**Launching and Installing Jenkin’s on EC2**

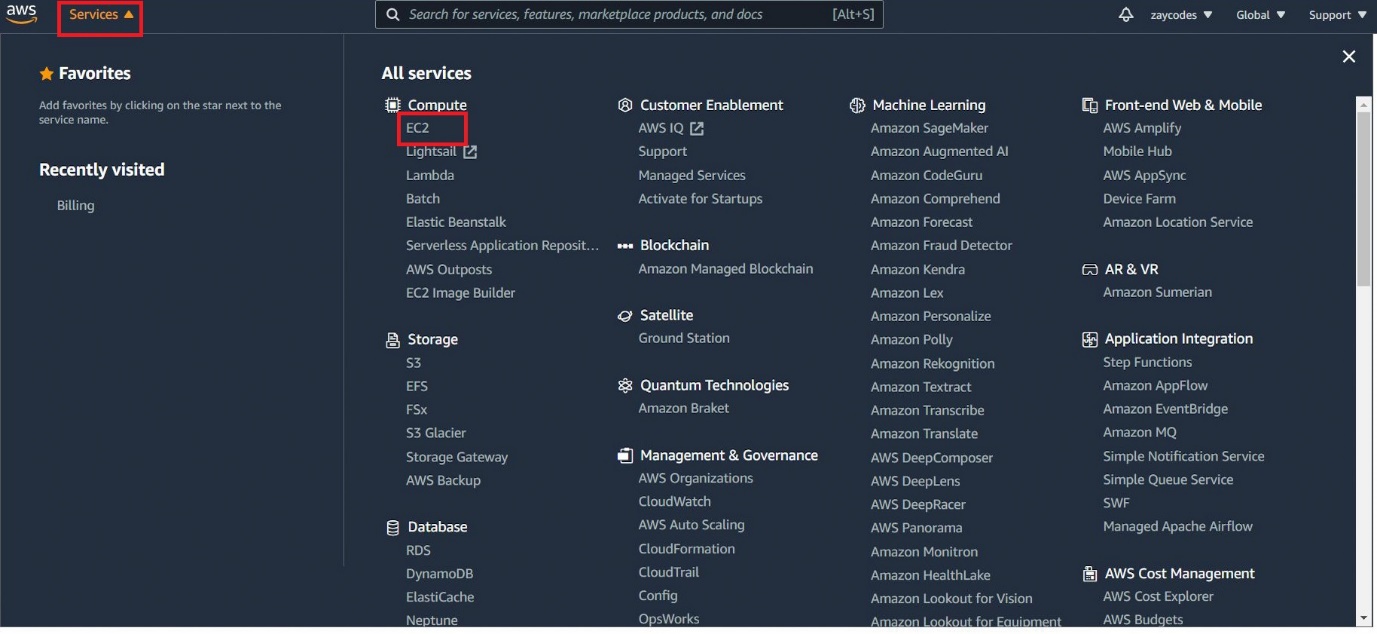
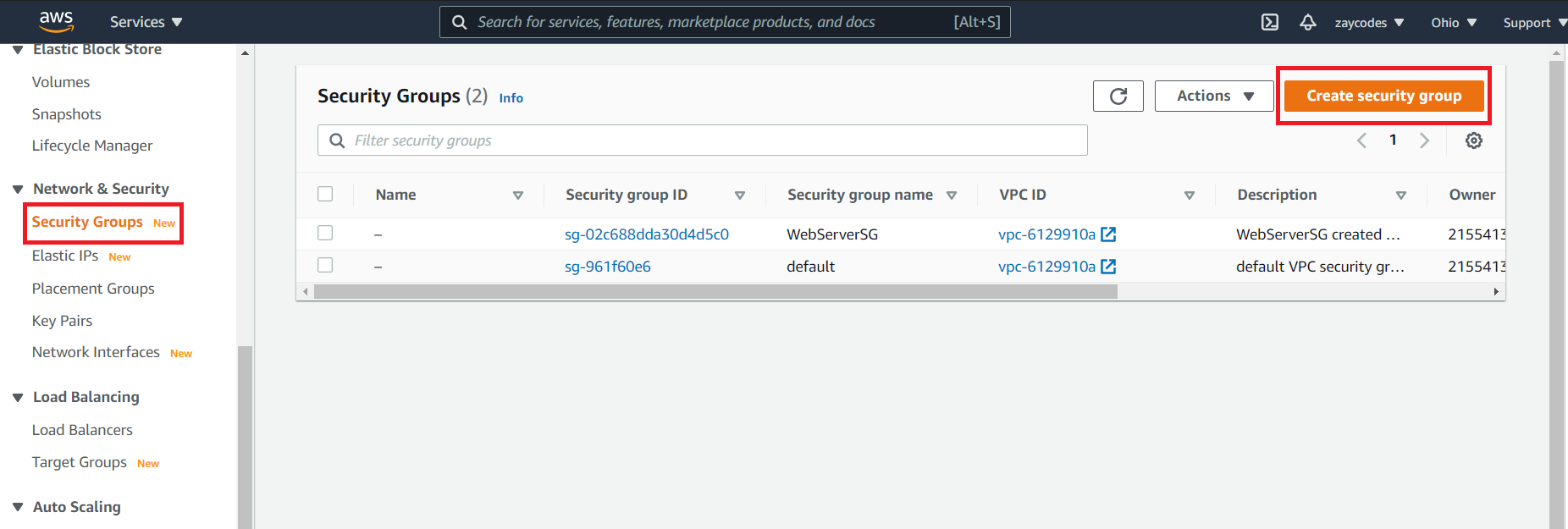
**Prerequisites**

* An Amazon EC2 key pair. If you don’t have one, refer to [Creating a key pair](https://www.jenkins.io/doc/tutorials/tutorial-for-installing-jenkins-on-AWS/#creating-a-key-pair).
* An AWS IAM User with programmatic key access and [permissions to launch EC2 instances](https://plugins.jenkins.io/ec2/#plugin-content-iam-setup)
* Creating a key pair
* Creating a key pair helps ensure that the correct form of authentication is used when you install Jenkins.

