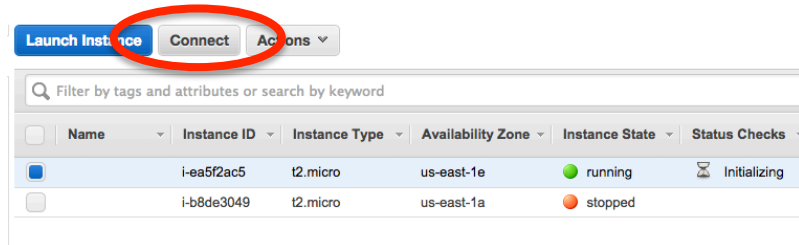


## Connecting to your Instance

Select the instance you created above (it should be running), and then click **Connect**.



If you are using a PC to connect, copy the IP address. If you are using a Mac, copy the “Example” ... this is your connection string.

### Connect To Your Instance ✕

I would like to connect with  A standalone SSH client  
 A Java SSH Client directly from my browser (Java required)

---

**To access your instance:**

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (server-key.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:  

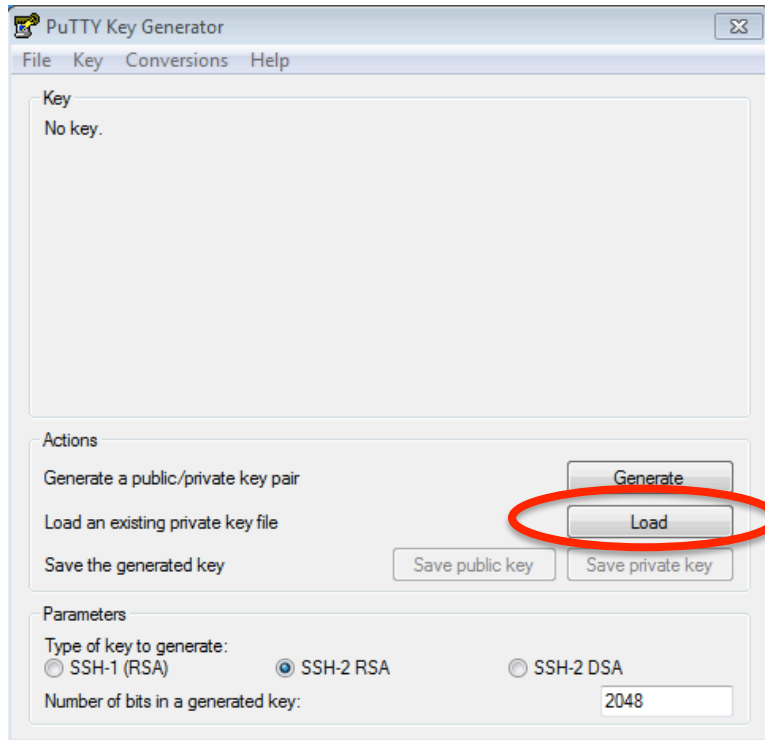
```
chmod 400 server-key.pem
```
4. Connect to your instance using its Public IP:  
**54.173.44.139**

