

## **SSM (Simple System Manager)**

---

- ❖ System manager is a central hub to control and view your entire AWS infrastructure.
  - ❖ System manager includes:
    - ✓ Session manager
    - ✓ Run Command
    - ✓ Patch Manager
    - ✓ State Manager
  - ❖ In order to Manage all the different nodes or all the instances you have a single place and that is System manager.
- **Session manager:**
- ✓ Session Manager is a fully managed AWS Systems Manager capability. With Session Manager, you can manage your Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs).
  - ✓ Some Pre\_Required things that are important to do is, we first need to make a particular IAM role and they are global. So no matter in which region you will make your EC2 you can use your IAM role.

Go to IAM > Roles > Create role > Check AWS service radio button > Select use case as EC2 > Click Next

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

## Select trusted entity [Info](#)

### Trusted entity type



#### AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.



#### AWS a

Allow ei  
account  
party to  
account



#### SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.



#### Custor

Create  
enable  
this acc

### Use case

Allow an AWS service like EC2, Lambda, or others to perform ac

#### Common use cases



#### EC2

Allows EC2 instances to call AWS services on your behalf.



#### Lambda

✓ Step 2 is to add Permissions

Permissions Policy > Type SSM > Select AmazonSSMFullAccess

## Permissions policies (1207) [Info](#)

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



AmazonSSMDirectoryServiceAccess

AWS m...

This policy allows SSM Agent to access Directory Service on behalf of the ...



AmazonSSMFullAccess

AWS m...

Provides full access to Amazon SSM.

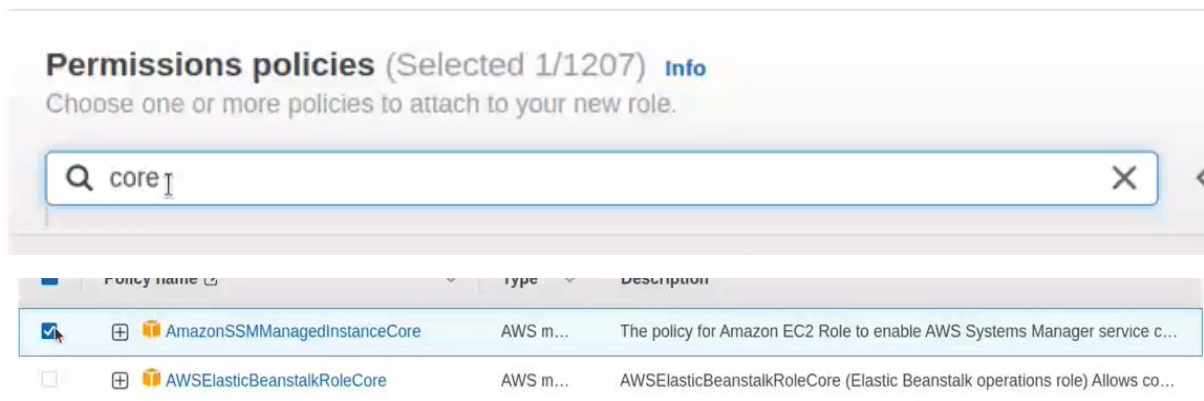


AmazonSSMAutomationPole

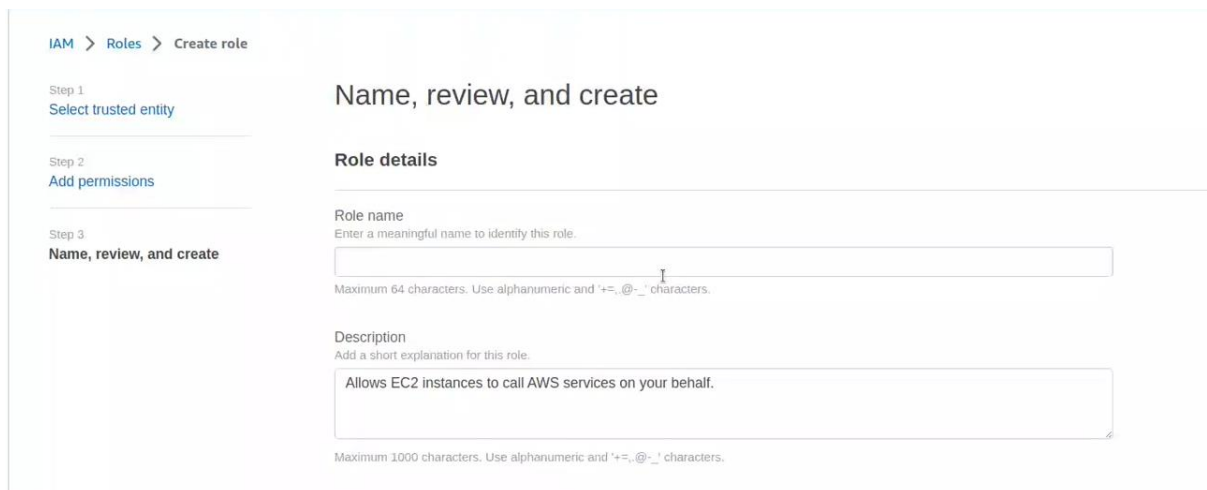
AWS m...

