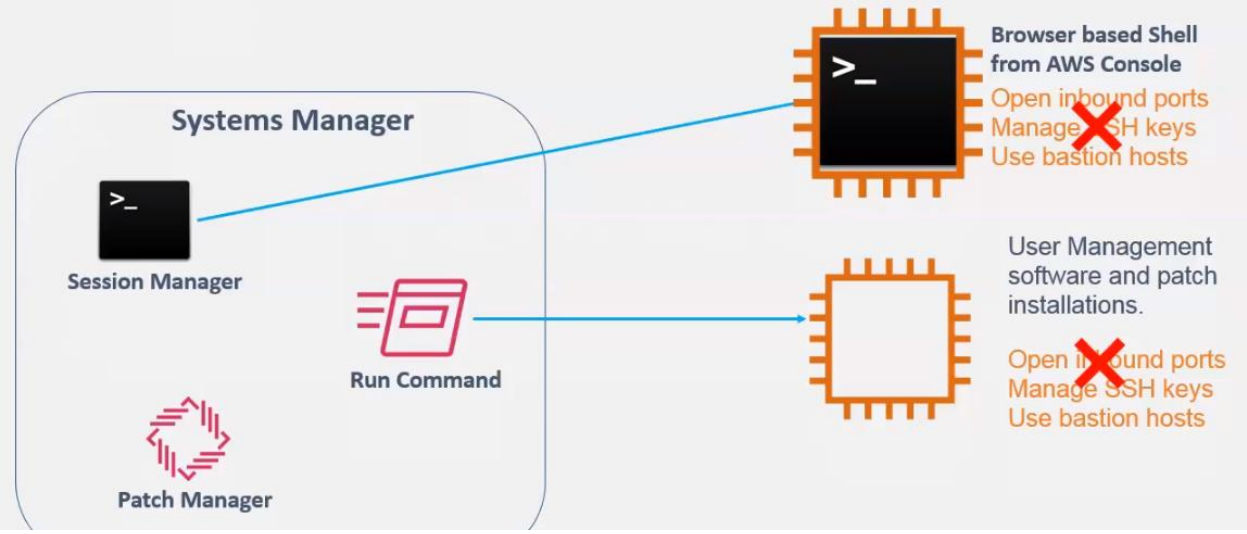
AWS Systems Manager Overview

- Systems Manager provides visibility and control of the infrastructure on AWS
- helps to view operational data from multiple AWS services and automates operational tasks across AWS resources.
- A managed instance is any EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager.
- works with managed instances, which are configured for use with Systems Manager
- helps configure and maintain managed instances.
- helps maintain security and compliance by scanning the *managed instances* and reporting on (or taking corrective action on) any policy violations it detects.
- supported machine types include EC2 instances, on-premises servers, and virtual machines (VMs), including VMs in other cloud environments.
- supported operating system types include Windows Server, multiple distributions of Linux, and Raspbian.



Operations Management

Capabilities that help manage the AWS resources

- Trusted Advisor is an online tool that provides real-time guidance to help you provision the resources following AWS best practices
- AWS Personal Health Dashboard provides information about AWS Health events that can affect your account
- OpsCenter provides a central location where operations engineers and IT professionals can view, investigate, and resolve operational work items (OpsItems) related to AWS resources

Application Management

SSM Parameter Store

- provides secure, scalable, hierarchical storage for configuration data and secrets management.
- can store data such as passwords, database strings, and license codes as parameter values.
- supports values as plain text or encrypted data
- parameters can be referenced by using the unique name specified during parameter creation
- supports versioning of configuration/secrets
- provides high availability as Parameter Store is hosted in multiple AZs in an AWS Region.
- can be configured for change notifications and invoke automated actions for both parameters and parameter policies

Change Management

Capabilities for taking action against or changing the AWS resources

Systems Manager Automation

- helps automate common maintenance and deployment tasks *for e.g. create and update AMIs, apply driver and agent updates, reset passwords on Windows instances, reset SSH keys on Linux instances, and apply OS patches or application updates.*

Maintenance Windows

- helps set up recurring schedules for managed instances to run administrative tasks like installing patches and updates without interrupting business-critical operations.

Node Management

Capabilities for managing the EC2 instances, on-premises servers and virtual machines (VMs) in the hybrid environment, and other types of AWS resources (nodes)

Systems Manager Configuration Compliance

- helps scan fleet of managed instances for patch compliance and configuration inconsistencies.
- helps collect and aggregate data from multiple AWS accounts and Regions, and then drill down into specific resources that aren't compliant.
- provides, by default, displays compliance data about Patch Manager patching and State Manager associations, but can be customized

Systems Manager Inventory

- provides visibility into the EC2 and on-premises computing environment
- collect metadata from the managed instances about applications, files, components, patches, and more on the managed instances
- collects only metadata from the managed instances and doesn't access proprietary information or data.
- supports custom metadata in addition to the pre-configured metadata
- supports inventory data collection from multiple regions and AWS Accounts

- supports inventory data storage in a single centralized location like S3 which can then be queried using Athena.

Systems Manager State Manager

- is a secure and scalable configuration management service that helps automate the process of keeping the managed instances in a defined state.
- helps ensure that the instances are bootstrapped with specific software at startup, joined to a Windows domain (Windows instances only), or patched with specific software updates.
- A State Manager association is a configuration that is assigned to the managed instances which defines the state that you want to maintain on the instances.

Shared Resources

Capabilities for managing and configuring the AWS resources

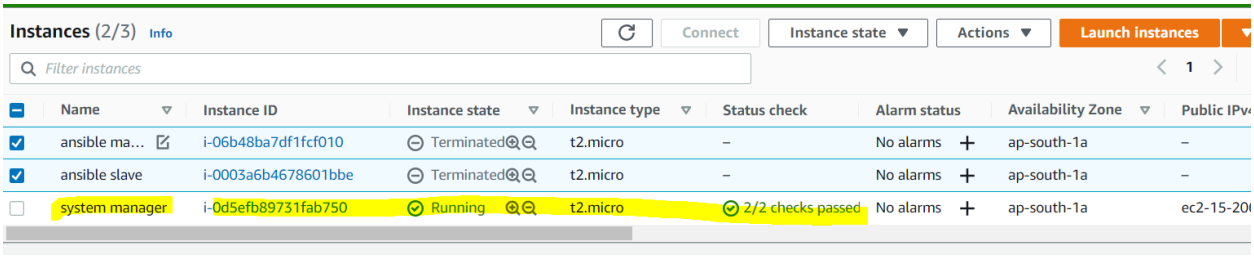
Systems Manager Document (SSM document)

- SSM document defines the actions that the Systems Manager performs.
- SSM document types include
  - *Command* documents, which are used by State Manager and Run Command, and
  - *Automation* documents, which are used by Systems Manager Automation.
- SSM Document can be defined in JSON or YAML and define parameters and actions.

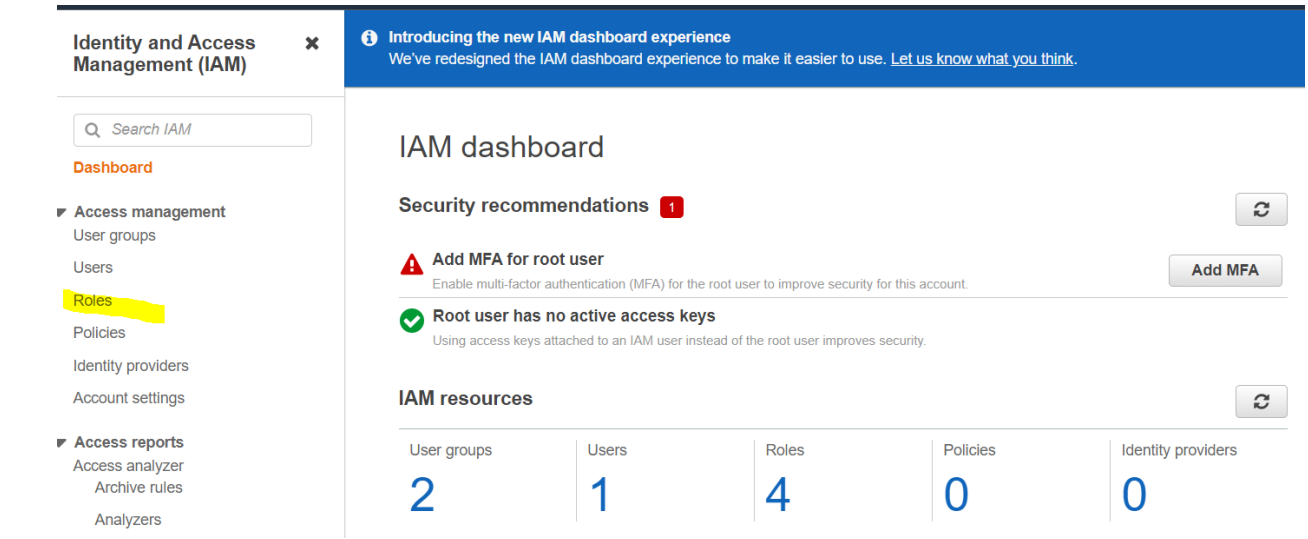
Systems Manager Agent

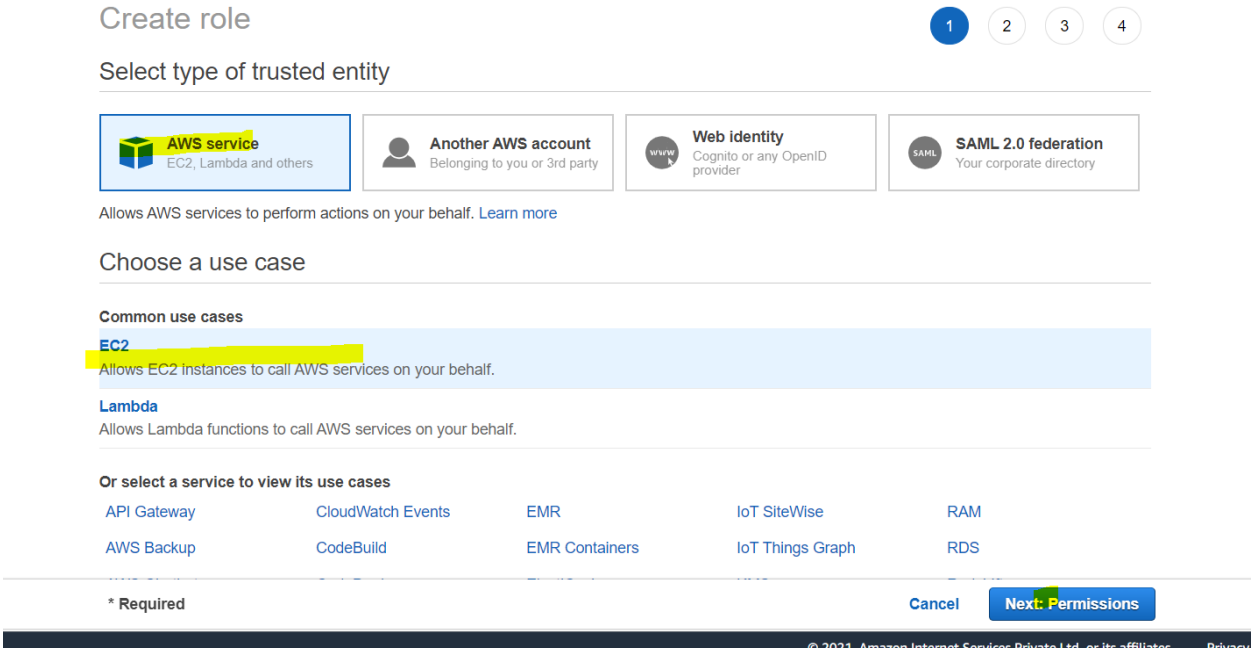
- is software that can be installed and configured on an EC2 instance, an on-premises server, or a virtual machine (VM)
- makes it possible for the Systems Manager to update, manage, and configure these resources
- must be installed on each instance to use with Systems Manager
- usually comes preinstalled with a lot of Amazon Machine Images (AMIs), while it must be installed manually on other AMIs, and on on-premises servers and virtual machines for the hybrid environment

