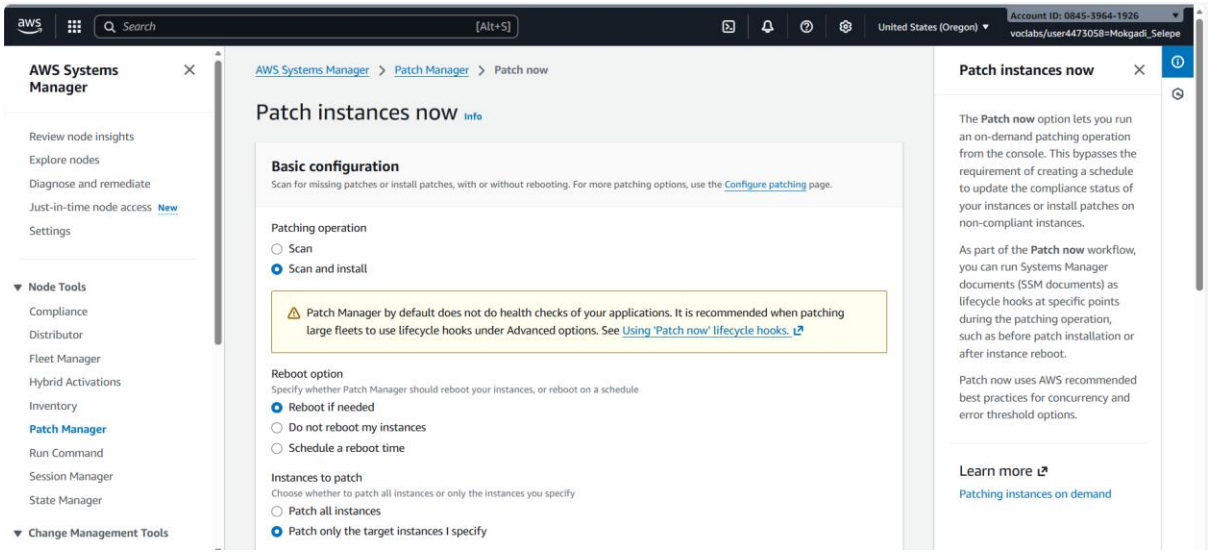

Systems Manager > Fleet Manager > Managed nodes > i-04d5c0d93866f09ce > General
Linux-1 Running
Node actions
General
Properties
General
Tags
Inventory
Associations
Patches
Configuration compliance
Tools
File system
Performance counters
Processes
Users and groups
Node ID
i-04d5c0d93866f09ce
Platform type
Linux
Source type
EC2 instance
Activation ID
-
Agent version
3.3.3050.0
Architecture
x86_64
Association status
-
Name
Linux-1
Computer name
ip-10-0-2-132.us-west-2.compute.internal
IAM role
-
Instance role
arn:aws:iam::084539641926:instance-profile/RoleForSSM
Node state
Running
IP address
10.0.2.132
Key name
vockey
Ping status
Online
Operating system
Amazon Linux
Platform version
2
Resource type
EC2 instance
Source ID
i-04d5c0d93866f09ce
Patch critical noncompliant count
-
Patch failed count
-
Patch installed count
-
Patch group
-
Image ID
ami-02373b999c076305d

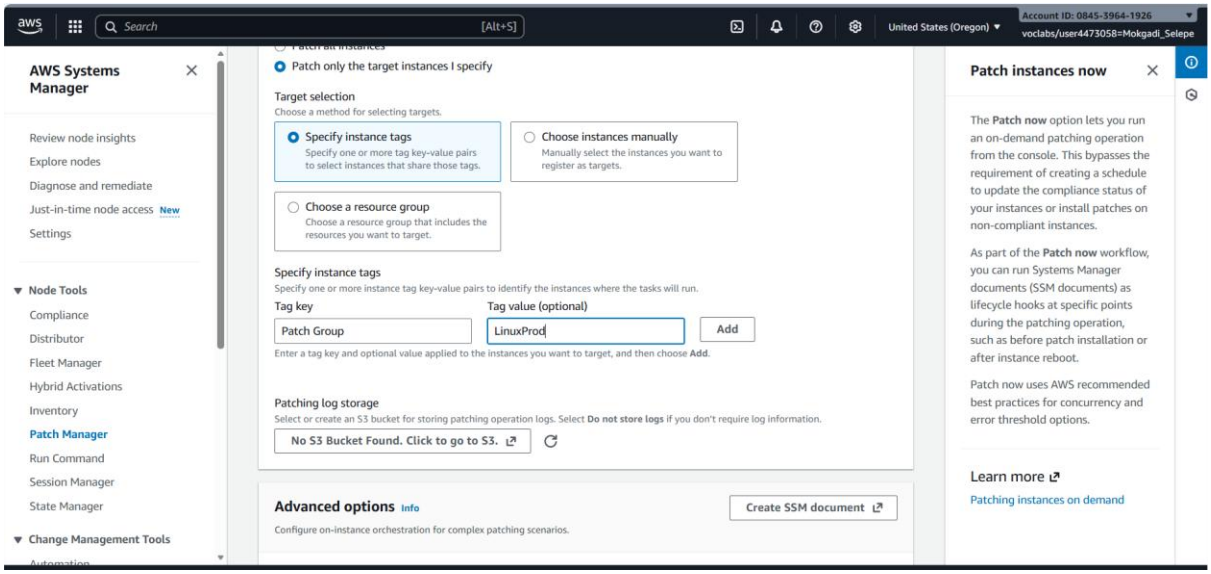

AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
Management & Governance
AWS 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
How it works
Create patch policy
Specify in a policy
View dashboard
Get a high-level view of
View compliance reports
Use cases and blog posts
Learn more
Latest blog post
More resources

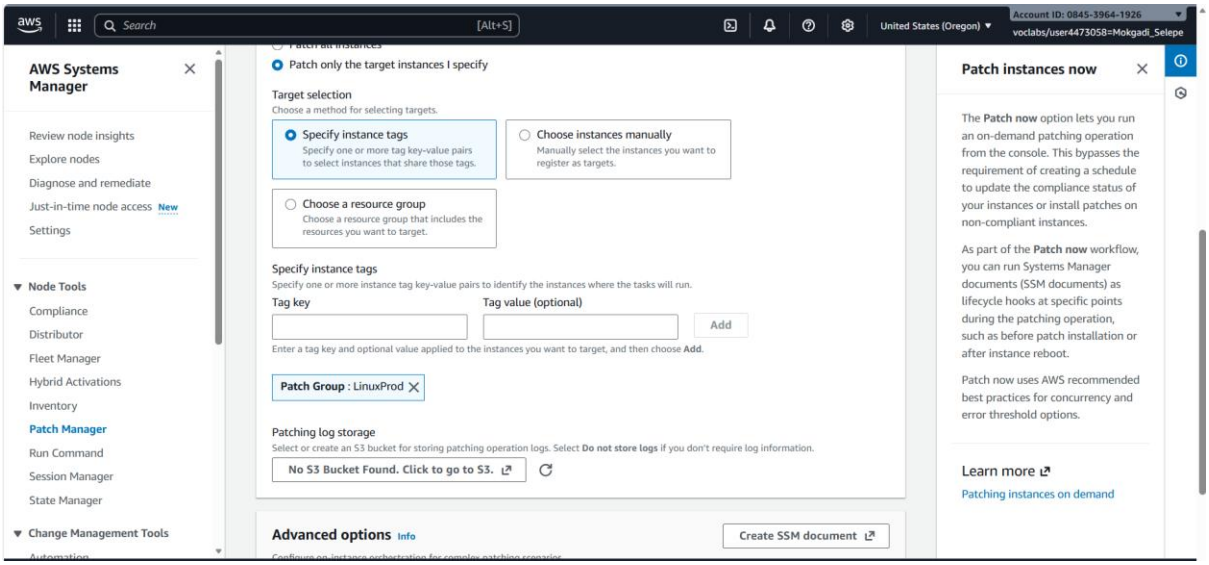

AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
AWS Systems Manager > Patch Manager > Compliance reporting
Patch Manager Info
Patch now
Create patch policy
Overview of patching operations - new
Dashboard
Compliance reporting
Patch baselines
Patches
Settings
Node patching details (6)
View log
View detail
Export to S3
View all S3 exports
Name
Node ID
Patch configuration name
Linux-2
i-0259abe0ffff021fd
Windows-1
i-05f8c7dd6707db6c8
No instance selected
Select an instance to see more details.

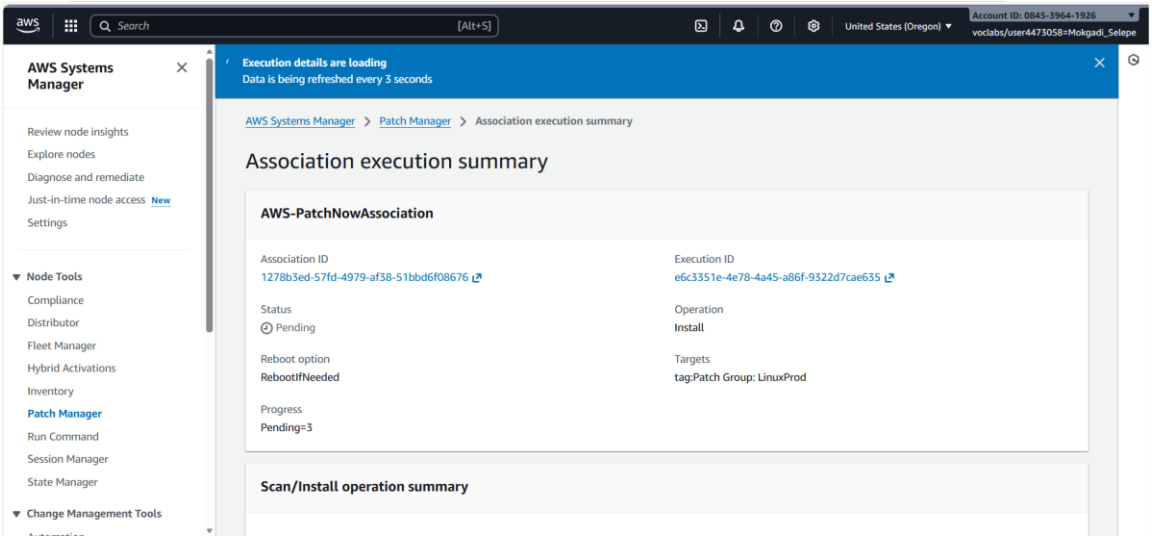

AWS Systems Manager
AWS Systems Manager > Patch Manager > Patch now
New Features
We listened to your concerns and now we provide a way to orchestrate complex patch operations in a way that does not compromise your fleet's availability. The Patch Lifecycle Hooks feature is available under advanced options below.
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
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
Patching log storage
Select or create an S3 bucket for storing patching operation logs. Select Do not store logs if you don't require log information.
No S3 Bucket Found. Click to go to S3.
Patch instances now
The Patch now option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.
As part of the Patch now workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.
Patch now uses AWS recommended best practices for concurrency and error threshold options.
Learn more
Patching instances on demand

