

## Runbook for AWS Systems Manager Capabilities

### **Summary:**

This runbook aims to provide hands-on experience with key AWS Systems Manager (SSM) capabilities: **Session Manager, Hybrid Activation, Resource Groups, Patch Manager, Run Command, Automation, and State Manager.**

By the end of this runbook, you will understand how to configure and utilize some of these SSM features to manage EC2 instances efficiently.

---

### **1. Setting Up Instances:**

**Goal:** Create and configure three EC2 instances to meet the prerequisites for becoming managed instances. A managed instance requires the SSM agent and an IAM role with the necessary permissions.

**Note:** Instances do not need port 22 open since we will use Session Manager for access. Open port 80 for HTTP traffic as we will install Apache via Run Command.

#### **Prerequisite:**

- A VPC (use VPC and more to create a VPC with prefix SSM, and 2 public subnets)
- create IAM role with necessary permissions for SSM

#### **Step 1: Launch EC2 Instances**

##### **1. CentOS Instance:**

- **Name:** centos
- **AMI:** CentOS 7

- o **Instance Type:** t2.micro
- o **Network:** Public Subnet
- o **Security Group:** Allow port 80 (HTTP) No need for port 22
- o **IAM Role:** Attach a role with `AmazonSSMManagedInstanceCore` policy.
- o **User Data:** Installs the SSM agent to meet the managed instance prerequisite.

```
#!/bin/bash
yum install -y
https://s3.amazonaws.com/amazon-ssm-us-east-1/latest/linux_amd64/amazon-ssm-agent.rpm
systemctl start amazon-ssm-agent
systemctl enable amazon-ssm-agent
```

## 2. Amazon Linux 2 Instance:

- o **Name:** `amazonLinux`
- o **AMI:** Amazon Linux 2
- o **Instance Type:** t2.micro
- o **Network:** Public Subnet
- o **Security Group:** Allow port 80 (HTTP) No need for port 22
- o **IAM Role:** Attach a role with `AmazonSSMManagedInstanceCore` policy.
- o **Note:** The SSM agent is pre-installed on Amazon Linux 2 instances, so no user data is needed.

## 3. RHEL 8 Instance:

### 1. Create Hybrid Activation:

- o Navigate to the Systems Manager console.
- o Under "Hybrid Activations," create a new activation.

- o Provide necessary details and download the activation code and ID.

## Create activation

**Activation setting**

Create a new activation. After you complete the activation, you receive an activation code and ID. Use the code and ID to register SSM Agent on hybrid and on-premises servers or virtual machines. [Learn more](#)

**Activation description- *Optional***

for simulating on-prem

Maximum 256 characters.

**Instance limit**

Specify the total number of servers and VMs that you want to register with AWS. The maximum is 1000.

1

Maximum number is 1000.

**① To register more than 1,000 managed instances in the current AWS account and Region, change your account settings to use advanced instances. [Learn more](#)**

**Change setting**

**IAM role**

To enable communication between SSM Agent on your managed instances and AWS, specify an IAM role

**Create a system default command execution role that has the required permissions**

If you select this option, AWS creates a new role for you named AmazonEC2RunCommandRoleForManagedInstances. The role uses the existing public managed policy AmazonSSMManagedInstanceCore and grants AssumeRole permission to the SSM service.

**Select an existing custom IAM role that has the required permissions**

**Activation expiry date**

This date specifies when the activation expires. If you want to register additional managed instances after the expiry date, you must create a new activation. This expiry date has no impact on already registered and running instances.

2024-08-10

The expiry date must be in the future, and not more than 30 days into the future

**Default instance name- *Optional***

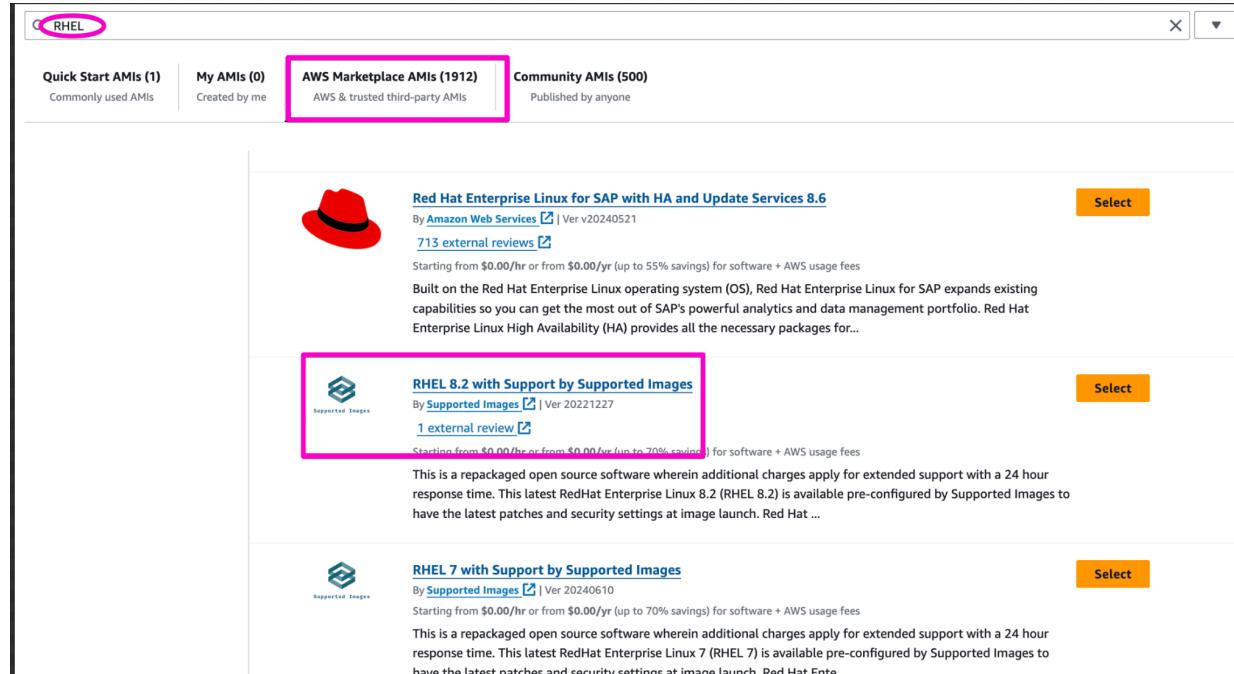
Specify a name to help you identify this managed instance when it is displayed in the console or when you call a List API.