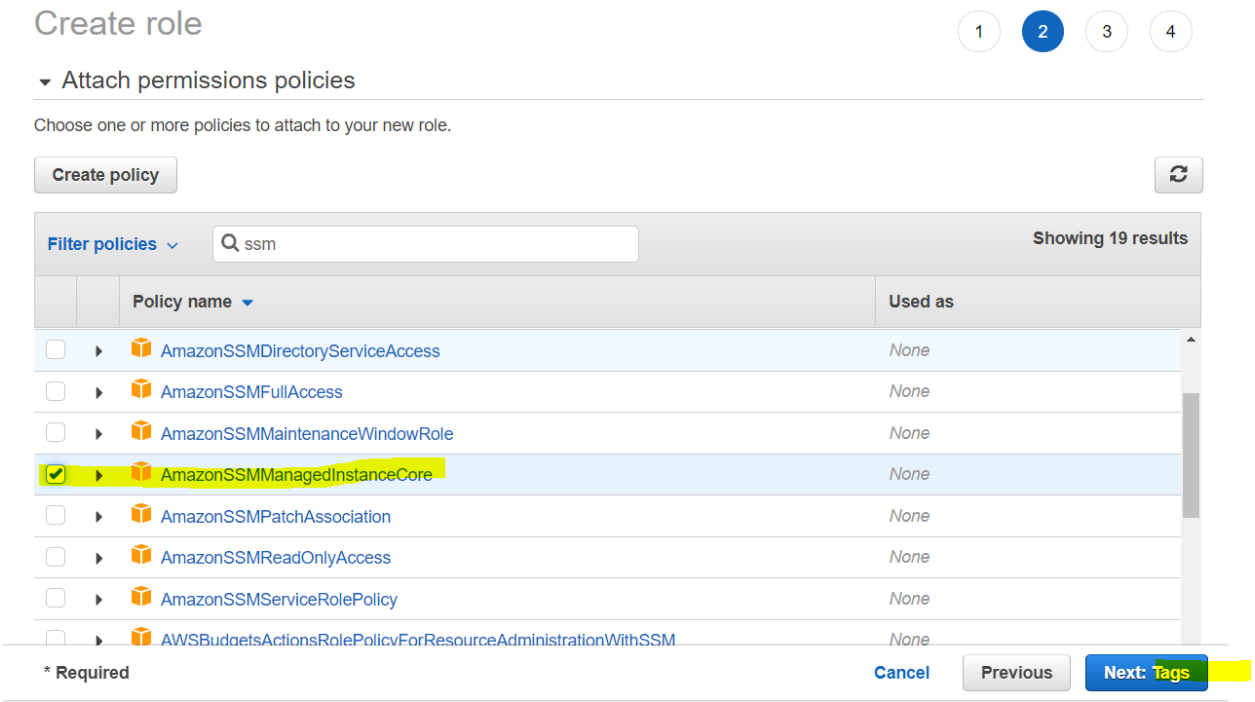
Create a EC2 Instance like below

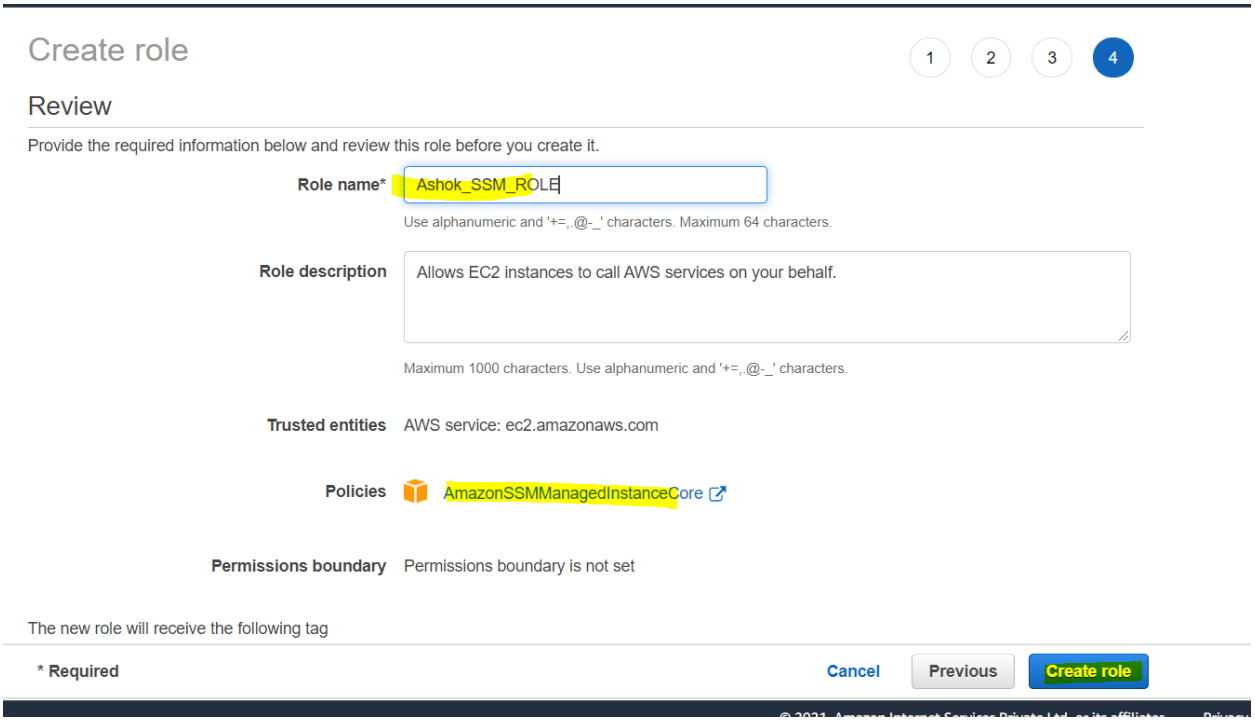


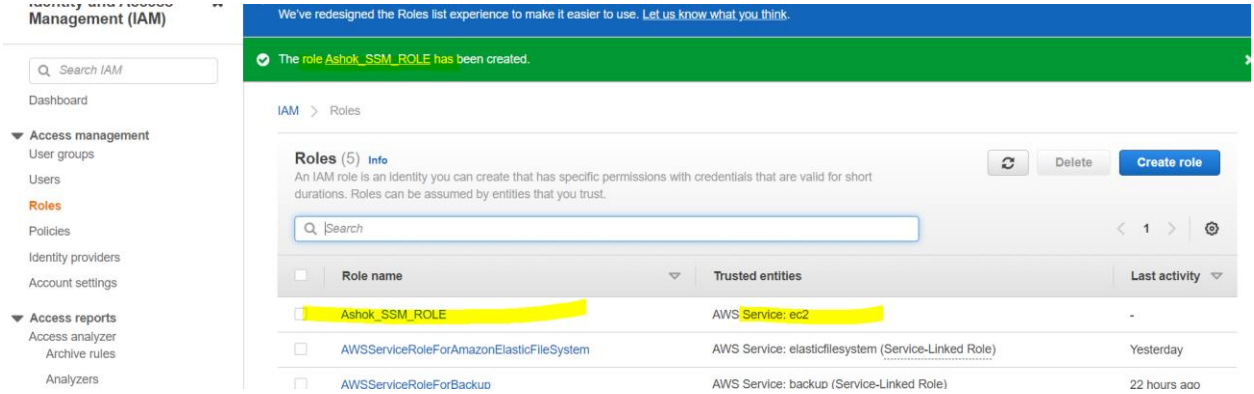
Create a Iam role and attached to the EC2 instance



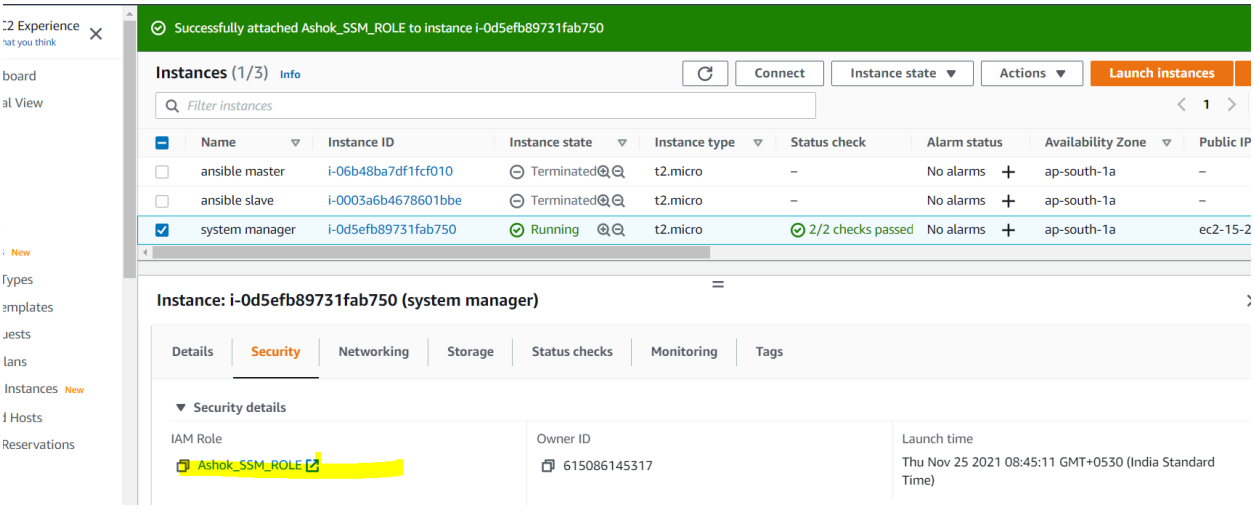



Create role
1
2
3
4
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
ssm
Showing 19 results
Policy name
Used as
AmazonSSMDirectoryServiceAccess
None
AmazonSSMFullAccess
None
AmazonSSMMaintenanceWindowRole
None
AmazonSSMManagedInstanceCore
None
AmazonSSMPatchAssociation
None
AmazonSSMReadOnlyAccess
None
AmazonSSMServiceRolePolicy
None
AWSBudgetsActionsRolePolicyForResourceAdministrationWithSSM
None
* Required
Cancel
Previous
Next: Tags

