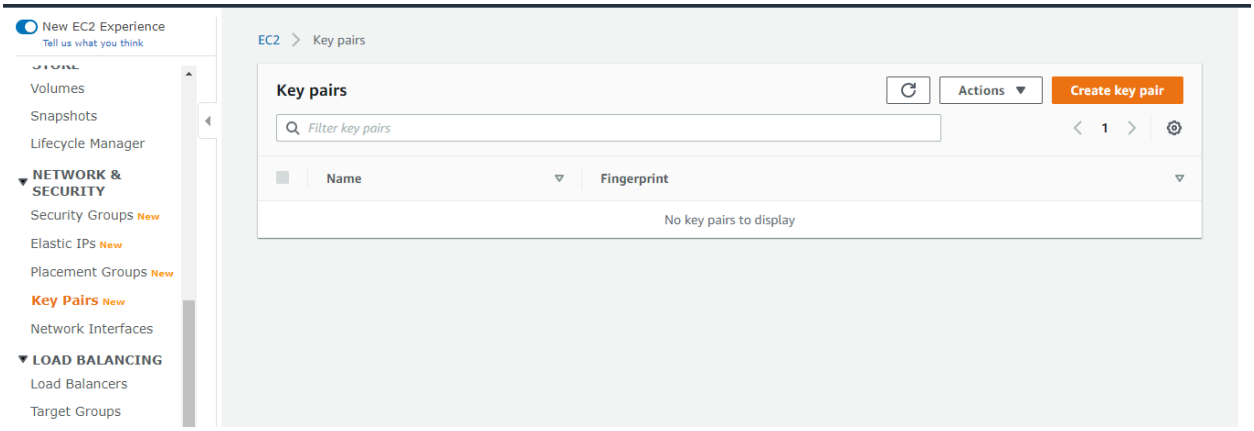
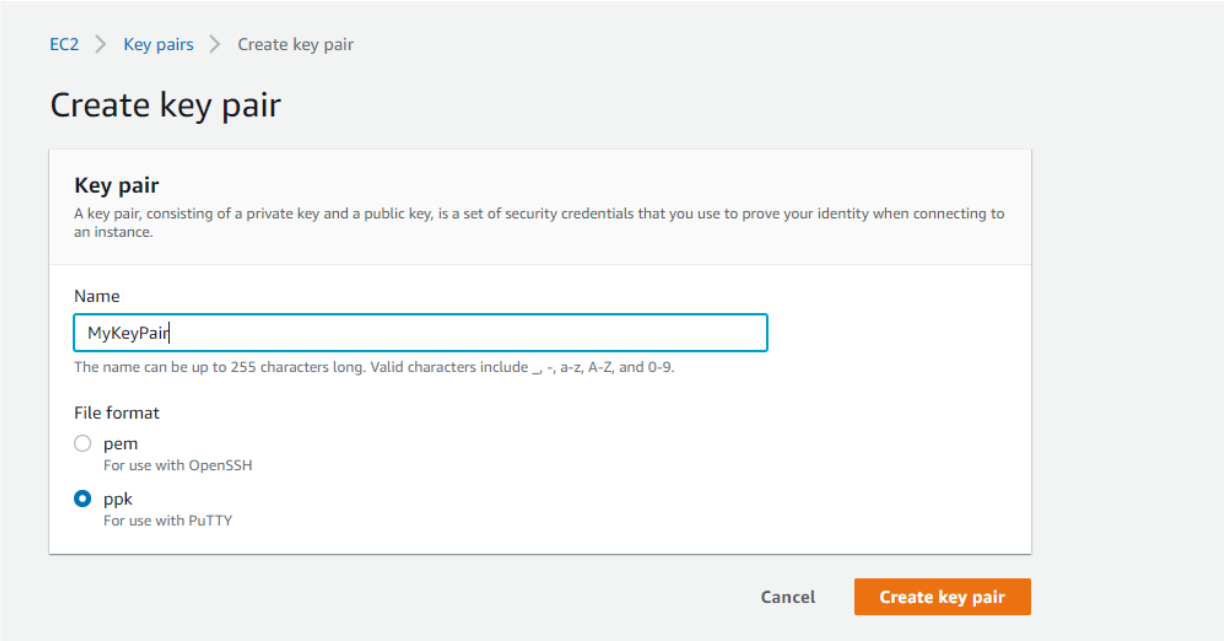
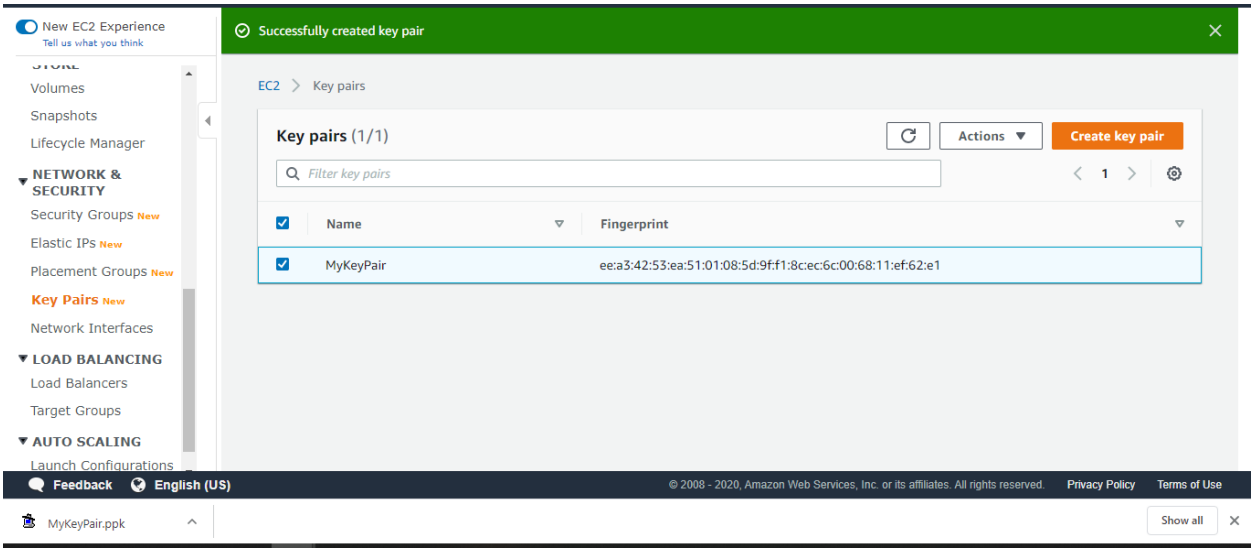
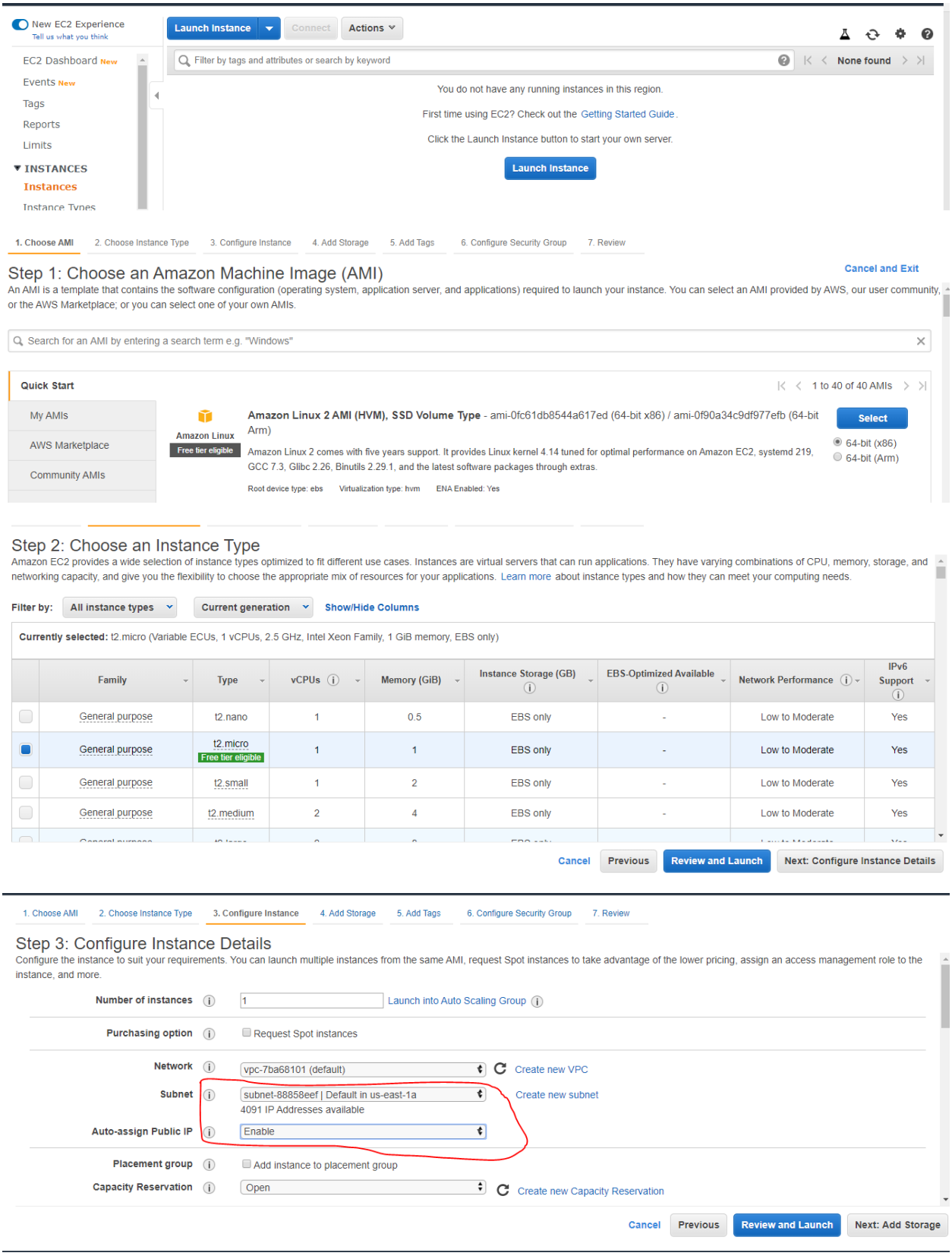
Key Pair


