Amazon Web Services

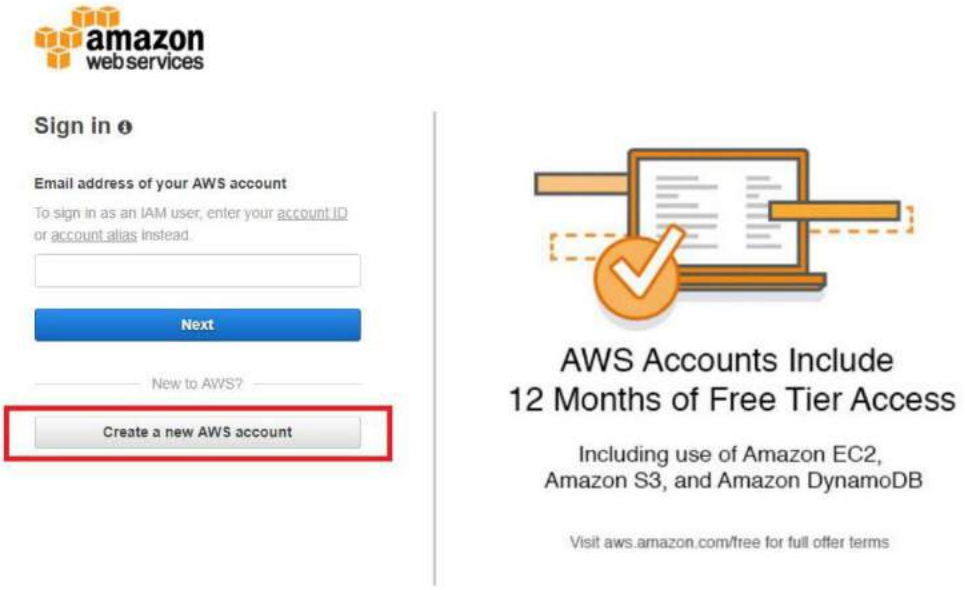
AWS Syllabus:

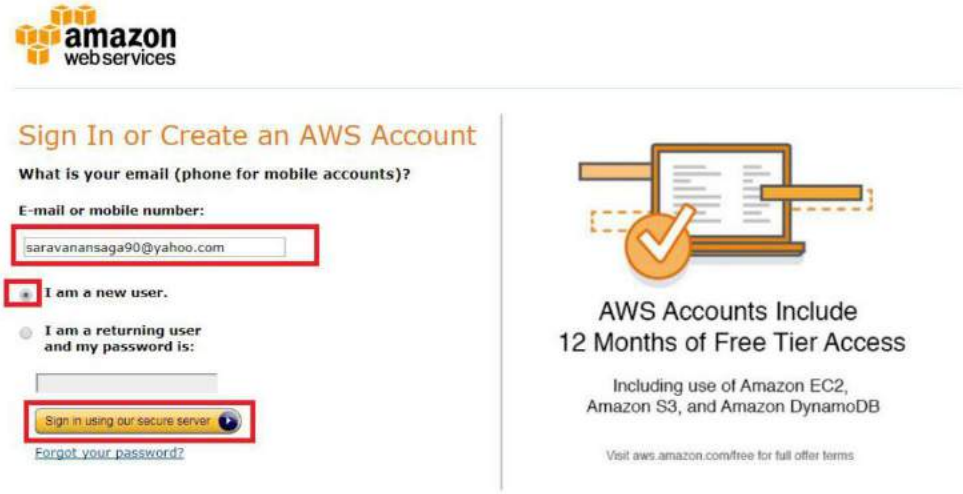
- Account Creation
- Cloud Computing
- Basic Linux Commands
- Installation and Initialization
- Boot and Package Management
- User Administration
- Service Protocols
- Virtualization
- AWS Overview
- Amazon EC2
- Amazon VPC
- Amazon Elastic Block Store (EBS)
- Amazon ELB
- Auto Scaling
- Amazon Route 53
- Amazon Simple Storage Service (S3) & Glacier
- Amazon Content Delivery Network (Cloud Front)
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon DynamoDB
- Amazon ElastiCache
- Elastic Beanstalk
- Lambda
- Security Management (Trusted Advisor)
- Amazon Simple Notification Service (SNS)
- Management Tools (Cloud Trail & Cloud Watch)
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- AWS Identity and Access Management (IAM)
- Amazon Command Line Interface
- S3-Browser
- Troubleshooting
- Pricing
- Architecture Design
- Dev-Ops Fundamentals (Chef, Puppet, Ansible, ANT, Maven & GIT)