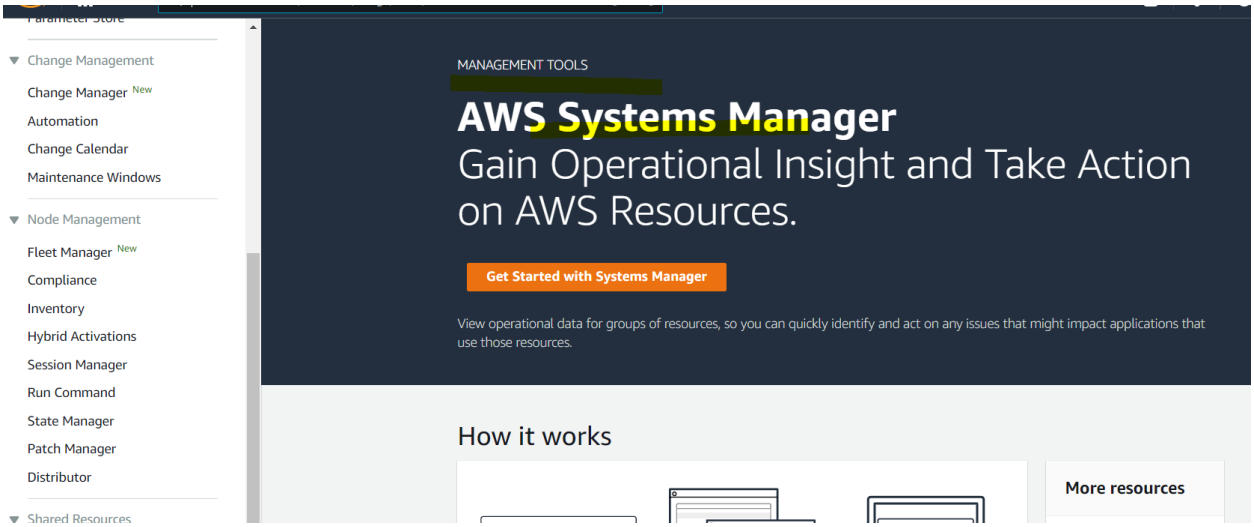

Create role
1
2
3
4
Review
Provide the required information below and review this role before you create it.
Role name*
Ashok_SSM_ROLE
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.
Role description
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Trusted entities
AWS service: ec2.amazonaws.com
Policies
AmazonSSMManagedInstanceCore
Permissions boundary
Permissions boundary is not set
The new role will receive the following tag
* Required
Cancel
Previous
Create role



Finally attached the Iam role in to ec2 instance like below



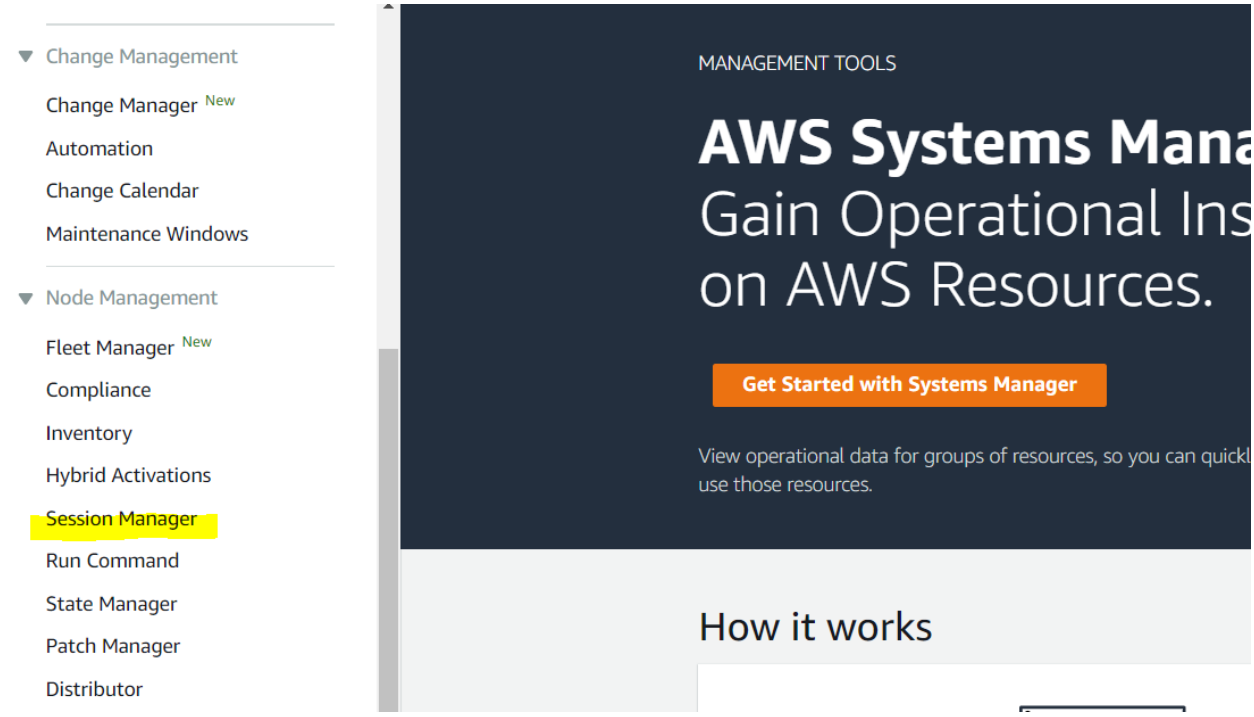
Now go to the systems manager on aws console



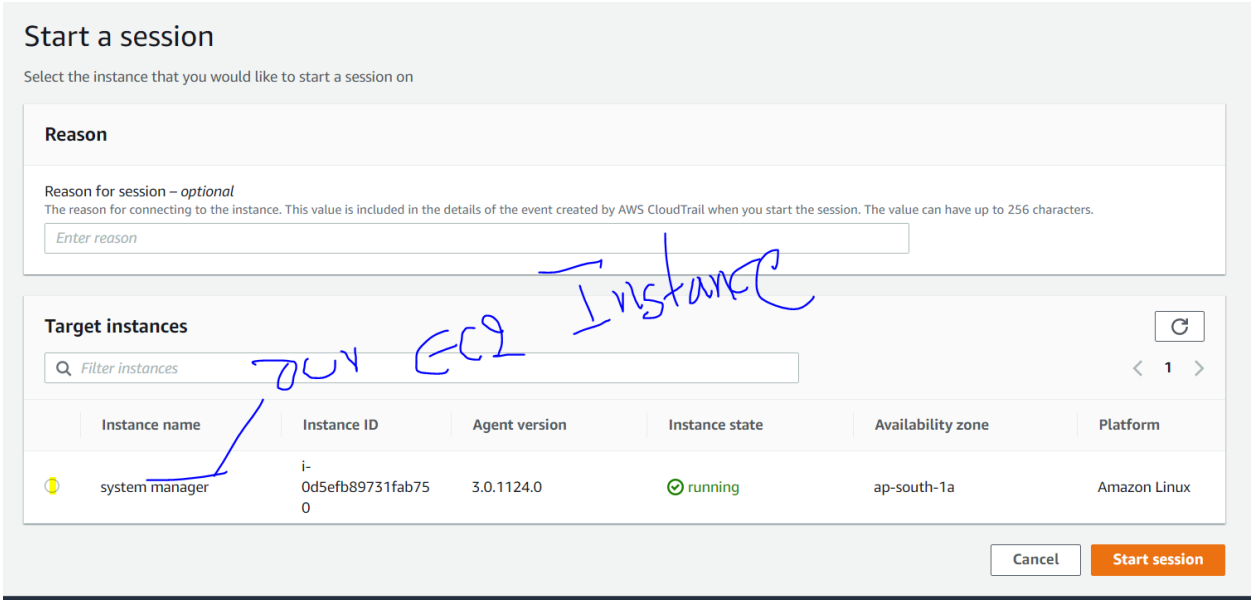
Now go to the Session manager

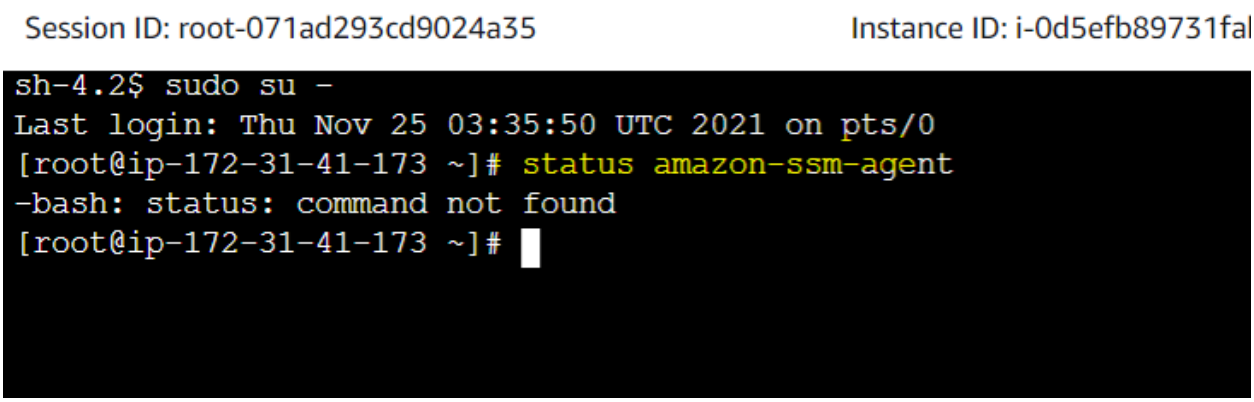
Session Manager

- helps manage EC2 instances through an interactive one-click browser-based shell or through the AWS CLI.
- provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.
- helps comply with corporate policies that require controlled access to instances, strict security practices, and fully auditable logs with instance access details, while still providing end users with simple one-click cross-platform access to the EC2 instances.


Change Management
Change Manager New
Automation
Change Calendar
Maintenance Windows
Node Management
Fleet Manager New
Compliance
Inventory
Hybrid Activations
Session Manager
Run Command
State Manager
Patch Manager
Distributor
MANAGEMENT TOOLS
AWS Systems Mana
Gain Operational Ins
on AWS Resources.
Get Started with Systems Manager
View operational data for groups of resources, so you can quickl
use those resources.
How it works


Management
Session Manager
Quickly and securely
access your Windows and
Linux instances
Session Manager is a managed service that provides you with one-click secure
access to your instances without the need to open inbound ports and manage
Start a session
Connect to your instances by starting a
secure and auditable session.
Start Session
Configure Preferences





We need to install ssm agent on ec2 instance

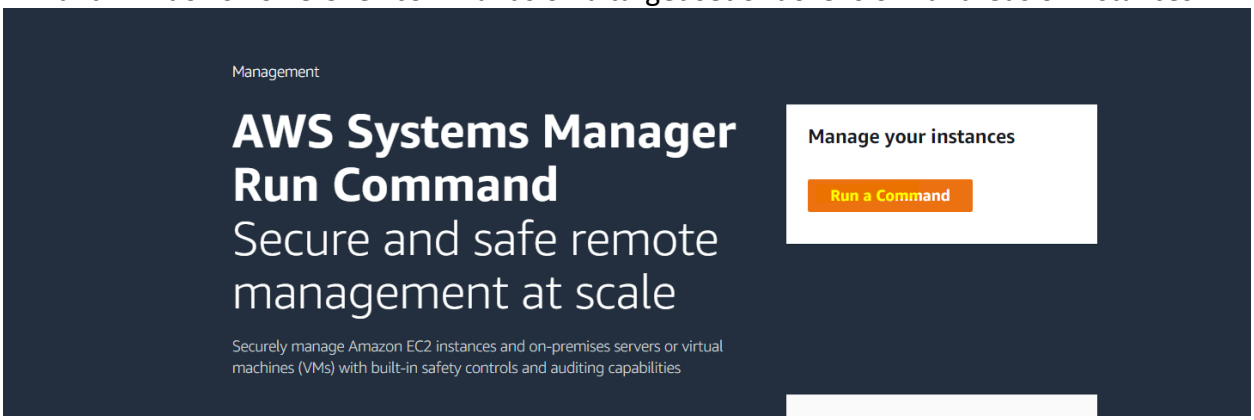
Ref:

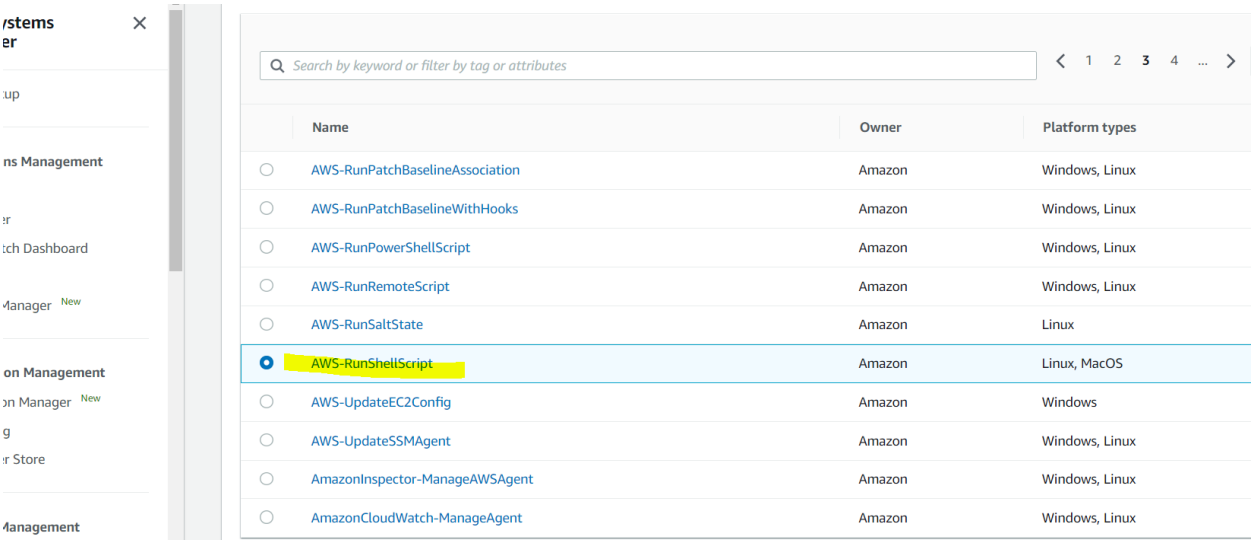
https://aws.amazon.com/premiumsupport/knowledge-center/install-ssm-agent-ec2-linux/

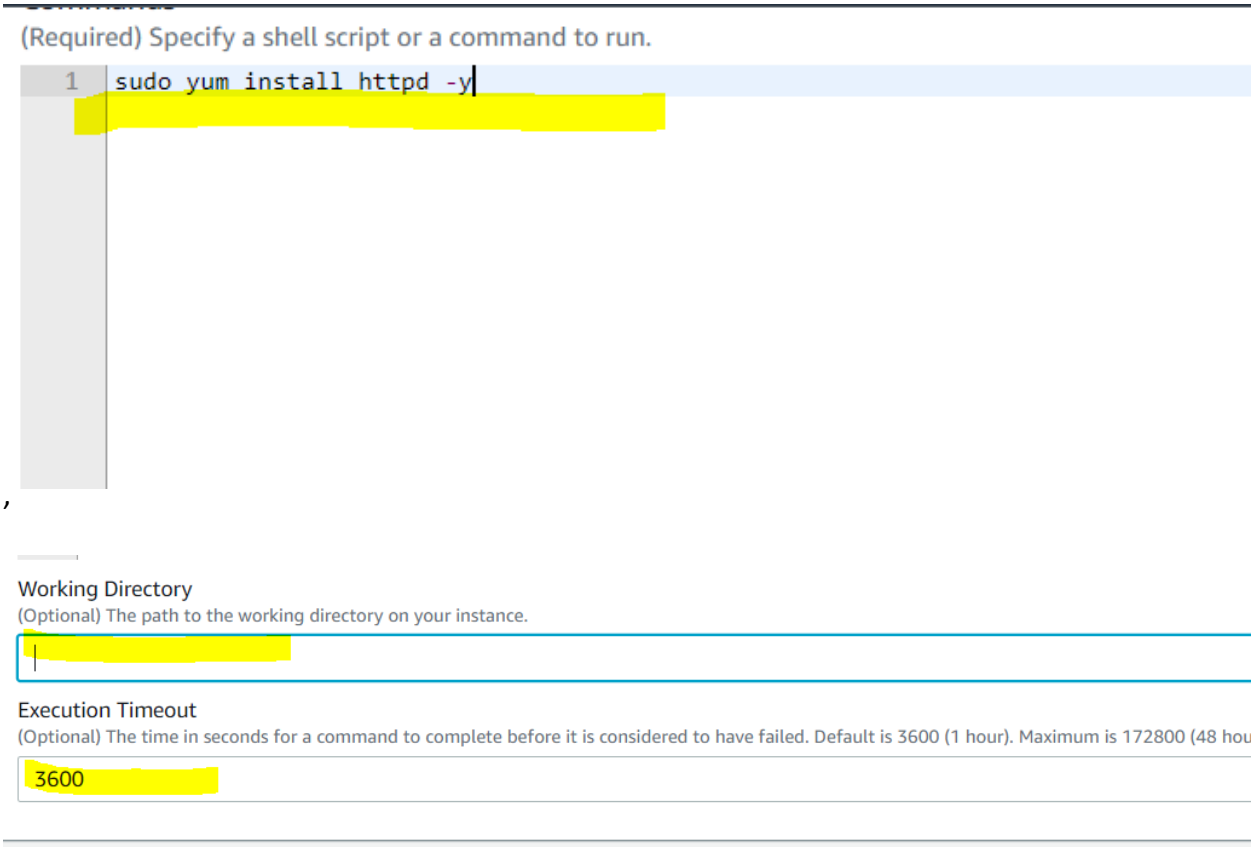
```
[root@ip-172-31-41-173 ~]# systemctl start amazon-ssm-agent
[root@ip-172-31-41-173 ~]# systemctl status amazon-ssm-agent
● amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-11-25 03:44:42 UTC; 1min 36s ago
 Main PID: 3526 (amazon-ssm-agen)
   CGroup: /system.slice/amazon-ssm-agent.service
           ├─3319 /usr/bin/ssm-session-worker root-01f970317359fe2cb i-0d5efb89731fab750
           ├─3338 sh
           ├─3375 /usr/bin/ssm-session-worker root-071ad293cd9024a35 i-0d5efb89731fab750
           ├─3388 sh
           ├─3526 /usr/bin/amazon-ssm-agent
           └─3581 /usr/bin/ssm-agent-worker

Nov 25 03:44:43 ip-172-31-41-173.ap-south-1.compute.internal amazon-ssm-agent[3526]: 2021-11-25 03:44:4
Nov 25 03:44:43 ip-172-31-41-173.ap-south-1.compute.internal amazon-ssm-agent[3526]: 2021-11-25 03:44:4
Nov 25 03:44:43 ip-172-31-41-173.ap-south-1.compute.internal amazon-ssm-agent[3526]: 2021-11-25 03:44:4
```

Systems Manager Run Command

- Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale.
- helps to remotely and securely manage the configuration of the managed instances at scale.
- helps perform on-demand changes like updating applications or running Linux shell scripts and Windows PowerShell commands on a target set of dozens or hundreds of instances.




Search by keyword or filter by tag or attributes
1 2 3 4 ...
Name
Owner
Platform types
AWS-RunPatchBaselineAssociation
Amazon
Windows, Linux
AWS-RunPatchBaselineWithHooks
Amazon
Windows, Linux
AWS-RunPowerShellScript
Amazon
Windows, Linux
AWS-RunRemoteScript
Amazon
Windows, Linux
AWS-RunSaltState
Amazon
Linux
AWS-RunShellScript
Amazon
Linux, MacOS
AWS-UpdateEC2Config
Amazon
Windows
AWS-UpdateSSMAgent
Amazon
Windows, Linux
AmazonInspector-ManageAWSAgent
Amazon
Windows, Linux
AmazonCloudWatch-ManageAgent
Amazon
Windows, Linux


(Required) Specify a shell script or a command to run.
1
sudo yum install httpd -y
Working Directory
(Optional) The path to the working directory on your instance.
Execution Timeout
(Optional) The time in seconds for a command to complete before it is considered to have failed. Default is 3600 (1 hour). Maximum is 172800 (48 hou
3600

Targets

Targets
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.

You haven't selected any instances.

Instances

Name	Instance ID	Instance state	Availability zone	Ping status	Last ping time
system manager	i-0d5efb89731fab750	running	ap-south-1a	Online	25/11/2021 at 09:35:52

Name	Instance ID	Instance state	Availability zone	Ping status
system manager	i-0d5efb89731fab750	running	ap-south-1a	Online

Other parameters

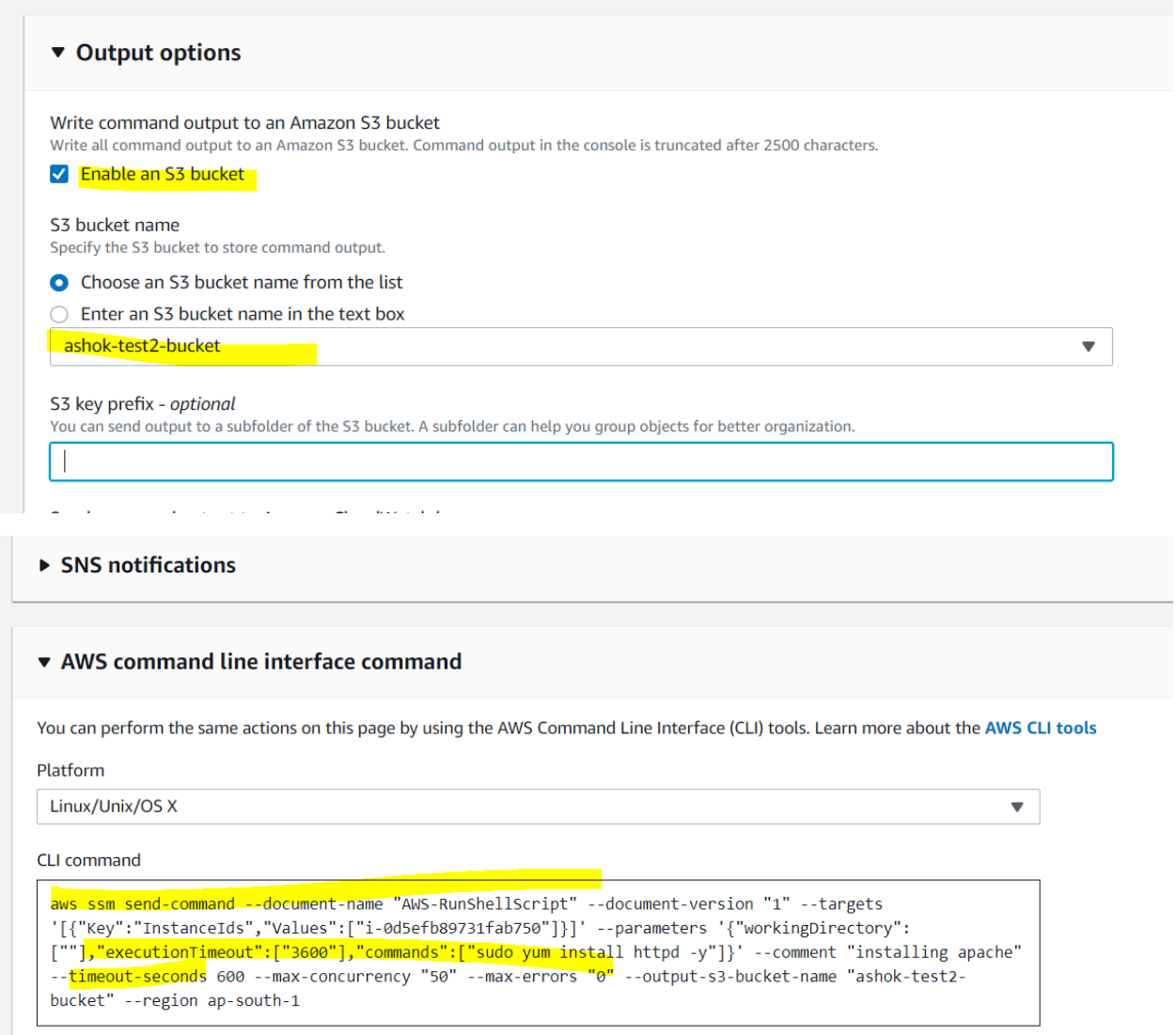
Comment
(Optional) Type a note about the command

