

**Running an Intelligent Analytical System on AWS**

**Using AWS Services & Solutions in AWS Marketplace**

*Prerequisites Guide*

Table of Contents

1. Setup AWS Account 3

1.1. Create an AWS Account 3

1.2. Create Identity and Access Management (IAM) Users 4

1.3. Assign Policies and Set Password 8

1.4. Generate your Private Keys 12

User Reference — Starting and Stopping EC2 Instances 14

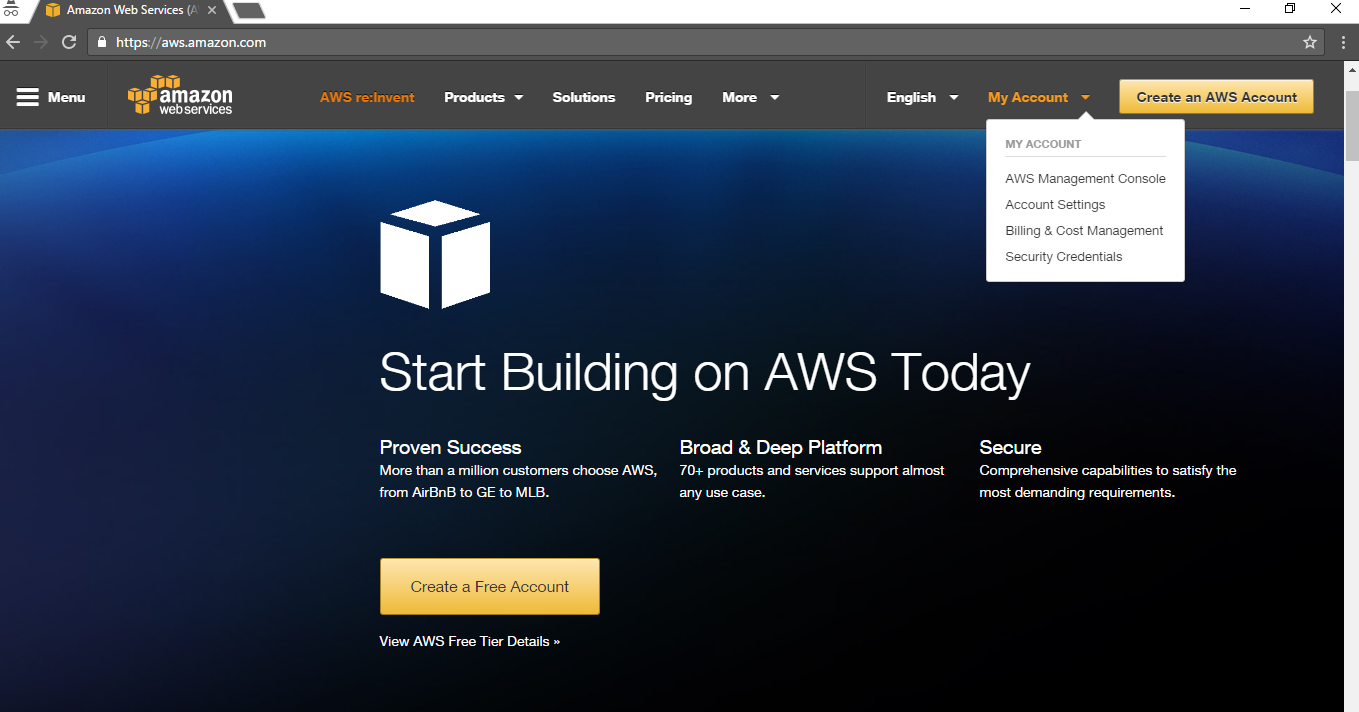
2.1. Starting the Instance: 14

2.2. Stopping the Instance 15

# Setup AWS Account

## Create an AWS Account

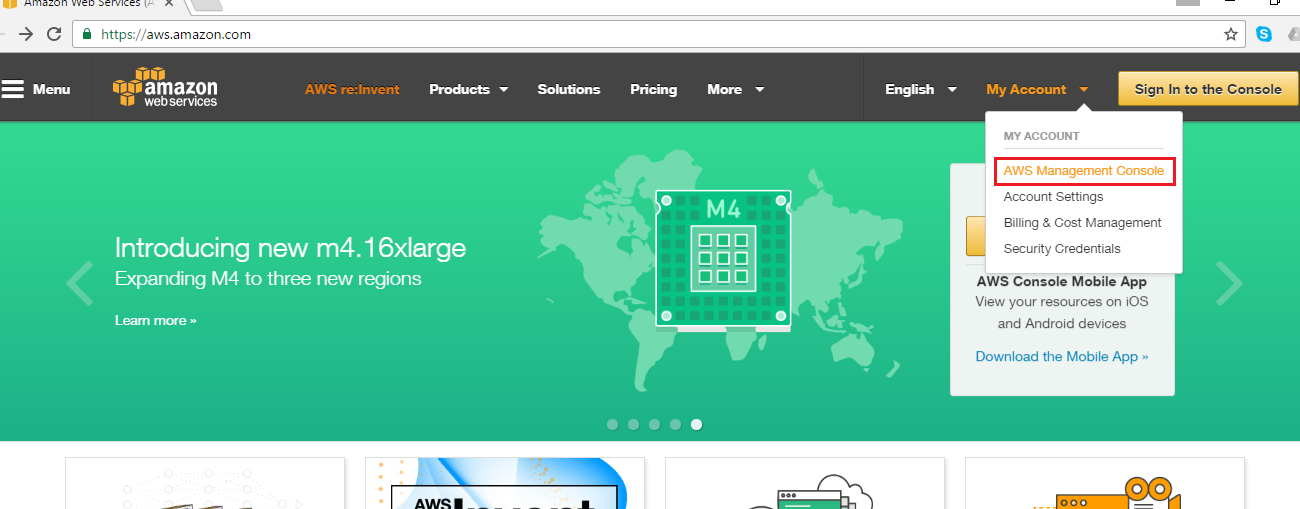