- o click on create Activation

**NB** copy the provided activation credentials before closing window

## 2. Launch the RHEL Instance with User Data: (simulating Onprem machine)

- o **Name:** RHEL
- o **AMI:** RHEL 8.2 (click on **Browse more AMIs** and search in *AWS marketplace*)



The screenshot shows the AWS Marketplace search results for 'RHEL'. A search bar at the top contains 'RHEL'. Below it, there are three tabs: 'Quick Start AMIs (1)', 'My AMIs (0)', and 'AWS Marketplace AMIs (1912)'. The 'AWS Marketplace AMIs' tab is selected and highlighted with a pink box. The results list three items:

- Red Hat Enterprise Linux for SAP with HA and Update Services 8.6**: By Amazon Web Services | Ver v20240521. It has a red hat icon and 713 external reviews. A 'Select' button is to the right.
- RHEL 8.2 with Support by Supported Images**: By Supported Images | Ver 20221227. It has a supported images logo and 1 external review. A 'Select' button is to the right. This item is also highlighted with a pink box.
- RHEL 7 with Support by Supported Images**: By Supported Images | Ver 20240610. It has a supported images logo and no reviews shown. A 'Select' button is to the right.

The screenshot shows the AWS Marketplace search results for 'RHEL'. A pink arrow points to the search bar at the top left. Below it, there are three tabs: 'Quick Start AMIs (1)', 'My AMIs (0)', and 'AWS Marketplace AMIs (1920)'. The 'AWS Marketplace AMIs (1920)' tab is highlighted with a pink border. The results list includes three items:

- RHEL 8.2 with Support by Supported Images** (By Supported Images | Ver 20221227) - This item is highlighted with a pink border. It has a 'Select' button on the right.
- RHEL 7 with Support by Supported Images** (By Supported Images | Ver 20240610) - It has a 'Select' button on the right.
- Red Hat Enterprise Linux (RHEL) 8 with support by ProComputers** (By ProComputers | Ver RHEL-8.10-Minimal-20240522-10GIB) - It has a 'Select' button on the right.

- o select the 8.2 the instance AMI and click on **subscribe on instance launch**. This will take you back to the (familiar) instance launch console, **confirm changes** and proceed.

This screenshot shows the product page for 'RHEL 8.2 with Support by Supported Images'.

**Product Details:**

- Supported Images
- 0 AWS reviews | 1 external review
- Free Tier

**Overview** | Product details | Pricing | Usage | Support

**Description:** This product has charges associated with it for seller support. This latest RedHat Enterprise Linux 8.2 (RHEL 8.2) is available pre-configured by Supported Images to have the latest patches and security setting at image launch. Red Hat Enterprise Linux 8 is the latest server deployment in the Red Hat family of products.

|  |   |   |
|--|---|---|
| Typical total price<br><b>\$0.526/Hr</b><br>Total pricing per instance for services hosted on t2.xlarge in us-east-1.<br><a href="#">See additional pricing information.</a> | Latest version<br>20221227                        | Video<br><a href="#">Product Video</a>    |
|  | Delivery methods<br>Amazon Machine Image          | Categories<br>Operating Systems           |
|  | Operating systems<br>Red Hat Enterprise Linux 8.2 | Application Servers<br>Application Stacks |

**Note:** A subscription to this AMI is required before you can launch an instance. Check the pricing details in the pricing tab before continuing.

You can subscribe to this AMI now or we will automatically subscribe for you when you launch this instance. We recommend that you 'Subscribe now' if you are sure this is the AMI you want to use to launch as it will reduce wait time on launch. Choose 'Subscribe on instance launch' if you are still choosing an AMI and don't want to commit to a subscription yet. By subscribing to this AMI you agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#).