installing apache

Timeout (seconds)
Specify the timeout for command in seconds

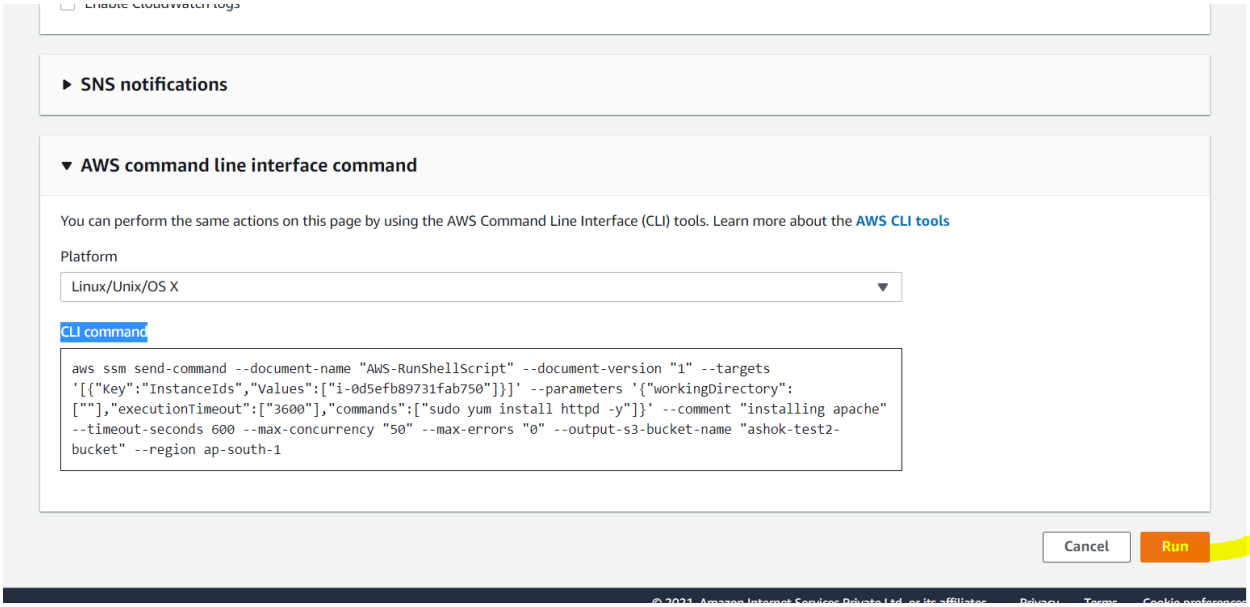
600

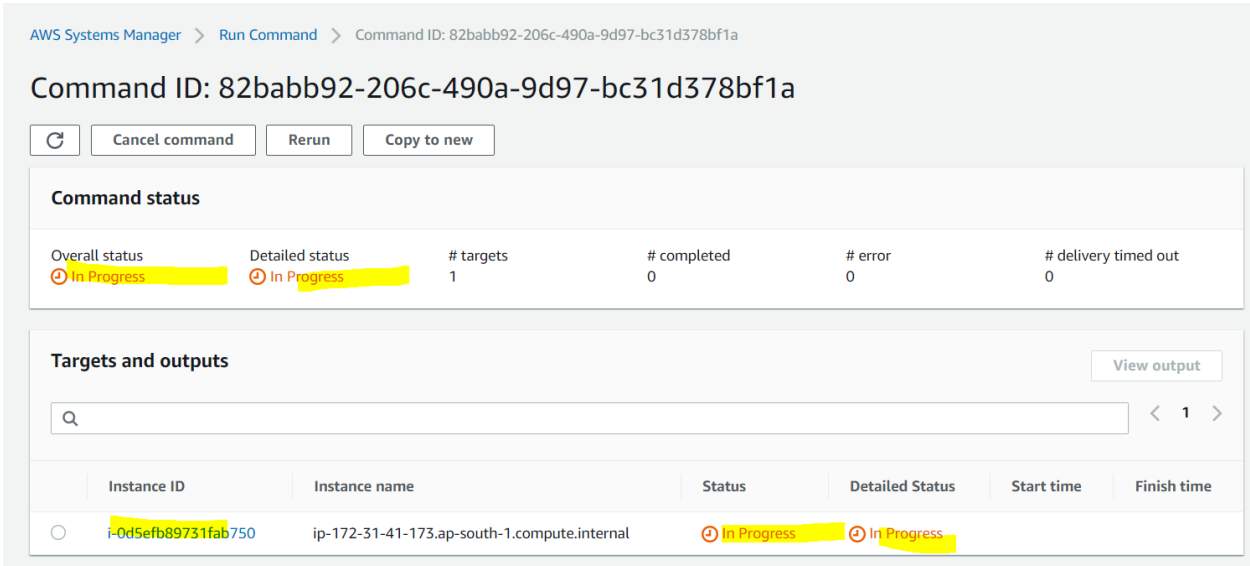
▸ Rate control

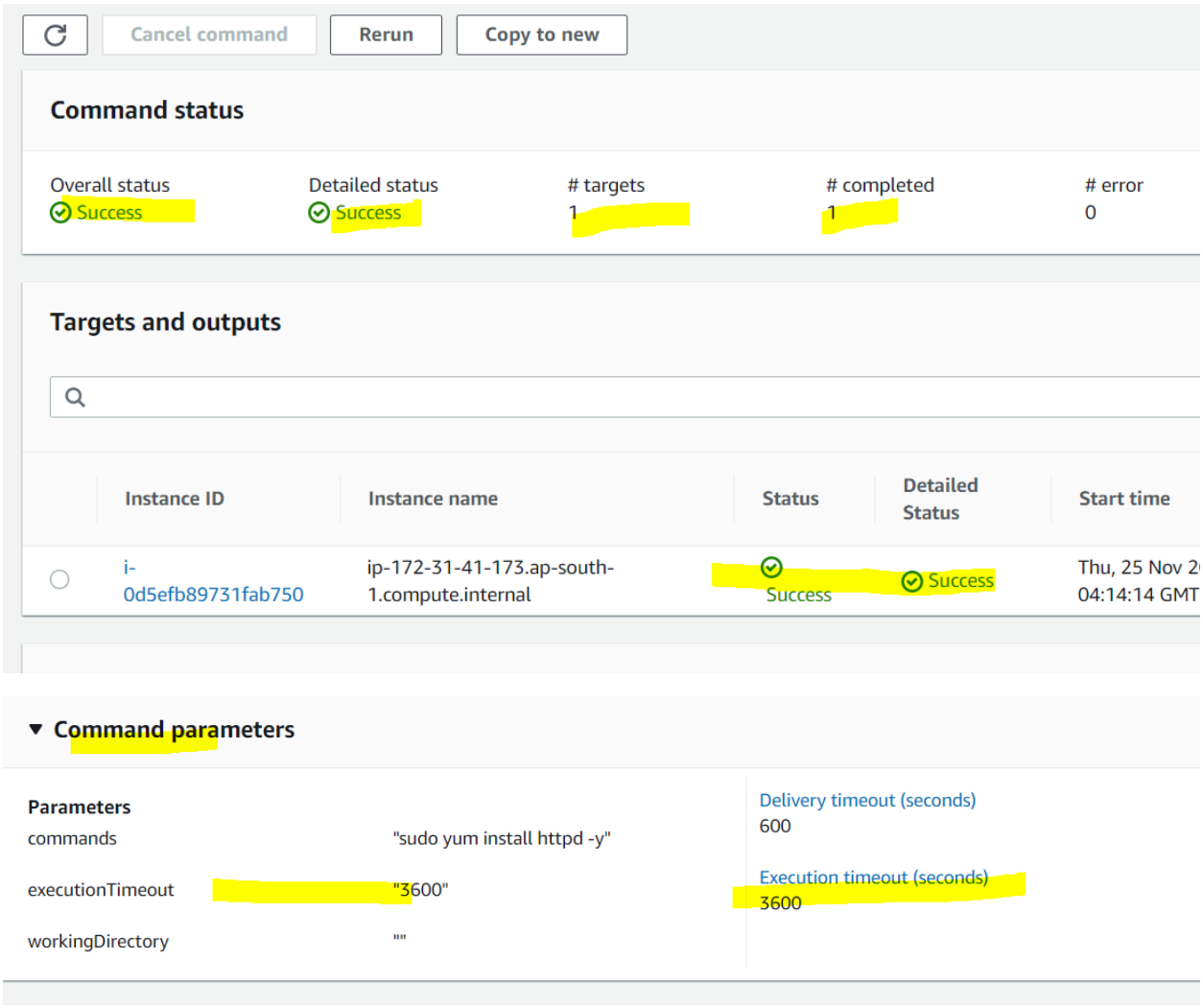


CLI command:

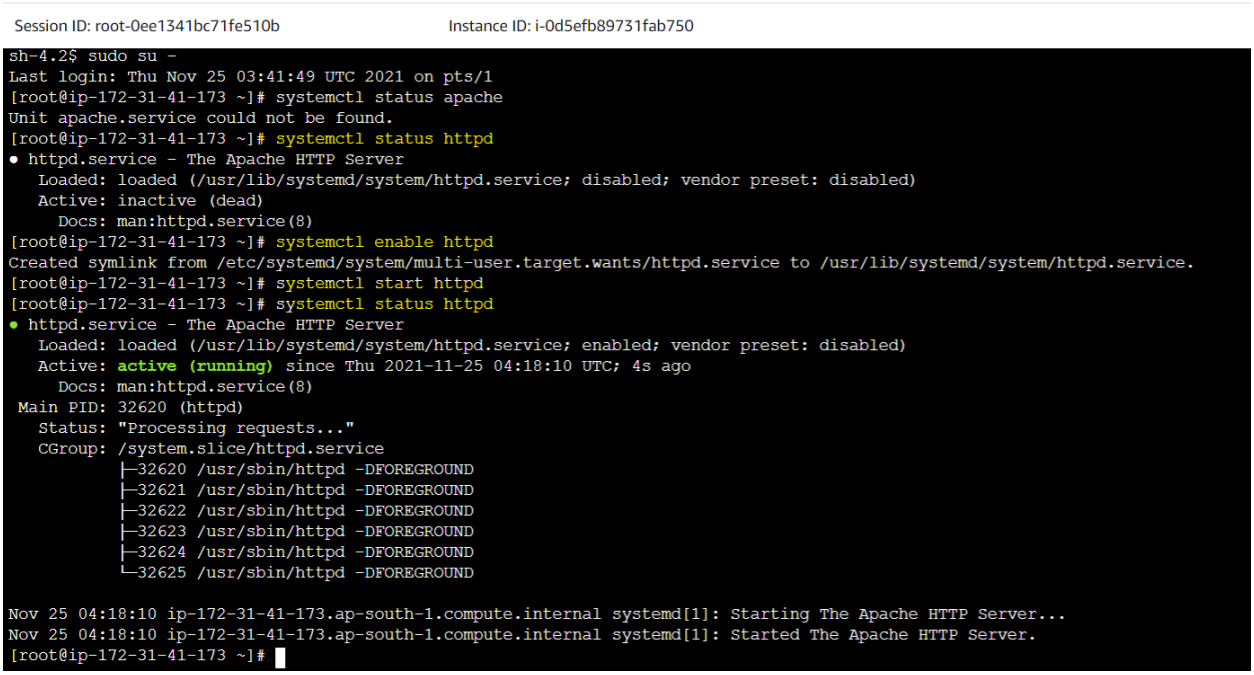
aws ssm send-command --document-name "AWS-RunShellScript" --document-version "1" --targets '[{"Key":"InstanceIds","Values":["i-0d5efb89731fab750"]}]' --parameters '{"workingDirectory":[""],"executionTimeout":["3600"],"commands":["sudo yum install httpd -y"]}' --comment "installing apache" --timeout-seconds 600 --max-concurrency "50" --max-errors "0" --output-s3-bucket-name "ashok-test2-bucket" --region ap-south-1


