 [**Dashboard**](https://cloudacademy.com/dashboard/)

 [**Training Library**](https://cloudacademy.com/library/)

 [**My Profile**](https://cloudacademy.com/profile/)

 [**Resources**](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/creating-an-ec2-instance/?context_id=954&context_resource=lp)

 [**Support**](https://cloudacademy.com/contact-us/)



 [**Capgemini - India**](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/creating-an-ec2-instance/?context_id=954&context_resource=lp)

* 

1. [Home](https://cloudacademy.com/)
2. [Training Library](https://cloudacademy.com/library/)
3. [**Create Your First Amazon EC2 Instance (Linux)**](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/?context_id=954&context_resource=lp)

**Creating an EC2 Instance**

**58m 31s** left

[100%](https://928905109032.signin.aws.amazon.com/console" \t "_blank)

[Open Environment](https://928905109032.signin.aws.amazon.com/console" \t "_blank)

[Setup completed](https://928905109032.signin.aws.amazon.com/console" \t "_blank)

**Credentials**

Account ID

Copy

Username

Copy

Password

Copy

Region

Copy

PEM[Download](https://s3-us-west-2.amazonaws.com/clouda-labs-key-pairs-production/aws-keypairs/928905109032.pem)

PPK[Download](https://s3-us-west-2.amazonaws.com/clouda-labs-key-pairs-production/aws-keypairs/928905109032.ppk)

**Lab Steps**

[1](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/log-in-to-the-amazon-web-service-console/?context_id=954&context_resource=lp)

[Logging in to the Amazon Web Services Console](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/log-in-to-the-amazon-web-service-console/?context_id=954&context_resource=lp/?context_id=954&context_resource=lp)

**[2](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/creating-an-ec2-instance/?context_id=954&context_resource=lp)**

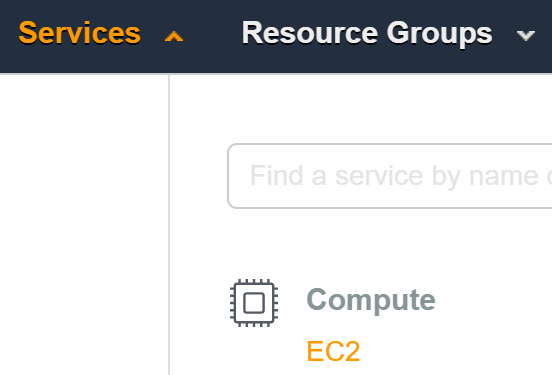
[**Creating an EC2 Instance**](https://cloudacademy.com/lab/create-your-first-amazon-ec2-instance/creating-an-ec2-instance/?context_id=954&context_resource=lp/?context_id=954&context_resource=lp)