**Example:**  
**ssh -i server-key.pem ec2-user@54.173.44.139**

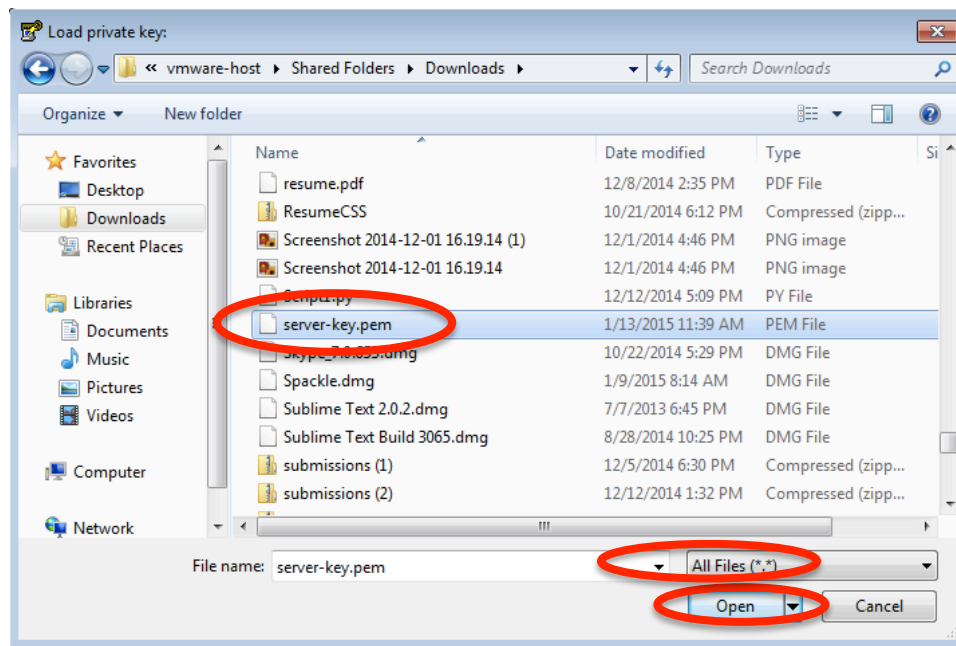
Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

### On a PC:

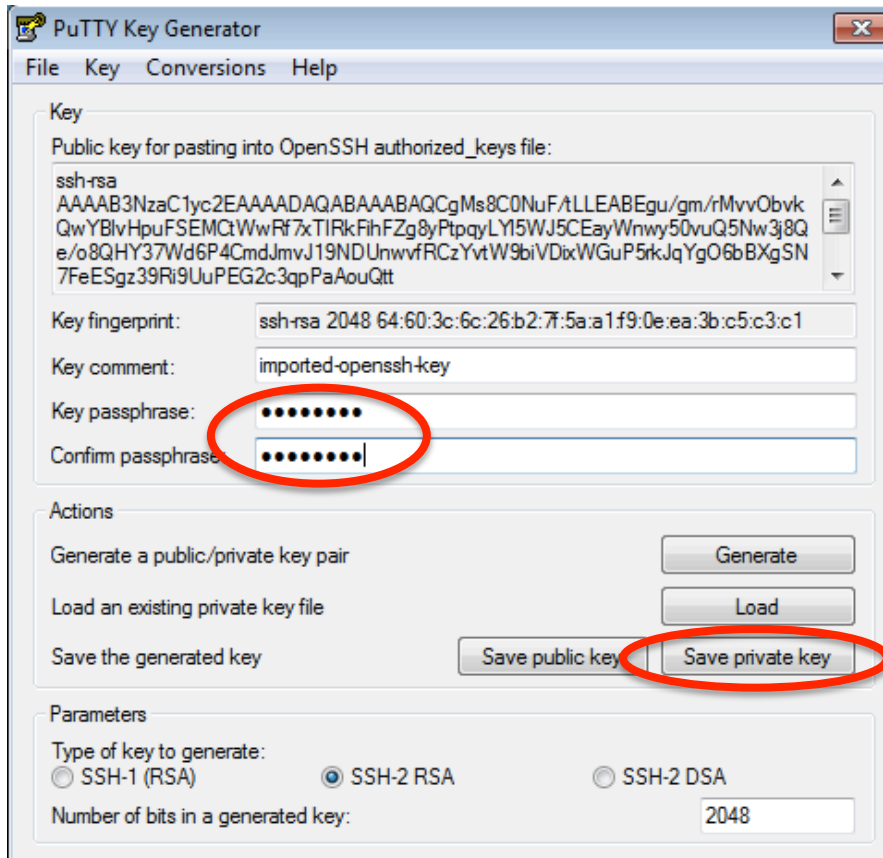
Download Putty and Puttygen from [putty.org](http://putty.org).  
Launch puttygen and click **Load**