SNS notifications
AWS command line interface command
You can perform the same actions on this page by using the AWS Command Line Interface (CLI) tools. Learn more about the AWS CLI tools
Platform
Linux/Unix/OS X
CLI command
aws ssm send-command --document-name "AWS-RunShellScript" --document-version "1" --targets '[{"Key":"InstanceIds","Values":["i-0d5efb89731fab750"]}]' --parameters '{"workingDirectory":[""],"executionTimeout":["3600"],"commands":["sudo yum install httpd -y"]}' --comment "installing apache" --timeout-seconds 600 --max-concurrency "50" --max-errors "0" --output-s3-bucket-name "ashok-test2-bucket" --region ap-south-1
Cancel
Run


AWS Systems Manager > Run Command > Command ID: 82babb92-206c-490a-9d97-bc31d378bf1a
Command ID: 82babb92-206c-490a-9d97-bc31d378bf1a
Cancel command
Rerun
Copy to new
Command status
Overall status
In Progress
Detailed status
In Progress
targets
1
completed
0
error
0
delivery timed out
0
Targets and outputs
View output
1
Instance ID
Instance name
Status
Detailed Status
Start time
Finish time
i-0d5efb89731fab750
ip-172-31-41-173.ap-south-1.compute.internal
In Progress
In Progress


Cancel command
Rerun
Copy to new
Command status
Overall status
Success
Detailed status
Success
targets
1
completed
1
error
0
Targets and outputs
Instance ID
Instance name
Status
Detailed Status
Start time
i-0d5efb89731fab750
ip-172-31-41-173.ap-south-1.compute.internal
Success
Success
Thu, 25 Nov 2
04:14:14 GMT

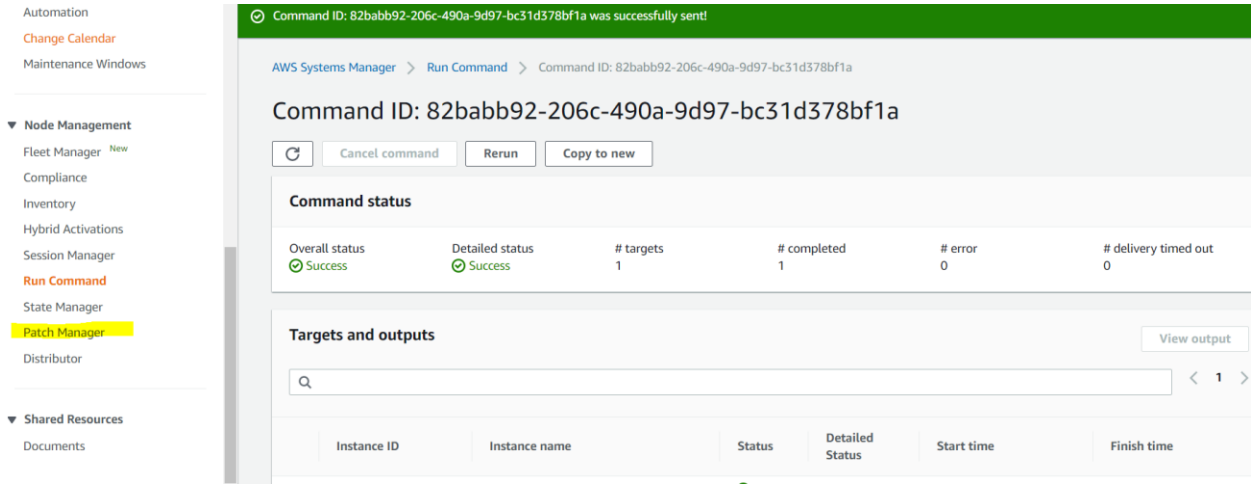
Command parameters
Parameters
commands
"sudo yum install httpd -y"
executionTimeout
"3600"
workingDirectory
""
Delivery timeout (seconds)
600
Execution timeout (seconds)
3600



Patch Manager

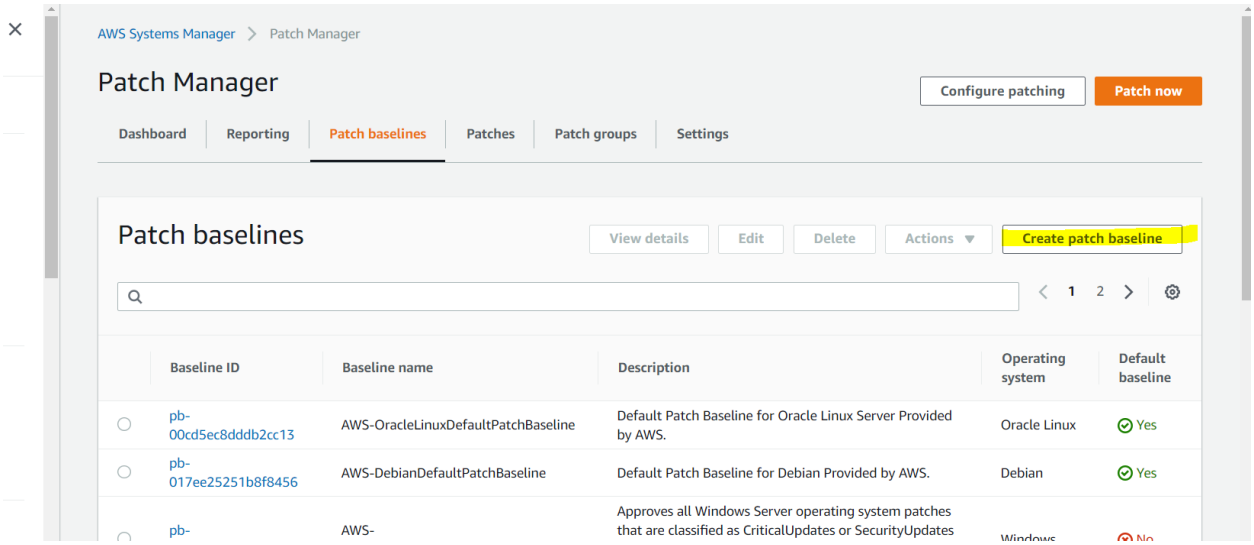
- helps automate the process of patching managed instances with both security-related and other types of updates.
- helps apply patches for both operating systems and applications. **(On Windows Server, application support is limited to updates for Microsoft applications.)**
- enables scanning of instances for missing patches and applies them individually or to a large group of instances by using EC2 instance tags.
- provides options to scan the instances and report compliance on a schedule, install available patches on a schedule, and patch or scan instances on-demand as needed.
  - Patch baselines
    - defines which patches should and shouldn't be installed
    - can include rules for auto-approving patches within days of their release, as well as a list of approved and rejected patches
    - helps install security patches on a regular basis by scheduling patching to run as a Systems Manager maintenance window task.
  - Patch group

    - helps associate a set of instances with a specific patch baseline
    - requires instances to be tagged with a tag key Patch Group


Automation
Change Calendar
Maintenance Windows
Node Management
Fleet Manager New
Compliance
Inventory
Hybrid Activations
Session Manager
Run Command
State Manager
Patch Manager
Distributor
Shared Resources
Documents
Command ID: 82babb92-206c-490a-9d97-bc31d378bf1a was successfully sent!
AWS Systems Manager > Run Command > Command ID: 82babb92-206c-490a-9d97-bc31d378bf1a
Command ID: 82babb92-206c-490a-9d97-bc31d378bf1a
Cancel command
Rerun
Copy to new
Command status
Overall status
Success
Detailed status
Success
targets
1
completed
1
error
0
delivery timed out
0
Targets and outputs
View output
Instance ID
Instance name
Status
Detailed Status
Start time
Finish time


Management tools
AWS Systems Manager Patch Manager
Automate patching with a native AWS solution
Centralized management for patching your fleet of Amazon EC2 Windows and Linux instances or your on-premises servers and virtual machines (VMs).
Patch your instances
Patch instances without a schedule.
Patch now
Create schedules to patch instances.
Configure patching
Not ready to configure patching? Learn more about patching options by viewing the predefined patch baselines.
View predefined patch baselines


Management tools
AWS Systems Manager Patch Manager
Automate patching with a native AWS solution
Centralized management for patching your fleet of Amazon EC2 Windows and Linux instances or your on-premises servers and virtual machines (VMs).
Patch your instances
Patch instances without a schedule.
Patch now
Create schedules to patch instances.
Configure patching
Not ready to configure patching? Learn more about patching options by viewing the predefined patch baselines.
View predefined patch baselines


AWS Systems Manager > Patch Manager
Patch Manager
Configure patching
Patch now
Dashboard
Reporting
Patch baselines
Patches
Patch groups
Settings
Patch baselines
View details
Edit
Delete
Actions
Create patch baseline
1
2
Baseline ID
Baseline name
Description
Operating system
Default baseline
pb-00cd5ec8dddb2cc13
AWS-OracleLinuxDefaultPatchBaseline
Default Patch Baseline for Oracle Linux Server Provided by AWS.
Oracle Linux
Yes
pb-017ee25251b8f8456
AWS-DebianDefaultPatchBaseline
Default Patch Baseline for Debian Provided by AWS.
Debian
Yes
pb-
AWS-
Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates
Windows
No

AWS Systems Manager > Patch Manager > Create patch baseline

Create patch baseline

Patch baseline details

Name

aws_ec2_patch_baseline

You can use letters, numbers, periods, dashes, and underscores in the name.

Description - *optional*

Operating system

Select the operating system you want to specify approval rules and patch exceptions for.

Amazon Linux

Default patch baseline

☐ Set this patch baseline as the default patch baseline for Amazon Linux instances.

Create auto-approval rules to specify that certain types of operating system patches are approved automatically.