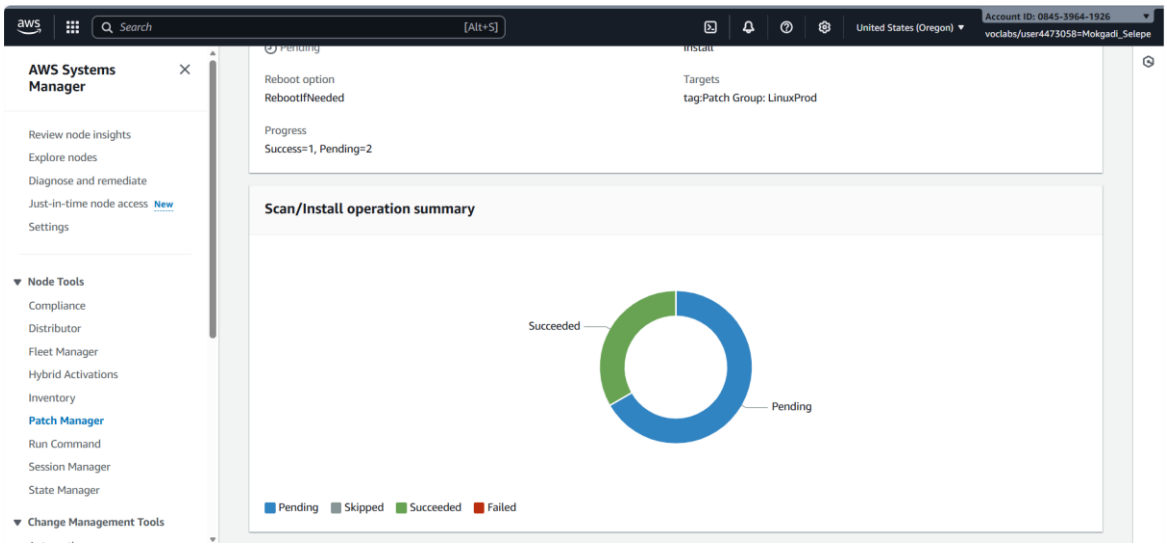

AWS Systems Manager
AWS Systems Manager > Patch Manager > Patch now
Patch instances now Info
Basic configuration
Scan for missing patches or install patches, with or without rebooting. For more patching options, use the Configure patching page.
Patching operation
Scan
Scan and install
Instances to patch
Choose whether to patch all instances or only the instances you specify
Patch all instances
Patch only the target instances I specify
Patching log storage
Select or create an S3 bucket for storing patching operation logs. Select Do not store logs if you don't require log information.
No S3 Bucket Found. Click to go to S3.
Patch now
Patch instances now
The Patch now option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.
As part of the Patch now workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.
Patch now uses AWS recommended best practices for concurrency and error threshold options.
Learn more
Patching instances on demand

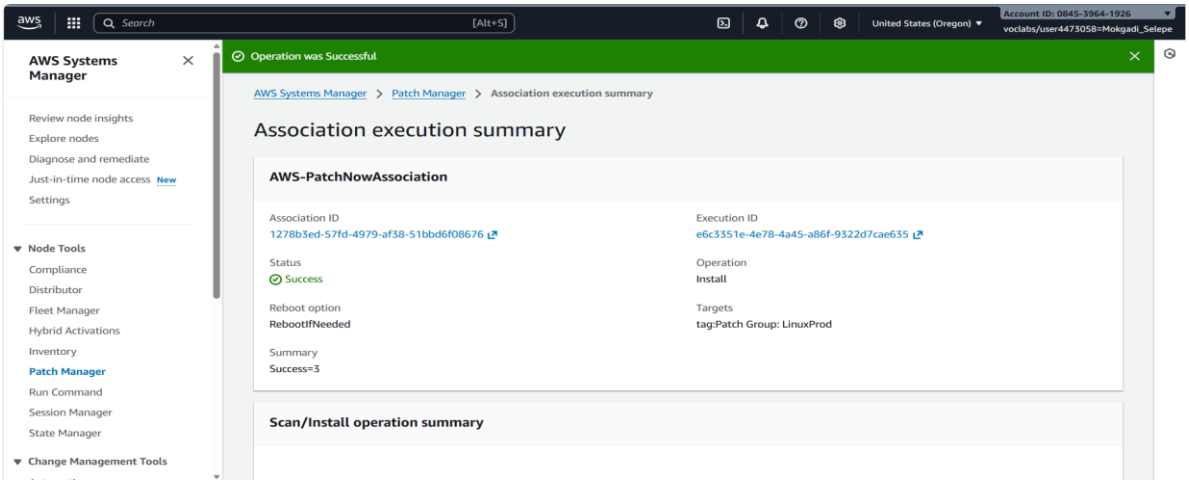

aws
Search
[Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
AWS Systems Manager > Patch Manager > Patch now
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
Patch Manager by default does not do health checks of your applications. It is recommended when patching large fleets to use lifecycle hooks under Advanced options. See Using 'Patch now' lifecycle hooks.
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
Patch instances now
The Patch now option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.
As part of the Patch now workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.
Patch now uses AWS recommended best practices for concurrency and error threshold options.
Learn more
Patching instances on demand

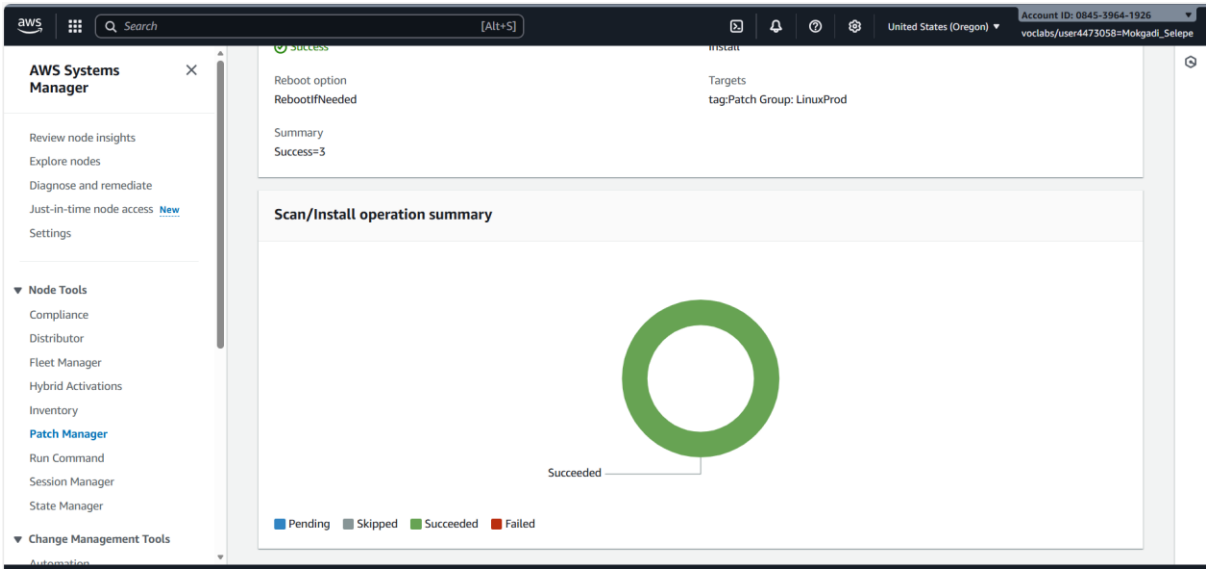

aws
Search
[Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
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)
Patch Group
LinuxProd
Add
Enter a tag key and optional value applied to the instances you want to target, and then choose Add.
Patching log storage
Select or create an S3 bucket for storing patching operation logs. Select Do not store logs if you don't require log information.
No S3 Bucket Found. Click to go to S3.
Advanced options Info
Configure on-instance orchestration for complex patching scenarios.
Create SSM document
Patch instances now
The Patch now option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.
As part of the Patch now workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.
Patch now uses AWS recommended best practices for concurrency and error threshold options.
Learn more
Patching instances on demand


AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
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
Patching log storage
Select or create an S3 bucket for storing patching operation logs. Select Do not store logs if you don't require log information.
No S3 Bucket Found. Click to go to S3.
Advanced options Info
Create SSM document
Patch instances now
The Patch now option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.
As part of the Patch now workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.
Patch now uses AWS recommended best practices for concurrency and error threshold options.
Learn more
Patching instances on demand


Execution details are loading
Data is being refreshed every 3 seconds
AWS Systems Manager > Patch Manager > Association execution summary
Association execution summary
AWS-PatchNowAssociation
Association ID
1278b3ed-57fd-4979-af38-51bbd6f08676
Execution ID
e6c3351e-4e78-4a45-a86f-9322d7cae635
Status
Pending
Operation
Install
Reboot option
RebootIfNeeded
Targets
tag:Patch Group: LinuxProd
Progress
Pending=3
Scan/Install operation summary

