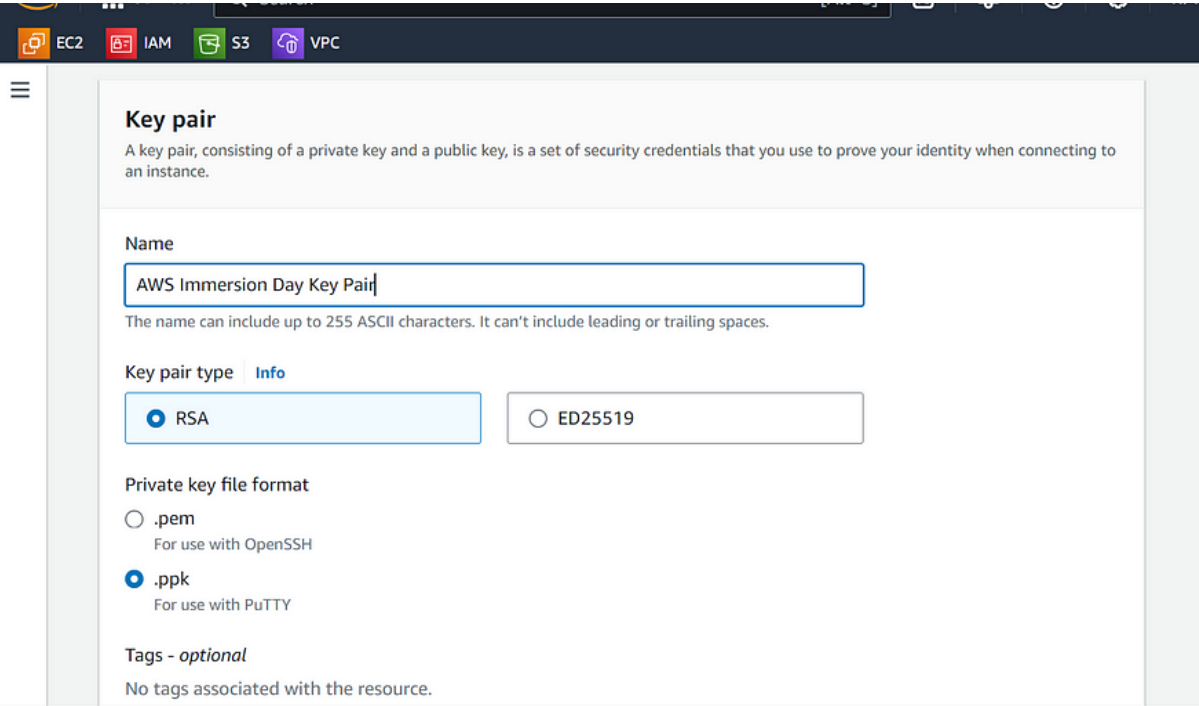


Task : Launching EC2 Linux instance and connect with Session Manager

Creating Key Pair



The screenshot shows the 'Key pair' creation page in the AWS Management Console. The top navigation bar includes icons for EC2, IAM, S3, and VPC. The page title is 'Key pair' with a subtitle explaining that a key pair consists of a private key and a public key used for authentication. The 'Name' field contains 'AWS Immersion Day Key Pair'. Below this, the 'Key pair type' section has two options: 'RSA' (selected) and 'ED25519'. The 'Private key file format' section has two options: '.pem' (for use with OpenSSH) and '.ppk' (selected, for use with PuTTY). At the bottom, there is a 'Tags - optional' section stating 'No tags associated with the resource.'

