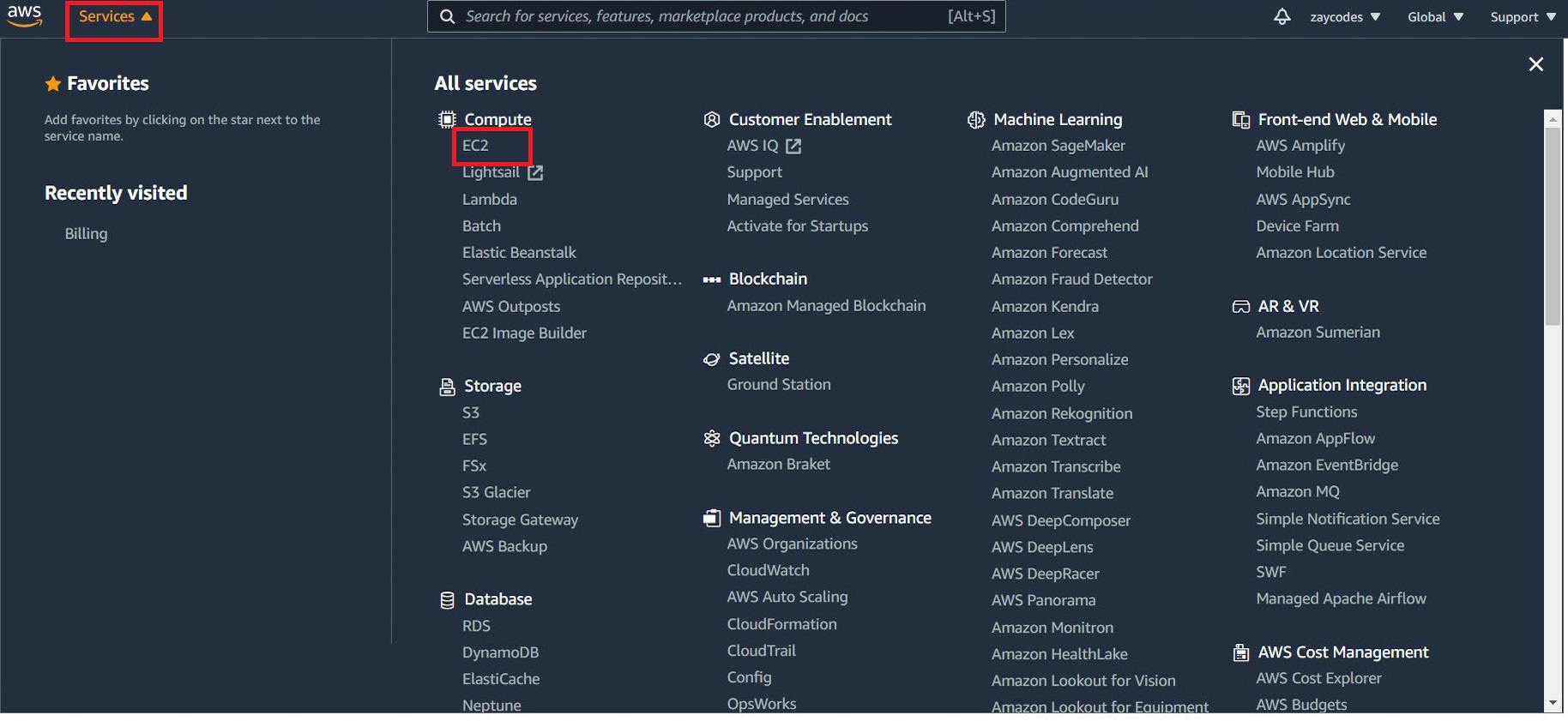
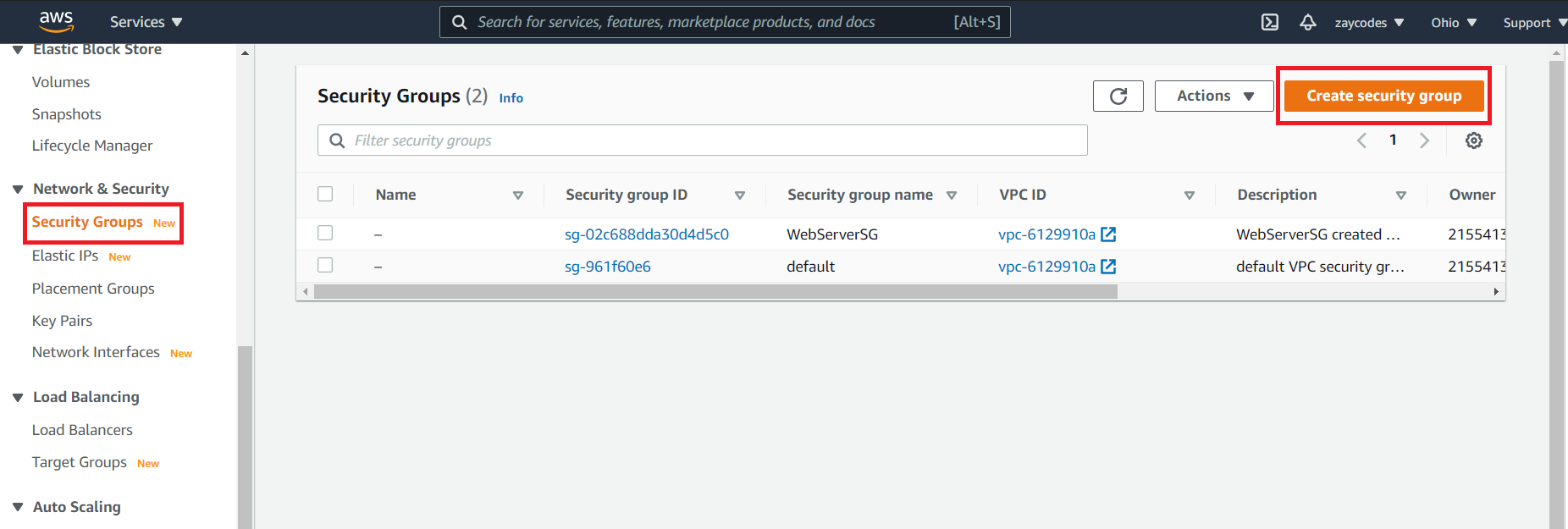
1. Sign in to the [AWS Management Console](https://console.aws.amazon.com/ec2/).
2. Open the Amazon EC2 console by selecting **EC2** under **Compute**.

In the left-hand navigation bar, select **Security Groups**, and then select **Create Security Group**.



1. In **Security group name**, enter **<as your wish>** or any preferred name of your choice, and provide a description.
2. Select your VPC from the list. You can use the default VPC.
3. On the **Inbound tab**, add the rules as follows:
   * Select **Add Rule**, and then select **SSH** from the Type list.
   * Under **Source**, select **Custom**, and in the text box, enter [the IP address from step 1](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#step1-security-group), followed by /32 indicating a single IP Address. For example, 104.34.241.123/32 is a single IP address, while 198.51.100.2/24 results in a range of 256 IP addresses.
   * Select **Add Rule**, and then select **HTTP** from the Type list.
   * Select **Add Rule**, and then select **Custom TCP Rule** from the Type list.
   * Under **Port Range**, enter **8080**.
4. Select Create.