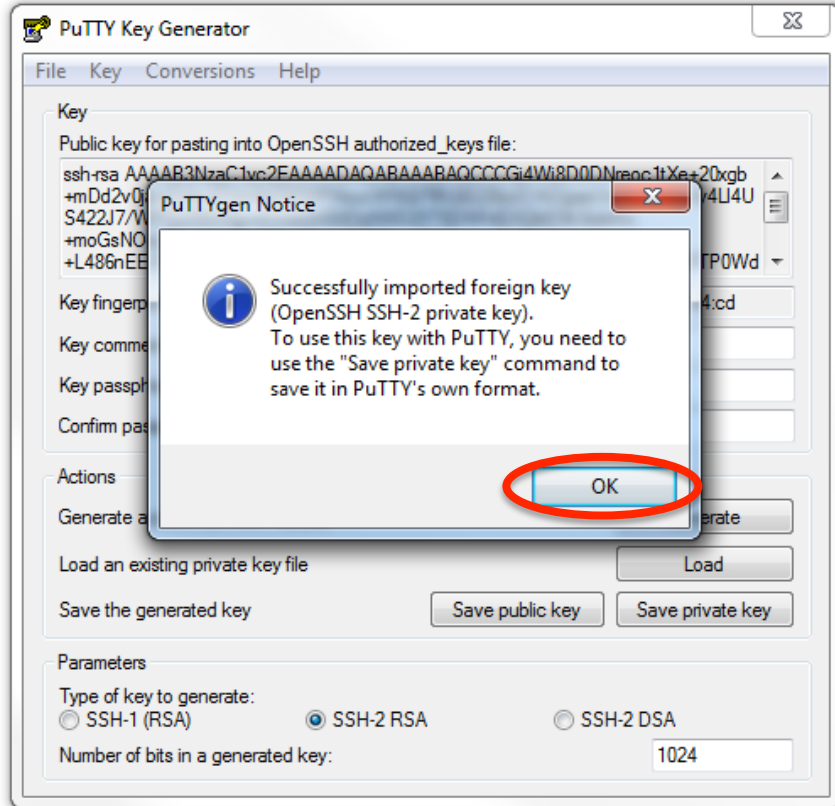
Select **All Files** and navigate to the .pem file you downloaded from AWS. Click **Open**.



Click **OK**, then enter and confirm a passphrase. Click **Save Private Key**.