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name
AWS Immersion Day Key Pair
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)
☒ RSA ☐ ED25519

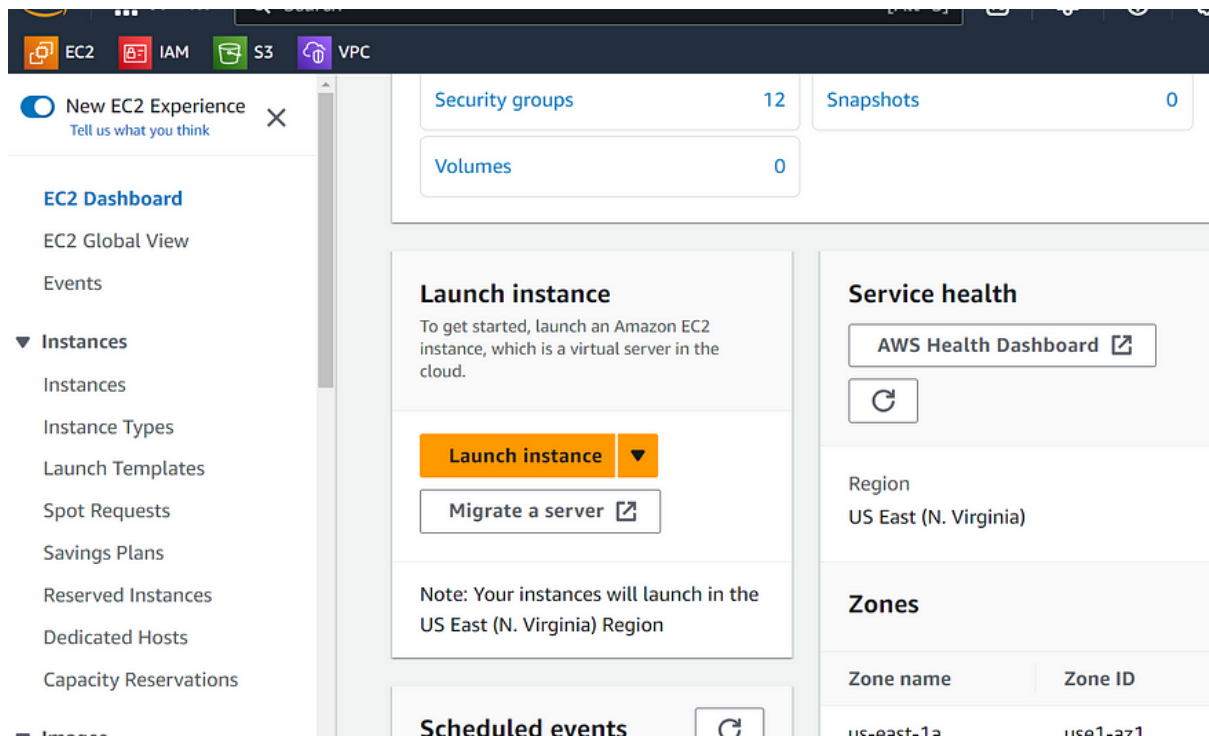
Private key file format
☐ .pem
For use with OpenSSH
☒ .ppk
For use with PuTTY

Tags - optional
No tags associated with the resource.

[Launch a Web Server Instance](#)

We will launch an Amazon Linux 2 instance, bootstrap Apache/PHP, and install a basic web page that will display information about our instance.

1. Click on EC2 Dashboard near the top of the leftmost menu. And Click on Launch instance.



2. Give the name of your choice

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

3. From Quick Start Choose **Amazon Linux**, Amazon Machine Image(AMI) is **Amazon Linux 2023 AMI** and Architecture as **64 bit(x86)**

Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

ami-067d1e60475437da2 (64-bit (x86)) / ami-04a3fea0ceec717e5 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.2.20231002.0 x86_64 HVM kernel-6.1