Converting a PEM Key to a PPK Key

Connecting to an Instance using SSH

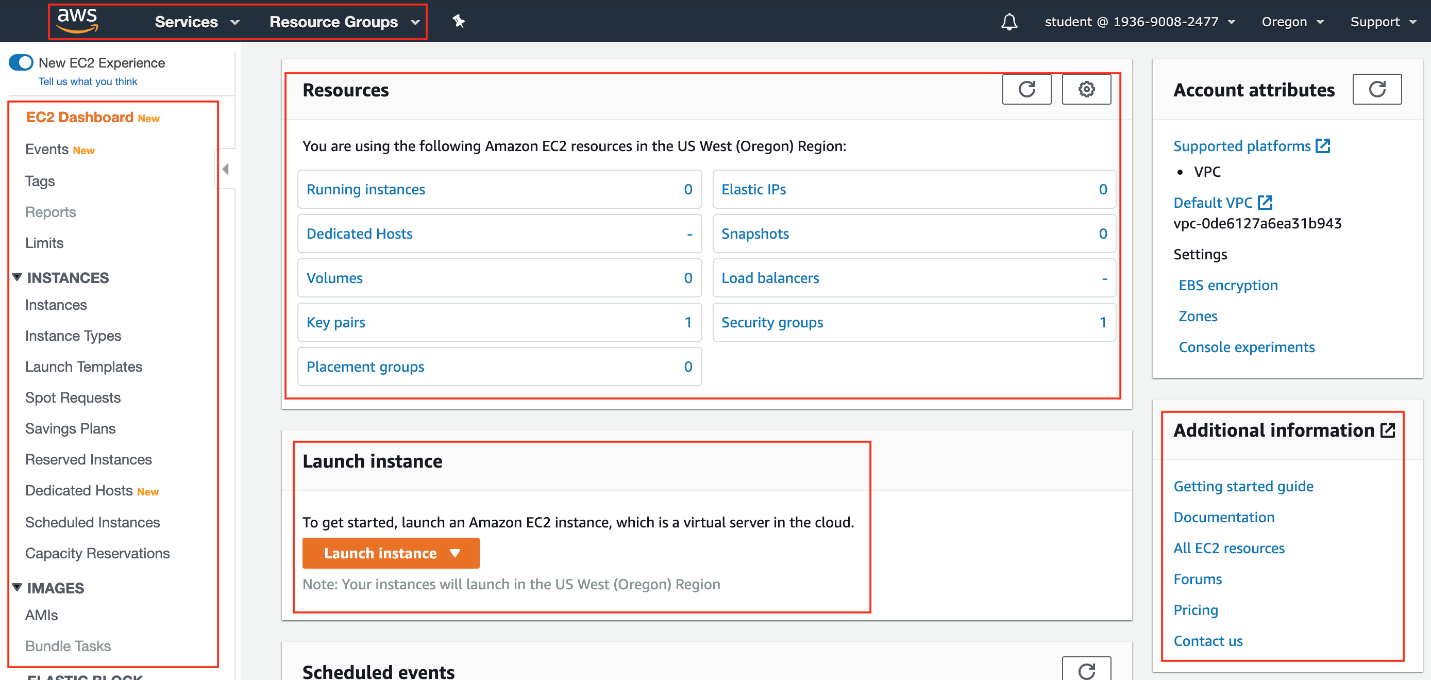
**Instructions**

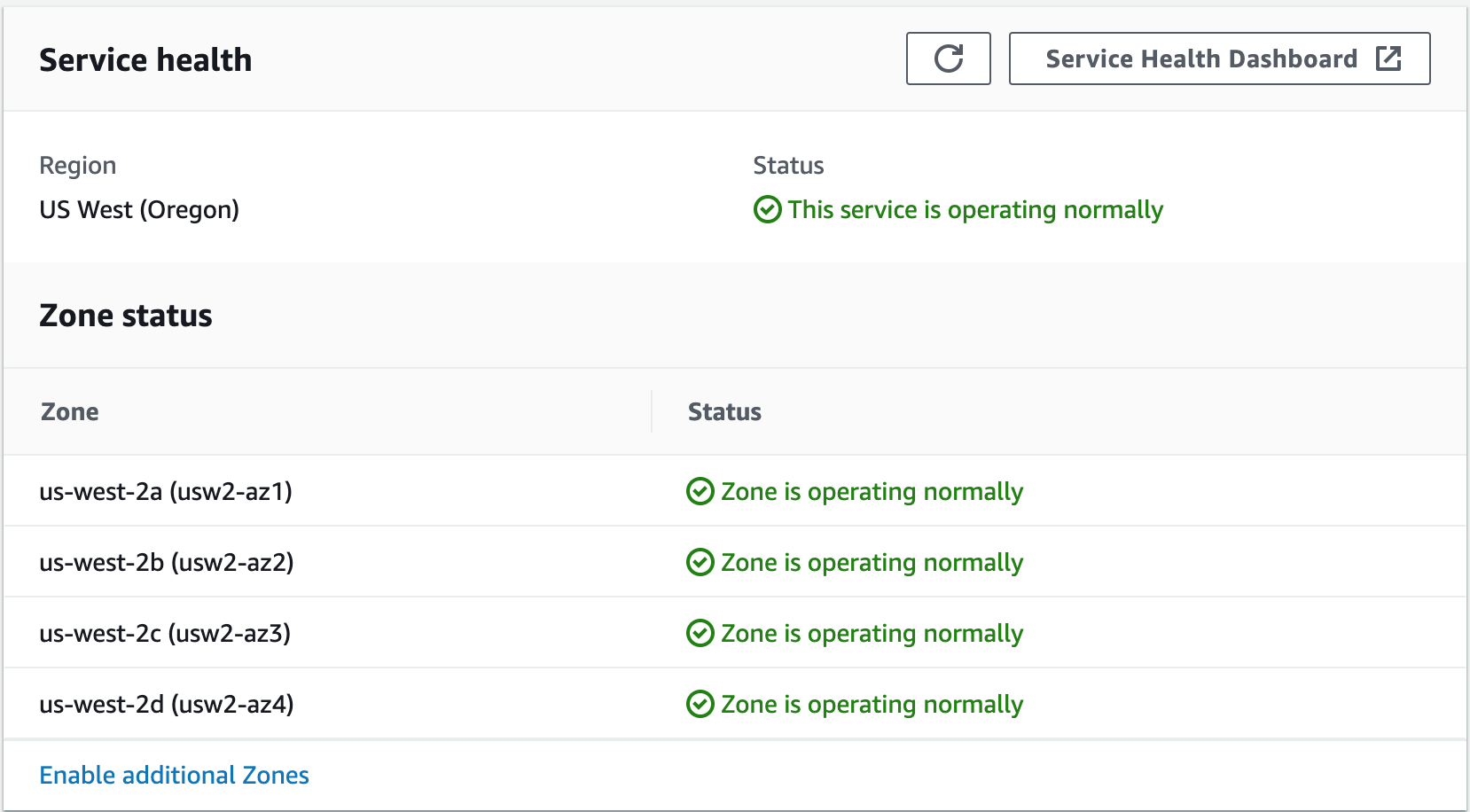
1. Select **Services** > **EC2** from the AWS Management Console home page:



You are placed in the EC2 Dashboard.

2. Since this may be your first exposure to the EC2 Dashboard, it's worth spending a minute or two learning a few important parts of the dashboard:





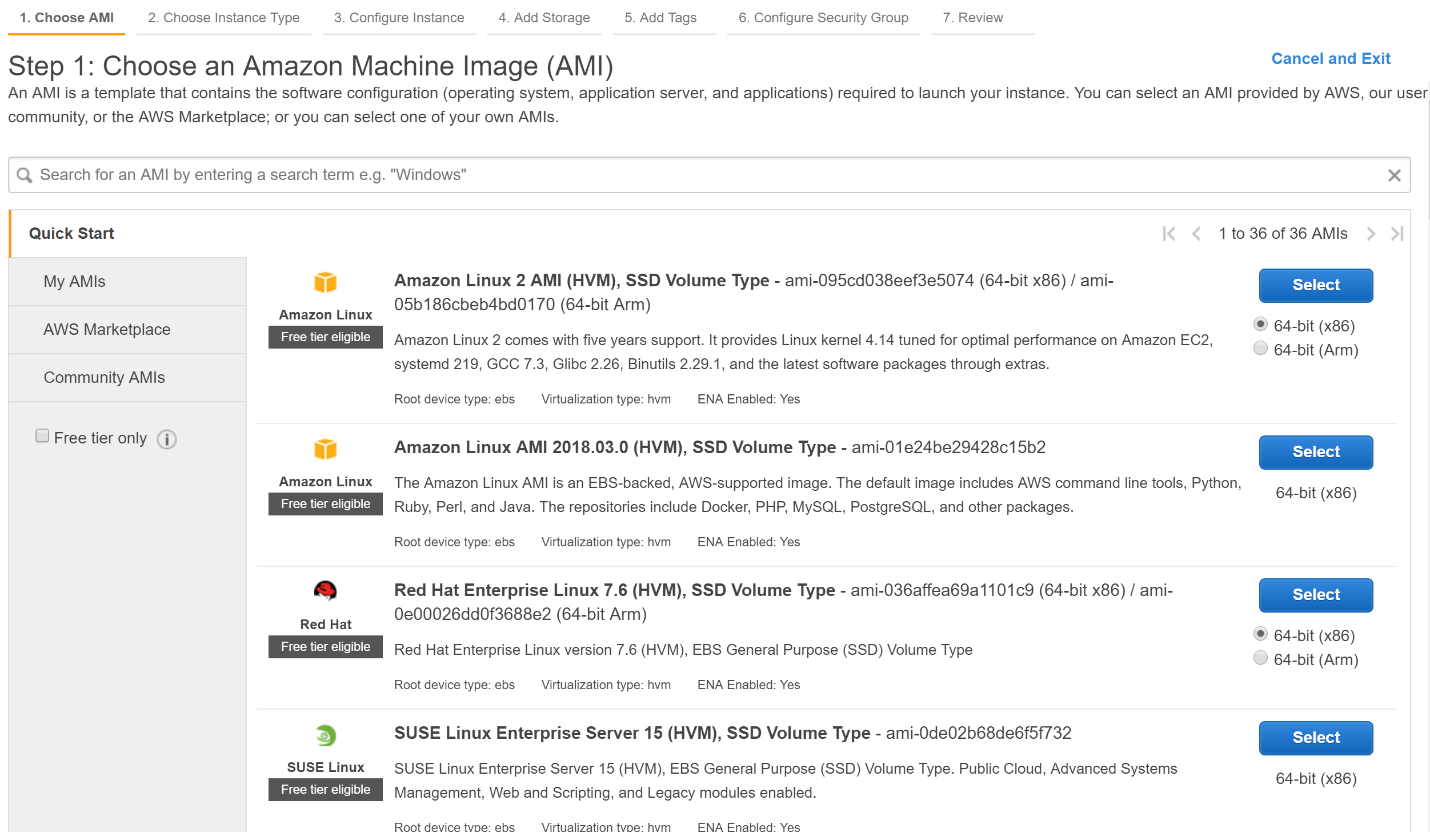
From left to right, top to bottom:

* Additional navigation options are across the top-left of the Dashboard
* Basic account information, current region, and **Support** options are across the top-right
* Navigation to additional EC2 resources and features are located in the left pane
* **Resources** section - provides a high-level summary of current EC2 resource usage
* **Create Instance**section**-**Offers a single click to start the process of launching a new EC2 instance (you'll do that next)
* **Service Health** section - Simple and quick way to obtain the high-level service health in your region (or click **Service Health Dashboard** for a more comprehensive AWS health check)
* **Additional Information** - Context sensitive help on Getting Started (with EC2) or a complete listing of all AWS documentation

3. Click **Launch Instance**.

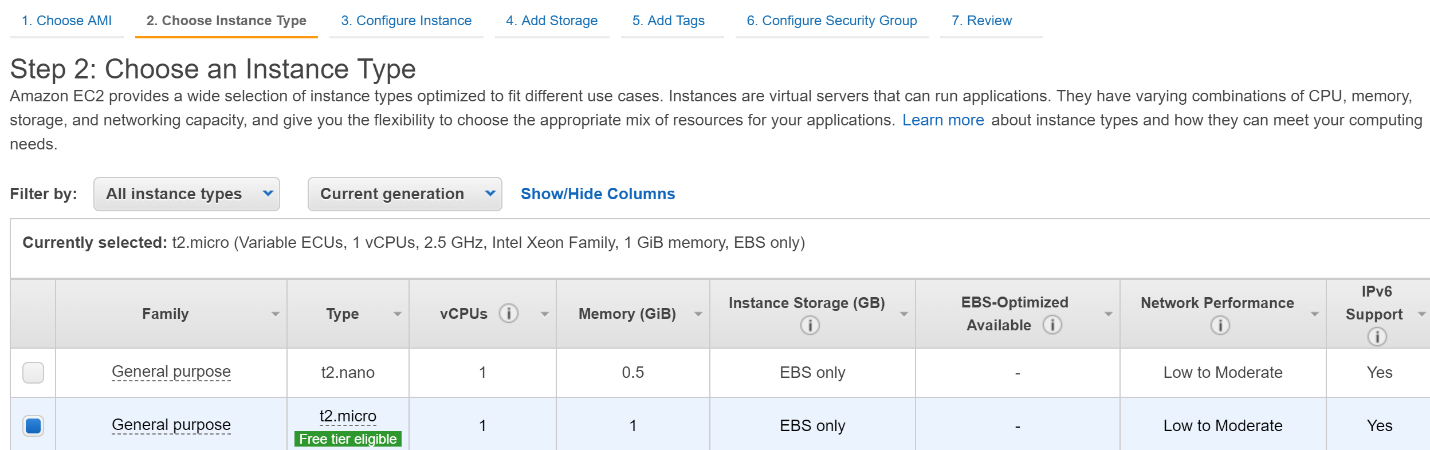
A seven-step wizard is started. That may sound like a lot, but don't worry... the instructions will guide you through the basics for each step.

4. Click the top **Select** button to choose the **Amazon Linux 2 AMI** (Amazon Machine Image):



As you can see, Amazon provides many AMIs, including the most popular versions of Linux and Windows, often in 32-bit and 64-bit variants. Look at the supporting text to find out what other software packages and development languages are already installed on the image (such as Perl, Python, Java, etc.). You can think of AMIs as the blueprint or DNA of the instance you plan to launch.

5. On the **Choose an Instance Type** page, you should not change any options. Simply make sure the default **t2.micro**is selected:

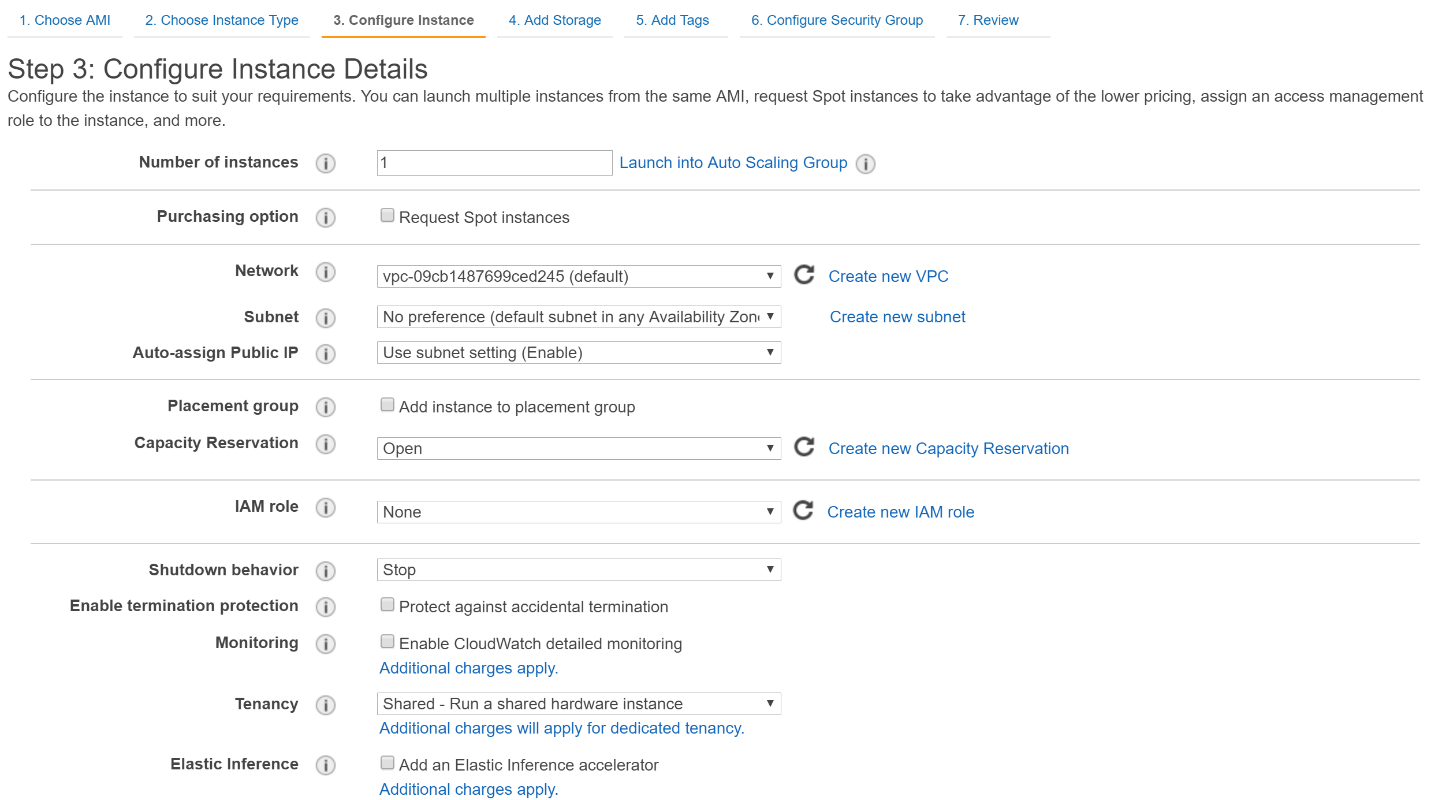


For whatever Instance Type is selected, the **Currently selected** list provides a helpful summary of hardware resources (such as the CPU type, number of virtual CPUs, and memory).

