

SSM Session Manager

Created IAM role with required permissions to establish connection via SSM Session Manager

Create a role in the IAM board

Roles (4) [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.

< 1 >

Select a service

[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 account**

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

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role 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.

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.

Use cases for other AWS services:

Choose a service to view use case

Add policy

Add permissions [Info](#)

Permissions policies (Selected 1/802) [Info](#)

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

Q Filter policies by property or policy name and press enter.

1 match

< 1 >

⚙

"amazonSSMManagedInstanceCore" X

Clear filters

<input checked="" type="checkbox"/>	Policy name ↗	Type	Description
<input checked="" type="checkbox"/>	AmazonSSMManagedInstanceCore	AWS m...	The policy for Amazon EC2 Role to enable AWS Systems Manager servic...

▶ Set permissions boundary - optional [Info](#)

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Creation of the role

<input type="checkbox"/>	SSMrole	AWS Service: ec2	-
--------------------------	-------------------------	------------------	---

Attach role to EC2 instance

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

⌂

Connect

Instance state ▼

Actions ▲

Launch instances ▼

Find instance by attribute or tag (case-sensitive)

1 > ⚙

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Zone	Public IP
<input checked="" type="checkbox"/>	nebo_instance	i-09c4ab8e17ed3bddd	Running	t2.micro	2/2 checks passed	ec2-...	ec2-...

Connect

View details

Manage instance state

Instance settings

Networking

Security

Image and templates

Monitor and troubleshoot

Change security groups

Get Windows password

Modify IAM role

EC2 > Instances > i-09c4ab8e17ed3bddd > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

i-09c4ab8e17ed3bddd (nebo_instance)

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.

SSMrole

Create new IAM role [↗](#)

Cancel

Update IAM role

Connect to the instance using SSM Session Manager

Target instances

Filter instances

< 1 >

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input type="radio"/>	nebo_instance	i-09c4ab8e17ed3bddd	3.2.286.0	✔ running	us-east-1b	Amazon Linux

Cancel

Start session

Session ID: root-0101fb266ce6b3de6Instance ID: i-09c4ab8e17ed3bddd

sh-4.2\$ pwd
/usr/bin
sh-4.2\$

Terminate