- Cancel** **Subscribe on instance launch** **Subscribe now**
- o **Instance Type:** t2.micro
  - o **Network:** Public Subnet
  - o **Security Group:** Allow port 80 (HTTP) No need for port 22

- o **User Data:** Installs the SSM agent and configures hybrid activation to simulate an on-premise environment. Ensure to pass your hybrid activation code, Id and region

```
#!/bin/bash
mkdir /tmp/ssm
sudo dnf install -y
https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux\_amd64/amazon-ssm-agent.rpm
sudo systemctl stop amazon-ssm-agent
sudo amazon-ssm-agent -register -code "qMTYsh/a2Jb+URVyMpxO" -id
"eb791b57-d612-443a-93b9-5d4702ab9152" -region "us-east-1"
sudo systemctl start amazon-ssm-agent
sudo systemctl enable amazon-ssm-agent
```

### Step 3: Confirm Instances in Fleet Manager

#### 1. Check Managed Instances:

- o Navigate to Systems Manager > Fleet Manager.
- o Ensure all three instances appear as managed instances.

### 2. Session Manager:

**Goal:** Use Session Manager to securely access and manage instances without needing SSH or bastion hosts.

#### 1. Access Instances via Session Manager:

- o Navigate to Systems Manager > Session Manager.
- o Start a new session and select an instance (CentOS, Amazon Linux 2, RHEL 8).

O

The screenshot shows the AWS Session Manager interface. On the left, a sidebar lists various management categories: Operations Management, Application Management, Change Management, Node Management (with sub-options like Fleet Manager, Compliance, Inventory, Hybrid Activations, and Session Manager), and a Run Command option. The 'Session Manager' option is highlighted with a pink border.

The main content area has a dark header with the title 'Session Manager' and the subtitle 'Quickly and securely access your Windows and Linux instances'. Below this, a paragraph explains the service's purpose: '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 bastion hosts. You have centralized access control over who can access your instances and full auditing capabilities to ensure compliance with corporate policies.'

A large central box is titled 'How it works' and contains four numbered steps:

- Configure your instances to use Session Manager
- Assign user IAM policies to control instance access
- Specify account options for session logs
- Start a session on your instances by launching bash or

On the right, there are two sections: 'Start a session' (with a 'Start Session' button) and 'Getting started' (with links to 'What is Session Manager?', 'Set up Session Manager', 'Set up session logging', 'Set up session notifications', and 'Create and manage sessions').

The bottom part of the screenshot shows the 'Specify target' step of the session creation wizard. It includes a 'Reason' section with a text input field for 'Enter reason' and a note that the value can have up to 256 characters. The 'Target instances' section displays a table of three instances:

| Instance n...                                   | Instance ID  | Agent ver... | Instance state       | Availabilit... | Platform     |
|---|--------------|--------------|----------------------|----------------|--------------|
| <input checked="" type="checkbox"/> amazonLi... | i-0f9bc0a... | 3.3.380.0    | <span>running</span> | us-east-1b     | Amazon Linux |
| <input type="radio"/> mi-05fc84...              |              |              |                      |                |              |
| <input type="radio"/> centos                    | i-013458e... | 3.3.551.0    | <span>running</span> | us-east-1b     | CentOS Linux |

At the bottom right of this section are 'Start session', 'Cancel', and 'Next' buttons.

- o this opens the terminal to the selected instance. Demonstrate basic command execution on each instance.

```
sh-4.2$  
sh-4.2$  
sh-4.2$ cd  
sh-4.2$  
sh-4.2$  
sh-4.2$ pwd  
/home/ssm-user  
sh-4.2$ ls  
sh-4.2$  
sh-4.2$  
sh-4.2$ mkdir -p modelbatch/ssm-demo  
sh-4.2$  
sh-4.2$ ls  
modelbatch  
sh-4.2$  
sh-4.2$ cd modelbatch/ssm-demo/  
sh-4.2$  
sh-4.2$ pwd  
/home/ssm-user/modelbatch/ssm-demo  
sh-4.2$
```

### 3. Resource Groups:

**Goal:** Use resource groups to organize and manage AWS resources more effectively. Resource groups allow you to group resources by specific criteria, such as tags, and manage them as a single entity.

#### 1. Create a Resource Group:

- o **Tag Instances:**
  - Tag each instance with Environment=Test.
- o **Navigate to Resource Groups:**
  - Go to the AWS Management Console and select "Resource Groups."
- o **Create a New Group:**
  - Click on "Create a resource group."
  - Choose the "Tag-based group" option.
  - Define the tag (e.g., Environment=Test) to include the instances.
  - Name the group (e.g **SSMResourceGroup**) and review the resource list to ensure all instances are included.
  - **Create the resource group.**

## Create query-based group

### Group type

Select a group type to define a group based on resource types and tags, or create a group based on your existing CloudFormation stack.

 Tag based

Group resources by specifying tags that are shared by the resources.

 CloudFormation

Create a resource group

### Grouping criteria

Define a group based on resource types and tags.