6. Click **Next: Configure Instance Details** when ready to continue.

*Tip*: There are **Previous** and **Next** buttons in the wizard for additional navigation options as you configure your instance.

Take a minute to look over the **Configure Instance Details** page:

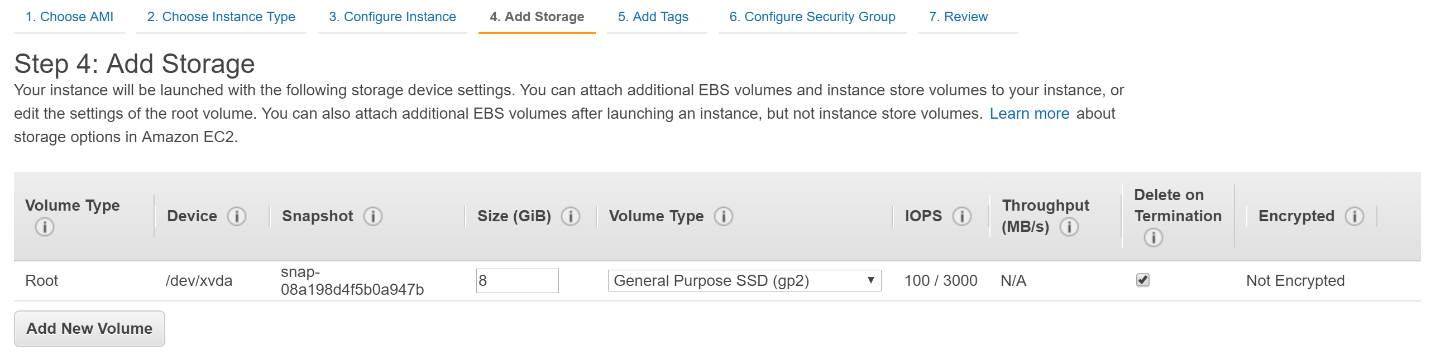


You can configure many different options on this page of the wizard, but it's best to keep your first launch simple. Skim the different fields, but leave the default values. If you are particularly interested in any particular field, hover over the **i** information icon next to it for a basic description.  The information icon is a useful feature for easing your learning curve while using the AWS Console. In many cases, the help text also includes a link to related documentation. To summarize a few key points:

* You will launch a single instance
* The Cloud Academy Lab environment has created a default VPC (Virtual Private Cloud) for you to launch your instance into
* The EC2 service will launch the instance into one of several subnets in the US West (Oregon) region

7. Click **Next: Add Storage**.

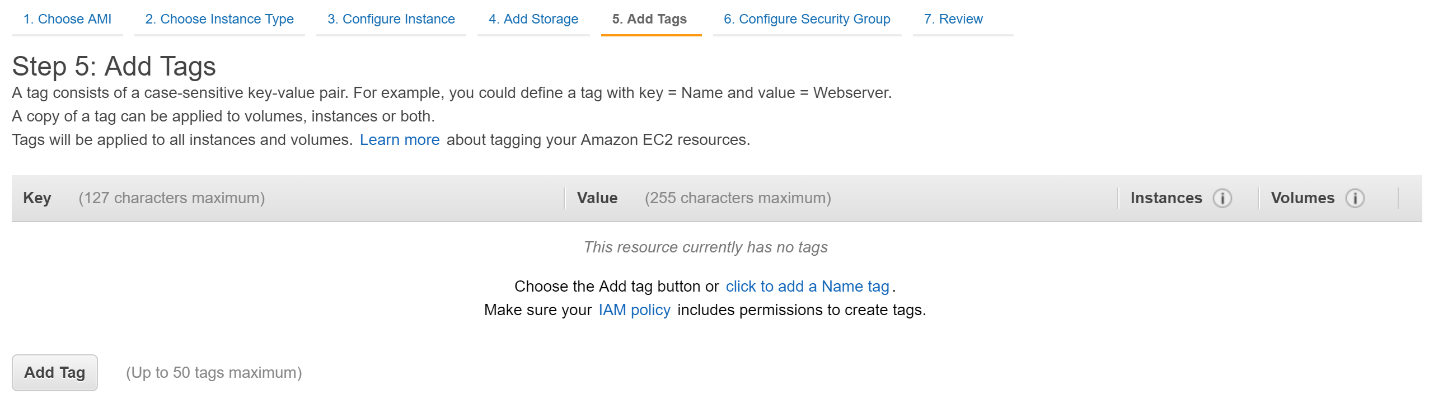
The **Add Storage** page enables you to further configure storage options:



The default values work fine here too. There is no need to add additional volumes, encrypt volumes, or change any other settings. Simply note this is where you can change storage settings if needed.

8. Click **Next: Add Tags** when ready.

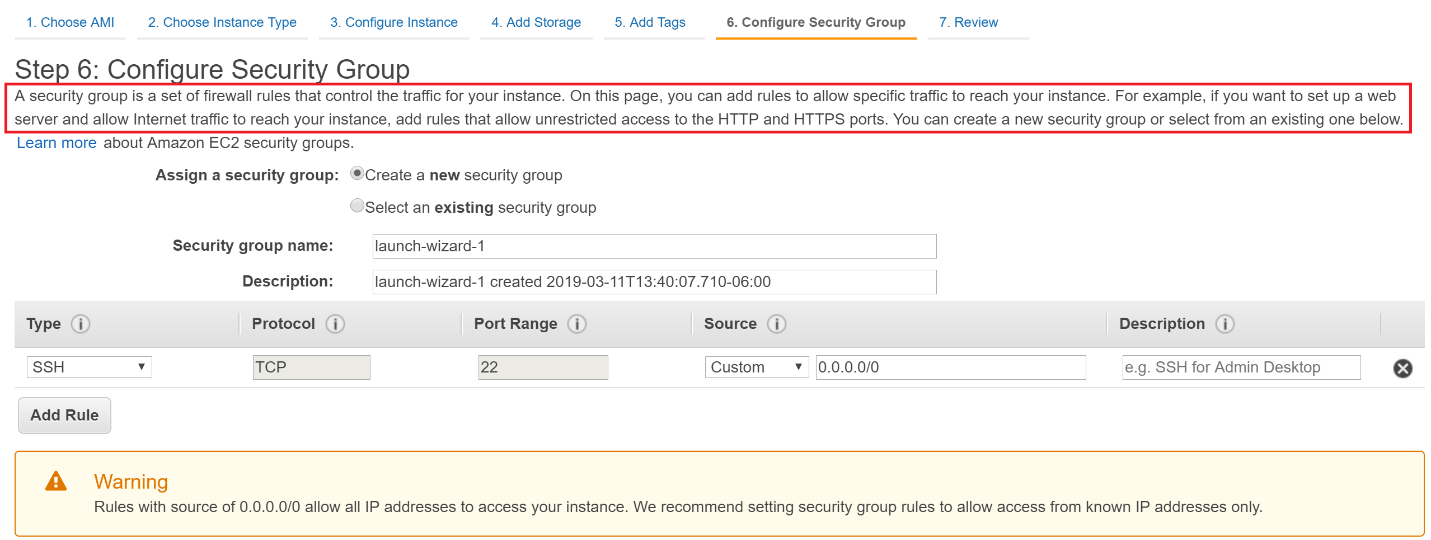
 The **Add Tags** page provides a helpful way to organize your EC2 instances:



Tags are specified as Key/Value pairs. They are not mandatory although it is useful to tag all of your AWS resources in production environments to stay organized. You can leave the tags empty for this Lab.