**Creating Key Pair:**

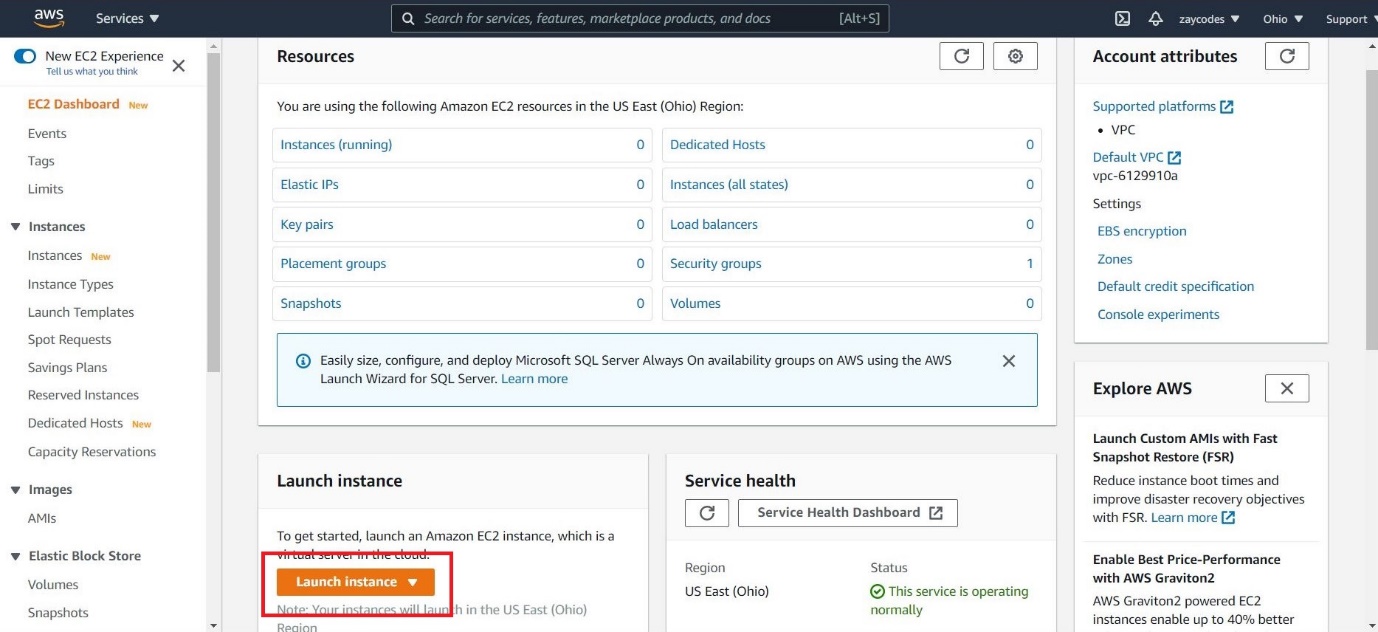
* Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/> and sign in.
* In the navigation pane, under NETWORK & SECURITY, select Key Pairs.
* Select Create key pair.
* For Name, enter a descriptive name for the key pair. Amazon EC2 associates the public key with the name that you specify as the key name. A key name can include up to 255 ASCII characters. It cannot include leading or trailing spaces.
* For File format, select the format in which to save the private key.
* For OpenSSH compatibility, select pem.
* For PuTTY compatibility, select ppk.
* Select Create key pair.
* The private key file downloads automatically. The base file name is the name you specified as the name of your key pair, and the file name extension is determined by the file format you chose. Save the private key file in a safe place.
* If you use an SSH client on a macOS or Linux computer to connect to your Linux instance, run the following command to set the permissions of your private key file so that only you can read it.
* $ chmod 400 <key\_pair\_name>.pem

**Creating a security group**

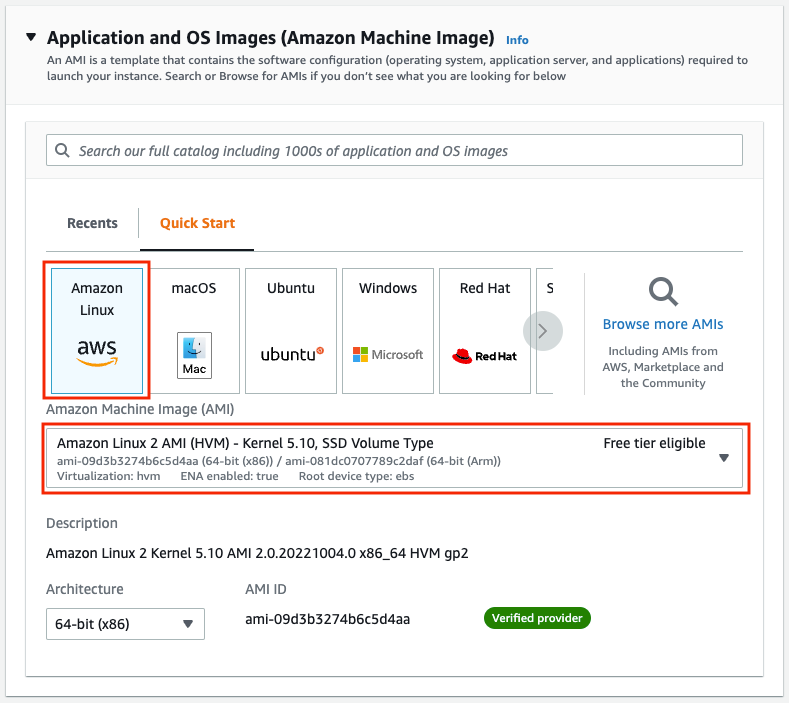
* A security group acts as a firewall that controls the traffic allowed to reach one or more EC2 instances. When you launch an instance, you can assign it one or more security groups. You add rules that control the traffic allowed to reach the instances in each security group. You can modify a security group’s rules any time, and the new rules take effect immediately.
* You will create a security group and add the following rules:
* Allow inbound HTTP access from anywhere.
* Allow inbound SSH traffic from your computer’s public IP address so you can connect to your instance.
* To create and configure your security group:
* Decide who may access your instance. For example, a single computer or all trusted computers on a network. For this tutorial, you can use the public IP address of your computer.
* To find your IP address, use the [check IP service tool](http://checkip.amazonaws.com/) from AWS3 or search for the phrase "what is my IP address" in any search engine.
* If you connect through an ISP or from behind your firewall without a static IP address, you will need the range of IP addresses used by client computers. If you don’t know this address range, you can use 0.0.0.0/0 for this tutorial.
* Sign in to the [AWS Management Console](https://console.aws.amazon.com/ec2/).
* 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.
* 
* In Security group name, enter WebServerSG or any preferred name of your choice, and provide a description.
* Select your VPC from the list. You can use the default VPC.
* 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.
* 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:**