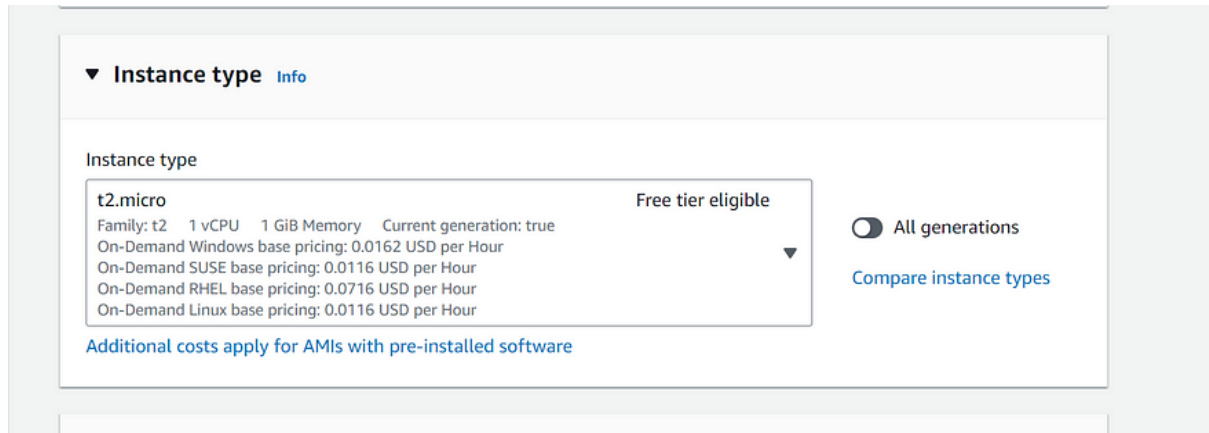
Architecture

64-bit (x86)

AMI ID

ami-067d1e60475437da2 Verified provider

4. Instance type would be t2.micro(As it is for free tier)



▼ Instance type [Info](#)

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

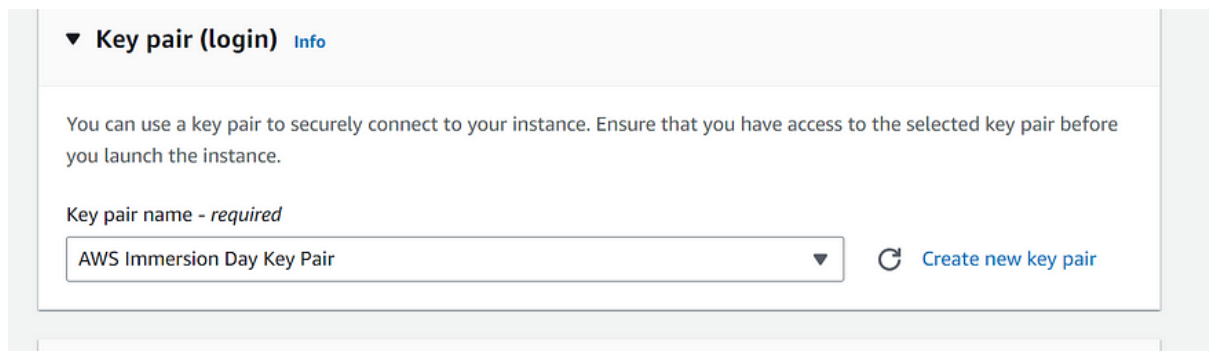
Free tier eligible

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

5. Choose Key Pair as we have created in the starting



▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

AWS Immersion Day Key Pair

↻ [Create new key pair](#)

6. Click on **Edit** for Network Settings

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-03d2b2555bf17ccdf

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-10' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

shell Feedback © 2023, Amazon Web Services India Private Limited or its aff

7. Choose VPC as Default VPC, Subnet as No Preference, and Auto Assign IP as “Enable”

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-03d2b2555bf17ccdf

(default) ▼

172.31.0.0/16

Subnet [Info](#)

No preference ▼

Create new subnet [↗](#)

Auto-assign public IP [Info](#)

Enable ▼

Firewall (security groups) [Info](#)

8. Give the Security Group name as “Immersion Day Security Group” and Description as “Immersion Day Security Group Description”

i). Rule 1 allows TCP traffic to port 22 for My AWS Web Server.

