CLOUD CONCEPTS (IAM AND EC2)

- Amazon is a giant amongst Cloud Service Providers. It provide various web services that can be used for different purposes with **pay-as-you-go** model. Based on global infrastructure the globe is divided in multiple regions with each region having its availibilty zone i.e. a physical data centre. Minimum 2 to 3 AZ must be present in a region. Say a region name is *regioneast1* the AZs in that region will foloow the naming convention as *regioneast1a, regioneast1b, … .*
- Services are global and region specific e.g., IAM is a global service while EC2 is not a global service. If a golabl service is luanched it does not require region selection but if a service that is not global then region selection is important. For example if a server is launched in Sydney and database is in North Virginia then to update the databse we must select North Virginia while for server Sydney as a region must be selected.

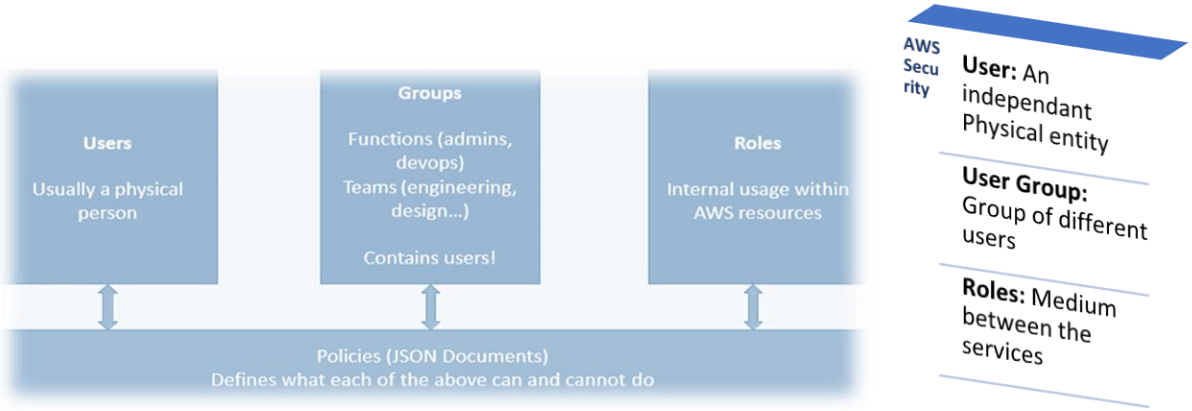
IAM (Identity Access and Management)

- It is a global service and is a center for AWS services. It allows you to create multiple users, user group and policies according to the requirement or need of any production environment or deployment. IAM has predefined policies, but new policies can be created. The format of policies is JSON. Permissions are governed by policies It is highly recommended to create an IAM user to access the services of amazon. Root user must not be used to access the services of amazon but to create other users. Credentials in either case must not be shared with anyone.
    - **Root user:** A super user account created with credit card information.
    - **IAM User:** created by super user.

Least Privilege principal: Give users minimal number of permissions they need to perform their jobs.

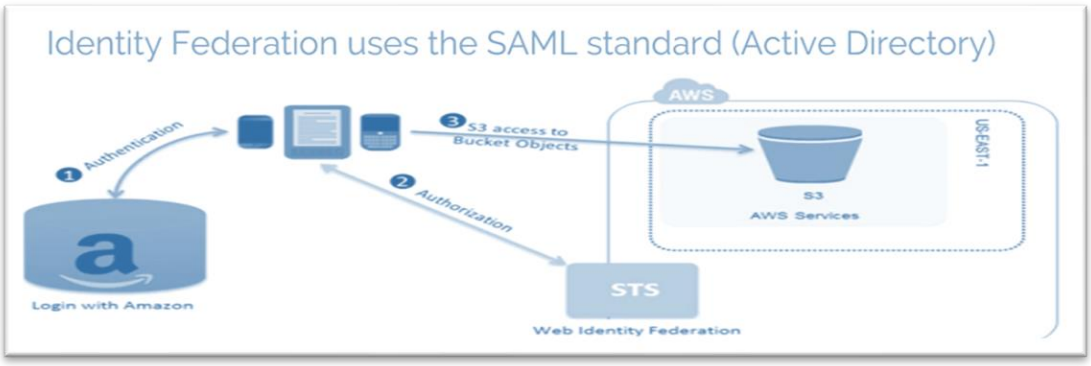
You must create your IAM account with administrative rights to use the services of Amazon.

Multi factor Authentication is recommended (can be enabled by root user).



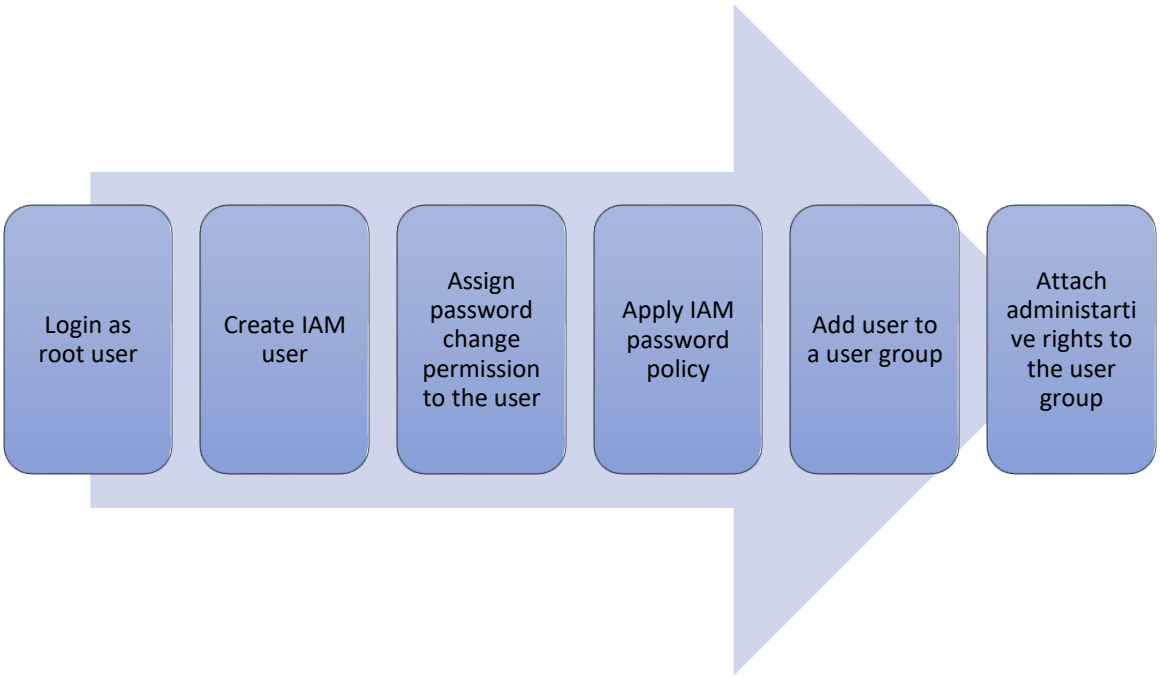
- A user U1 created in group A having permissions A1 will have the permissions A1 by default. A user U1 in group A with a permission U1_1 will not be attached with another user U2 in group A.
- *Say* if a server and a database is to be linked, only one role must be defined. Multiple roles are not possible. If new role is created for existing scenario previous role will be overwritten by the new one.