Rule 1

Remove rule

Product

Select patches by product

Select products

AmazonLinux2012.03 ✕

Severity

Select patches by severity

Select severities

Critical ✕

Classification

Select patches by classification

Select classifications

Enhancement ✕

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

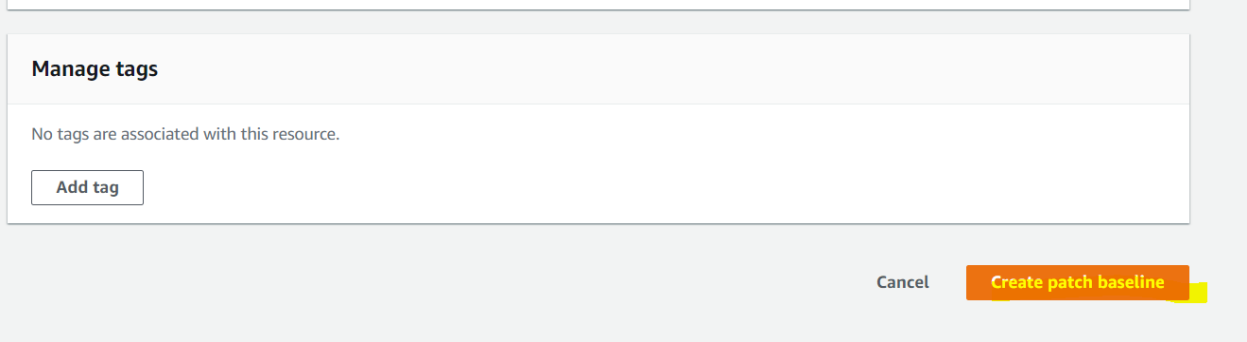
0 days

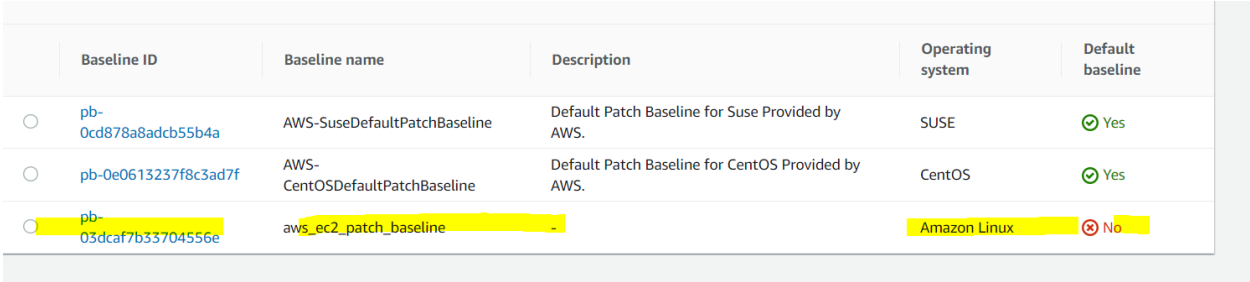
Compliance reporting - *optional*

Specify the severity level to report for patches that match this rule.

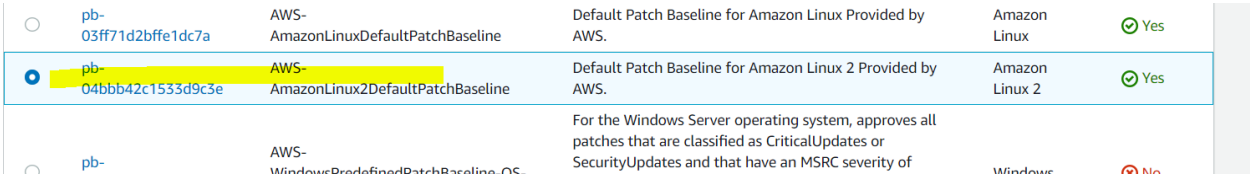
High

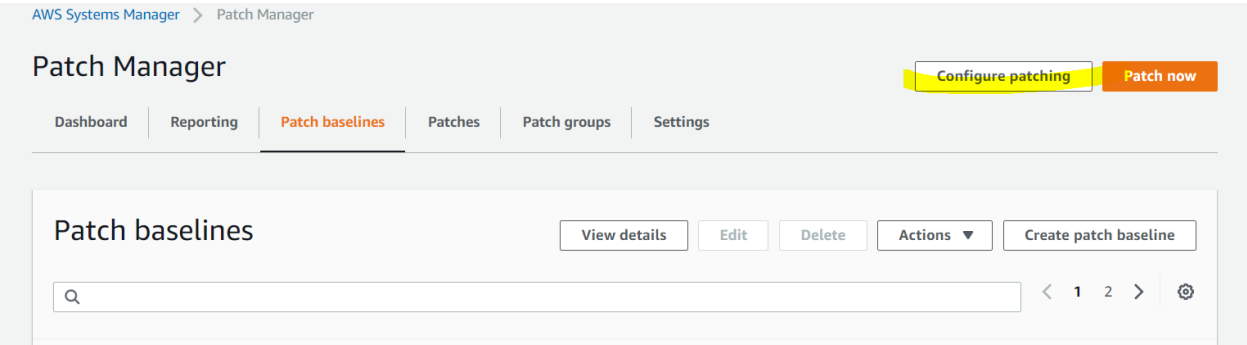
Include nonsecurity updates

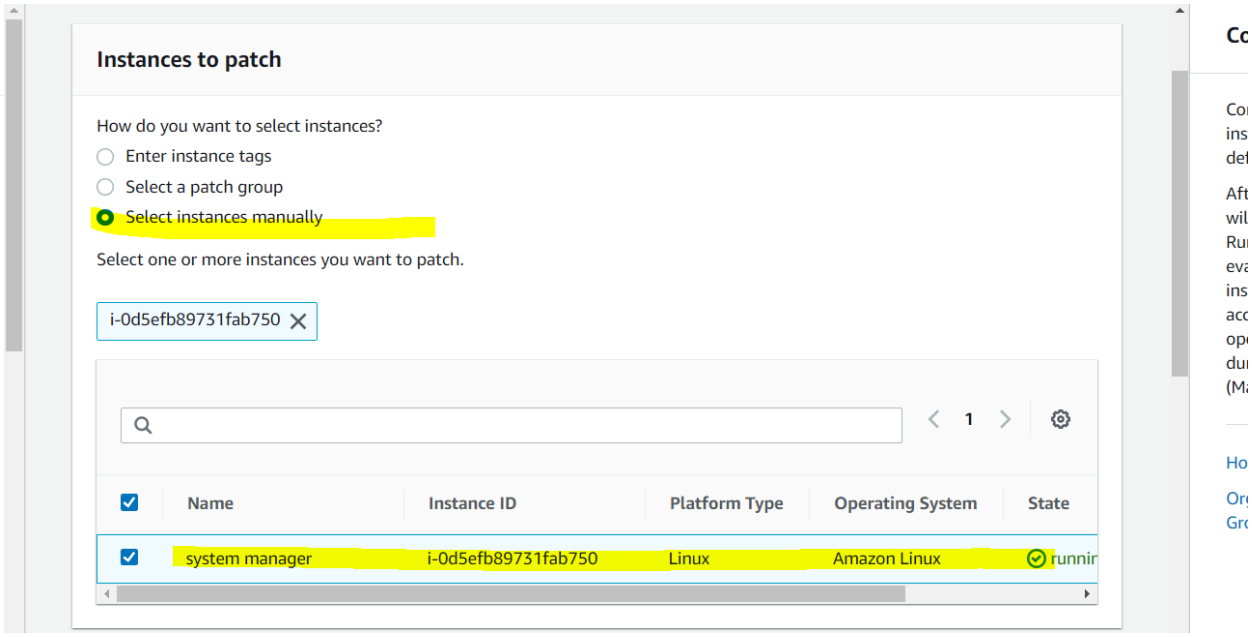

Manage tags
No tags are associated with this resource.
Add tag
Cancel
Create patch baseline

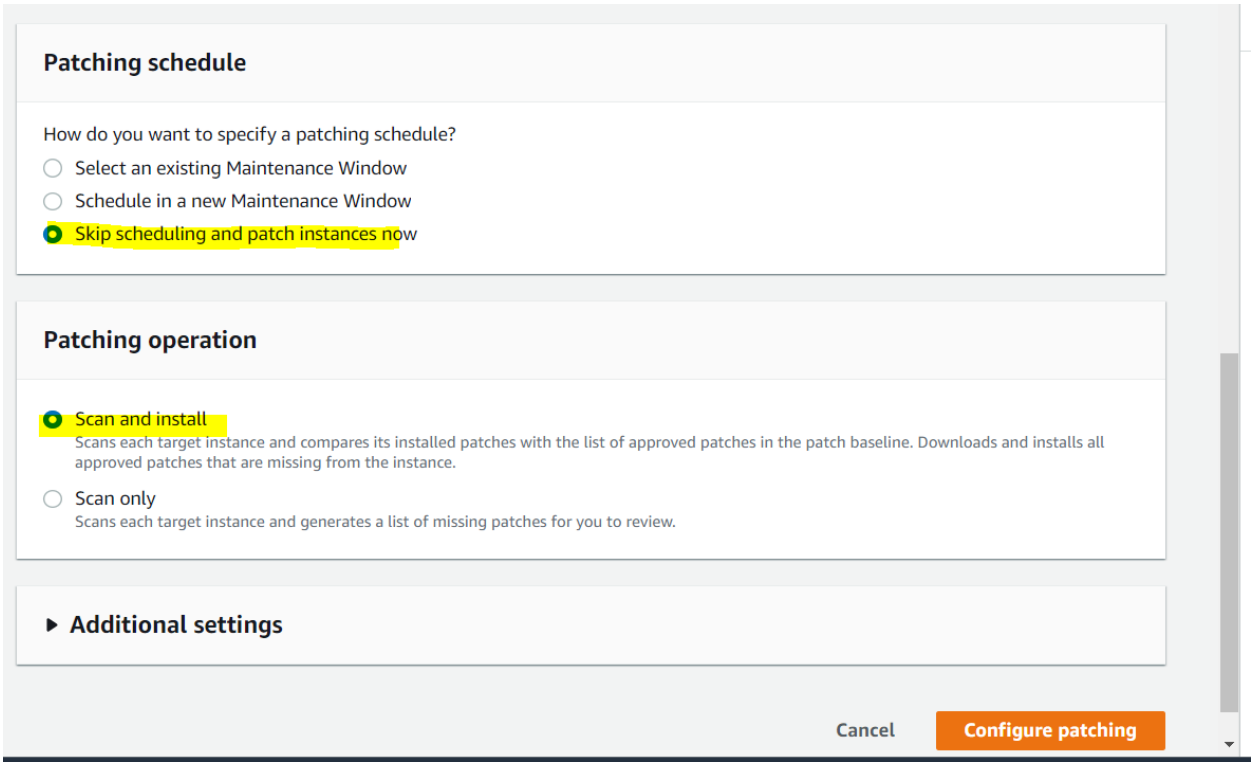

Baseline ID
Baseline name
Description
Operating system
Default baseline
pb-0cd878a8adcb55b4a
AWS-SuseDefaultPatchBaseline
Default Patch Baseline for Suse Provided by AWS.
SUSE
Yes
pb-0e0613237f8c3ad7f
AWS-CentOSDefaultPatchBaseline
Default Patch Baseline for CentOS Provided by AWS.
CentOS
Yes
pb-03dcaf7b33704556e
aws_ec2_patch_baseline
Amazon Linux
No