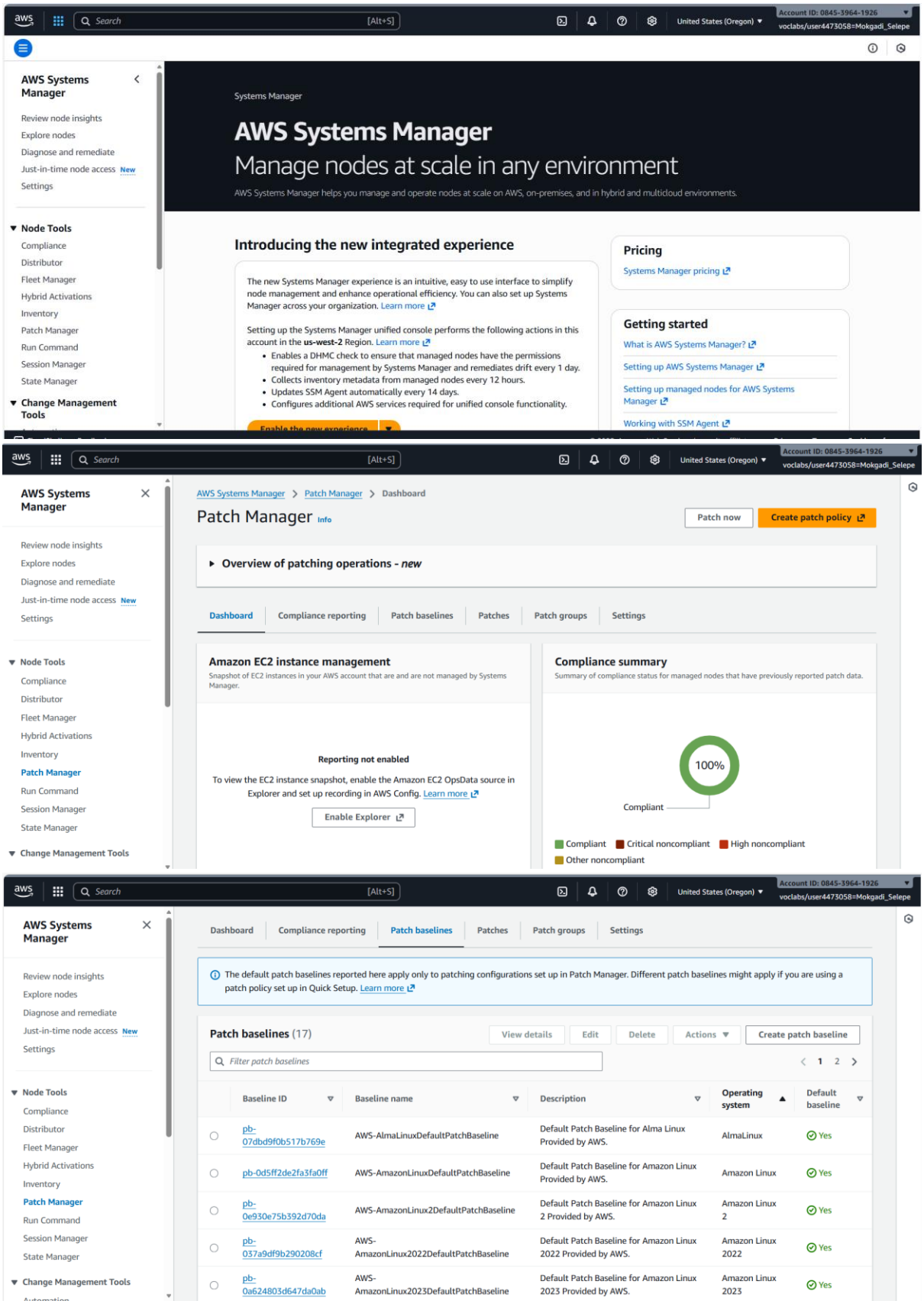

Reboot option
RebootIfNeeded
Targets
tag:Patch Group: LinuxProd
Progress
Success=1, Pending=2
Scan/Install operation summary
Succeeded
Pending
Pending
Skipped
Succeeded
Failed

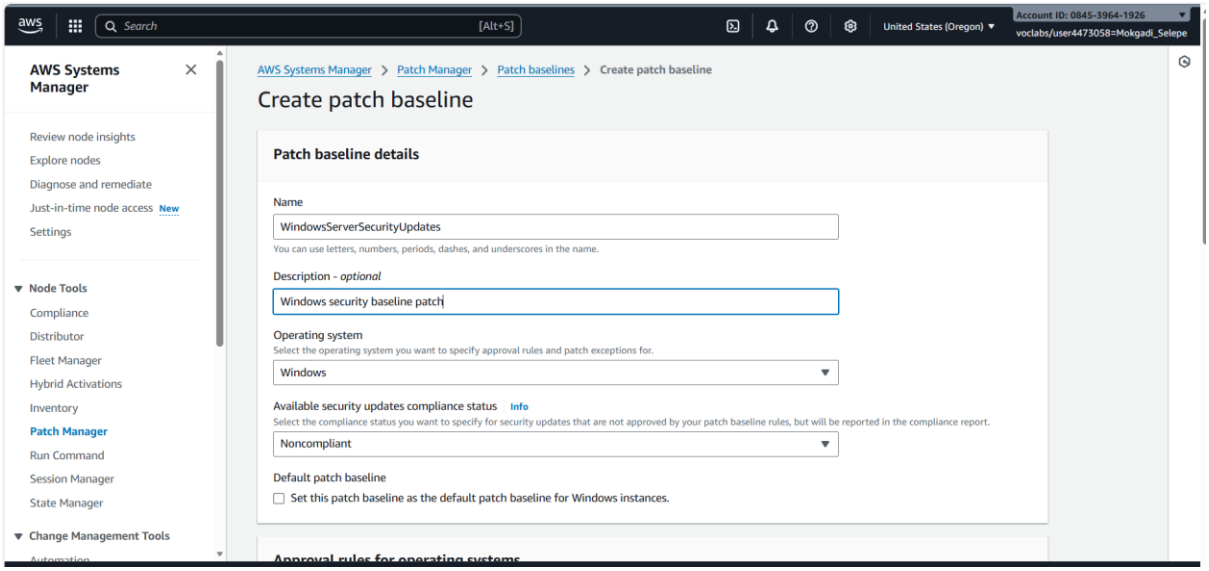


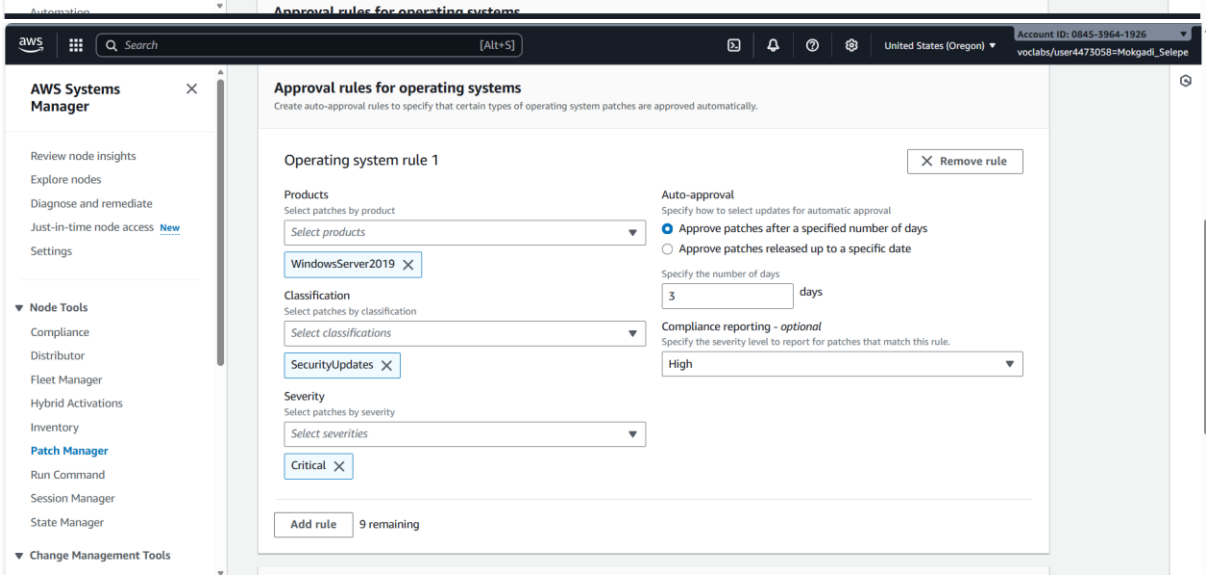


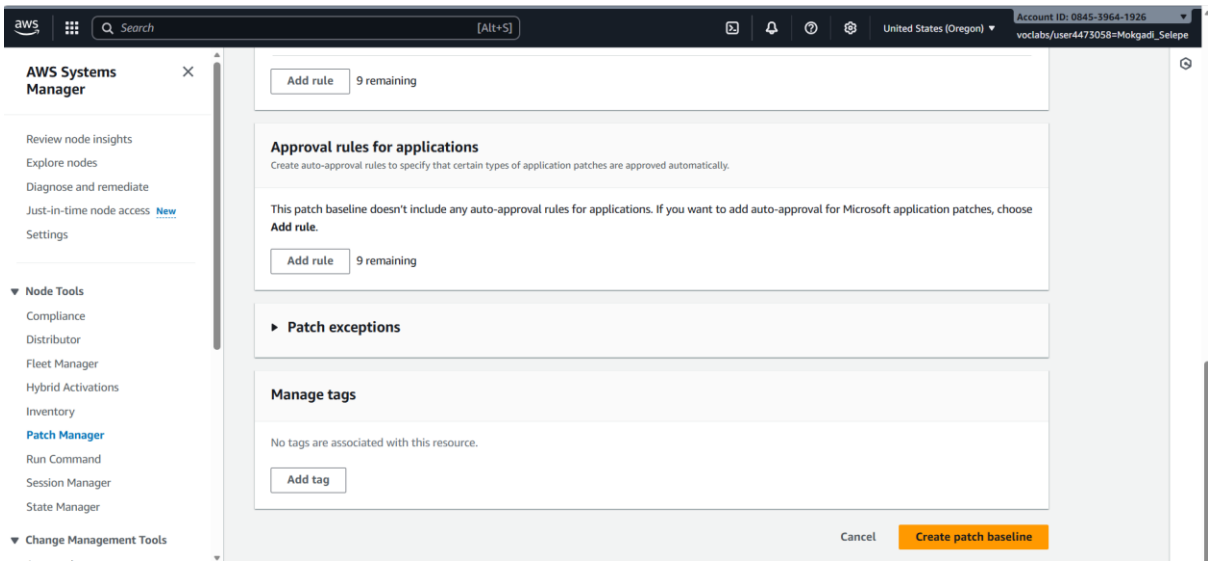
I opened Systems Manager from the console search bar and went to the Fleet Manager page, where I could see the three Linux EC2 instances (and three Windows ones) that are part of the lab.
- I ticked the box next to Linux-1 and clicked Node actions → View details to check its info (OS, IAM role, etc.).
- I went back to the Systems Manager home page and chose Patch Manager under Node Management.
- I clicked Patch now to apply the default baseline AWS-AmazonLinux2DefaultPatchBaseline to the Linux instances.
- In the configuration I set:
  - Patching operation: Scan and install
  - Reboot option: Reboot if needed
  - Instances to patch: Patch only the target instances I specify
  - Target selection: Specify instance tags → Tag key: Patch Group, Tag value: LinuxProd
- After clicking Add and then Patch now, the console showed a status panel with three instances being patched and a visual summary of the scan/install progress.
- I kept an eye on the page until the patch job finished on all three Linux instances.
So, I used the built-in patch baseline to scan for and install updates on the three Linux EC2 instances, and I watched the progress until everything was done.

