# 



AWS Immersion Day

EC2 Hands-On Lab

Getting Started with Linux on Amazon EC2

# EC2 Overview

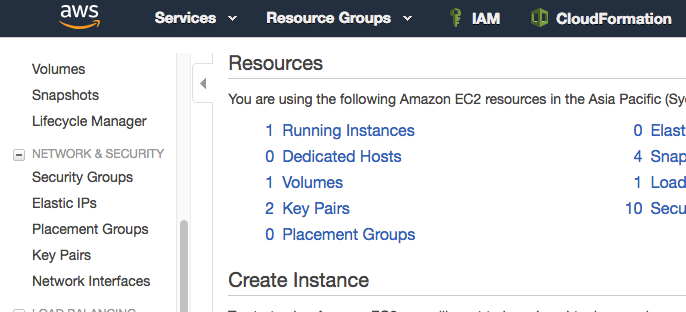
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2’s simple web service interface allows you to obtain and configure capacity with minimal friction. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use.

This lab will walk you through launching, configuring, and customizing an EC2 web server using the AWS Management Console.

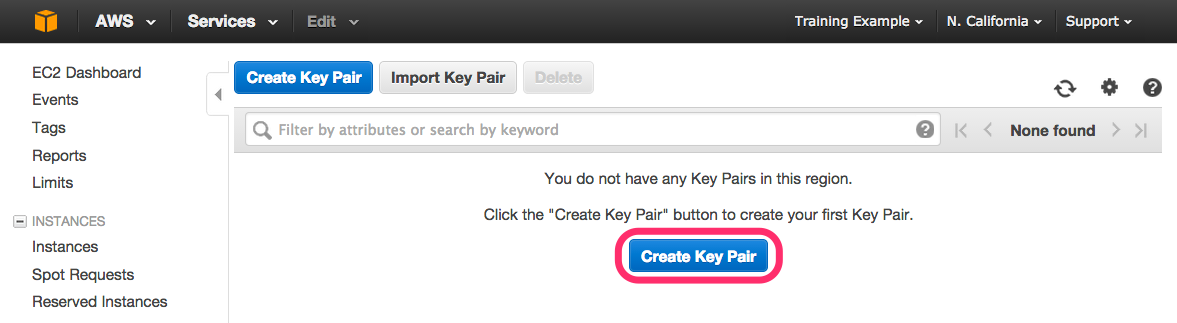
# Create a new Key Pair

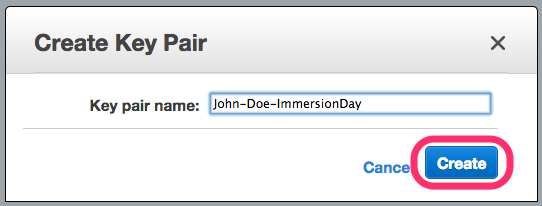
In this lab, you will need to create an EC2 instance using an SSH keypair. The following steps outline creating a unique SSH keypair for you to use in this lab.

1. Sign into the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2>.
2. In the upper-right corner of the AWS Management Console, confirm you are in the desired AWS region (e.g., Sydney).
3. 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.



1. To create a new SSH key pair, click the Create Key Pair button at the top of the browser window.



1. In the resulting pop up window, type *[First Name]-[Last Name]-ImmersionDay* into the **Key Pair Name:** text box and click **Create.  
     
   **
2. 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.
3. Remember the full path to the file .pem file you just downloaded.

# Launch a Web Server Instance

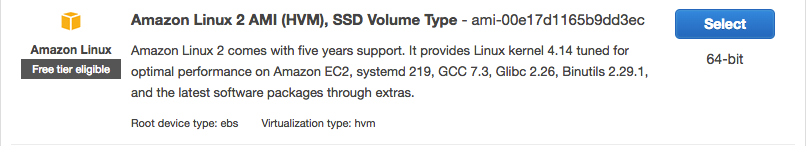
In this example we will launch an Amazon Linux 2 instance, bootstrap Apache/PHP, and install a basic web page that will display information about our instance.

Sign into your AWS Management Console and choose EC2 from the Services menu.