1. Open <http://aws.amazon.com/>
2. Click on the **Create an AWS Account** button present at upper right corner of **AWS home page**.
3. Follow the online instructions.
4. Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

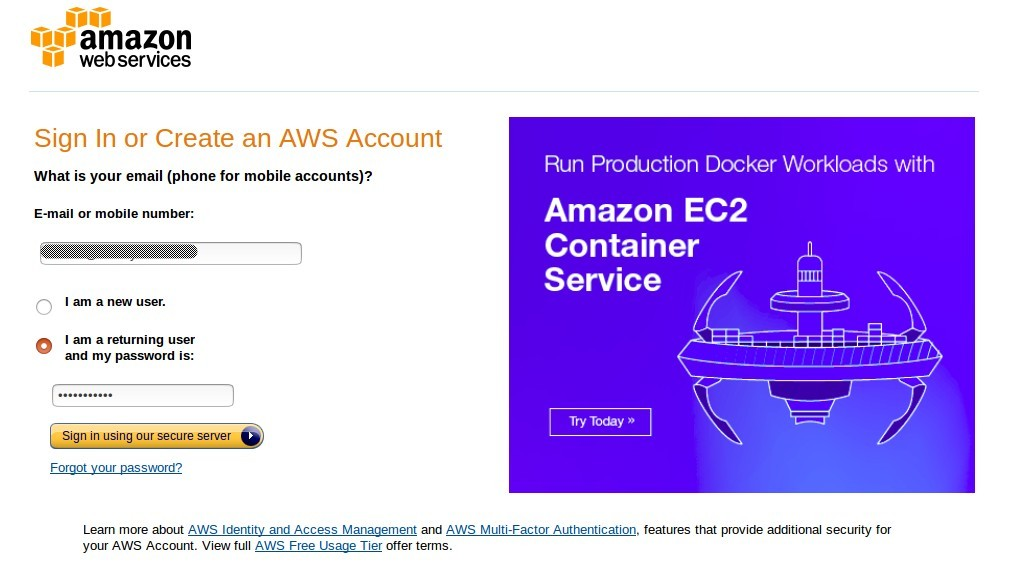


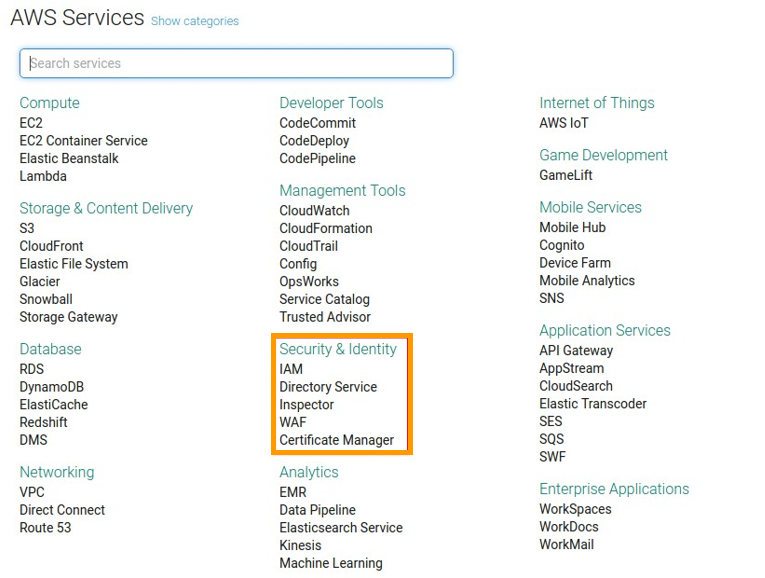
## Create Identity and Access Management (IAM) Users

You can create one or more IAM users in your AWS account. You might create an IAM user when someone joins your organization, or when you have a new application that needs to make API calls to AWS.