New EC2 Experience
Tell us what you think
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups New
Elastic IPs New
Placement Groups New
Key Pairs New
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
EC2 > Key pairs
Key pairs
Actions
Create key pair
Filter key pairs
1
Name
Fingerprint
No key pairs to display


EC2 > Key pairs > Create key pair
Create key pair
Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.
Name
MyKeyPair
The name can be up to 255 characters long. Valid characters include _, -, a-z, A-Z, and 0-9.
File format
pem
For use with OpenSSH
ppk
For use with PuTTY
Cancel
Create key pair


New EC2 Experience
Tell us what you think
Successfully created key pair
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups New
Elastic IPs New
Placement Groups New
Key Pairs New
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
EC2 > Key pairs
Key pairs (1/1)
Actions
Create key pair
Filter key pairs
1
Name
Fingerprint
MyKeyPair
ee:a3:42:53:ea:51:01:08:5d:9f:f1:8c:ec:6c:00:68:11:ef:62:e1
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
MyKeyPair.ppk
Show all

Launch EC2 Instance



1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | **4. Add Storage** | 5. Add Tags | 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	Encryption
Root	/dev/xvda	snap-0e27a39c6e2f9f079	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypte

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: Add Tags

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | **5. Add Tags** | 6. Configure Security Group | 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Jenkin-Test	☑	☑

Add another tag (Up to 50 tags maximum)

Cancel | Previous | Review and Launch | Next: Configure Security Group

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | **6. Configure Security Group** | 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ◉ Create a **new** security group
○ Select an **existing** security group

