DATASTAX

DataStax Academy SSH Guide

Table of Contents

Logging into your instance

Use your favorite SSH client to log into the instance. You will need to log into the instance with the user **ubuntu** and the private key pair file that you've downloaded or selected when you launched the instance.

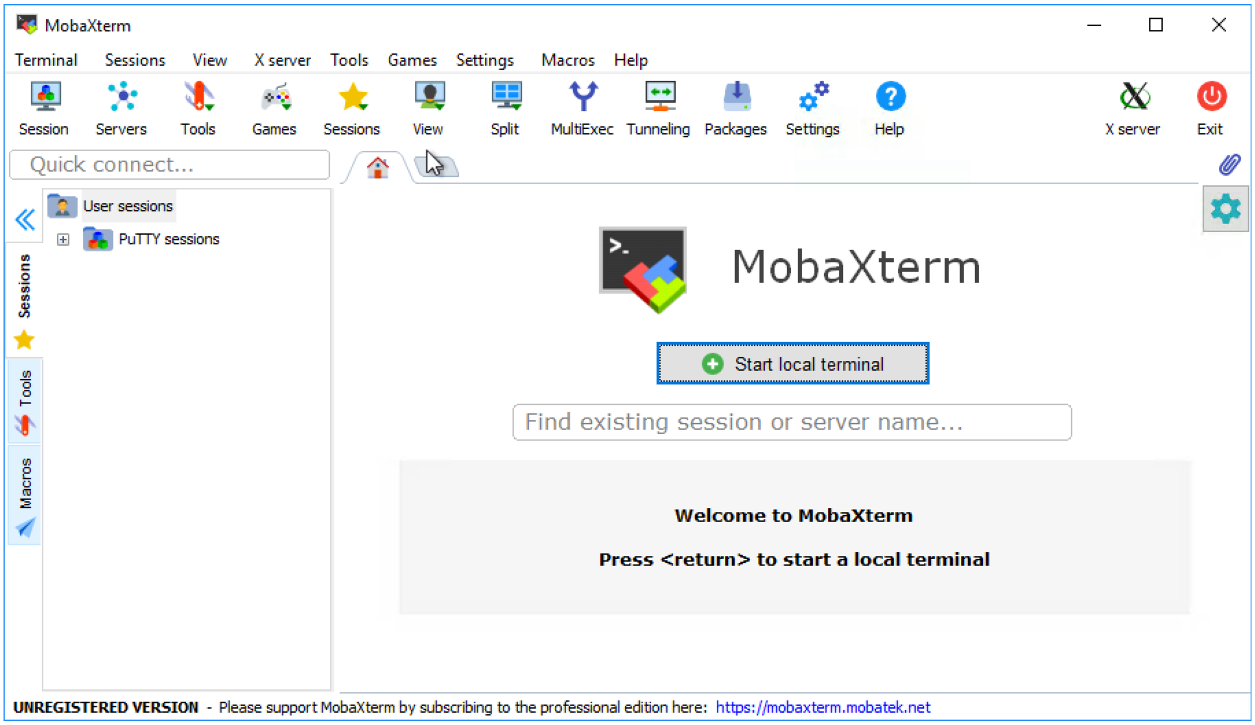
Windows

Windows does not come with a SSH pre-installed. If you do not already have a SSH client that you use, you can consider the following:

MobaXterm

A portable SSH client (with a free version!) that's easy to set up and connect to your instance. You can download from the Mobatek website at https://mobaxterm.mobatek.net.

After starting the application, you should see the following window:



Welcome to MobaXterm

Press <return> to start a local terminal

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Start a local terminal, and then modify the below command to SSH into your instance with the ***ubuntu*** user:

```
ssh -i /drives/c/path/to/privatekey.pem ubuntu@ip-address
```

PuTTY

One of the most popular SSH clients available on Windows. Check out the guide from Amazon on using the PuTTY client: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

Mac OS X / Linux

Both Mac OS X and Linux systems come with a SSH client pre-installed. You can use SSH by opening a *Terminal* window.