#### Resource types

Select resource types

AWS::EC2::Instance X

#### Tags

Tag key

Optional tag value

Environment: Test X

### Group resources (3)

Filter resources

| Identifier          | ▼ | Tag: Name   | ▼ | Service | ▼ | Type     | ▼ | Region    | ▼ | Tag: Envir | ▼ | Tags |
|---------------------|---|-------------|---|---------|---|----------|---|-----------|---|------------|---|------|
| i-013458eab769b0f91 |   | centos      |   | EC2     |   | Instance |   | us-east-1 |   | Test       |   | 4    |
| i-08d5ad4c78608373e |   | rhel8.2     |   | EC2     |   | Instance |   | us-east-1 |   | Test       |   | 4    |
| i-0f9bc0a2d74e4ff4a |   | amazonLinux |   | EC2     |   | Instance |   | us-east-1 |   | Test       |   | 4    |

### Group details

**Create query-based group**

**Group type**  
Select a group type to define a group based on resource types and tags, or create a group based on your existing CloudFormation stack.

Tag based  
Group resources by specifying tags that are shared by the resources.

Cloud Create

**Grouping criteria**  
Define a group based on resource types and tags.

Resource types

AWS::EC2::Instance X

Tags

Environment: Test X

**Group resources (3)**

| Identifier          | Tag: Name   | Service | Type     | Region    | Tag: Envir | Tags |
|---------------------|-------------|---------|----------|-----------|------------|------|
| i-013458eab769b0f91 | centos      | EC2     | Instance | us-east-1 | Test       |      |
| i-08d5ad4c78608373e | rhel8.2     | EC2     | Instance | us-east-1 | Test       |      |
| i-0f9bc0a2d74e4ff4a | amazonLinux | EC2     | Instance | us-east-1 | Test       |      |

**Group details**

Group name  
  
Maximum 300 characters. Must contain only letters, numbers, hyphens, underscores, and periods.

Group description - optional

## 4. Patch Manager:

**Goal:** Automate patching of instances to ensure they are up-to-date with the latest security and software updates.

1. **Tag Instances:**
  - o Ensure each instance is tagged with Patch Group=TestGroup.
2. **Create Patch Baseline:**
  - o **Navigate to Patch Manager:**
    - Go to Systems Manager > Patch Manager.
  - o **Create a Patch Baseline:**
    - Click on “Start with an overview”

- select **Patch baselines** and click on "Create patch baseline."

| Baseline ID                          | Baseline name                           | Description   | Operating system  |
|--------------------------------------|---|---|-------------------|
| <a href="#">pb-0cb0c4966f86b059b</a> | AWS-AlmaLinuxDefaultPatchBaseline       | Default Patch Baseline for Alma Linux Provided by AWS.        | AlmaLinux         |
| <a href="#">pb-0c10e657807c7a700</a> | AWS-AmazonLinuxDefaultPatchBaseline     | Default Patch Baseline for Amazon Linux Provided by AWS.      | Amazon Linux      |
| <a href="#">pb-0be8c61cde3be63f3</a> | AWS-AmazonLinux2DefaultPatchBaseline    | Default Patch Baseline for Amazon Linux 2 Provided by AWS.    | Amazon Linux 2    |
| <a href="#">pb-0028ca011460d5eaf</a> | AWS-AmazonLinux2022DefaultPatchBaseline | Default Patch Baseline for Amazon Linux 2022 Provided by AWS. | Amazon Linux 2022 |

- Provide a name (e.g. ssm-PatchManagerDemo) and description for the baseline.
- Select the operating system (e.g., Amazon Linux, CentOS, RHEL).

- Define the patch rules, such as including all patches or only critical/security patches, etc.

AWS Systems Manager > Patch Manager > Patch baselines > Create patch baseline

## Create patch baseline

### Patch baseline details

**Name**  
ssm-PatchManagerDemo  
You can use letters, numbers, periods, dashes, and underscores in the name.

**Description - optional**  
for testing patching of managed nodes

**Operating system**  
Select the operating system you want to specify approval rules and patch exceptions for.  
Amazon Linux 2

### 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   | X Remove rule  |
|---|--|
| <b>Products</b><br>Select patches by product<br><input type="button" value="Select products"/><br><b>All X</b>                          | <b>Auto-approval</b><br>Specify how to select updates for automatic approval<br><input checked="" type="radio"/> Approve patches after a specified number of days<br><input type="radio"/> Approve patches released up to a specific date<br>Specify the number of days<br><input type="text" value="0"/> days |
| <b>Classification</b><br>Select patches by classification<br><input type="button" value="Select classifications"/><br><b>Security X</b> | <b>Compliance reporting - optional</b><br>Specify the severity level to report for patches that match this rule.<br><input type="button" value="Unspecified"/>   |
| <b>Severity</b><br>Select patches by severity<br><input type="button" value="Select severities"/><br><b>Critical X</b>                  | <b>Include nonsecurity updates</b><br><input checked="" type="checkbox"/> Select this box to also install nonsecurity patches that meet the approval rules.  |
| <input type="button" value="Add rule"/> 9 remaining   |  |

- Scroll down and create the baseline.

- o Set Baseline as Default Baseline:**

If Patch Manager was accessed in a region prior to December 2022, you can set a baseline as the default baseline during or after creation using both console and CLI

In regions accessed after Dec 2022, only the CLI option is possible using the command below.

```
aws ssm register-default-patch-baseline --baseline-id baseline-id-or-ARN
```

### 3. Assign Patch Baseline to Patch Group:

- o Navigate to the Patch Baseline:

- In the Patch Manager console, select the patch baseline you created earlier.