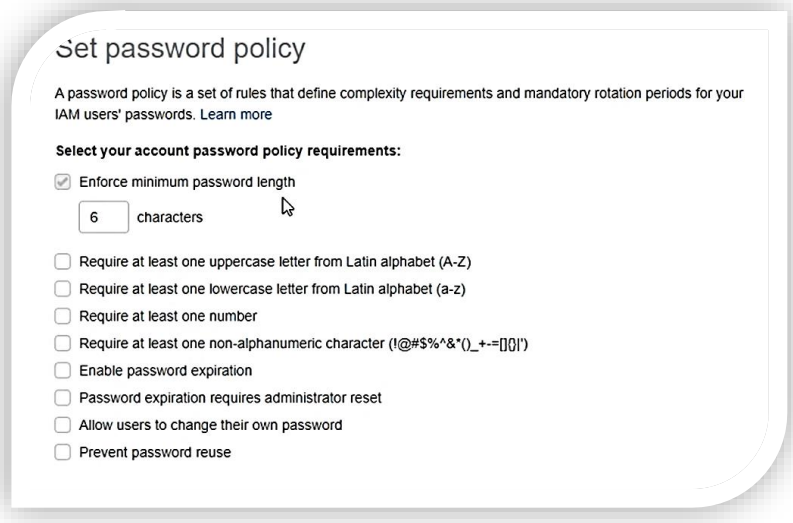
- IAM provide **IAM Federation** which allows big enterprise or organization with hundreds of employees to access amazon services using their organization credentials.
    - They integrate their own repository of users with IAM, hence employees can login to AWS using their organizational credentials. *(Why? It is very difficult to create IAM accounts for all the employees to access the services.)*



- It is just like we use to access any website using our google credentials (i.e., sign in/sign up through Google or Facebook or LinkedIn).

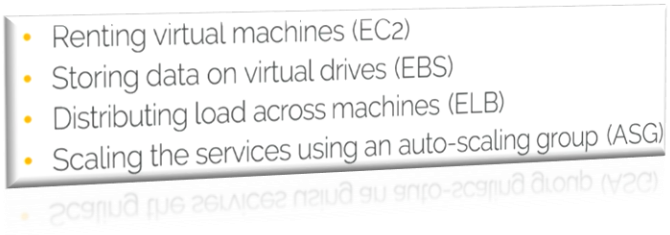
TASK: *(ignore if executed in previous sessions, just check how to set password policy)*

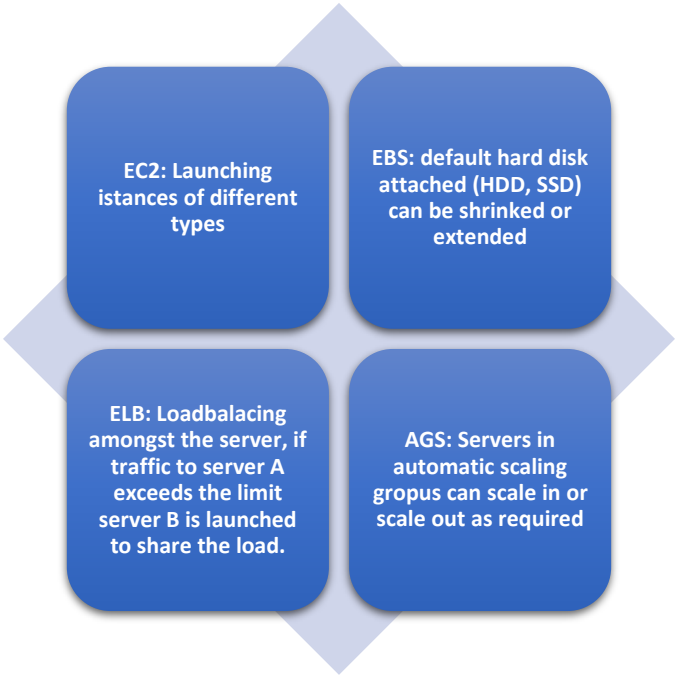




EC2 (Elastic Compute)

- EC2 is the most popular service used across the globe. Netflix pays about 90 million dollars to amazon just for this service. It allows you to launch instances of different types by renting virtual machines, providing storage on virtual drives, load balancing amongst the servers and auto scaling.

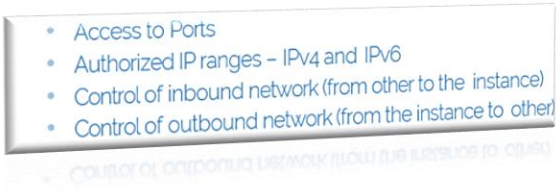




- Each module can be modified after the server launch or with the running server, but it is recommended to stop the running server and reboot or restart after updating or any modifications.
    - Cloud watch is used to monitor the settings and can generate alarms when required.
    - Traffic is increased than usual launch a new server and route the traffic for load balancing else server may get down.
    - Launch server to route type B traffic to other server while continuing type A traffic on first server.
    - Scale In (add the server) from the AGS after certain trigger.
    - Scale out (remove the server) from AGS after certain trigger.
    - Increase the volume size if more data is to be stored.
    - Create a new volume for running instance.
    - *Etc.*