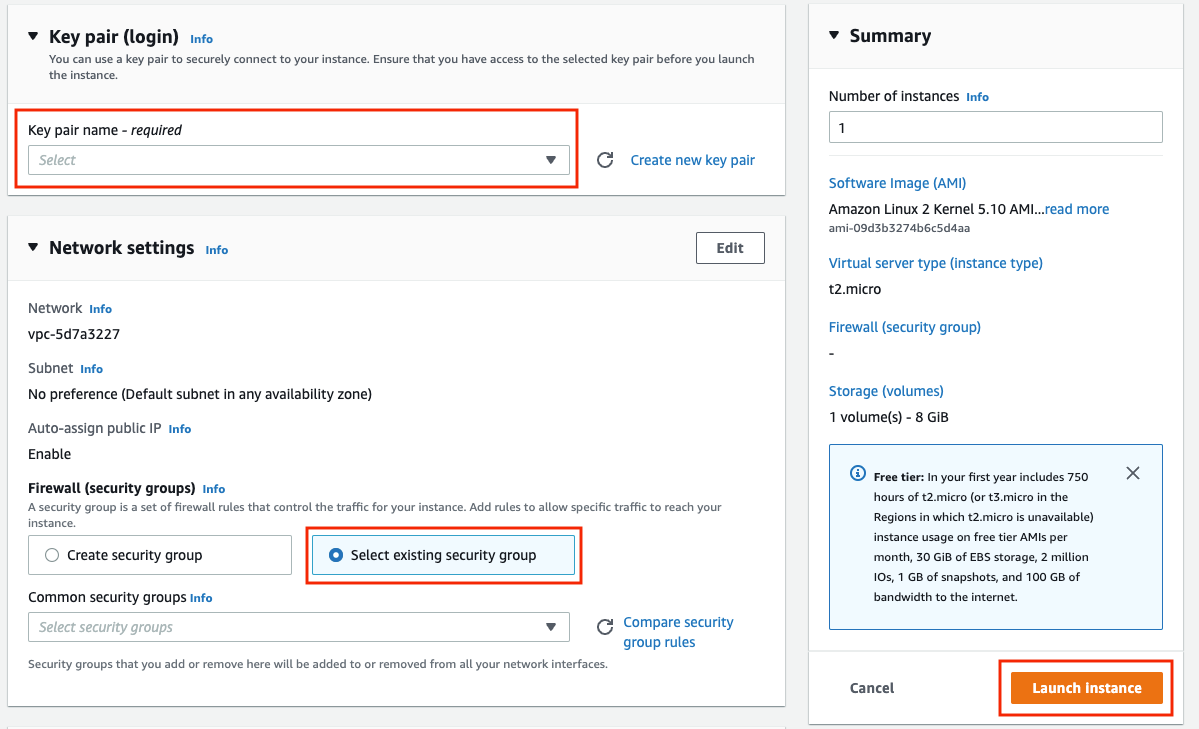
* Sign in to the the [AWS Management Console](https://console.aws.amazon.com/ec2/).
* Open the Amazon EC2 console by selecting EC2 under Compute.
* From the Amazon EC2 dashboard, select Launch Instance.



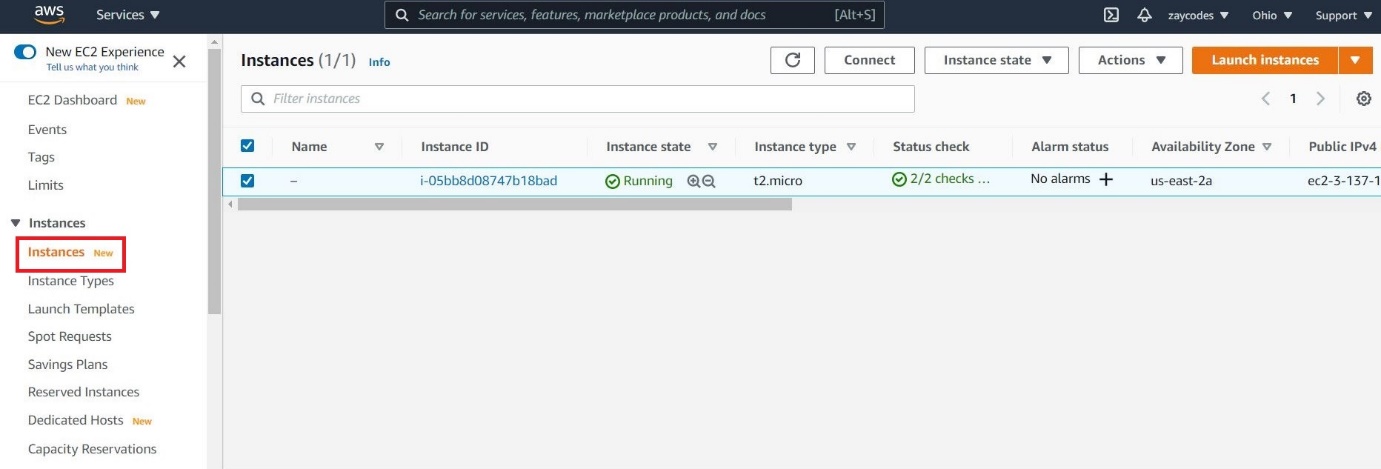
* The Choose an Amazon Machine Image (AMI) page displays a list of basic configurations called Amazon Machine Images (AMIs) that serve as templates for your instance. Select the HVM edition of the Amazon Linux AMI.



* Scroll down and select the key pair you created in the creating a key pair section above or any existing key pair you intend to use.
* Select an existing security group.
* Select the security group that you created before.
* Select Launch Instance.



* 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.

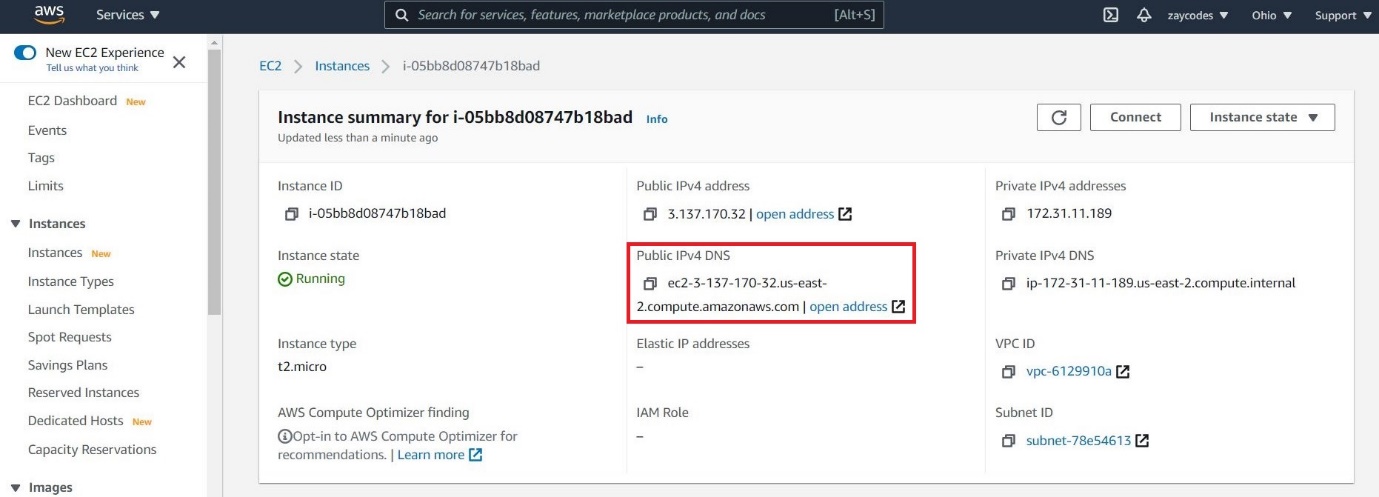


**Installing and configuring Jenkins**

* 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:

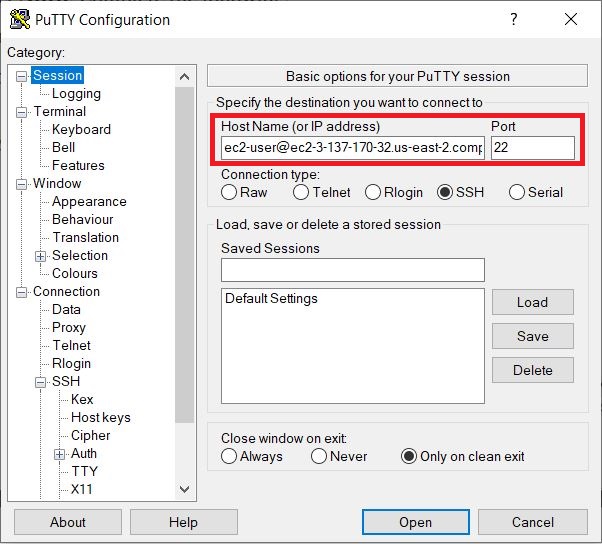
**Connecting to your Linux instance**

* 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.
* Select the instance and locate Public DNS.

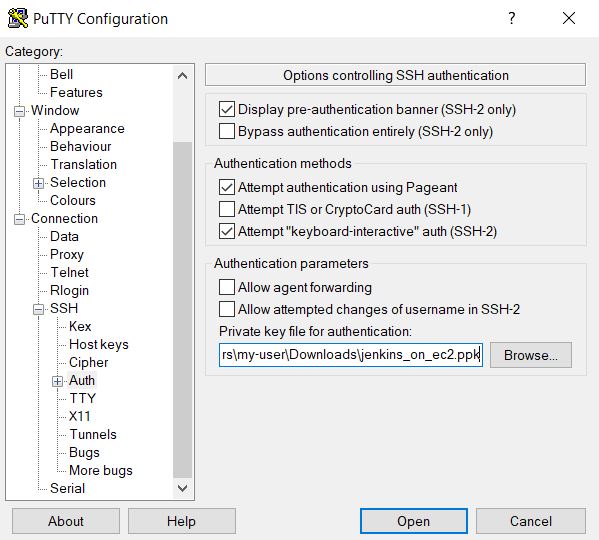


**Prerequisites**

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



* In the Category pane, expand Connection, expand SSH, and then select Auth. Complete the following:
* Select Browse.
* 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.
* Select Open to start the PuTTY session.



* Using SSH to connect to your instance
* Use the ssh command to connect to the instance. You will specify the private key (.pem) file and ec2-user@public\_dns\_name.

**$ ssh -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com**

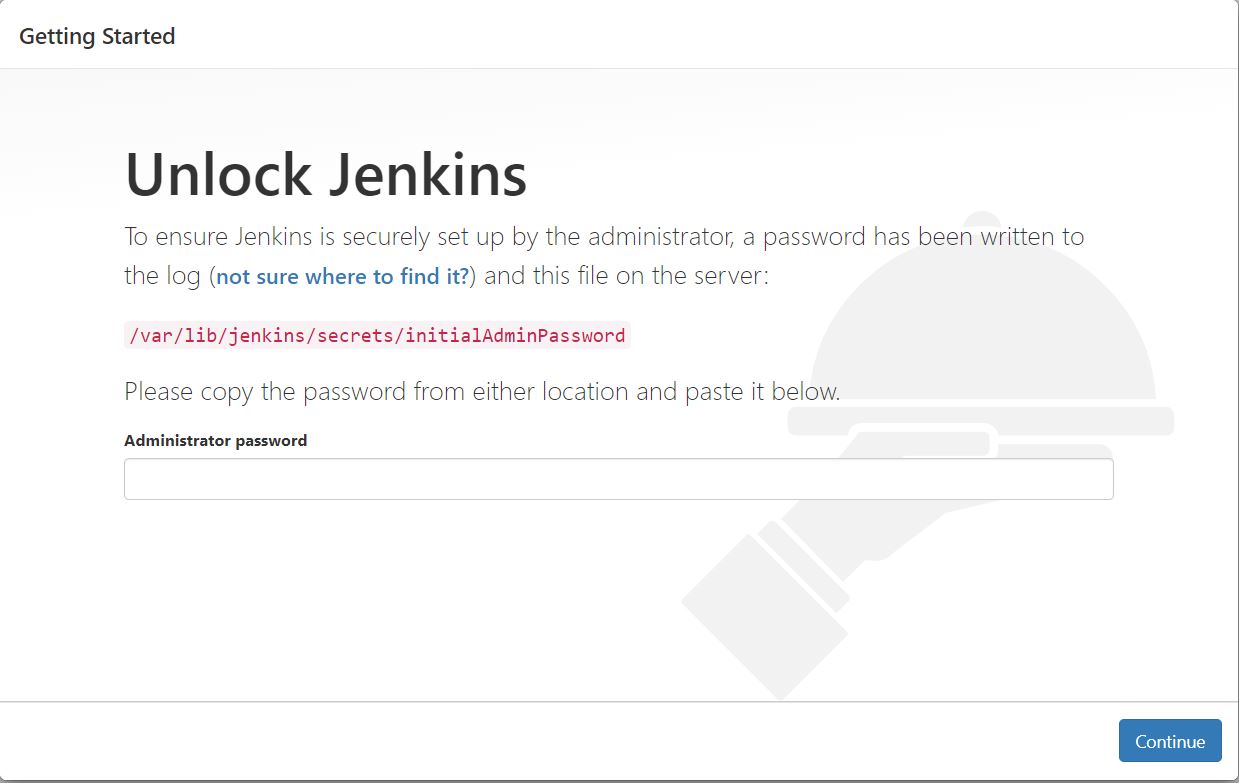
* You will receive a response like the following:
* The authenticity of host 'ec2-198-51-100-1.compute1.amazonaws.com (10.254.142.33)' cant be established.
* RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
* Are you sure you want to continue connecting
* (yes/no)?
* 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:
* Ensure that your software packages are up to date on your instance by using the following command to perform a quick software update:
* [ec2-user ~]$ sudo yum update –y
* Add the Jenkins repo using the following command:
* [ec2-user ~]$ sudo wget -O /etc/yum.repos.d/jenkins.repo \
* https://pkg.jenkins.io/redhat-stable/jenkins.repo
* Import a key file from Jenkins-CI to enable installation from the package:
* [ec2-user ~]$ sudo rpm --import https://pkg.jenkins.io/redhat-stable/jenkins.io-2023.key
* [ec2-user ~]$ sudo yum upgrade
* Install Java (Amazon Linux 2023):
* [ec2-user ~]$ sudo dnf install java-17-amazon-corretto -y
* Install Jenkins:
* [ec2-user ~]$ sudo yum install jenkins -y
* Enable the Jenkins service to start at boot:
* [ec2-user ~]$ sudo systemctl enable jenkins
* Start Jenkins as a service:
* [ec2-user ~]$ sudo systemctl start jenkins
* You can check the status of the Jenkins service using the command:
* [ec2-user ~]$ sudo systemctl status jenkins