1. Visit <http://aws.amazon.com/>
2. Click the **My Account** button present on right side of upper menu bar.
3. Select **AWS Management Console** from the dropdown list to open **Identity and Access Management (IAM) console**.



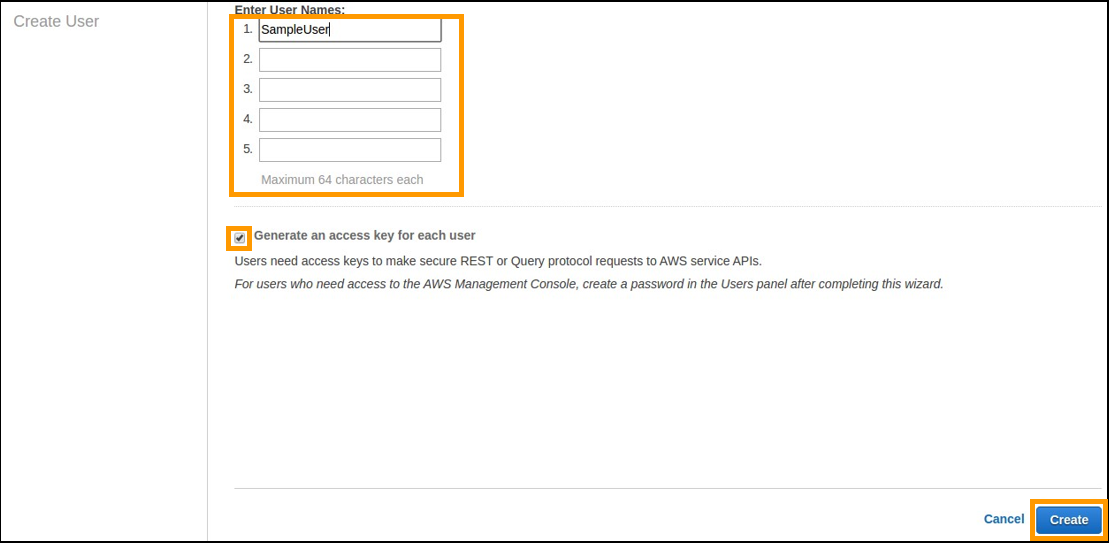
1. Enter the **E-Mail id** used for creating the AWS account in Sub-Section 1.1.
2. Select the Radio option “**I am a returning user and my password is:”**
3. Enter the Password and hit **Sign in using our secure server** button.
4. Click on the **IAM** link listed under **Security & Identity** AWS Service.



1. In the navigation pane, choose **Users** and then choose **Create New Users**.



This will open up a page as shown below.



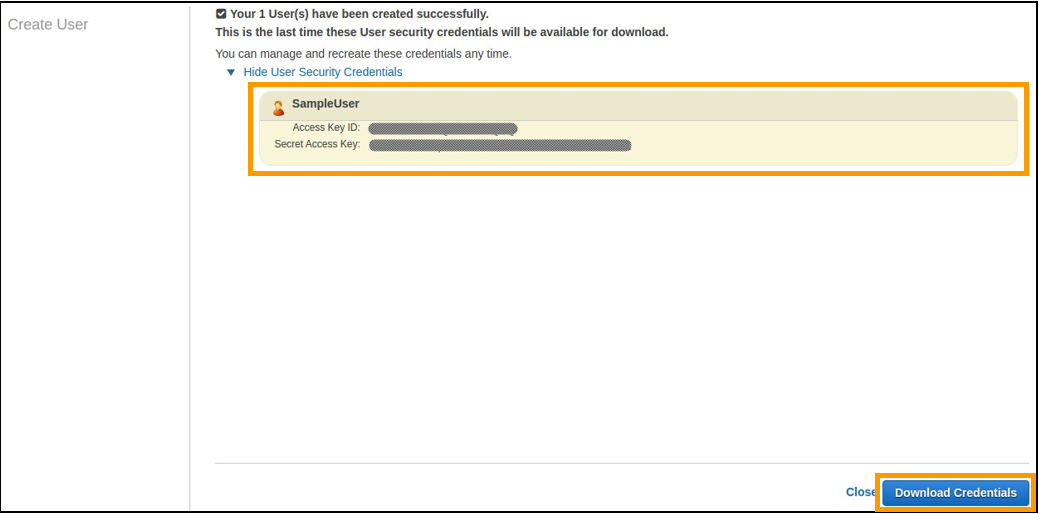
In the page above, fill in the information mentioned under the 3 points (9, 10 and 11) below:

1. Type the user names for the users to create. You can create up to five users at one time.
2. If the users require access to the API, AWS CLI, or Tools for Windows PowerShell, then they must have access keys. To generate an access key for new users at this time, select **Generate an access key for each user**.
3. Press the **Create** button.

Once the users are created, it will redirect you to the **Download Credentials** page.

You will find the **Access Key** and the **Secret Key** have been generated.

1. Now download the keys by clicking on the **Download Credentials button.**
2. Save the file to a safe location on your computer.



1. Click on the **Close** button at the bottom of the screen to navigate back to the IAM Dashboard.

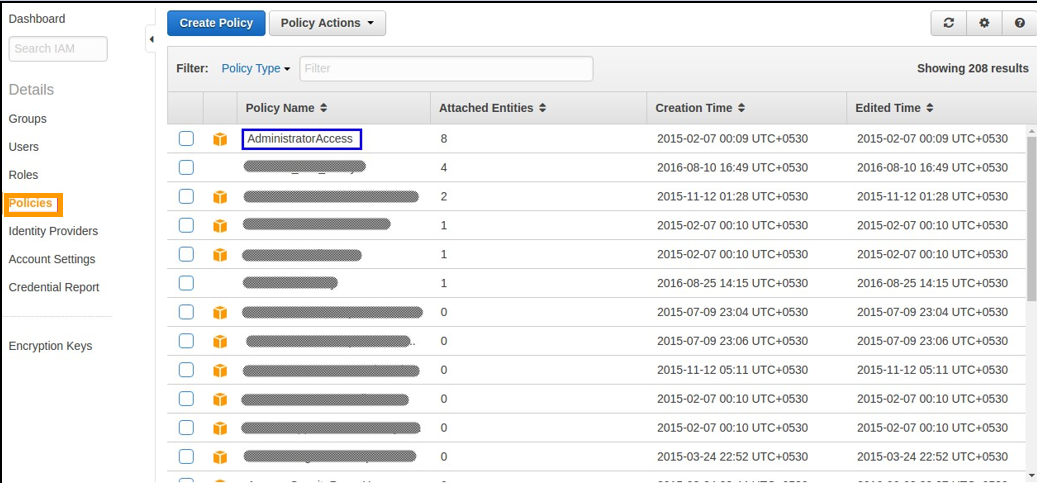
## Assign Policies and Set Password

A policy is a document that formally states one or more permissions.

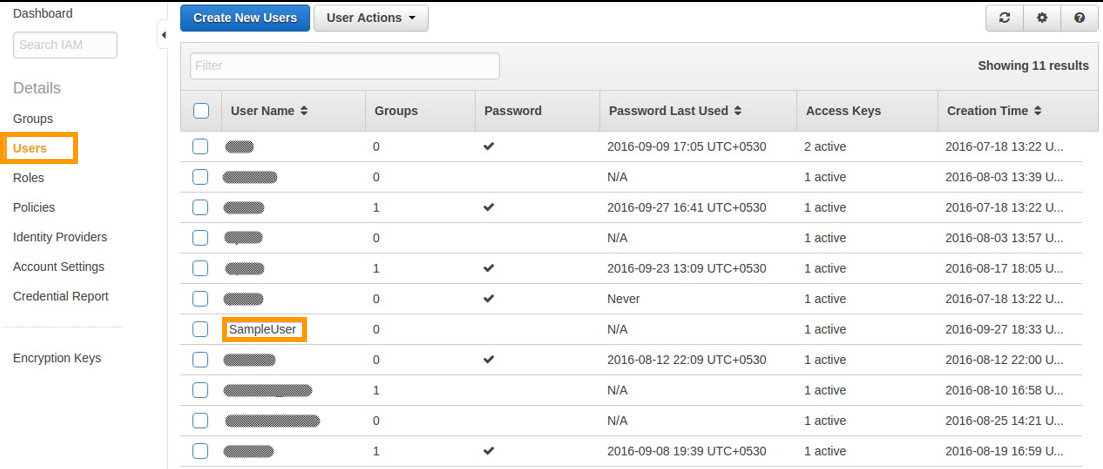
1. In the Navigation pane, choose **Policies.**

It will open up a tab, where you can see the list of all the defined policies. You can create your own custom policy by clicking on the button **Create Policy** (shown above in the image).

