



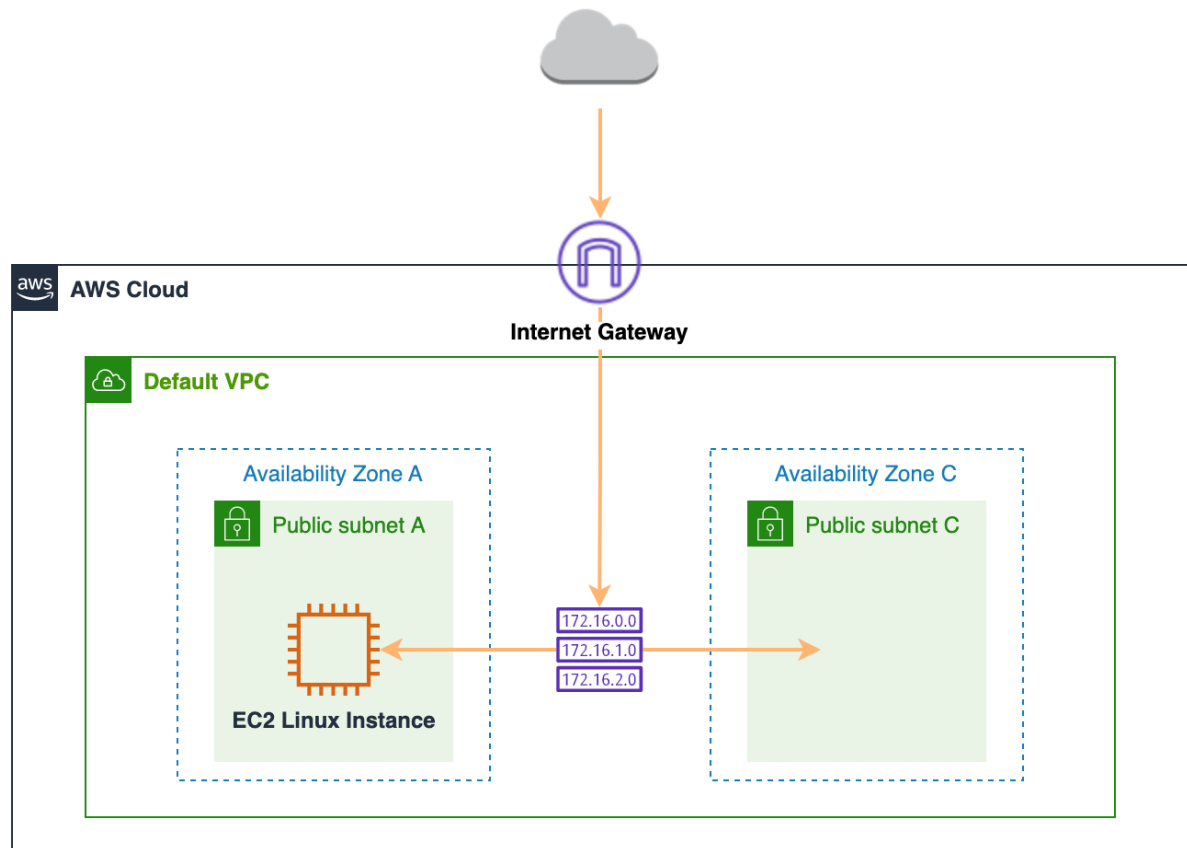
General Immersion Day

Lab 1

EC2 Linux Hands on Lab

Amazon EC2 Overview

Amazon EC2 provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.



