

# SSH to Server for Labs

Once you have a copy of the SSH Private Key downloaded to your computer...

We then need to SSH to the Server that the CloudFormation service created for the purpose of conducting our Red Teaming engagements.

We will need a SSH client to access the Server, so common options include:

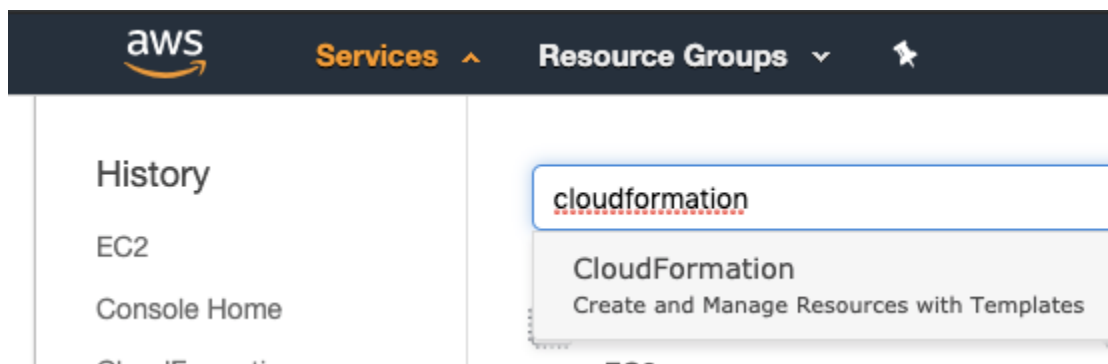
- SSH via macOS
- SSH via Windows 10 April 2018 Update or Newer
- SSH via Older Versions of Windows

## SSH Keys

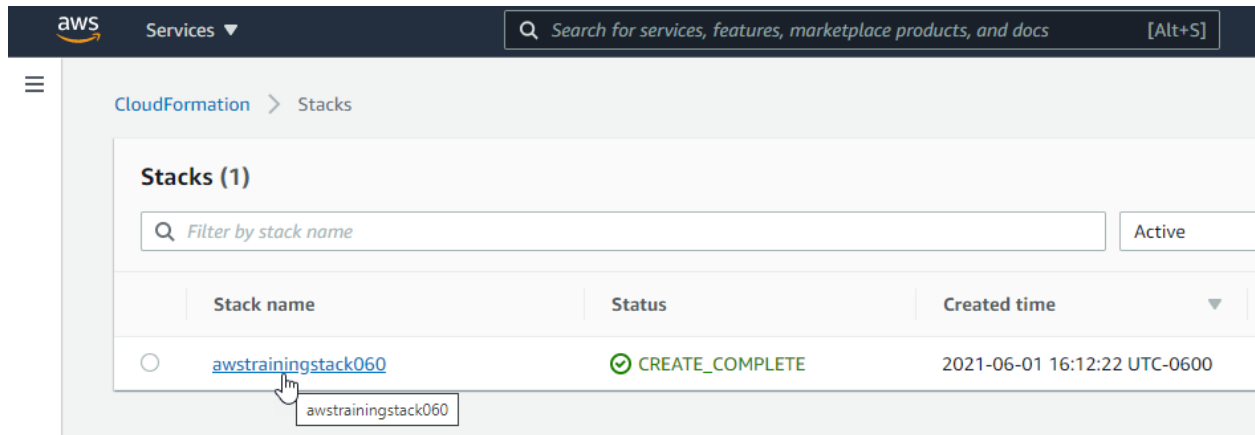
Download a copy of the SSH Keys (e.g. aws\_training\_000.pem, aws\_training\_000.ppk, etc.) via downloading the aws\_training\_000.zip ZIP file from the slides/resources section of this course lab guide and then extracting the contents of this ZIP file into a directory locally on your laptop.