9.Click**Next: Configure Security Group** when ready.

Read the supporting text near the top of the **Configure Security Group** page of the wizard:

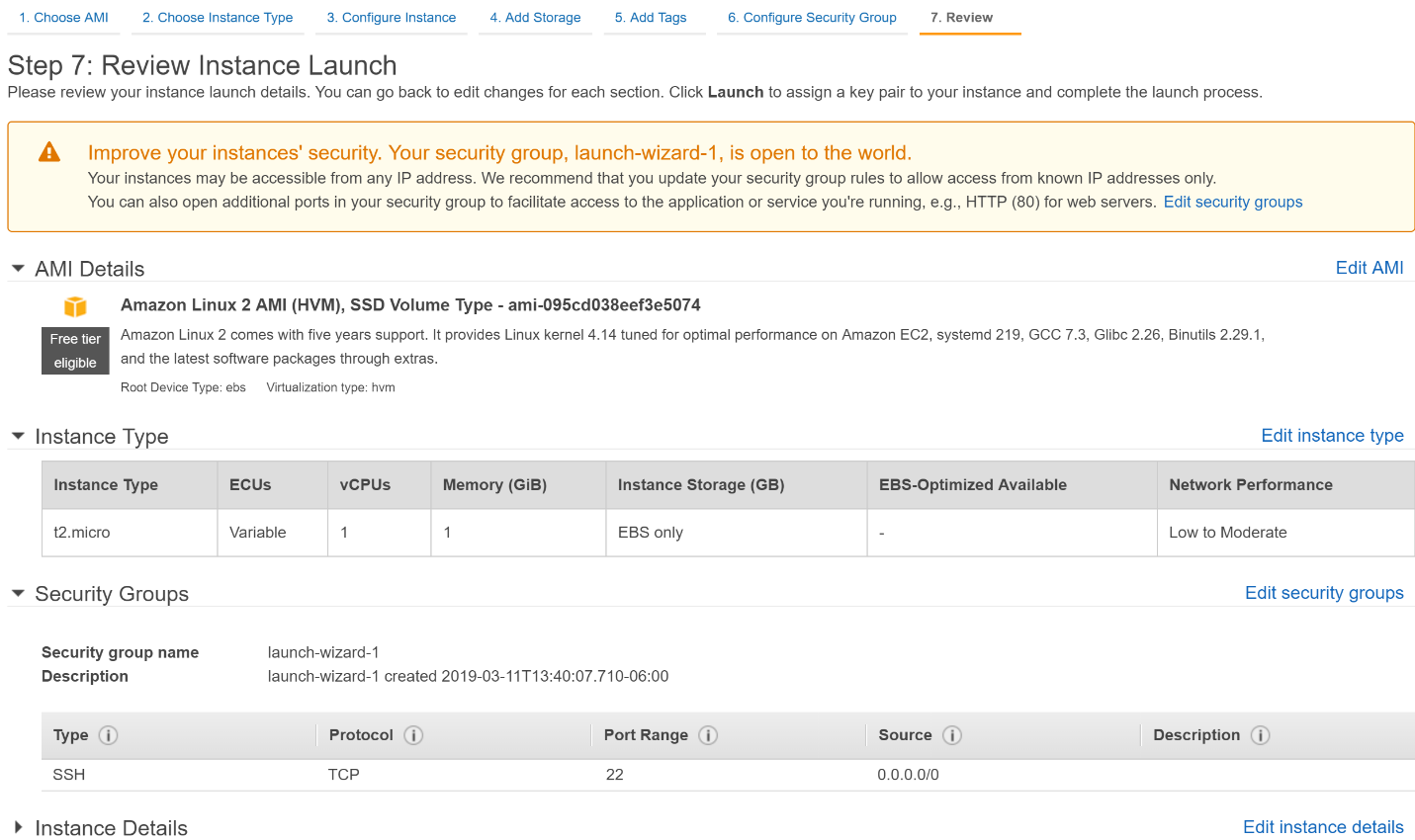


The **Warning** from AWS is letting you know the default configuration for the security group that is about to be created will grant SSH access from any source IP address (0.0.0.0/0). Production environments should be more restrictive. For the purposes of this Lab, this configuration is fine.

*Tip*: A handy feature for testing purposes is to select **My IP** from the **Source** drop-down. That will restrict SSH access to only your current IP address. In network environments with Dynamic Host Configuration Protocol (DHCP), multiple routers or firewalls, and other features that make IP addresses subject to change, this setting is not a permanent security feature. However, it is sometimes a helpful feature while you perform various tests using your EC2 instance.