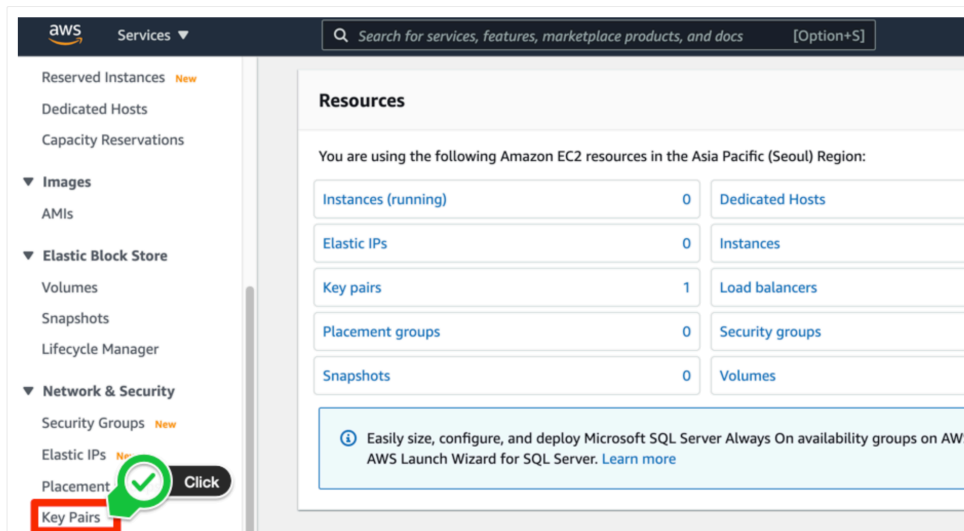
Create your own web server by going through the labs in the order below:

1. [Create a new key pair](#)
2. [Launch a Web Server Instance](#)
3. [Connect to your linux instance](#)
4. [Connect to your Linux instance using Session Manager](#)

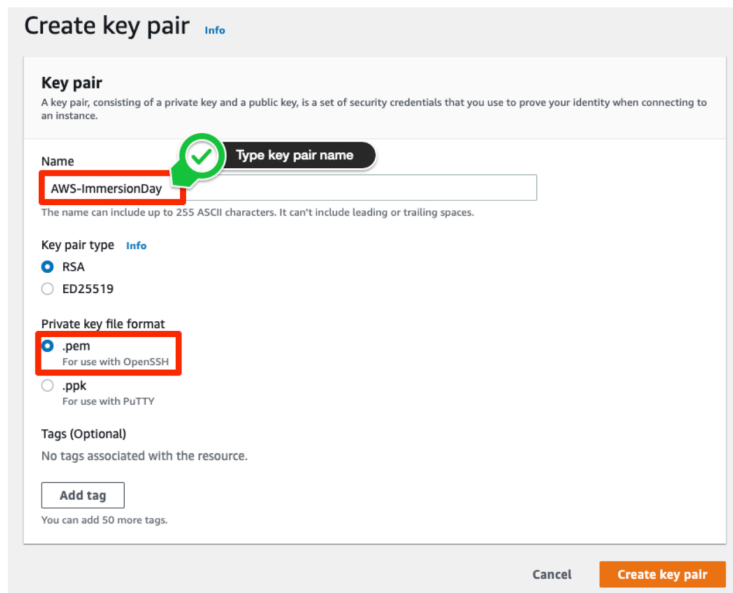
1-1 Create a new Key Pair

In this lab, you will need to create an EC2 instance using an SSH keypair. The following steps outline creating a unique SSH keypair for you to use in this lab.

1. Sign into the AWS Management Console and open the **Amazon EC2 console**. In the upper-right corner of the AWS Management Console, confirm you are in the desired AWS region.
2. Click on **Key Pairs** in the Network & Security section near the bottom of the leftmost menu. This will display a page to manage your SSH key pairs.