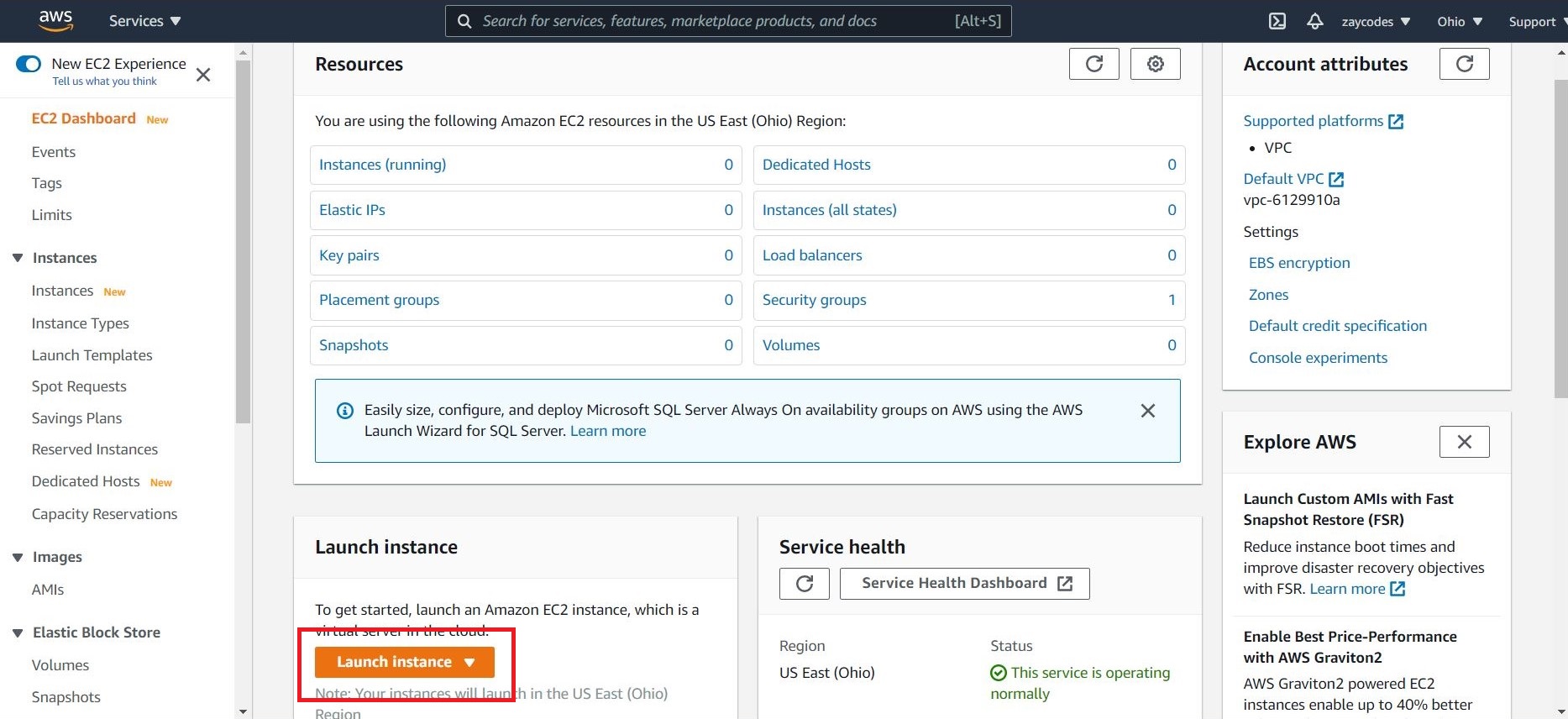
For more information, refer to [Security Groups](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html) in the Amazon EC2 User Guide for Linux Instances.

Launching an Amazon EC2 instance

Now that you have configured a key pair and security group, you can launch an EC2 instance.

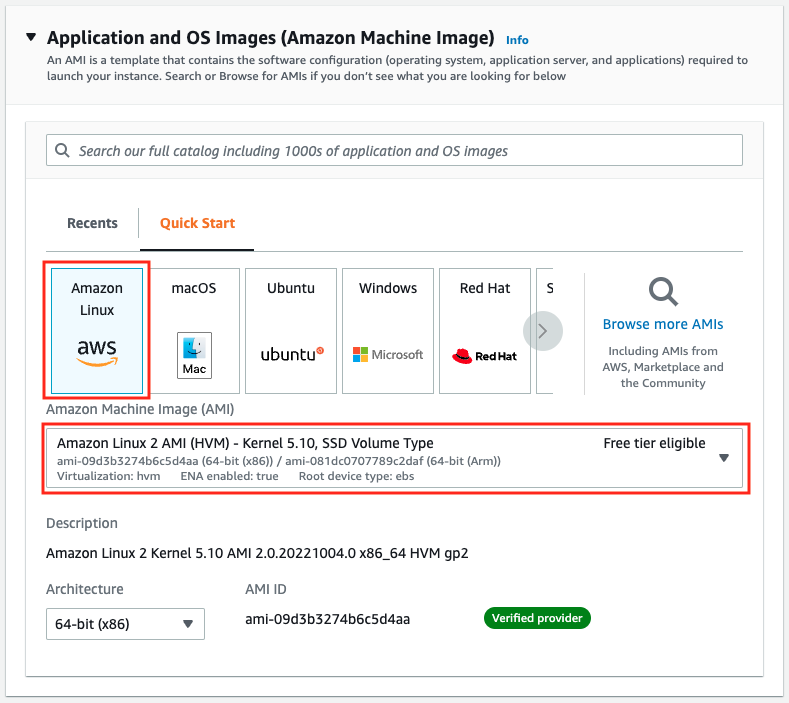
To launch an EC2 instance:

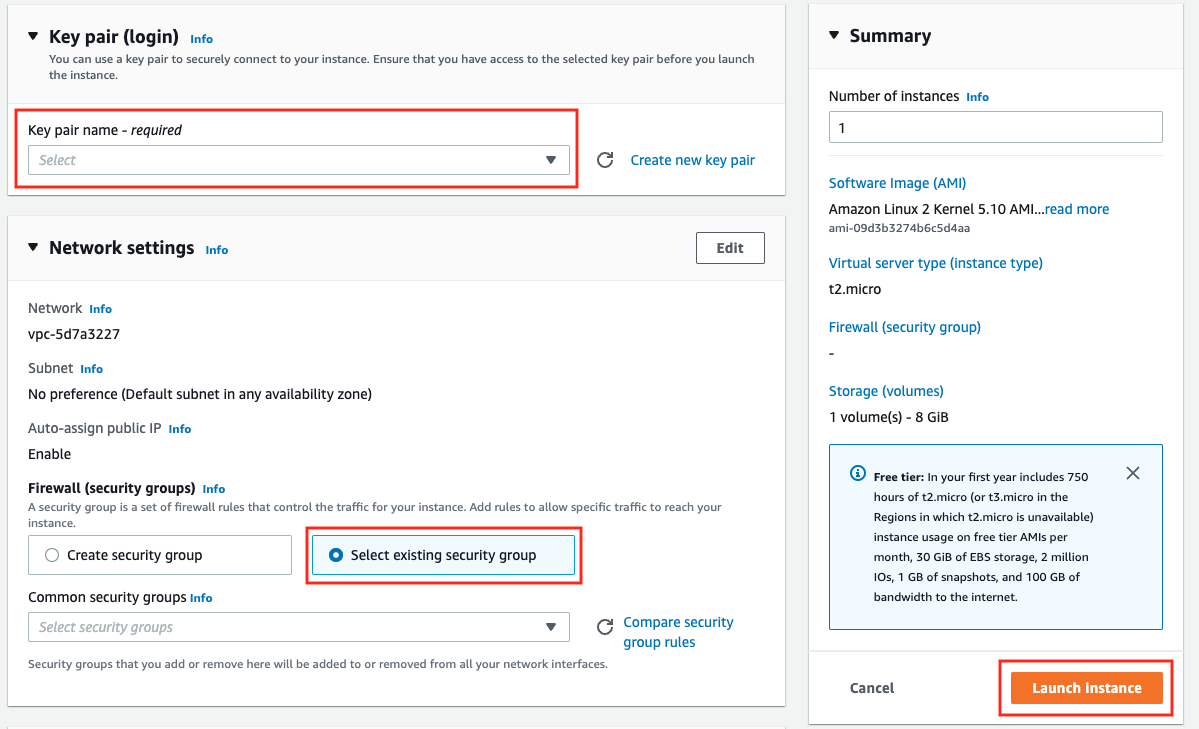
1. Sign in to the the [AWS Management Console](https://console.aws.amazon.com/ec2/).
2. Open the Amazon EC2 console by selecting EC2 under **Compute**.
3. From the Amazon EC2 dashboard, select **Launch Instance**.