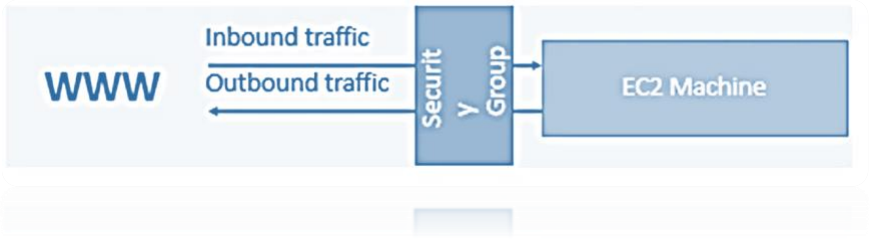
- SSH is most important function that allows to control a remote machine through command line. It basically allows to access a server through a local machine (remote login) through a secure connection. If any app in the server is causing a problem, you can easily get into the server to see the problem from your local computer. You can use command line, MAC terminal or power shell or any software like *putty* (windows only).
- Port associated with SSH is 22.
    - OPEN SSH port must be used to access the server through.

❖ **Security Group** is the fundamental of network security in AWS and control how traffic is allowed in and out of EC2 machines. They act as firewall on EC2 instances.

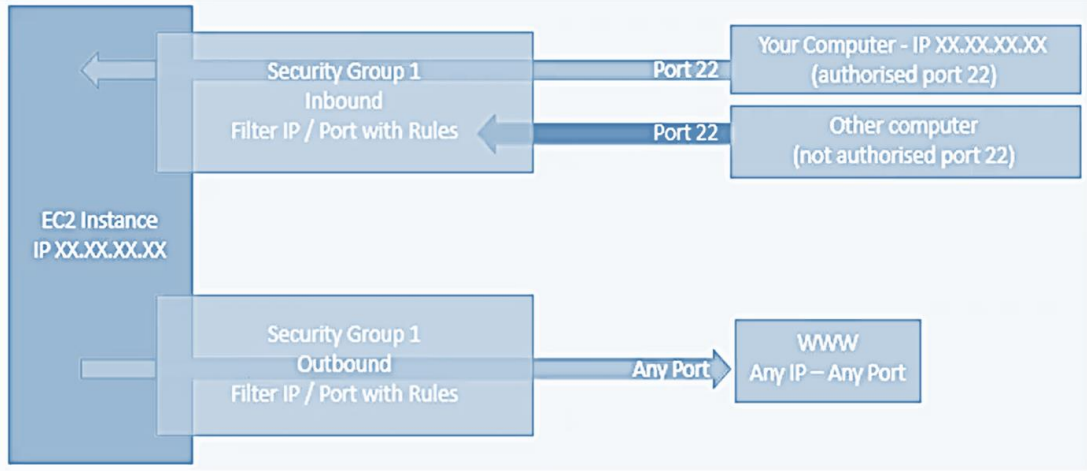


Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	test http page
SSH	TCP	22	122.149.196.85/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app

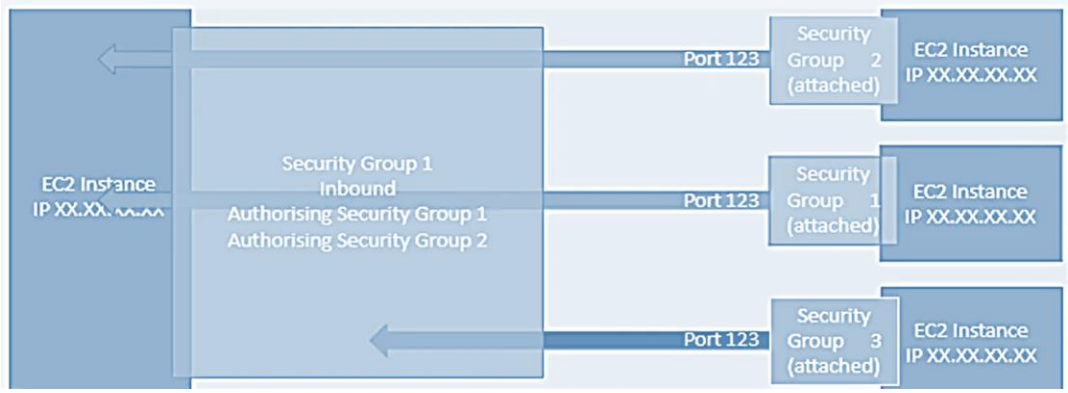
1. Type HTTP: All type of traffic is allowed.
2. Type SSH: Only my IP is allowed.
3. Type Custom TCP Rule: All type of traffic is allowed.



* Public traffic can enter or leave the server depending attached SG.



* In Scenario above your system with authorized port is allowed to access the EC2 instance while any other system with unauthorized port will not be able to access the EC2 instance. In case of outbound any type of traffic from any port is allowed to leave the server.



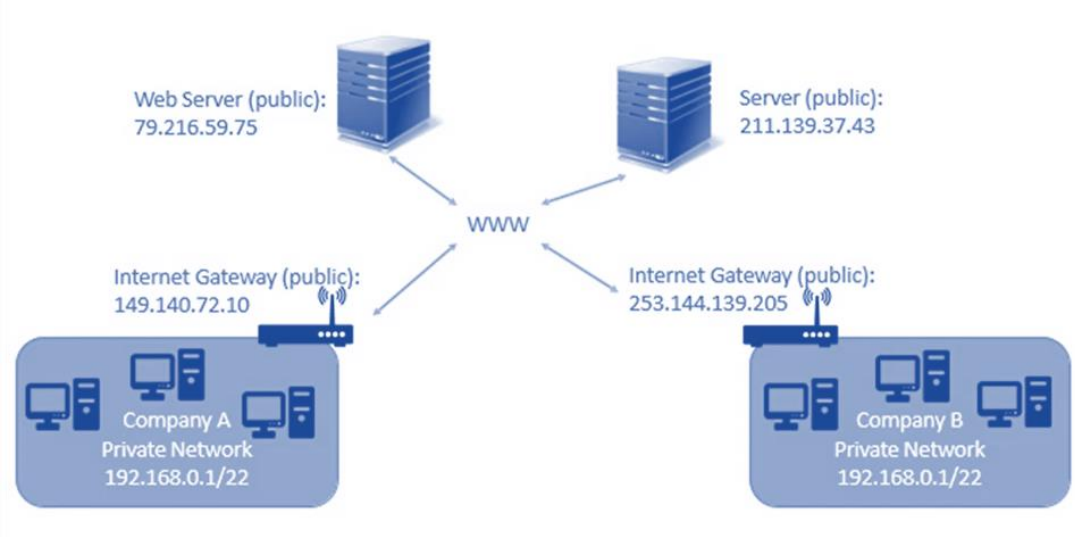
* In this scenario the instances with SG1 or SG2 can only access the server with SG1 and SG2, the instance with different SG (SG3) cannot access the server.