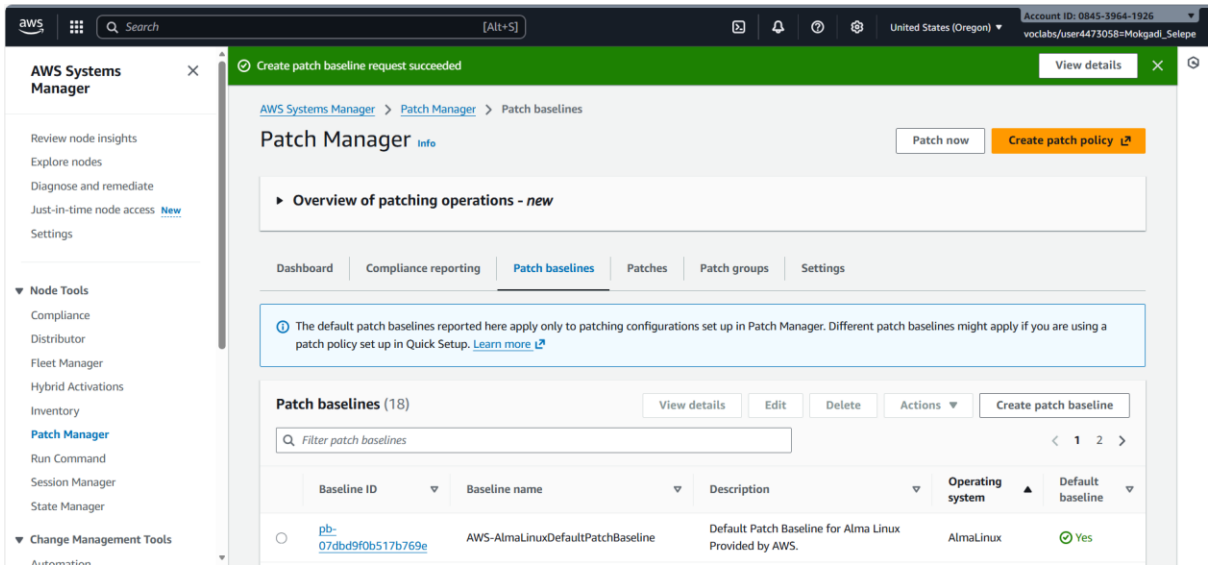
2: Create a custom patch baseline for Windows instances

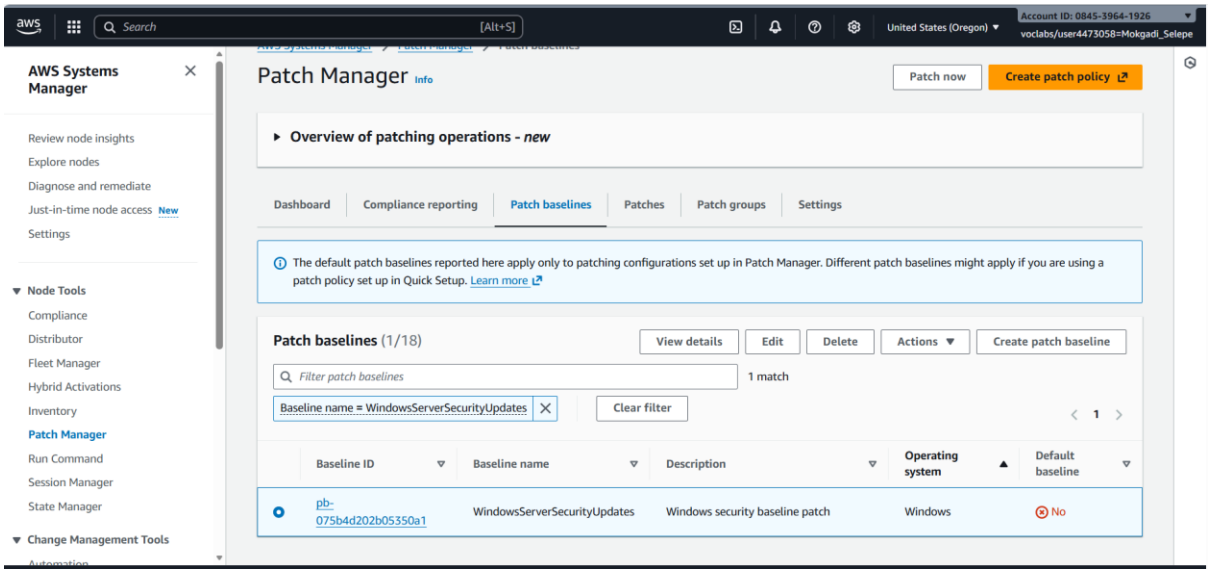

Search [Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
Systems Manager
AWS Systems Manager
Manage nodes at scale in any environment
AWS Systems Manager helps you manage and operate nodes at scale on AWS, on-premises, and in hybrid and multicloud environments.
Introducing the new integrated experience
The new Systems Manager experience is an intuitive, easy to use interface to simplify node management and enhance operational efficiency. You can also set up Systems Manager across your organization. Learn more
Setting up the Systems Manager unified console performs the following actions in this account in the us-west-2 Region. Learn more
Enables a DHMC check to ensure that managed nodes have the permissions required for management by Systems Manager and remediates drift every 1 day.
Collects inventory metadata from managed nodes every 12 hours.
Updates SSM Agent automatically every 14 days.
Configures additional AWS services required for unified console functionality.
Pricing
Systems Manager pricing
Getting started
What is AWS Systems Manager?
Setting up AWS Systems Manager
Setting up managed nodes for AWS Systems Manager
Working with SSM Agent
AWS Systems Manager > Patch Manager > Dashboard
Patch Manager Info
Patch now
Create patch policy
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
The default patch baselines reported here apply only to patching configurations set up in Patch Manager. Different patch baselines might apply if you are using a patch policy set up in Quick Setup. Learn more
Patch baselines (17)
View details
Edit
Delete
Actions
Create patch baseline
Filter patch baselines
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

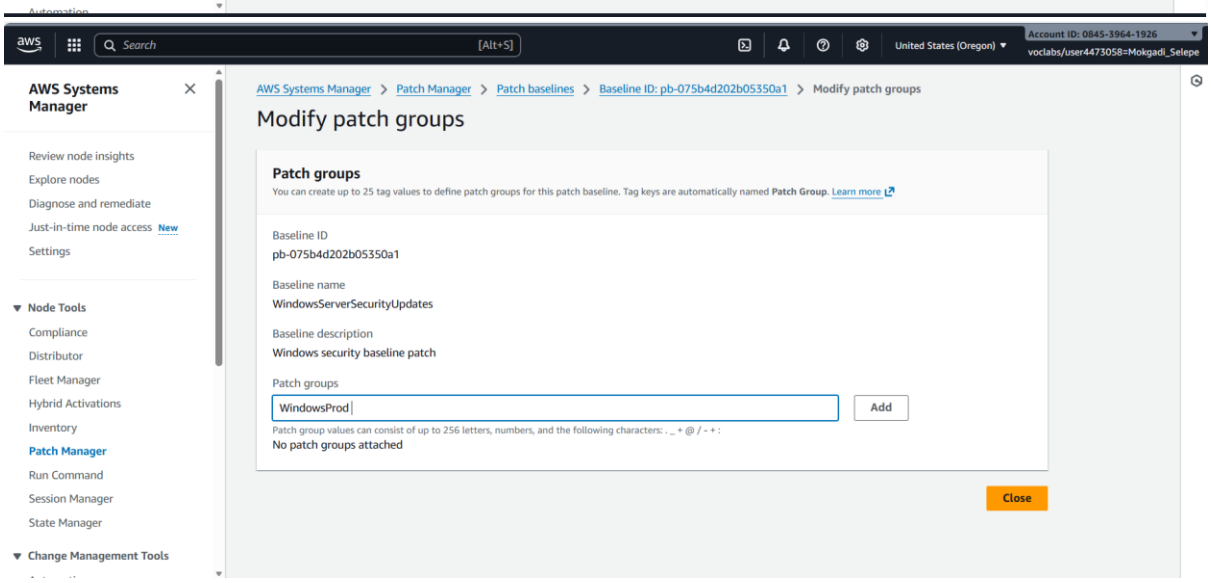

aws
Search
[Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
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
Available security updates compliance status Info
Select the compliance status you want to specify for security updates that are not approved by your patch baseline rules, but will be reported in the compliance report.
Noncompliant
Default patch baseline
Set this patch baseline as the default patch baseline for Windows instances.

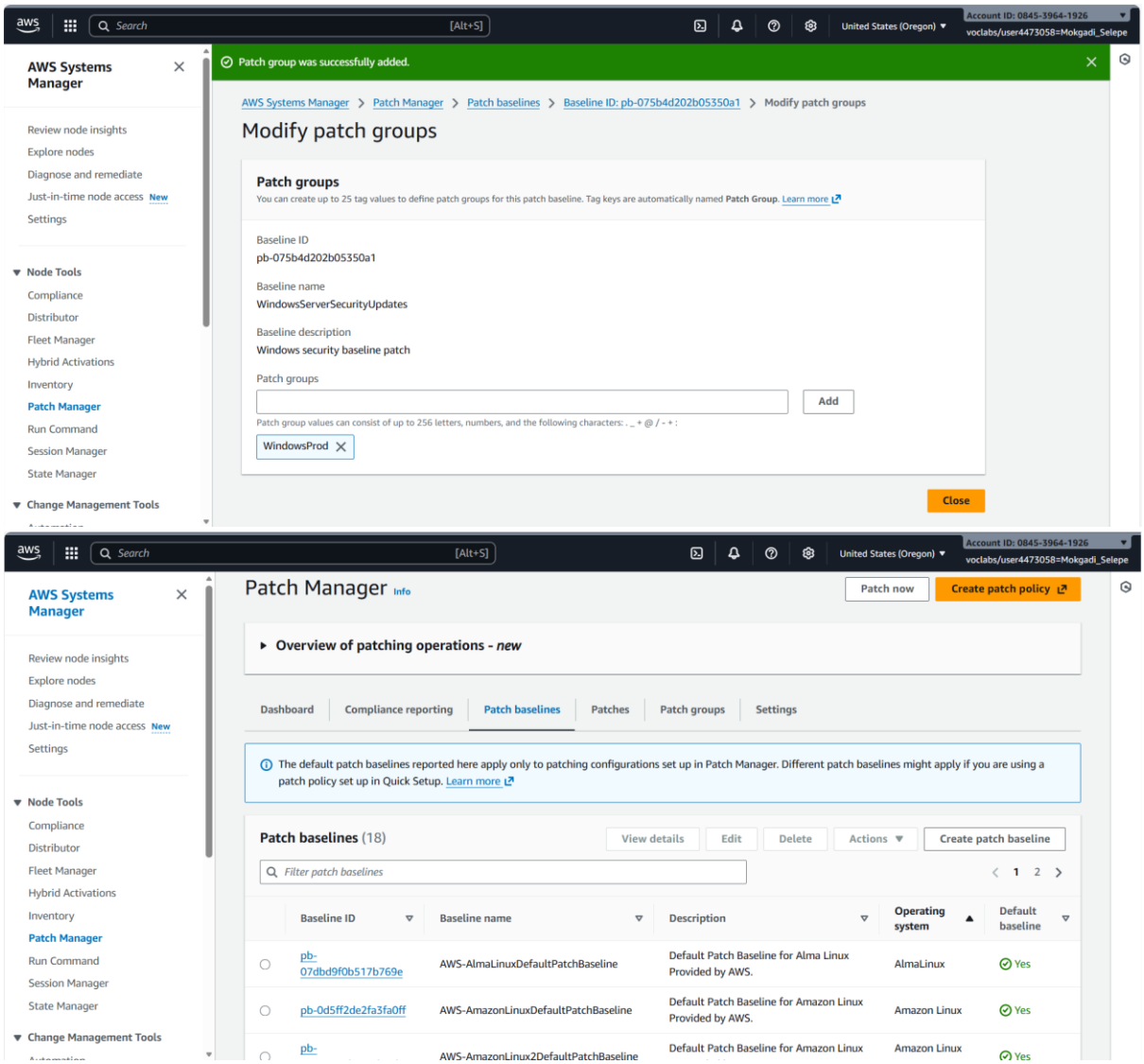

aws
Search
[Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
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.
High
Add rule
9 remaining


aws
Search
[Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
Add rule
9 remaining
Approval rules for applications
Create auto-approval rules to specify that certain types of application patches are approved automatically.
This patch baseline doesn't include any auto-approval rules for applications. If you want to add auto-approval for Microsoft application patches, choose Add rule.
Add rule
9 remaining
Patch exceptions
Manage tags
No tags are associated with this resource.
Add tag
Cancel
Create patch baseline