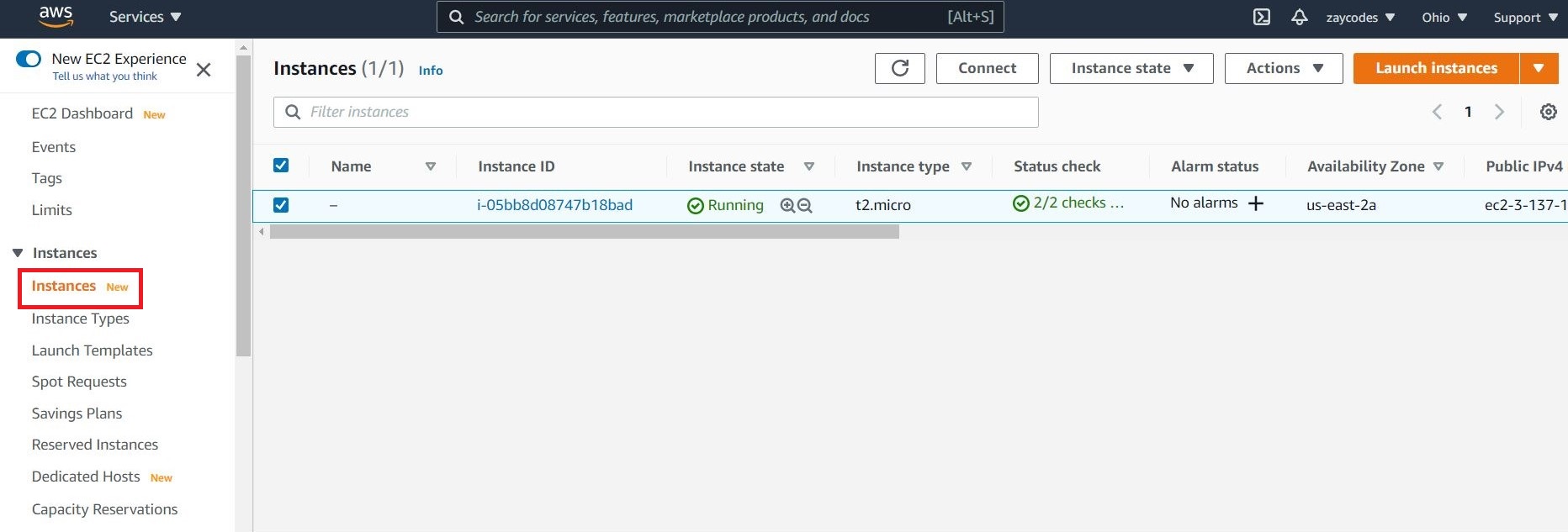
1. The **Choose an Amazon Machine Image (AMI)** page displays a list of basic configurations called Amazon Machine Images (AMIs) that serve as templates for your instance. Select the HVM edition of the **Amazon Linux AMI**.

|  |  |
| --- | --- |
|  | This configuration is marked **Free tier eligible**. |

1. 
2. Scroll down and select the key pair you created in the [creating a key pair](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#creating-a-key-pair) section above or any existing key pair you intend to use.
   1. **Select an existing security group**.
   2. Select the **WebServerSG** security group that you created.
   3. Select **Launch Instance**.



1. In the left-hand navigation bar, choose **Instances** to view the status of your instance. Initially, the status of your instance is pending. After the status changes to running, your instance is ready for use.



Installing and configuring Jenkins

Now that the Amazon EC2 instance has been launched, Jenkins can be installed properly.

In this step you will deploy Jenkins on your EC2 instance by completing the following tasks:

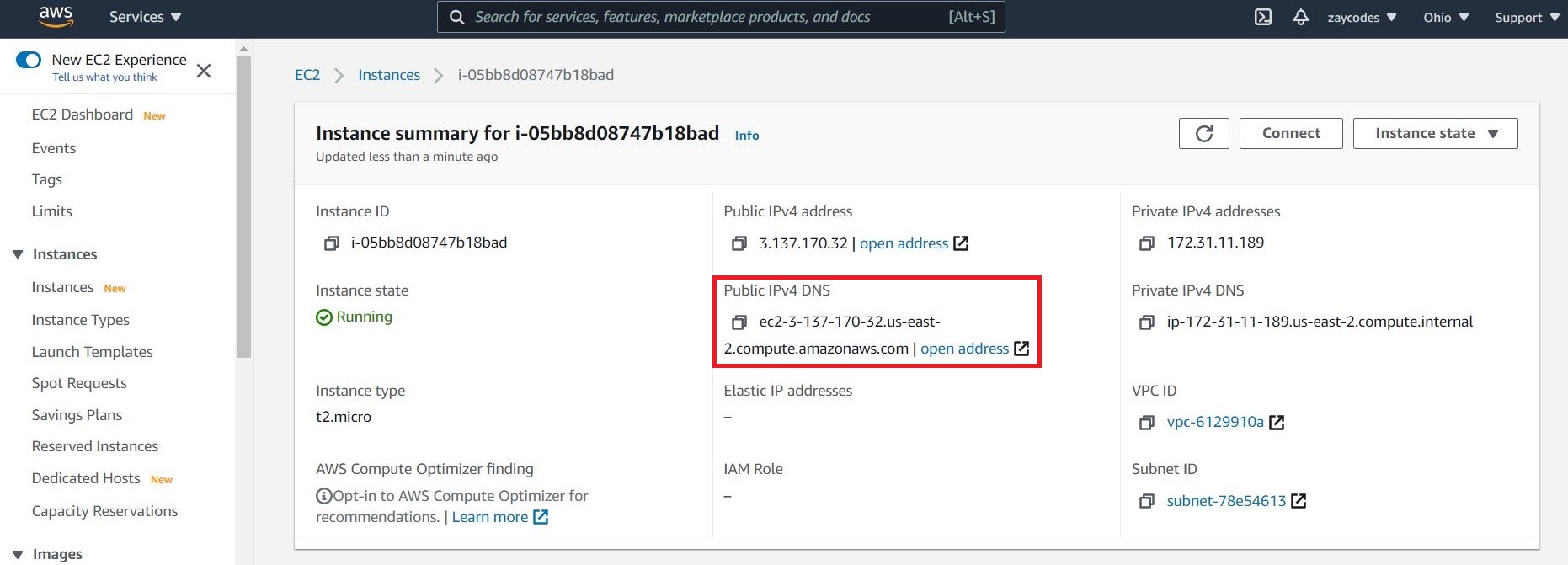
1. [Connecting to your Linux instance](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#connecting-to-your-linux-instance)
2. [Downloading and installing Jenkins](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#downloading-and-installing-jenkins)
3. [Configuring Jenkins](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#configuring-jenkins)

Connecting to your Linux instance

After you launch your instance, you can connect to it and use it the same way as your local machine.

Before you connect to your instance, get the **public DNS** name of the instance using the Amazon EC2 console.