- Locked down to a region / VPC combination
- Does live "outside" the EC2 – if traffic is blocked the EC2 instance won't see it
- It's good to maintain one separate security group for SSH access

Private vs Public IP (IPv4)

- Networking has two sorts of IPs. IPv4 and IPv6
  - IPv4: **1.160.10.240**
  - IPv6: 3ffe: **1900:4545:3:200:f8ff:fe21:67cf**

- IPv4 is still the most common format used online.
- IPv6 is newer and solves problems for the Internet of Things (IoT).
- IPv4 allows for 3.7 billion different addresses in the public space
- IPv4: [0-255].[0-255].[0-255].[0-255].



* In this scenario the Company A and Company B has their private network while they are accessing the servers with a public IP. Here Internet gateway is used as proxy as public internet is not accessible through private IPs.

- Private IP means the machine can only be identified on a private network only
- The IP must be unique across the private network
- BUT two different private networks (two companies) can have the same IPs.
- Machines connect to WWW using an internet gateway (a proxy)
- Only a specified range of IPs can be used as private IP

- Public IP means the machine can be identified on the internet (WWW)
- Must be unique across the whole web (not two machines can have the same public IP).
- Can be geo-located easily

- With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- You can only have 5 Elastic IP in your account (you can ask AWS to increase that).

- Elastic IP can be attached with one instance only. Only one server instance can be given elastic IP. Five elastic IPs in your account are allowed extension can be requested. If any EP is reserved, it will be charged.

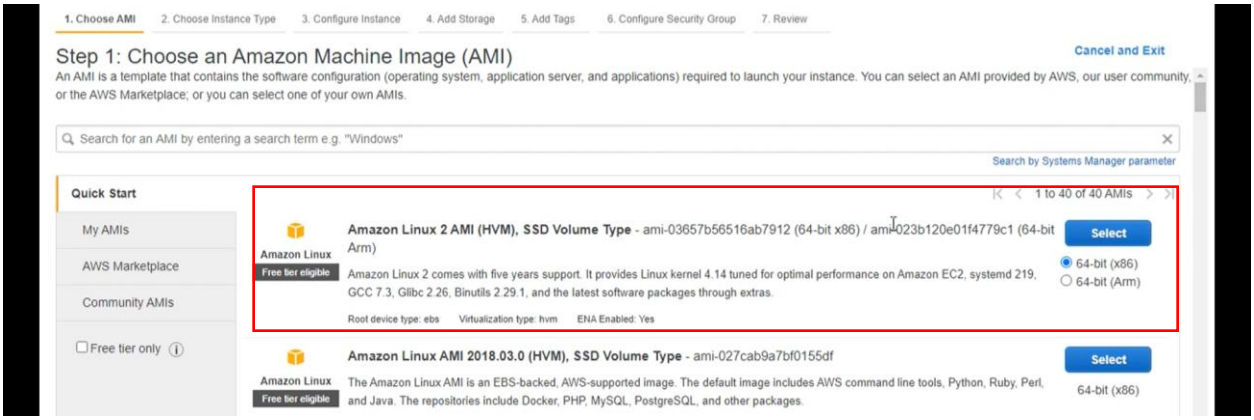
Key Notes:

Key pair is used to access the server. It is the type of credentials required to access the server. If the file is lost server will be launched but the access is not possible.
When ever server is rebooted the assigned public IP is changed. In production environment this IP must be changed where ever it is mentioned. To avoid this overhead Elastic IP is used.
Bidding based instances are spot instances.
Copy of server (instance) is AMI.
Copy of hard disk (volume) is Snapshot.
Inbound traffic means traffic coming towards the server.
Outbound traffic means traffic moving out of the server.
Outbout traffic is allowed by default while inbound is defined explicitly.
All in bound traffic is blocked by default and all out bound traffic is allowed by default.
Rules defines the type of traffic comingtowards or leaving the server.
One security group can be attached with multipe instances.
One server can have multiple security groups.
If there is **timeout problem** it is related to the security group while **connection refused** error means server is not launched properly.

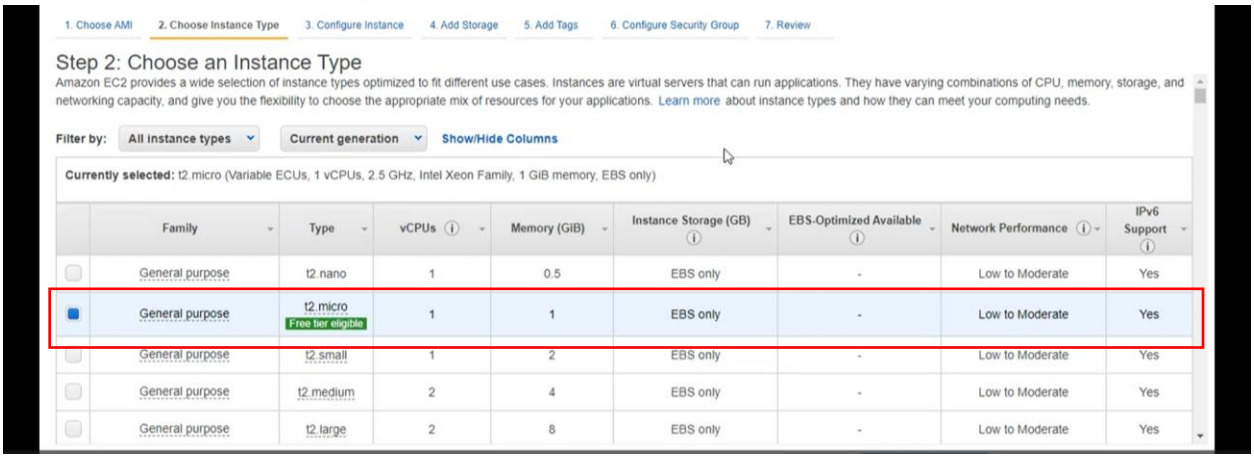
Launching an EC2 instance running on Linux and SSH into EC2 instance through command line (Linux/MacOS/Windows (*putty*)):

We have already launched a window server; similar steps will be followed.