Security group name: JenKinSG

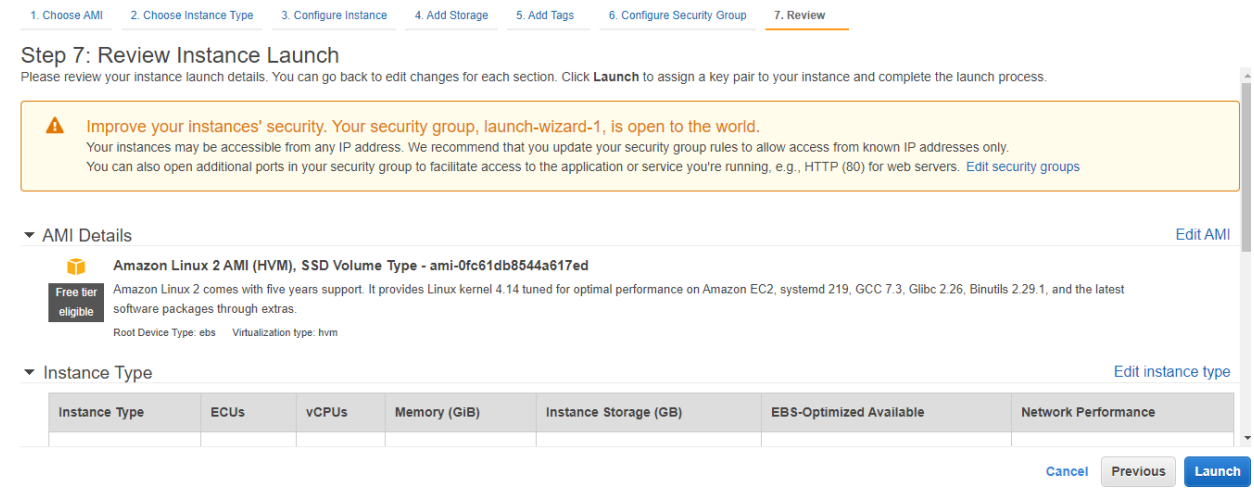
Description: JenKinSG Testing

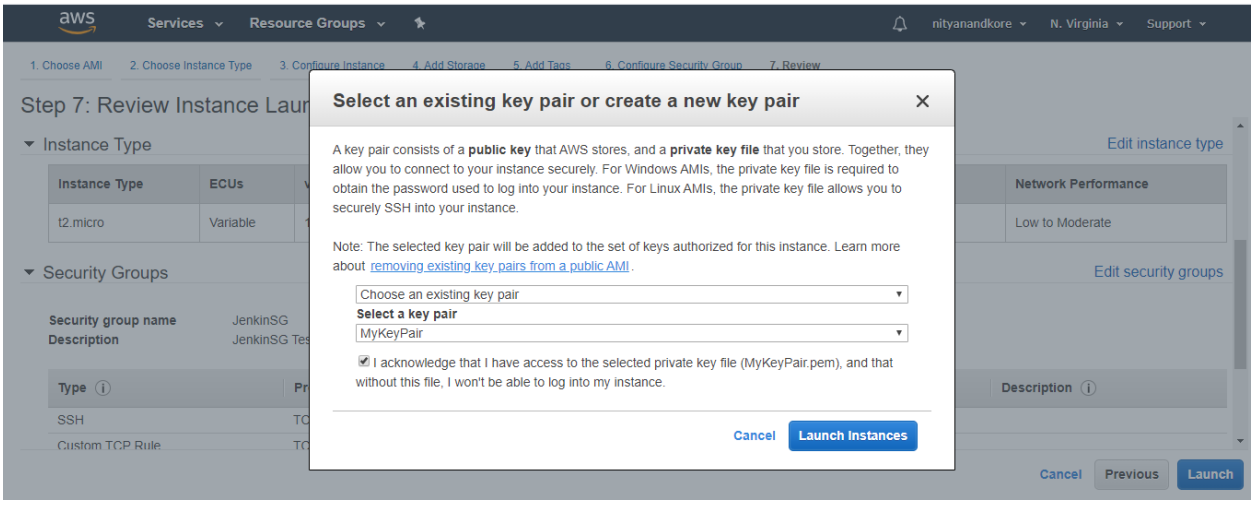
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP R	TCP	8080	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