- o Assign to Patch Group:

- click on *Actions* and *modify the patch baseline* by adding the tag value `TestGroup` assigned to the tag key “PatchGroup”

The screenshot shows the AWS Patch Manager interface. The top navigation bar includes links for AWS Systems Manager, Patch Manager, and Patch baselines. Below the navigation is a toolbar with 'Patch now' and 'Create patch policy'. A sidebar on the left contains sections for Overview of patching operations, Dashboard, Compliance reporting, Patch baselines (which is selected and highlighted with a pink border), Patches, Patch groups, and Settings. A message in the sidebar states: '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.' A 'Learn more' link is provided. The main content area displays a table titled 'Patch baselines (1/18)' with one entry. The entry details are: Baseline ID: pb-0ec397c4c618a0d7c, Baseline name: ssm-PatchManagerDemo, Description: for testing patching of managed nodes, Operating system: Amazon Linux 2, and Default baseline: No. A filter bar at the top of the table shows 'Baseline name = ssm-PatchManagerDemo' with a clear filter button. The 'Actions' menu is open, showing options: 'View details', 'Edit', 'Delete', 'Set default patch baseline', and 'Modify patch groups' (which is highlighted with a pink border). A pink number '4' is placed above the 'Actions' button, and a pink number '5' is placed next to the 'Modify patch groups' option. Navigation arrows are visible at the bottom right of the table.

The screenshot shows the 'Modify patch groups' dialog box for the baseline 'pb-0ec397c4c618a0d7c'. The title bar indicates the full path: AWS Systems Manager > Patch Manager > Patch baselines > Baseline ID: pb-0ec397c4c618a0d7c > Modify patch groups. The dialog has a header 'Patch groups' and a note: '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.' Below this are input fields for Baseline ID (pb-0ec397c4c618a0d7c), Baseline name (ssm-PatchManagerDemo), and Baseline description (for testing patching of managed nodes). A 'Patch groups' input field contains 'TestGroup' (highlighted with a pink border) and an 'Add' button (also highlighted with a pink border). A note below the input field specifies: 'Patch group values can consist of up to 256 letters, numbers, and the following characters: . \_ + @ / - :'. At the bottom right is a 'Close' button.

If the patch **baseline ID** details page does not include an *Actions* menu, patch groups can't be configured in the console, use the CLI with the below command

```
aws ssm register-patch-baseline-for-patch-group --baseline-id "value" --patch-group "value"
```

e.g

```
aws ssm register-patch-baseline-for-patch-group \
--baseline-id "pb-0e2ba677964f29e91" \
--patch-group "TestGroup" \
--region us-east-1
```

#### 4. Patch Using Patch Policy:

From DEC 2022 AWS recommends using **patch policies** to patch managed nodes.

- o **create patch policy**

- Navigate the SSM console and select “Patch Manager”
  - select create patch policy
  - configure patching
  - Under Patch Baseline section, select the custom baseline created earlier



- **configure patching:**
    1. name: ssm-demo-patch-policy
    2. patch operation: Scan or Scan and install
    3. scanning schedule: custom scan schedule
    4. scanning frequency: Daily, and enter suitable time in UTC

## Customize Patch Manager configuration options

### Define a patch policy that keeps your instances up to date

This Quick Setup configuration type makes it easy to setup patch scanning and patch installation for your EC2 and on-premises instances, regardless of whether you want to do so across all instances in your AWS Organization or select instances within a specific account and Region. For more details about Patch Manager and Patch Policies, follow this link. [Learn more](#)

#### Patch policy name

ssm-demo-patch-policy

The policy name can have up to 113 characters. Policy names are case sensitive.

Valid characters: A-Z, a-z, 0-9, \_, space, and - (hyphen)

#### Scanning and installation

##### Patch operation

Scans the targets and compares their installed patches against a list of approved patches in the patch baseline. Select to scan or to scan and install missing patches.

- Scan  
 Scan and install

##### Scanning schedule

- Use recommended defaults  
Patch Manager scans your nodes daily at 1:00 AM UTC.

- Custom scan schedule  
Create a custom scanning schedule.

##### Scanning frequency

Daily ▾

Every day at 10:05 UTC

- Under Patch Baseline, select the custom baseline created earlier

## Patch baseline

Patch baselines include rules for auto-approving patches within days of their release, in addition to a list of approved and rejected patches. [Learn more](#)

### Use recommended defaults

The default patch baseline defined for each operating system supported by AWS.

### Custom patch baseline

Select a custom patch baseline. Custom patch baselines must be in the home AWS Region specified for Quick Setup and can be up to 3,336 bytes.