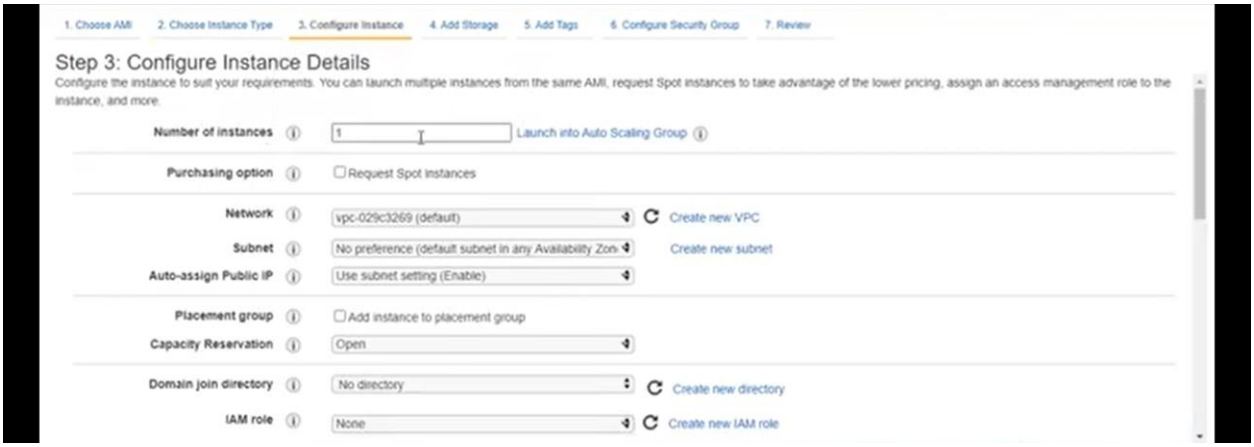
- Choose Amazon Linux 2 AMI (free tier).



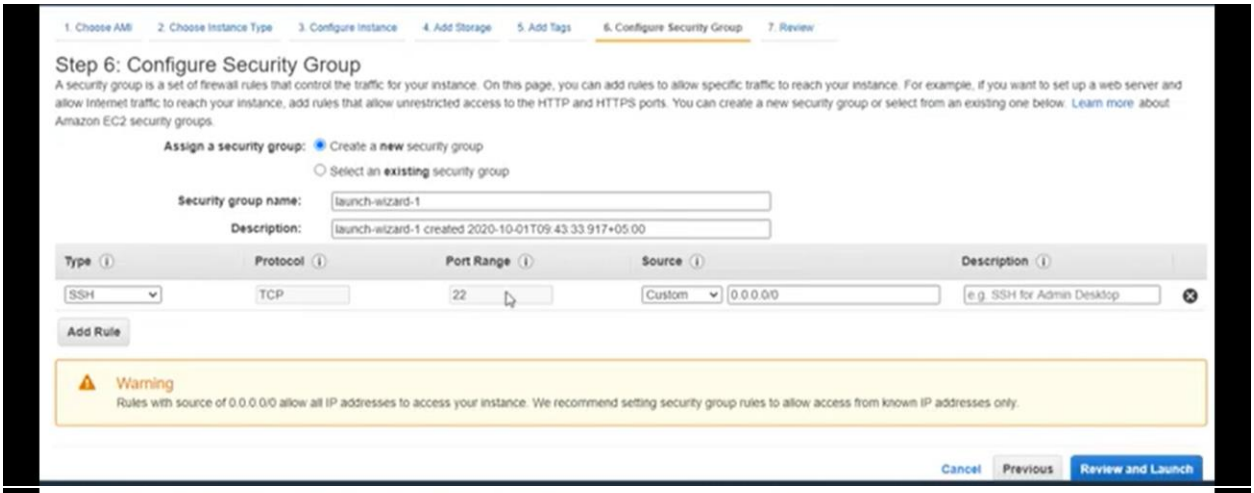
- Choose instance type.
  - Recommended for Testing purpose i.e., General purpose.
  - EBS is 8GB by default (Can be extended and type can be changed HDD to SSD and vice versa).

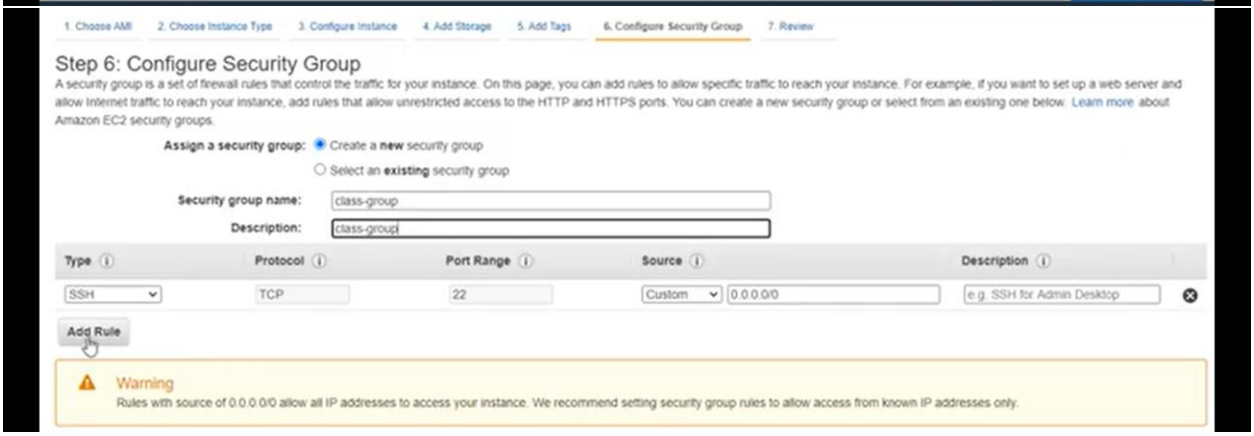


- Configuration:
  - No of instances = no of servers launched.
  - Subnet can be selected (else default) Subnet is one AZ.
  - IAM role can be attached.
  - Tagging is optional.
  - Default storage.