Create patch baseline request succeeded
View details
AWS Systems Manager > Patch Manager > Patch baselines
Patch Manager Info
Patch now
Create patch policy
Overview of patching operations - new
Dashboard
Compliance reporting
Patch baselines
Patches
Patch groups
Settings
The default patch baselines reported here apply only to patching configurations set up in Patch Manager. Different patch baselines might apply if you are using a patch policy set up in Quick Setup. Learn more
Patch baselines (18)
View details
Edit
Delete
Actions
Create patch baseline
Filter patch baselines
Baseline ID
Baseline name
Description
Operating system
Default baseline
pb-07dbd9f0b517b769e
AWS-AlmaLinuxDefaultPatchBaseline
Default Patch Baseline for Alma Linux Provided by AWS.
AlmaLinux
Yes


Patch Manager Info
Patch now
Create patch policy
Overview of patching operations - new
Dashboard
Compliance reporting
Patch baselines
Patches
Patch groups
Settings
The default patch baselines reported here apply only to patching configurations set up in Patch Manager. Different patch baselines might apply if you are using a patch policy set up in Quick Setup. Learn more
Patch baselines (1/18)
View details
Edit
Delete
Actions
Create patch baseline
Filter patch baselines
1 match
Baseline name = WindowsServerSecurityUpdates
Clear filter
Baseline ID
Baseline name
Description
Operating system
Default baseline
pb-075b4d202b05350a1
WindowsServerSecurityUpdates
Windows security baseline patch
Windows
No


AWS Systems Manager > Patch Manager > Patch baselines > Baseline ID: pb-075b4d202b05350a1 > 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-075b4d202b05350a1
Baseline name
WindowsServerSecurityUpdates
Baseline description
Windows security baseline patch
Patch groups
WindowsProd
Add
Patch group values can consist of up to 256 letters, numbers, and the following characters: . _ + @ / - + :
No patch groups attached
Close



I went back to the Systems Manager console and opened Patch Manager.

- Clicked Patch baselines and then Create patch baseline.
- Filled in the details:
  - Name: WindowsServerSecurityUpdates
  - Description: Windows security baseline patch
  - Operating system: Windows (left “Default patch baseline” unchecked)

- Set up the first approval rule:
  - Products: WindowsServer2019 (removed “All”)
  - Severity: Critical
  - Classification: SecurityUpdates
  - Auto-approval: 3 days
  - Compliance reporting: Critical

- Added a second rule:
  - Products: WindowsServer2019 (again, no “All”)

- Severity: Important
- Classification: SecurityUpdates
- Auto-approval: 3 days
- Compliance reporting: High

- Hit Create patch baseline.

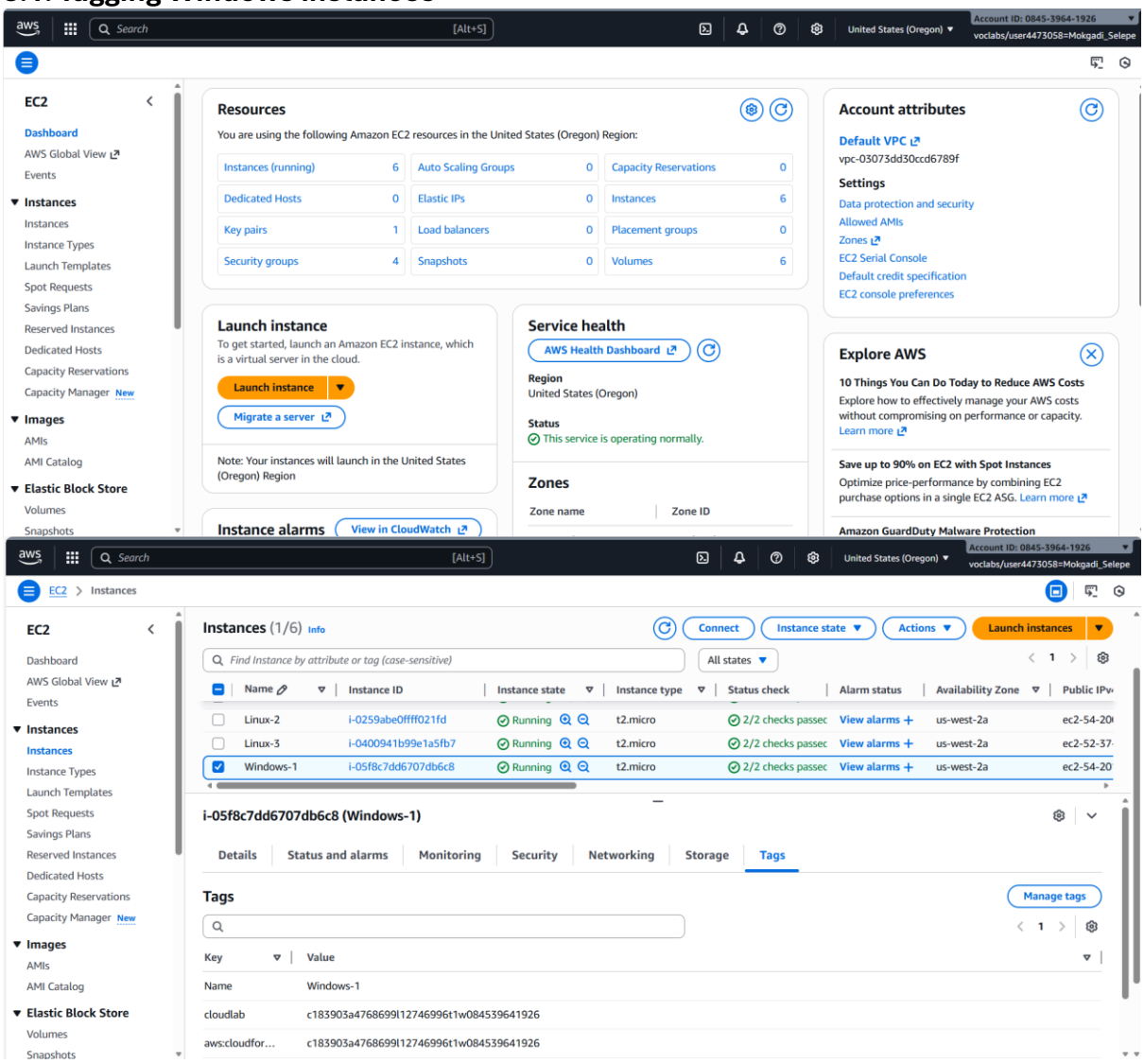
Next, I linked the new baseline to a patch group:

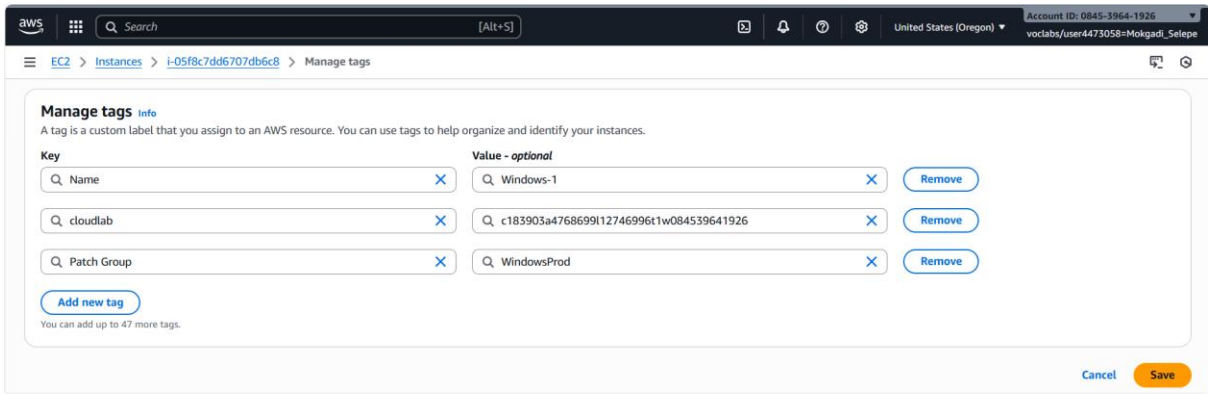
- Selected the newly created WindowsServerSecurityUpdates baseline (had to search or go to the next page).
- Chose Actions → Modify patch groups.
- Entered WindowsProd as the patch group, clicked Add, then Close.

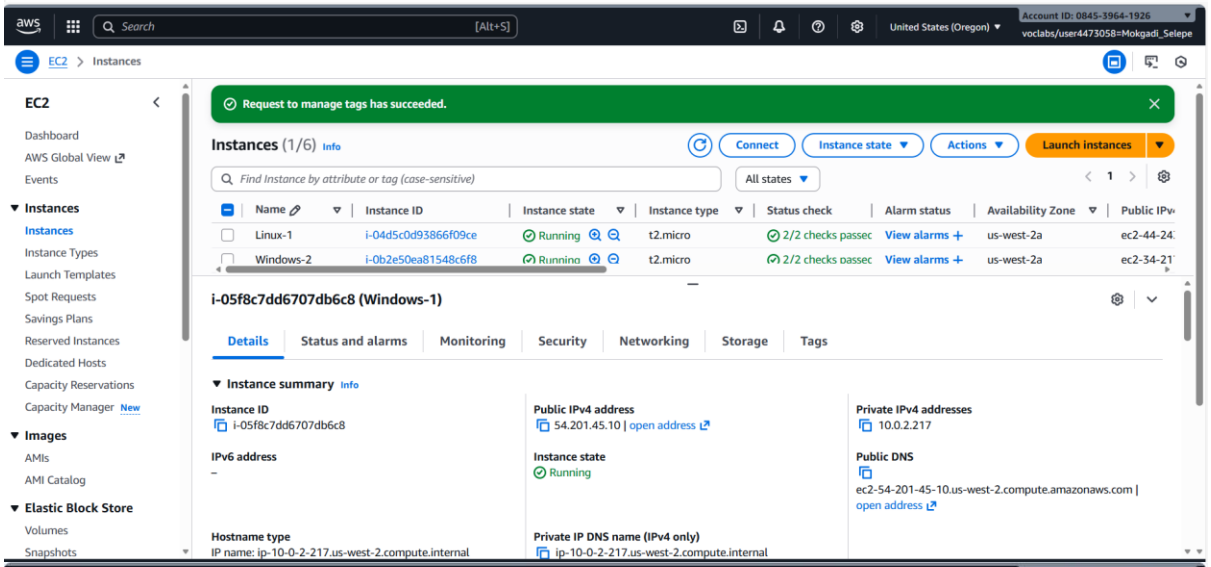
So, I built a custom patch baseline that only pulls critical and important security updates for Windows Server 2019 and tied it to the “WindowsProd” patch group. This will let me apply those updates automatically to the Windows instances I tag that way.