10. Click **Review and Launch** when ready.

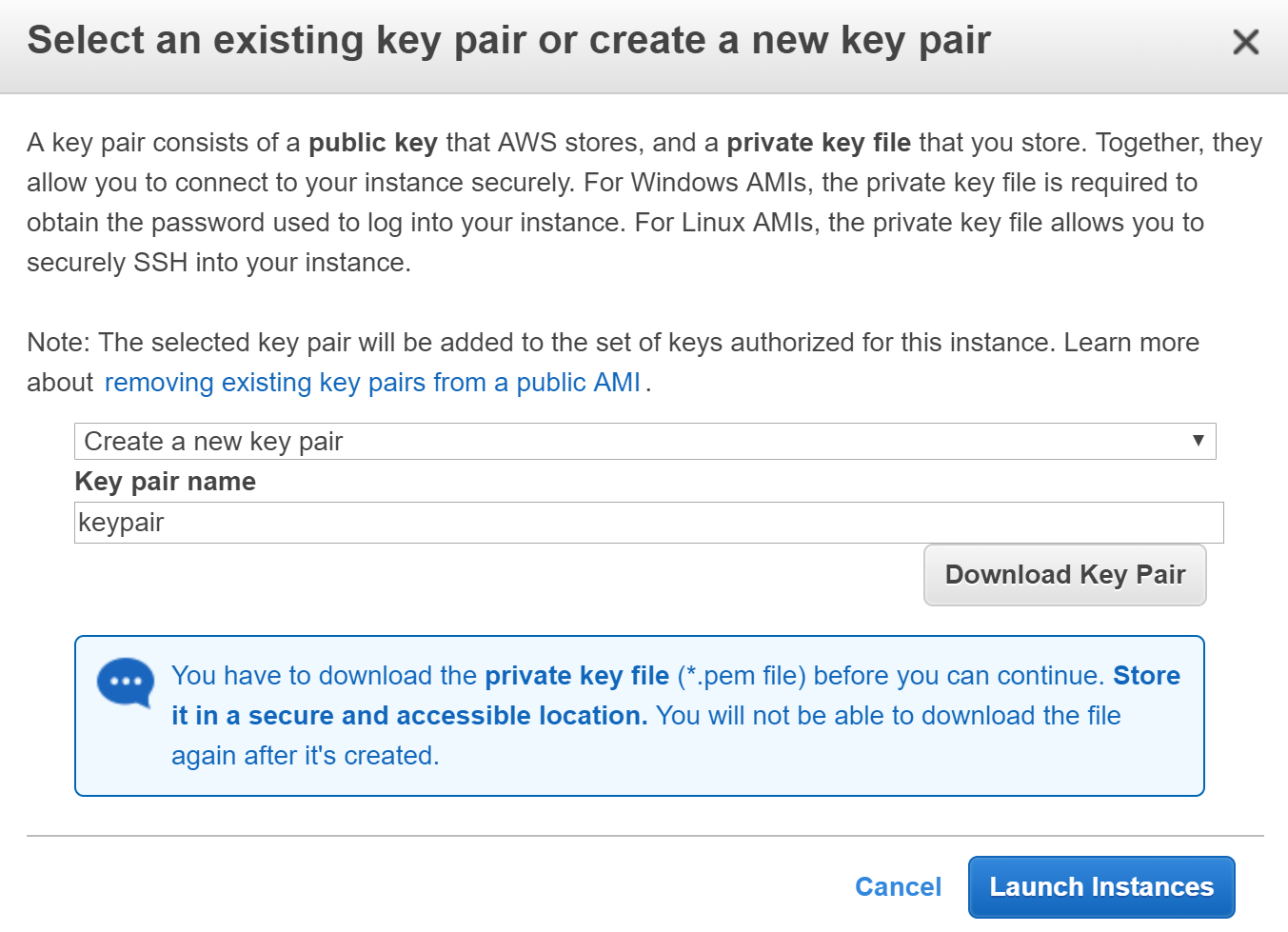
Spend a few minutes expanding/collapsing the various sections on the **Review Instance Launch** page of the wizard:



Be sure to look over the **Instance Type**, **Instance Details** and **Storage** sections. You do not need to change any of these settings at this point, but it's helpful to learn the type of information and configuration options available.

11. Click **Launch**when ready.

12. In the **Select an existing key pair or create a new key pair** dialog box, select **Create a new key pair.**Enter *keypair* for the **Key pair name** and then click **Download Key Pair:**

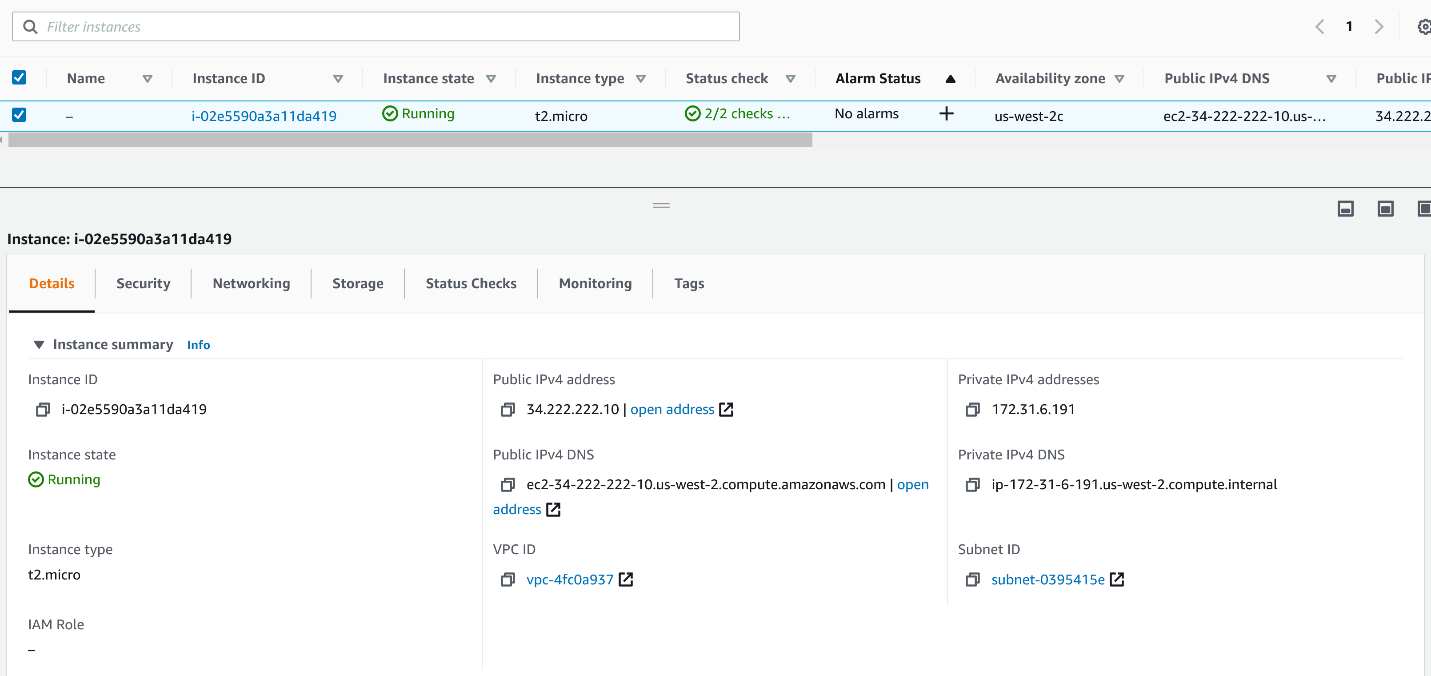
****

The download will create a file named keypair.pem on your local system. It contains a private key that you can use to connect to the EC2 instance via SSH.

13. Click **Launch Instances**. A confirmation page will let you know that your instance is launching.

14. Click the **View Instances** button (lower right) to close the confirmation page and return to the **Instances** screen of the EC2 console.

You can view the status of your instance on the **Instances** screen of the EC2 console:



The **Details** tab contains a wealth of information on your instance. When you launch an instance, its initial **Instance state** defaults to **Pending**. After the instance starts, its **Instance state** transitions to **Running**, and it receives a**Public IPv4** address and **Public IPv4 DNS** name. It typically takes about 30 seconds for the AWS Linux instance to transition to a running state.

Congratulations...you just launched your first EC2 instance

172.31.41.135

ip-172-31-41-135.us-west-2.compute.internal

**Summary**

In this Lab Step, you launched an EC2 instance. You learned key areas of configuration for your EC2 instance using the Launch Instance wizard. Although many configuration options were left at their default values, you should have a pretty good understanding of the type of configuration options available to you within the wizard. Now that you have a running instance, you can treat it as any other Linux host. That is, you can connect to it, install and configure software, develop applications, and other tasks.