First, make sure that the private key file for the instance is not group or world readable:

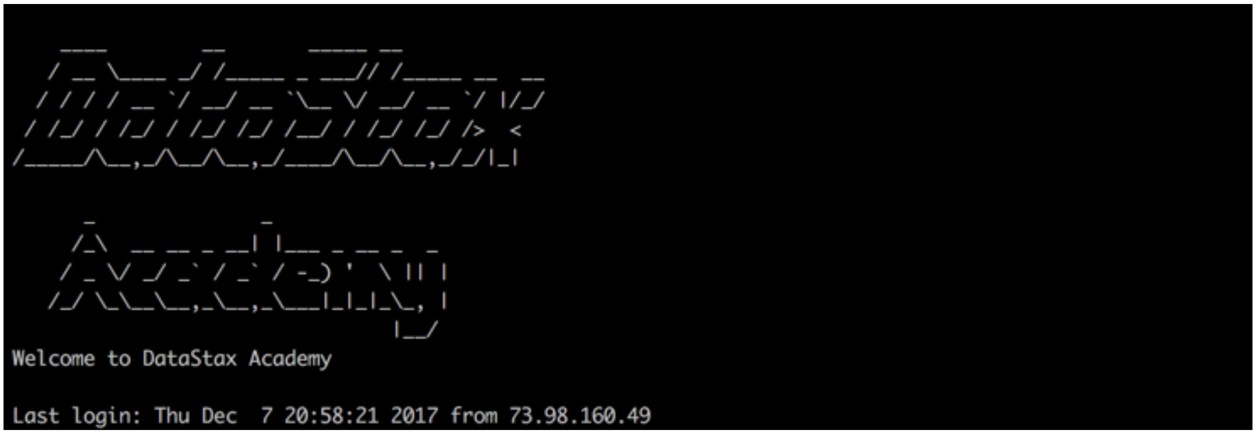
```
chmod 400 /path/to/privatekey.pem
```

Modify the below command to SSH into your instance with the ***ubuntu*** user:

```
ssh -i /path/to/privatekey.pem ubuntu@ip-address
```

Additional documentation on logging into an instance is available from Amazon here:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html

You will see the DataStax Academy banner if you are able to log in successfully.



```
    ____        __        _____ __
   / __ \____ _/ /_____ _/ ___// /_____ __  __
  / / / / __ `/ __/ __ `/\__ \/ __/ __ `/ |/_/
 / /_/ / /_/ / /_/ /_/ /___/ / /_/ /_/ />  <
/_____/\__,_/\__/\__,_//____/\__/\__,_/_/|_|


    _               _
   /_\  __ __ _ __| |___ _ __ _  _
  / _ \/ _/ _` / _` / -_) '  \ || |
 /_/ \_\__\__,_\__,_\___|_|_|_\_, |
                              |__/
Welcome to DataStax Academy

Last login: Thu Dec  7 20:58:21 2017 from 73.98.160.49
```

Troubleshooting

Unprotected private key file (Mac OS X / Linux)

You may fail to login to the instance with the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Permissions 0777 for 'privatekey.pem' are too open.

It is required that your private key files are NOT accessible by others.

This private key will be ignored.

Load key "privatekey.pem": bad permissions

Permission denied (publickey).
```

In this case, please modify the file permissions for the private key file and try again.

```
chmod 400 /path/to/privatekey.pem
```

Too many authentication failures (Mac OS X / Linux)

When logging into the instance you, may see the error message:

```
Received disconnect from 54.153.124.232 port 22:2: Too many authentication
failures

Authentication failed.
```

First, double-check that you are using the corresponding private key file for the key pair set for the instance.

If you are sure that you are using the correct private key file, the problem may be that you have too many keys stored in your ~/.ssh/ directory.

Please check out this post https://serverfault.com/questions/36291/how-to-recover-from-too-many-authentication-failures-for-user-root for possible solutions.

Remote host identification has changed (Mac OS X / Linux)

You may encounter this issue if you regularly spin up new instances. When logging into the instance, you may get the error:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
```

```
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
78:16:03:b0:88:c3:9b:a7:7d:34:87:a5:8b:36:f1:4f.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending RSA key in ~/.ssh/known_hosts:1
ECDSA host key for 127.0.0.1 has changed and you have requested strict
checking.
Host key verification failed.
```

This error can occur when you are connecting to an instance with the same IP address of a different instance you have connected to before.

To fix the error, you can edit your *~/.ssh/known_hosts* file to add the correct host key corresponding with the IP address of the instance you are logging in to.

Alternatively, a more drastic action would be to just completely remove the *~/.ssh/known_hosts* file and let it regenerate once you log into the instance. You should do this only if you understand the implications of removing the file.