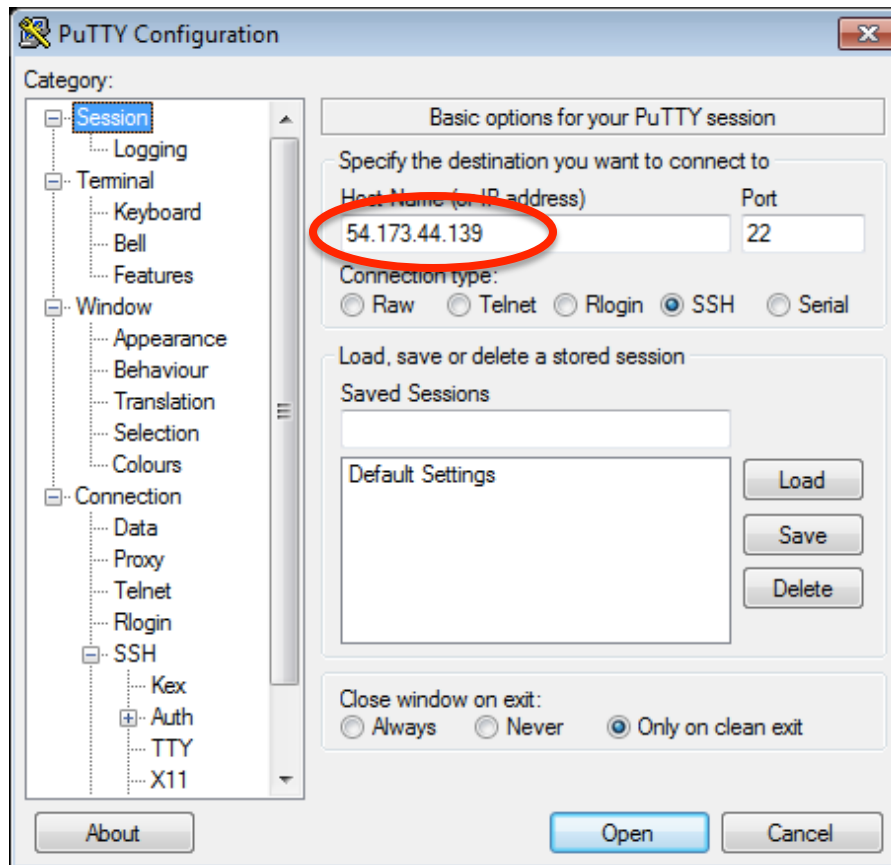


Click OK, and close Puttygen.

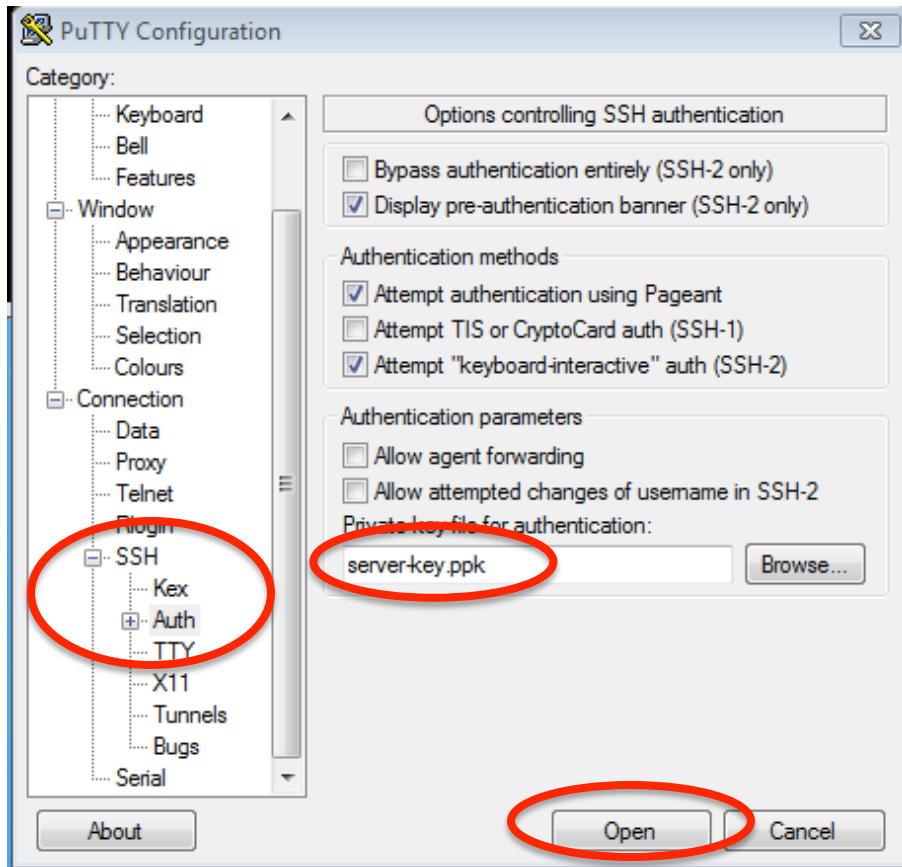


Now you have a .ppk file.

Launch Putty. Enter the IP address of your server instance. (You copied this from AWS, above.)