1. Select the instance and locate Public DNS.



|  |  |
| --- | --- |
|  | If your instance doesn’t have a public DNS name, open the VPC console, select the VPC, and check the **Summary** tab. If either DNS resolution or DNS hostnames is **no**, select **Edit** and change the value to **yes**. |

Prerequisites

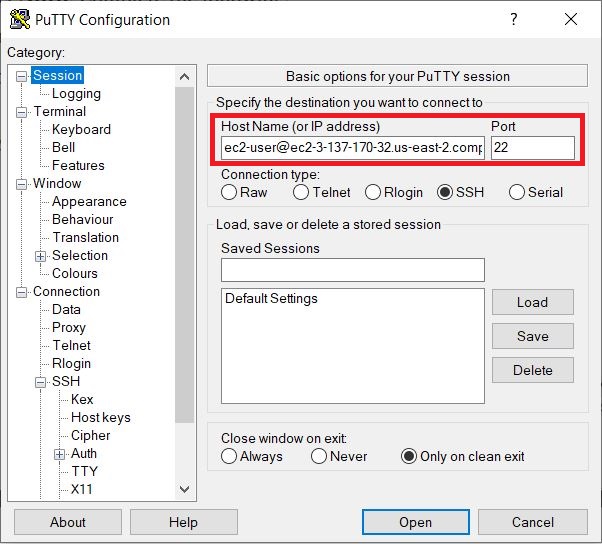
The tool that you use to connect to your Linux instance depends on your operating system.

* If your computer runs Windows, you will connect using PuTTY.
* If your computer runs Linux or Mac OS X, you will connect using the SSH client.

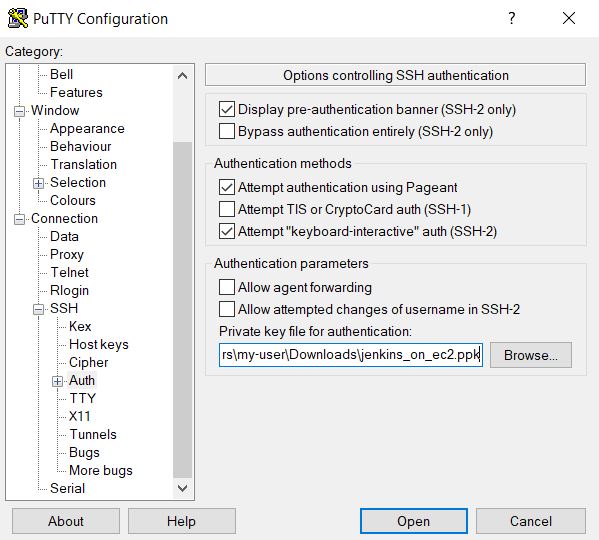
These tools require the use of your key pair. Be sure that you have created your key pair as described in [Creating a key pair](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#creating-a-key-pair).

Using PuTTY to connect to your instance

1. From the **Start** menu, select **All Programs** > **PuTTY** > **PuTTY**.
2. In the **Category** pane, select **Session**, and complete the following fields:
   1. In **Host Name**, enter ec2-user@public\_dns\_name.
   2. Ensure that **Port** is 22.



1. In the **Category** pane, expand **Connection**, expand **SSH**, and then select **Auth**. Complete the following:
   1. Select **Browse**.
   2. Select the .ppk file that you generated for your key pair, as described in [Creating a key pair](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#creating-a-key-pair) and then select **Open**.
2. Select **Open** to start the PuTTY session.



Using SSH to connect to your instance

1. Use the ssh command to connect to the instance. You will specify the private key (.pem) file and ec2-user@public\_dns\_name.
2. $ ssh -i /path/my-key-pair.pem ec2-user@ec2-198-51-

100-1.compute-1.amazonaws.com

You will receive a response like the following:

The authenticity of host 'ec2-198-51-100-1.compute1.amazonaws.com (10.254.142.33)' cant be

established.

RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.

Are you sure you want to **continue** connecting

**(**yes/no**)**?

1. Enter yes.

You will receive a response like the following:

Warning: Permanently added 'ec2-198-51-100-1.compute1.amazonaws.com' **(**RSA**)** to the list of known hosts.

Downloading and installing Jenkins

Completing the previous steps enables you to download and install Jenkins on AWS. To download and install Jenkins:

**Sudo yum update -y**

**sudo wget -O /etc/yum.repos.d/jenkins.repo \https://pkg.jenkins.io/redhat-stable/jenkins.repo**

**yum repolist**

**sudo rpm --import https://pkg.jenkins.io/redhat-stable/jenkins.io-2023.key**

**sudo yum upgrade**

**clear**

**sudo yum search java**

**sudo yum install java-11-amazon-corretto.x86\_64 -y**

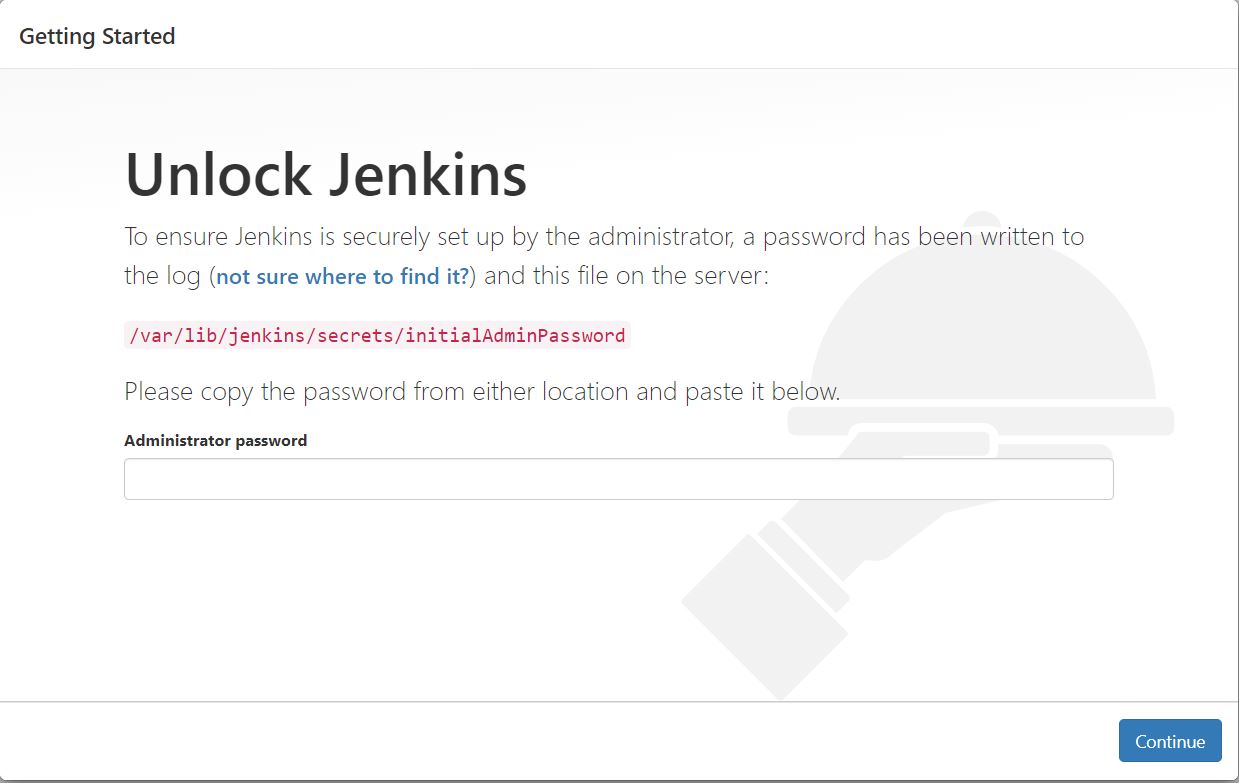
**java --version**

**sudo yum install jenkins -y**

Configuring Jenkins

Jenkins is now installed and running on your EC2 instance. To configure Jenkins:

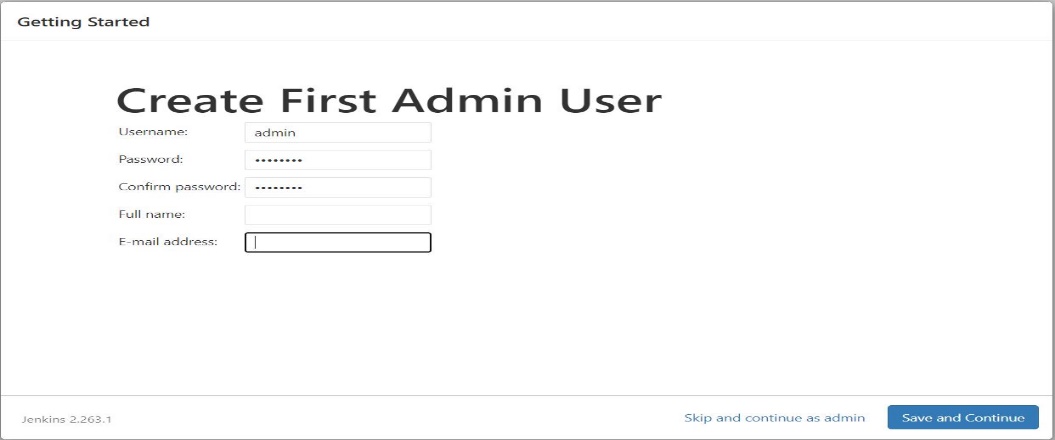
1. Connect to http://<your\_server\_public\_DNS>:8080 from your browser. You will be able to access Jenkins through its management interface:



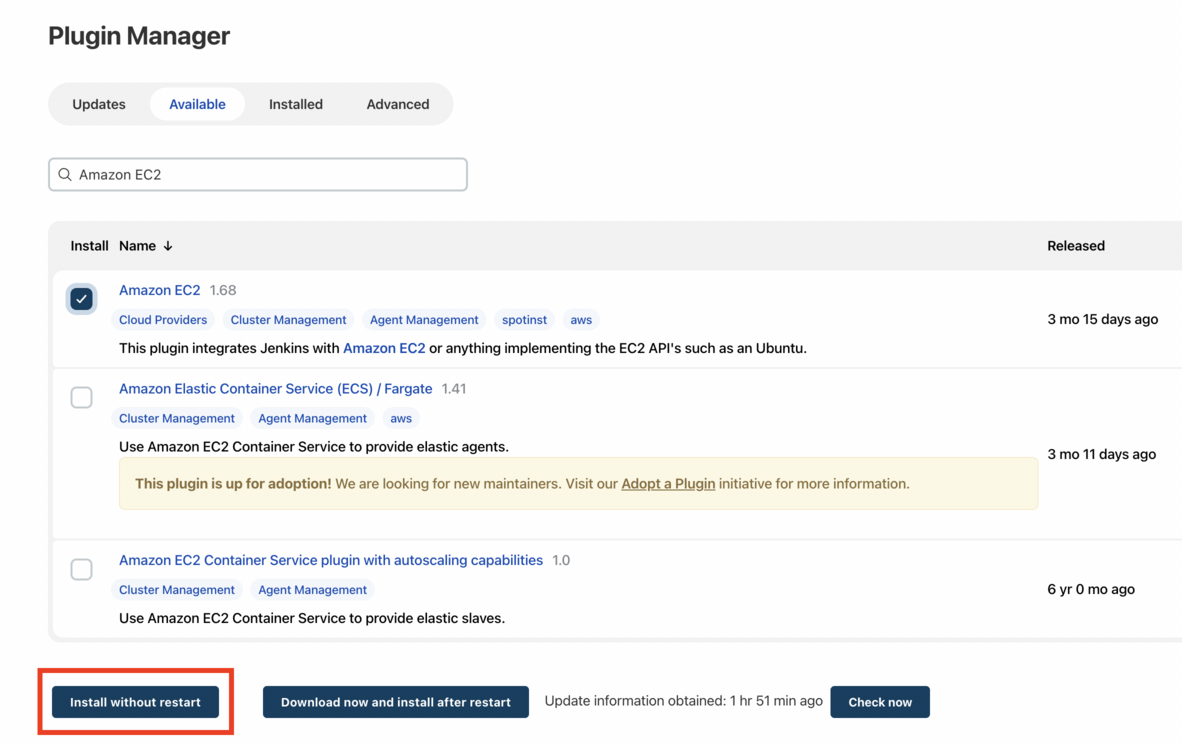
1. As prompted, enter the password found in **/var/lib/jenkins/secrets/initialAdminPassword**.
   1. Use the following command to display this password:

**[**ec2-user ~]$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword

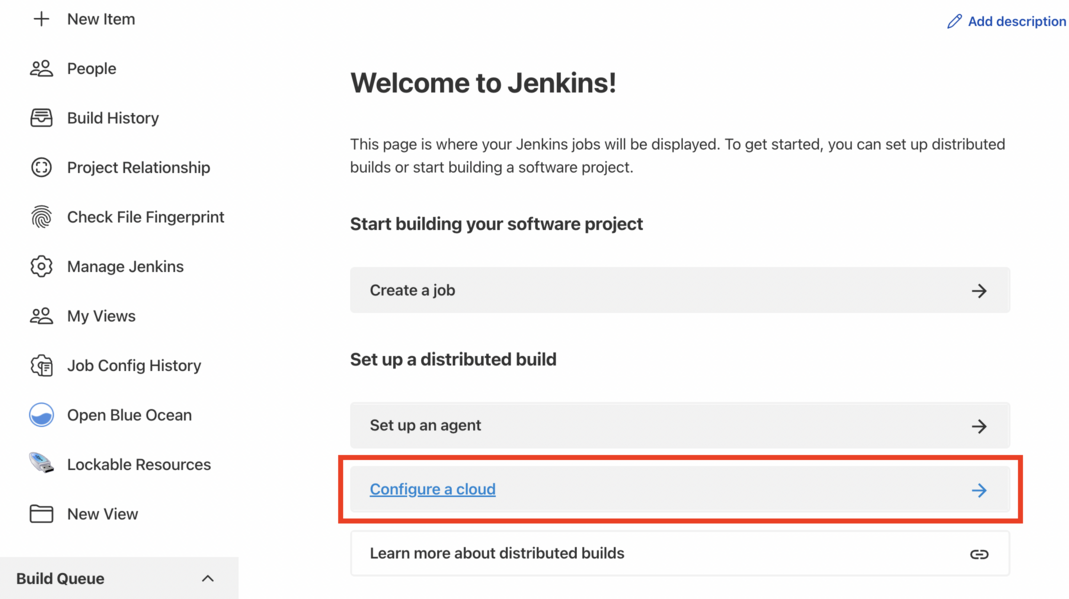
1. The Jenkins installation script directs you to the **Customize Jenkins page**. Click **Install suggested plugins**.
2. Once the installation is complete, the **Create First Admin User** will open. Enter your information, and then select **Save and Continue**.



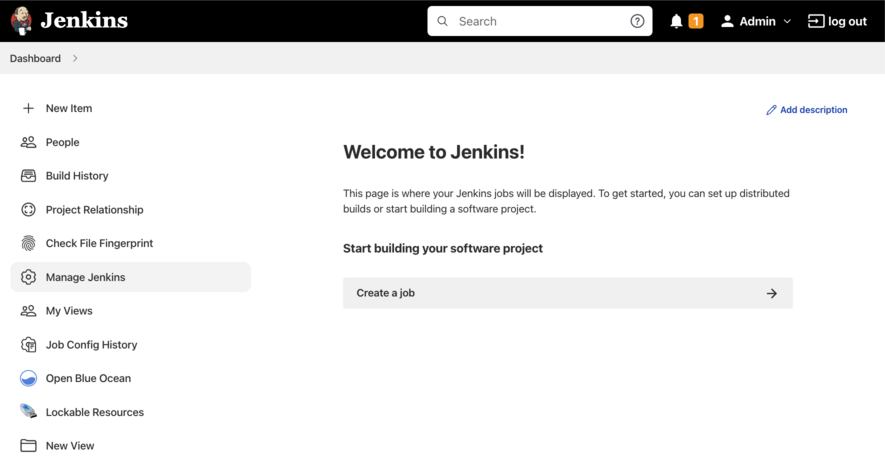
1. On the left-hand side, select **Manage Jenkins**, and then select **Manage Plugins**.
2. Select the **Available** tab, and then enter **Amazon EC2 plugin** at the top right.
3. Select the checkbox next to **Amazon EC2 plugin**, and then select **Install without restart**.