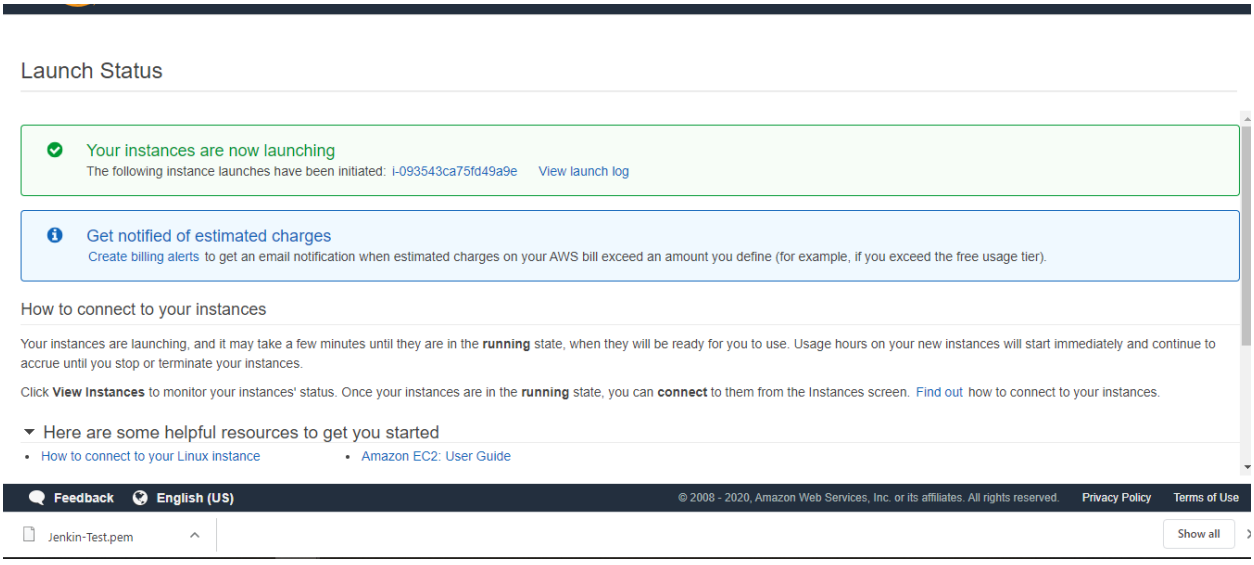
Add Rule

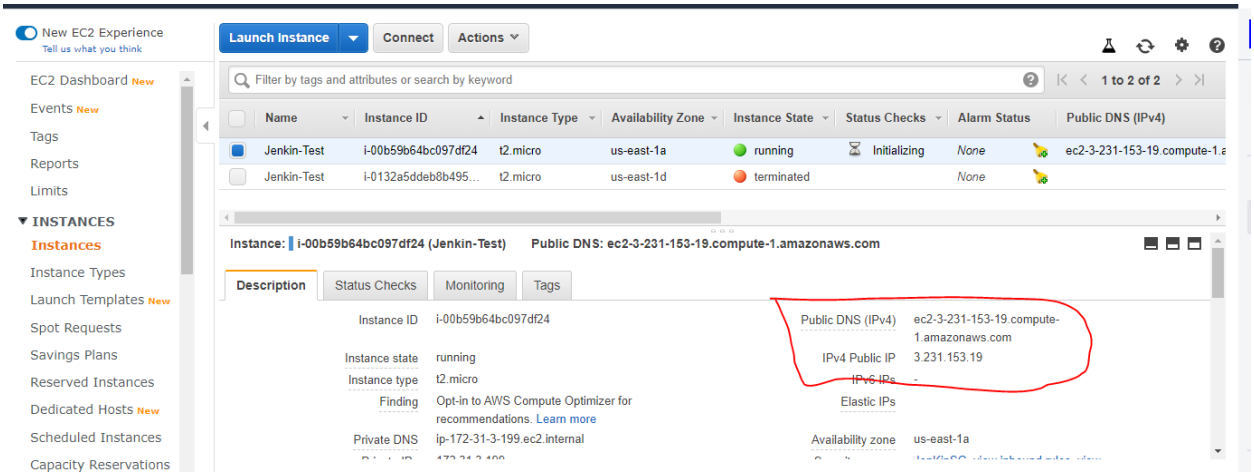
⚠ Warning

Cancel | Previous | Review and Launch

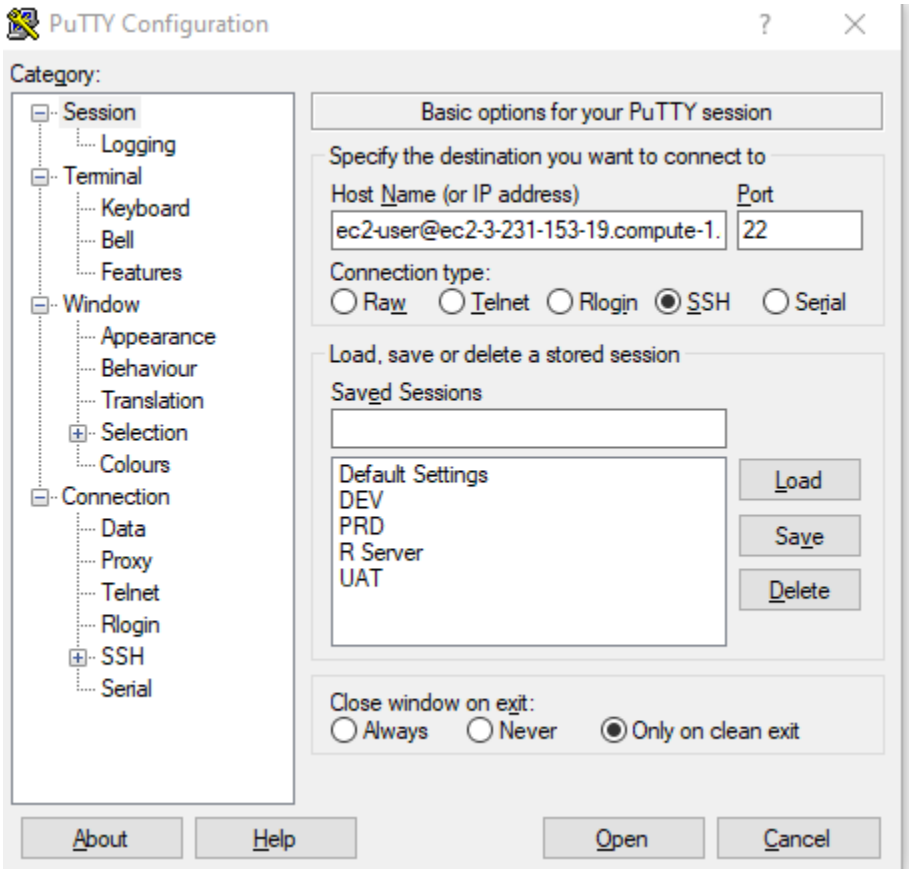

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance 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 2 AMI (HVM), SSD Volume Type - ami-0fc61db8544a617ed
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
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
Cancel
Previous
Launch

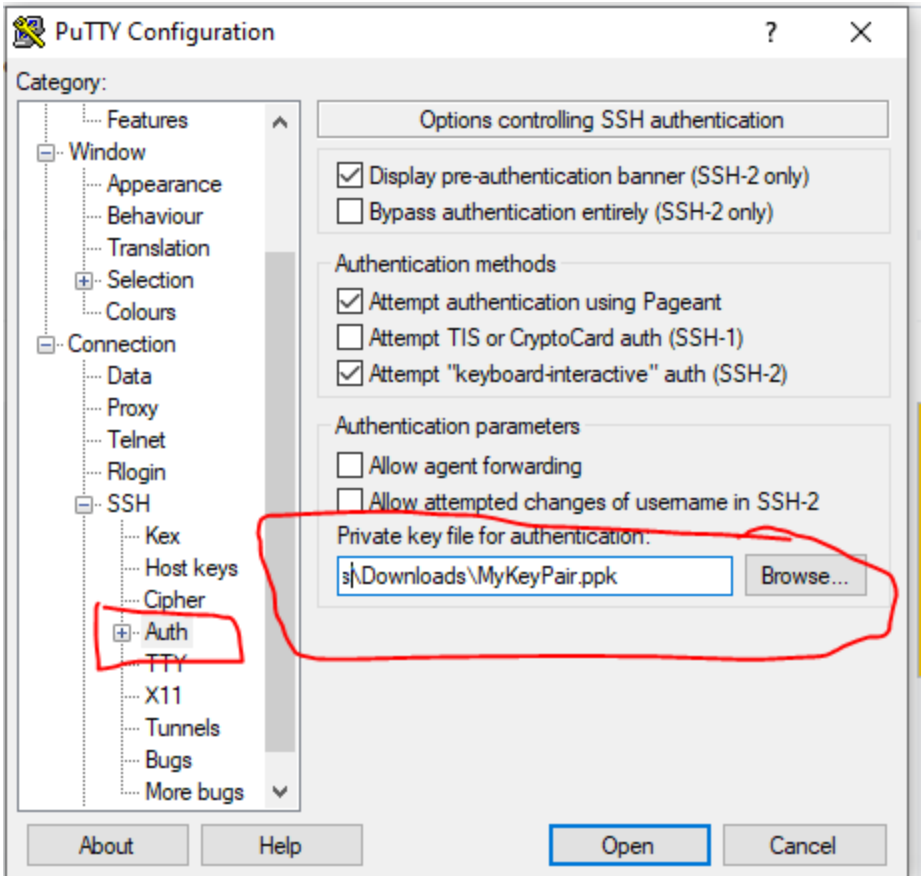

aws
Services
Resource Groups
nityanandkore
N. Virginia
Support
Step 7: Review Instance Laur
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For 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.
Choose an existing key pair
Select a key pair
MyKeyPair
I acknowledge that I have access to the selected private key file (MyKeyPair.pem), and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances
Instance Type
Edit instance type
t2.micro
Variable
Low to Moderate
Security Groups
Edit security groups
Security group name JenkinSG
Description
Type
Description
SSH
Custom TCP Rule
Cancel
Previous
Launch