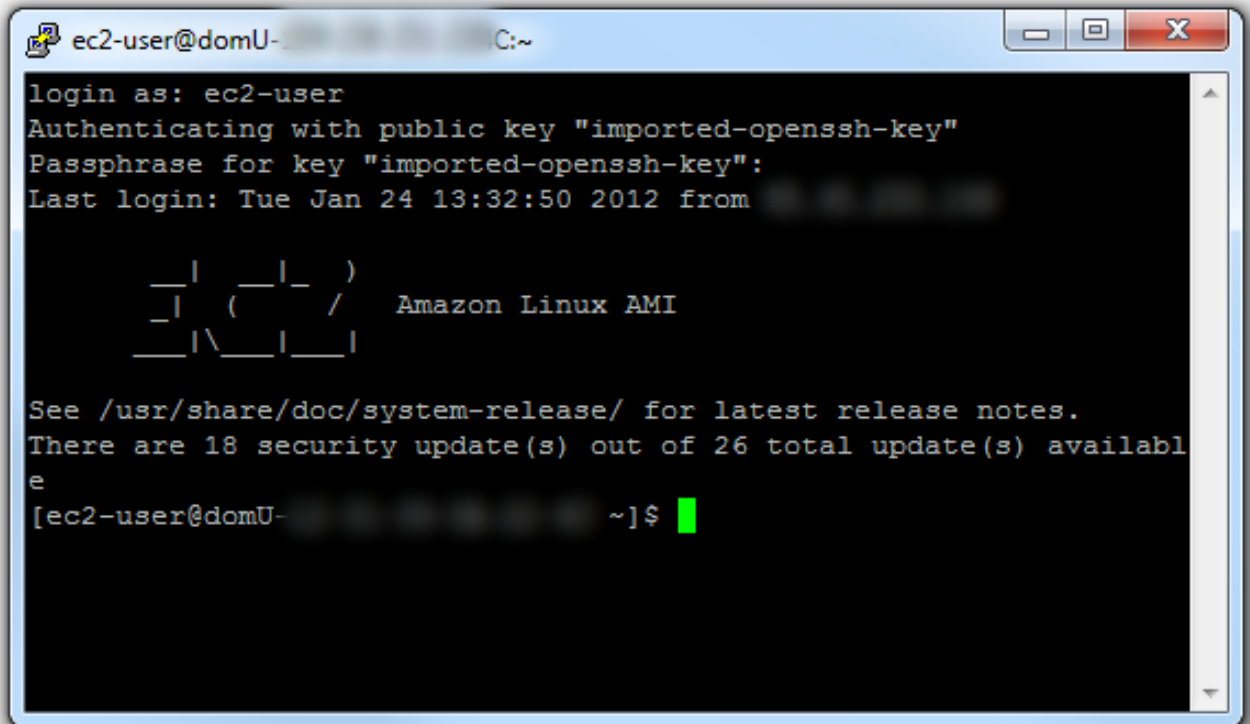


Navigate to Connection→SSH→Auth in the left pane. Click **Browse** and select the .ppk file you exported from puttygen. Click **Open**, then click **Yes**.



Finally, click **Open**. When the connection comes up for the first time, Putty will ask you if you want to save the server's credentials; click **Yes**. In the *login as* prompt, type *ec2-user* and then your passphrase key for your key pair. You are now logged-in

into your instance!



```
ec2-user@domU-... C:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Last login: Tue Jan 24 13:32:50 2012 from ...

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux AMI
  _ | \ _ | _ |

See /usr/share/doc/system-release/ for latest release notes.
There are 18 security update(s) out of 26 total update(s) available
[ec2-user@domU-... ~]$ █
```

#### On a Mac:

Launch a terminal window.

Navigate to the directory that contains your key file.

```
$ cd Downloads
```

Change the file permissions on your key file:

```
$ chmod 400 server-key.pem
```

Paste your connection string into the terminal window. (Note: every time you connect to your instance, the IP address will be different.)

```
$ ssh -i server-key.pem ec2-user@54.86.135.18
```

When you are asked if you want to continue, type **yes** and press Enter.

```
The authenticity of host '54.86.135.18
(54.86.135.18)' can't be established.
RSA key fingerprint is
c1:c6:5a:69:04:4d:08:d8:2c:a9:38:51:04:7e:f0:be
.
```

```
Are you sure you want to continue connecting  
(yes/no)? yes  
Warning: Permanently added '54.86.135.18' (RSA)  
to the list of known hosts.
```

Congratulations! You're connected.

Now, on to installing Node.js.