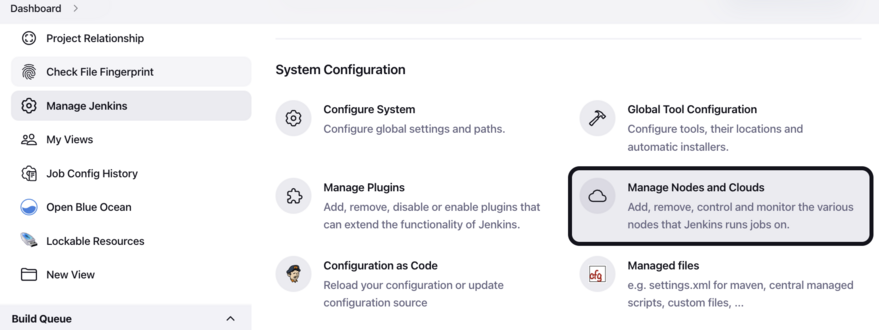
1. Once the installation is done, select **Back to Dashboard**.
2. Select **Configure a cloud** if there are no existing nodes or clouds.



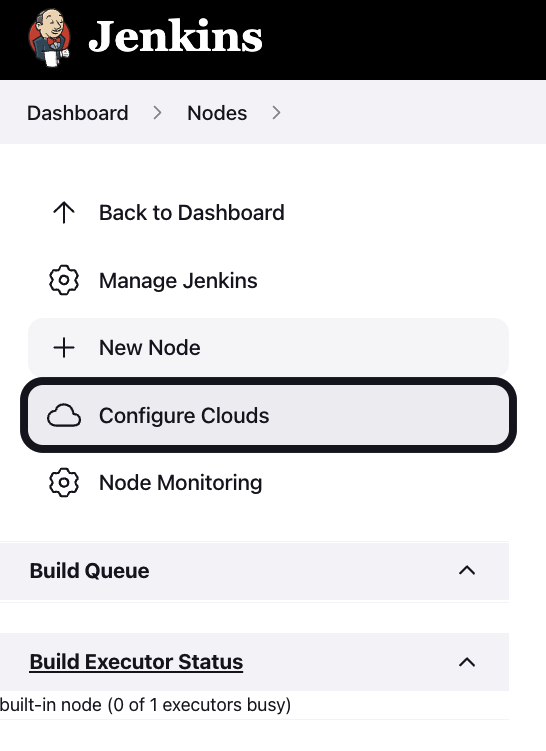
1. If you already have other nodes or clouds set up, select **Manage Jenkins**.



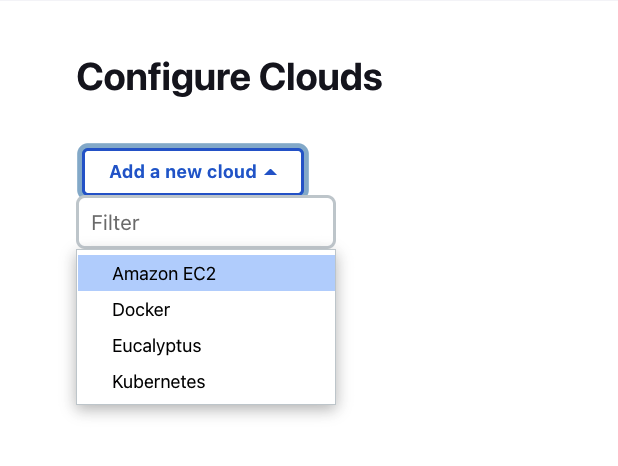
* 1. After navigating to **Manage Jenkins**, select **Configure Nodes and Clouds** from the left hand side of the page.



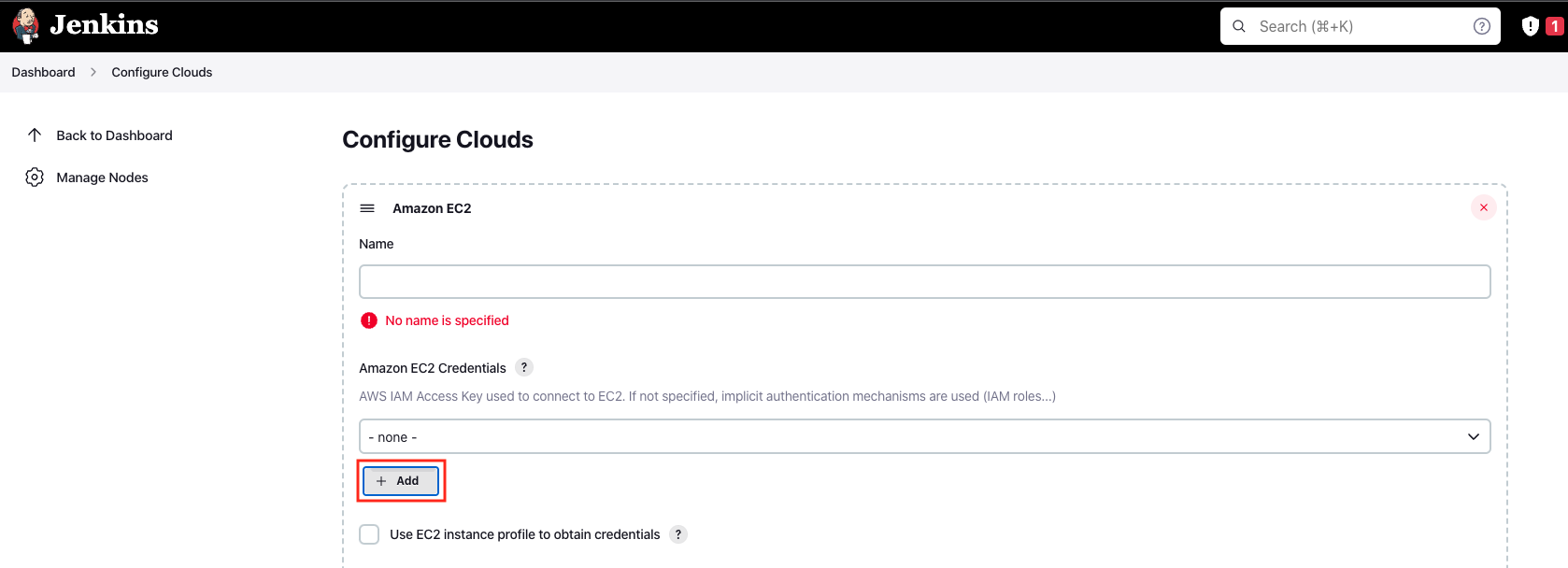
* 1. From here, select **Clouds**.