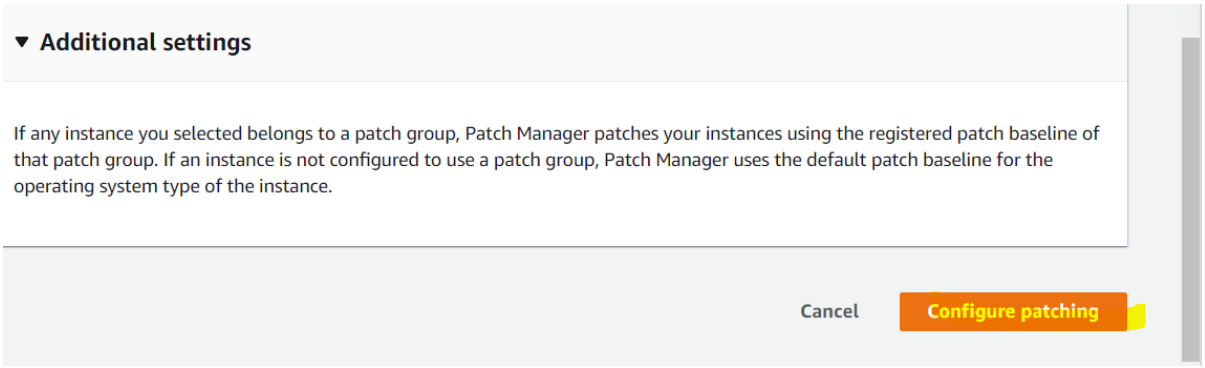
Applying

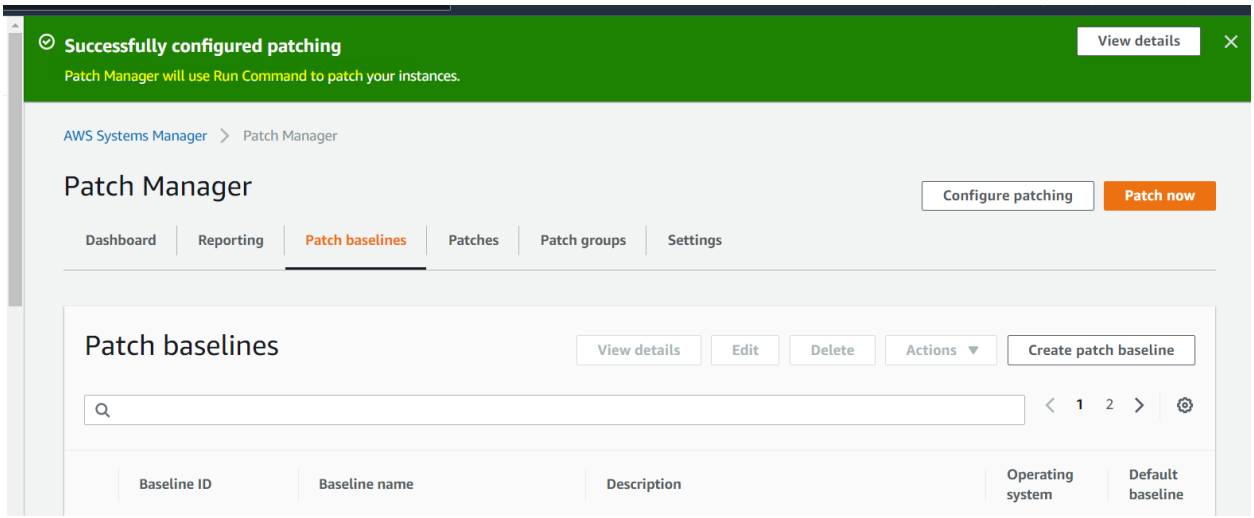

pb-03ff71d2bffe1dc7a
AWS-AmazonLinuxDefaultPatchBaseline
Default Patch Baseline for Amazon Linux Provided by AWS.
Amazon Linux
Yes
pb-04bbb42c1533d9c3e
AWS-AmazonLinux2DefaultPatchBaseline
Default Patch Baseline for Amazon Linux 2 Provided by AWS.
Amazon Linux 2
Yes
pb-
AWS-
For the Windows Server operating system, approves all patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of
Windows

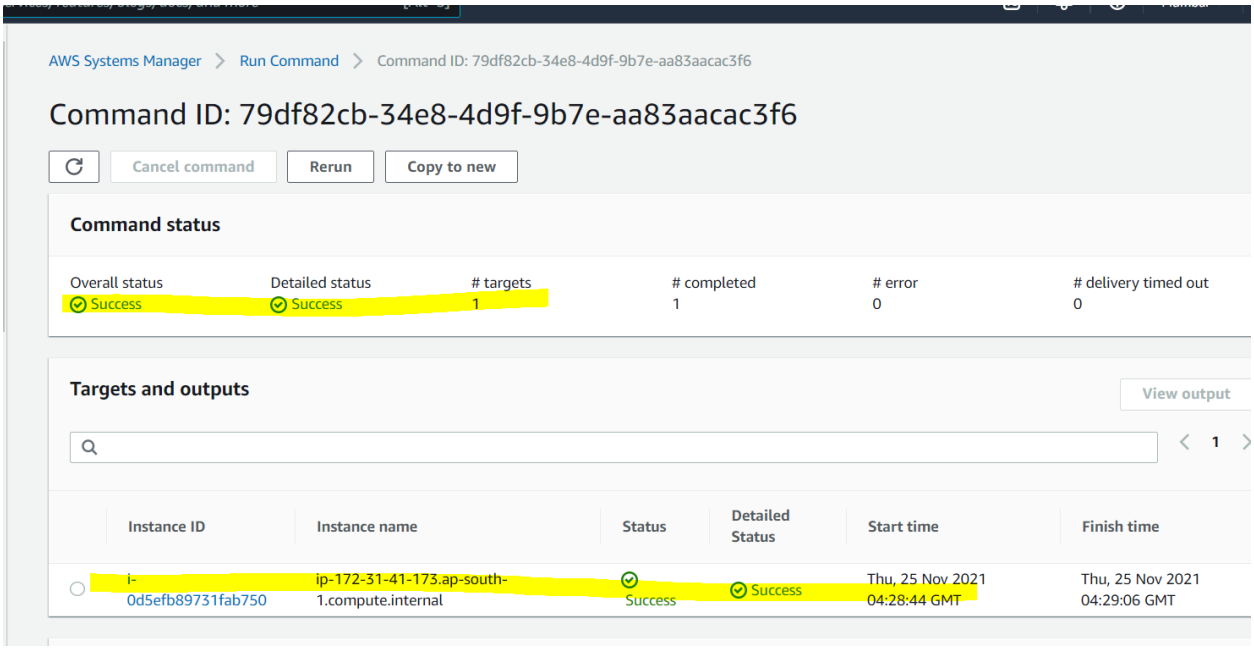

AWS Systems Manager
Patch Manager
Patch Manager
Configure patching
Patch now
Dashboard
Reporting
Patch baselines
Patches
Patch groups
Settings
Patch baselines
View details
Edit
Delete
Actions
Create patch baseline
1
2


Instances to patch
How do you want to select instances?
Enter instance tags
Select a patch group
Select instances manually
Select one or more instances you want to patch.
i-0d5efb89731fab750
1
Name
Instance ID
Platform Type
Operating System
State
system manager
i-0d5efb89731fab750
Linux
Amazon Linux


Patching schedule
How do you want to specify a patching schedule?
Select an existing Maintenance Window
Schedule in a new Maintenance Window
Skip scheduling and patch instances now
Patching operation
Scan and install
Scans each target instance and compares its installed patches with the list of approved patches in the patch baseline. Downloads and installs all approved patches that are missing from the instance.
Scan only
Scans each target instance and generates a list of missing patches for you to review.
Additional settings
Cancel
Configure patching


Additional settings
If any instance you selected belongs to a patch group, Patch Manager patches your instances using the registered patch baseline of that patch group. If an instance is not configured to use a patch group, Patch Manager uses the default patch baseline for the operating system type of the instance.
Cancel
Configure patching


Successfully configured patching
Patch Manager will use Run Command to patch your instances.
View details
AWS Systems Manager > Patch Manager
Patch Manager
Configure patching
Patch now
Dashboard
Reporting
Patch baselines
Patches
Patch groups
Settings
Patch baselines
View details
Edit
Delete
Actions
Create patch baseline
1
2
Baseline ID
Baseline name
Description
Operating system
Default baseline


AWS Systems Manager > Run Command > Command ID: 79df82cb-34e8-4d9f-9b7e-aa83aacac3f6
Command ID: 79df82cb-34e8-4d9f-9b7e-aa83aacac3f6
Cancel command
Rerun
Copy to new
Command status
Overall status
Success
Detailed status
Success
targets
1
completed
1
error
0
delivery timed out
0
Targets and outputs
View output
1
Instance ID
Instance name
Status
Detailed Status
Start time
Finish time
i-0d5efb89731fab750
ip-172-31-41-173.ap-south-1.compute.internal
Success
Success
Thu, 25 Nov 2021 04:28:44 GMT
Thu, 25 Nov 2021 04:29:06 GMT

Command description

Command ID
79df82cb-34e8-4d9f-9b7e-aa83aacac3f6

Command document
AWS-RunPatchBaseline

Document version
$DEFAULT

Command steps
3

Comment

Date requested
Thu, 25 Nov 2021 04:28:43 GMT

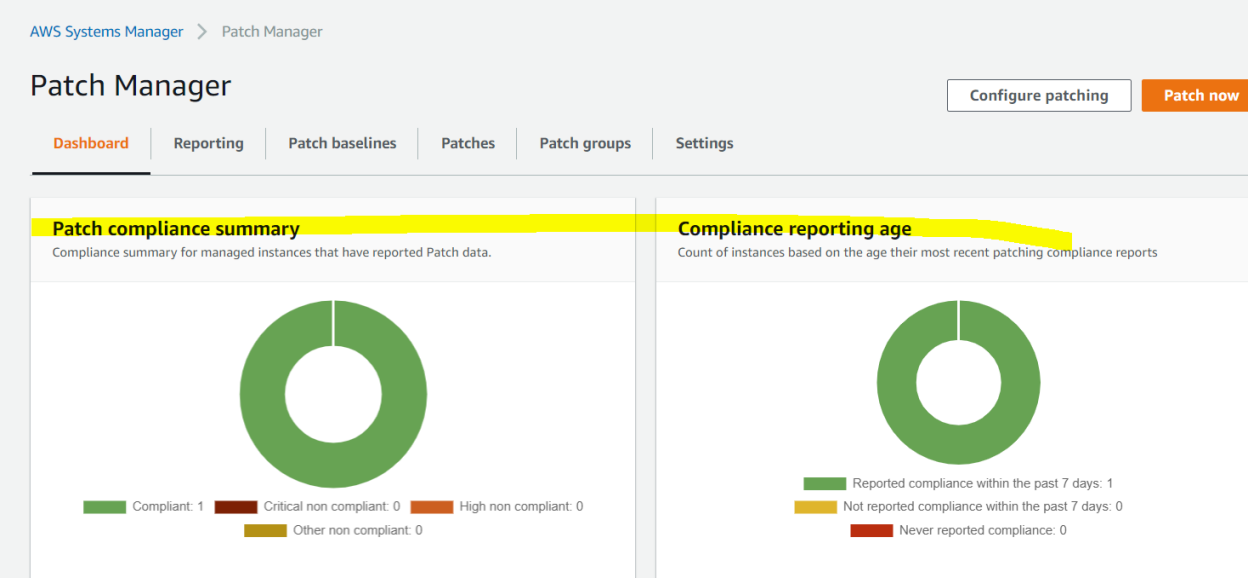
Command parameters

Parameters

Operation	"Install"
SnapshotId	""

Delivery timeout (seconds)
600

Execution timeout (seconds)
21600



Patch states

Count of instance for each of the most common causes of noncompliance.

Total managed instances	Instances with missing patches	Instances with failed patches	Instances pending reboot
1	0	0	0

Patch operations history

This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

Patch operations history

This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

Filter tasks

1

Patch operation	Started by	Document name	End time	Status	Targets
Install	Association	AWS-RunPatchBaseline	25 November 2021, 10:01 GMT+5:30	Success	InstanceIds: i-0d5efb89731fab750
Install	Other	AWS-RunPatchBaseline	25 November 2021, 09:58 GMT+5:30	Success	InstanceIds: i-0d5efb89731fab750

Recurring patching tasks

The following is a list of State Manager associations and maintenance windows that run any patching-related task. Choose a task name to view its details

1

Patching task name	Task type	Document name	Schedule
AWS-PatchNowAssociation	Association	AWS-RunPatchBaseline	-