AWS Certificate dump files could be downloaded from below URL:
https://drive.google.com/file/d/1HW_rR9f7grvDymB2FEQjk-LUdioKq7bF/view?usp=sharing
And please download the User Guide which was provided by AWS from below URL.
https://drive.google.com/file/d/13Dz5SwgzA-bxJyHXZPvEJjiYU8-4ildv/view?usp=sharing

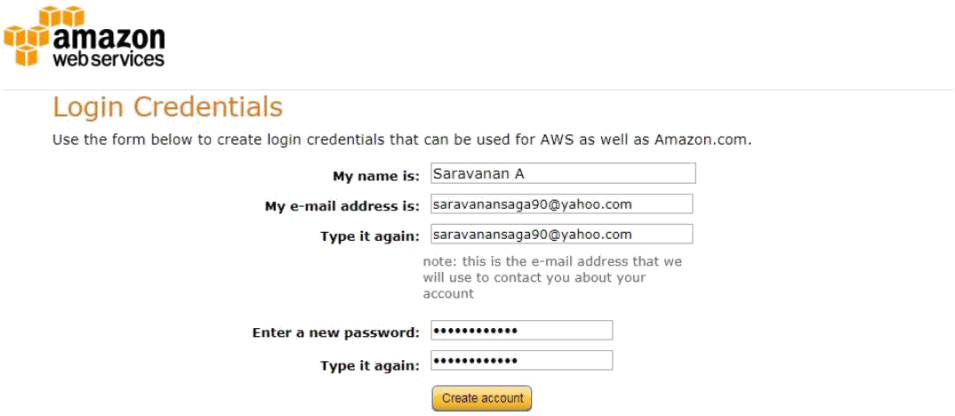
AWS Account Creation:

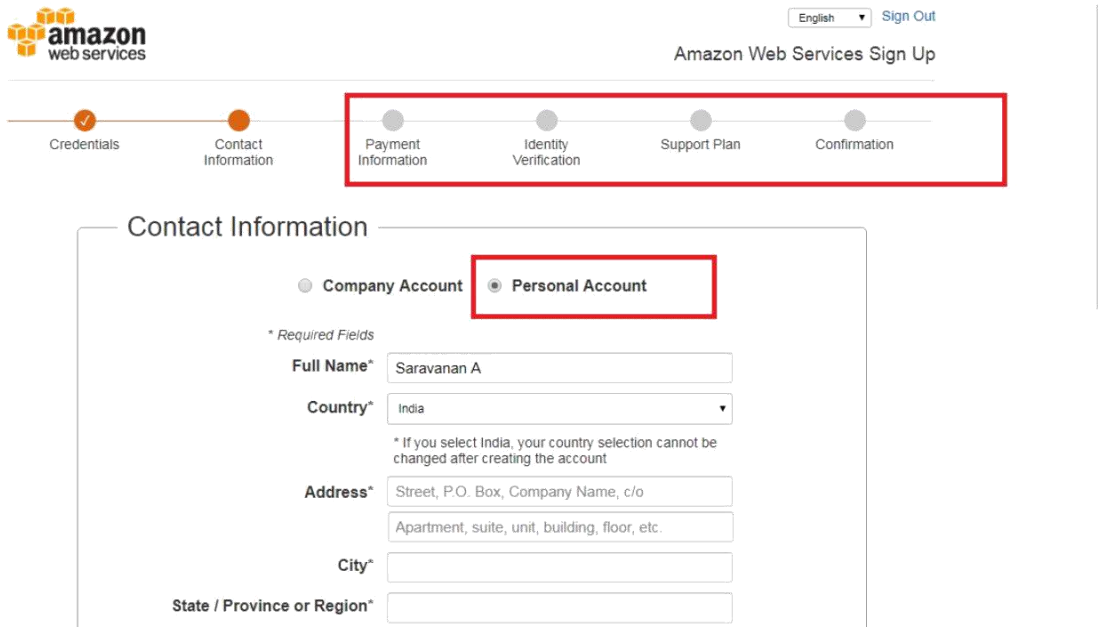
- Click on below given URL to create a new AWS Account.
  https://signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fportal.aws.amazon.com%2Fbilling%2Fsignup%3Fredirect_url%3Dhttps%253A%252F%252Faws.amazon.com%252Fregistrati on-confirmation%26state%3DhashArgs%2523%26isauthcode%3Dtrue&client_id=arn%3Aaws%3Aiam%3A%3A015428540659%3Auser%2Fawssignupportal&forceMobileApp=0
- Provide the necessary information as like below screenshot for creating a new account.