**Configuring Jenkins**

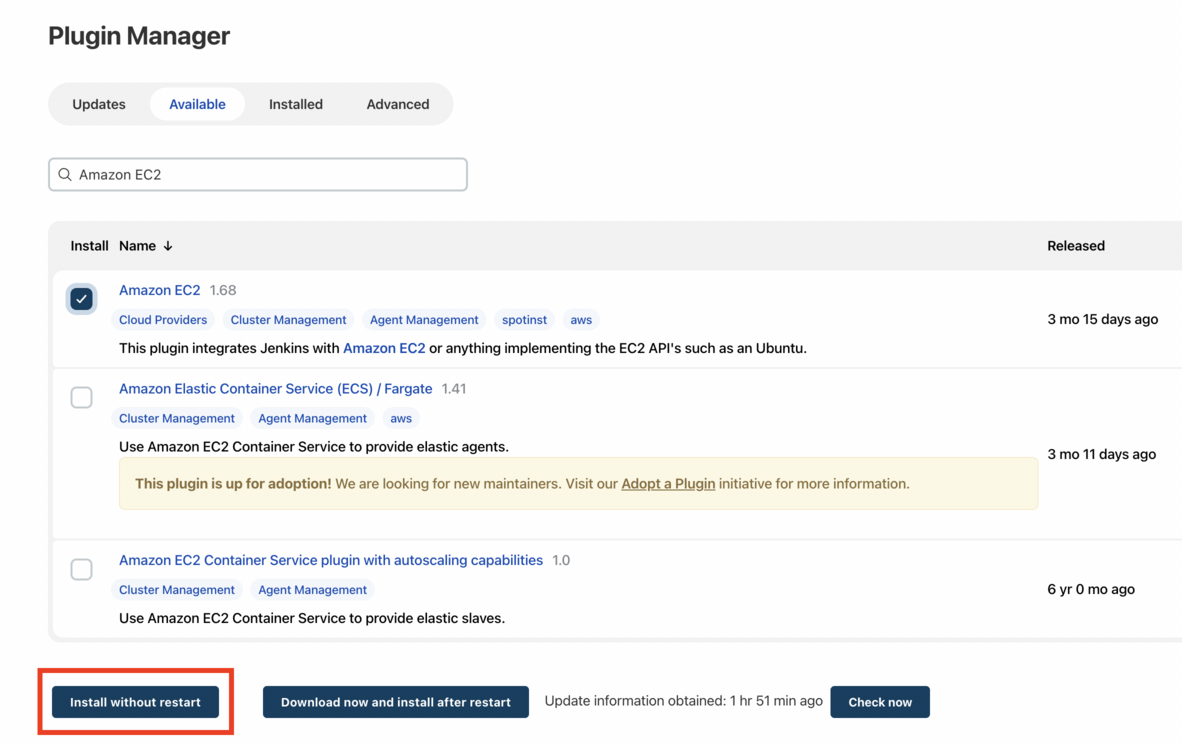
* Jenkins is now installed and running on your EC2 instance. To configure Jenkins:
* Connect to http://<your\_server\_public\_DNS>:8080 from your browser. You will be able to access Jenkins through its management interface:



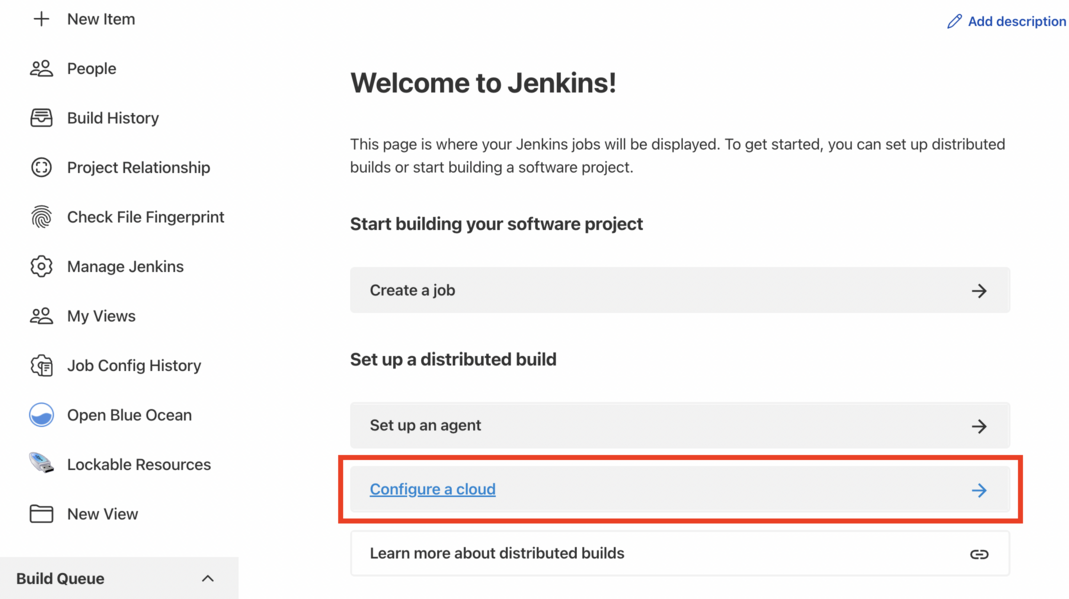
* As prompted, enter the password found in /var/lib/jenkins/secrets/initialAdminPassword.
* Use the following command to display this password:
* [ec2-user ~]$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
* The Jenkins installation script directs you to the Customize Jenkins page. Click Install suggested plugins.
* Once the installation is complete, the Create First Admin User will open. Enter your information, and then select Save and Continue.



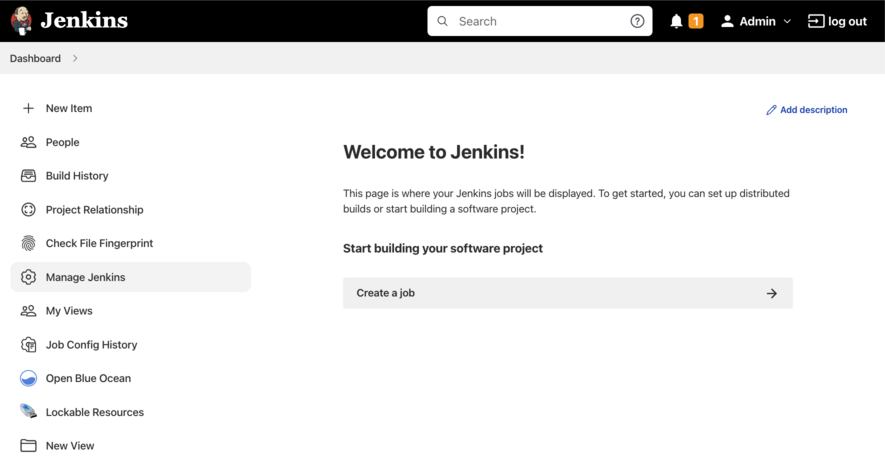
* On the left-hand side, select Manage Jenkins, and then select Manage Plugins.
* Select the Available tab, and then enter Amazon EC2 plugin at the top right.
* Select the checkbox next to Amazon EC2 plugin, and then select Install without restart.