1. Click on Launch Instance

## 

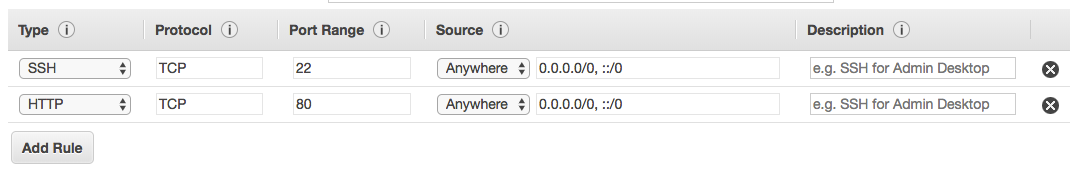
1. In the Quick Start section, select the first Amazon Linux 2 AMI and click Select.



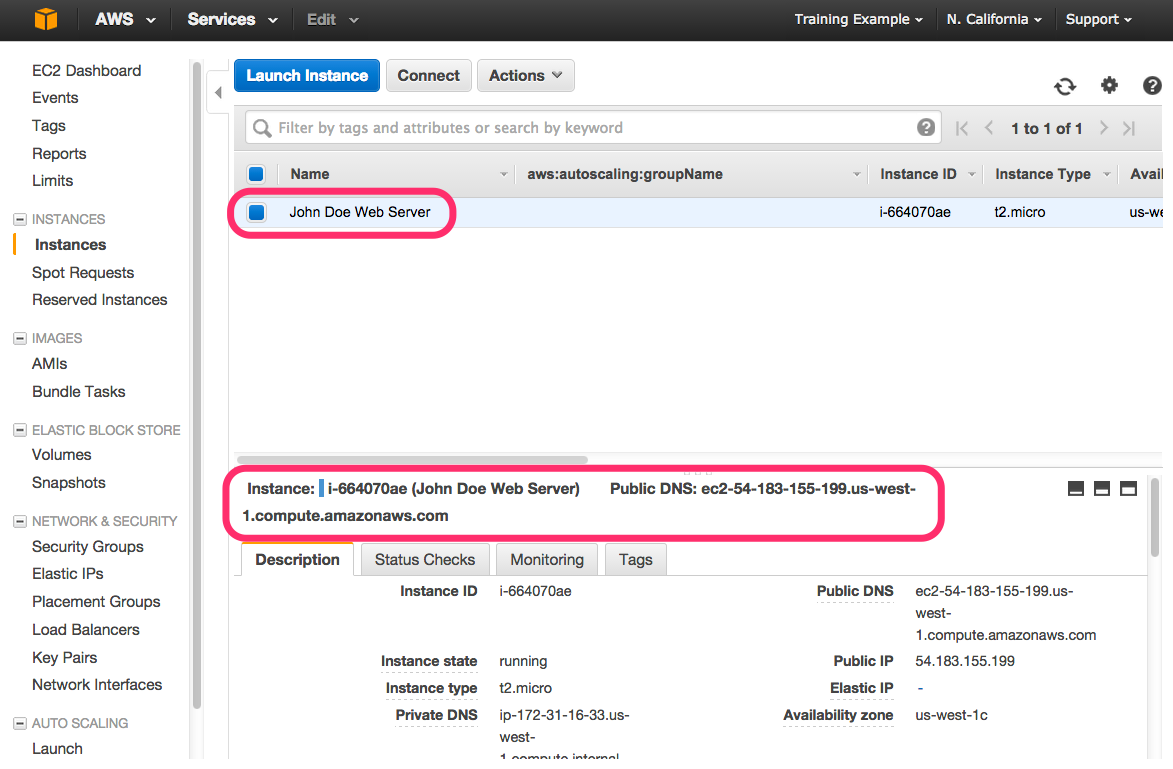
1. In the Choose Instance Type tab, select the t2.micro instance size and click Next.
2. On the Configure Instance Details page, expand the Advanced Details section, copy/paste the script below into the User Data field (this shell script will install Apache & PHP, start the web service, and deploy a simple web page). Click Next.

|  |
| --- |
| #include  https://s3.amazonaws.com/immersionday-labs/bootstrap.sh |