- After providing Contact information, provide Debit / Credit Card Information in Payment Information tab.
- On 4th Step, Identity Verification needs to be carried out by typing PIN on your mobile after receiving a call from AWS.
- Choose the Support Plan as Basic and Click to proceed further.
- Sometimes, Account registration would take 24 hours of time and 2Rs INR would be deducted from your bank and it would be credited back to your account.





Cloud Computing:

- Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, like a public utility.

- Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance. Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand. Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.

IaaS (Infrastructure As A Service)

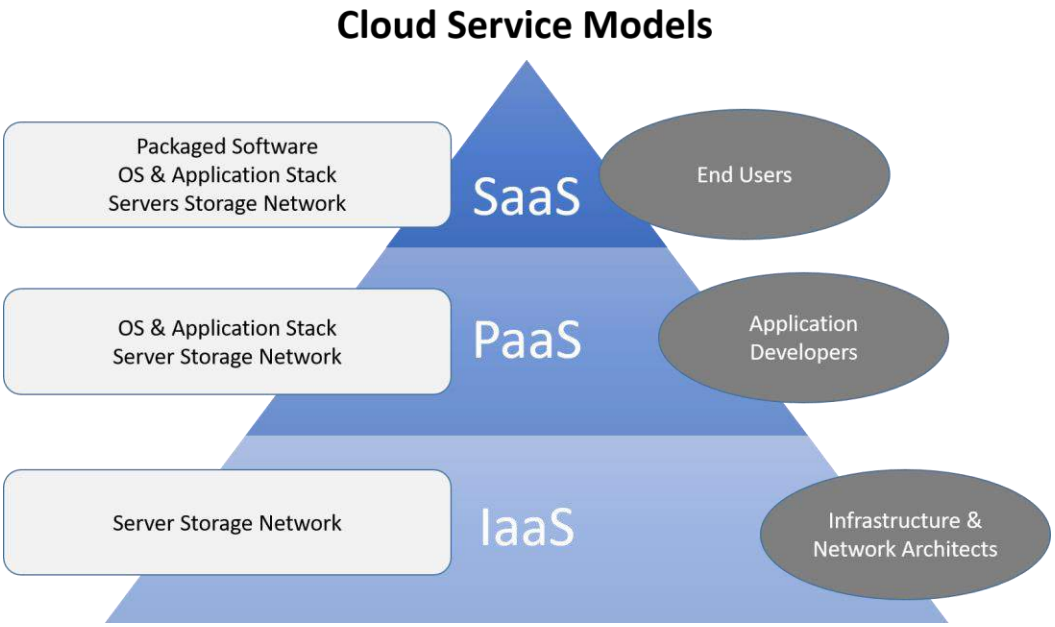
- "Infrastructure as a service" (IaaS) refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, LXD, runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.