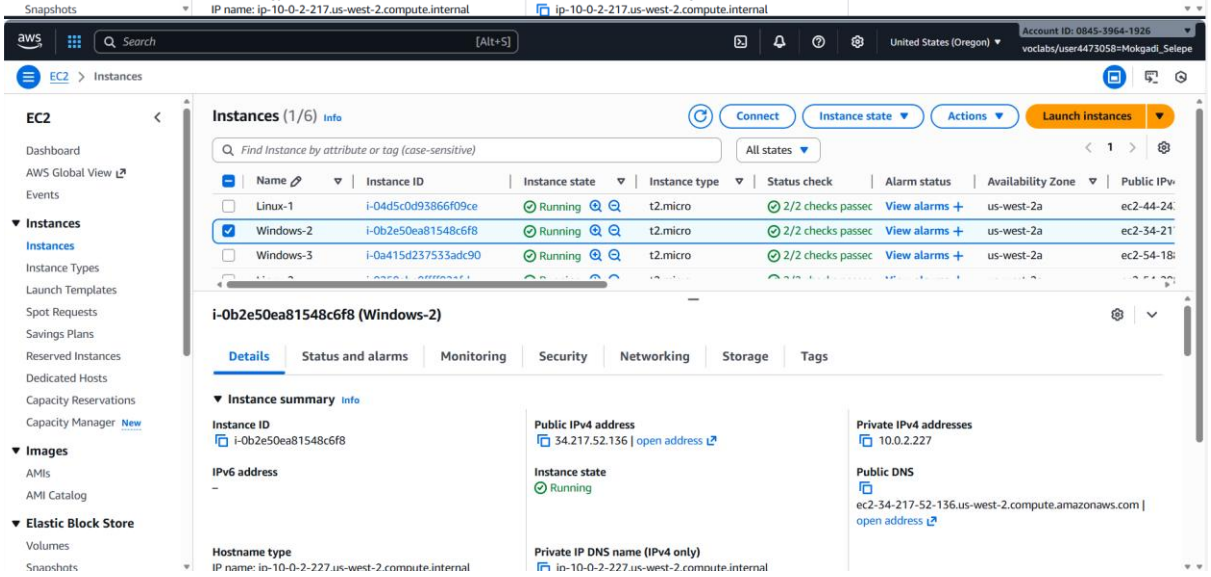
3: Patching the Windows instances

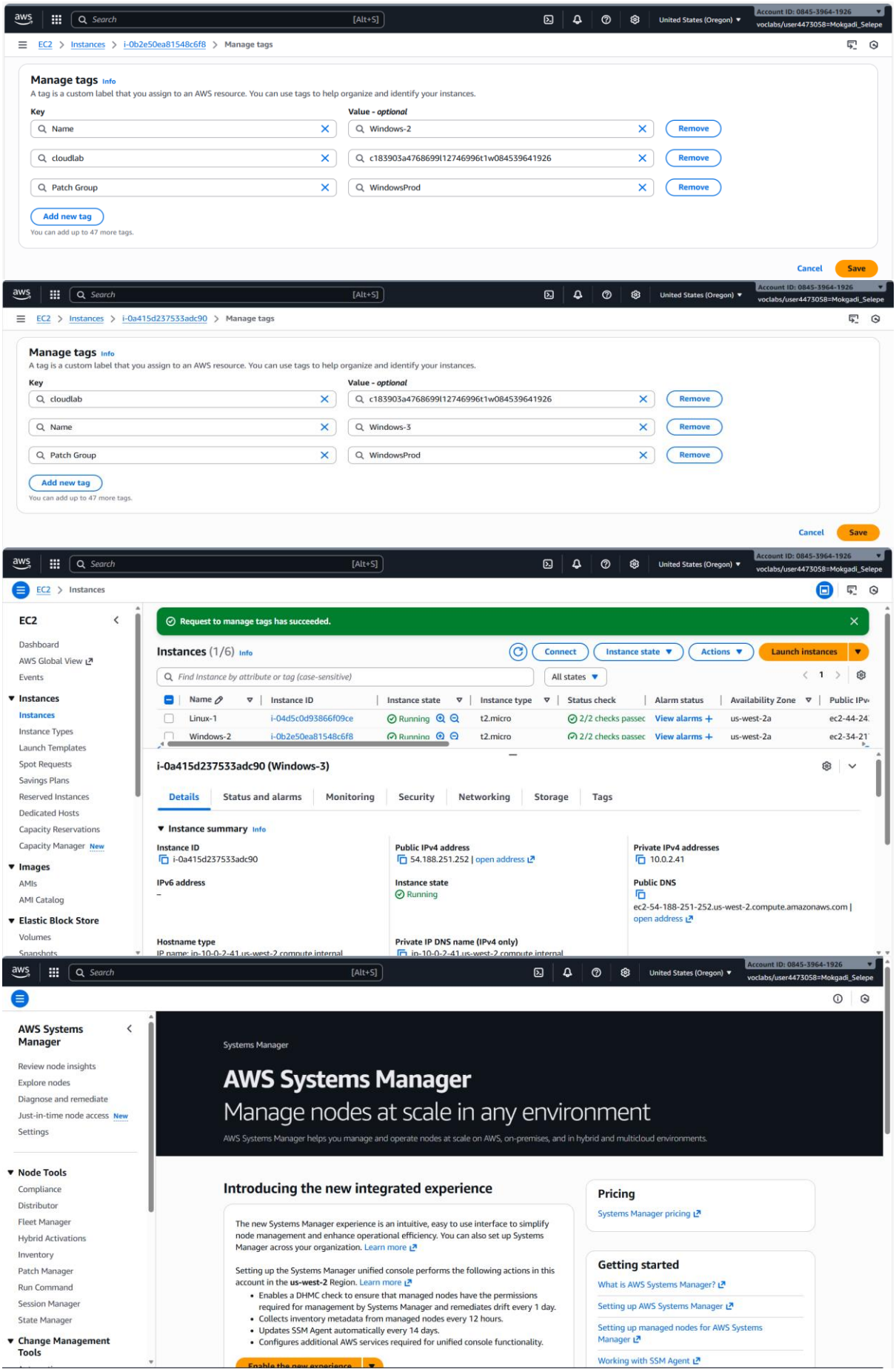
3.1: Tagging Windows instances

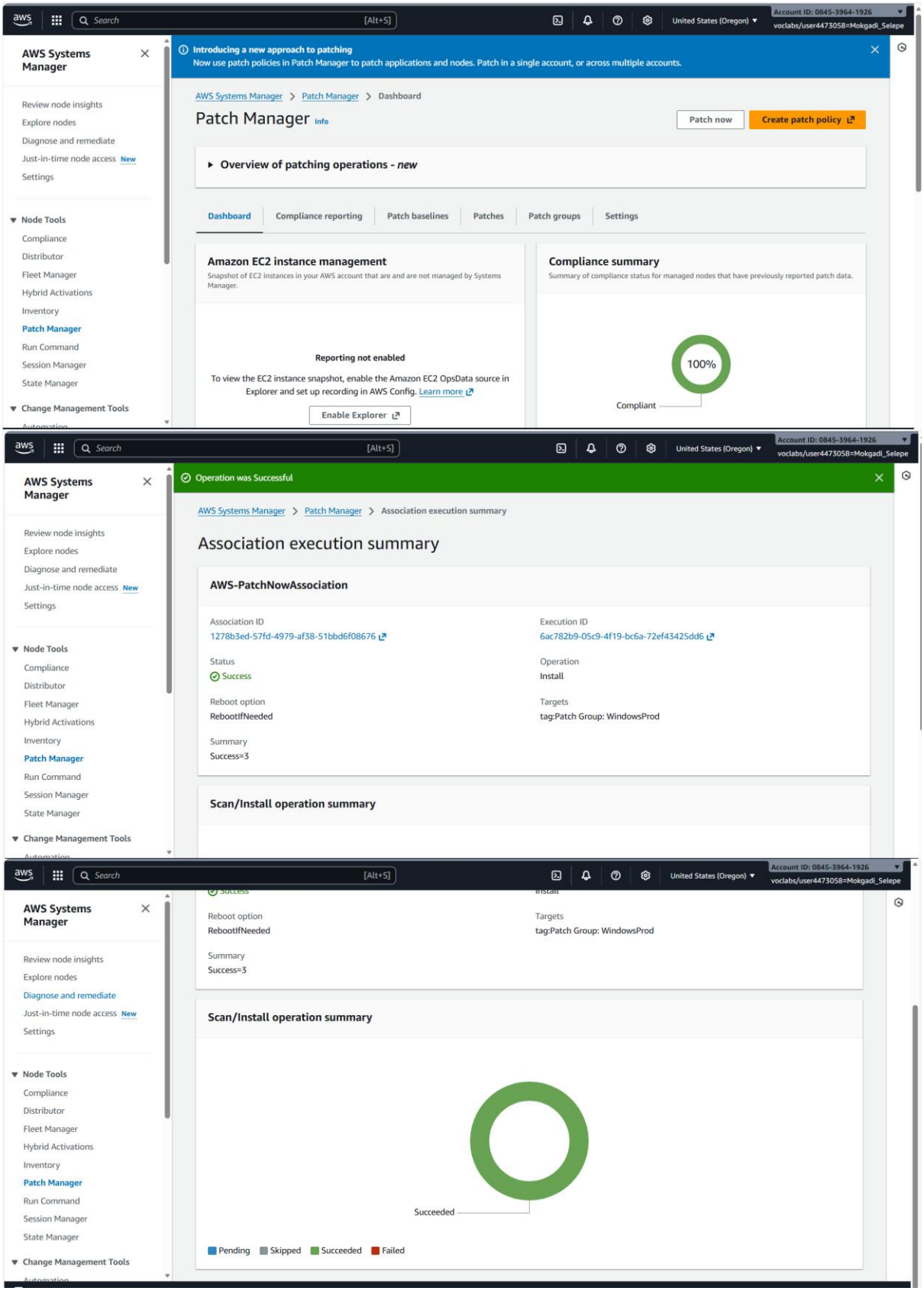


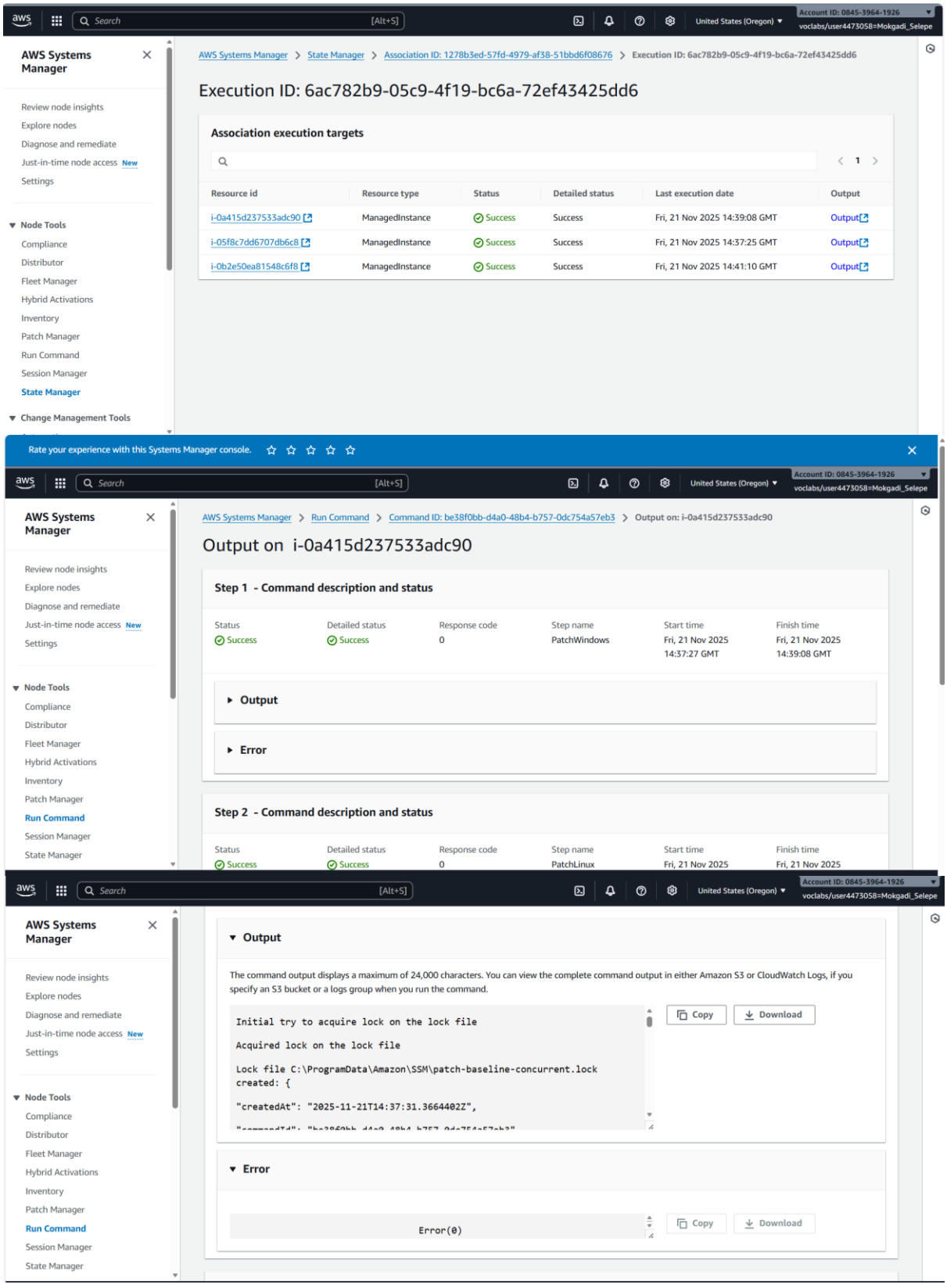

Search [Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
EC2 > Instances > i-05f8c7dd6707db6c8 > Manage tags
Manage tags Info
A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.
Key
Value - optional
Name
Windows-1
Remove
cloudlab
c183903a4768699l12746996t1w084539641926
Remove
Patch Group
WindowsProd
Remove
Add new tag
You can add up to 47 more tags.
Cancel
Save


Search [Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
EC2 > Instances
EC2
Request to manage tags has succeeded.
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1/6) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv
Linux-1
i-04d5c0d93866f09ce
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
Windows-2
i-0b2e50ea81548c6f8
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
i-05f8c7dd6707db6c8 (Windows-1)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-05f8c7dd6707db6c8
Public IPv4 address
54.201.45.10 | open address
Private IPv4 addresses
10.0.2.217
IPv6 address
–
Instance state
Running
Public DNS
ec2-54-201-45-10.us-west-2.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-2-217.us-west-2.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-2-217.us-west-2.compute.internal


Search [Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
EC2 > Instances
EC2
Instances (1/6) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Linux-1
i-04d5c0d93866f09ce
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
Windows-2
i-0b2e50ea81548c6f8
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
Windows-3
i-0a415d237533adc90
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
i-0b2e50ea81548c6f8 (Windows-2)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0b2e50ea81548c6f8
Public IPv4 address
34.217.52.136 | open address
Private IPv4 addresses
10.0.2.227
IPv6 address
–
Instance state
Running
Public DNS
ec2-34-217-52-136.us-west-2.compute.amazonaws.com | open address
Hostname type
Private IP DNS name (IPv4 only)


Search [Alt+S]
United States (Oregon)
Account ID: 0845-3964-1926
voclabs/user4473058=Mokgadi_Selepe
EC2 > Instances > i-0b2e50ea81548c6f8 > Manage tags
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
Name
Windows-2
Remove
cloudlab
c183903a4768699l12746996t1w084539641926
Remove
Patch Group
WindowsProd
Remove
Add new tag
You can add up to 47 more tags.
Cancel
Save
EC2 > Instances > i-0a415d237533adc90 > Manage tags
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
cloudlab
c183903a4768699l12746996t1w084539641926
Remove
Name
Windows-3
Remove
Patch Group
WindowsProd
Remove
Add new tag
You can add up to 47 more tags.
Cancel
Save
EC2 > Instances
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Request to manage tags has succeeded.