The screenshot shows the AWS Management Console interface for creating a security group. The 'Security group name' field is filled with 'Immersion Day Security Group'. Below it, a note states: 'This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*'. The 'Description' field is filled with 'Immersion Day Security Group Description'. Under 'Inbound Security Group Rules', there is one rule: 'Security group rule 1 (TCP, 22, 49.36.56.143/32)'. The rule configuration is as follows:

Type	Protocol	Port range	Source type	Name	Description - optional
ssh	TCP	22	My IP	49.36.56.143/32	e.g. SSH for admin desktop

At the bottom, there is a button labeled 'Add security group rule'.

ii) Rule 2 allow HTTP traffic to My AWS Web Server

▼ Security group rule 2 (TCP, 80, 49.36.56.143/32) Remove

Type Info	Protocol Info	Port range Info
<input type="text" value="HTTP"/>	<input type="text" value="TCP"/>	<input type="text" value="80"/>
Source type Info	Name Info	Description - optional Info
<input type="text" value="My IP"/>	<input type="text" value="Add CIDR, prefix list or security group ID"/> <input type="text" value="49.36.56.143/32"/>	<input type="text" value="e.g. SSH for admin desktop"/>

9. Configure storage should be kept as it is.

▼ **Configure storage** [Info](#) Advanced

1x GiB Root volume (Not encrypted)

[i](#) Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ×

0 x File systems Edit

► **Advanced details** [Info](#)

10. Go to Advanced Details

Scroll down to Metadata version and select V2 only(token required)

Metadata accessible [Info](#)


Select ▼

Metadata transport

Select ▼

Metadata version [Info](#)

V2 only (token required) ▼


 For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit [Info](#)

11. Under userdata add the script

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

 Choose file

```
#!/bin/sh

#Install a LAMP stack
dnf install -y httpd wget php-fpm php-mysql php-json php php-devel
dnf install -y mariadb105-server
dnf install -y httpd php-mbstring

#Start the web server
chkconfig httpd on
systemctl start httpd

#Install the web pages for our lab
if [ ! -f /var/www/html/immersion-day-app-php7.zip ]; then
  cd /var/www/html
  wget -O 'immersion-day-app-php7.zip' 'https://static.us-east-
```



```
#!/bin/sh
```

```
#Install a LAMP stack
```

```
dnf install -y httpd wget php-fpm php-mysqli php-json php  
php-devel
```

```
dnf install -y mariadb105-server
```

```
dnf install -y httpd php-mbstring
```

```
#Start the web server
```

```
chkconfig httpd on
```

```
systemctl start httpd
```

```
#Install the web pages for our lab
```

```
if [ ! -f /var/www/html/immersion-day-app-php7.zip ]; then
```

```
cd /var/www/html
```

```
wget -O 'immersion-day-app-php7.zip'
```

```
'https://static.us-east-1.prod.workshops.aws/public/444df362-a2  
11-4686-869b-77496f0dd3be/assets/immersion-day-app-php7.  
zip'
```

```
unzip immersion-day-app-php7.zip
```

```
fi
```

```
#Install the AWS SDK for PHP
```

```
if [ ! -f /var/www/html/aws.zip ]; then
```

```
cd /var/www/html
```

```
mkdir vendor
```

```
cd vendor
```

```
wget
```

```
https://docs.aws.amazon.com/aws-sdk-php/v3/download/aws.zip
```

```
p
```

```
unzip aws.zip
```

```
fi
```

```
# Update existing packages
```

dnf update -y

12. Click on Launch Instance

Number of instances [Info](#)

1

[Firewall \(security group\)](#)

New security group

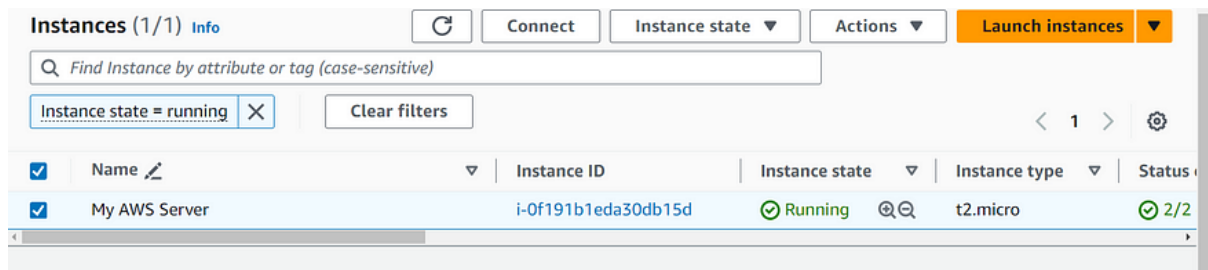
[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel [Launch instance](#) [Review commands](#)

13. Click the View Instances button in the lower right hand portion of the screen to view the list of EC2 instances. Once your instance has launched, you will see your Web Server as well as the Availability Zone the instance is in, and the publicly routable DNS name. Click the checkbox next to your web server to view details about this EC2 instance.

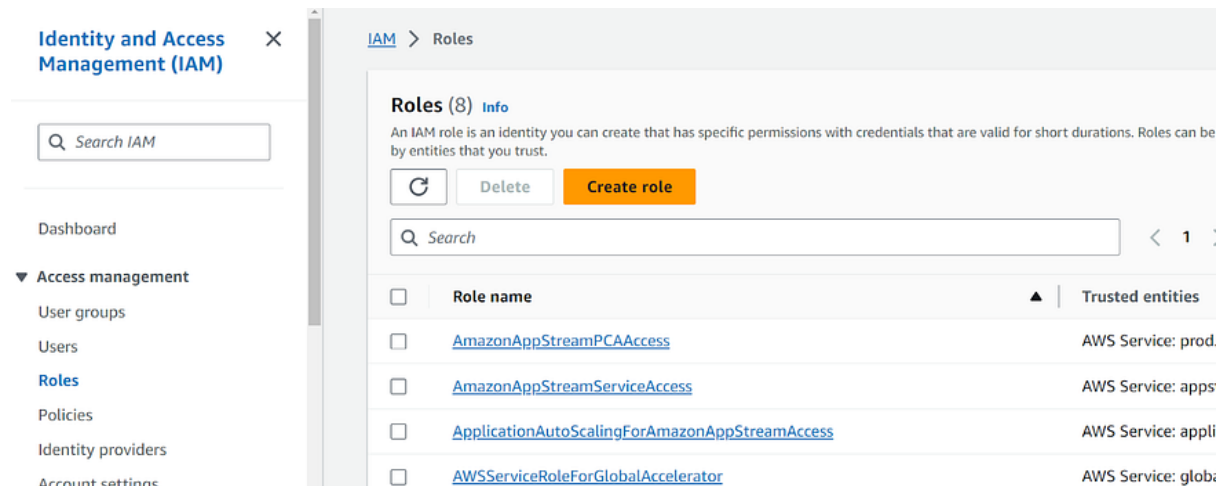


Connect to your Linux instance using Session Manager (Optional)

