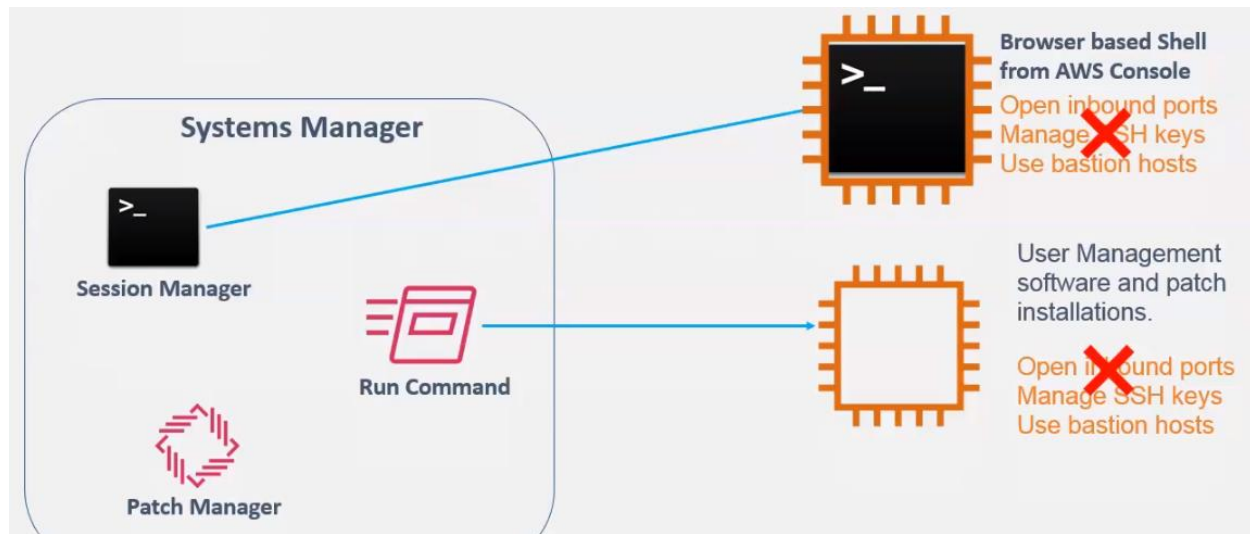


## AWS Systems Manager Overview

- 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

| Instances (2/3) Info                          |                |                     |                |               |                   |              |                   |             |
|---|----------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-------------|
| <input type="text" value="Filter instances"/> |                |                     |                |               |                   |              |                   |             |
| <input checked="" type="checkbox"/>           | Name           | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 |
| <input checked="" type="checkbox"/>           | ansible ma...  | i-06b48ba7df1fcf010 | Terminated     | t2.micro      | -                 | No alarms    | ap-south-1a       | -           |
| <input checked="" type="checkbox"/>           | ansible slave  | i-0003a6b4678601bbe | Terminated     | t2.micro      | -                 | No alarms    | ap-south-1a       | -           |
| <input type="checkbox"/>                      | system manager | i-0d5efb89731fab750 | Running        | t2.micro      | 2/2 checks passed | No alarms    | ap-south-1a       | ec2-15-201  |

## Create a lam role and attached to the EC2 instance

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

**Roles**

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analzers

Introducing the new IAM dashboard experience

We've redesigned the IAM dashboard experience to make it easier to use. [Let us know what you think.](#)

### IAM dashboard

Security recommendations 1

Add MFA for root user

Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups

2

Users

1

Roles

4

Policies

0

Identity providers

0

### Create role

1

2

3

4

#### Select type of trusted entity

**AWS service**  
EC2, Lambda and others

**Another AWS account**  
Belonging to you or 3rd party

**Web identity**  
Cognito or any OpenID provider

**SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

#### Choose a use case

**Common use cases**

**EC2**

Allows EC2 instances to call AWS services on your behalf.

**Lambda**

Allows Lambda functions to call AWS services on your behalf.