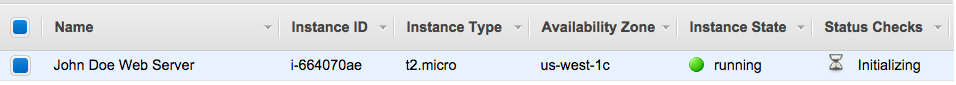
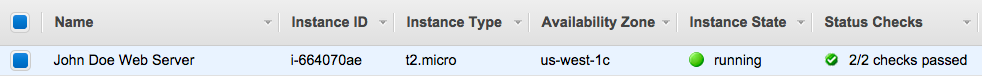
1. On this page you have the ability to modify or add storage and disk drives to the instance. For this lab, we will simply accept the storage defaults and click Next.
2. Here, we choose a “friendly name” for your instance by choosing ‘click to add a Name tag’. This name, more correctly known as a tag, will appear in the console once the instance launches. It makes it easy to keep track of running machines in a complex environment. Name yours as: “[Your Name] Web Server”, and then click Next.
3. You will be prompted to create a new security group, which will be your firewall rules. On the assumption that we are building out a Web server, name your new security group “[Your Name] Web Tier”, and confirm an existing SSH rule exists which allows TCP port 22 from Anywhere. Click Add Rule.:
4. Select HTTP from the ‘Type’ dropdown menu, and confirm TCP port 80 is allowed from Anywhere *(you’ll notice, that “Anywhere is the same as ‘0.0.0.0/0’)*. Click Add Rule.



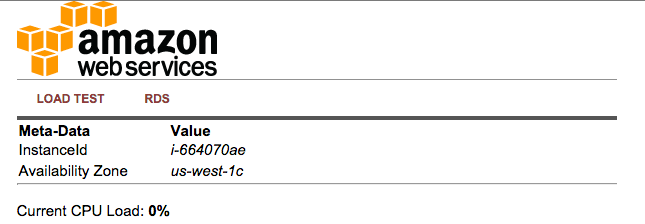
1. Click the Review and Launch button after configuring the security group.
2. Review your cofiguration and choices, and then click Launch.
3. Select the key pair that you created in the beginning of this lab from the drop-down and check the "I acknowledge" checkbox. Then click the Launch Instances button.
4. Click the View Instances button in the lower righthand 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.
5. Click the checkbox next to your web server to view details about this EC2 instance.



# Browse the Web Server

1. Wait for the instance to pass the Status Checks to finish loading.  
   Finished initializing  
   

Open a new browser tab and browse the Web Server by entering the EC2 instance’s Public DNS name into the browser. The EC2 instance’s Public DNS name can be found in the console by reviewing the “Public DNS” name line highlighted above.  
  
You should see a website that looks like the following:

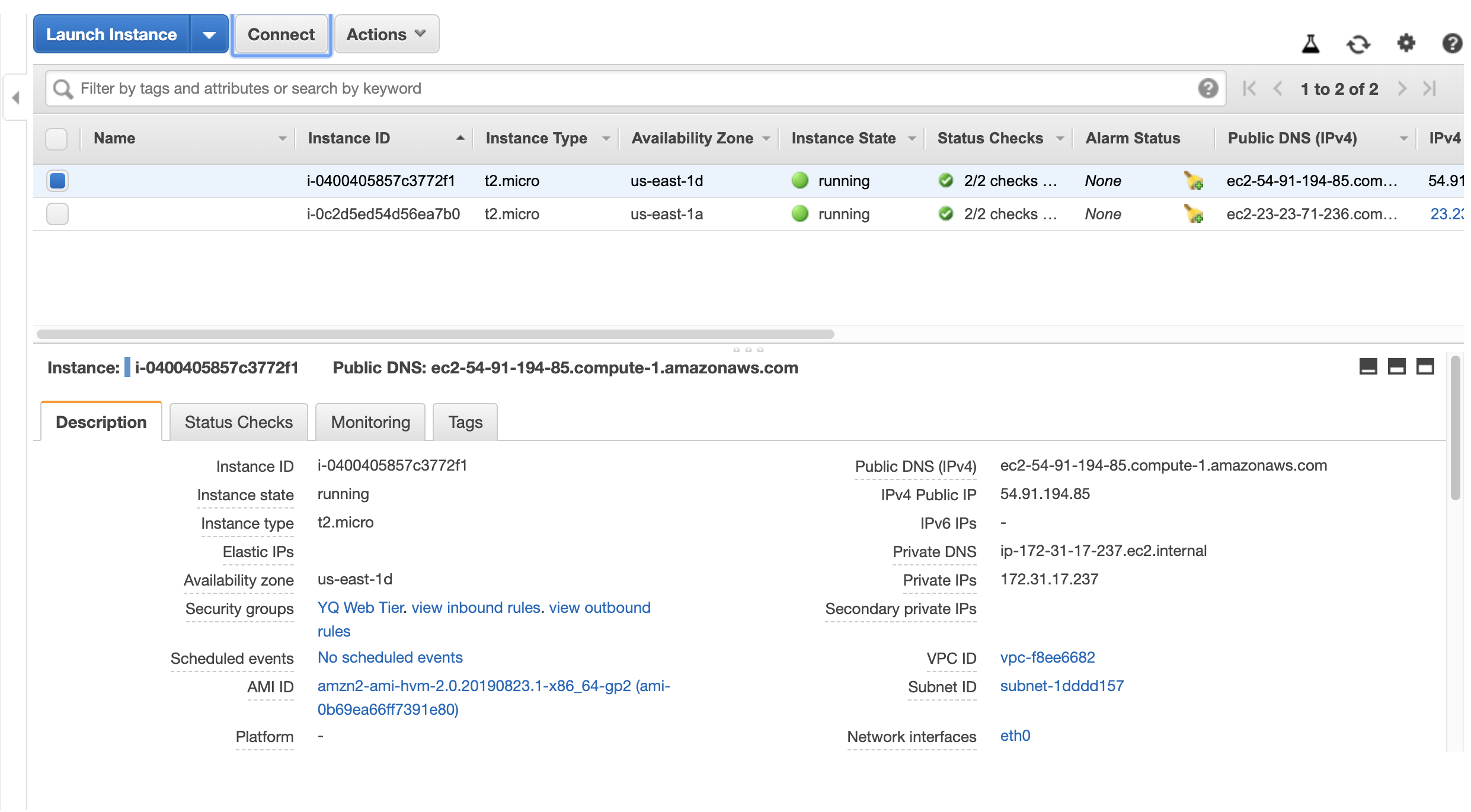


# SSH into the EC2 instance

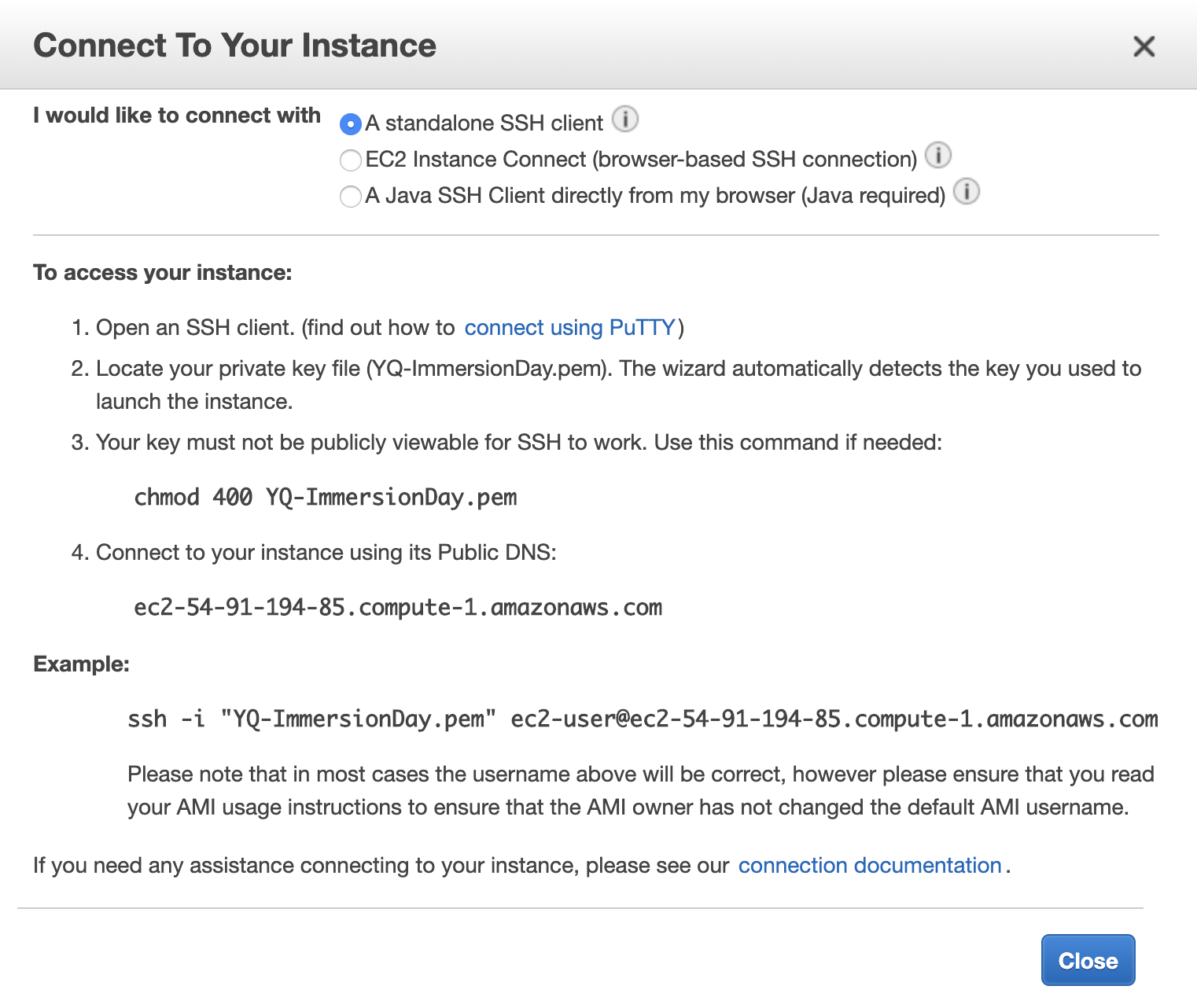
We will now SSH into the newly created EC2 instance.