In this lab, we used an already-defined policy – **Administrator Access** (see the blue box in the image below).

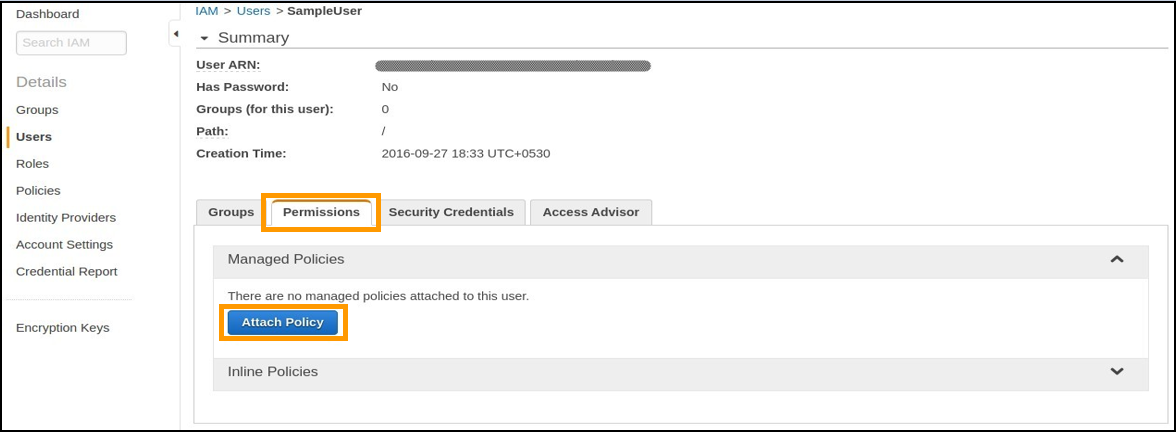


1. In the Navigation pane, choose **Users.**
2. Click on the name of the user from the users list to whom you want to attach a policy.

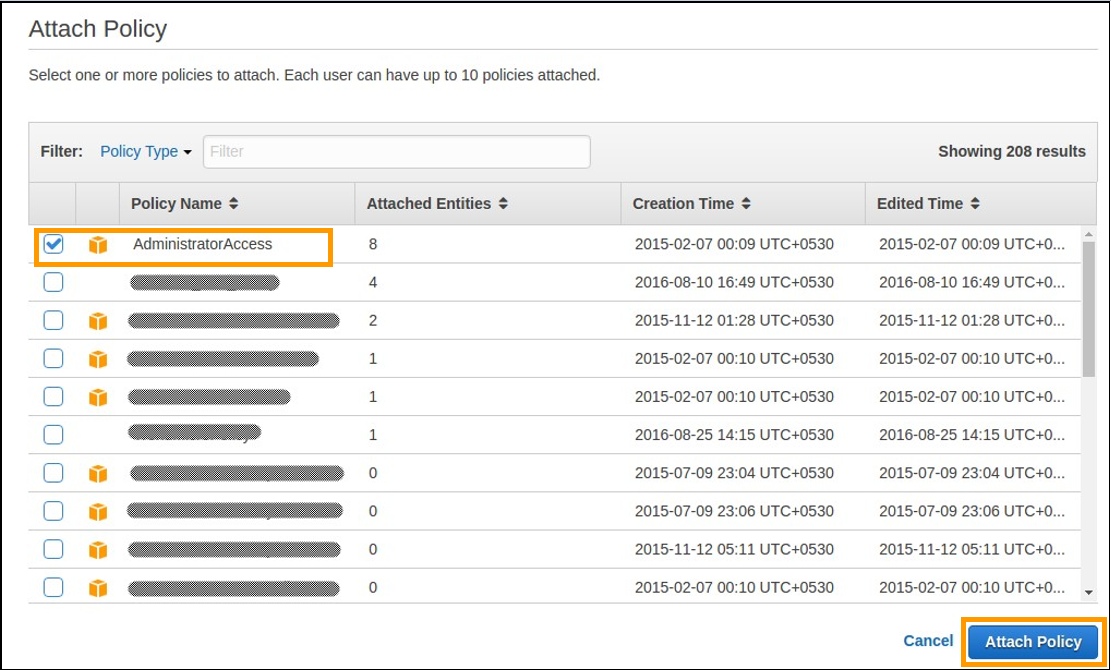


This will open the summary page of user’s details containing four tabs: **Groups, Permissions, Security Credentials,** and **Access Advisor**.