**Or select a service to view its use cases**

API Gateway

CloudWatch Events

EMR

IoT SiteWise

RAM

AWS Backup

CodeBuild

EMR Containers

IoT Things Graph

RDS

\* Required

Cancel

Next: **Permissions**

© 2021 Amazon Internet Services Private Ltd. or its affiliates. Privacy

## Create role

1

2

3

4

### ▼ Attach permissions policies









Choose one or more policies to attach to your new role.

[Create policy](#)

Filter policies ▾

Q ssm

Showing 19 results

|                                     |   | Policy name ▾   | Used as |
|-------------------------------------|---|---|---------|
| <input type="checkbox"/>            | ▶ |  AmazonSSMDirectoryServiceAccess                             | None    |
| <input type="checkbox"/>            | ▶ |  AmazonSSMFullAccess   | None    |
| <input type="checkbox"/>            | ▶ |  AmazonSSMMaintenanceWindowRole                              | None    |
| <input checked="" type="checkbox"/> | ▶ |  AmazonSSMManagedInstanceCore                                | None    |
| <input type="checkbox"/>            | ▶ |  AmazonSSMPatchAssociation                                   | None    |
| <input type="checkbox"/>            | ▶ |  AmazonSSMReadOnlyAccess                                     | None    |
| <input type="checkbox"/>            | ▶ |  AmazonSSMServiceRolePolicy                                  | None    |
| <input type="checkbox"/>            | ▶ |  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\*

Use alphanumeric and '+,=, @, \_' characters. Maximum 64 characters.

Role description

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](#)

Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers

We've redesigned the Roles list experience to make it easier to use. Let us know what you think.

The role **Ashok\_SSM\_ROLE** has been created.

IAM > Roles

**Roles (5)** Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

| <input type="checkbox"/>            | Role name                                | Trusted entities                                     | Last activity |
|-------------------------------------|--|--|---------------|
| <input checked="" type="checkbox"/> | Ashok_SSM_ROLE                           | AWS Service: ec2                                     | -             |
| <input type="checkbox"/>            | AWSServiceRoleForAmazonElasticFileSystem | AWS Service: elasticfilesystem (Service-Linked Role) | Yesterday     |
| <input type="checkbox"/>            | AWSServiceRoleForBackup                  | AWS Service: backup (Service-Linked Role)            | 22 hours ago  |

Finally attached the iam role in to ec2 instance like below

2 Experience

board

al View

New

Types

emplates

ests

lans

Instances **New**

Hosts

Reservations

Successfully attached Ashok\_SSM\_ROLE to instance i-0d5efb89731fab750

**Instances (1/3)** Info

Filter instances

| <input type="checkbox"/>            | Name           | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IP |
|-------------------------------------|----------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-----------|
| <input type="checkbox"/>            | ansible master | i-06b48ba7df1fc010  | Terminated     | t2.micro      | -                 | No alarms    | ap-south-1a       | -         |
| <input type="checkbox"/>            | ansible slave  | i-0003a6b4678601bbe | Terminated     | t2.micro      | -                 | No alarms    | ap-south-1a       | -         |
| <input checked="" type="checkbox"/> | system manager | i-0d5efb89731fab750 | Running        | t2.micro      | 2/2 checks passed | No alarms    | ap-south-1a       | ec2-15-2  |