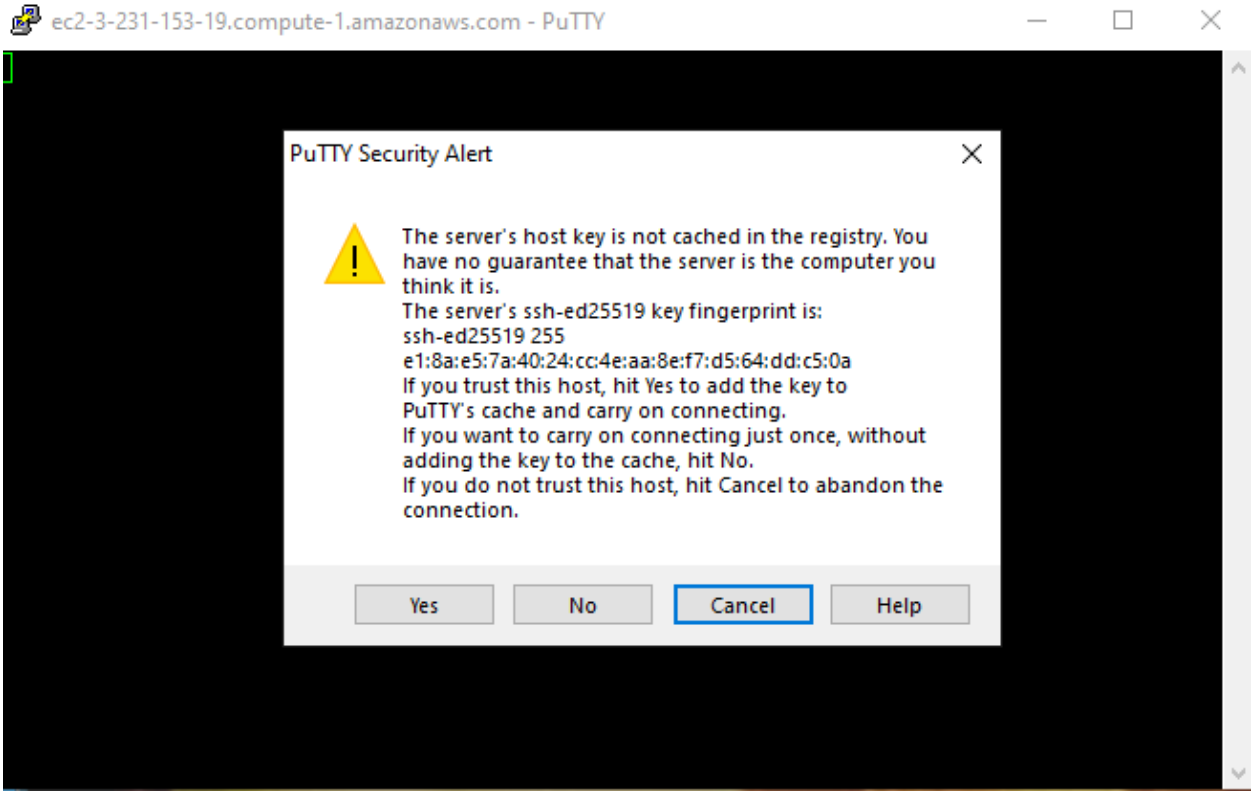

Launch Status
Your instances are now launching
The following instance launches have been initiated: i-093543ca75fd49a9e View launch log
Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, 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
Amazon EC2: User Guide
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Jenkin-Test.pem
Show all



To Connect to Your Linux Instance from Windows Using PuTTY 1. From the Start menu, choose All Programs > PuTTY > PuTTY. 2. In the Category pane, select Session, and complete the following fields: a. In Host Name, enter ec2-user@ec2-3-231-153-19.compute-1.amazonaws.com




PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (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:
s\Downloads\MyKeyPair.ppk
Browse...
About
Help
Open
Cancel


ec2-3-231-153-19.compute-1.amazonaws.com - PuTTY
PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255
e1:8a:e5:7a:40:24:cc:4e:aa:8e:f7:d5:64:dd:c5:0a
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes
No
Cancel
Help

Before doing the steps make sure you have java1.8 rather then default java1.7 ship with Amazon AMI. If you could see the 1.7 version you can uninstall and install the 1.8 using following commands,
[ec2-user ~]$ sudo yum remove java-1.7.0-openjdk
[ec2-user ~]$ sudo yum install java-1.8.0

Download and Install Jenkins

1. To ensure that your software packages are up to date on your instance, use the following command to perform a quick software update:

[ec2-user ~]$ sudo yum update –y

2. Add the Jenkins repo using the following command:

[ec2-user ~]$ sudo wget -O /etc/yum.repos.d/jenkins.repo http://pkg.jenkins-ci.org/redhat/jenkins.repo

3. Import a key file from Jenkins-CI to enable installation from the package:

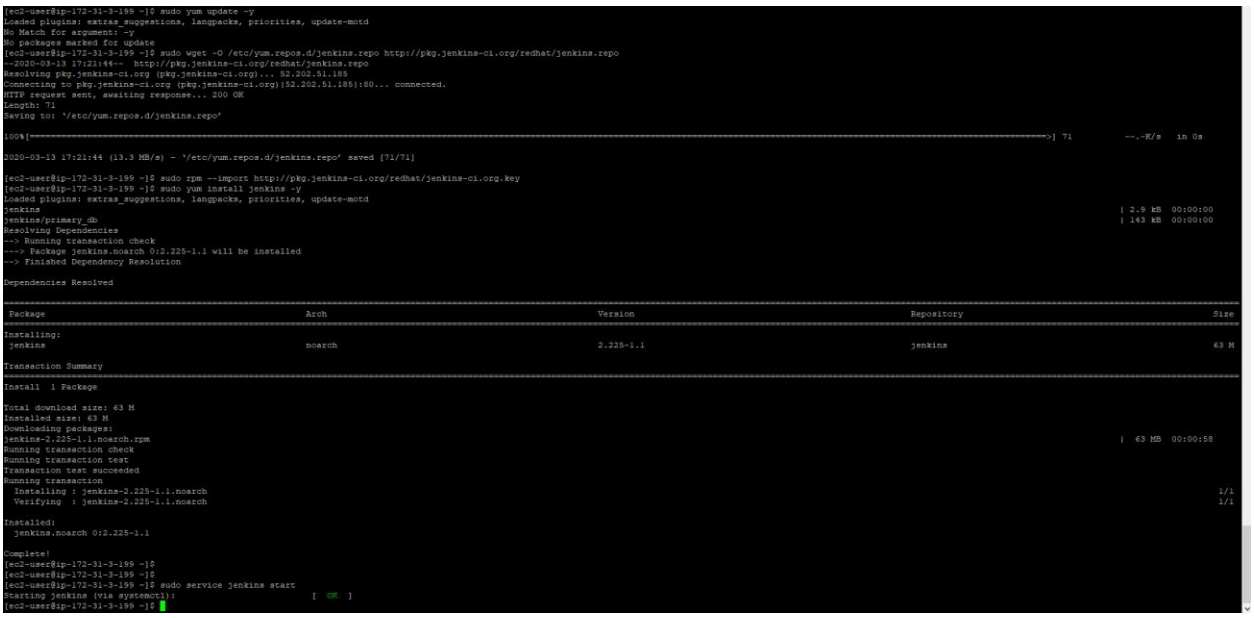
[ec2-user ~]$ sudo rpm --import http://pkg.jenkins-ci.org/redhat/jenkins-ci.org.key

4. Install Jenkins:

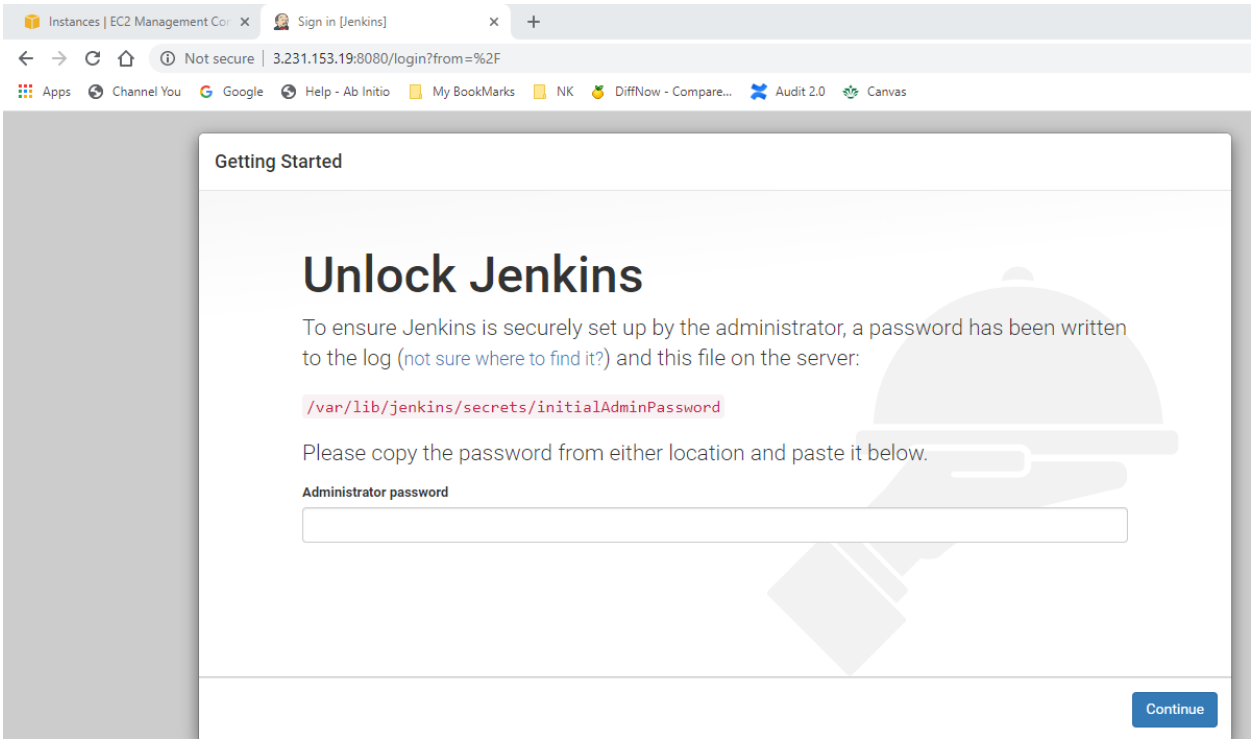
[ec2-user ~]$ sudo yum install jenkins -y