1. To attach the policy, click on the **Permissions** tab.

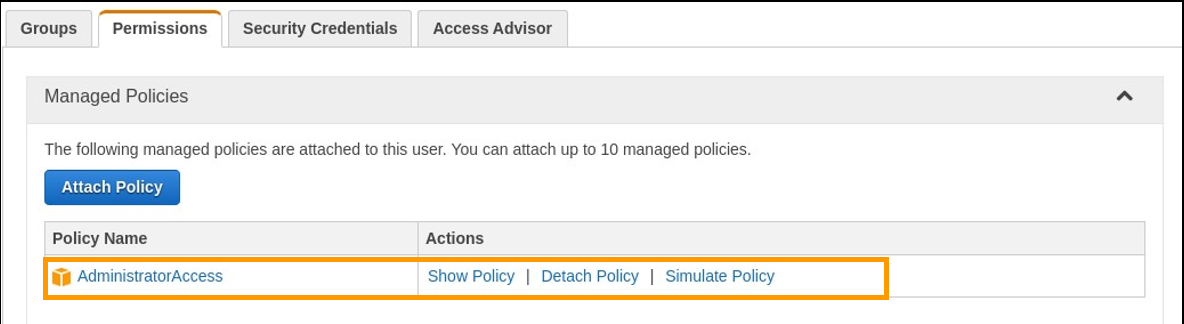


1. Now click the **Attach Policy** button. It will bring up the list of all defined policies.
2. Select **Administrator Access** policy by checking the check box next to the name of policy.

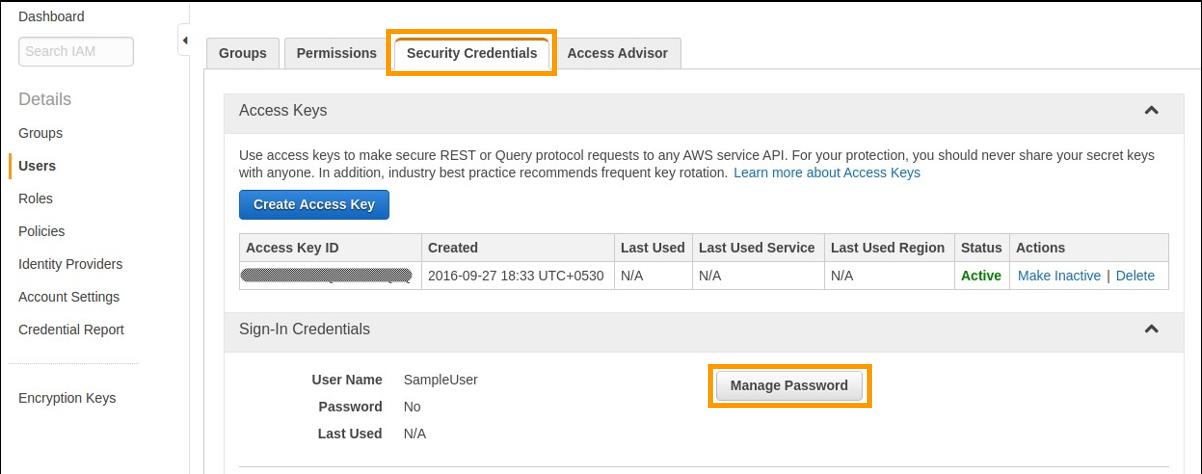


1. Press the **Attach Policy** button present at the bottom.

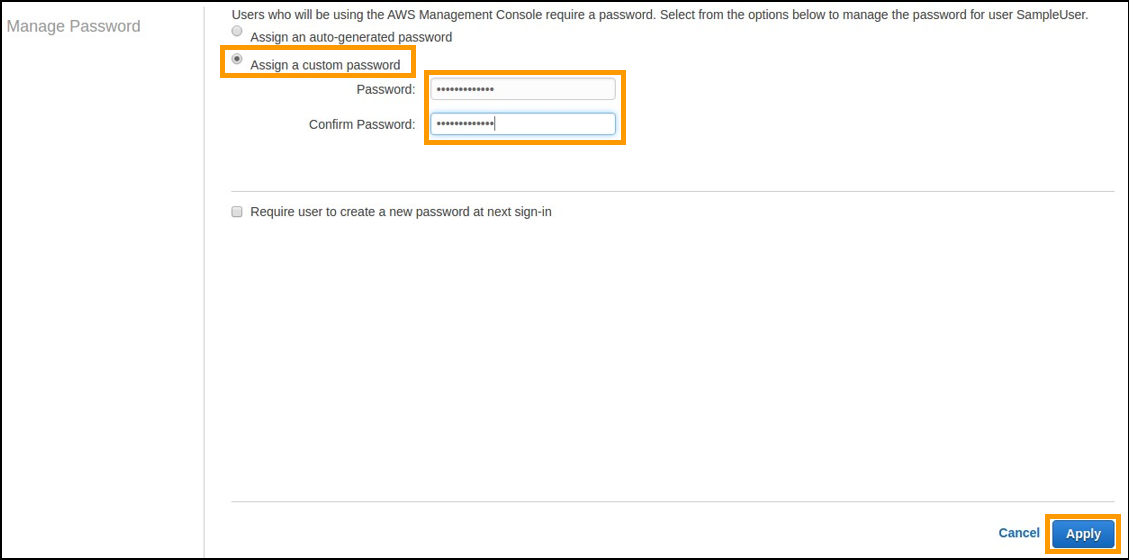
After the successful attachment of a policy, the name of the policy will be listed in the **Permissions** tab as shown in the image below.