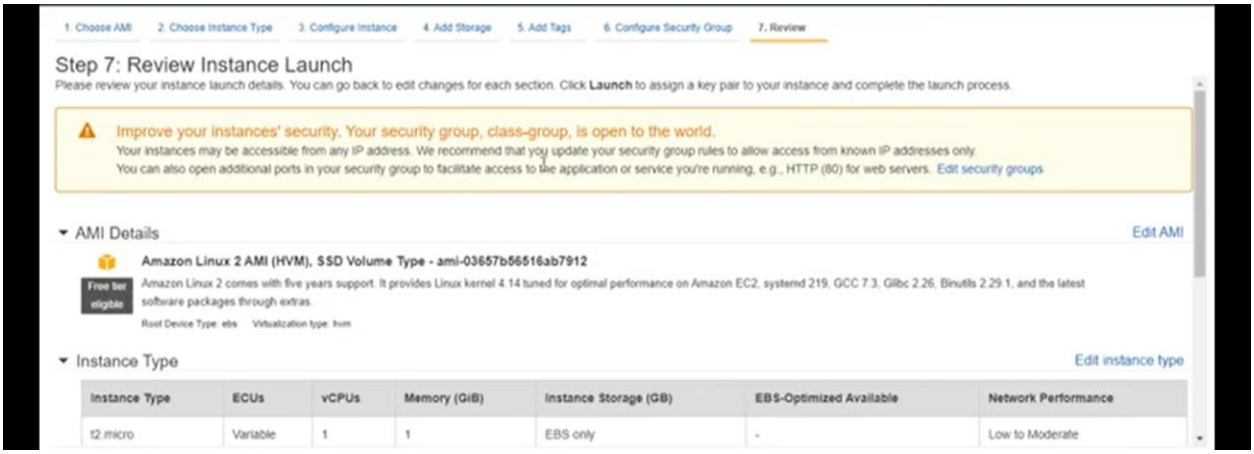


- Attach security groups.
    - Use existing SG.
    - Create a new SG.
        - Default SSH port is ON.
        - New rules can be added.



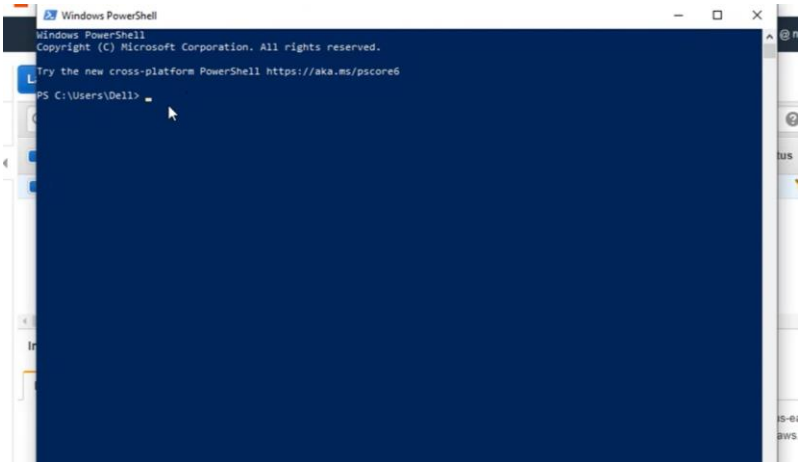


- Review and launch the instance.

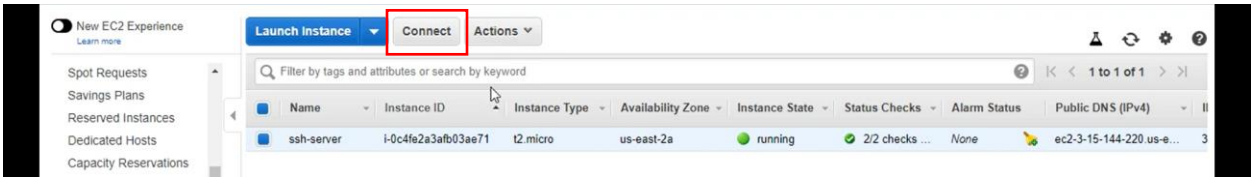


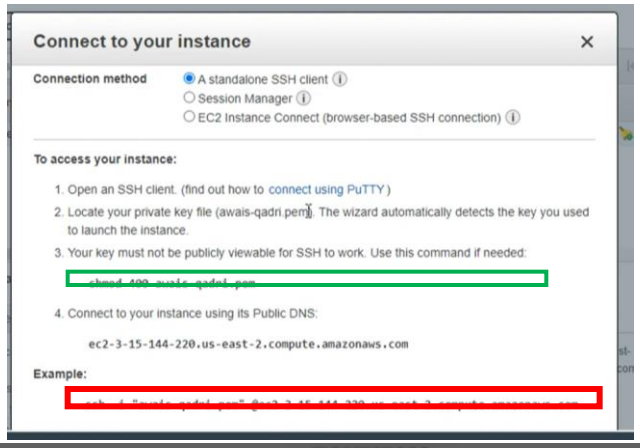
- ❖ Keep your key pair saved. *If the key pair is lost SSH will not be possible, but server will be launched.*
- ❖ Default key pair file extension is. *pem.* This file is required for accessing the server through MAC OS, Linux, or windows power shell. For *putty software* (on windows) *.ppk* file is required. (*.pem* file is converted to. *ppk* by putty)