PaaS (Platform As A Service):

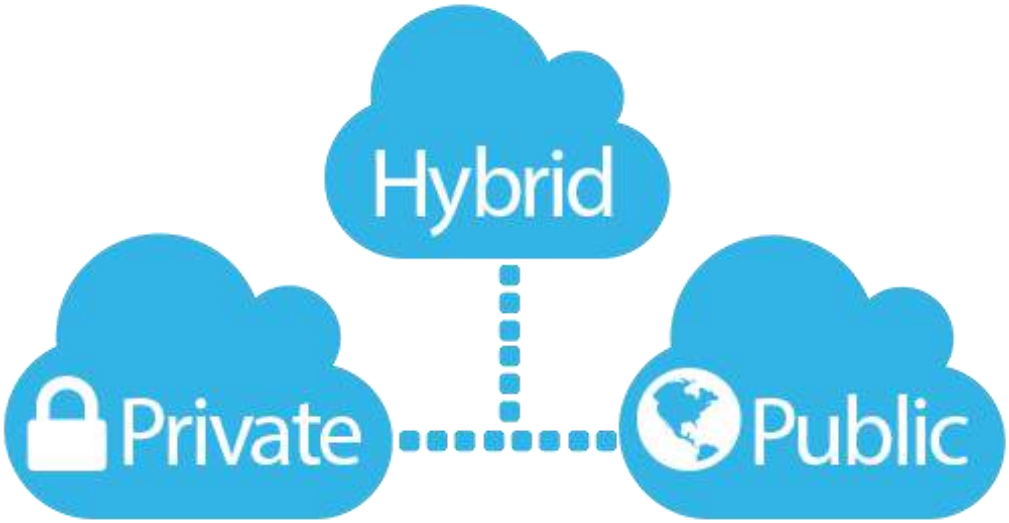
- PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

SaaS (Software As A Service):

- In the software as a service (SaaS) model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs.



Types of Cloud:



Public Cloud:

- A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is affected over a non-trusted network.

Private Cloud:

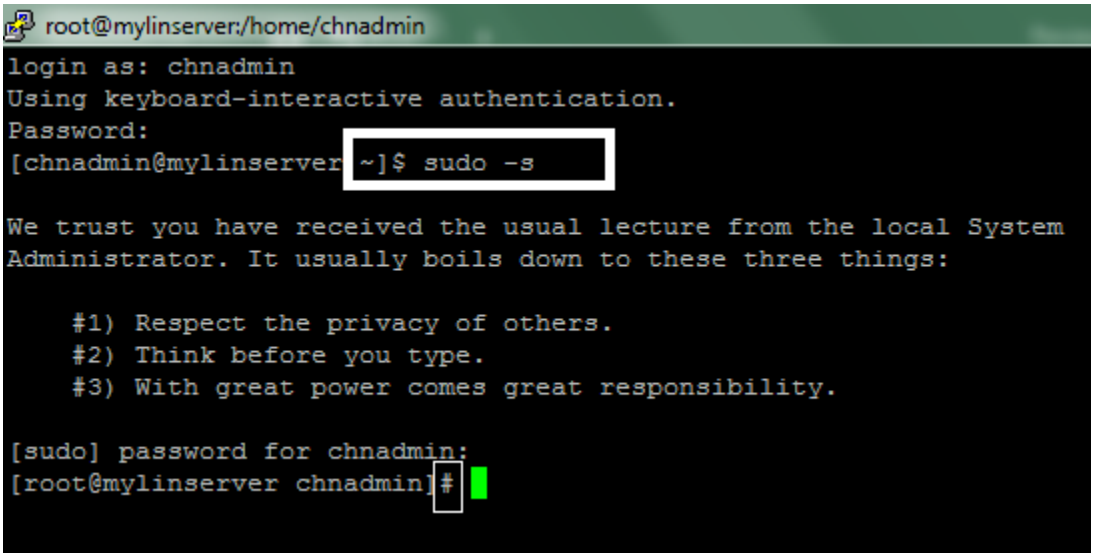
- Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Undertaking a private cloud project requires significant engagement to virtualize the business environment and requires the organization to reevaluate decisions about existing resources.

Hybrid Cloud:

- Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Gartner defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers.