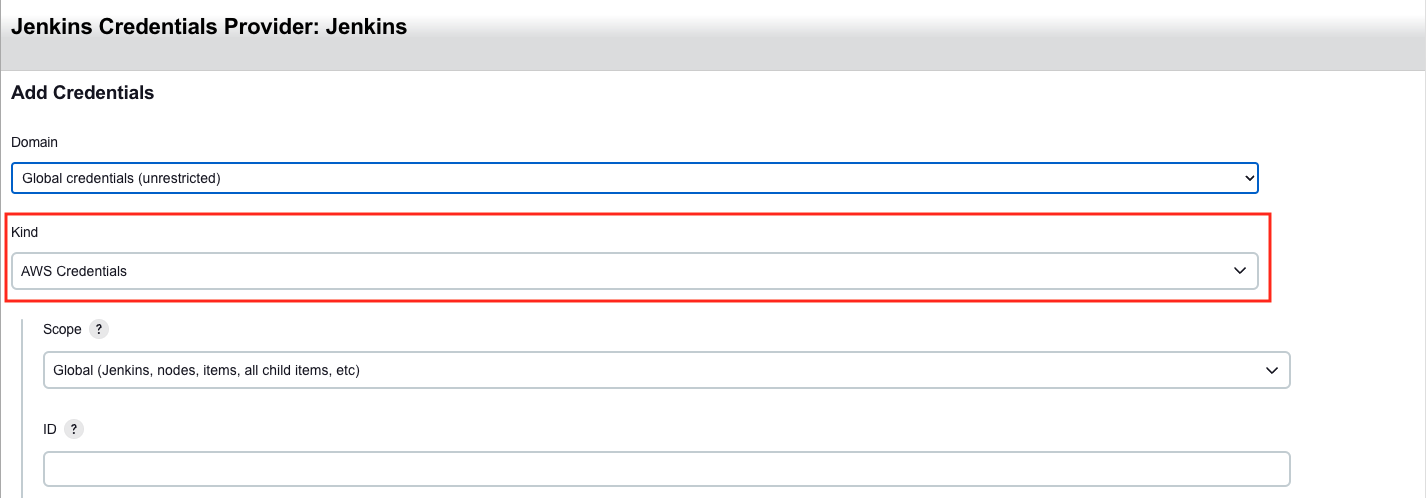
1. Select **Add a new cloud**, and select **Amazon EC2**. A collection of new fields appears.



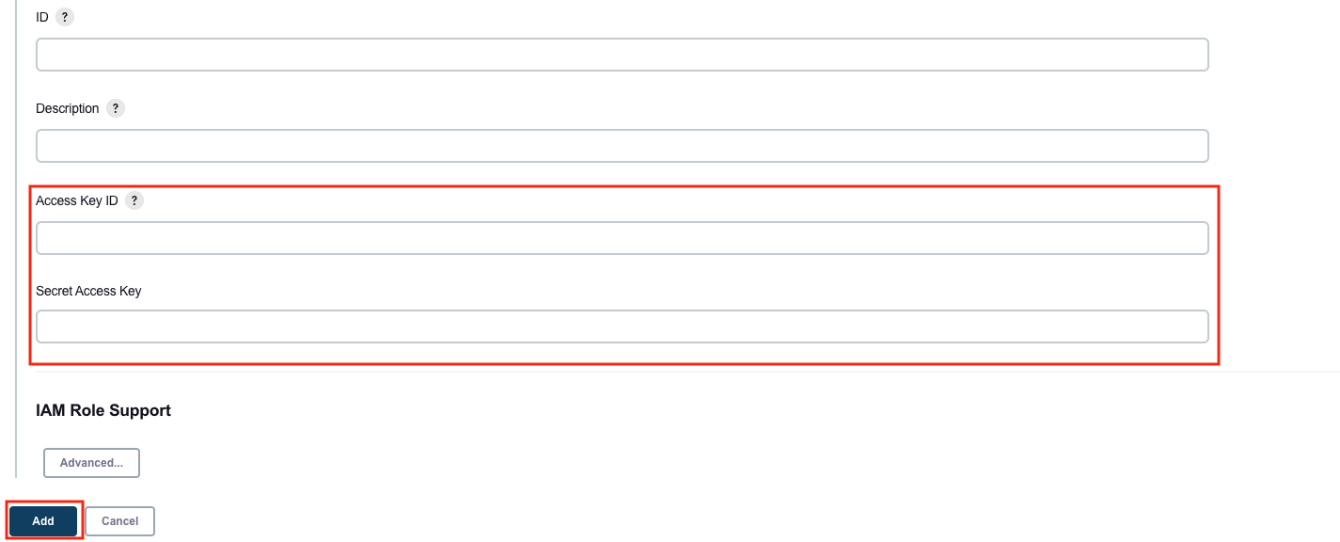
1. Click **Add** under Amazon EC2 Credentials



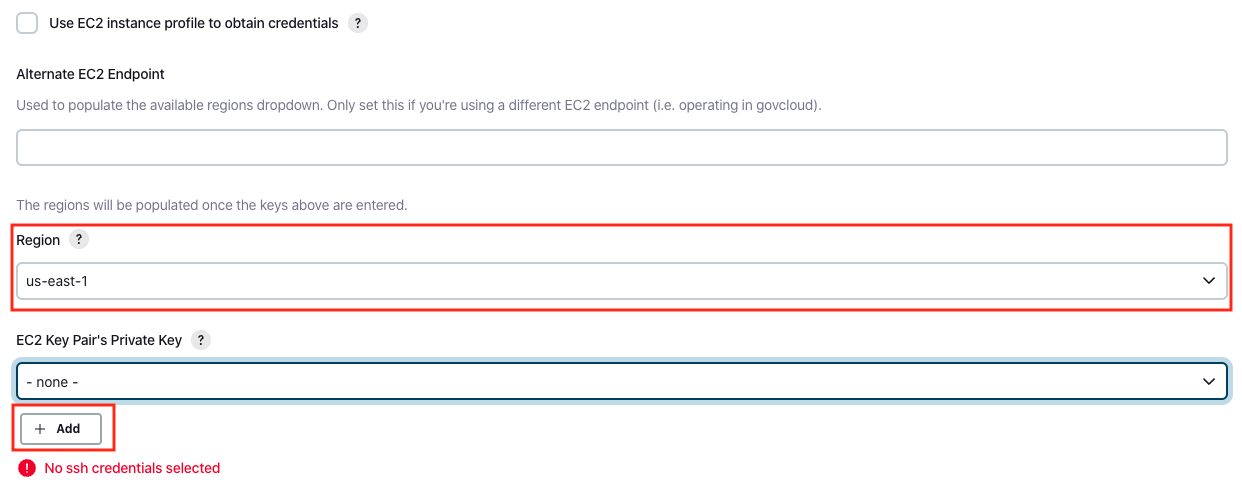
* 1. From the Jenkins Credentials Provider, select AWS Credentials as the **Kind**.