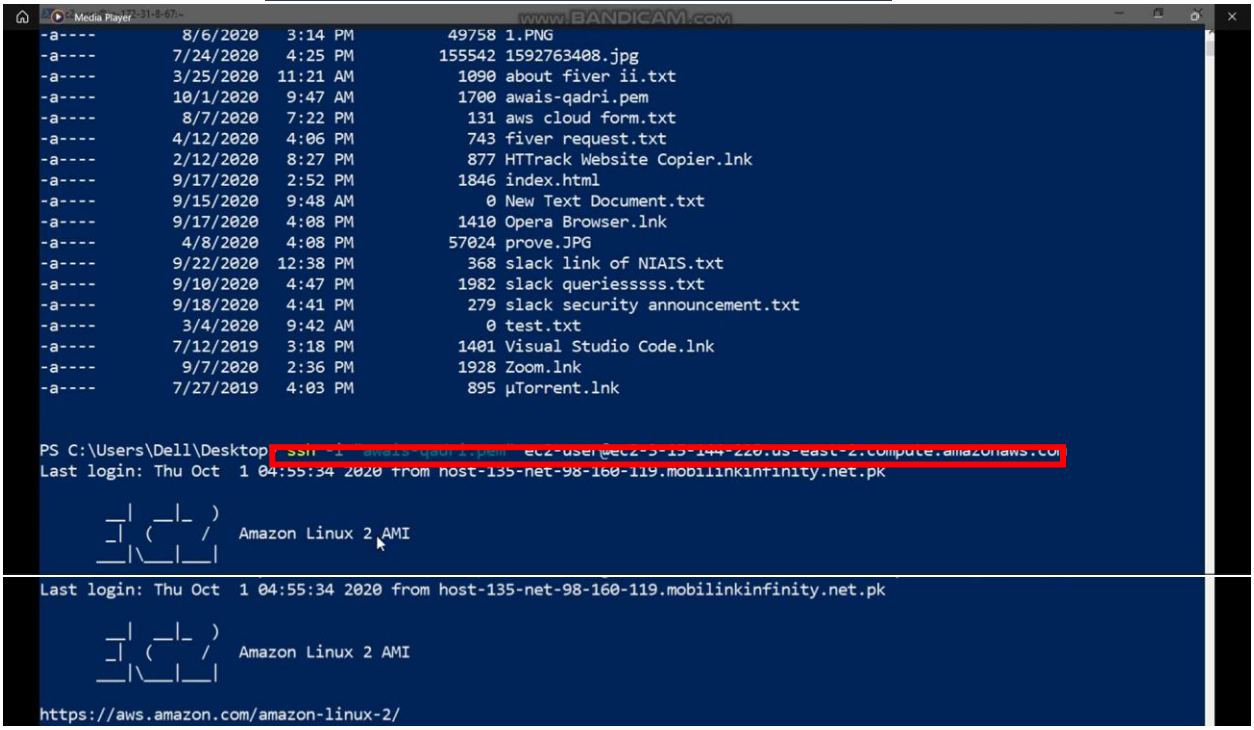
- Launch windows **power shell.**



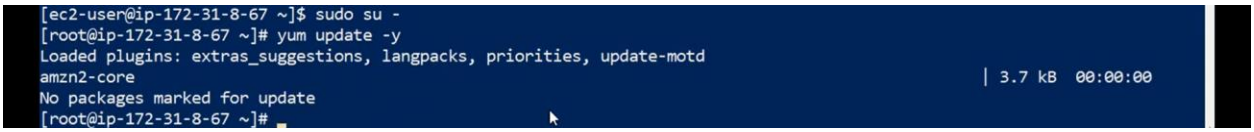
- Enter the following commands:
    1. cd (to change directory) -> move to the folder where *.pem* file is saved.
    2. ls (to list all the files in that folder) -> to see the *.pem* file.
- Write a new command or simply go to dashboard and click connect and copy the command and paste it in power shell.
    - Same commands are used in linux for mac OS chmod permission is required.







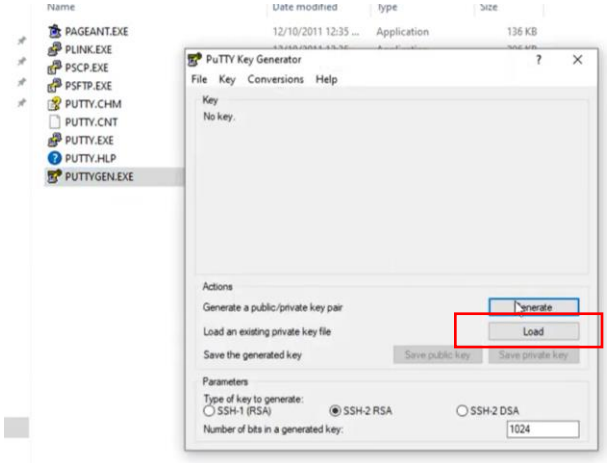
- Enter the following commands:
    - sudo su (sudo means administrator access and su is super user) -> make you root user.
    - yum update -y (update the packages, and -y flag means yes to all options)

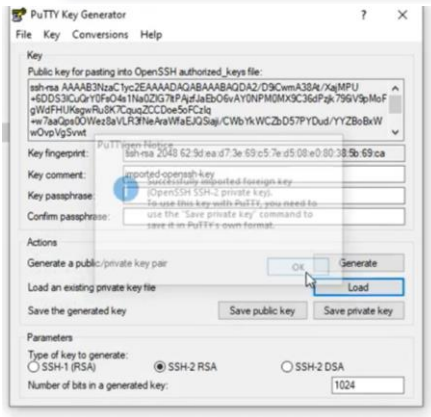


```
Last login: Thu Oct  1 04:55:34 2020 from host-135-net-98-160-119.mobilinkinfinity.net.pk

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI <- Your AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/  <- Your AMI url
[ec2-user@ip-172-31-8-67 ~]$ sudo su -
[root@ip-172-31-8-67 ~]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                               | 3.7 kB  00:00:00
No packages marked for update
[root@ip-172-31-8-67 ~]# exit
logout                    <- logged out as root user.
[ec2-user@ip-172-31-8-67 ~]$
```

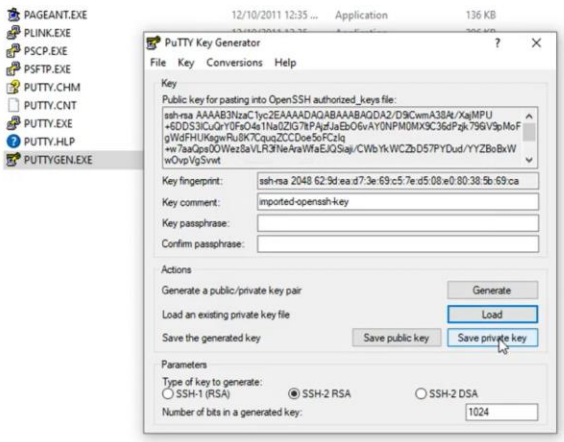
user @ public ip or server

- **Through putty:**
    - Use Puttygen.exe to convert pem to ppk.
    - Click on load and browse the file.