1. If you are using a Mac, follow this step. If you are using Windows, skip to the next step

On the EC2 console, click on the “Connect” button at the top of the page



You will see the following appear:



Open up your Terminal window, then follow the instructions from steps 2 through 4 in the above illustration (locate your private key file).

1. If you are using Windows, follow this step:

Download and install PuTTY from the [PuTTY download page](http://www.chiark.greenend.org.uk/~sgtatham/putty/" \t "_blank).

Convert your Private Key using PuTTYgen: PuTTY does not natively support the private key format (.pem) generated by Amazon EC2. PuTTY has a tool named PuTTYgen, which can convert keys to the required PuTTY format (.ppk). You must convert your private key into this format (.ppk) before attempting to connect to your instance using PuTTY.

**To convert your private key**

1. From the **Start** menu, choose **All Programs**, PuTTY, PuTTYgen.
2. Under **Type of key to generate**, choose **RSA**.


							RSA key in PuTTYgen
						

If you're using an older version of PuTTYgen, choose **SSH-2 RSA**.

1. Choose **Load**. By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types.


							Select all file types
						

1. Select your .pem file for the key pair that you specified when you launched your instance and choose **Open**. Choose **OK**.
2. To save the key in the format that PuTTY can use, choose **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Choose **Yes**.

**Note**

A passphrase on a private key is an extra layer of protection. Even if your private key is discovered, it can't be used without the passphrase. The downside to using a passphrase is that it makes automation harder because human intervention is needed to log on to an instance, or to copy files to an instance.

1. Specify the same name for the key that you used for the key pair (for example, my-key-pair). PuTTY automatically adds the .ppk file extension.

Your private key is now in the correct format for use with PuTTY. You can now connect to your instance using PuTTY's SSH client.

## Connecting to Your Linux Instance

**To connect to your instance using PuTTY**

1. Start PuTTY (from the **Start** menu, choose **All Programs, PuTTY, PuTTY**).
2. In the **Category** pane, choose **Session** and complete the following fields:
   1. In the **Host Name** box, enter *ec2-user*@*public\_dns\_name (get the public DNS name of your instance from the EC2 console)*
   2. Under **Connection type**, select **SSH**.
   3. Ensure that the **Port** value is 22.


							PuTTY configuration - Session
						

1. (Optional) You can configure PuTTY to automatically send 'keepalive' data at regular intervals to keep the session active. This is useful to avoid disconnecting from your instance due to session inactivity. In the **Category** pane, choose **Connection**, and then enter the required interval in the **Seconds between keepalives** field. For example, if your session disconnects after 10 minutes of inactivity, enter 180 to configure PuTTY to send keepalive data every 3 minutes.
2. In the **Category** pane, expand **Connection**, expand **SSH**, and then choose **Auth**. Complete the following:
   1. Choose **Browse**.
   2. Select the .ppk file that you generated for your key pair and choose **Open**.
   3. (Optional) If you plan to start this session again later, you can save the session information for future use. Under **Category**, choose **Session**, enter a name for the session in **Saved Sessions**, and then choose **Save**.
   4. Choose **Open**.


							PuTTY configuration - Auth
						

1. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host to which you are connecting.
2. Choose **Yes**. A window opens and you are connected to your instance.

**Note**

If you specified a passphrase when you converted your private key to PuTTY's format, you must provide that passphrase when you log in to the instance.

If you receive an error while attempting to connect to your instance, see [Troubleshooting Connecting to Your Instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html).

## Great Job! You have deployed a server, launched a web site and connected to the server via SSH in a matter of minutes!!