Linux Basic Commands:

- We need to use Putty / WinSCP / VNC viewer to connect a SSH of Linux environments. Please find the below basic commands which could be used for your reference.
- To get into Sudo / Root User,
- **'sudo -s'**



- To check the available disk size,
- **'df -h'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2        32G  2.2G   30G   7% /
devtmpfs        2.0G     0  2.0G   0% /dev
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           2.0G  8.4M  2.0G   1% /run
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/sda1       497M  117M  381M  24% /boot
/dev/sdb1       7.8G  2.1G  5.3G  28% /mnt/resource
tmpfs           394M     0  394M   0% /run/user/0
tmpfs           394M     0  394M   0% /run/user/1000
[root@mylinserver chnadmin]#
```

- To see free RAM Size,
- **'free -m'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# free -m
              total        used        free      shared  buff/cache   available
Mem:           3936         201        3453           8         281        3468
Swap:          2047           0        2047
[root@mylinserver chnadmin]#
```

- To see in which location you are,
- **'pwd'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# pwd
/home/chnadmin
[root@mylinserver chnadmin]#
```

- To create a new folder,
- **'mkdir <foldername>'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# mkdir sample
[root@mylinserver chnadmin]#
```

- To View the folder / files,
- **'ls'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# mkdir sample
[root@mylinserver chnadmin]# ls
sample
[root@mylinserver chnadmin]#
```

- To view the files and folders in a detailed view,
- **'ls -l'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# mkdir sample
[root@mylinserver chnadmin]# ls
sample
[root@mylinserver chnadmin]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 14:37 sample
[root@mylinserver chnadmin]#
```

- To delete the folder/file,
- **'rm -rf <folder/file name>'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 14:40 sample
[root@mylinserver chnadmin]# rm -rf sample/
[root@mylinserver chnadmin]# ls -l
total 0
[root@mylinserver chnadmin]#
```

- To copy the file / folder along with permissions,
- **'cp -avr /<source folder> /<target location>'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample1
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample12
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample123
[root@mylinserver chnadmin]# cp -avr sample sample1 sample12 sample123/ /home/
'sample' -> '/home/sample'
'sample1' -> '/home/sample1'
'sample12' -> '/home/sample12'
'sample123/' -> '/home/sample123'
[root@mylinserver chnadmin]#
```

- To go back previous folder,
- **'cd ..'**

```
root@mylinserver:/home
[root@mylinserver chnadmin]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample1
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample12
drwxr-xr-x. 2 root root 6 Feb 27 14:42 sample123
[root@mylinserver chnadmin]# cp -avr sample sample1 sample12 sample123/ /home/
'sample' -> '/home/sample'
'sample1' -> '/home/sample1'
'sample12' -> '/home/sample12'
'sample123/' -> '/home/sample123'
[root@mylinserver chnadmin]# cd ..
[root@mylinserver home]# ls -l
total 0
drwx------. 8 chnadmin chnadmin 153 Feb 27 14:42 chnadmin
drwxr-xr-x. 2 root     root       6 Feb 27 14:42 sample
drwxr-xr-x. 2 root     root       6 Feb 27 14:42 sample1
drwxr-xr-x. 2 root     root       6 Feb 27 14:42 sample12
drwxr-xr-x. 2 root     root       6 Feb 27 14:42 sample123
[root@mylinserver home]#
```

