

Experiment No. : 07

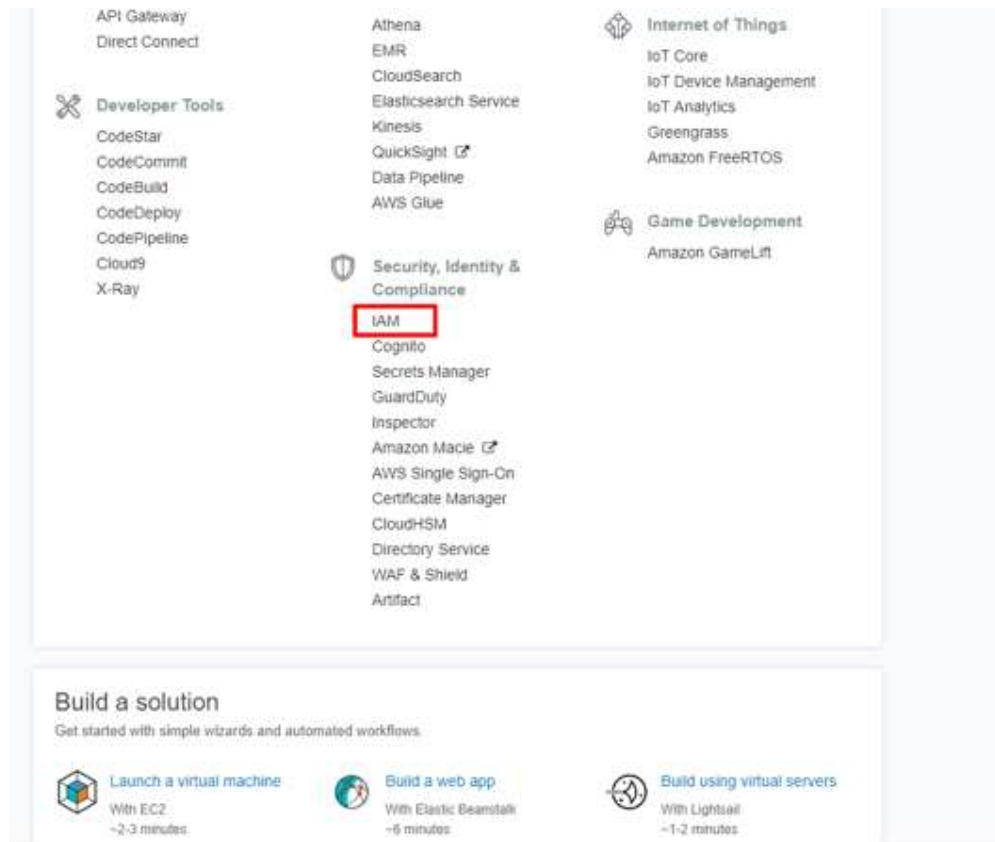
Title: Launch a Linux VM: Launch then connect to a Linux instance in the cloud.

1. Sign-up for AWS

The button and the link open a new tab so you can follow this tutorial in the AWS console.

a. Enter the Amazon EC2 Console

Open the AWS Management Console, so you can keep this step-by-step guide open. When the screen loads, enter your user name and password to get started. Then type *EC2* in the search bar and select Amazon EC2 to open the service console.



b. Launch an Instance

Select Launch Instance to create and configure your virtual machine.

The screenshot shows the AWS Management Console's EC2 Dashboard. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main area is titled 'Resources' and shows a summary of EC2 resources in the US East (N. Virginia) region: 0 Running Instances, 0 Volumes, 0 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 1 Security Groups. Below this is a 'Create Instance' section with a red box around the 'Launch Instance' button. To the right, there are sections for 'Service Health' and 'Scheduled Events'.

3. Configure your Instance

You are now in the EC2 Launch Instance Wizard, which will help you configure and launch your instance.

a. In this screen, you are shown options to choose an Amazon Machine Image (AMI). AMIs are preconfigured server templates you can use to launch an instance. Each AMI includes an operating system, and can also include applications and application servers.

For this tutorial, find *Amazon Linux AMI* and click Select.

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen in the AWS Management Console. The left sidebar has a 'Quick Start' section with 'My AMIs', 'AWS Marketplace', and 'Community AMIs'. The main area lists various AMIs. The first one, 'Amazon Linux AMI 2015.03.1 (HVM), SSD Volume Type - ami-0d4cfd66', is highlighted with a red box. Other AMIs listed include Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12, Ubuntu Server 14.04 LTS, and Microsoft Windows Server 2012 R2. At the bottom, there is a section for 'Are you launching a database instance? Try Amazon RDS'.

b. You will now choose an instance type. Instance types comprise of varying combinations of CPU, memory, storage, and networking capacity so you can choose the appropriate mix for your applications. For more information, see [Amazon EC2 Instance Types](#).

The default option of *t2.micro* should already be checked. This instance type is covered within the Free Tier and offers enough compute capacity to tackle simple workloads. Click Review and Launch at the bottom of the page.

Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: **All instance types** **Current generation** **Show/Hide Columns**

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs (1)	Memory (GiB)	Instance Storage (GiB) (1)	EBS-Optimized Available (1)	Network Performance (1)
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
<input type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

c. You can review the configuration, storage, tagging, and security settings that have been selected for your instance. While you have the option to customize these settings, we recommend accepting the default values for this tutorial.

Click Launch at the bottom of the page.

Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, launch-wizard-1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)
Amazon Linux AMI 2015.03.1 (HVM), SSD Volume Type - ami-0d4cf086
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1
Description: launch-wizard-1 created 2015-09-11T13:35:57.265-07:00

Type (1)	Protocol (1)	Port Range (1)	Source (1)
SSH	TCP	22	0.0.0.0/0

[Instance Details](#) [Edit instance details](#)
[Storage](#) [Edit storage](#)
[Tags](#) [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

d. On the next screen you will be asked to choose an existing key pair or create a new key pair. A key pair is used to securely access your Linux instance using SSH. AWS stores the public part of the key pair which is just like a house lock. You download and use the private part of the key pair which is just like a house key.

Select Create a new key pair and give it the name MyKeyPair. Next click the Download Key Pair button.

After you download the MyKeyPair key, you will want to store your key in a secure location. If you lose your key, you won't be able to access your instance. If someone else gets access to your key, they will be able to access your instance.

Windows users: We recommend saving your key pair in your user directory in a sub-directory called .ssh (ex. C:\user\{yourusername}\.ssh\MyKeyPair.pem).

Tip: You can't use Windows Explorer to create a folder with a name that begins with a period unless you also end the folder name with a period. After you enter the name (.ssh.), the final period is removed automatically.

Mac/Linux users: We recommend saving your key pair in the .ssh sub-directory from your home directory (ex. ~/.ssh/MyKeyPair.pem).

Tip: On MacOS, the key pair is downloaded to your Downloads directory by default. To move the key pair into the .ssh sub-directory, enter the following command in a terminal window: `mv ~/Downloads/MyKeyPair.pem ~/.ssh/MyKeyPair.pem`

After you have stored your key pair, click Launch Instance to start your Linux instance.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

MyKeyPair

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

e. Click View Instances on the next screen to view your instances and see the status of the instance you have just started.

Launch Status

✓ **Your instances are now launching**

The following instance launches have been initiated: i-██████████ [View launch log](#)

ℹ **Get notified of estimated charges**

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

View Instances

f. In a few minutes, the *Instance State* column on your instance will change to "running" and a Public IP address will be shown. You can refresh these Instance State columns by pressing the refresh button on the right just above the table. Copy the Public IP address of your AWS instance, so you can use it when we connect to the instance using SSH in Step 4.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with options like EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main area displays the 'Instances' tab with a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. One instance is listed with a status of 'running' and a Public IP address. Below the table, the details for the selected instance are shown, including the Public IP address, which is highlighted with a red box.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
	i-██████████	t2.micro	us-east-1a	running	2/2 checks ...	None	

Instance: i-██████████ **Public IP: 52.██████████.5**

Description | Status Checks | Monitoring | Tags

Instance ID	i-██████████	Public DNS	-
Instance state	running	Public IP	52.██████████.5
Instance type	t2.micro	Elastic IP	-
Private DNS	ip-██████████.ec2.internal	Availability zone	us-east-1a
Private IPs	██████████	Security groups	launch-wizard-4, view rules
Secondary private IPs	-	Scheduled events	No scheduled events
VPC ID	vpc-434f9a27	AMI ID	amzn-ami-hvm-2015.09.1.x86_64-gp2

4. Connect to your Instance

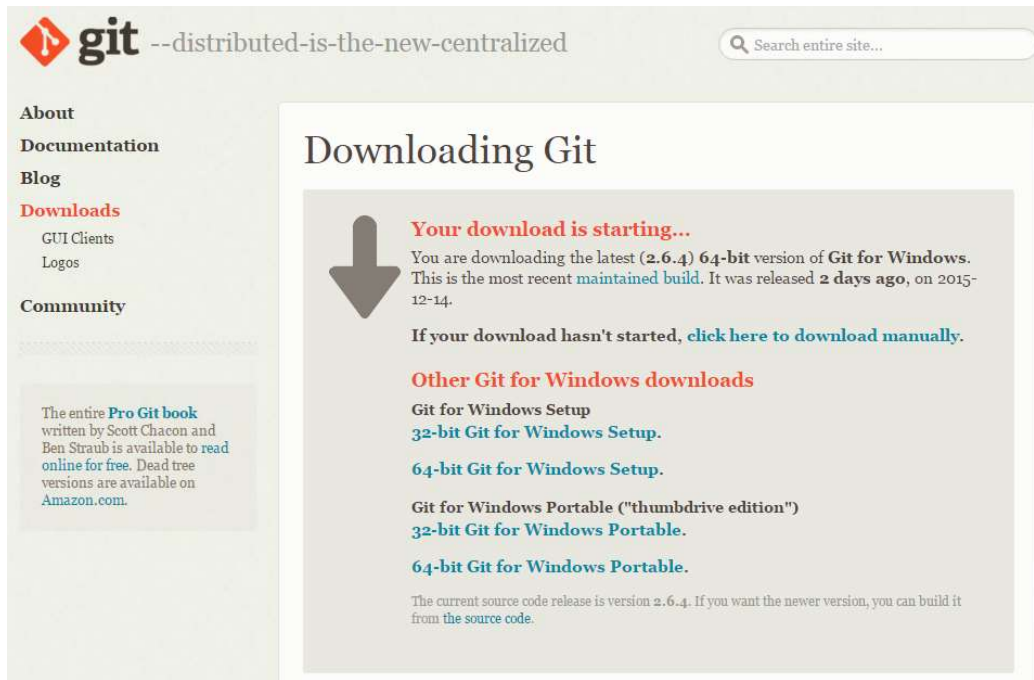
After launching your instance, it's time to connect to it using SSH.

Windows users: Select Windows below to see instructions for installing Git Bash which includes SSH.

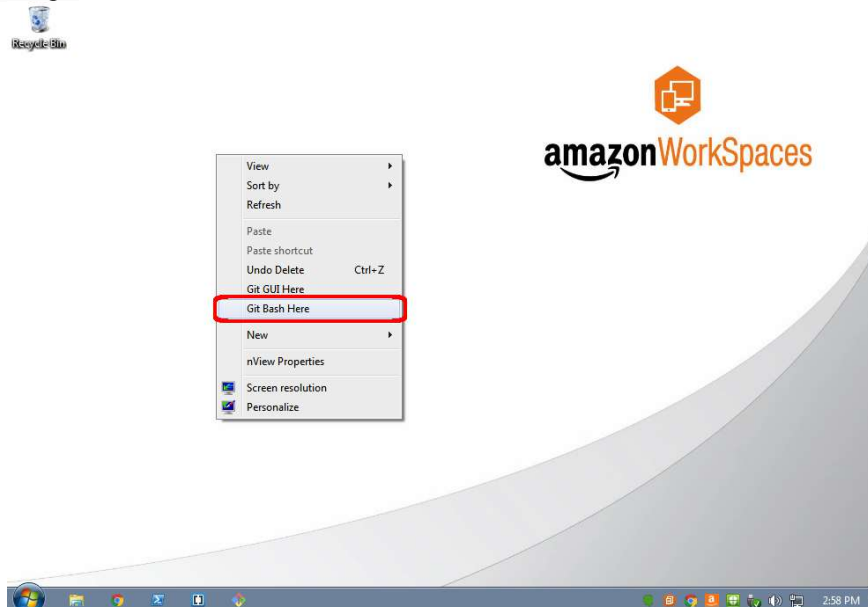
Mac/Linux user: Select Mac / Linux below to see instructions for opening a terminal window.

- Windows

a. Download Git for Windows [here](#). Run the downloaded installer accepting the default settings (this will install Git Bash as part of Git).



b. Right click on your desktop (not on an icon or file) and select Git Bash Here to open a Git Bash command prompt.

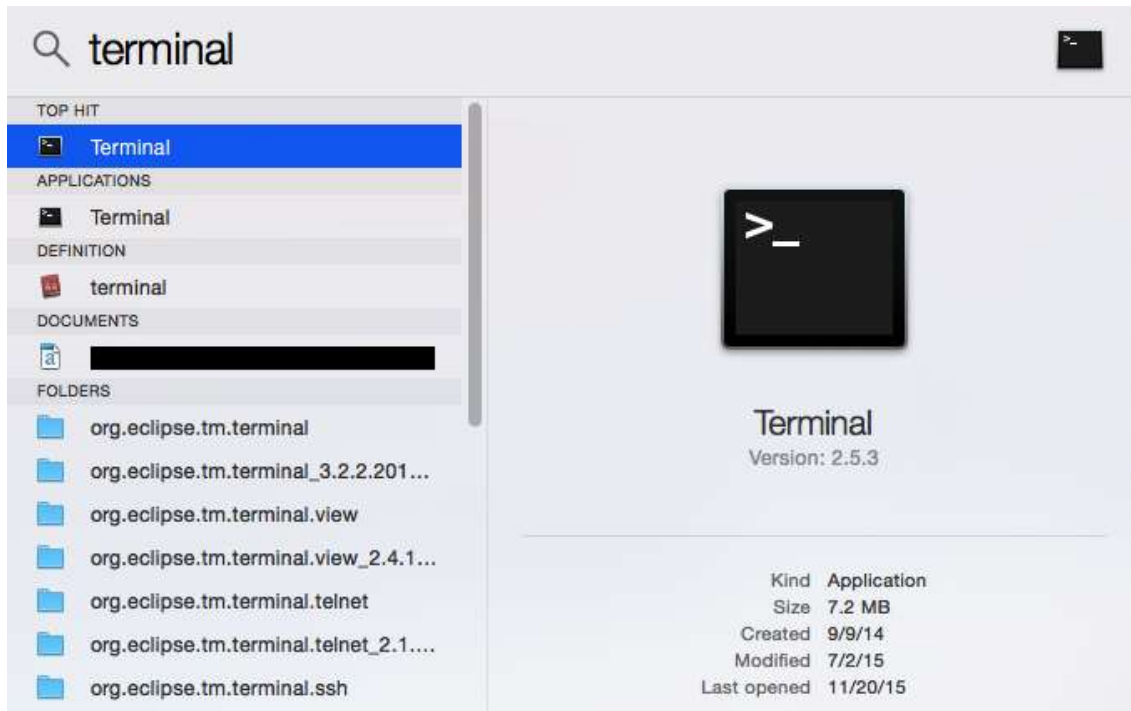


- **Mac**

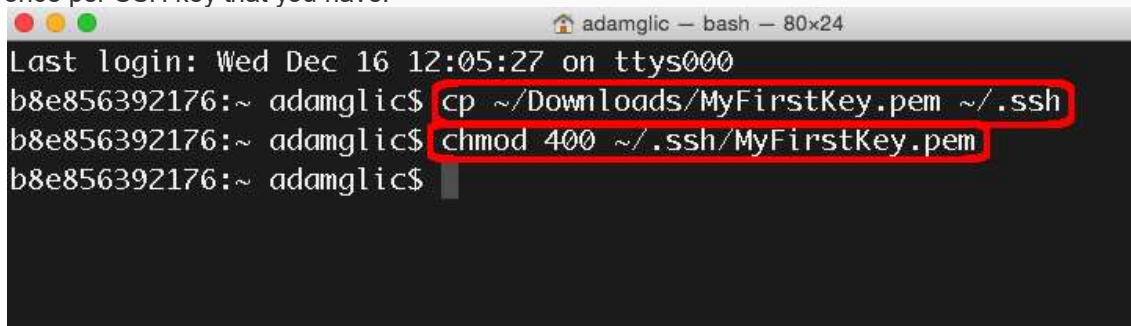
a. Your Mac or Linux computer most likely includes an SSH client by default. You can check for an SSH client by typing `ssh` at the command line. If your computer doesn't recognize the command, the [OpenSSH project](#) provides a free implementation of the full suite of SSH tools that you can download.

Mac users: Open a terminal window by pressing Command + Space and typing terminal in the search window. Then press enter to open the terminal window.

Linux users: Open a terminal window.



b. Use the `chmod` command to make sure your private key file is not publicly viewable by entering the following command to restrict permissions to your private SSH key:
`chmod 400 ~/.ssh/mykeypair.pem`
You do not need to do this every time you connect to you instance, you only need to set this once per SSH key that you have.



c. Use SSH to connect to your instance. In this case the user name is ec2-user, the SSH key is stored in the directory we saved it to in step 3 part d, and the IP address is from step 3 part f. The format is:
`ssh -i {full path of your .pem file} ec2-user@{instance IP address}`

Enter the following:

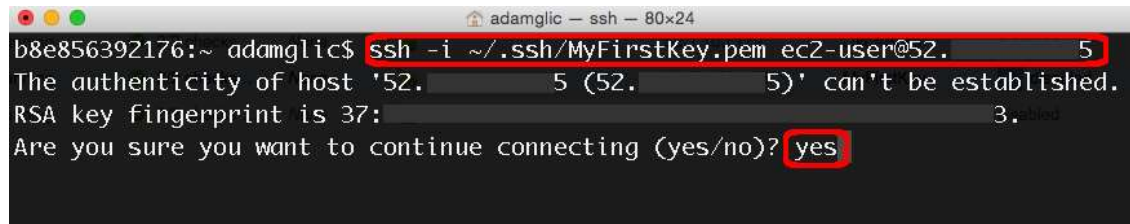
```
ssh -i 'c:\Users\yourusername\.ssh\MyKeyPair.pem' ec2-user@{IP_Address}
```

Example: `ssh -i 'c:\Users\adamglic\.ssh\MyKeyPair.pem' ec2-user@52.27.212.125`

You'll see a response similar to the following:

The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established. RSA key fingerprint is 1f:51:ae:28:df:63:e9:d8:cf:38:5d:87:2d:7b:b8:ca:9f:f5:b1:6f.
Are you sure you want to continue connecting (yes/no)?

Type yes and press enter.

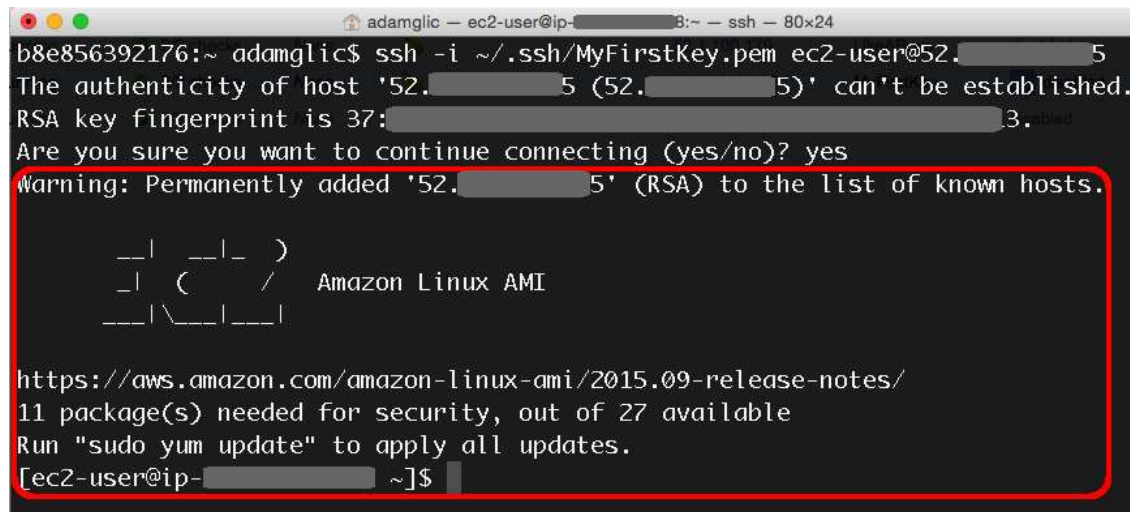


```
adamglic — ssh — 80x24
b8e856392176:~ adamglic$ ssh -i ~/.ssh/MyFirstKey.pem ec2-user@52.27.212.125
The authenticity of host '52.27.212.125 (52.27.212.125)' can't be established.
RSA key fingerprint is 37:1f:51:ae:28:df:63:e9:d8:cf:38:5d:87:2d:7b:b8:ca:9f:f5:b1:6f.
Are you sure you want to continue connecting (yes/no)? yes
```

d. You'll see a response similar to the following:

Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA) to the list of known hosts.

You should then see the welcome screen for your instance and you are now connected to your AWS Linux virtual machine in the cloud.



```
adamglic — ec2-user@ip-10-254-142-33:~ — ssh — 80x24
b8e856392176:~ adamglic$ ssh -i ~/.ssh/MyFirstKey.pem ec2-user@52.27.212.125
The authenticity of host '52.27.212.125 (52.27.212.125)' can't be established.
RSA key fingerprint is 37:1f:51:ae:28:df:63:e9:d8:cf:38:5d:87:2d:7b:b8:ca:9f:f5:b1:6f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.27.212.125' (RSA) to the list of known hosts.

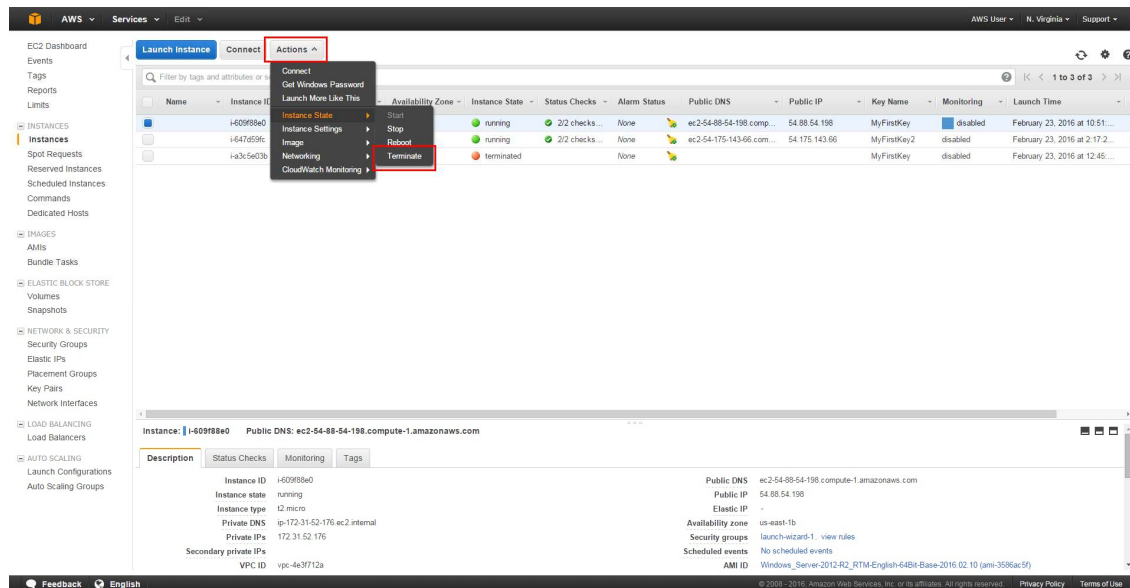
  __|  __|  )
 _| (  ___/   Amazon Linux AMI
___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
11 package(s) needed for security, out of 27 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-254-142-33 ~]$
```

5. Terminate Your Instance

You can easily terminate the instance from the EC2 console. In fact, it is a best practice to terminate instances you are no longer using so you don't keep getting charged for them.

a. Back on the EC2 Console, select the box next to the instance you created. Then click the Actions button, navigate to *Instance State*, and click Terminate.



b. You will be asked to confirm your termination - select Yes, Terminate.

Note: This process can take several seconds to complete. Once your instance has been terminated, the Instance State will change to *terminated* on your EC2 Console.