5. Start Jenkins as a service.

[ec2-user ~]$ sudo service jenkins start



Open Browser and paste : http://3.231.153.19:8080/



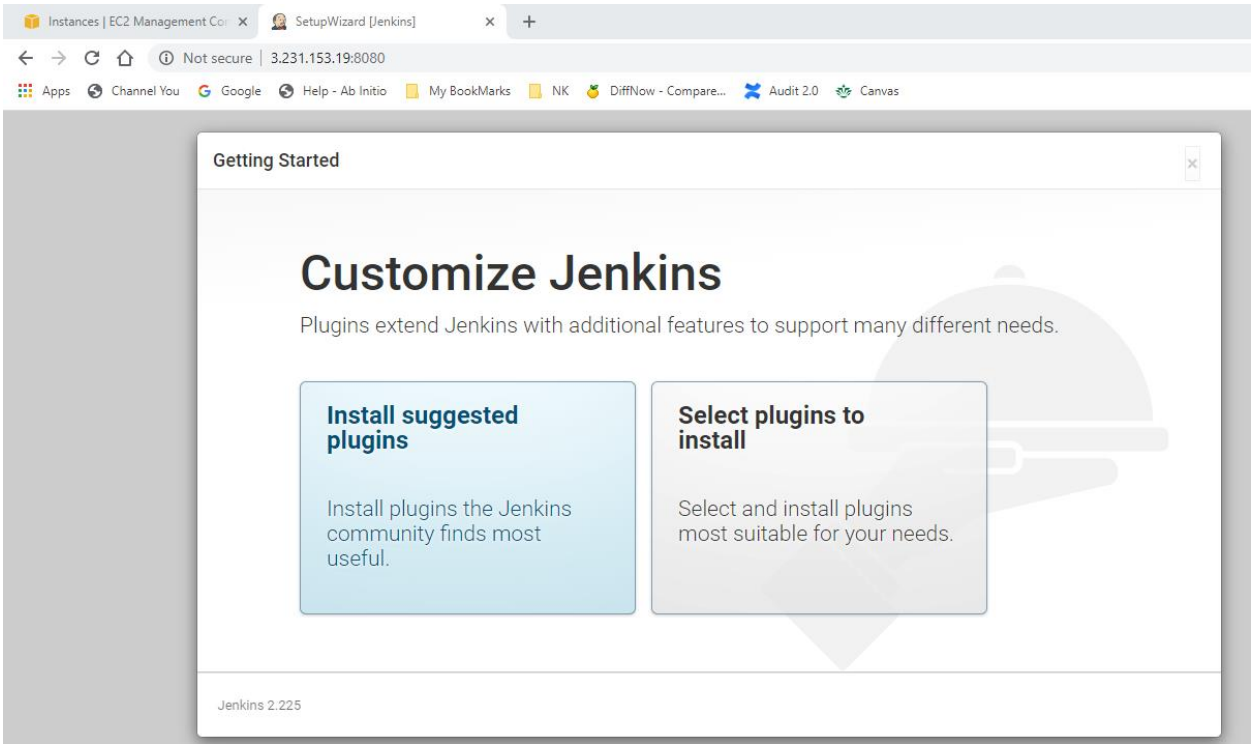
Getting Started Jenkins Page

Then you could visit the directory path shown in above image and get the initial password to proceed with the installation.

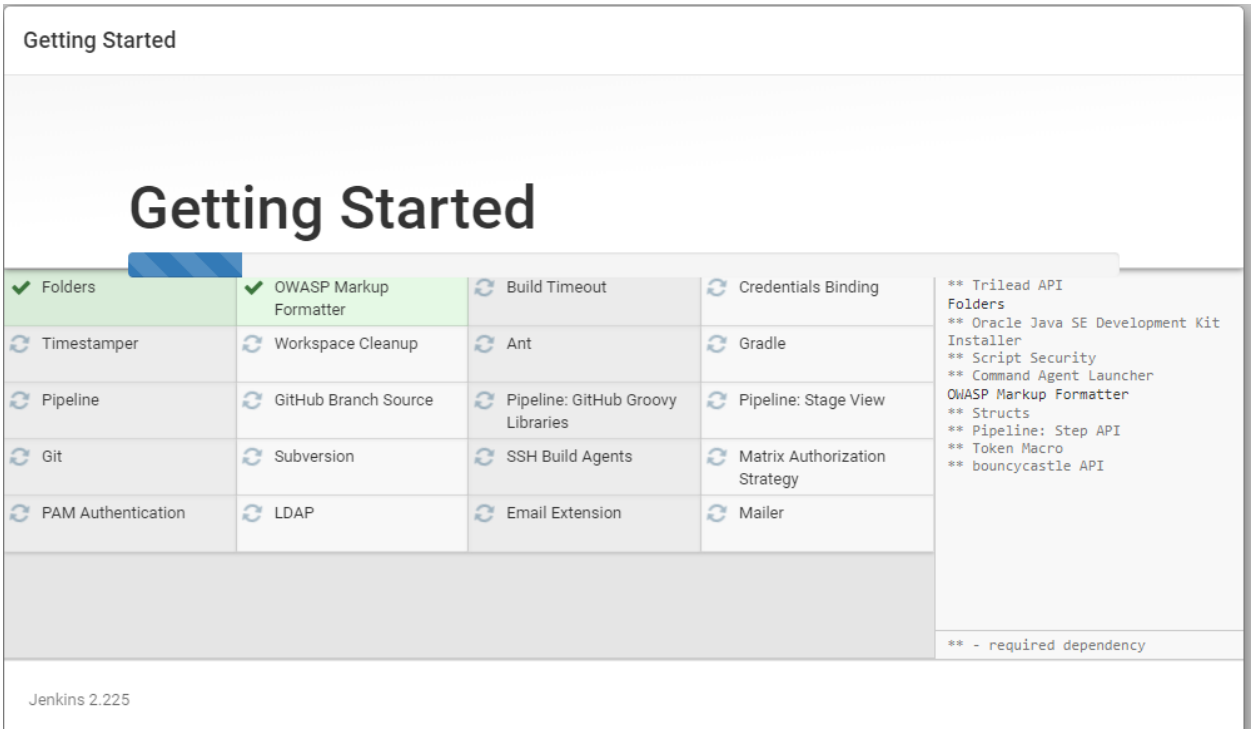
[ec2-user ~]$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword

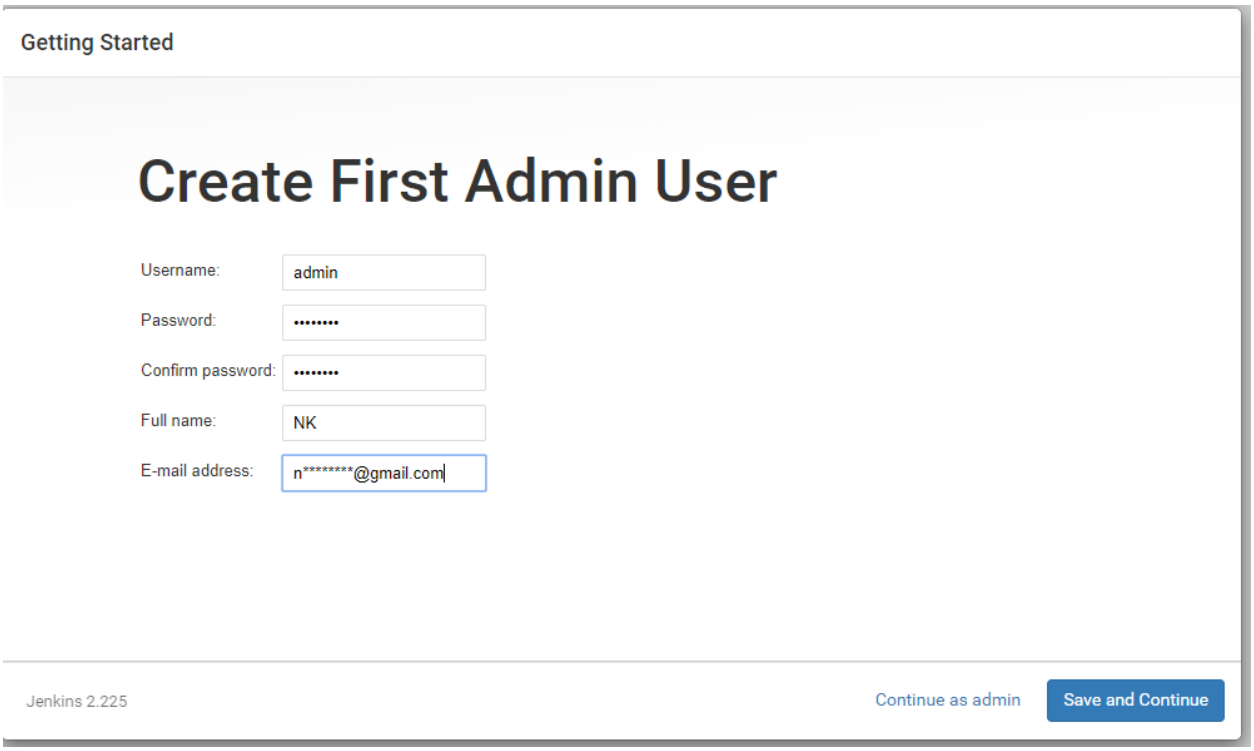
```
[ec2-user@ip-172-31-3-199 ~]$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
3ec104e837294c81801c229785298acc
[ec2-user@ip-172-31-3-199 ~]$
```

and paste it in the above image.