*Note*: In this Lab Step you learned how to generate your own SSH key pair for connecting to a running Linux instance. It is important to learn the mechanics behind accomplishing this. However, the Cloud Academy lab engine generates both a PEM and PPK formatted key pair. It is made available to you for the sake of convenience in the **Your lab data**section of the Cloud Academy lab window. This is where you initially copied your random student account password used for signing into the AWS console. In other Labs, you may be directed to use an existing key (the one generated for you), not create your own key prior to launching an instance.

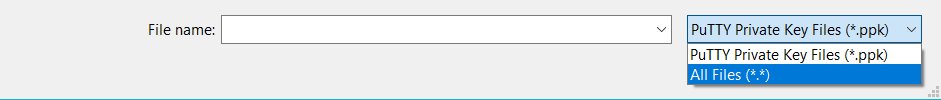
### Instructions

1. If you do not already have PuTTYgen, download the PuTTYgen executable from the following link: [PuTTYgen](https://the.earth.li/~sgtatham/putty/latest/w32/puttygen.exe" \o "PuTTYgen).

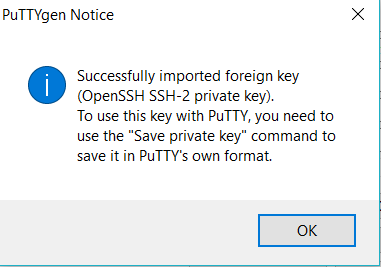
Note: [Cloud Academy enterprise accounts also provide an enterprise bridge feature](https://support.cloudacademy.com/hc/en-us/articles/360044562991) that allows you to bypass corporate network and software installation policies that may otherwise prevent you from completing this lab step.

2. Start PuTTYgen. (no installation is required)

3. Click **Load** and browse to the location of the private key file that you want to convert (for example keypair.pem). By default, PuTTYgen displays only files with a .ppk extension. You'll need to change the drop-down adjacent to **File name** to **All Files** in order to see your PEM file:



4. Select your .pem key file and click **Open**. PuTTYgen displays the following message:



5. Click **OK**. PuTTYgen displays a dialog with information about the key you loaded, including the public key and the fingerprint.

6. Click **Save private key** to save the key in PuTTY's format. Do NOT select a passphrase. (Additional security is not required.) Be sure to save your private key somewhere secure.

**Instructions (Linux / macOS Users)**

1. Open your Terminal application

2. Run the following ssh command:

ssh -i /*path/to/your/keypair.pem* user@server-ip

* server-ip is the Public IP of your server, found on the **Description** tab of the running instance in the EC2 Console
* user is the remote system user (ec2-user for Amazon Linux) that will be used for the remote authentication. In this Lab, you must use **ec2-user**.

Note that the Amazon Linux AMIs typically use ec2-user as a username. Other popular Linux distributions use the following user names:

* Debian: admin
* RedHat: ec2-user
* Ubuntu: ubuntu

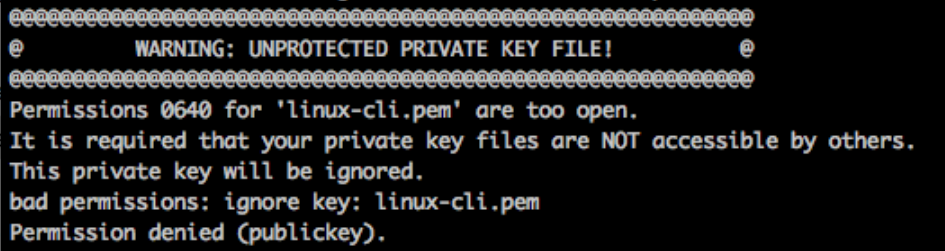
Assuming that you selected the Amazon Linux AMI, your assigned public IP is 123.123.123.123, and your keypair (named "keypair.pem") is stored in /home/youruser/keypair.pem, the example command to run is:

ssh -i /home/youruser/keypair.pem [ec2-user@123.123.123.123](mailto:ec2-user@123.123.123.123)

***Important!***Your SSH client may refuse to start the connection, warning that the key file is unprotected. You should deny the file access to any other system users by changing its permissions. From the directory where the public key is stored on your local machine, issue the following command and then try again:

chmod 600  /home/youruser/keypair.pem

The change mode (chmod) command shown above will change the permissions on your private key file so only you can read and write (modify) it. No other users on the system can modify it, or even read it.

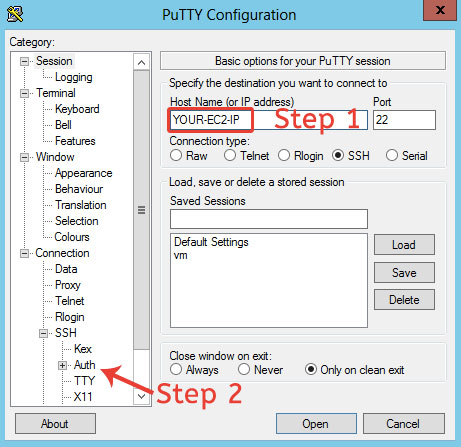


*Tip:*The **Instances** page provides a helpful shortcut for connecting to a Linux instance. Select the running instance and click the **Connect** button. It will formulate an example ssh command for you, including the required key name and public IP address. However, it is still useful to learn the basics of manually using the ssh command.

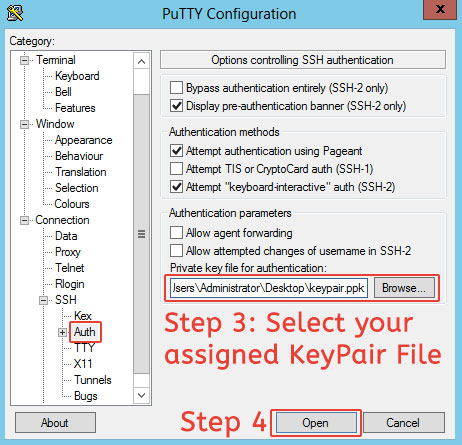
**Instructions (Windows Users)**

Windows has no SSH client, so you must install one. This part of the Lab Step will use PuTTY (freely available [here](http://www.putty.org/) on their website) and a previously converted PEM key (converted from PPK using PuTTYgen).

1. Open PuTTY and insert the EC2 instance public IP Address in the **Host Name** field:

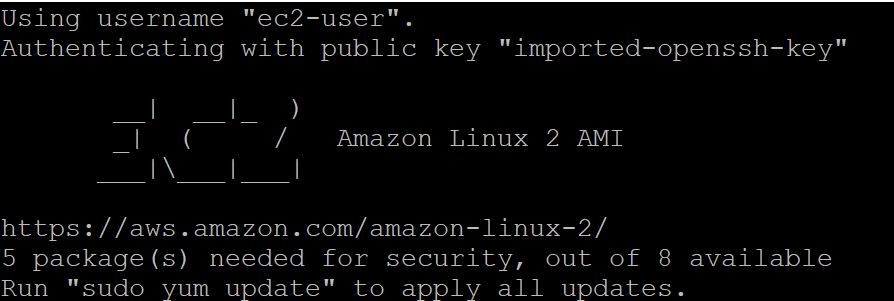


2. Navigate to **Connection**>**SSH**>**Auth** in the left pane and then select the downloaded private key in PPK format:



After a few seconds, you will see the authentication form.