3. To create a new SSH key pair, click the **Create key pair** button at the top of the browser window.

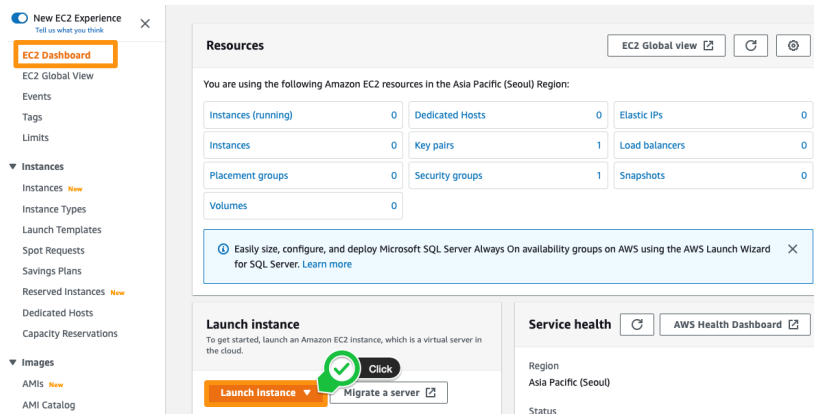


4. Type **[Your Name]-ImmersionDay** into the Key Pair Name: text box and click **Create key pair** button. For Windows users, please select **ppk** for file format.
5. The page will download the file **[Your Name]-ImmersionDay.pem** to the local drive. Follow the browser instructions to save the file to the default download location. Remember the full path to the key pair file you just downloaded.

1-2 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 instances**.



2. In **Name**, put the value **Web server for IMD**. And check the default setting for Amazon Machine Image below.

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


[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


Recents

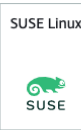
Quick Start











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

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-0cbec04a61be382d9 (64-bit (x86)) / ami-0386e0bbb1ac2e393 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220426.0 x86_64 HVM gp2

Architecture

AMI ID

64-bit (x86) ▼

ami-0cbec04a61be382d9

3. Select **t2.micro** in Instance Type.

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0144 USD per Hour
On-Demand Windows pricing: 0.019 USD per Hour

Free tier eligible

[Compare instance types](#)

4. Select the key pair that you created in the beginning of this lab from the drop-down.

▼ 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-ImmersionDay

↕

[Create new key pair](#)

5. Click the Edit button in Network settings to set the space where EC2 will be located.

▼ Network settings [Edit](#)

Network

vpc-0587c58f5e4d82b38

Subnet

No preference (Default subnet in any availability zone)

Auto-assign public IP

Enable

Security groups (Firewall) [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.

We'll create a new security group called 'launch-wizard-1' 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

☐ Allow HTTP traffic from the internet

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

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

✕

Check **default VPC** and **subnet**. **Auto-assign public IP** is set to **Enable**. Right below it, create **Security groups** to act as a network firewall. Security groups will specify the protocols and addresses you want to allow in your firewall policy. For the security group you are currently creating, this is the rule that applies to the EC2 that will be created. After entering *Immersion Day - Web Server* in Security group name and Description, select Add Security group rule and set HTTP to Type.

▼ Network settings

VPC - required [Info](#)

vpc-0587c58f5e4d82b38 (default) ↕
172.31.0.0/16

Subnet [Info](#)

subnet-059b9087c44372eaf
VPC: vpc-0587c58f5e4d82b38 Owner: 025482651656
Availability Zone: ap-northeast-2a IP addresses available: 4091

↕ Create new subnet [↗](#)

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

Security group name - required

Immersion Day - Web Server

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 _-:/!@#,%&*~`

Description - required [Info](#)

Immersion Day - Web Server

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 54.239.119.3/32)

Remove

Type [Info](#)

ssh ↕

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

My IP ↕

Source [Info](#)

X

Description - optional [Info](#)

Add security group rule

✓ Add security group

► Advanced network configuration

Also allow TCP/80 for Web Service and TCP/443 by specifying it. Select **My IP** in the source.

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 194.223.129.6/32)

Remove

Type [Info](#)

ssh ▼

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

My IP ▼

Source [Info](#)

🔍 Add CIDR, prefix list or security

194.223.129.6/32 ✕

Description - optional [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 194.223.129.6/32)

Remove

Type [Info](#)

HTTP ▼

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source type [Info](#)

My IP ▼

Source [Info](#)

🔍 Add CIDR, prefix list or security

194.223.129.6/32 ✕

Description - optional [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 443, 194.223.129.6/32)

Remove

Type [Info](#)

HTTPS ▼

Protocol [Info](#)

TCP

Port range [Info](#)

443

Source type [Info](#)

My IP ▼

Source [Info](#)

🔍 Add CIDR, prefix list or security

194.223.129.6/32 ✕

Description - optional [Info](#)

e.g. SSH for admin desktop

6. All other values accept the default values, expand by clicking on the **Advanced Details** tab at the bottom of the screen. Enter the following values in the **User data** field and select **Launch instance**.

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

1x

GiB

▼

Root volume

ⓘ

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

×

Add new volume

0 x File systems

[Edit](#)

▶ **Advanced details** [Info](#)

User data [Info](#)

```
#!/bin/sh

# Install a LAMP stack
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum -y install 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.tar.gz ]; then
    cd /var/www/html
    wget https://aws-joozero.s3.ap-northeast-2.amazonaws.com/immersion-day-app-php7.tar.gz
    tar xvfz immersion-day-app-php7.tar.gz
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
    unzip aws.zip
fi

# Update existing packages
yum -y update
```

Note: Do **not** copy and paste the codes from this manual into the **User Data** field. Please make sure to download the file “ec2bootstrap.txt” and copy the codes from there.


```
#!/bin/sh

# Install a LAMP stack
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum -y install 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.tar.gz ]; then
    cd /var/www/html
    wget https://aws-joozero.s3.ap-northeast-2.amazonaws.com/immersion-day-app-php7.tar.gz
    tar xvfz immersion-day-app-php7.tar.gz
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
    unzip aws.zip
fi

# Update existing packages
yum -y update
```

- 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.

The screenshot shows the AWS Management Console interface. At the top, there's a header with 'Instances (1/1)' and a search bar. Below this is a table of instances. The first instance, 'Web server for IMD', is highlighted with a blue row and its name is also highlighted with an orange box. The instance is in a 'Running' state, using a 't2.micro' instance type, and has '2/2 checks passed'. Below the table, the details for the selected instance 'i-089d22683ed0fc34e (Web server for IMD)' are shown. The 'Details' tab is active, displaying the instance summary. The 'Public IPv4 DNS' field is highlighted with an orange box, showing the address 'ec2-35-210-158.ap-northeast-2.compute.amazonaws.com'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Web server for IMD	i-089d22683ed0fc34e	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-089d22683ed0fc34e (Web server for IMD)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary

Instance ID i-089d22683ed0fc34e (Web server for IMD)	Public IPv4 address 3.35.210.158 open address	Private IPv4 addresses 172.31.43.213
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-35-210-158.ap-northeast-2.compute.amazonaws.com open address

Browse the Web Server

Wait for the instance to pass the Status Checks to finish loading. Open a new browser tab and browse the Web Server by entering the EC2 instance's **Public DNS name** into the browser.

Note: Remove "S" from HTTPS. Browse with HTTP instead.

The EC2 instance's Public DNS name can be found in the console by reviewing the **Public IPv4 DNS** name line highlighted above. You should see a website that looks like the following.



LOAD TEST	RDS
Meta-Data	Value
InstanceId	i-0f9c0154bbc266ca9
Availability Zone	ap-northeast-2c

Current CPU Load: 1%

Great Job! You have deployed a server and launched a web site in a matter of minutes!

1-3 Connect to your Linux Instance using Session Manager

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**.

The image shows two screenshots of the AWS IAM console. The top screenshot is the IAM dashboard, and the bottom screenshot is the Roles page.

IAM dashboard

Security recommendations 1

Add MFA for root user
Enable multi-factor authentication (MFA) for the root user to improve security for this account.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	1	18	3	0

What's new [View all](#)

- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 4 months ago
- IAM Access Analyzer helps you generate IAM policies based on access activity found in your organization trail. 4 months ago
- IAM Access Analyzer adds new policy checks to help validate conditions during IAM policy authoring. 6 months ago
- AWS Amplify announces support for IAM permissions boundaries on Amplify-generated IAM roles. 6 months ago

[more](#)

IAM Roles

Roles (18) [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.

[Search](#)

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForAmazonElasticsearchService	AWS Service: es (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_AppStreamFleet	AWS Service: appstream.application-autoscaling (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest	AWS Service: ec2.application-autoscaling (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_ECSService	AWS Service: ecs.application-autoscaling (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_RDSInstance	AWS Service: rds.application-autoscaling (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForAuditManager	AWS Service: auditmanager (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForAWSCloud9	AWS Service: cloud9 (Service-Linked Role)	-

- Under **Select type of trusted entity**, choose **AWS service**. Immediately under **Choose the service that will use this role**, choose **EC2**, and then choose **Next**.