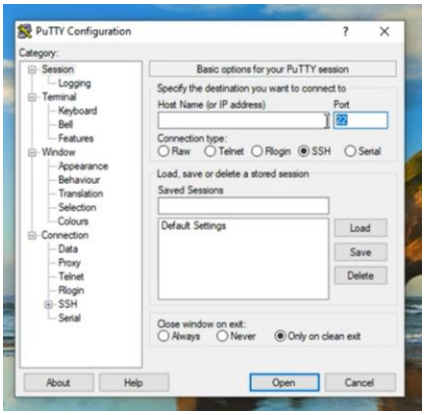




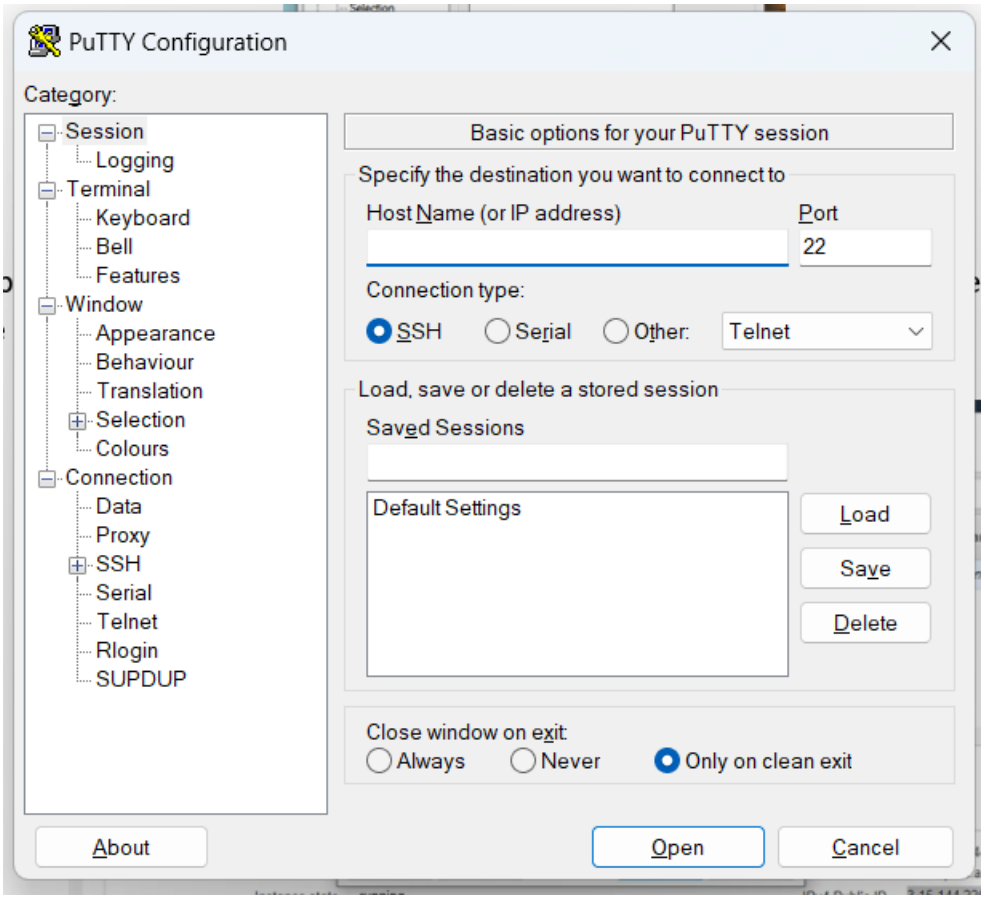
- Click on save private key. Keep the file name same for .ppk as of .pem. it will be easily locatable.

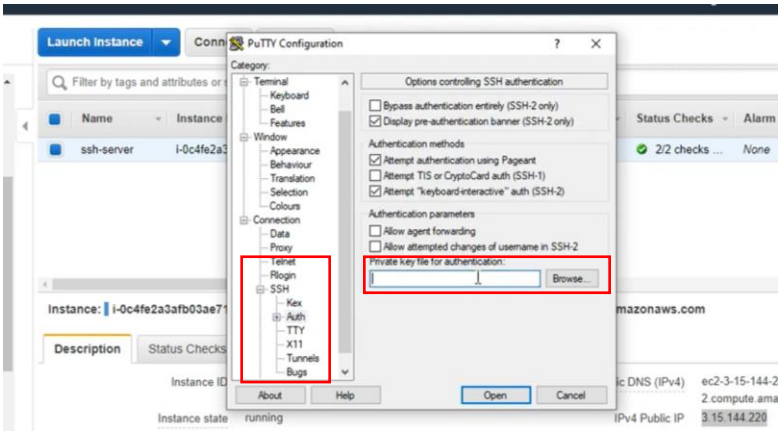


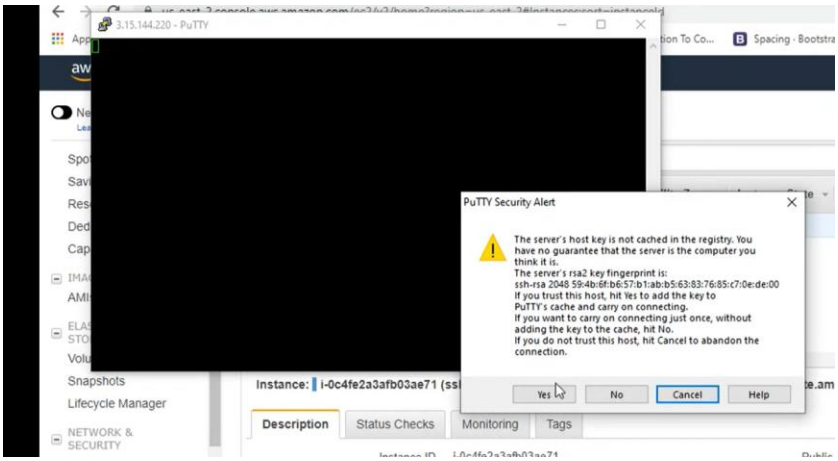
- Run the putty software. Default port 22 must be there.



- Copy the public IP of server and paste it. Click on auth in ssh on the side bar and browse the .ppk file.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel


Launch Instance
PuTTY Configuration
Category:
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:
Browse...
Name
Instance
Status Checks
Alarm
ssh-server
2/2 checks ...
None
Description
Status Checks
About
Help
Open
Cancel



- Access server through putty.