1. Select the **Security Credentials** tab.
2. Click the **Manage Password** button.



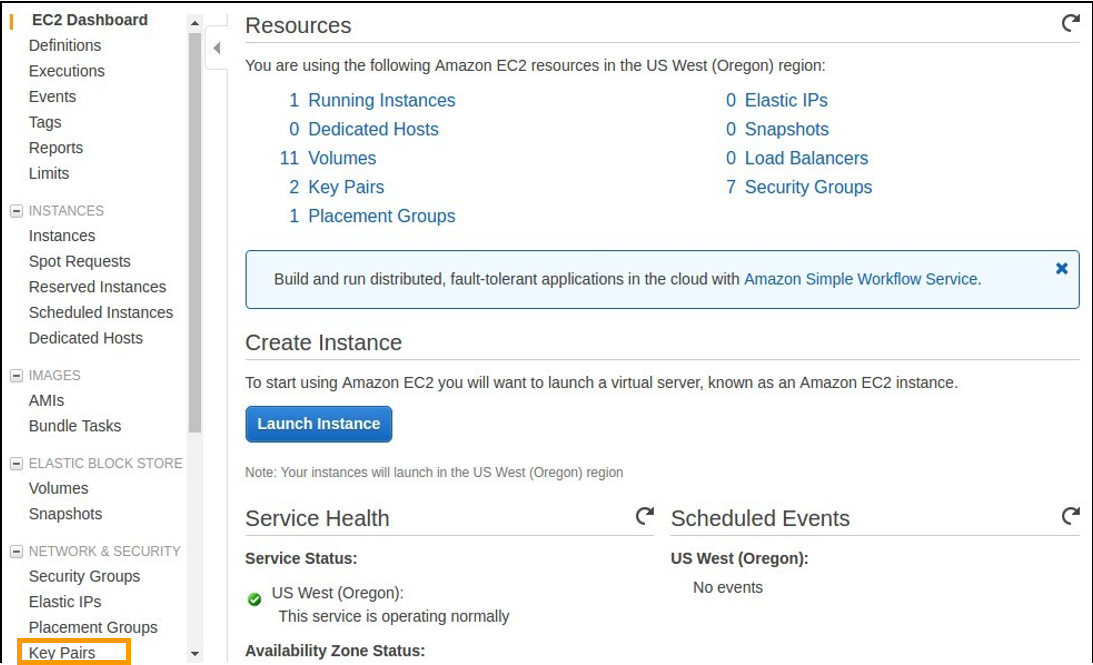
1. In the **Manage Password** tab, select the radio button **Assign a custom password**.
2. Set the Password and hit the **Apply** button present at the bottom of the screen.



## Generate your Private Keys

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

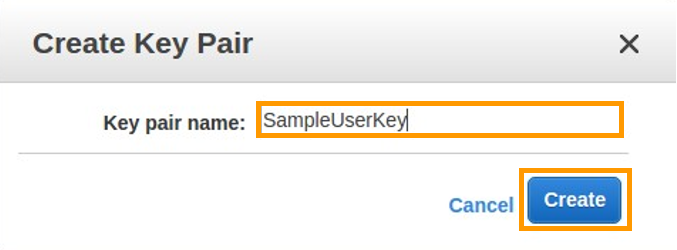
1. Open the **Amazon EC2 console** at <https://console.aws.amazon.com/ec2/>
2. In the navigation pane, under **NETWORK & SECURITY**, choose **Key Pairs**.