Select trusted entity

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

Cancel **Next**

- 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

Permissions policies (Selected 1/736)
Choose one or more policies to attach to your new role.

1 match

☒ "AmazonSSMManagedInstanceCore" X

<input checked="" type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	AmazonSSMManag...	AWS m...	The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.

► **Set permissions boundary - optional**
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.

Cancel Previous **Next**

- For **Role name**, enter a name for your new instance profile, such as **SSMInstanceProfile**. Choose **Create role**. The system returns you to the **Roles** page.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

SSMInstanceProfile

Maximum 128 characters. Use alphanumeric and '+=, @-.' characters.

Description

Add a short explanation for this policy.

Allows EC2 instances to call AWS services on your behalf.

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

Step 1: Select trusted entities


Edit

```
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 }
```

Step 2: Add permissions

Edit

Permissions policy summary

Policy name 	Type	Attached as
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

Tags

Add tags (Optional)

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 tag

You can add up to 50 more tags

Cancel

Previous

Create role

Make a note of the role name. You will choose this role when you create new instances that you want to manage by using Systems Manager.

Attach the Systems Manager instance profile to an existing instance (console)

1. Sign in to the AWS Management Console and open the Amazon EC2 console at [Amazon EC2 console](#).
2. In the navigation pane, under **Instances**, choose **Instances**. Choose your EC2 instance from the list and click Actions.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type
Web server for custom AMI	i-0addafa0b1b733810	Running	t2.micro

Instance: i-0addafa0b1b733810 (Web server for custom AMI)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary Info

Instance ID i-0addafa0b1b733810 (Web server for custom AMI)	Public IPv4 address 18.208.167.131 open address	Private IPv4 addresses 172.31.92.202
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-18-208-167-131.compute-1.amazonaws.com open address

3. In the **Actions** menu, choose **Security, Modify IAM role**.

Instances (1/1) Info

Name	Instance ID
Web server for custom AMI	i-0a03b2d86fad9a1

Actions menu options:

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

4. For IAM role, select the instance profile you created **SSMInstanceProfile**.

EC2 > Instances > i-077a60e25bcc216ad > Modify IAM role

Modify IAM role Info

Attach an IAM role to your instance.

Instance ID
i-077a60e25bcc216ad (Web server for IMD)

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.

SSMInstanceProfile

[Create new IAM role](#)

Cancel **Update IAM role**

5. Choose **Update IAM role**.

EC2 > Instances > i-0a03b2d86fad9a1d6 > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
i-0a03b2d86fad9a1d6 (Web server for custom AMI)

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.

SSMInstanceProfile ▼ [Create new IAM role](#)

Cancel **Save**

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.

Instances (1/1) [Info](#) [Refresh](#) **Connect** Instance state ▼ Actions ▼ **Launch instances** ▼

Filter instances

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability zone
<input checked="" type="checkbox"/>	Web server for custom AMI	i-0f9c0154bbc266ca9	Running	t2.micro	2/2 checks passed...	No alarms	ap-northeast-1

1. Check 2. Click

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

EC2 > Instances > i-0addafa0b1b733810 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-0addafa0b1b733810 (Web server for custom AMI) using any of these options

[Click](#)

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

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**

Feedback English (US) © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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.

EC2 > Instances > i-0a03b2d86fad9a1d6 > Connect to Instance

Connect to instance [Info](#)

Connect to your instance i-0a03b2d86fad9a1d6 (Web server for custom AMI) 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 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**


Note: If you receive an error like shown below, wait for few seconds and refresh your browser. Behind the scenes the EC2 instance is being setup for use with Session Manager

EC2 > Instances > i-034588912ae28c8ae > Connect to Instance

Connect to instance [Info](#)

Connect to your instance i-034588912ae28c8ae using any of these options

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**