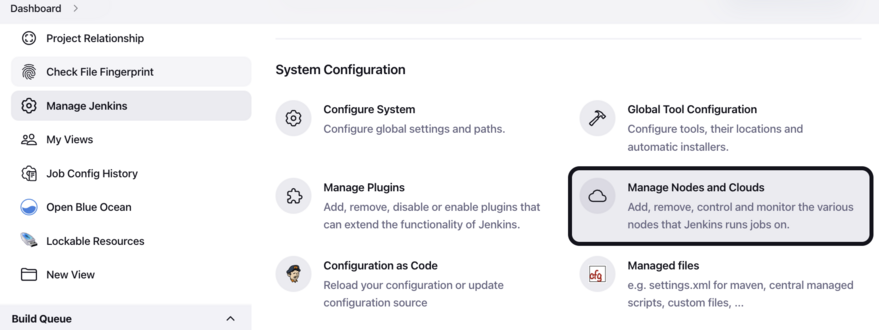
* Once the installation is done, select Back to Dashboard.
* Select Configure a cloud if there are no existing nodes or clouds.



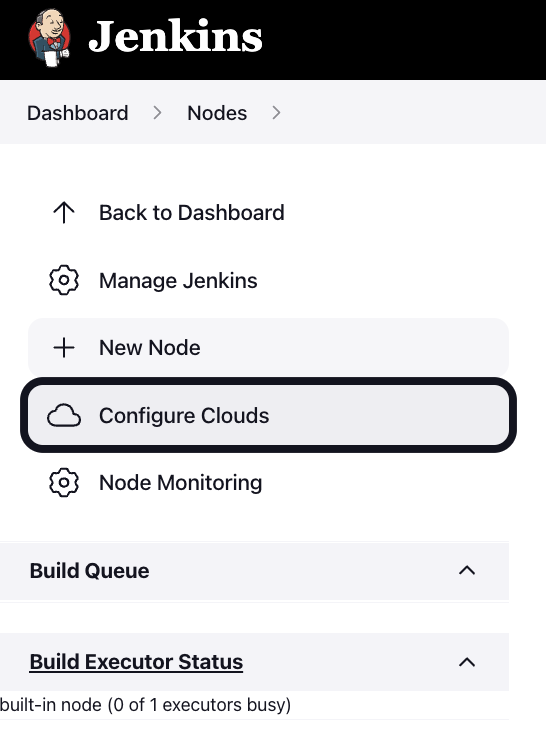
* If you already have other nodes or clouds set up, select Manage Jenkins.



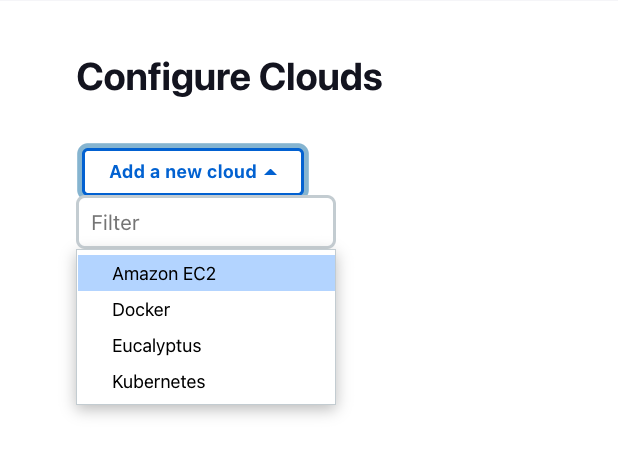
* After navigating to Manage Jenkins, select Configure Nodes and Clouds from the left hand side of the page.



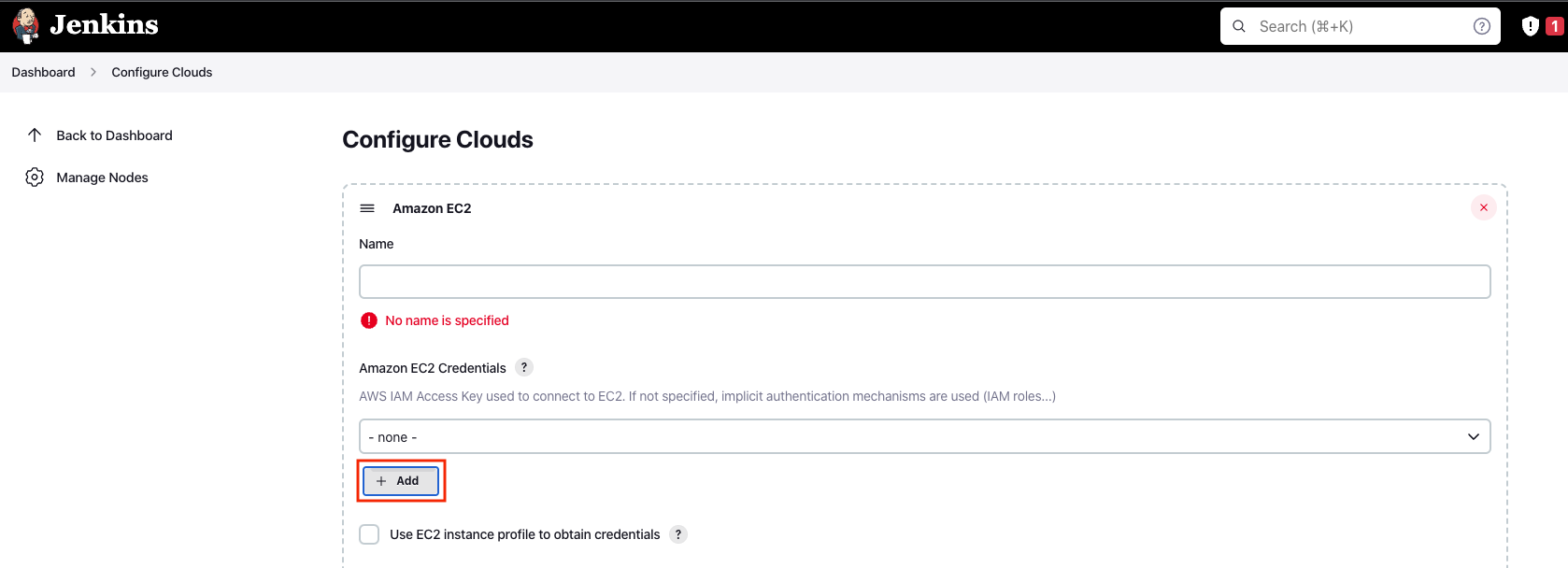
* From here, select Clouds.