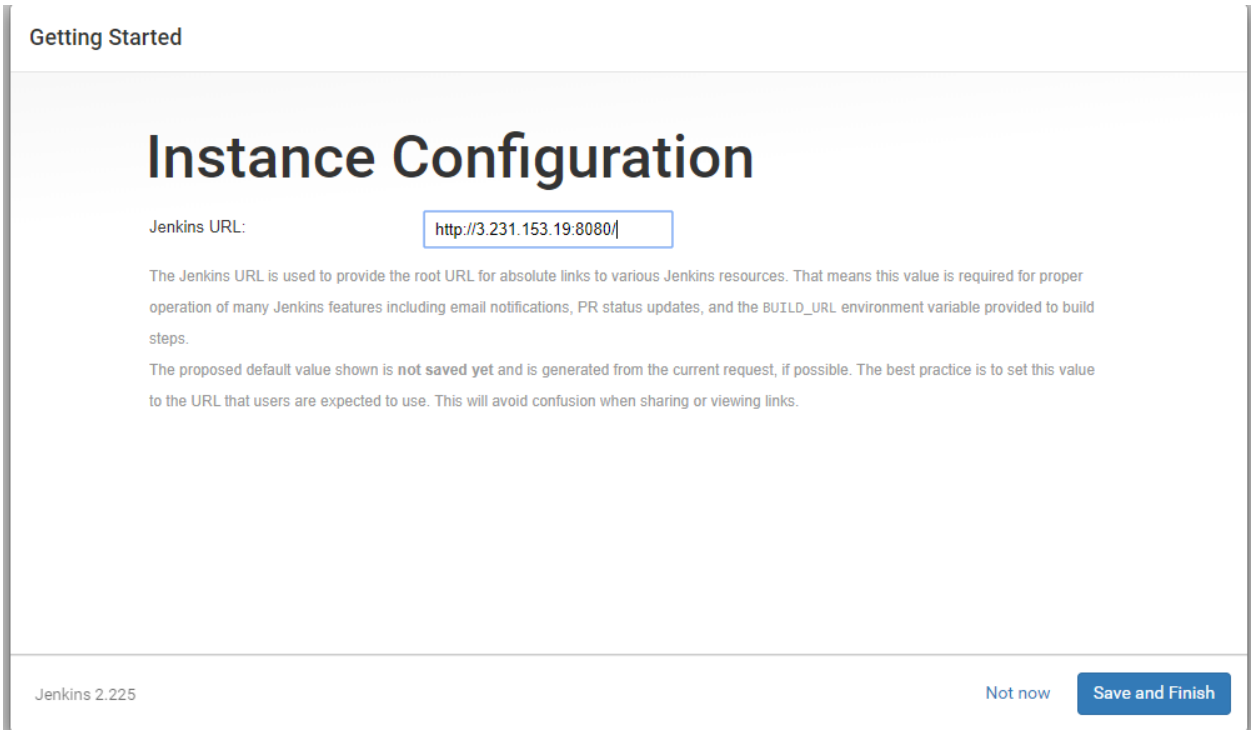
Click on Install suggested plugins

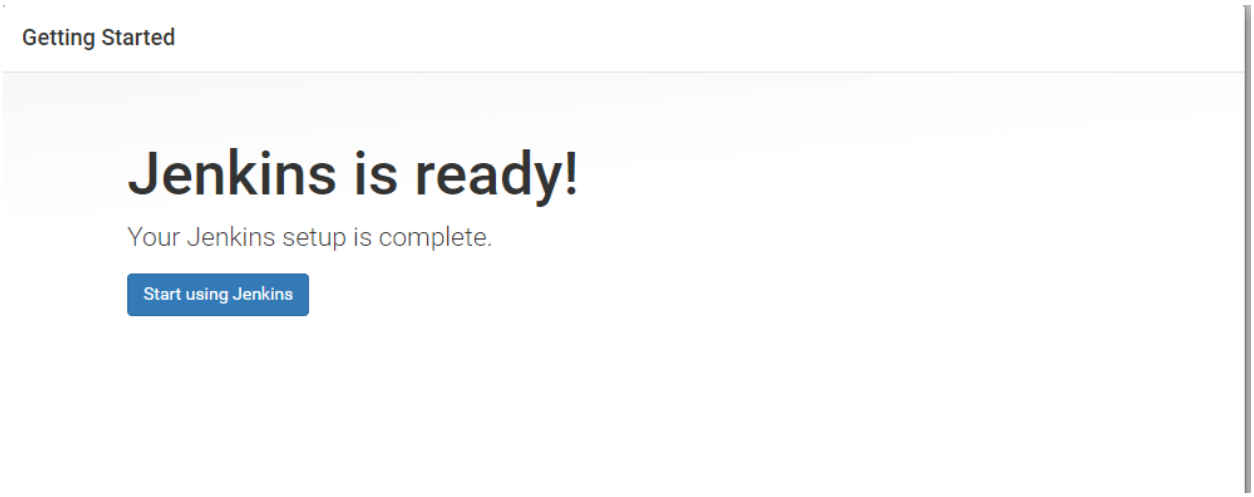


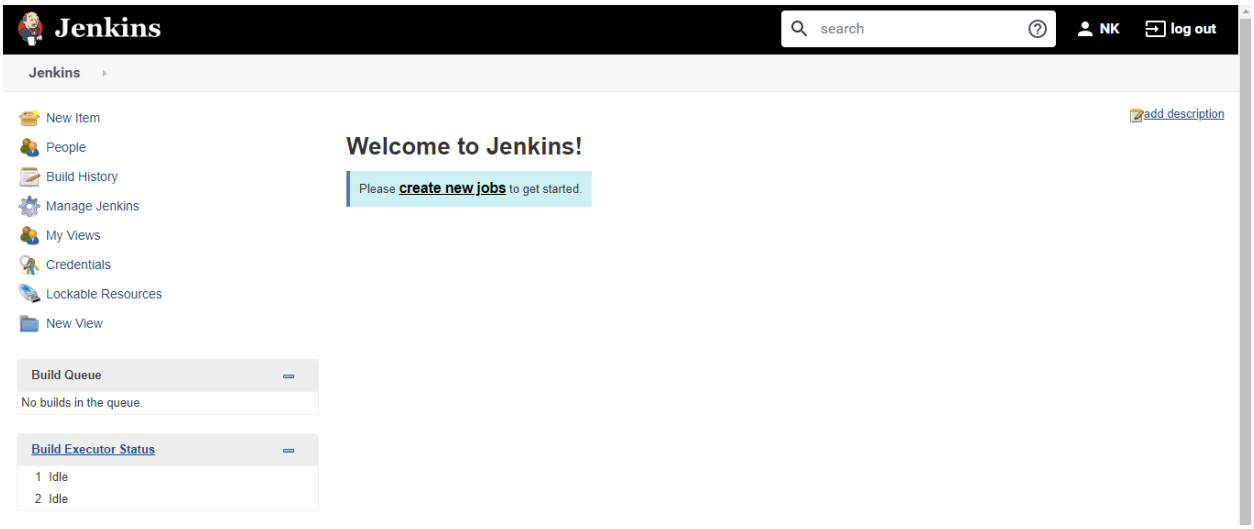


Username: admin

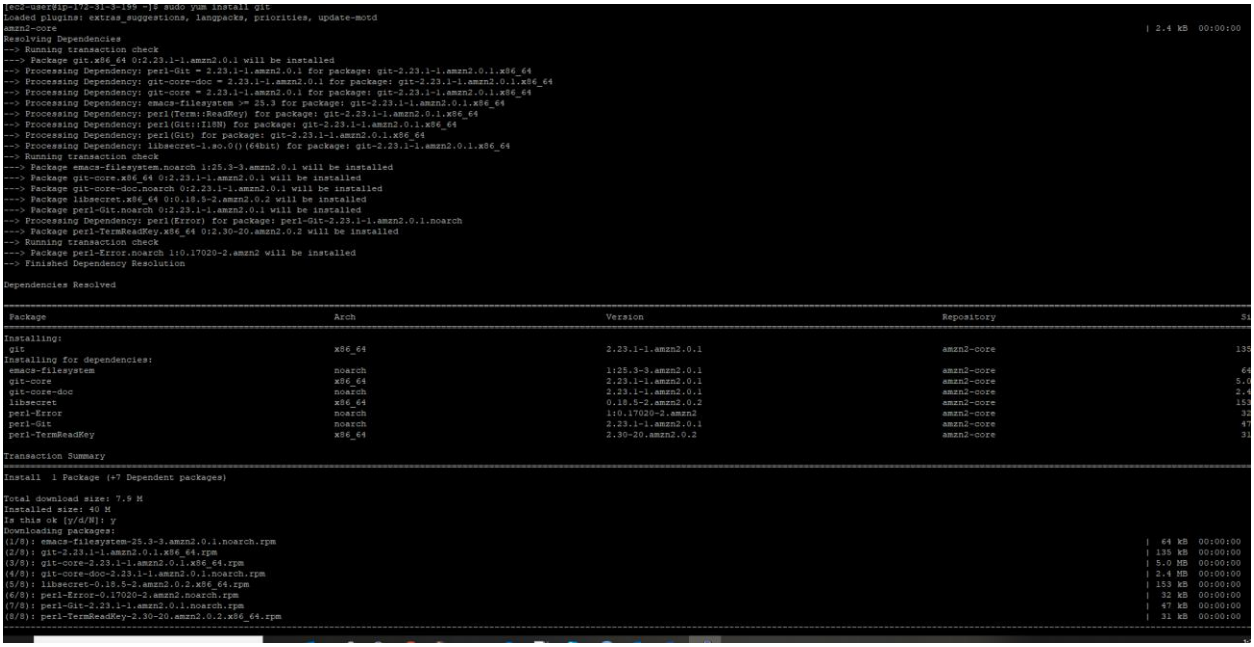
Password: Password







sudo yum install git



Create another Instance:

Open Putty and get the latest Hugo release

wget https://github.com/gohugoio/hugo/releases/download/v0.67.0/hugo_0.67.0_Linux-32bit.tar.gz

tar xzvf hugo_0.67.0_Linux-32bit.tar.gz

Manage Genkins -> Manage PlugIns

Search Git in Filter Option