#### ▼ View or change baselines

| Operating system                    | Select baseline  | Baseline ID          |
|-------------------------------------|--|----------------------|
| Alma Linux                          | AWS-AlmaLinuxDefaultPatchBaseline  | pb-0c512885f94eceb9e |
| Amazon Linux                        | AWS-AmazonLinuxDefaultPatchBaseline  | pb-0e392de35e7c563b7 |
| Amazon Linux 2                      | AWS-AmazonLinux2DefaultPatchBaseline   | pb-07e6d4e9bc703f2e3 |
| Amazon Linux 2022                   | AWS-AmazonLinux2022DefaultPatchBaseline  | pb-0d02b7674ff76a48d |
| Amazon Linux 2023                   | AWS-AmazonLinux2023DefaultPatchBaseline  | pb-0366438d3e092e1d3 |
| CentOS                              | AWS-CentOSDefaultPatchBaseline   | pb-0574b43a65ea646ed |
| Debian Server                       | AWS-DebianDefaultPatchBaseline   | pb-0d215380aec1af2f0 |
| macOS                               | AWS-MacOSDefaultPatchBaseline  | pb-0f9cdff0b6da47181 |
| Oracle Linux                        | AWS-OracleLinuxDefaultPatchBaseline  | pb-0bf2738c5e3b55542 |
| Raspberry Pi OS                     | <input type="text" value="Search"/>  | pb-07335117835e9e63a |
| Red Hat Enterprise Linux (RHEL)     | AWS-UbuntuDefaultPatchBaseline<br>Default Patch Baseline for Ubuntu Provided by AWS. | pb-0e9c1ce8d831d57e0 |
| Rocky Linux                         | <input type="text" value="Search"/>  | pb-056dd3ed0db4e2121 |
| SUSE Linux Enterprise Server (SLES) | <input type="text" value="Search"/>  | pb-0123fdb36e334a3b2 |
| Ubuntu Server                       | AWS-UbuntuDefaultPatchBaseline   | pb-052a2e04b3b354d69 |
| Windows Server                      | AWS-DefaultPatchBaseline   | pb-020d361a05defe4ed |

- Under Targets, select resource groups or use all managed nodes
- Review and create policy

## 5. Run Patching:

### Navigate to Patch Now:

- In the Patch Manager console, select "Patch now."

### Select the Patch Baseline:

- Choose the patch baseline you created.

The screenshot shows the AWS Systems Manager Patch Manager interface. The top navigation bar includes 'AWS Systems Manager > Patch Manager > Patch baselines'. Below the navigation is a header with 'Patch Manager' and 'Info' buttons, along with 'Patch now' and 'Create patch policy' buttons. A sub-header 'Overview of patching operations - new' is present. The main content area has tabs for 'Dashboard', 'Compliance reporting', 'Patch baselines' (which is selected and highlighted with a pink border), 'Patches', 'Patch groups', and 'Settings'. A note at the top states: '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](#)'.

| Baseline ID                          | Baseline name        | Description                           | Operating system | Default baseline |
|--------------------------------------|----------------------|---------------------------------------|------------------|------------------|
| <a href="#">pb-0ec397c4c618a0d7c</a> | ssm-PatchManagerDemo | for testing patching of managed nodes | Amazon Linux 2   | No               |
| <a href="#">pb-0e2ba677964f29e91</a> | ssm-demoCentos       | customBaseline for CentOS             | CentOS           | No               |

- o **Target Instances:**
  - Select the instances individually or use the tag-based patch group.
- o **Run the Patching:**
  - Execute the patching process and monitor its progress to ensure patches are applied successfully.

The screenshot shows the AWS Systems Manager Patch Manager interface. The top navigation bar includes 'AWS Systems Manager > Patch Manager > Patch now'. Below the navigation is a header with 'Patch instances now' and 'Info' buttons. A sub-header 'Basic configuration' is present, with a note: 'Scan for missing patches or install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.' The 'Patching operation' section shows 'Scan' selected (highlighted with a pink border). The 'Instances to patch' section shows 'Patch all instances' selected. The 'Target selection' section shows 'Choose instances manually' selected (highlighted with a pink border). The 'Managed instances (1/3)' section lists one instance: 'amazonLinux' (Instance ID: i-0f9bc0a2d74e4ff4a). The instance is selected (highlighted with a pink border).

| Name  | Instance ID          | Platform type | Operating system | Instance state    | Agent version |
|---|----------------------|---------------|------------------|-------------------|---------------|
| <input checked="" type="checkbox"/> amazonLinux | i-0f9bc0a2d74e4ff4a  | Linux         | Amazon Linux     | running           | 3.3.551.0     |
| <input type="checkbox"/>                        | mi-05fc84a2b8ba78274 | undefined     | undefined        | <a href="#">i</a> |               |

click on Patch Now

## 6. (Optional- legacy) Maintenance Window:

- o Create a maintenance window to understand how it can be used with Patch Manager.
- o **Create a Maintenance Window:**
  - Navigate to Systems Manager > Maintenance Windows.
  - Click on "Create maintenance window."
  - Provide a name, schedule (e.g., weekly on Sunday at 2 AM), duration, and cutoff time.
  - Register the target instances using the `Patch Group=TestGroup` tag.
  - Register a task to apply patches using the patch baseline.

## 5. Run Command:

**Goal:** Use Run Command to execute commands across instances simultaneously.

### 1. Create a Run Command Document:

- o **Navigate to Run Command:**
  - Go to Systems Manager > Shared Resources.
- o **Create a New Document:**
  - Click on "Create document."
  - Choose "Command document."
  - Provide a name (`ssm-Demo-InstallApache`) and description for the document.
  - for target type, select `/AWS::EC2::Instance`
  - document type(optional): select **command**
  - In the content section, use the following script to install Apache:

```
{  
    "schemaVersion": "2.2",  
    "description": "Install Apache HTTP Server",  
    "mainSteps": [  
        {  
            "action": "aws:runShellScript",  
            "name": "installApache",  
            "inputs": {  
                "runCommand": [  
                    "sudo yum install -y httpd",  
                    "systemctl start httpd",  
                    "systemctl enable httpd"  
                ]  
            }  
        }  
    ]  
}
```

- Save and create the document.