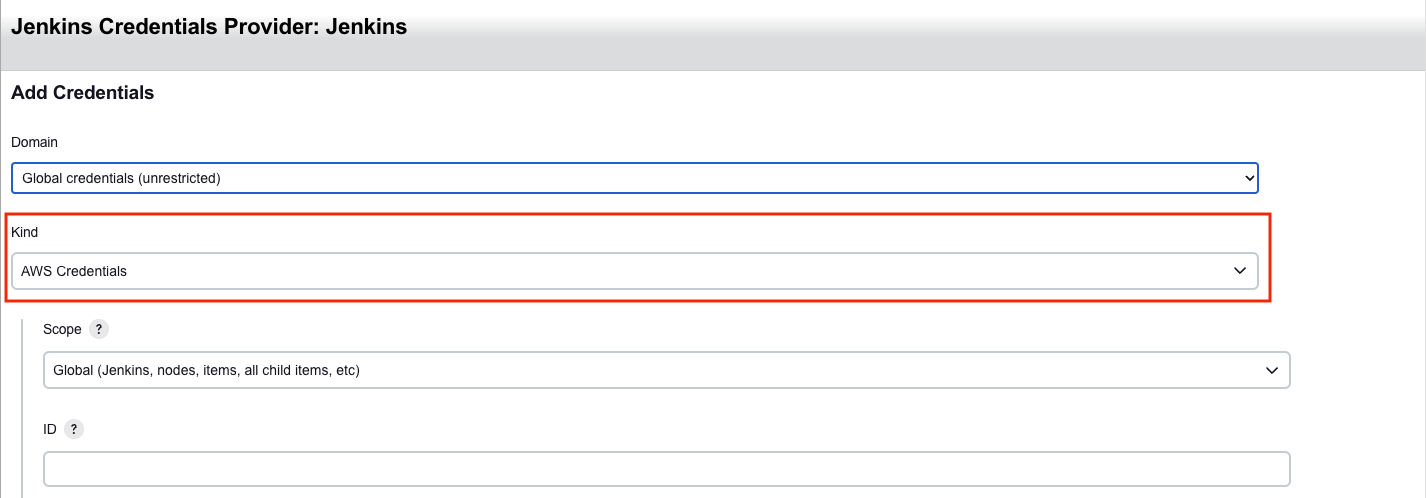
* Select Add a new cloud, and select Amazon EC2. A collection of new fields appears.



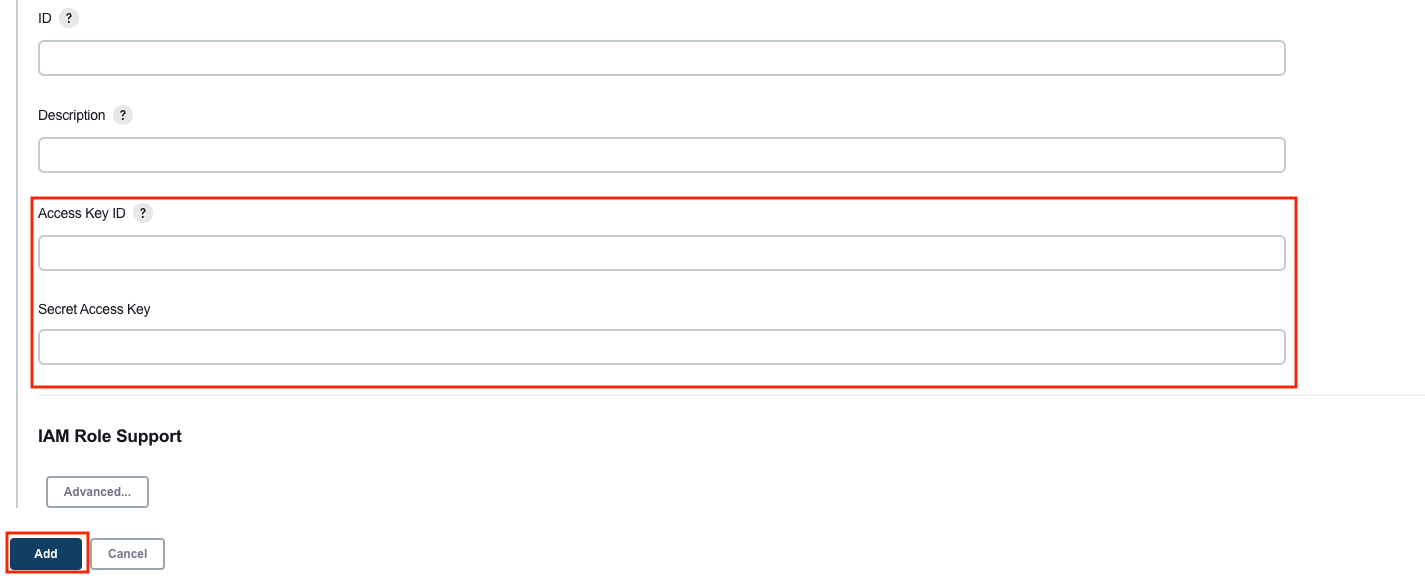
* Click Add under Amazon EC2 Credentials



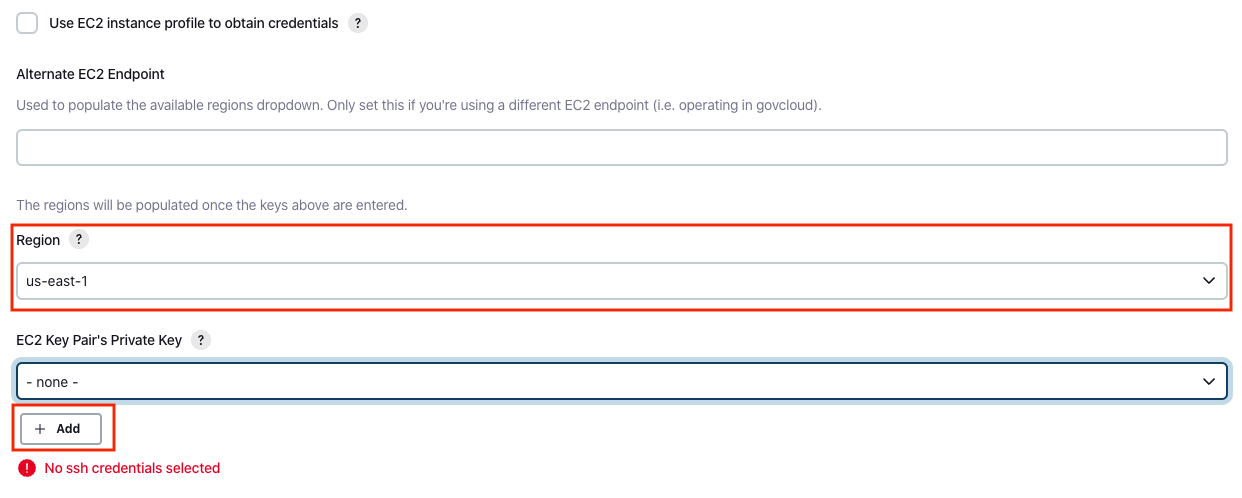
* From the Jenkins Credentials Provider, select AWS Credentials as the Kind.



