<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html>

1. In a command line shell, change directories to the location of the private key file that you created when you launched the instance.
2. Use the **chmod** command to make sure your private key file isn't publicly viewable. For example, if the name of your private key file is my-key-pair.pem, you would use the following command:

chmod 400 my-key-pair.pem

1. Use the **ssh** command to connect to the instance. You'll specify the private key (.pem) file and *user\_name*@*public\_dns\_name*. For Amazon Linux, the user name is ec2-user. For RHEL5, the user name is either root or ec2-user. For Ubuntu, the user name is ubuntu. For Fedora, the user name is either fedora or ec2-user. For SUSE Linux, the user name is root. Otherwise, if ec2-user and root don't work, check with your AMI provider.

ssh -i my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com