Instances (1/6) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
Linux-1
i-04d5c0d93866f09ce
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
ec2-44-24
Windows-2
i-0b2e50ea81548c6f8
Running
t2.micro
2/2 checks passed
View alarms +
us-west-2a
ec2-34-21
i-0a415d237533adc90 (Windows-3)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0a415d237533adc90
Public IPv4 address
54.188.251.252 | open address
Private IPv4 addresses
10.0.2.41
IPv6 address
–
Instance state
Running
Public DNS
ec2-54-188-251-252.us-west-2.compute.amazonaws.com | open address
Hostname type
Private IP DNS name (IPv4 only)
AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
Systems Manager
AWS Systems Manager
Manage nodes at scale in any environment
AWS Systems Manager helps you manage and operate nodes at scale on AWS, on-premises, and in hybrid and multicloud environments.
Introducing the new integrated experience
The new Systems Manager experience is an intuitive, easy to use interface to simplify node management and enhance operational efficiency. You can also set up Systems Manager across your organization. Learn more
Setting up the Systems Manager unified console performs the following actions in this account in the us-west-2 Region. Learn more
Enables a DHMC check to ensure that managed nodes have the permissions required for management by Systems Manager and remediates drift every 1 day.
Collects inventory metadata from managed nodes every 12 hours.
Updates SSM Agent automatically every 14 days.
Configures additional AWS services required for unified console functionality.
Pricing
Systems Manager pricing
Getting started
What is AWS Systems Manager?
Setting up AWS Systems Manager
Setting up managed nodes for AWS Systems Manager
Working with SSM Agent


AWS Systems Manager
Introducing a new approach to patching
Now use patch policies in Patch Manager to patch applications and nodes. Patch in a single account, or across multiple accounts.
AWS Systems Manager > Patch Manager > Dashboard
Patch Manager Info
Patch now
Create patch policy
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
Operation was Successful
AWS Systems Manager > Patch Manager > Association execution summary
Association execution summary
AWS-PatchNowAssociation
Association ID
1278b3ed-57fd-4979-af38-51bbd6f08676
Execution ID
6ac782b9-05c9-4f19-bc6a-72ef43425dd6
Status
Success
Operation
Install
Reboot option
RebootIfNeeded
Targets
tag:Patch Group: WindowsProd
Summary
Success=3
Scan/Install operation summary
Succeeded
Pending
Skipped
Succeeded
Failed



I opened the EC2 console and tagged the three Windows instances so they belong to the same patch group:

- Selected Windows-1, went to the Tags tab, clicked Manage tags, added a tag Patch Group = WindowsProd, and saved.

- Repeated the same steps for Windows-2 and Windows-3.

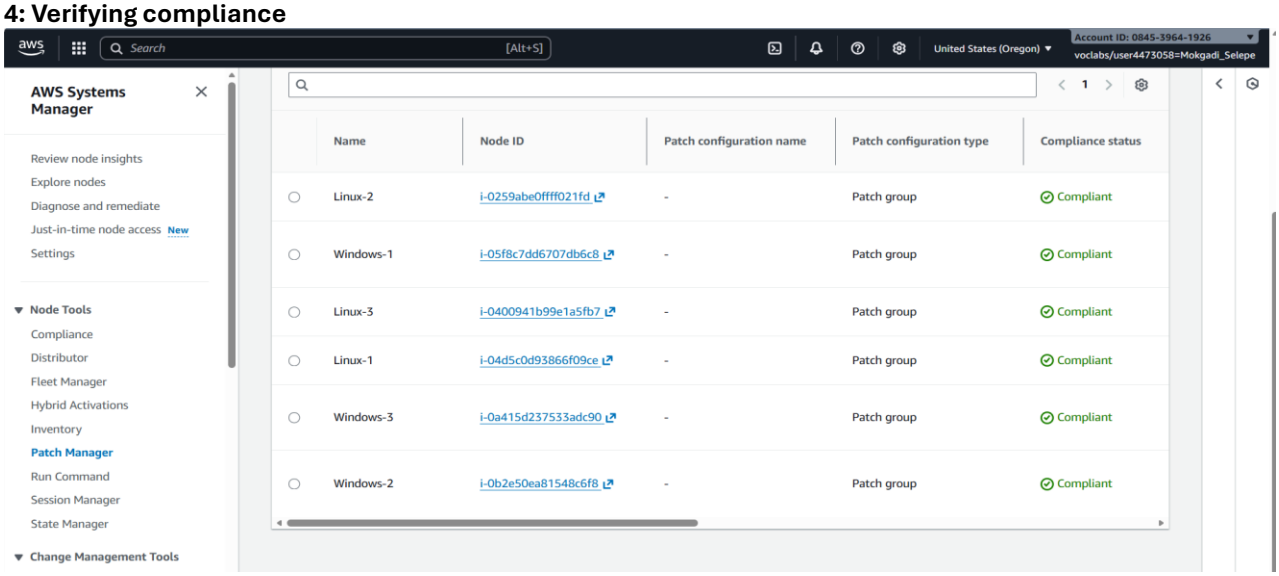
Then I went back to Systems Manager and used Patch Manager to apply the custom Windows patch baseline:

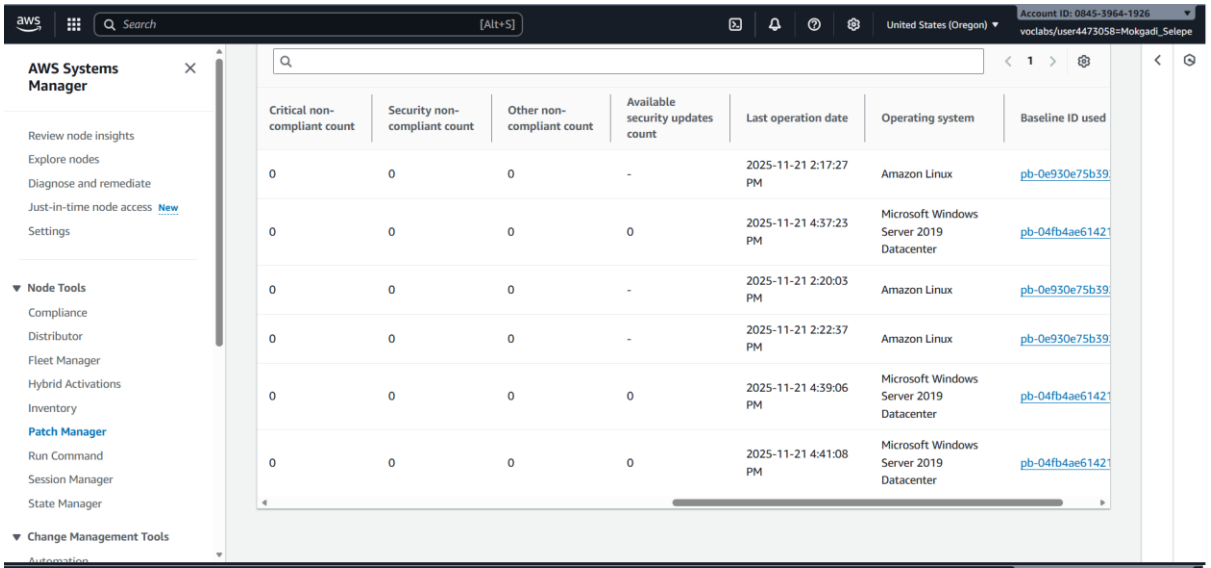
- Opened Patch Manager, chose Patch now.
- Set the options:
  - Patching operation: Scan and install
  - Reboot option: Reboot if needed
  - Instances to patch: Patch only the target instances I specify
  - Target selection: Specify instance tags → Tag key: Patch Group, Tag value: WindowsProd
- Clicked Add and then Patch now.

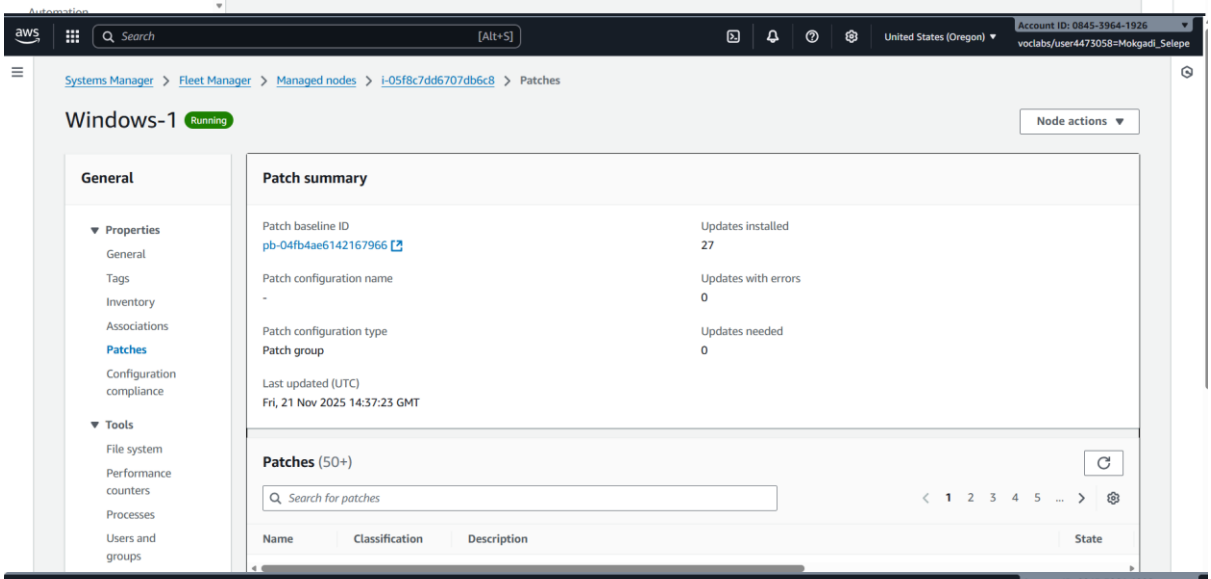
A new page showed the patch job starting. When the Execution ID link appeared, I clicked it, which opened the State Manager page. From there I opened the Output for one of the instances that was InProgress, which took me to the Run Command page. Expanding the output let me see the details of the patch operation, including the line PatchGroup: WindowsProd.

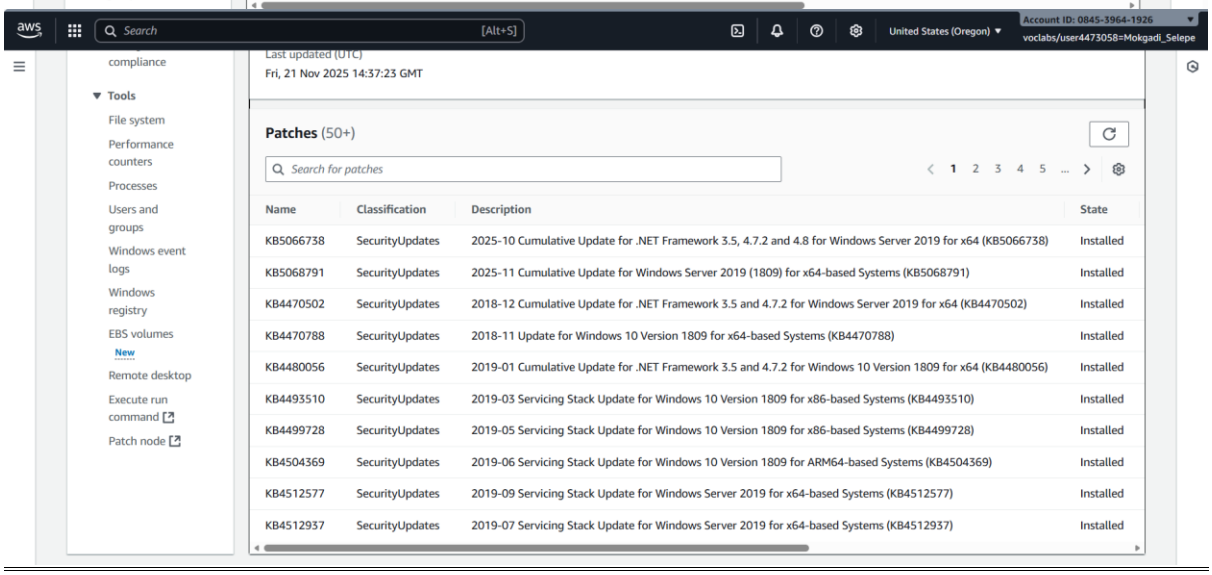
In short, I tagged the Windows EC2 instances, told Patch Manager to scan and install patches only on those tagged instances, and watched the patch job run and report its results.

4: Verifying compliance




AWS Systems Manager
Review node insights
Explore nodes
Diagnose and remediate
Just-in-time node access New
Settings
Node Tools
Compliance
Distributor
Fleet Manager
Hybrid Activations
Inventory
Patch Manager
Run Command
Session Manager
State Manager
Change Management Tools
Critical non-compliant count
Security non-compliant count
Other non-compliant count
Available security updates count
Last operation date
Operating system
Baseline ID used
0 0 0 - 2025-11-21 2:17:27 PM Amazon Linux pb-0e930e75b39
0 0 0 0 2025-11-21 4:37:23 PM Microsoft Windows Server 2019 Datacenter pb-04fb4ae6142
0 0 0 - 2025-11-21 2:20:03 PM Amazon Linux pb-0e930e75b39
0 0 0 - 2025-11-21 2:22:37 PM Amazon Linux pb-0e930e75b39
0 0 0 0 2025-11-21 4:39:06 PM Microsoft Windows Server 2019 Datacenter pb-04fb4ae6142
0 0 0 0 2025-11-21 4:41:08 PM Microsoft Windows Server 2019 Datacenter pb-04fb4ae6142


Systems Manager > Fleet Manager > Managed nodes > i-05f8c7dd6707db6c8 > Patches
Windows-1 Running
Node actions
General
Properties
General
Tags
Inventory
Associations
Patches
Configuration compliance
Tools
File system
Performance counters
Processes
Users and groups
Patch summary
Patch baseline ID
pb-04fb4ae6142167966
Patch configuration name
-
Patch configuration type
Patch group
Last updated (UTC)
Fri, 21 Nov 2025 14:37:23 GMT
Updates installed
27
Updates with errors
0
Updates needed
0
Patches (50+)
Search for patches
Name
Classification
Description
State


Last updated (UTC)
Fri, 21 Nov 2025 14:37:23 GMT
Tools
File system
Performance counters
Processes
Users and groups
Windows event logs
Windows registry
EBS volumes New
Remote desktop
Execute run command
Patch node
Patches (50+)
Search for patches
Name Classification Description State
KB5066738 SecurityUpdates 2025-10 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5066738) Installed
KB5068791 SecurityUpdates 2025-11 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5068791) Installed
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
KB4512937 SecurityUpdates 2019-07 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4512937) Installed

I went back into Patch Manager and opened the Dashboard.

- Under Compliance summary I saw Compliant: 6 – that means all six of my instances (the three Linux and three Windows ones) passed the patch check.
- I switched to the Compliance reporting tab, which lists every instance that's managed by Systems Manager. All of them showed a status of Compliant, so nothing was left out of date.

I scrolled the table to the right to see more details for each node:

- Critical non-compliant count – 0
- Security non-compliant count – 0
- Other non-compliant count – 0
- Last operation date – shows when the last patch job ran
- Baseline ID – the patch baseline that was applied

Then I clicked the Node ID for one of the Windows instances. On that node's page I chose the Patch tab, scrolled down, and saw a list of the patches that were installed, along with the Installed Time for each one.

So, the dashboard confirmed that every Linux and Windows instance is up-to-date and compliant, and I could drill into each node to see exactly which patches were applied and when.

Conclusion

I just wrapped up the lab and here's what I did, in plain English:

- I patched the three Linux EC2 instances using the built-in default baseline (AWS-AmazonLinux2DefaultPatchBaseline).
- I created a custom patch baseline called WindowsServerSecurityUpdates that grabs only critical and important security updates for Windows Server 2019.
- I tagged the three Windows instances with Patch Group = WindowsProd, added that tag to the custom baseline, and ran "Patch now" so the Windows machines got the updates from my custom baseline.
- I checked the Patch Manager dashboard and saw "Compliant: 6", confirming that all six instances (Linux and Windows) are up-to-date and compliant.