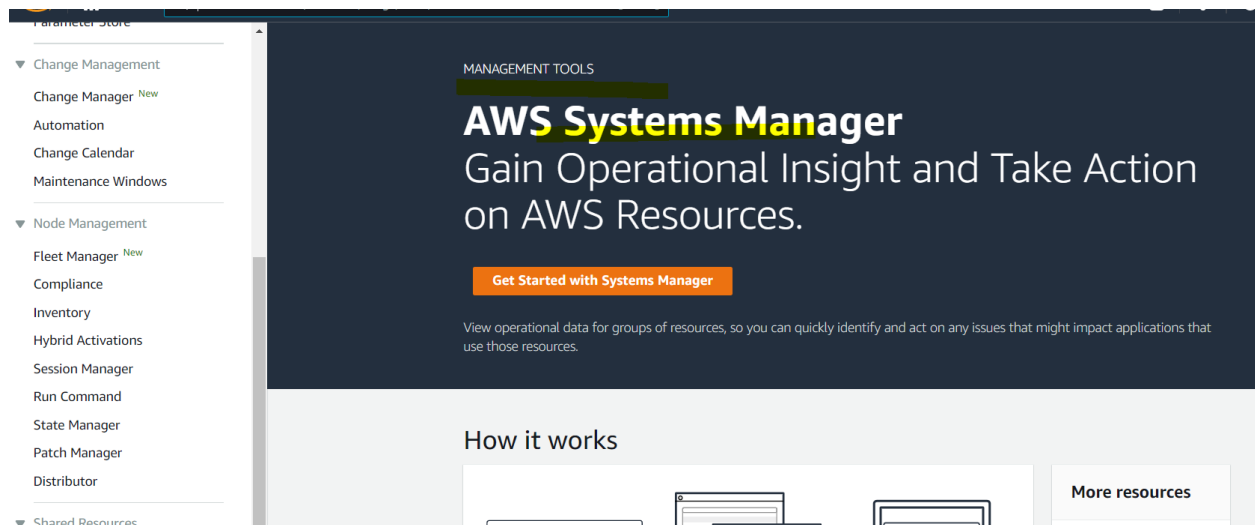
**Instance: i-0d5efb89731fab750 (system manager)**

Details **Security** Networking Storage Status checks Monitoring Tags

**Security details**

|                |              |   |
|----------------|--------------|---|
| IAM Role       | Owner ID     | Launch time   |
| Ashok_SSM_ROLE | 615086145317 | Thu Nov 25 2021 08:45:11 GMT+0530 (India Standard Time) |

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 <sup>New</sup>

Automation

Change Calendar

Maintenance Windows

▼ Node Management

Fleet Manager <sup>New</sup>

Compliance

Inventory

Hybrid Activations

**Session Manager**

Run Command

State Manager

Patch Manager

Distributor

MANAGEMENT TOOLS

# AWS Systems Manager

## Gain Operational Insights on AWS Resources.

**Get Started with Systems Manager**

View operational data for groups of resources, so you can quickly 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

## Start a session

Select the instance that you would like to start a session on



**Reason**

Reason for session – optional  
The reason for connecting to the instance. This value is included in the details of the event created by AWS CloudTrail when you start the session. The value can have up to 256 characters.

Enter reason

**Target instances**

Filter instances

| Instance name  | Instance ID         | Agent version | Instance state  | Availability zone | Platform     |
|--|---------------------|---------------|---|-------------------|--------------|
|  system manager | i-0d5efb89731fab750 | 3.0.1124.0    |  running | ap-south-1a       | Amazon Linux |

Cancel Start session

Session ID: root-01f970317359fe2cb Instance ID: i-0d5efb89731fab750 Terminate

sh-4.2\$ sudo su -  
[root@ip-172-31-41-173 ~]#

Session ID: root-071ad293cd9024a35

Instance ID: i-0d5efb89731fab750

```
sh-4.2$ sudo su -  
Last login: Thu Nov 25 03:35:50 UTC 2021 on pts/0  
[root@ip-172-31-41-173 ~]# status amazon-ssm-agent  
-bash: status: command not found  
[root@ip-172-31-41-173 ~]#
```

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 ~]# sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm  
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd  
amazon-ssm-agent.rpm  
Examining /var/tmp/yum-root-bHDSsr/amazon-ssm-agent.rpm: amazon-ssm-agent-3.1.501.0-1.x86_64  
Marking /var/tmp/yum-root-bHDSsr/amazon-ssm-agent.rpm as an update to amazon-ssm-agent-3.0.1124.0-1.amzn2.x86_64  
Resolving Dependencies
```