**Document details**

Documents define the actions that AWS Systems Manager performs on your resources.

**Name**  
Enter a unique name for the document.

`ssm-Demo-InstallApache`

The name must be between 3 and 128 characters. Valid characters are a-z, A-Z, 0-9, and \_, -, and . only

**Target type - optional**  
Specify the types of resources the document can run on. For example, "/AWS::EC2::Instance" or "/" for all resource types. [Learn more](#)

/AWS::EC2::Instance

**Document type - optional**  
Select a document type based on the service that you want to use.

Command

**Content**

**JSON**  
Specify document content in JSON format.

```

1 * {
2   "schemaVersion": "2.2",
3   "description": "Install Apache HTTP Server",
4   "mainSteps": [
5     {
6       "action": "aws:runShellScript",
7       "name": "installApache",
8       "inputs": {
9         "runCommand": [
10           "sudo yum install -y httpd",
11           "systemctl start httpd",
12           "systemctl enable httpd"
13         ]
14       }
15     }
16   ]
17 }
```

**YAML**  
Specify document content in YAML format.

**2. Execute Run Command:**

- o **Select the Document:**
  - In Run Command, select the created document.

**Run a command**

**Command document**  
Select the type of command that you want to run.

Search by keyword or filter by tag or attributes

Search: demo  Clear filters

| Name                               | Owner        | Platform types |
|------------------------------------|--------------|----------------|
| <code>ssm-DemoInstallApache</code> | 945685952191 | Linux, MacOS   |

**Description**  
Install Apache HTTP Server

**Document version**  
Choose the document version you want to run.

1 (Default)

**Command parameters**

o **Specify Targets:**

- Select Instance manually or Choose the resource group created earlier.

Target selection

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.

i-0f9bc0a2d74e4ff4a X

Instances

| Name  | Instance ID         | Instance state | Availability zone | Ping status | Last ping time   |
|---|---------------------|----------------|-------------------|-------------|--|
| <input checked="" type="checkbox"/> amazonLinux | i-0f9bc0a2d74e4ff4a | running        | us-east-1b        | Online      | 08/08/2024 at 15:57:08 GMT+0200 (Central European Summer Time) |
| <input type="checkbox"/> centos                 | i-013458eab769b0f91 | running        | us-east-1b        | Online      | 08/08/2024 at 15:53:06 GMT+0200 (Central European Summer Time) |

o **Run the Command:**

- Click run to Execute the command and monitor its progress.

## 6. Automation:

**Goal:** Use SSM Automation to automate common tasks using AWS-provided automation documents (runbooks).

### 1. Execute an Automation Document:

o **Navigate to Automation:**

- Go to Systems Manager , and under Change Management, click on Automation.

AWS Systems Manager

Management

**AWS Systems Manager Automation**  
Fleet-wide automation for common administration tasks

Define common IT tasks as a collection of steps in an SSM runbook, and execute all steps on a collection of AWS resources at scale. Create event-based automations, trigger approvals for principals, track progress, and audit executions.