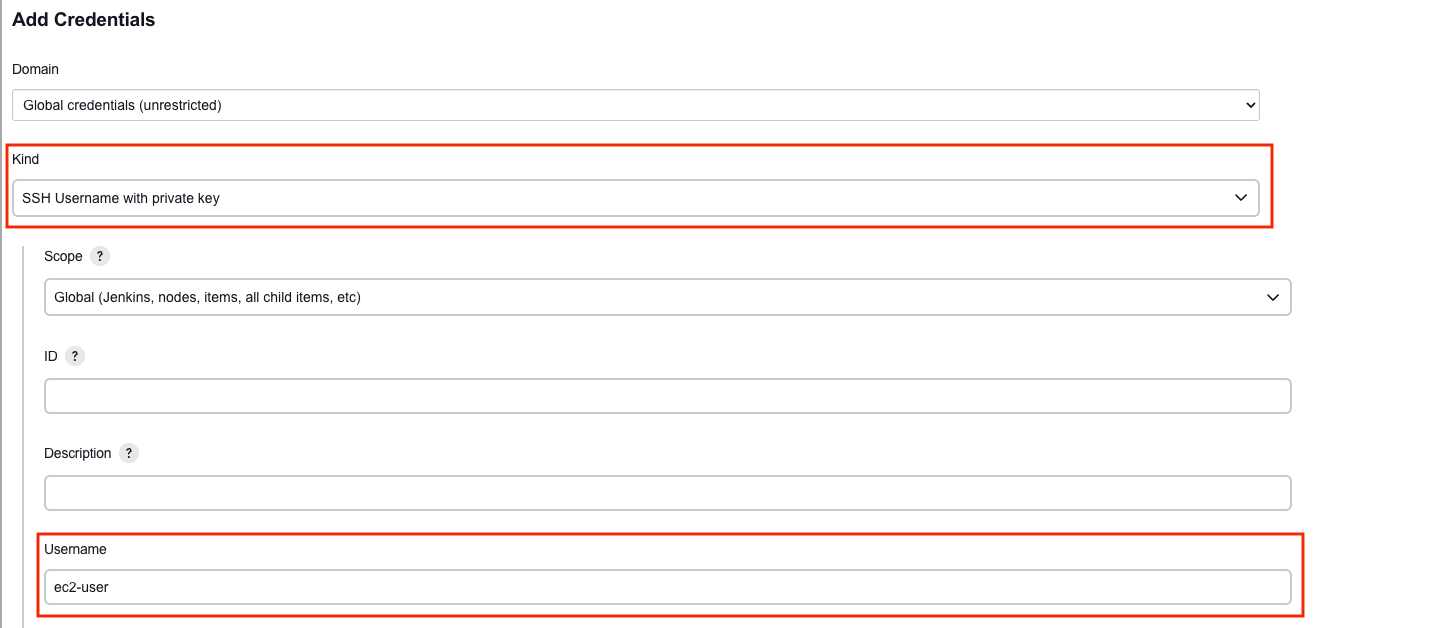
* Scroll down and enter in the IAM User programmatic access keys with permissions to launch EC2 instances and select Add.



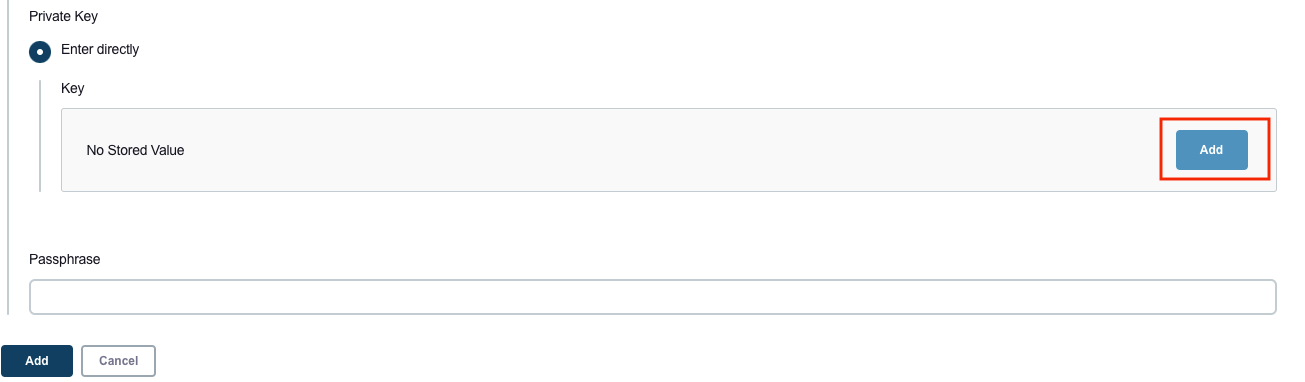
* Scroll down to select your region using the drop-down, and select Add for the EC2 Key Pair’s Private Key.



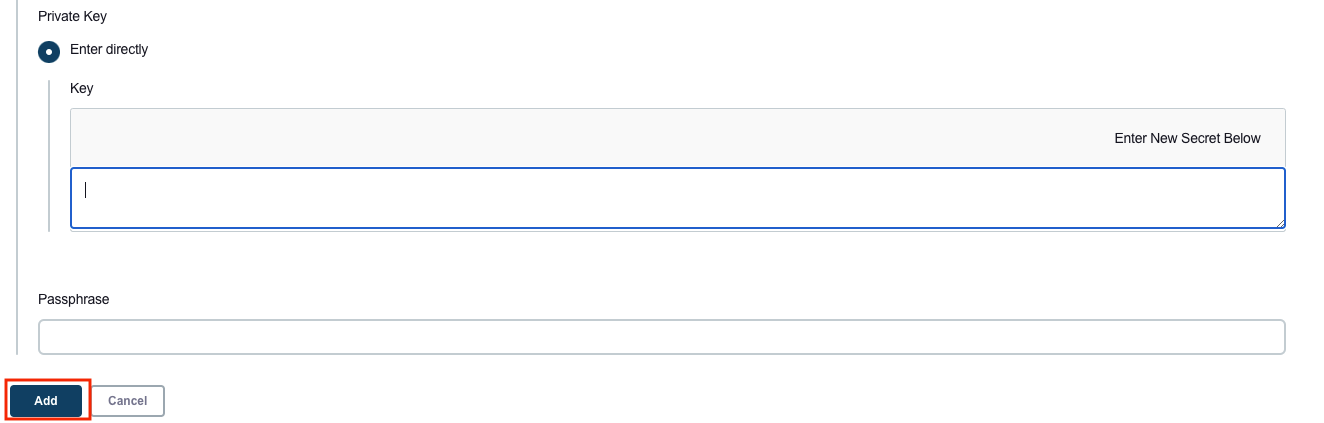
* From the Jenkins Credentials Provider, select SSH Username with private key as the Kind and set the Username to ec2-user.



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



* 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.



* 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.