```

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

```

## 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.

Management

# AWS Systems Manager Run Command

Secure and safe remote  
management at scale

Securely manage Amazon EC2 instances and on-premises servers or virtual machines (VMs) with built-in safety controls and auditing capabilities

Manage your instances

Run a Command

Systems Manager

Setup

Instance Management

Tools

CloudWatch Dashboard

Systems Manager Manager New

Instance Management

Instance Manager New

Groups

Instance Store

Instance Management

Search by keyword or filter by tag or attributes

< 1 2 3 4 ... >

|                                  | Name                            | Owner  | Platform types |
|----------------------------------|---------------------------------|--------|----------------|
| <input type="radio"/>            | AWS-RunPatchBaselineAssociation | Amazon | Windows, Linux |
| <input type="radio"/>            | AWS-RunPatchBaselineWithHooks   | Amazon | Windows, Linux |
| <input type="radio"/>            | AWS-RunPowerShellScript         | Amazon | Windows, Linux |
| <input type="radio"/>            | AWS-RunRemoteScript             | Amazon | Windows, Linux |
| <input type="radio"/>            | AWS-RunSaltState                | Amazon | Linux          |
| <input checked="" type="radio"/> | AWS-RunShellScript              | Amazon | Linux, MacOS   |
| <input type="radio"/>            | AWS-UpdateEC2Config             | Amazon | Windows        |
| <input type="radio"/>            | AWS-UpdateSSMAgent              | Amazon | Windows, Linux |
| <input type="radio"/>            | AmazonInspector-ManageAWSAgent  | Amazon | Windows, Linux |
| <input type="radio"/>            | 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 hours).

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



1



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

## ▼ Output options

Write command output to an Amazon S3 bucket

Write all command output to an Amazon S3 bucket. Command output in the console is truncated after 2500 characters.

☒ Enable an S3 bucket

S3 bucket name

Specify the S3 bucket to store command output.

☒ Choose an S3 bucket name from the list

☐ Enter an S3 bucket name in the text box

ashok-test2-bucket ▼

S3 key prefix - optional

You can send output to a subfolder of the S3 bucket. A subfolder can help you group objects for better organization.

|

## ► 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
```

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
```

☐ Enable CloudWatch logs

#### ► 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

© 2021 Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookies preferences

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 | Detailed status | # targets | # completed | # error | # delivery timed out |
| In Progress    | In Progress     | 1         | 0           | 0       | 0                    |

### Targets and outputs

View output

Q

< 1 >

|                       | Instance ID         | Instance name                                | Status      | Detailed Status | Start time | Finish time |
|-----------------------|---------------------|--|-------------|-----------------|------------|-------------|
| <input type="radio"/> | 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 2023 04:14:14 GMT |

Command parameters

Parameters

commands

"sudo yum install httpd -y"

executionTimeout

"3600"

workingDirectory

""

Delivery timeout (seconds)

600

Execution timeout (seconds)

3600



```

sh-4.2$ sudo su -
Last login: Thu Nov 25 03:41:49 UTC 2021 on pts/1
[root@ip-172-31-41-173 ~]# systemctl status apache
Unit apache.service could not be found.
[root@ip-172-31-41-173 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[root@ip-172-31-41-173 ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-41-173 ~]# systemctl start httpd
[root@ip-172-31-41-173 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-11-25 04:18:10 UTC; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 32620 (httpd)
    Status: "Processing requests..."
    CGroup: /system.slice/httpd.service
            └─32620 /usr/sbin/httpd -DFOREGROUND
            └─32621 /usr/sbin/httpd -DFOREGROUND
            └─32622 /usr/sbin/httpd -DFOREGROUND
            └─32623 /usr/sbin/httpd -DFOREGROUND
            └─32624 /usr/sbin/httpd -DFOREGROUND
            └─32625 /usr/sbin/httpd -DFOREGROUND