Provides permissions for EC2 Automation service to execute activities defi

To add another Policy type Core > AmazonSSMManagedInstanceCore > Click Next

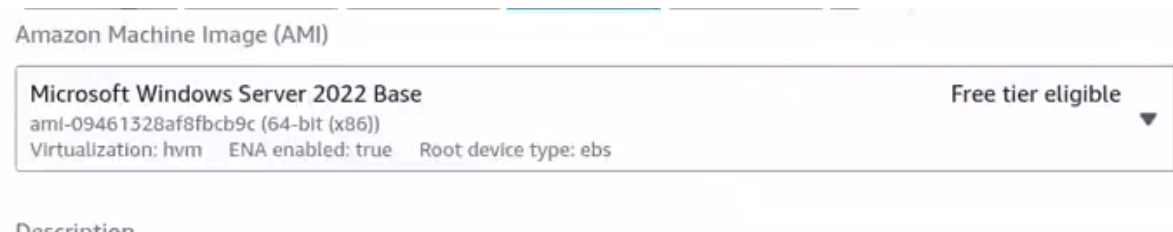


- ✓ Now step 3 is “Name, Review, Create”, Here you have to give the tags and Click on Create Role.



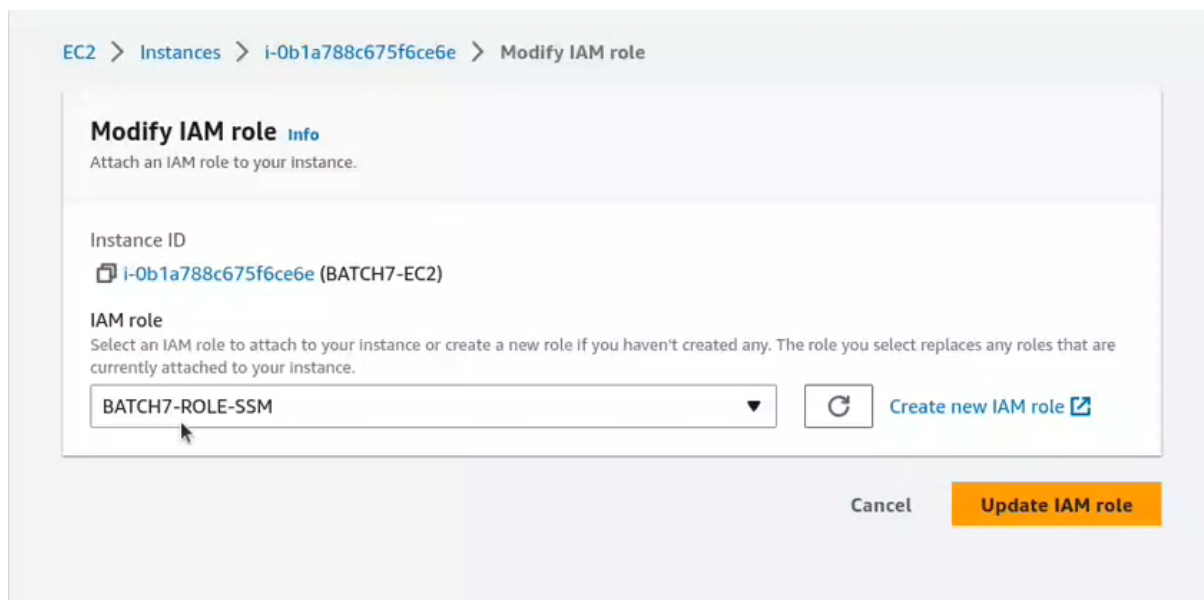
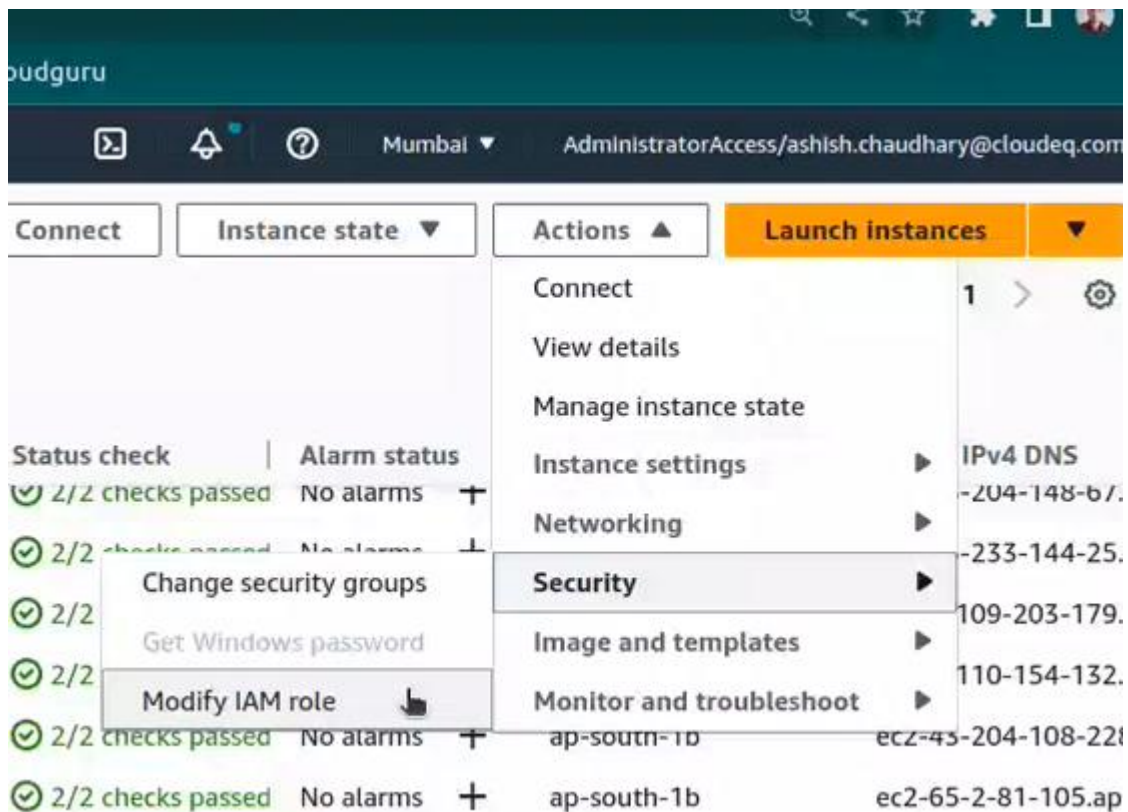
- ✓ After creating this role goto your EC2 and Create EC2 Instance.

AWS console> EC2 > Name > Select AMI as Windows > AMI as Microsoft Windows Server 2022 Base > Key pair > Launch.



- ✓ No need to do anything with network security and Security group.

After launching a instance go to your instance, Select the instance, go to actions > security > Modify IAM role



- ✓ Now to start a session you can either use one of following two ways.(bellowed image )

Go to AWS Systems manager > Session Manager > Start Session > Give ID of your EC2 instance to which you want to start a session.

The screenshot shows the 'Start a session' page in the AWS Systems Manager console. The breadcrumb navigation at the top reads 'AWS Systems Manager > Session Manager > Start a session'. The main heading is 'Start a session'. Below it, a prompt says 'Select the instance that you would like to start a session on'. There are two main sections: 'Reason' and 'Target instances'. The 'Reason' section has a sub-heading 'Reason for session – optional' and a description: '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'. It contains a text input field with the placeholder 'Enter reason' and a note: 'This value can have up to 256 characters.' The 'Target instances' section has a search bar with a magnifying glass icon and the placeholder text 'Filter instances'.

OR

The screenshot shows the 'Connect to instance' page in the AWS Systems Manager console. The breadcrumb navigation at the top reads 'EC2 > Instances > i-0b1a788c675f6ce6e > Connect to instance'. The main heading is 'Connect to instance' with an 'Info' link. Below it, a description says: 'Connect to your instance i-0b1a788c675f6ce6e (BATCH7-EC2) using any of these options'. There are four tabs: 'EC2 Instance Connect', 'Session Manager' (which is selected), 'SSH client', and 'EC2 serial console'. Below the tabs, the 'Session Manager usage:' section contains a bulleted list: 'Connect to your instance without SSH keys or a bastion host.', 'Sessions are secured using an AWS Key Management Service key.', 'You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.', and 'Configure sessions on the Session Manager [Preferences](#) page.' At the bottom right, there are 'Cancel' and 'Connect' buttons.

After Connecting you are good to go

```
PS C:\Windows\system32> get-command
```

## RUN COMMAND:

- ✓ With the help of this you can run different commands.
- ✓ Using Run Command, a capability of AWS Systems Manager, you can remotely and securely manage the configuration of your managed nodes.
- ✓ A managed node is any Amazon Elastic Compute Cloud (Amazon EC2) instance, edge device, or on-premises server or virtual machine (VM) in your hybrid environment that has been configured for Systems Manager.
- ✓ Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale.

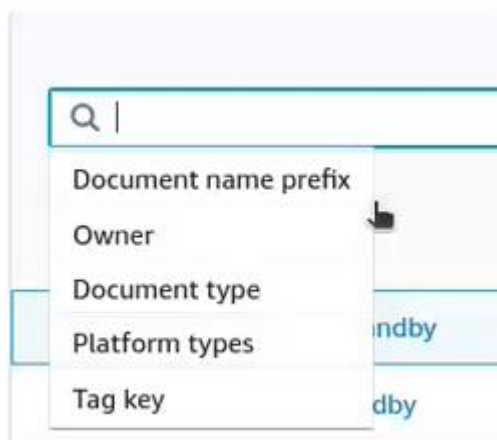
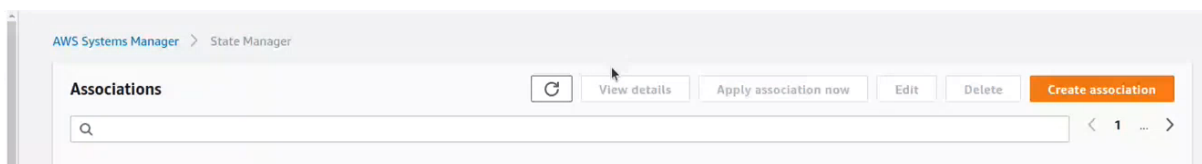
## NEED:

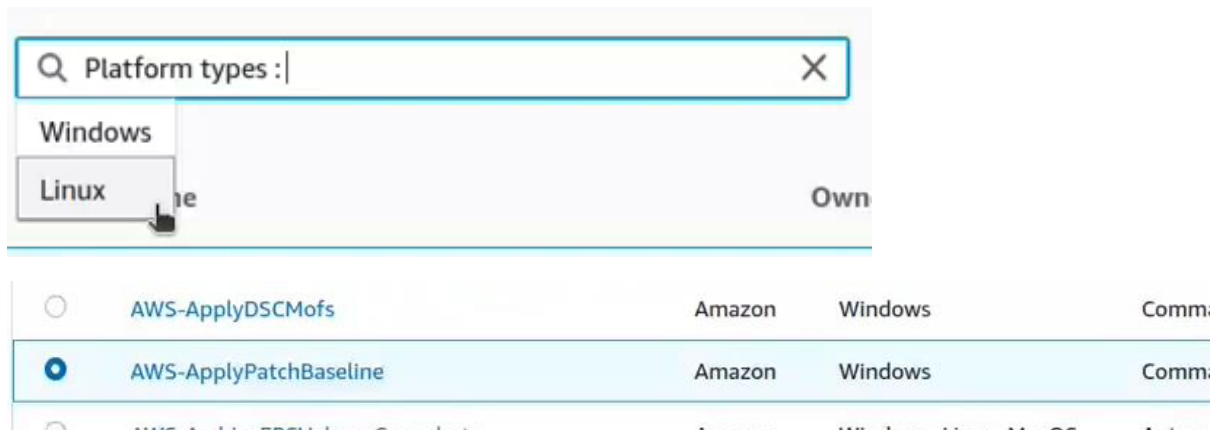
Suppose you are in a team, and you need to run a particular commands hundred time, right? So obviously you will not write the script again and again but here what you can do is you can just have it in the run command, and you are good to go.

## STATE Manager:

- ✓ In State manager we used to make association.
- ✓ Lets create a association

AWS System manager > State Manager > Create Association > Name > Select “Platform Type” > Target Selection > Select the instance manually > Select the severity as High > Click create.



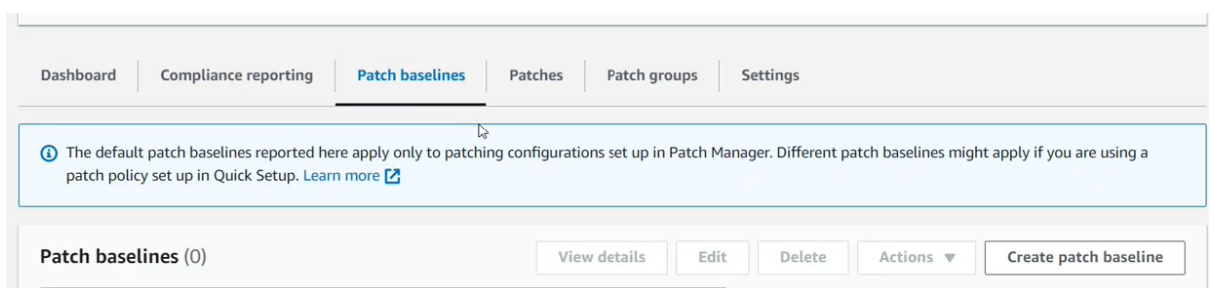


After creating association wait for Status as “SUCCESS”.

## PATCH MANAGER:

- ✓ Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security-related updates and other types of updates.
- ✓ You can use Patch Manager to install Service Packs on Windows nodes and perform minor version upgrades on Linux nodes. You can patch fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs) by operating system type.
- ✓ Only the instances in which SSM agent is installed are eligible for Patching and inventory.
- ✓ First thing that we need to do before creating and apply a patch is to create a baseline.

AWS SYSTEM MANAGER > Patch Manager > Patch Baseline > Give Name > Description > Select Operating System > Select Product as ALL > Select the Severity as ALL > Select Classification as ALL > Specify the number of days for Updating > add tags > Click Create.



In order to add another rule Click on add rule.

#### Classification

Select patches by classification

Select classifications

All X

All ^

#### 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

7 days

#### Compliance reporting - optional

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

Unspecified

Add rule 9 remaining

In order to Patch it select the patch baseline, and click on PATCH NOW.

Patch now

Create patch policy



### Basic configuration

Scan for missing patches or install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

Patching operation

☒ Scan

☐ Scan and install

Instances to patch

Choose whether to patch all instances or only the instances you specify

☒ Patch all instances

☐ Patch only the target instances I specify

Patching log storage New

Select or create an S3 bucket for storing patching operation logs. Select **Do not store logs** if you don't require log information.

Do not store logs ▾

↻

### Advanced options Info New

Configure on-instance orchestration for complex patching scenarios.

Create SSM document ↗

Lifecycle hooks - *optional*

Choose Systems Manager documents (SSM documents) to run at certain points during the patching operation. (Requires SSM Agent version 3.0.502 or later.)

☐ Use lifecycle hooks

Patch now

Click Patch Now. It'll display the following window.

AWS Systems Manager > Patch Manager > Association execution summary

## Association execution summary

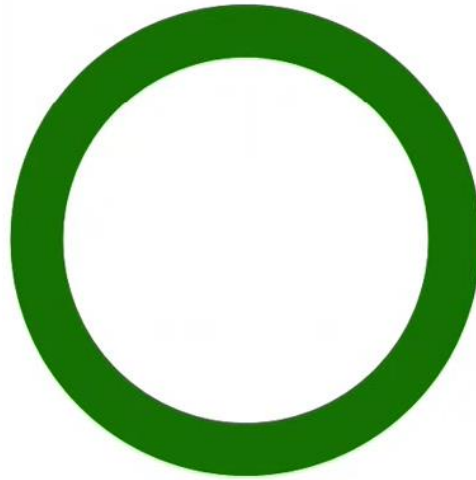
### AWS-PatchNowAssociation

Association ID	Execution ID
<a href="#">3b4baacf-beea-42c3-84b8-0595094df81e</a>	<a href="#">3940df88-e27c-4285-85fb-80b70521fd72</a>
Status	Operation
<span>⌚ Pending</span>	Scan
Reboot option	Targets
NoReboot	InstanceIds: *
Progress	
Pending=1	

If the patching is successful than it'll show the following screen.

### Scan/Install operation summary

■ Succeeded ■ Failed ■ Skipped ■ Pending



### INVENTORY:

AWS System manager > Inventory > SetUp Inventory > Give name > Select target as “manually selecting the instance” > give instance ID > Give the time after that you want to collect your inventory data > Click Set up.