Determine the Public IP Address

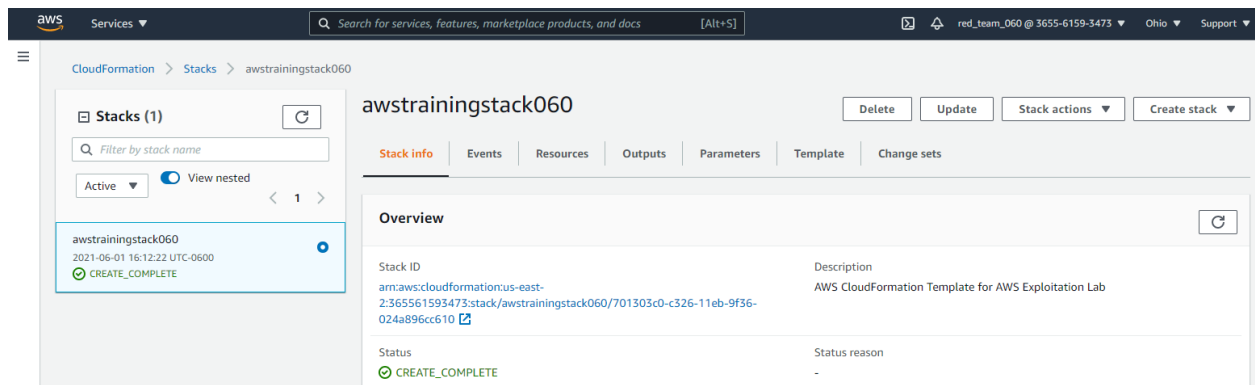
We will browse to the CloudFormation AWS Services via the web interface...



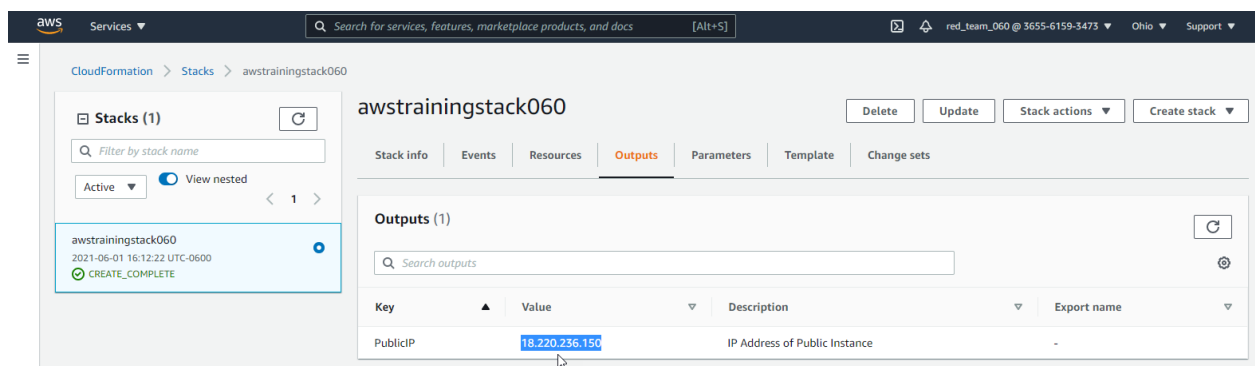
The click on the stack name (e.g. awstrainingstack####, replacing #### with your student number)....



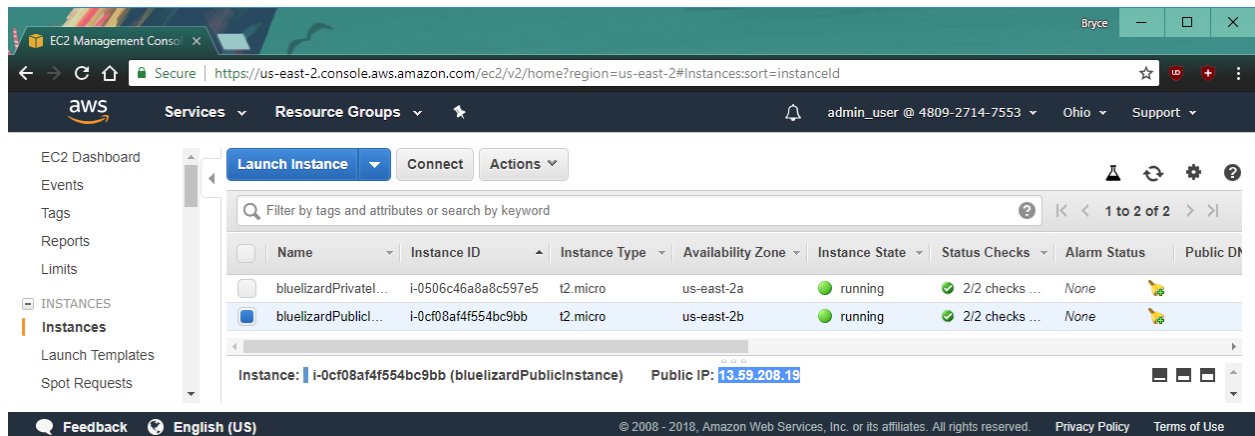
We should then see the "Status" of the CloudFormation stack to be "CREATE\_COMPLETE"...