- To go any file / folder location,
- **'cd /<Target Location'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver home]# cd chnadmin/
[root@mylinserver chnadmin]#
```

- To rename the file / folder,
- **'mv <old file/folder name> <new file/folder name>'**

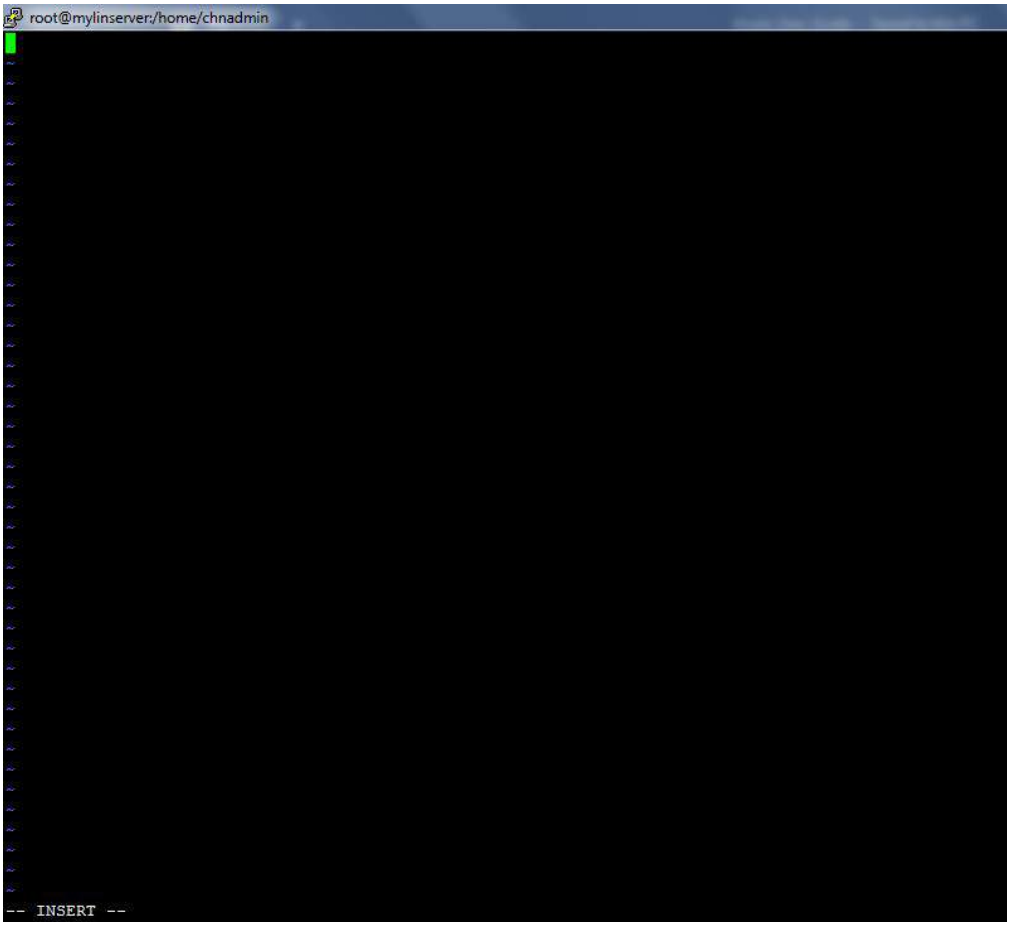
```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls
samplesss
[root@mylinserver chnadmin]# mv samplesss/ sample
[root@mylinserver chnadmin]# ls
sample
[root@mylinserver chnadmin]#
```

- To move the file / folder to different location,
- **'mv <source file / folder> /<target location>'**

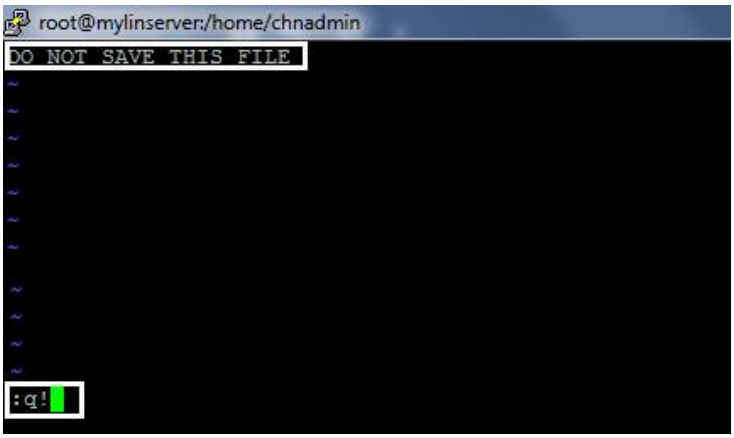
```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls
sample
[root@mylinserver chnadmin]# mv sample/ /home/
[root@mylinserver chnadmin]# ls
[root@mylinserver chnadmin]#
```

- To create a new text file,
- **'vi sample.txt'**

- File will be opened, to type something,
- **'I'**

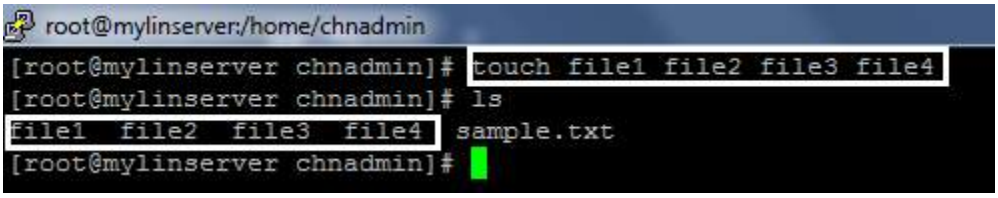


- If you do not want to save this text file,
- **'ESC** + **:q!**



- If you want to save this text file,
- **'ESC + :wq'**

- To create number of text files in a single command,
- **'touch file1 file2 file3 file4'**



- To install any inbuilt tools or software,
- **'yum install <file / software name> -y'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# yum install java -y
Loaded plugins: langpacks, product-id, search-disabled-repos
Resolving Dependencies
--> Running transaction check
---> Package java-1.8.0-ibm.x86_64 1:1.8.0.5.10-1jpp.1.el7 will be installed
--> Processing Dependency: jpackage-utils >= 1.5.38 for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Processing Dependency: libXext.so.6()(64bit) for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Processing Dependency: libXft.so.2()(64bit) for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Processing Dependency: libXi.so.6()(64bit) for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Processing Dependency: libXrender.so.1()(64bit) for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Processing Dependency: libXtst.so.6()(64bit) for package: 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64
--> Running transaction check
---> Package javapackages-tools.noarch 0:3.4.1-11.el7 will be installed
--> Processing Dependency: python-javapackages = 3.4.1-11.el7 for package: javapackages-tools-3.4.1-11.el7.noarch
---> Package libXext.x86_64 0:1.3.3-3.el7 will be installed
---> Package libXft.x86_64 0:2.3.2-2.el7 will be installed
--> Processing Dependency: fontconfig >= 2.2-1 for package: libXft-2.3.2-2.el7.x86_64
--> Processing Dependency: libfontconfig.so.1()(64bit) for package: libXft-2.3.2-2.el7.x86_64
---> Package libXi.x86_64 0:1.7.9-1.el7 will be installed
---> Package libXrender.x86_64 0:0.9.10-1.el7 will be installed
---> Package libXtst.x86_64 0:1.2.3-1.el7 will be installed
--> Running transaction check
---> Package fontconfig.x86_64 0:2.10.95-11.el7 will be installed
--> Processing Dependency: font(:lang=en) for package: fontconfig-2.10.95-11.el7.x86_64
```

```
root@mylinserver:/home/chnadmin
(9/11): python-javapackages-3.4.1-11.el7.noarch.rpm                                   |  31 kB  00:00:00
(10/11): paratype-pt-sans-caption-fonts-20101909-3.el7.noarch.rpm                     | 204 kB  00:00:00