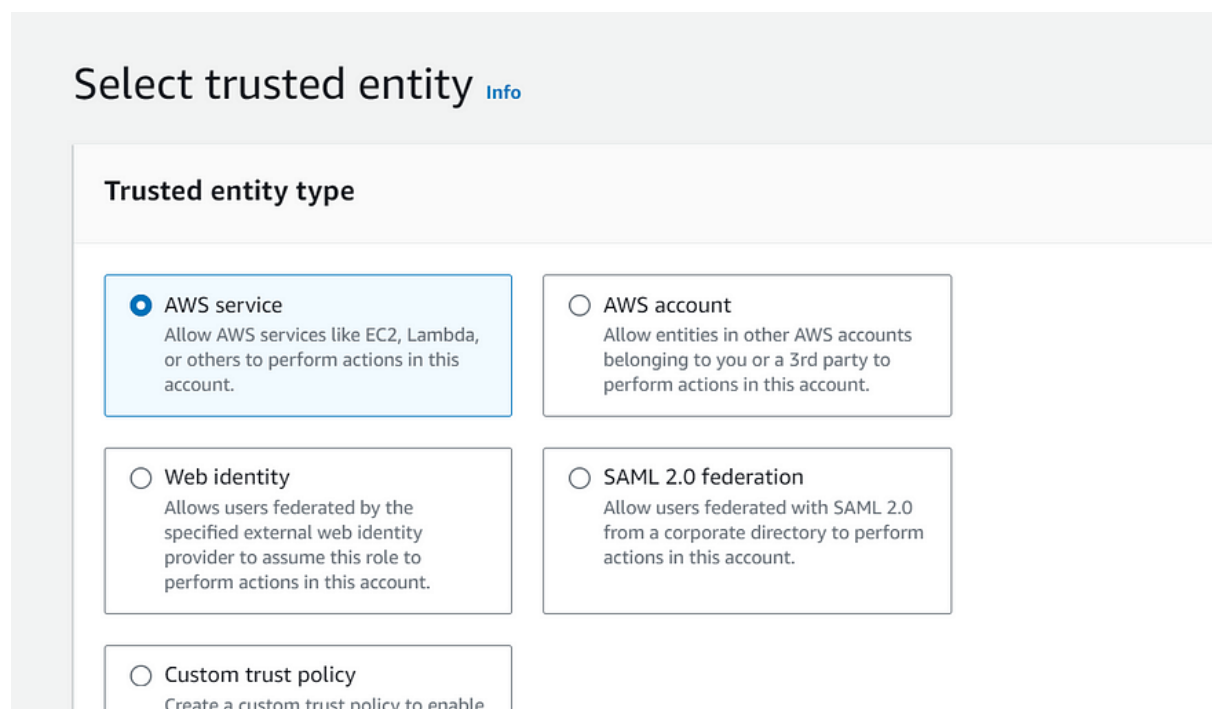
Session Manager is a fully managed AWS Systems Manager capability that lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. You can use Session Manager to start a session with an instance in your account. After the session is started, you can run bash commands as you would through any other connection type.

Create an IAM instance profile for Systems Manager

1. Sign in to the AWS Management Console and open the [IAM console](#). In the navigation pane, choose Roles, and then choose Create role



2. Keep AWS Service for Trusted Entity type



3. Use case select EC2 and click Next

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.

☐ EC2 Role for AWS Systems Manager

4. On the Attach permissions policies page, do the following:

Use the Search field to locate the

AmazonSSMManagedInstanceCore. Select the box next to its name. Choose Next.

Add permissions [Info](#)

Permissions policies (1/882) [Info](#)

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

Q AmazonSSMManagedInstanceCore X


Filter by Type

All types

1 match

< 1 >

⚙

<input checked="" type="checkbox"/>	Policy name ↗	Type	Description
<input checked="" type="checkbox"/>	 AmazonSSMManagedInstanceCore	AWS managed	The policy for Amazon EC2 Role to ena..

► Set permissions boundary - *optional*

Cancel

Previous

Next

5. For Role name, enter a name for your new instance profile, such as **SSMInstanceRole**. Choose Create role. The system returns you to

Role details

Role name
Enter a meaningful name to identify this role.