Nov 25 04:18:10 ip-172-31-41-173.ap-south-1.compute.internal systemd[1]: Starting The Apache HTTP Server...
Nov 25 04:18:10 ip-172-31-41-173.ap-south-1.compute.internal systemd[1]: Started The Apache HTTP Server.
[root@ip-172-31-41-173 ~]#

```

## 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 | Detailed status | # targets | # completed | # error | # delivery timed out |
| Success        | Success         | 1         | 1           | 0       | 0                    |

Targets and outputs

View output

Q

< 1 >

| 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

Dashboard

Reporting

Patch baselines

Patches

Patch groups

Settings

Configure patching

Patch now

Patch baselines

View details

Edit

Delete

Actions ▾

Create patch baseline

Q

< 1 2 > ⚙

|                       | Baseline ID          | Baseline name                       | Description  | Operating system | Default baseline |
|-----------------------|----------------------|-------------------------------------|--|------------------|------------------|
| <input type="radio"/> | pb-00cd5ec8dddb2cc13 | AWS-OracleLinuxDefaultPatchBaseline | Default Patch Baseline for Oracle Linux Server Provided by AWS.  | Oracle Linux     | ✔ Yes            |
| <input type="radio"/> | pb-017ee25251b8f8456 | AWS-DebianDefaultPatchBaseline      | Default Patch Baseline for Debian Provided by AWS.   | Debian           | ✔ Yes            |
| <input type="radio"/> | pb-                  | AWS-                                | Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates | Windows          | ✖ No             |

## 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

Product

Select patches by product

Select products

AmazonLinux2012.03

Severity

Select patches by severity

Select severities

Critical

Remove rule

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 |
|-----------------------|----------------------|--------------------------------|--|------------------|------------------|
| <input type="radio"/> | pb-0cd878a8adcb55b4a | AWS-SuseDefaultPatchBaseline   | Default Patch Baseline for Suse Provided by AWS.   | SUSE             | ✔ Yes            |
| <input type="radio"/> | pb-0e0613237f8c3ad7f | AWS-CentOSDefaultPatchBaseline | Default Patch Baseline for CentOS Provided by AWS. | CentOS           | ✔ Yes            |
| <input type="radio"/> | pb-03dcdf7b33704556e | aws_ec2_patch_baseline         | -  | Amazon Linux     | ✘ No             |

## Applying

|                                  |                      |  |   |                |       |
|----------------------------------|----------------------|--|---|----------------|-------|
| <input type="radio"/>            | pb-03ff71d2bffe1dc7a | AWS-AmazonLinuxDefaultPatchBaseline    | Default Patch Baseline for Amazon Linux Provided by AWS.  | Amazon Linux   | ✔ Yes |
| <input checked="" type="radio"/> | pb-04bbb42c1533d9c3e | AWS-AmazonLinux2DefaultPatchBaseline   | Default Patch Baseline for Amazon Linux 2 Provided by AWS.  | Amazon Linux 2 | ✔ Yes |
| <input type="radio"/>            | pb-                  | AWS-WindowsProDefinedPatchBaseline_OS- | For the Windows Server operating system, approves all patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of | Windows        | ✘ No  |

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

Q

< 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

☒

system manager

☐

Instance ID

☐

i-0d5efb89731fab750

☐

Platform Type

☐

Linux

☐

Operating System

☐

Amazon Linux

☒

State

☐

running

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 | Detailed status | # targets | # completed | # error | # delivery timed out |
|----------------|-----------------|-----------|-------------|---------|----------------------|
| ☑ Success      | ☑ Success       | 1         | 1           | 0       | 0                    |

### Targets and outputs

View output



< 1 >

| Instance ID             | Instance name                                    | Status       | Detailed Status | Start time                       | Finish time                      |
|-------------------------|--|--------------|-----------------|----------------------------------|----------------------------------|
| i-<br>Od5efb89731fab750 | ip-172-31-41-173.ap-south-<br>1.compute.internal | ☑<br>Success | ☑ Success       | Thu, 25 Nov 2021<br>04:28:44 GMT | Thu, 25 Nov 2021<br>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

AWS Systems Manager > Patch Manager

## Patch Manager

Configure patching

Patch now

Dashboard Reporting Patch baselines Patches Patch groups Settings

### Patch compliance summary

Compliance summary for managed instances that have reported Patch data.



### Compliance reporting age

Count of instances based on the age their most recent patching compliance reports





### Patch states

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

Total managed instances

1

Instances with missing patches

0

Instances with failed patches

0

Instances pending reboot

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.

Q Filter tasks

< 1 >

| Patch operation         | Started by  | Document name        | End time                         | Status  | Targets                          |
|-------------------------|-------------|----------------------|----------------------------------|---------|----------------------------------|
| <a href="#">Install</a> | Association | AWS-RunPatchBaseline | 25 November 2021, 10:01 GMT+5:30 | Success | InstanceIds: i-0d5efb89731fab750 |
| <a href="#">Install</a> | 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 |
|---|-------------|----------------------|----------|
| <a href="#">AWS-PatchNowAssociation</a> | Association | AWS-RunPatchBaseline | -        |