(11/11): java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64.rpm                              | 108 MB  00:00:01
--------------------------------------------------------------------------------------------------------------
Total                                                                    78 MB/s | 109 MB  00:00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libXext-1.3.3-3.el7.x86_64                                                          1/11
  Installing : libXi-1.7.9-1.el7.x86_64                                                            2/11
  Installing : libXrender-0.9.10-1.el7.x86_64                                                      3/11
  Installing : libXtst-1.2.3-1.el7.x86_64                                                          4/11
  Installing : fontpackages-filesystem-1.44-8.el7.noarch                                           5/11
  Installing : paratype-pt-sans-caption-fonts-20101909-3.el7.noarch                                6/11
  Installing : fontconfig-2.10.95-11.el7.x86_64                                                    7/11
  Installing : libXft-2.3.2-2.el7.x86_64                                                           8/11
  Installing : python-javapackages-3.4.1-11.el7.noarch                                             9/11
  Installing : javapackages-tools-3.4.1-11.el7.noarch                                             10/11
  Installing : 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64                                      11/11
rhui-rhel-server-rhui-rhscl-7-rpms/7Server/x86_64/productid                              | 2.1 kB  00:00:00
  Verifying  : libXext-1.3.3-3.el7.x86_64                                                          1/11
  Verifying  : libXi-1.7.9-1.el7.x86_64                                                            2/11
  Verifying  : python-javapackages-3.4.1-11.el7.noarch                                             3/11
  Verifying  : libXrender-0.9.10-1.el7.x86_64                                                      4/11
  Verifying  : javapackages-tools-3.4.1-11.el7.noarch                                              5/11
  Verifying  : fontconfig-2.10.95-11.el7.x86_64                                                    6/11
  Verifying  : paratype-pt-sans-caption-fonts-20101909-3.el7.noarch                                7/11
  Verifying  : libXtst-1.2.3-1.el7.x86_64                                                          8/11
  Verifying  : libXft-2.3.2-2.el7.x86_64                                                           9/11
  Verifying  : 1:java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7.x86_64                                      10/11
  Verifying  : fontpackages-filesystem-1.44-8.el7.noarch                                          11/11

Installed:
  java-1.8.0-ibm.x86_64 1:1.8.0.5.10-1jpp.1.el7

Dependency Installed:
  fontconfig.x86_64 0:2.10.95-11.el7          fontpackages-filesystem.noarch 0:1.44-8.el7        javapackages-tools.noarch 0:3.4.1-11.el7
  libXext.x86_64 0:1.3.3-3.el7                libXft.x86_64 0:2.3.2-2.el7                        libXi.x86_64 0:1.7.9-1.el7
  libXrender.x86_64 0:0.9.10-1.el7            libXtst.x86_64 0:1.2.3-1.el7                       paratype-pt-sans-caption-fonts.noarch 0:20101909-3.el7
  python-javapackages.noarch 0:3.4.1-11.el7

Complete!
```