1. Press the **Create Key Pair** buttonpresent at the top of the Key Pairs tab.



1. Enter the appropriate name for the key pair in the **Create Key Pair** popup window.

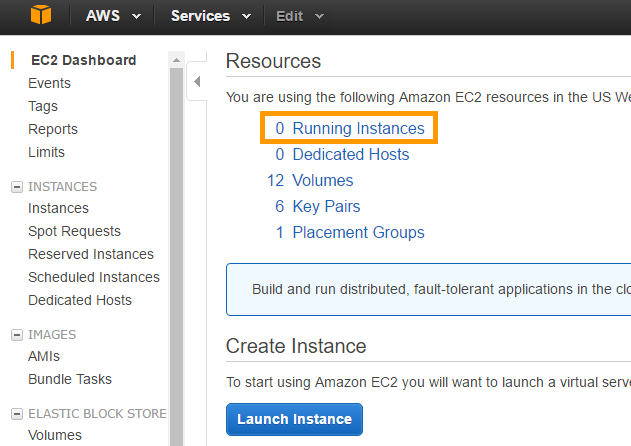


Once you click on the **Create** button, the key pair will be generated, and a file with a “**.pem”** extension containing a private key will be downloaded. Save the file, since you will use this file to login to your EC2 instance remotely.

# User Reference — Starting and Stopping EC2 Instances

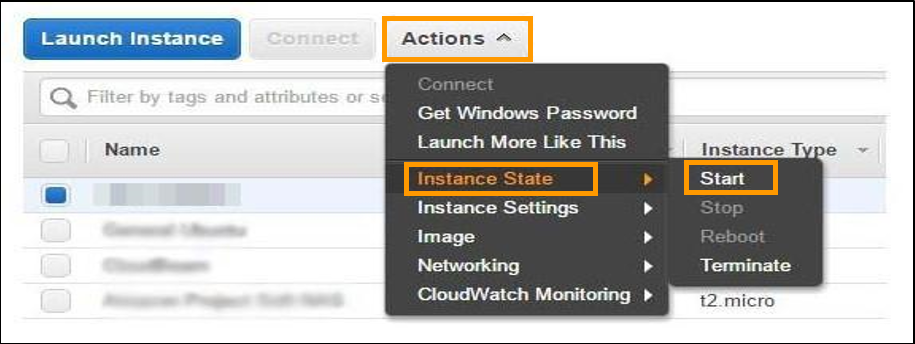
You will be working with EC2 instances as part of the AWS Marketplace Fusion Solution you’re about to build. When you start working with EC2 Instances, you can refer back here for instructions on how to start and stop them.

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>
2. Click on the link **Running Instances** to get a list of all EC2 instances created in an AWS account.



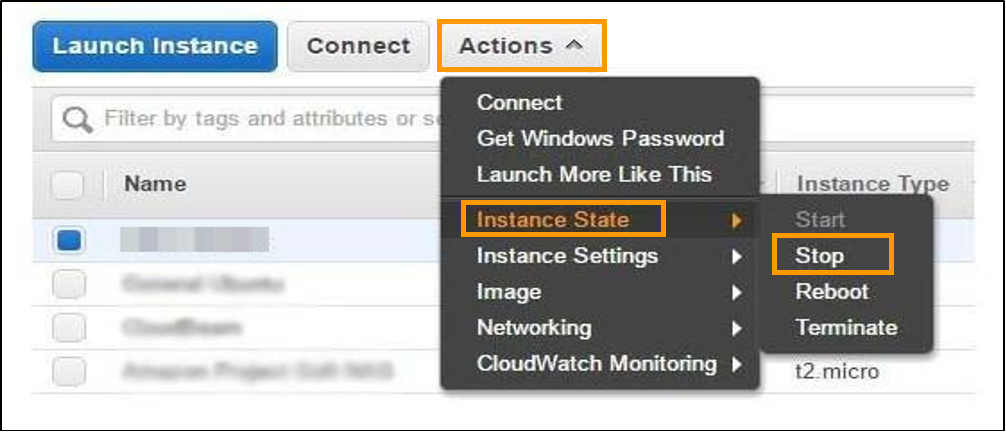
## 2.1. Starting the Instance:

1. Go to the EC2 dashboard.
2. Select an EC2 instance to start.
3. Click on the **Actions** button.
4. Select **Instance State > Start** to start the instance.



## 2.2. Stopping the Instance

1. Go to the **EC2 dashboard**.
2. Select the EC2 instance to stop.
3. Click on the **Actions** button.
4. Select **Instance State > Stop** to stop the instance.



You will get a warning message to confirm whether you want to stop the instance or not, because all the data stored on the ephemeral storage will be lost after stopping the instance. You will get the following message:

