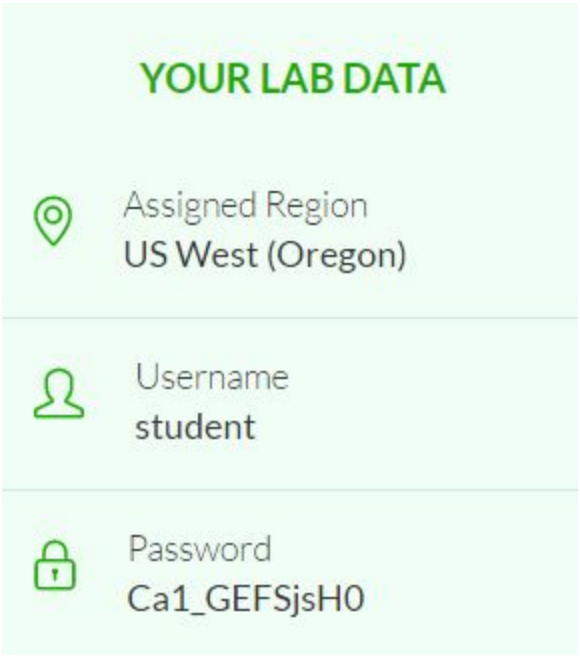
LAB1 : EC2 CREATION



Step 1 Login to the Amazon Web Service Console

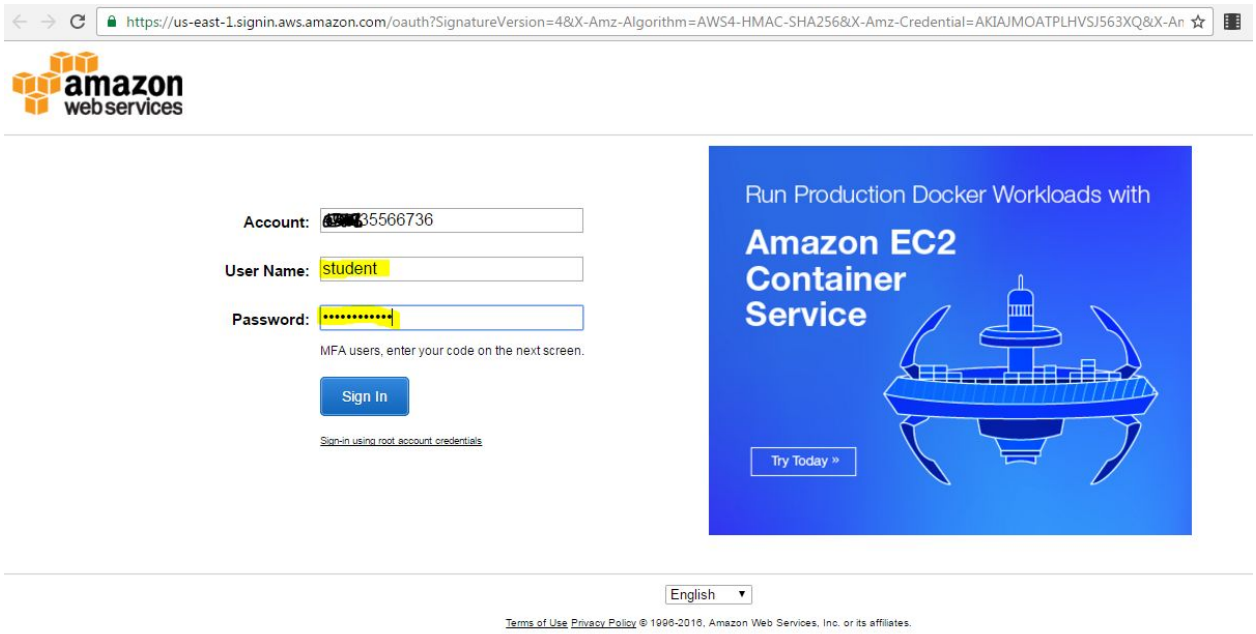
This laboratory experience is about Amazon Web Services and you will use the AWS Management Console in order to complete all the lab steps.

The AWS Management Console is a web control panel for managing all your AWS resources, from EC2 instances to SNS topics. The console enables cloud management for all aspects of the AWS account, including managing security credentials, or even setting up new IAM Users.

Log in to the AWS Management Console

In order to start the laboratory experience, open the Amazon Console by clicking this button:

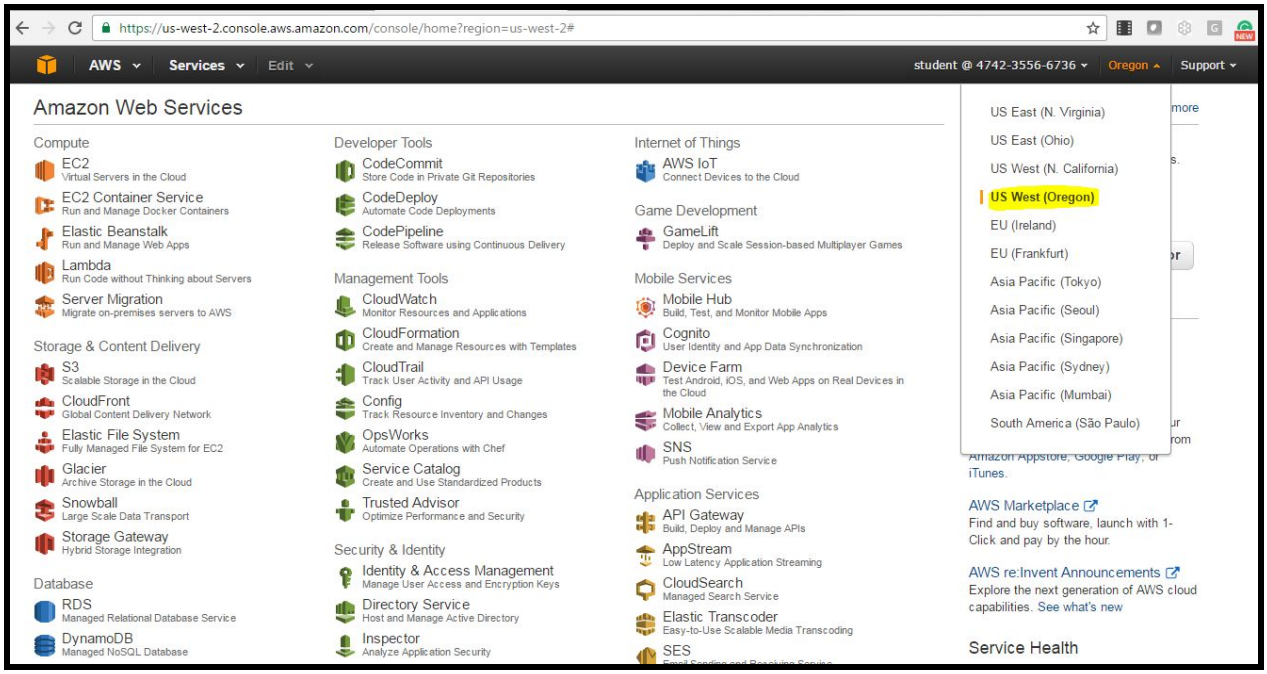
https://aws.amazon.com or custom sign-in link of your company



Select the right AWS Region

Amazon Web Services is available in different regions all over the world, and the console lets you provision resources across multiple regions. You usually choose a region that best suits your business needs to optimize your customer's experience, but you must use the region **US West (Oregon)** for this laboratory.

You can select the **US West (Oregon)** region using the upper right dropdown menu on the AWS Console page.



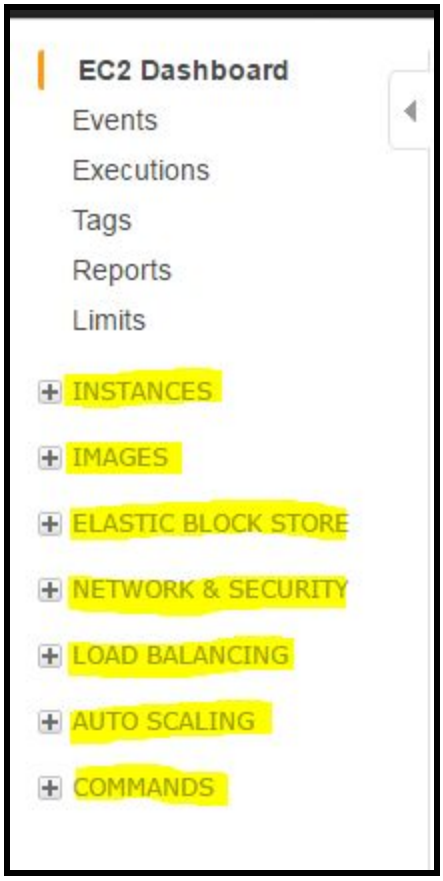
Step 2 Create an EC2 instance

You can launch an EC2 instance using the EC2 launch wizard.

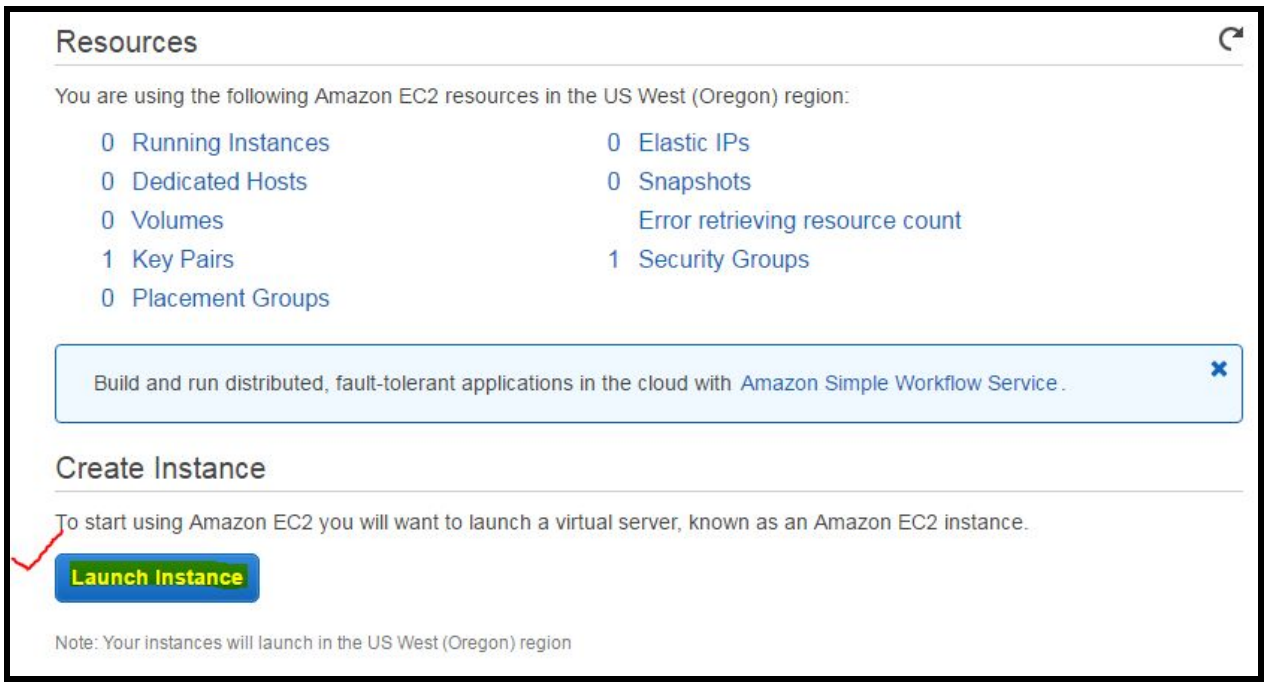
Select the EC2 service from the Management Console dashboard:

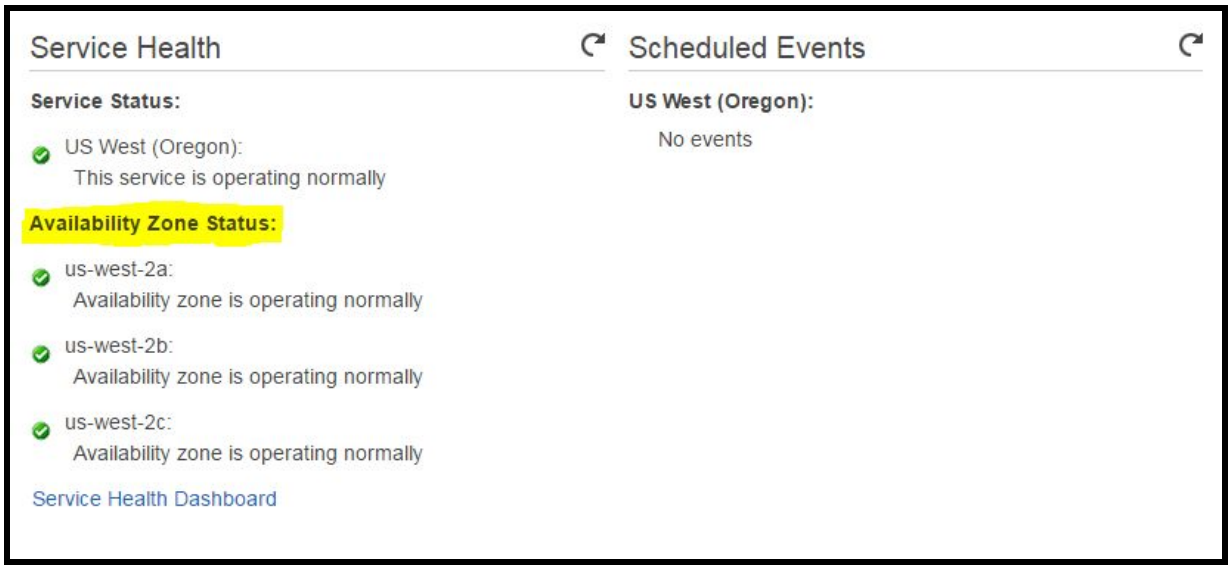
From the EC2 dashboard, click **Launch Instance**.

Left Hand Side Pane

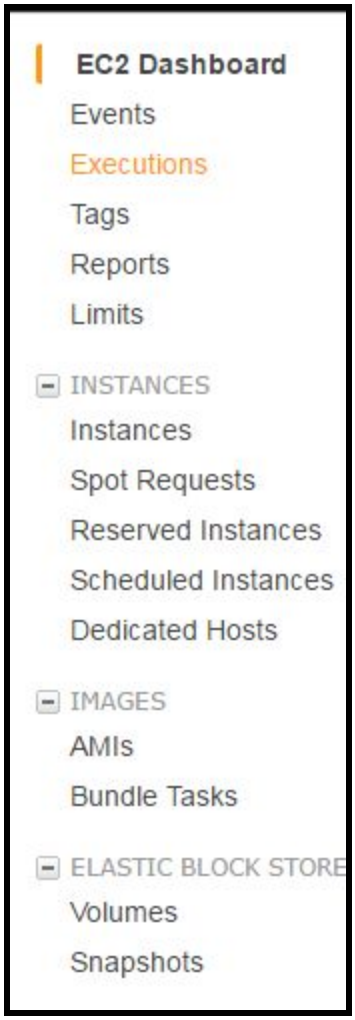


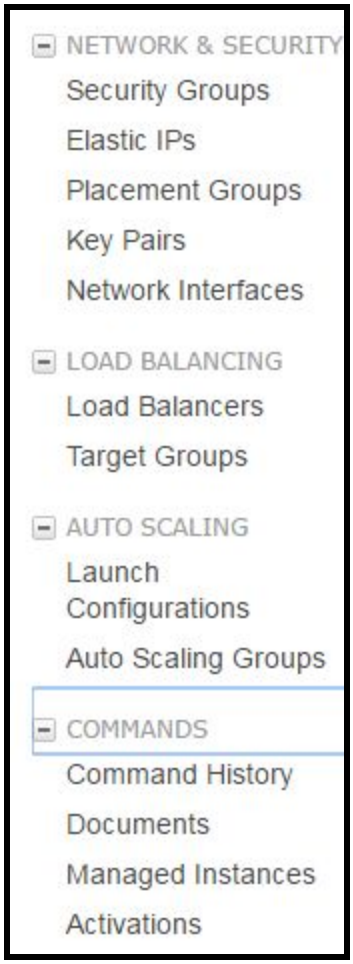
Right Hand side Pane



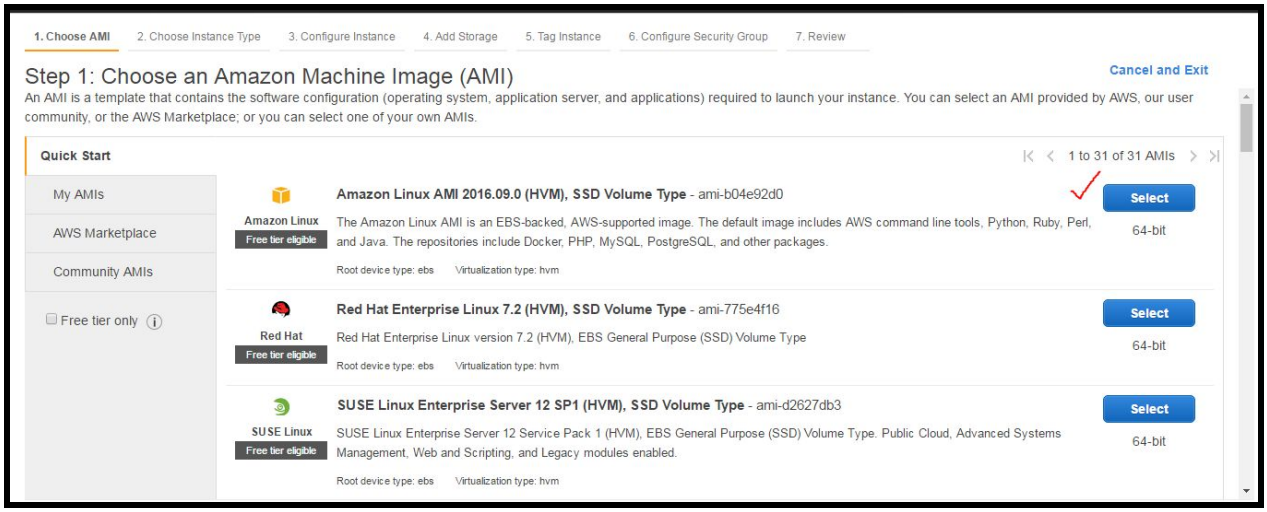


Detail about Left Pane

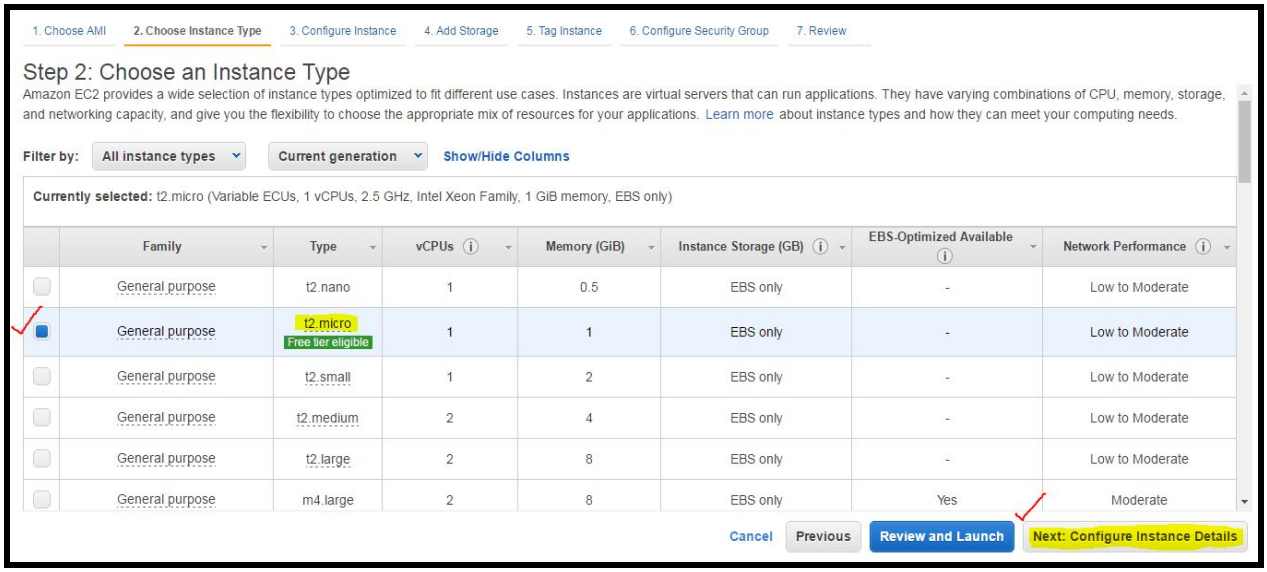

EC2 Dashboard
Events
Executions
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots


NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
COMMANDS
Command History
Documents
Managed Instances
Activations

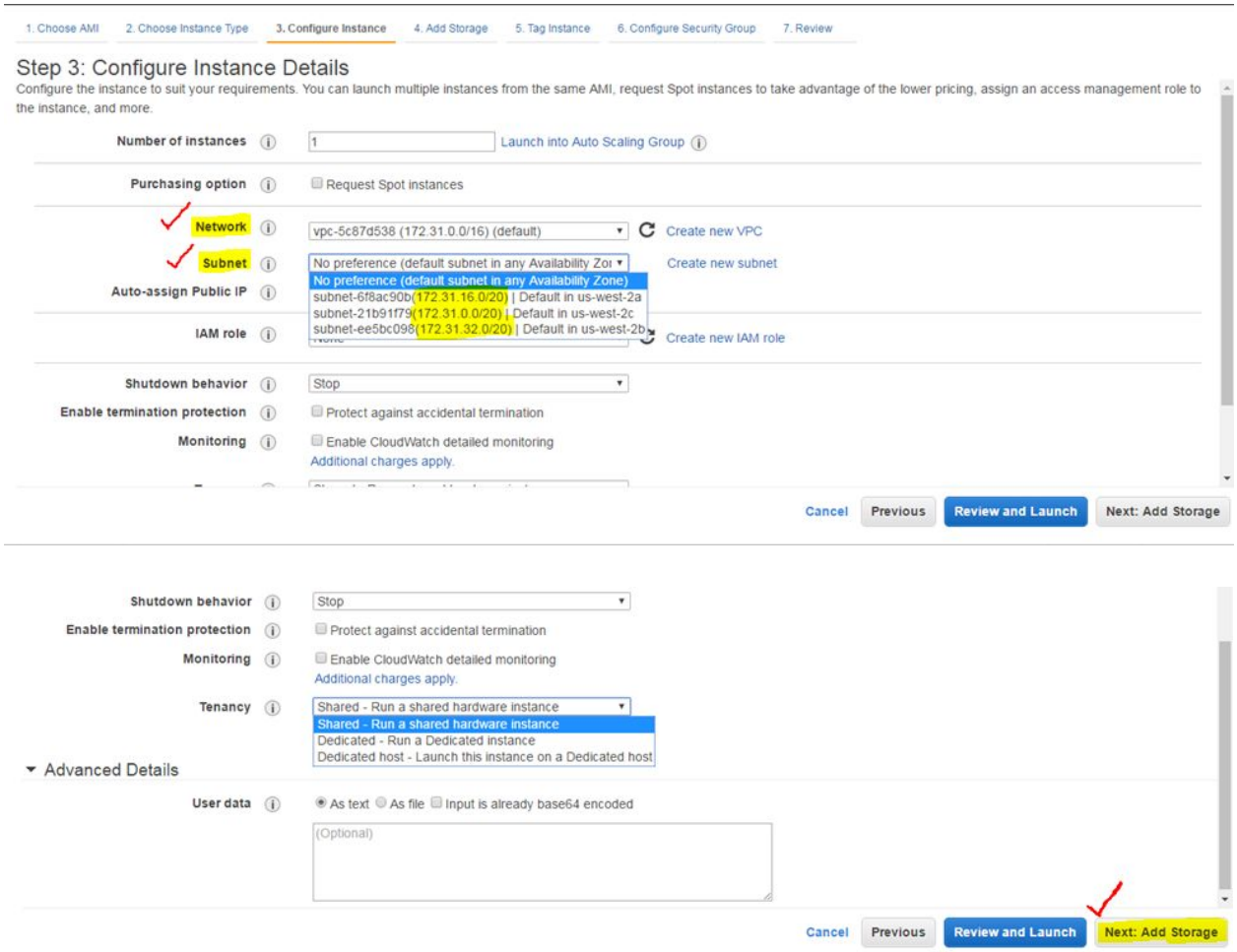
The **Choose an Amazon Machine Image (AMI)** page displays a list of basic configurations called **Amazon Machine Images (AMIs)** that serve as templates for your instance. Select the first listed 64-bit **Amazon Linux AMI**.



On the **Choose an Instance Type** page, do **not** change any options and click **Next: Configure Instance Details.**



On the **Configure Instance Details** tab, check the selected **Network (VPC)** and **Subnet**. Change them, if needed, and then click **Next: Add Storage.**



On the **Add Storage** tab, do **not** change any options, and click the **Review and Launch** button.

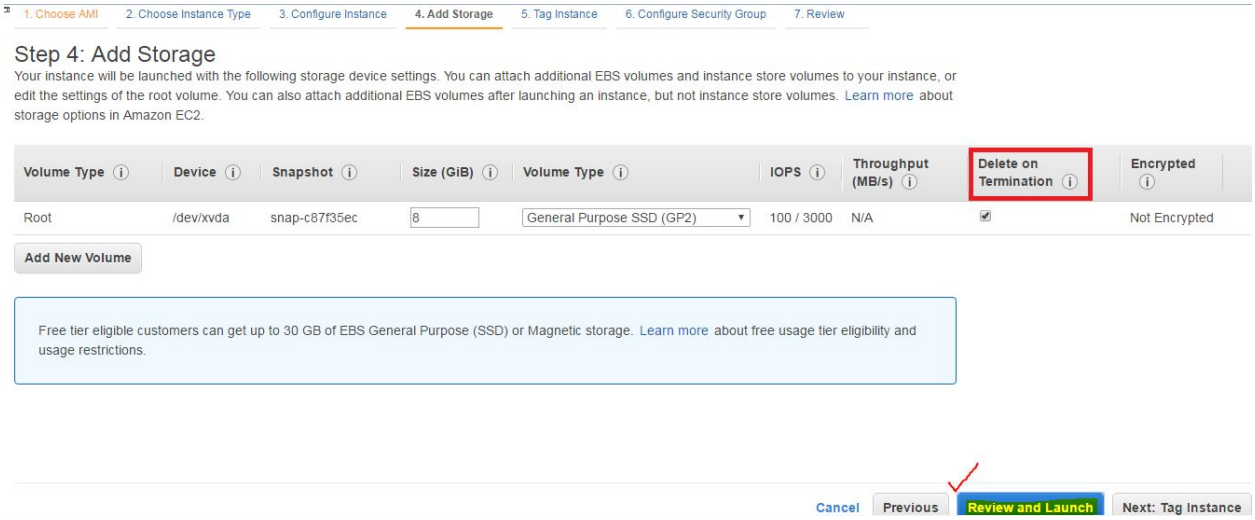
On the Review Instance Launch page, click **Launch**.

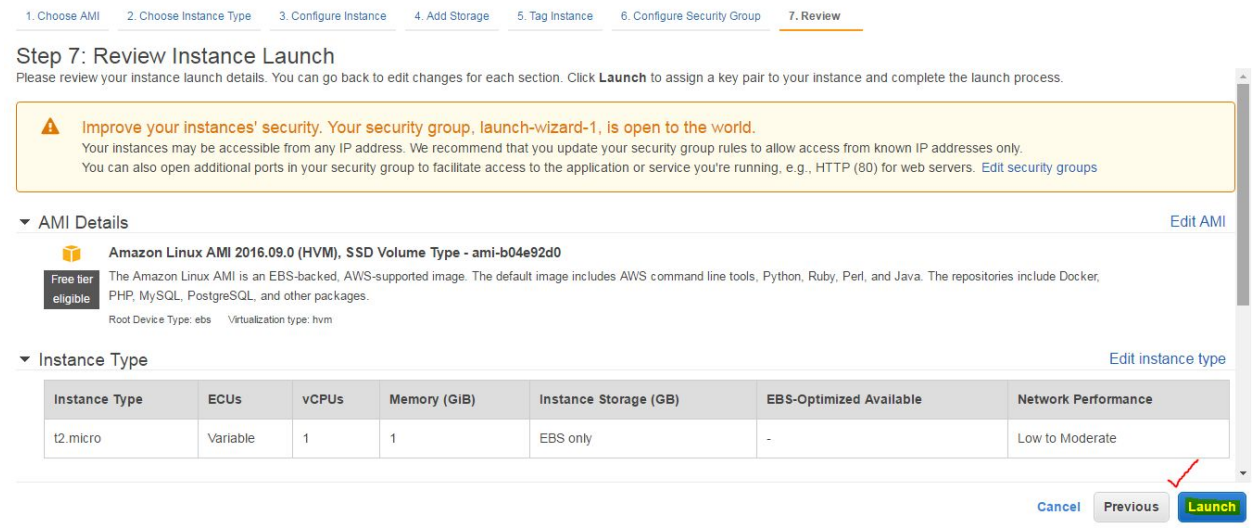
In the **Select an existing key pair or create a new key pair** dialog box, select **Create a new key pair**, then type a KeyPair name (e.g., "TestKeys") and download it.

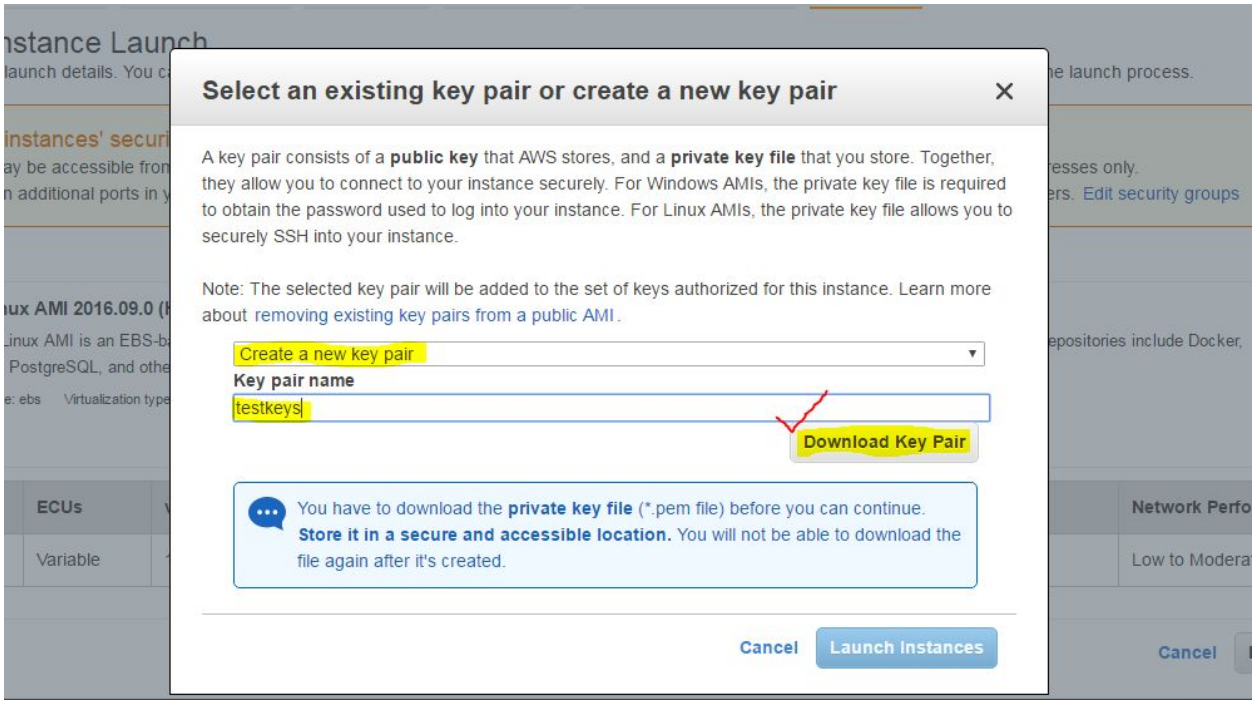
Select the acknowledgment checkbox, and then click **Launch Instances**.

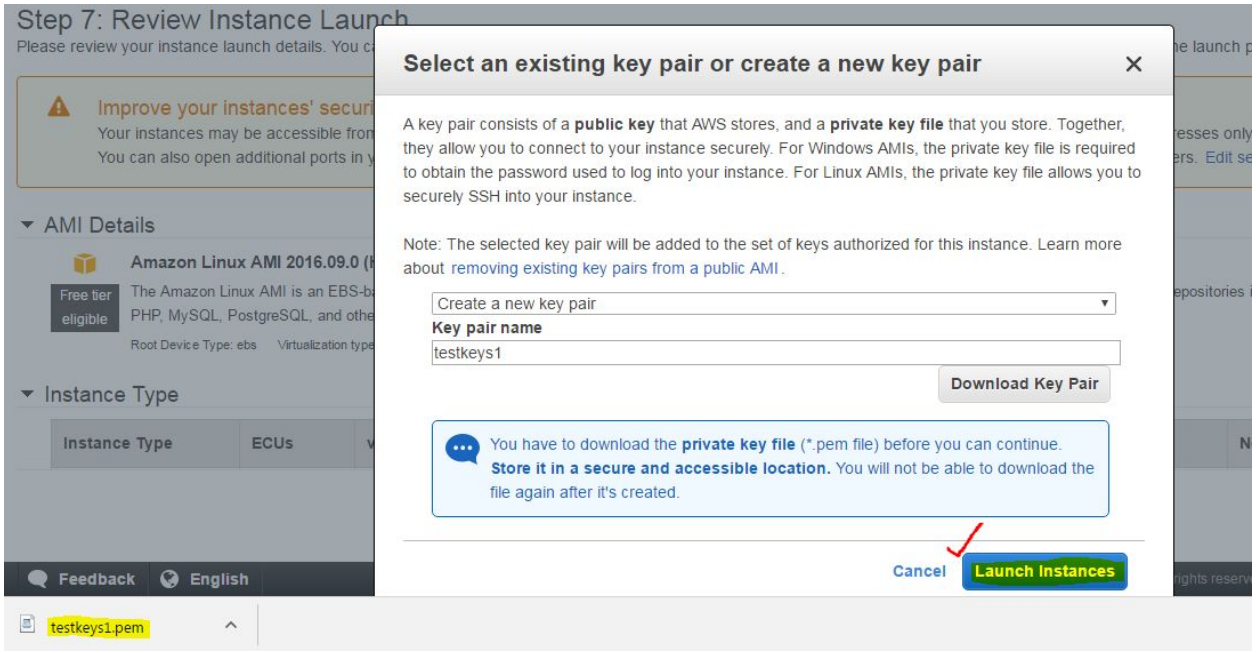
A confirmation page will let you know that your instance is launching. Click **View Instances** to close the confirmation page and return to the console.

On the Instances Screen, you can view the status of your instance. It will take a short time for your instance to be launched. When you launch an instance, its initial state defaults to *pending*. After the instance starts, its Instance State changes to *running*, and it receives a public DNS name.


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encrypted
Root
/dev/xvda
snap-c87f35ec
8
General Purpose SSD (GP2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Tag Instance


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review
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 2016.09.0 (HVM), SSD Volume Type - ami-b04e92d0
Free tier eligible
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 (GB)
EBS-Optimized Available
Network Performance
t2.micro
Variable
1
1
EBS only
-
Low to Moderate
Cancel
Previous
Launch


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
testkeys
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


Step 7: Review Instance Launch
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
testkeys1
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
AMI Details
Instance Type
Feedback
English
testkeys1.pem

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0d88d399ffef652e8 View launch log

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
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

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.

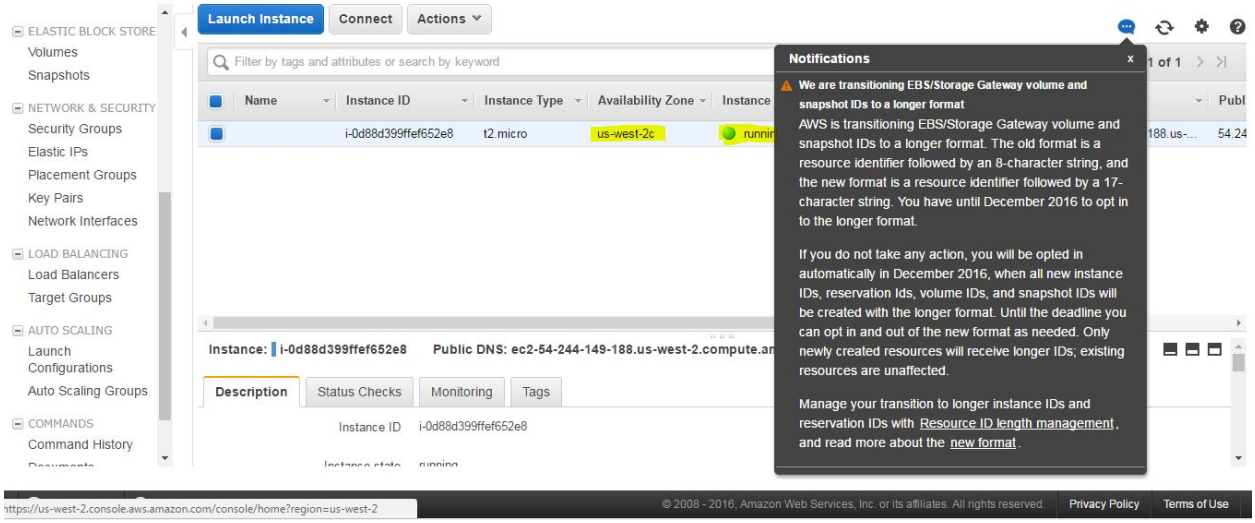
Here are some helpful resources to get you started

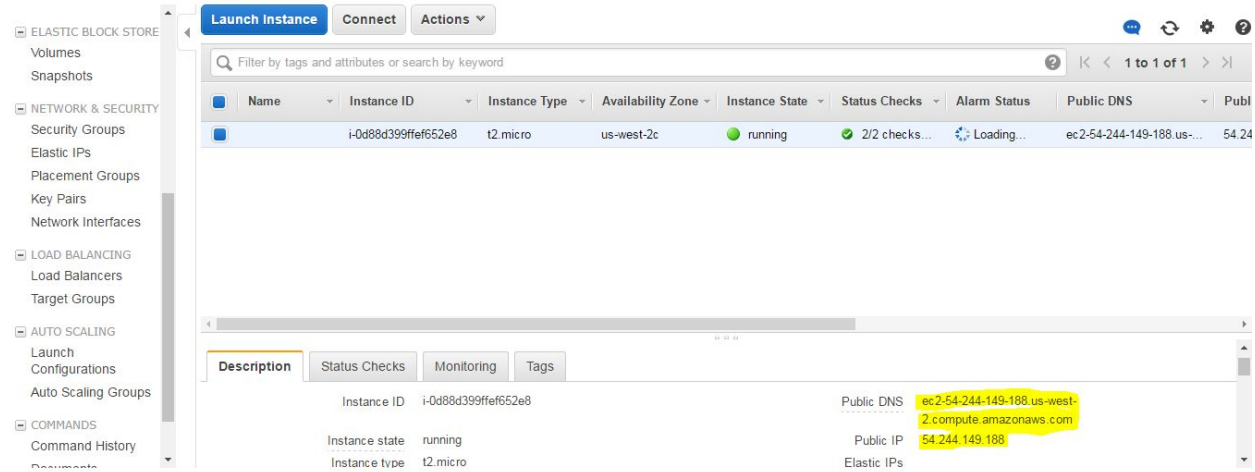
- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

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


Launch Instance
Connect
Actions
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
COMMANDS
Command History
Filter by tags and attributes or search by keyword
1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance
i-0d88d399ffef652e8
t2.micro
us-west-2c
Notifications
We are transitioning EBS/Storage Gateway volume and snapshot IDs to a longer format
AWS is transitioning EBS/Storage Gateway volume and snapshot IDs to a longer format. The old format is a resource identifier followed by an 8-character string, and the new format is a resource identifier followed by a 17-character string. You have until December 2016 to opt in to the longer format.
If you do not take any action, you will be opted in automatically in December 2016, when all new instance IDs, reservation Ids, volume IDs, and snapshot IDs will be created with the longer format. Until the deadline you can opt in and out of the new format as needed. Only newly created resources will receive longer IDs; existing resources are unaffected.
Manage your transition to longer instance IDs and reservation IDs with Resource ID length management, and read more about the new format.
Instance: i-0d88d399ffef652e8
Public DNS: ec2-54-244-149-188.us-west-2.compute.an
Description
Status Checks
Monitoring
Tags
Instance ID
i-0d88d399ffef652e8
https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

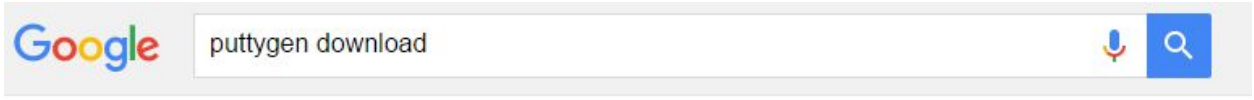

Launch Instance
Connect
Actions
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
COMMANDS
Command History
Filter by tags and attributes or search by keyword
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS
i-0d88d399ffef652e8
t2.micro
us-west-2c
running
2/2 checks...
Loading...
ec2-54-244-149-188.us-...
Description
Status Checks
Monitoring
Tags
Instance ID
i-0d88d399ffef652e8
Instance state
running
Instance type
t2.micro
Public DNS
ec2-54-244-149-188.us-west-2.compute.amazonaws.com
Public IP
54.244.149.188
Elastic IPs

Step 3 Convert a PEM key to a PPK key

If you are a Windows user, you will probably use **PuTTY** for connecting to the remote instance. PuTTY is a great SSH client, but it does not natively support the PEM key format. Fortunately, PuTTY has a tool called **PuTTYgen**, which can convert keys to the required PPK format.

Converting a PEM key is easy and fast:

- If you do not already have it, download the PuTTYgen executable from its main website: **PuTTYgen**
- Start PuTTYgen (no installation required).
- Click **Load** and browse to the location of the private key file that you want to convert (e.g. ec2key.pem). By default, PuTTYgen displays only files with extension .ppk. You'll need to change that default to display files of all types in order to see your .pem key file.zy
    - Select your .pem key file and click **Open**. PuTTYgen displays the following message.



All News Videos Images More Search tools

About 55,900 results (0.60 seconds)

PuTTY Download Page - Chiark
www.chiark.greenend.org.uk/~sgtatham/putty/**download**.html
Sep 29, 2016 - To **download** our public keys and find out more about our signature policy, visit the Keys ... **PuTTYgen**: **puttygen**.exe (or by FTP) (signature).

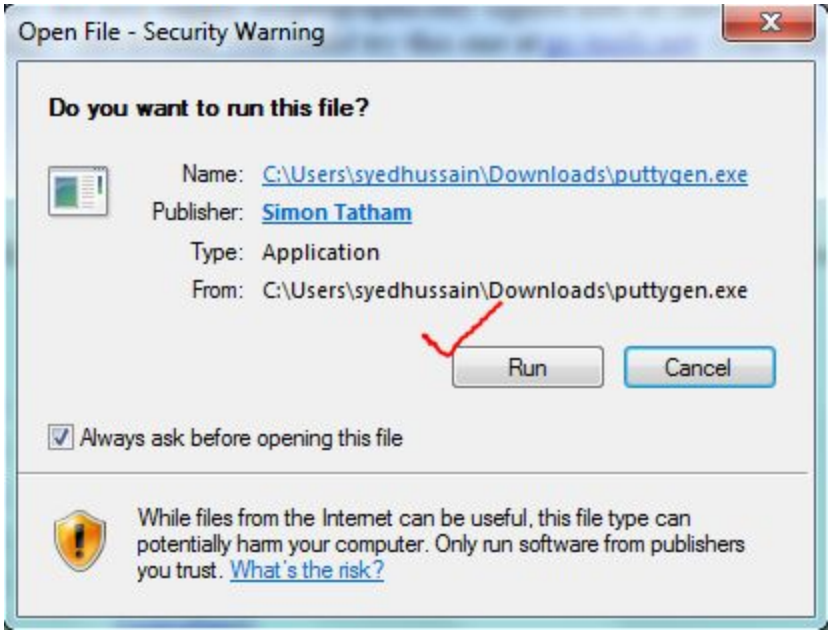
Download PuTTY - a free SSH and telnet client for Windows
www.putty.org/
Download PuTTY. PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is ...
You've visited this page 2 times. Last visit: 26/11/15

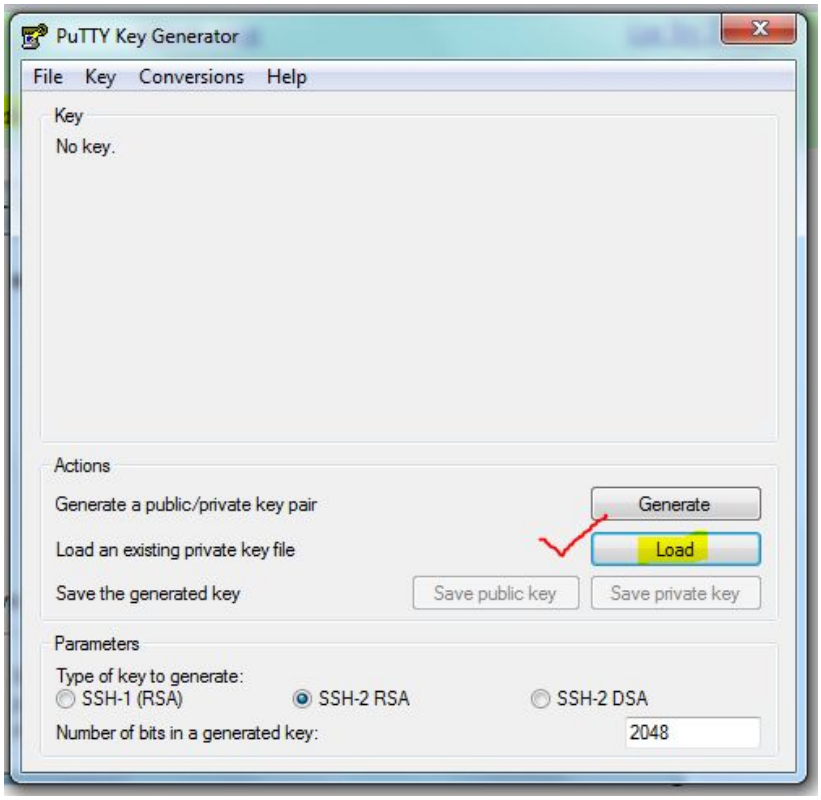
PuTTYGen 0.6 Download (Free) - PuTTYGen.exe
puttygen.software.informer.com › System Tools › General
Sep 21, 2016 - **PuTTYgen** is an open source RSA and DSA key generation utility. The program allows you to generate a public or private key pair, you can ...

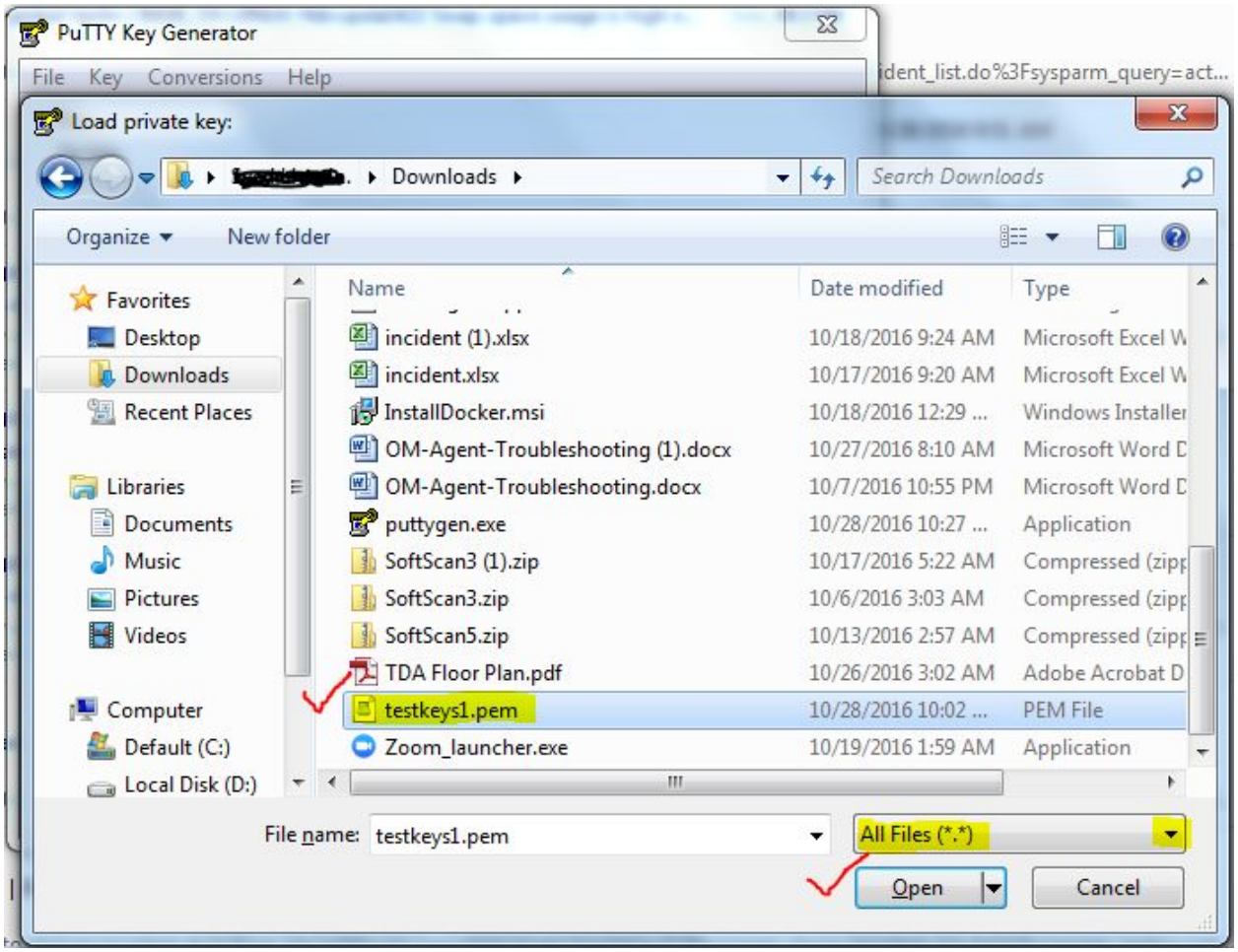
PuTTY Key Generator (PuTTYgen) Download - Softpedia
www.softpedia.com › Windows › Network Tools › Misc. Networking Tools
Jun 15, 2016 - Free **Download** PuTTY Key Generator (**PuTTYgen**) 2016-06-03.7b9ad09 / 0.67 beta - An efficient and easy to use RSA and DSA key generator ...

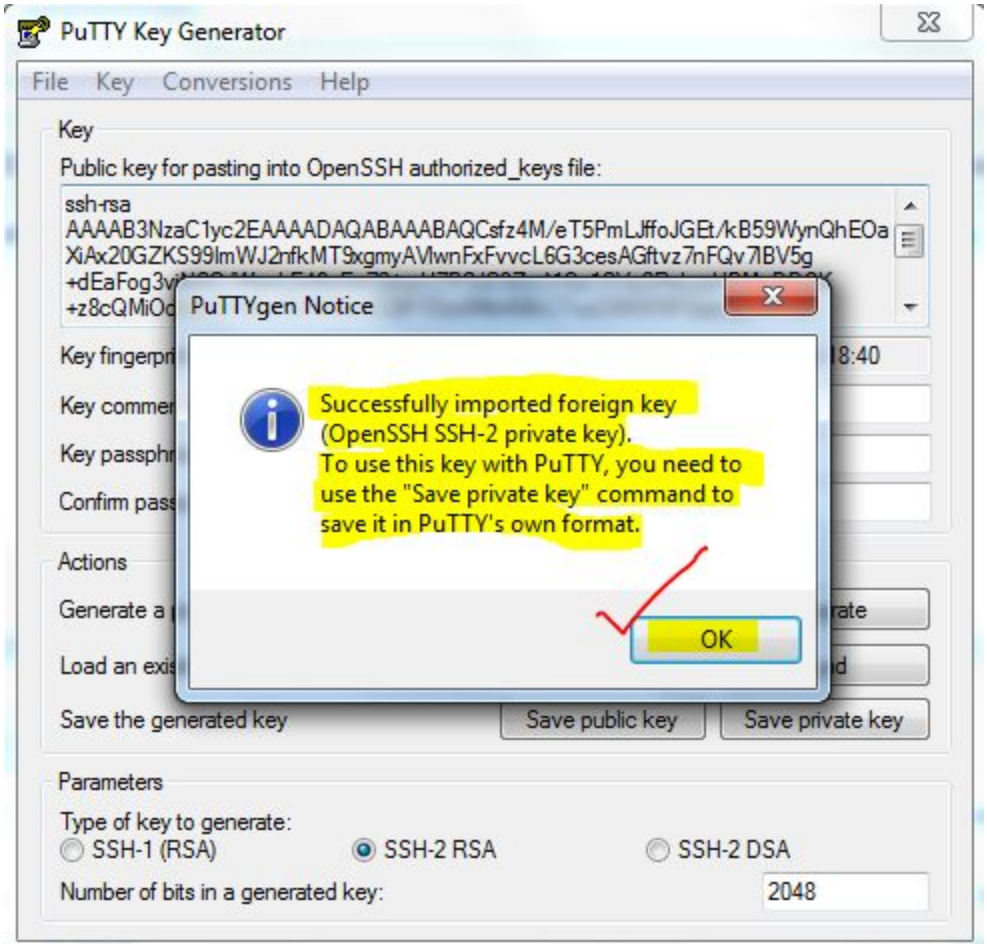
For Windows on Intel x86

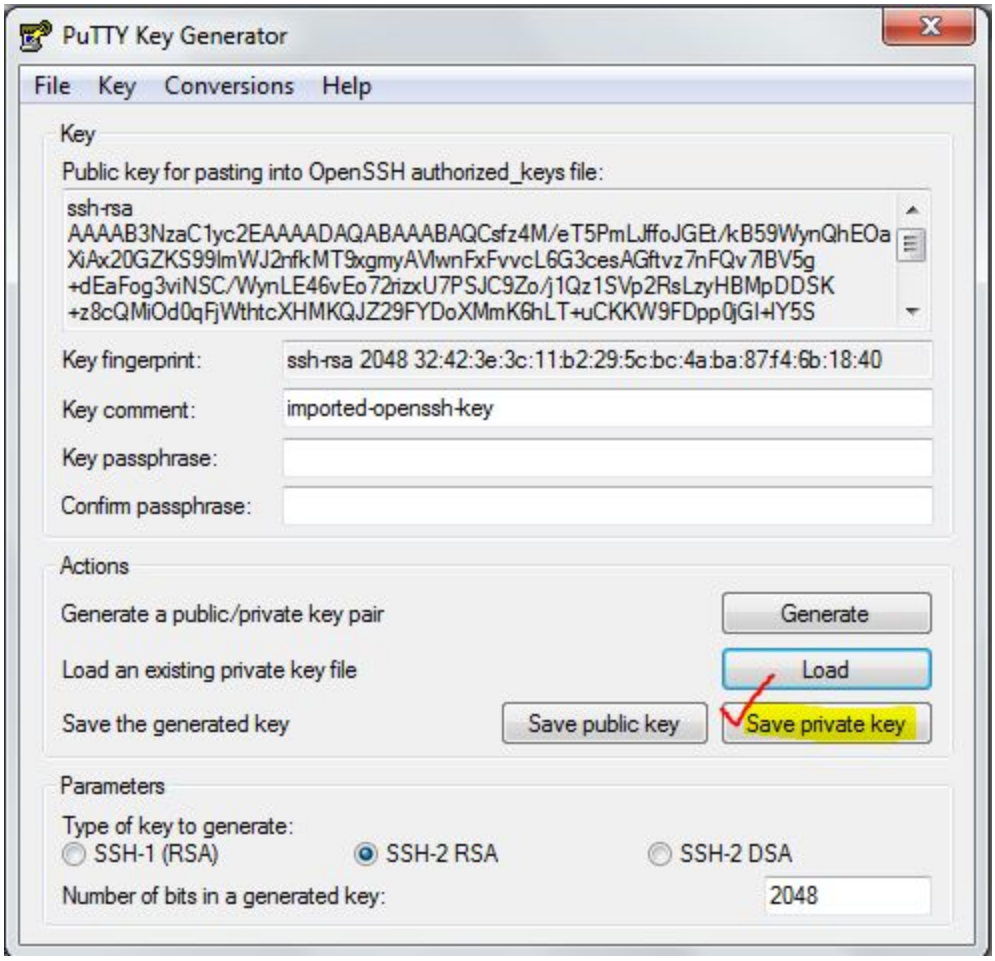
PuTTY:	putty.exe	(or by FTP)	(signature)
PuTTYtel:	puttytel.exe	(or by FTP)	(signature)
PSCP:	pscp.exe	(or by FTP)	(signature)
PSFTP:	psftp.exe	(or by FTP)	(signature)
Plink:	plink.exe	(or by FTP)	(signature)
Pageant:	pageant.exe	(or by FTP)	(signature)
PuTTYgen:	puttygen.exe	(or by FTP)	(signature)


Open File - Security Warning
Do you want to run this file?
Name: C:\Users\syedhussain\Downloads\puttygen.exe
Publisher: Simon Tatham
Type: Application
From: C:\Users\syedhussain\Downloads\puttygen.exe
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?


PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
SSH-1 (RSA)
SSH-2 RSA
SSH-2 DSA
Number of bits in a generated key:
2048


PuTTY Key Generator
File Key Conversions Help
Load private key:
Downloads
Search Downloads
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Default (C:)
Local Disk (D:)
Name
Date modified
Type
incident (1).xlsx 10/18/2016 9:24 AM Microsoft Excel W
incident.xlsx 10/17/2016 9:20 AM Microsoft Excel W
InstallDocker.msi 10/18/2016 12:29 ... Windows Installer
OM-Agent-Troubleshooting (1).docx 10/27/2016 8:10 AM Microsoft Word D
OM-Agent-Troubleshooting.docx 10/7/2016 10:55 PM Microsoft Word D
puttygen.exe 10/28/2016 10:27 ... Application
SoftScan3 (1).zip 10/17/2016 5:22 AM Compressed (zipp
SoftScan3.zip 10/6/2016 3:03 AM Compressed (zipp
SoftScan5.zip 10/13/2016 2:57 AM Compressed (zipp
TDA Floor Plan.pdf 10/26/2016 3:02 AM Adobe Acrobat D
testkeys1.pem 10/28/2016 10:02 ... PEM File
Zoom_launcher.exe 10/19/2016 1:59 AM Application
File name: testkeys1.pem
All Files (*.*)
Open
Cancel


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCsfz4M/eT5PmLJffoJGEt/kB59WynQhEOa
XiAx20GZKS99lmWJ2nfkMT9xgmyAVlwnFxFvvcL6G3cesAGftvz7nFQv7lBV5g
+dEaFog3vi
+z8cQMiOc
Key fingerpri
Key commer
Key passphr
Confirm pass
Actions
Generate a
Load an exis
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
SSH-1 (RSA)
SSH-2 RSA
SSH-2 DSA
Number of bits in a generated key:
2048
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK



When you click **OK**, PuTTYgen displays a dialog box with information about the key you loaded, such as the public key and the fingerprint.

- Click **Save private key** to save the key in PuTTY's format.
- Do NOT select a passphrase and save your private key somewhere secure.

Now you are ready to use PuTTY for connecting to the previously created instance!

Step 4 Connect to a remote shell using an SSH connection

In order to manage a remote Linux server, you must employ an **SSH Client**. Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network. Common applications include remote command-line login and remote command execution.

Connect using Linux / Mac OS

Linux distributions and Mac OS are shipped with a fully working SSH client that accepts standard PEM Keys.

Starting a remote SSH session is easy:

- Open your **Terminal** application
- Write and run the following command: `ssh -i /path/to/your/keypair.pem user@server-ip`.

  `server-ip` is the Public IP of your server, you can find it in the EC2 instance details

  `user` is the remote system user that will be used for the remote authentication

Amazon Linux AMIs typically use `ec2-user` as username.

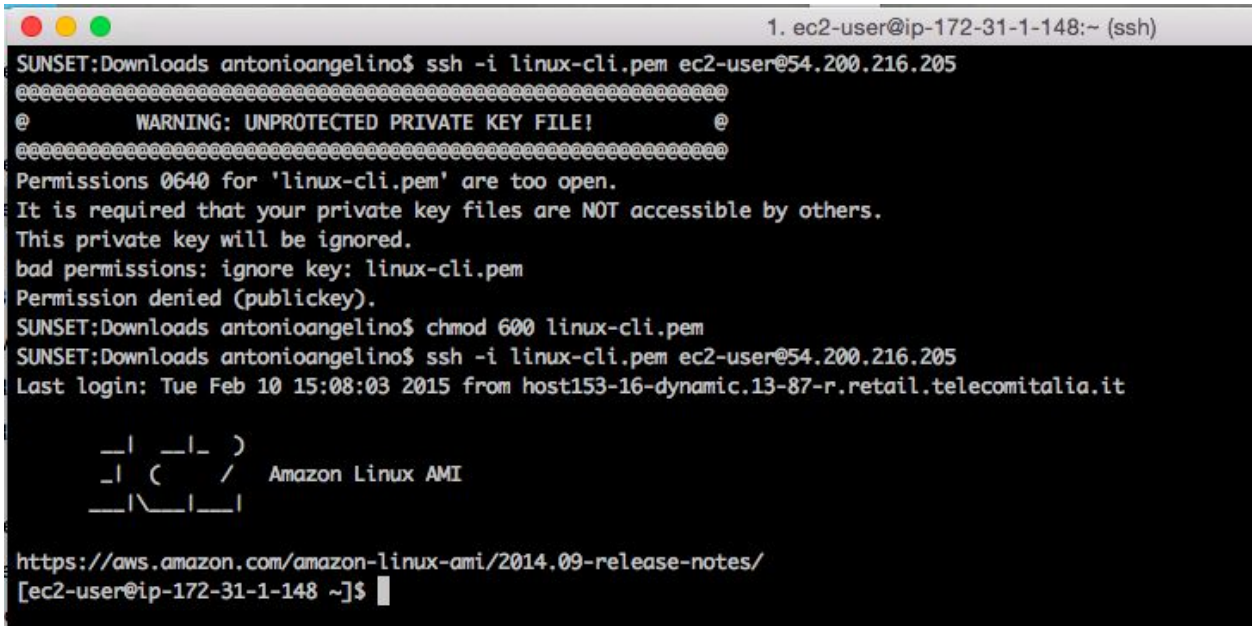
Ubuntu AMIs login user is `ubuntu`, Debian AMIs use `admin` instead.

Assuming that you selected the Amazon Linux AMI, your assigned public IP is 123.123.123.123, and your keypair (named "keypair.pem") is stored in /home/youruser/keypair.pem, the right command to run is:

```
ssh -i /home/youruser/keypair.pem ec2-user@123.123.123.123
```

Note: your SSH Client may refuse to start the connection, warning that the key file is unprotected. You should deny the file access to any other system user by changing its permissions. Issue the following command and then try again:

```
chmod 600  /home/youruser/keypair.pem
```

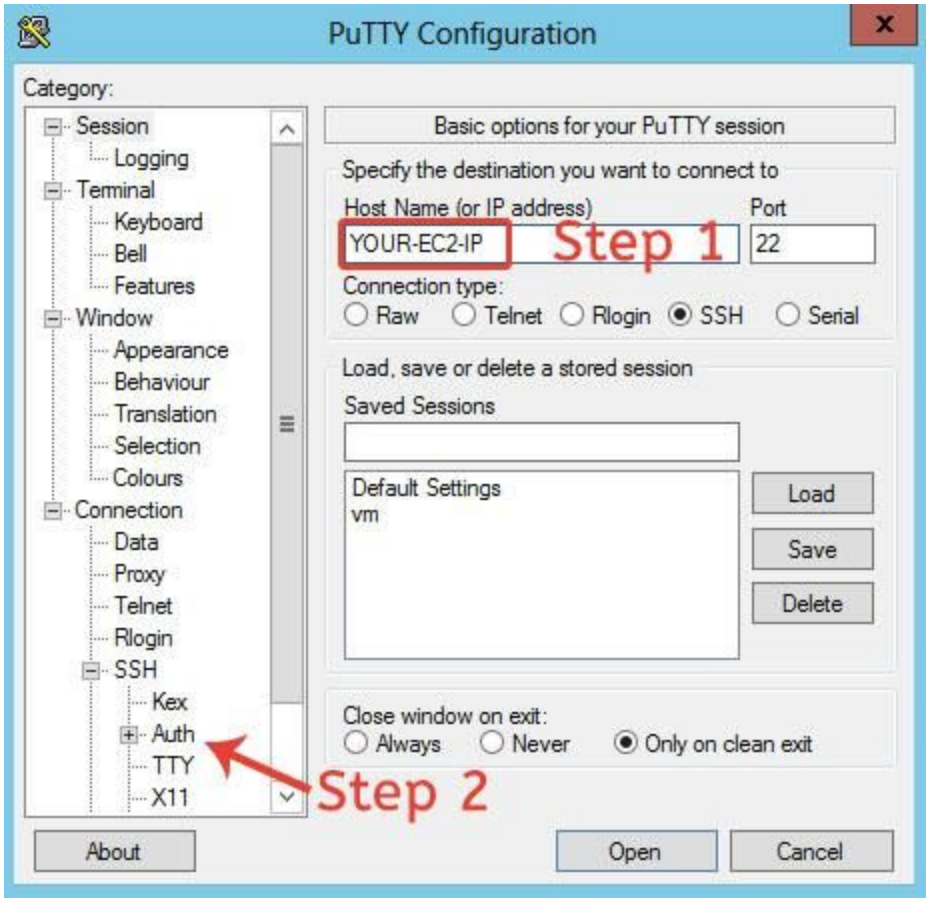


Connect using Windows

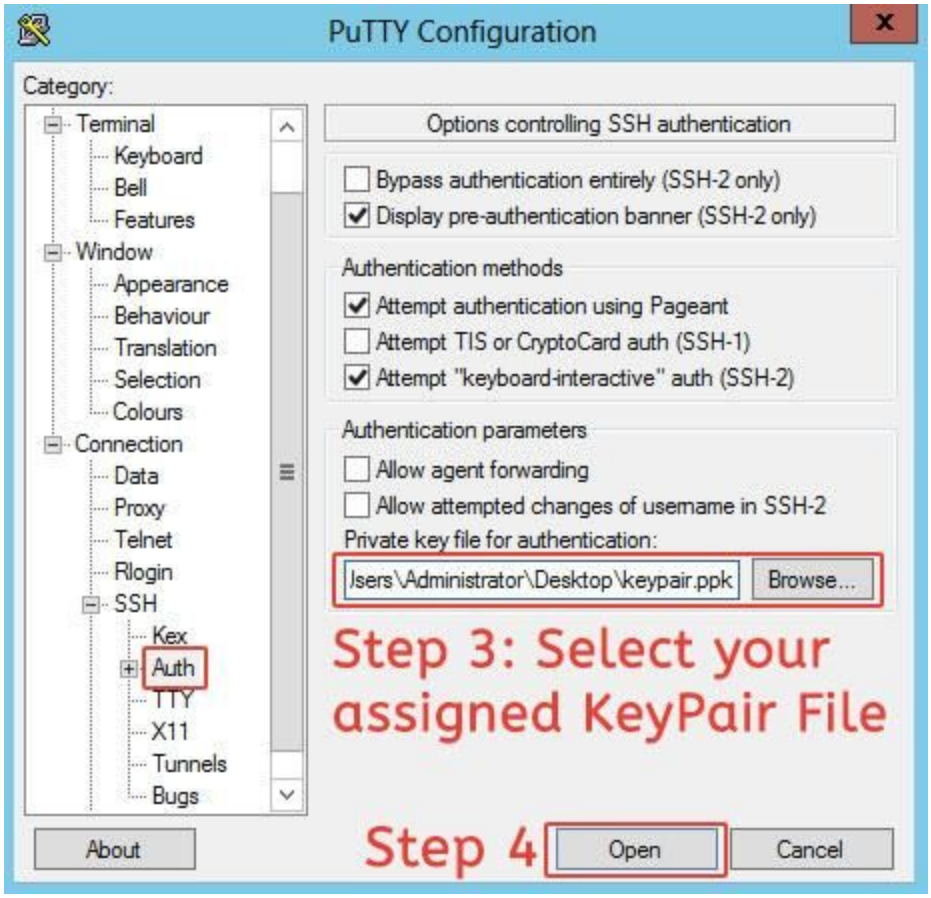
Windows has no SSH client, so you must use PuTTY and convert the PEM key to PPK using PuTTYgen.

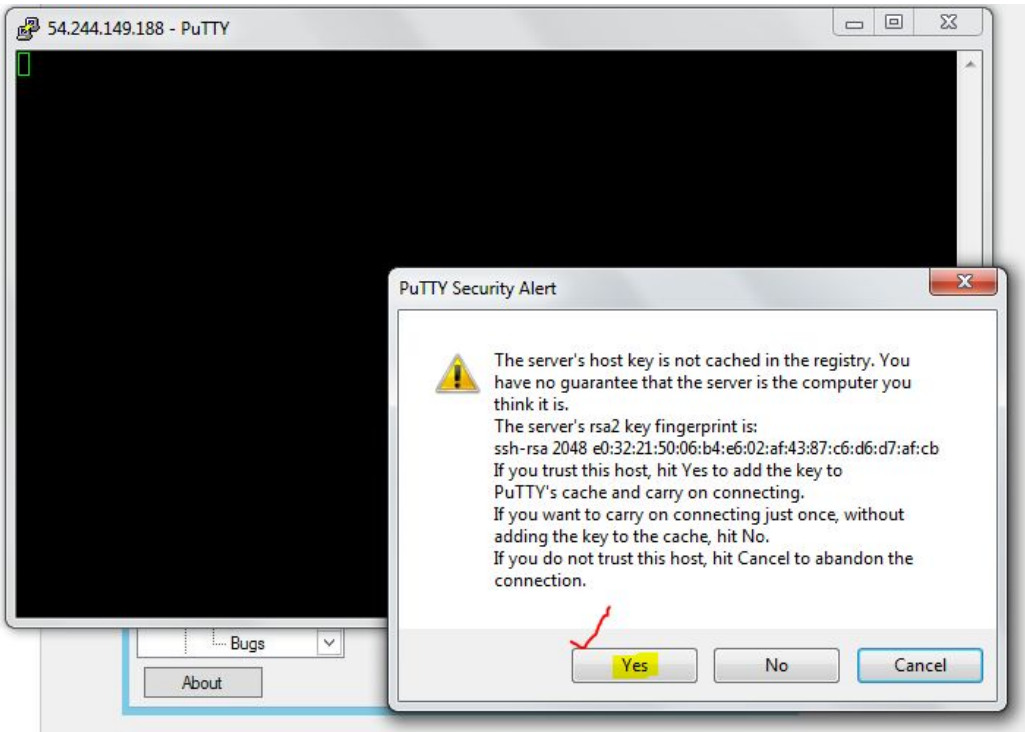
Starting a remote SSH session using PuTTY is easy:

- Open PuTTY and insert the EC2 instance IP Address in the Host Name field.

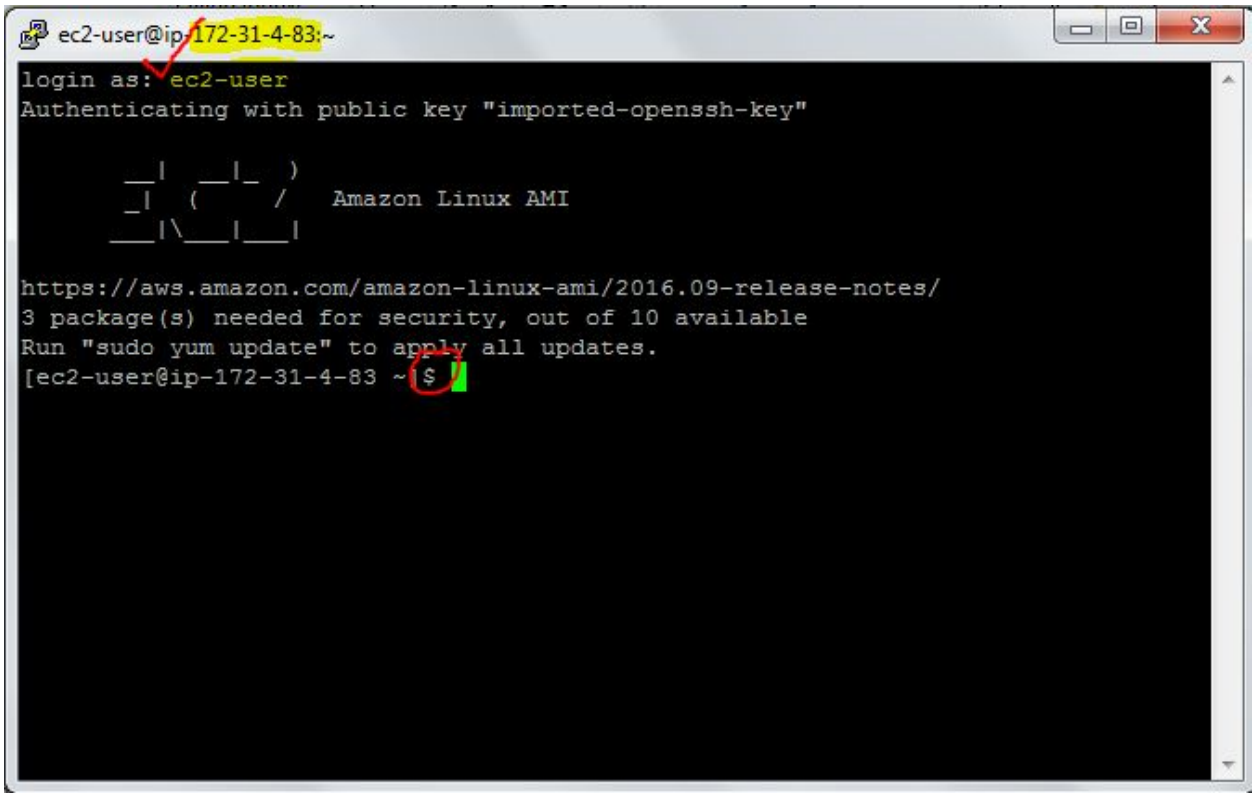


Select **Connection > SSH > Auth** section and then select the downloaded Keypair that you previously converted to PPK format.


PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Options controlling SSH authentication
Bypass authentication entirely (SSH-2 only)
Display pre-authentication banner (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
/sers\Administrator\Desktop\keypair.ppk
Browse...
Step 3: Select your assigned KeyPair File
About
Step 4
Open
Cancel



- After some seconds, you will see the authentication form. **Login as** `ec2-user` and you will see the EC2 server welcome banner.

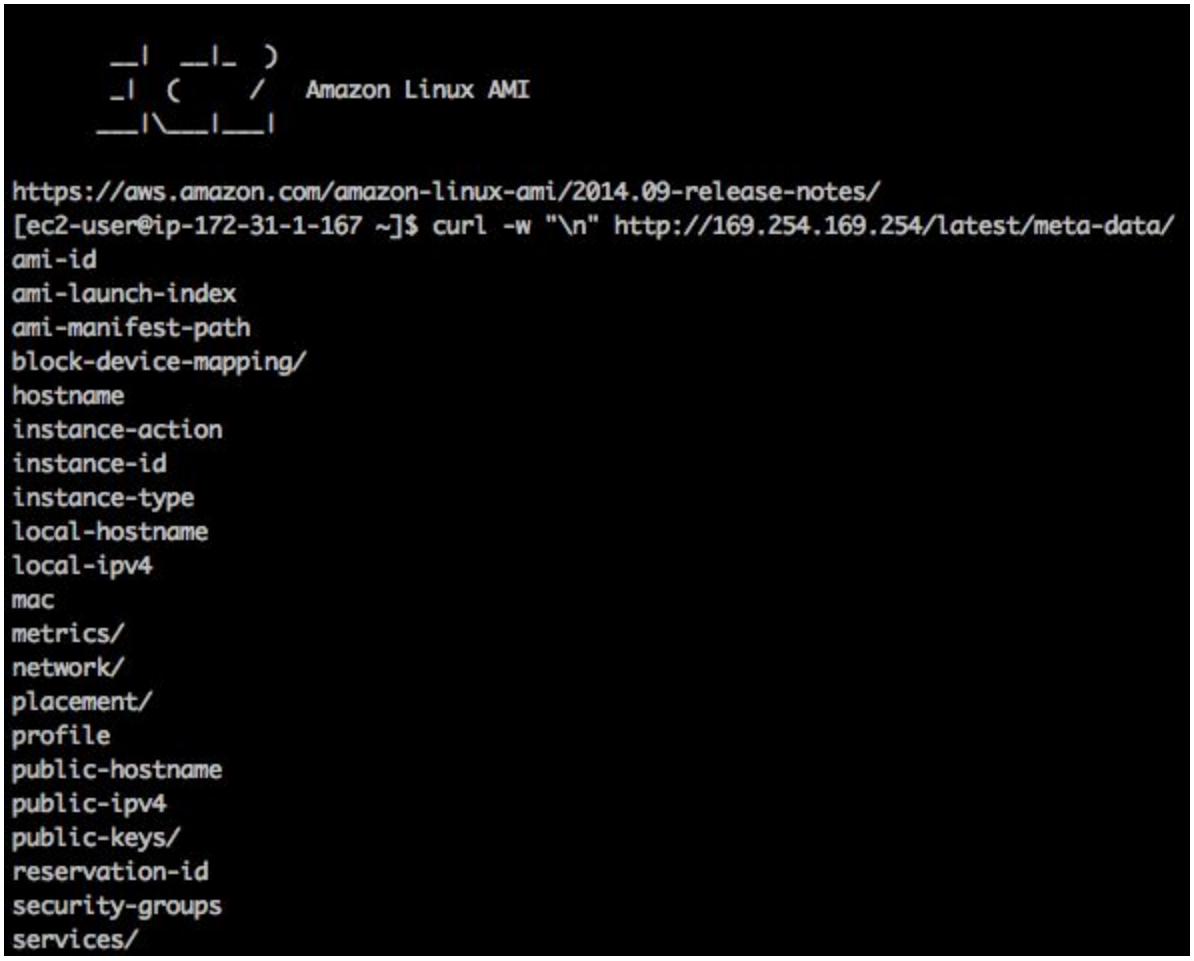


Step 5 Get the EC2 instance metadata

Now you are ready to send the first commands to your EC2 linux instance. Let's check the EC2 instance metadata by hitting a specific AWS node only available from within the instance itself.

Instance metadata is data about your instance that you can use to configure or manage the running instance. You can list all instance metadata by issuing the following command:

```
curl -w "\n" http://169.254.169.254/latest/meta-data/
```



You can easily check the list of security groups attached to the instance, its ID, the hostname, or the ID of the used AMI. These commands are extremely useful when you want to automate the setup of new instances:

```
curl -w "\n" http://169.254.169.254/latest/meta-data/security-groups
```

```
curl -w "\n" http://169.254.169.254/latest/meta-data/ami-id
```

```
curl -w "\n" http://169.254.169.254/latest/meta-data/hostname
```

```
curl -w "\n" http://169.254.169.254/latest/meta-data/instance-id
```

```
curl -w "\n" http://169.254.169.254/latest/meta-data/instance-type
```

```
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/services

[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/security-groups
launch-wizard-1
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/ami-id
ami-dfc39aef
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/hostname
ip-172-31-1-167.us-west-2.compute.internal
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/instance-id
i-532c1e5f
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/instance-type
t2.micro
```

Finally, you can also get the public key of the attached Keypair using the public-keys metadata:

```
curl -w "\n" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

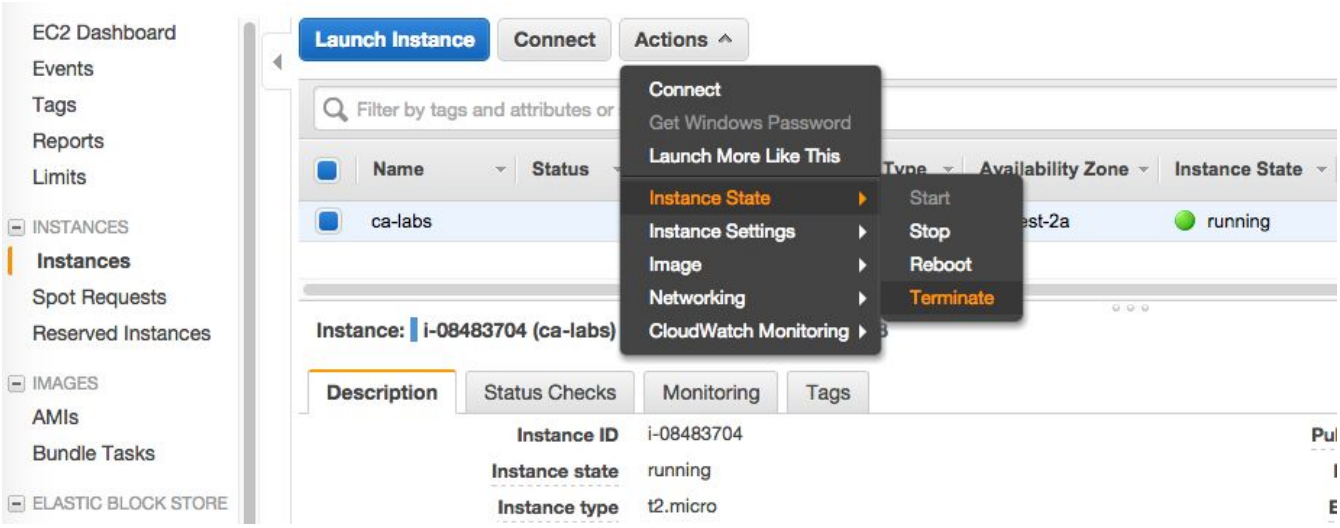
```
[ec2-user@ip-172-31-1-167 ~]$ curl -w "\n" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjbI3OTa27LTNuZru3QahbVEXVZ9sZZsDk6Bc3FpTomqUCCVno/gx96o7RuFIYxWSSR4CWc
jbI7hoJXy1UMSNktf1YG341tN5gwS+vtmeeZifxKbfT5PaUtIoWGvPkHcV2SGERPyHZ/clNuYEAq3Pmc6tGK0Bh2SJDqzdxUo3CU0+wMc/+sS
jakMLSu4LIwyJnmP2gcoj6z0PVmoLzC5FRQjPlccY15xorkRmsHeTpm+waDBhVPdYvpsPfunx+uuSOpXn8NcXNHUBsIMpXUI/sRYW9Z/PP+IO
lMSQwqBcHUCvzS93xUVSVgsefUbL2hdN2Ww0twAFC5NDs+tj1+tcf test
```

Step 6 Terminate an EC2 instance

When you've decided that you no longer need an instance, you can terminate it.

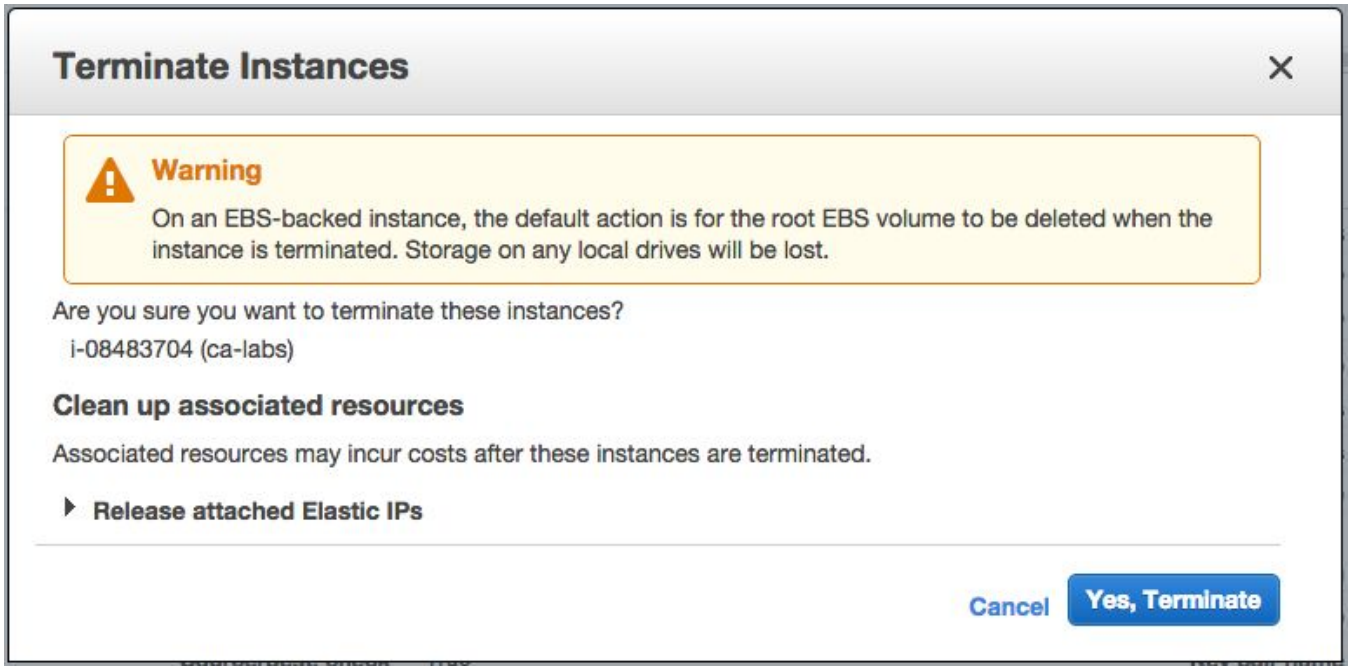
Select the EC2 service from the Management Console dashboard:

In the navigation pane, click **Instances**.



Select the instance ec2instance, click **Actions**, select **Instance State**, and then click **Terminate**.

Click **Yes, Terminate** when prompted for confirmation.



Now your instance is completely destroyed.