Automate IT Tasks

**Execute automation**

Create automation runbook

Configure preferences

Getting started

Quick start guide to Automation

Automation examples

How it works

Use pre-defined Automation runbooks or create

Quick Setup

Operations Management

Application Management

Change Management

Automation New

Change Manager

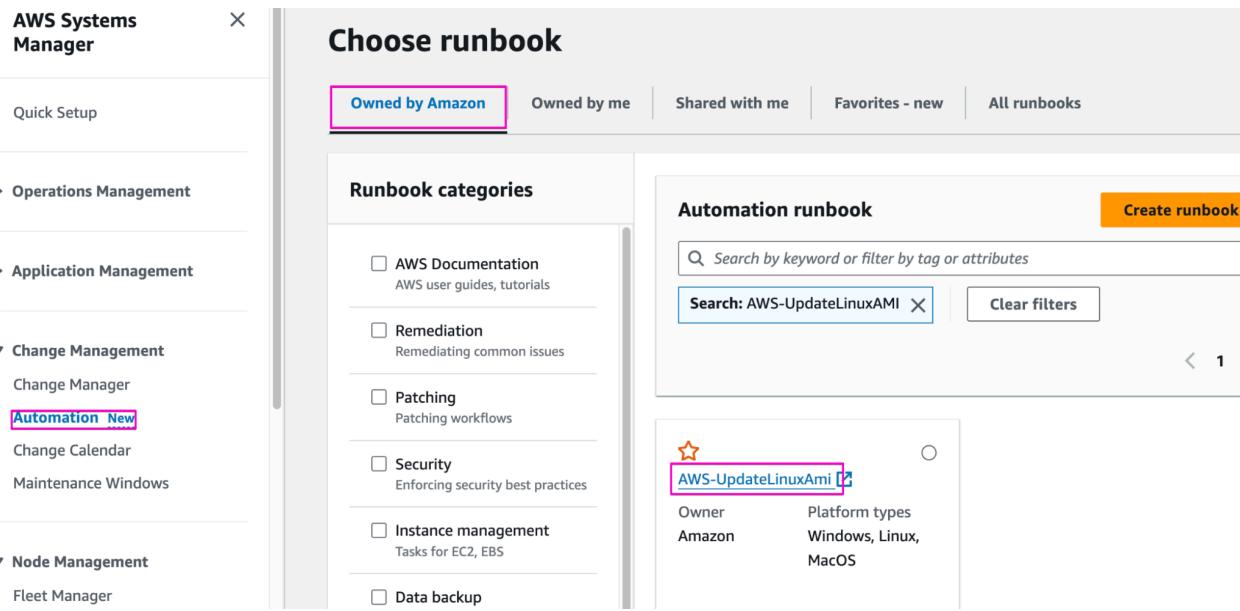
Change Calendar

Maintenance Windows

Node Management

o **Start Automation Execution:**

- Click on "Execute automation."
- Choose AWS-provided runbooks, and select AWS-UpdateLinuxAMI and click on Next.



- In the Execution mode section, choose **Simple Execution**,
- In the Input parameters section, provide the required parameters (
  1. source AMI id
  2. create AutomationRole for systems Manager service name **ssmAdmin** (create role with *Admin* or *AmazonSSMAutomationRole* policy)
  3. IamInstanceProfile Name: role with EC2-service that gives SSM necessary permissions.
  4. target AMI name etc

## Input parameters

**SourceAmiId**  
(Required) The source Amazon Machine Image ID.

**AutomationAssumeRole**

(Required) The ARN of the role that allows Automation to perform the actions on your behalf.

**InstanceType**

(Optional) Type of instance to launch as the workspace host. Instance types vary by region. Default is t3.micro.

**SubnetId**

(Optional) Specify the SubnetId if you want to launch EC2 instance in a specific subnet.

**PostUpdateScript**

(Optional) URL of a script to run after package updates are applied. Default ("none") is to not run a script.

**ExcludePackages**

(Optional) Names of packages to hold back from updates, under all conditions. By default ("none"), no package is excluded.

**IamInstanceProfileName**

(Optional) The instance profile that enables Systems Manager (SSM) to manage the instance.

**TargetAmiName**

(Optional) The name of the new AMI that will be created. Default is a system-generated string including the source AMI id, and the creation time and date.

**SecurityGroupIds**

(Optional) A comma separated list of security group IDs with the required Inbound and Outbound connectivity rules.

**PreUpdateScript**

(Optional) URL of a script to run before updates are applied. Default ("none") is to not run a script.

**IncludePackages**

(Optional) Only update these named packages. By default ("all"), all available updates are applied.

**MetadataOptions**

(Optional) The metadata options for the instance.

- Execute the automation and monitor its progress under **Executed Steps**

## Execution status

Overall status

In Progress

All executed steps

3

# Succeeded

3

# Failed

0

# Cancelled

0

# TimedOut

0

## Executed steps (6)

Find Steps

< 1 >

| Step ID                              | Step # | Step name         | Action                  | Status      | Start time                    | End time                      |
|--------------------------------------|--------|-------------------|-------------------------|-------------|-------------------------------|-------------------------------|
| 9932ff2b-abd8-41d5-90d4-bafadfdc6d69 | 1      | launchInstance    | aws:runInstances        | ⌚ Success   | Thu, 08 Aug 2024 18:02:37 GMT | Thu, 08 Aug 2024 18:06:03 GMT |
| 15921ef8-c7c2-4a7e-be4a-eff654512353 | 2      | verifySsmInstall  | aws:runCommand          | ⌚ Success   | Thu, 08 Aug 2024 18:06:03 GMT | Thu, 08 Aug 2024 18:06:06 GMT |
| a2c52d87-3118-454b-a49e-82c607f4c67f | 3      | updateOSSoftware  | aws:runCommand          | ⌚ Success   | Thu, 08 Aug 2024 18:06:06 GMT | Thu, 08 Aug 2024 18:06:17 GMT |
| dd6c2d49-f6eb-4aad-b041-20216b215e18 | 4      | stopInstance      | aws:changeInstanceState | In Progress | Thu, 08 Aug 2024 18:06:17 GMT | -                             |
| ff0e81fa-a32e-4c35-808a-eb4cf2d85755 | 5      | createImage       | aws:createImage         | ⌚ Pending   | -                             | -                             |
| 373c147e-3651-4a9c-a1b5-e49c1fdf998a | 6      | terminateInstance | aws:changeInstanceState | ⌚ Pending   | -                             | -                             |

## **7. State Manager:**

**Goal:** Use State Manager to ensure instances are in a consistent state.

### **1. Create a State Manager Association:**

- o **Navigate to State Manager:**
  - Go to Systems Manager > State Manager.
- o **Create Association:**
  - Click on "Create association."
  - Choose a document, such as AWS-UpdateSSMAgent to ensure the SSM agent is always running.
  - Provide association details, such as targets (e.g., instances tagged with Environment=Test).
  - Configure the schedule and parameters as needed.
  - Create the association.

### **2. Monitor Compliance:**

- o **Check Compliance Status:**
  - In State Manager, monitor the compliance status of the instances.
  - Ensure that the SSM agent remains active and up-to-date.