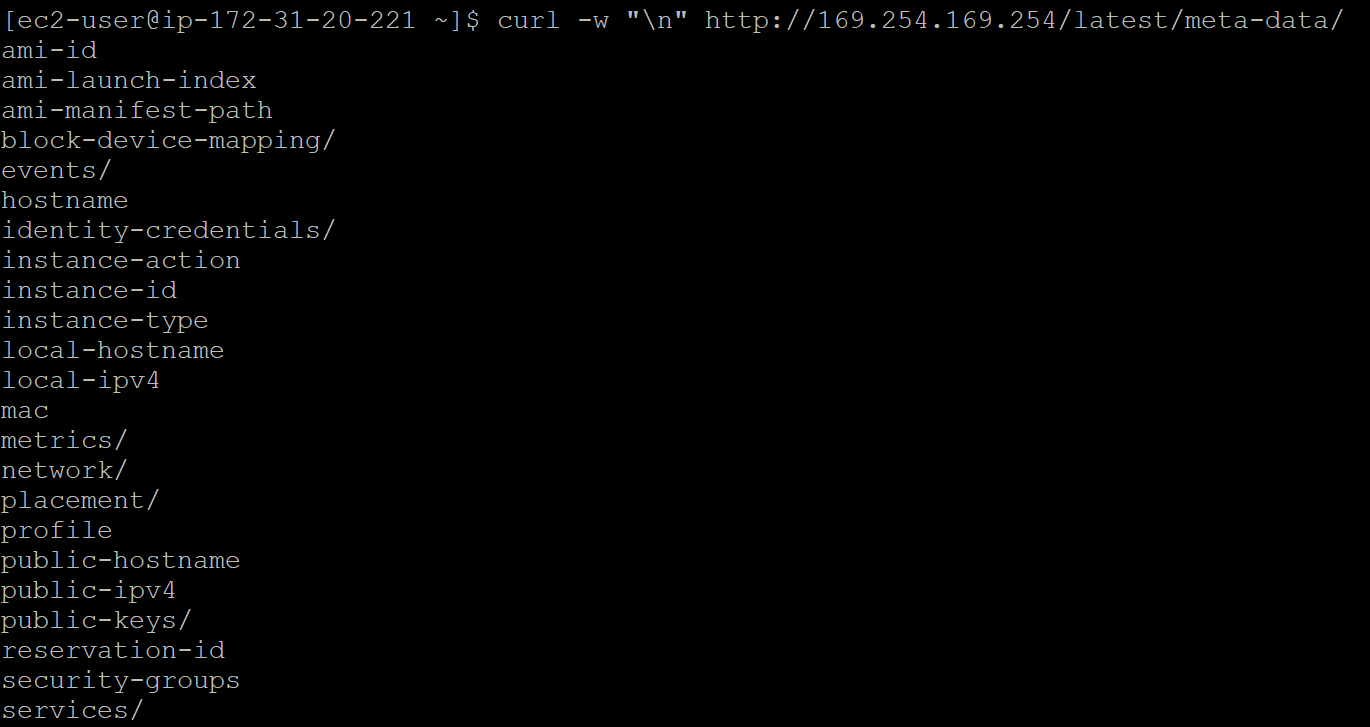
3. Login as *ec2-user* and you will see the EC2 server welcome banner and be placed in the Linux shell:



### Instructions

1. List all instance metadata by issuing the following command:

curl -w "\n" http://169.254.169.254/latest/meta-data/



To extract specific metadata append key words to the end of the http path URL provided in the curl request. For example, you can easily check the list of security groups attached to the instance, its ID, the hostname, or the AMI ID. The "-w" command line option tells curl to write the output to standard output (STDOUT).

2. Enter the following commands to extract specific metadata associated with your running instance:

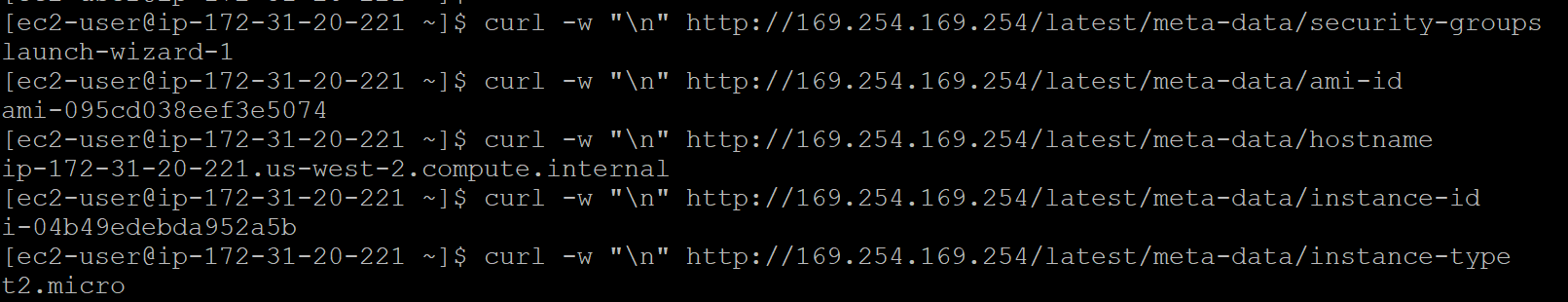
$ curl -w "\n" http://169.254.169.254/latest/meta-data/security-groups

$ curl -w "\n" http://169.254.169.254/latest/meta-data/ami-id

$ curl -w "\n" http://169.254.169.254/latest/meta-data/hostname

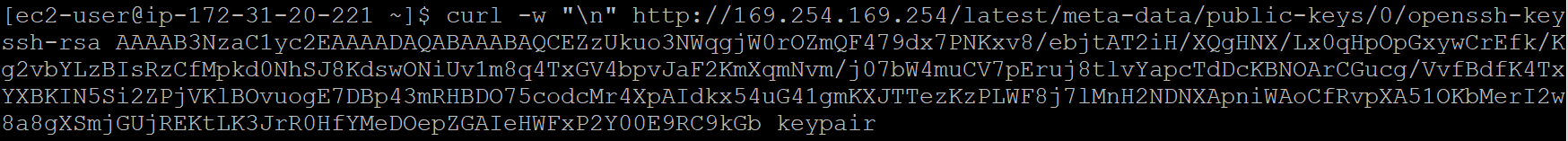
$ curl -w "\n" http://169.254.169.254/latest/meta-data/instance-id

$ curl -w "\n" http://169.254.169.254/latest/meta-data/instance-type



3. Enter the following command to get the public SSH key of the attached key pair using the public-keys metadata:

curl -w "\n" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key



### Summary

In this Lab Step, you learned how you can obtain instance metadata. This metadata can be extremely useful if you want to automate the setup of new instances.