Click on the "Outputs" tab under the CloudFormation service to see the Public IP of our utility server...



Alternatively... Under AWS Services → EC2, you should now see one instance in the "running" state, and you can obtain the publicly Internet IP address for the public instance (e.g. 13.59.208.19):



## SSH via macOS

Follow these steps:

- Open up the "Terminal" application
- Locate the \*.pem file you created (e.g. "cd" to the directory)

SSH using the following syntax:

```
cd ~/Downloads
chmod 400 aws_training_000.pem
ssh -i aws_training_000.pem ubuntu@ip.ip.ip.ip
sudo su -
```

## SSH via Windows 10 April 2018 Update or Newer

In the Windows 10 April 2018 Update, Microsoft has brought a native Secure Shell (SSH) application to Windows.

If you are running a version of Windows 10 which has the SSH application installed, follow these steps:

Start the Windows "Command Prompt" application

Shortcut in Windows: Use keyboard shortcuts for this route: Windows key + X, followed by A (admin)

Change to the directory that contains your SSH private key

```
cd C:\Users\yourusername\Downloads
```

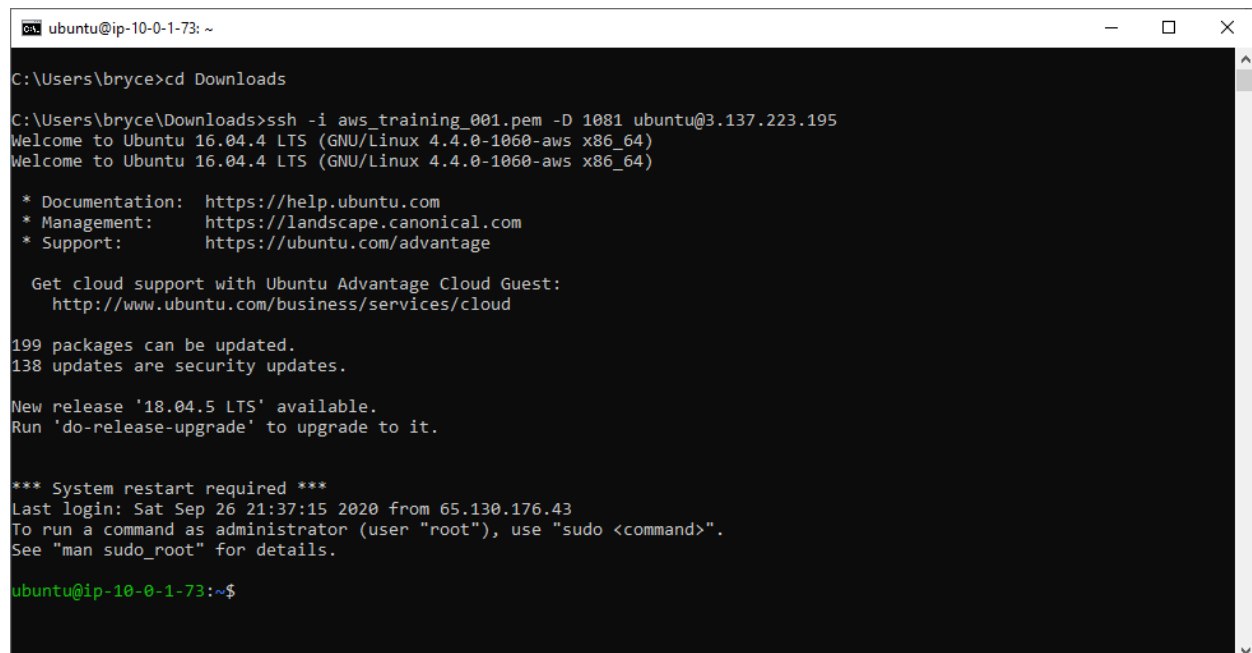
SSH into the remote server using syntax similar to the following:

```
ssh -i aws_training_000.pem ubuntu@ip.ip.ip.ip
```