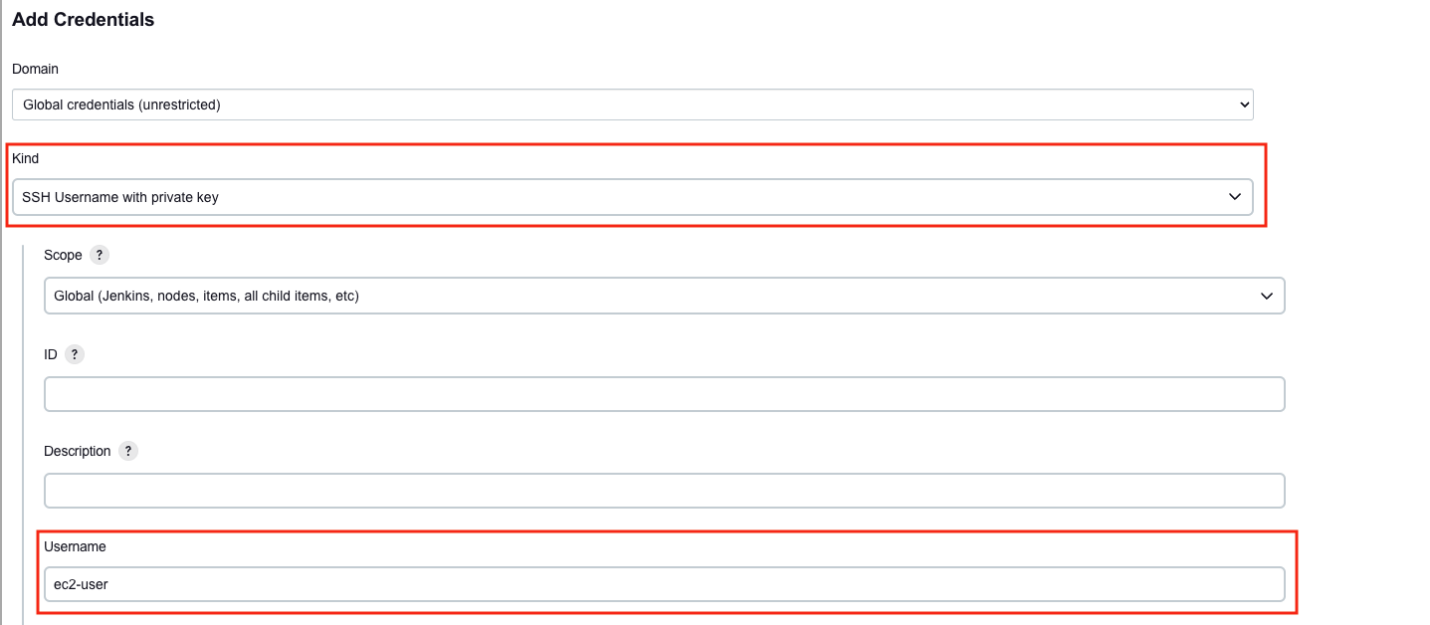
* 1. Scroll down and enter in the IAM User programmatic access keys with permissions to launch EC2 instances and select **Add**.



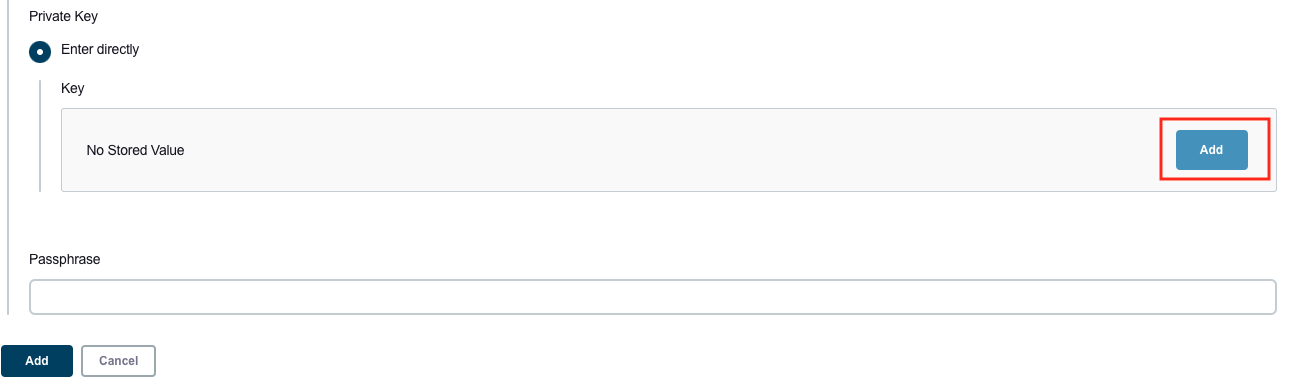
* 1. Scroll down to select your region using the drop-down, and select **Add** for the EC2 Key Pair’s Private Key.



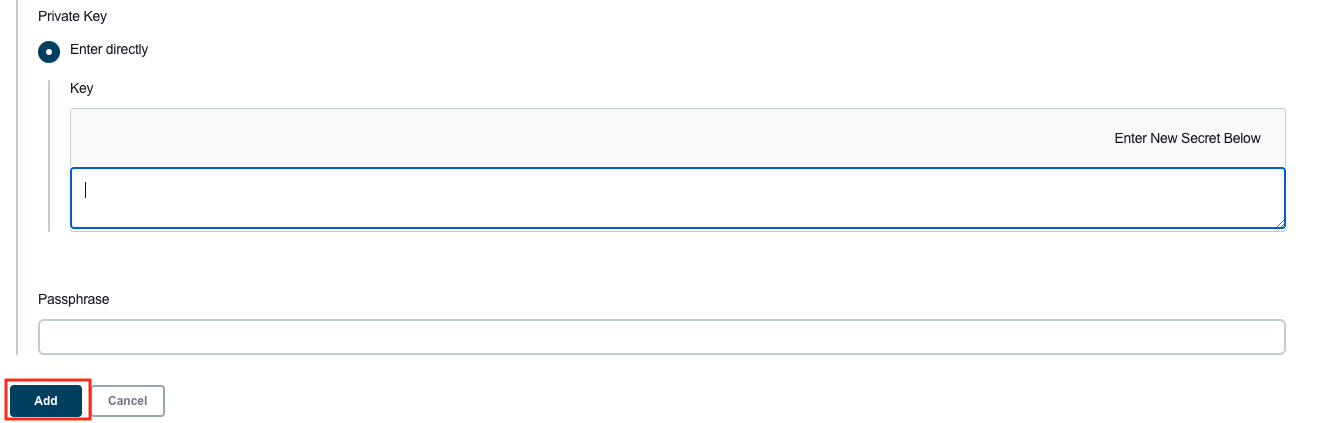
* 1. From the Jenkins Credentials Provider, select SSH Username with private key as the Kind and set the Username to ec2-user.



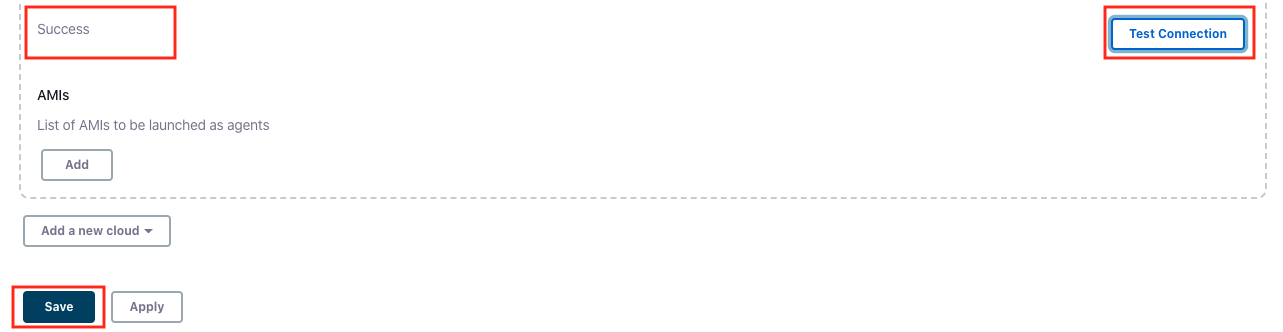
* 1. Scroll down and select **Enter Directly** under Private Key, then select **Add**.



* 1. Open the private key pair you created in the [creating a key pair](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#creating-a-key-pair) step and paste in the contents from "-----BEGIN RSA PRIVATE KEY-----" to "-----END RSA PRIVATE KEY-----". Select **Add** when completed.



* 1. Scroll down to "Test Connection" and ensure it states "Success". Select **Save** when done



You are now ready to use EC2 instances as Jenkins agents.

Cleaning up

After completing this tutorial, be sure to delete the AWS resources that you created so you do not continue to accrue charges.

Deleting your EC2 instance

1. In the left-hand navigation bar of the Amazon EC2 console, select **Instances**.
2. Right-click on the instance you created earlier, and select **Terminate**.

