

AUTOMATE EC2 MANAGEMENT USING AWS SYSTEMS MANAGER

AWS Systems Manager (SSM) Agent Prerequisites

AWS SSM Prerequisites:

- ❖ Availability of AWS Systems Manager (SSM) Agent in EC2.
 - ❖ [List of AMIs with SSM Agent Preinstalled.](#)
- ❖ IAM Role / EC2 instance Profile with required privileges.
- ❖ EC2 Security Group should allow outbound connection to SSM

AWS Systems Manager Capabilities



AWS Systems Manager

-  **Automation**
-  **Maintenance Window**
-  **Patch Manager**
-  **State Manager**
-  **Parameter Store**
-  **Inventory**
-  **Documents**
-  **Run Command**
-  **Session Manager**

STEP 1 :- Create an Instance

Instances (2) Info			
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>			
<input type="checkbox"/>	Name ✎	Instance ID	Insta
<input type="checkbox"/>	Amazon-2	i-0812797eb2353a74f	🕒 P

STEP 2 :- Take Access

```
ec2-user@ip-1
Using username "ec2-user".
Authenticating with public key "Meow"

#_
~\_##### Amazon Linux 2
~~\_#####\
~~\_####| AL2 End of Life is 2025-06-30.
~~\_#/\
~~\_V~'-'>
~~~~
~~~.~.~
_/_m/'_/_/_/_/_
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

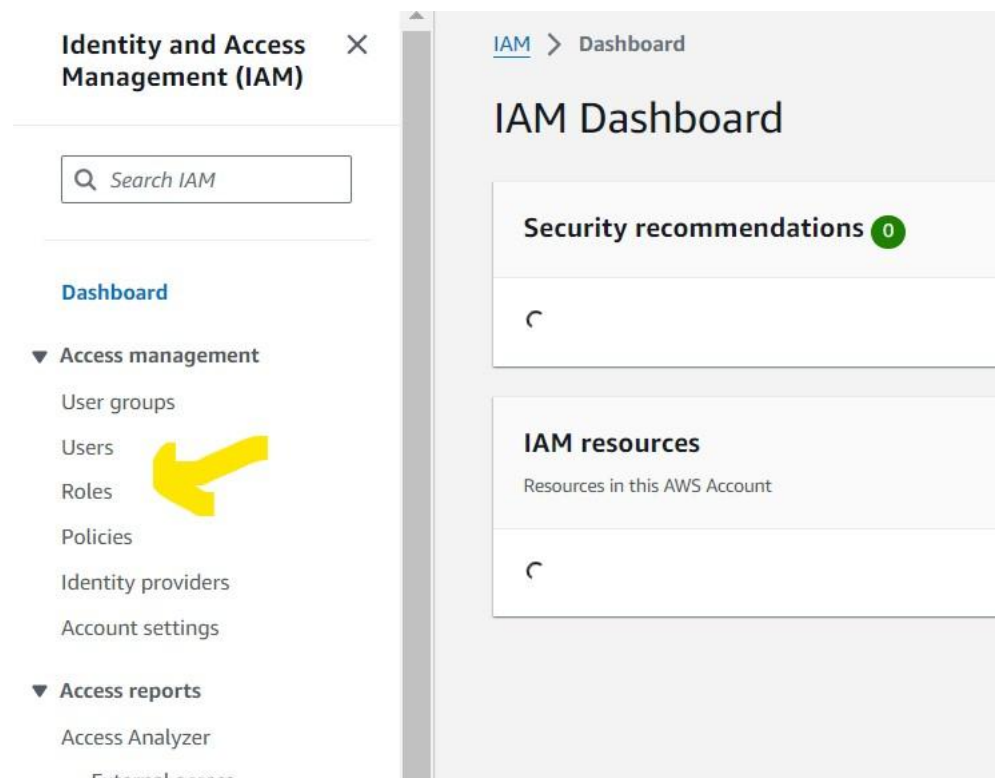
[ec2-user@ip-10-0-2-188 ~]$
[ec2-user@ip-10-0-2-188 ~]$
[ec2-user@ip-10-0-2-188 ~]$
```

STEP 3 :- Checking, If the SSM agent is installed or not. Although, by default it is installed in amazon Linux.

```
[ec2-user@ip-10-0-2-188 ~]$ yum info amazon-ssm-agent
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name       : amazon-ssm-agent
Arch       : x86_64
Version    : 3.3.380.0
Release    : 1.amzn2
Size       : 137 M
Repo       : installed
Summary    : Manage EC2 Instances using SSM APIs
URL        : http://docs.aws.amazon.com/ssm/latest/APIReference/Welcome.html
License    : ASL 2.0
Description: This package provides Amazon SSM Agent for managing EC2 Instances
           : using SSM APIs

[ec2-user@ip-10-0-2-188 ~]$
```

STEP 4 :- We first have to attach role to the EC2 Instance for managing SSM agent on instance.



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 account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

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

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

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

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.

Add permissions [Info](#)

Permissions policies (1/945) [Info](#)

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

	Policy name ↗	
<input type="checkbox"/>	AmazonSSMAutomationApproverAccess	↗
<input type="checkbox"/>	AmazonSSMAutomationRole	↗
<input type="checkbox"/>	AmazonSSMDirectoryServiceAccess	↗
<input type="checkbox"/>	AmazonSSMFullAccess	↗
<input type="checkbox"/>	AmazonSSMMaintenanceWindowRole	↗
<input type="checkbox"/>	AmazonSSManagedEC2InstanceDefaultPolicy	↗
<input checked="" type="checkbox"/>	AmazonSSManagedInstanceCore	↗
<input type="checkbox"/>	AmazonSSMPatchAssociation	↗

STEP 5 :’ Attaching IAM role to the EC2 Instance.

Instances (1/2) [Info](#)

All states ▾

	Name ↗	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability
<input type="checkbox"/>	Test	i-056809deb8717d6fd	Terminated 🔍	t2.micro	–	View alarms +	us-east-1b
<input checked="" type="checkbox"/>	Amazon-2	i-0812797eb2353a74f	Running 🔍	t2.micro	2/2 checks passed	View alarms +	us-east-1b

[Change security groups](#)
[Get Windows password](#)
[Modify IAM role](#)

[Connect](#)
[View details](#)
[Manage instance state](#)
[Instance settings](#)
[Networking](#)
[Security](#)
[Image and templates](#)
[Monitor and troubleshoot](#)

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
📄 i-0812797eb2353a74f (Amazon-2)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role ▴

No IAM Role
Choose this option to detach an IAM role
AWSCloud9SSMInstanceProfile
arn:aws:iam::533267372710:instance-profile/cloud9/AWSCloud9SSMInstanceProfile
SSM_Core
arn:aws:iam::533267372710:instance-profile/SSM_Core

[Create new IAM role](#)

Warning: The instance will be removed. Are you sure?

[Cancel](#) [Update IAM role](#)

STEP 6 :- Go to System Manager Dashboard in AWS Environment.

The screenshot shows the AWS Systems Manager console. The left-hand navigation pane is expanded, showing the following categories:

- Application Management**
 - Application Manager New
 - AppConfig
 - Parameter Store New
- Change Management**
 - Change Manager
 - Automation New
 - Change Calendar
 - Maintenance Windows
- Node Management**
 - Fleet Manager
 - Compliance
 - Inventory
 - Hybrid Activations
 - Session Manager
 - Run Command
 - State Manager
 - Patch Manager
 - Distributor

A yellow arrow points to the **Session Manager** option in the Node Management section.

The main content area displays the **AWS Systems Manager** dashboard with the heading "MANAGEMENT TOOLS" and "Gain Operational Insight and Take Action on AWS". A prominent orange button says "Get Started with Systems Manager". Below this, a section titled "How it Works" illustrates the workflow with three steps:

- Group your resources**: Group your AWS resources and save them into resource groups.
- View insights**: See relevant operational data and dashboards about your grouped resources.
- Take Action**: Mitigate issues by performing operations directly on grouped resources.

The screenshot shows the "Specify target" step in the AWS Systems Manager console. The left-hand navigation pane shows the following steps:

- Step 1: **Specify target** (Current step)
- Step 2 - optional: Specify session document
- Step 3: Review and launch

The main content area is titled "Specify target" and includes the instruction: "Select an instance to connect to using Session Manager."

The "Reason" section contains a text input field labeled "Enter reason" with a placeholder "Enter reason". Below the field, it states: "This value can have up to 256 characters."

The "Target instances" section features a search bar labeled "Filter instances" and a table of available instances:

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input type="radio"/>	Amazzon-2	i-0812797eb235...	3.3.380.0	running	us-east-1b	Amazon Li...

STEP 7 :- Visit EC2 Instance and Click on Connect and Through Session, connect your Instance.

Connect to instance [Info](#)

Connect to your instance ec2-10-0-10-10.us-east-2.compute.amazonaws.com (Amazon-2) using any of these options


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- 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.
- Configure sessions on the Session Manager [Preferences](#)  page.

Cancel

Connect