If prompted, type "yes":

```
The authenticity of host 'ip.ip.ip.ip (ip.ip.ip.ip)' can't be established.  
ECDSA key fingerprint is  
SHA256:q+wU76EpNn7f0DZUKQ1pQt01C6mylF1EbMy25QW2hI8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

For example:

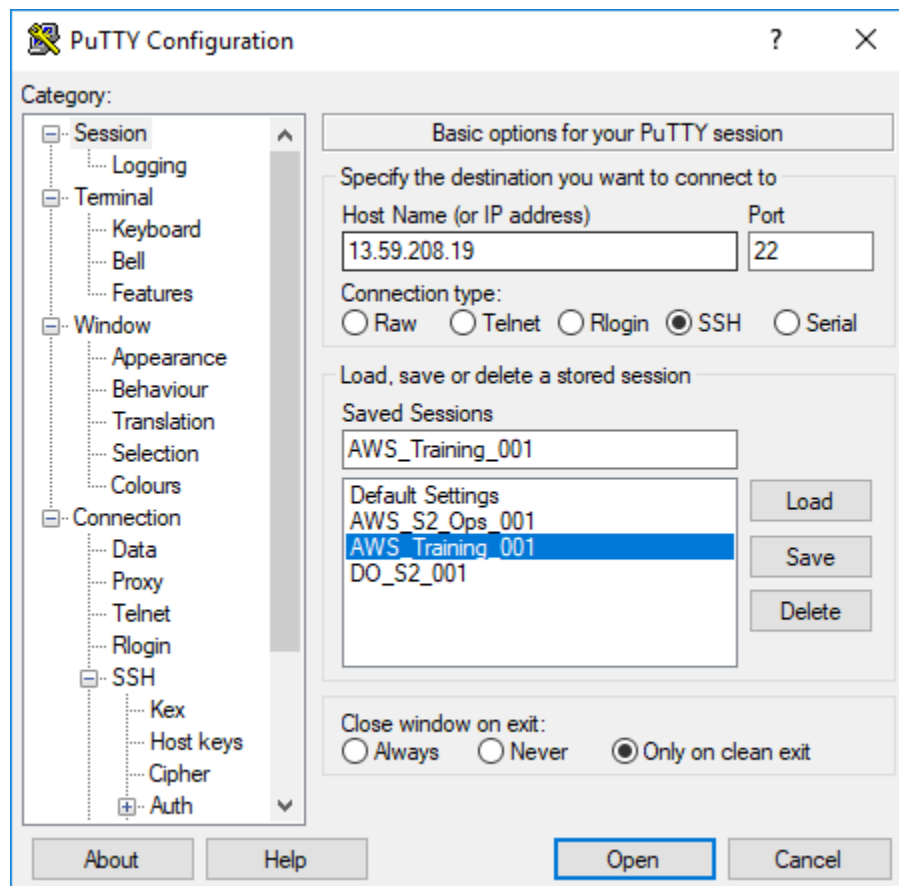


```
ubuntu@ip-10-0-1-73: ~  
C:\Users\bryce>cd Downloads  
C:\Users\bryce\Downloads>ssh -i aws_training_001.pem -D 1081 ubuntu@3.137.223.195  
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1060-aws x86_64)  
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1060-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
199 packages can be updated.  
138 updates are security updates.  
  
New release '18.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Sat Sep 26 21:37:15 2020 from 65.130.176.43  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-10-0-1-73:~$
```

# SSH via Older Versions of Windows

Alternatively, follow these steps for older versions of Windows:

- Download and Install the MSI ('Windows Installer') for Putty (e.g. 64-bit: putty-64bit-0.74-installer.msi) from:  
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
- Download and Install WinScp (e.g. WinSCP-5.17.9-Setup.exe) from:  
<https://winscp.net/eng/download.php> (Links to an external site.)
  - Install for All Users
- Run the "Pageant" application
  - In your system tray, right-click on the "Pageant" icon and click "add key"
  - Select the "aws\_training\_000.ppk" file
- Run the "PuTTY" application
  - Go to the "Session" screen
  - In the "Host Name" field, put the public IP of the EC2 instance that was previously created (e.g. 13.59.208.19 )
  - Under "Saved Sessions" put the name "AWS\_Training\_###" e.g. AWS\_Training\_001
  - Click the "Save" Button



- Within the "PuTTY" application
  - Click the "Open" Button to start the SSH Session
  - Click the "Yes" Button to trust the remote server
  - login as: ubuntu

You should now be SSH'd into the lab environment!

```
ubuntu@ip-10-0-1-244: ~  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
41 packages can be updated.  
27 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-10-0-1-244:~$
```

## Root Access

Most of the labs are designed around being run as the root user, so we leverage sudo once we have SSH into the EC2 instance to gain root access

```
ubuntu@ip-10-0-1-215:~$ sudo su -  
root@ip-10-0-1-215:~#
```

NOTE: If you change into root via an alternative method (e.g. "sudo bash"), you may not have loaded the bash aliases & functions into your root shell (e.g. the `cnio_*` commands), and hence subsequent lab guides may fail until you sudo into root using the above method, or manually load the bash aliases & functions (e.g. "source /shared/other/bashrc.sh").