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

Description
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Step 1: Select trusted entities

Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    }  
15  ]  
16 }
```


Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

Step 3: Add tags

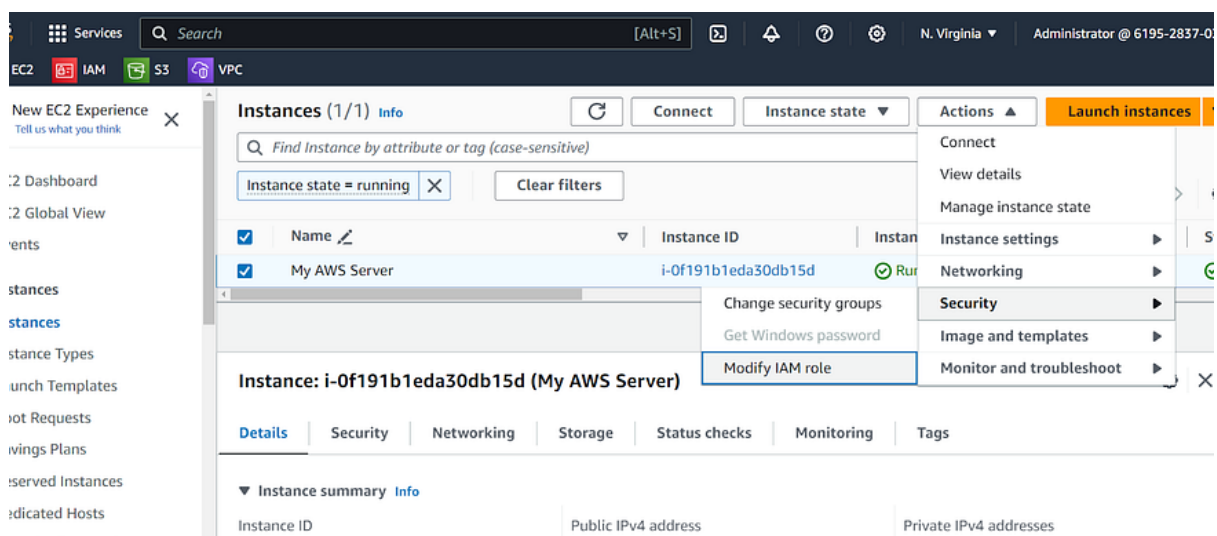
Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

6. Move to EC2 console and In the navigation pane, under Instances, choose Instances. Choose your EC2 instance from the list and click Actions, go to Security and Modify IAM Role




7. Choose SSMInstanceRole and click Update IAM Role.

EC2 > Instances > i-Of191b1eda30db15d > Modify IAM role

Modify IAM role [Info](#)


Attach an IAM role to your instance.



Instance ID

 i-Of191b1eda30db15d (My AWS Server)

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.

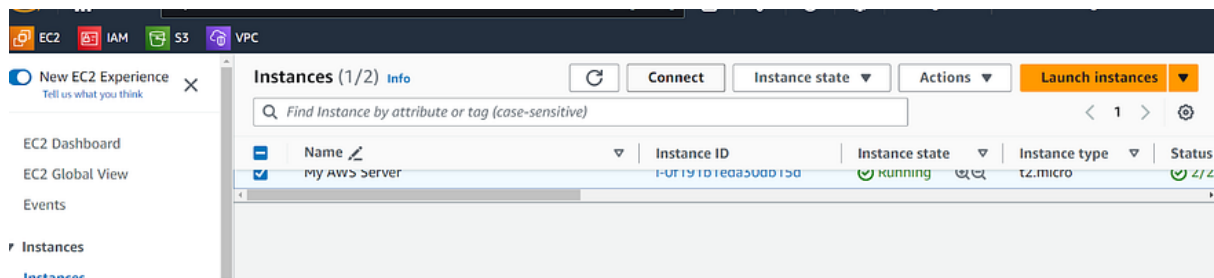


 [Create new IAM role](#) 

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

[Connect to your Linux instance using Session Manager](#)

1. In the EC2 instance console, select the instance you want to connect to, and then click the Connect button.

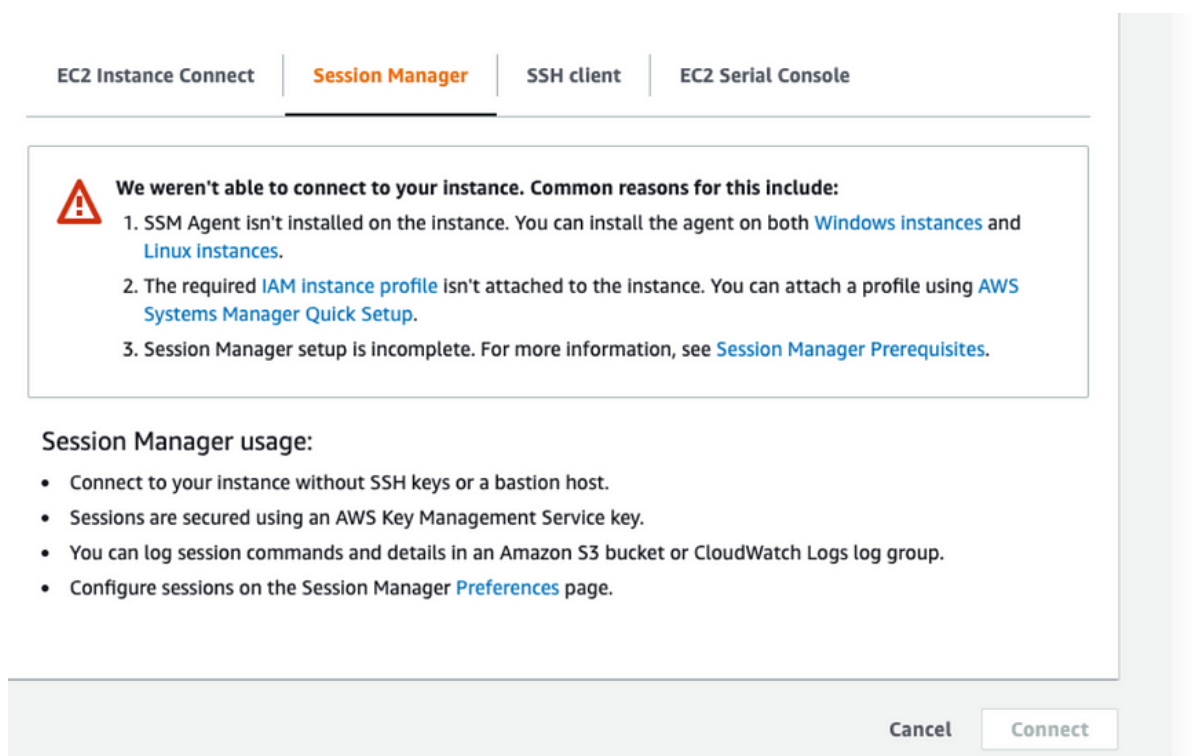


2. In the Connect to instance page, select Session Manager.
- Follow the instructions below.

3. Review the Session Manager usage section for advantages of using Session Manager.


4. Choose Connect. A new session will be started in a new tab.

After the session is started, you can run bash commands as you would through any other connection type.



The screenshot shows the AWS Management Console interface for connecting to an EC2 instance. At the top, there are four tabs: "EC2 Instance Connect", "Session Manager" (which is selected and highlighted in orange), "SSH client", and "EC2 Serial Console". Below the tabs, a large error message is displayed in a white box with a red warning icon. The message states: "We weren't able to connect to your instance. Common reasons for this include:" followed by three numbered points. Below the error message, there is a section titled "Session Manager usage:" with a bulleted list of four items. At the bottom right of the console, there are two buttons: "Cancel" and "Connect".

EC2 Instance Connect | **Session Manager** | SSH client | EC2 Serial Console

 **We weren't able to connect to your instance. Common reasons for this include:**

1. SSM Agent isn't installed on the instance. You can install the agent on both [Windows instances](#) and [Linux instances](#).
2. The required [IAM instance profile](#) isn't attached to the instance. You can attach a profile using [AWS Systems Manager Quick Setup](#).
3. Session Manager setup is incomplete. For more information, see [Session Manager Prerequisites](#).

Session Manager usage:

- 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.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel Connect