- To ensure java has been installed successfully,
- **'java -version'**

```
root@mylinserver:/opt
[root@mylinserver opt]# java -version
java version "1.8.0_161"
Java(TM) SE Runtime Environment (build 8.0.5.10 - pxa6480sr5fp10-20180214_01(SR5 FP10))
IBM J9 VM (build 2.9, JRE 1.8.0 Linux amd64-64 Compressed References 20180208_378436 (JIT enabled, AOT enabled)
OpenJ9   - 39bb844
OMR      - c04ccb2
IBM      - 2321a81)
JCL - 20180209_01 based on Oracle jdk8u161-b12
[root@mylinserver opt]#
```

- To zip the files / folders,
- **'zip -r <filename.zip> <files / folders to be zipped>'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls
file1  file2  file3  file4  sample.txt
[root@mylinserver chnadmin]# zip -r demo.zip file1 file2 file3 file4
  adding: file1 (stored 0%)
  adding: file2 (stored 0%)
  adding: file3 (stored 0%)
  adding: file4 (stored 0%)
[root@mylinserver chnadmin]# ls
demo.zip  file1  file2  file3  file4  sample.txt
[root@mylinserver chnadmin]#
```

- To unzip the file in same location where you are,
- **'unzip <filename.zip>'**

```
root@mylinserver:/home/chnadmin
[root@mylinserver chnadmin]# ls
demo.zip
[root@mylinserver chnadmin]# unzip demo.zip
Archive:  demo.zip
 extracting: file1
 extracting: file2
 extracting: file3
 extracting: file4
[root@mylinserver chnadmin]# ls
demo.zip  file1  file2  file3  file4
[root@mylinserver chnadmin]#
```

- To unzip the file in different location,
- **'unzip <filename.zip> -d /<target location>'**

```
root@mylinserver:/opt
[root@mylinserver chnadmin]# ls
demo.zip
[root@mylinserver chnadmin]# unzip demo.zip
Archive:  demo.zip
 extracting: file1
 extracting: file2
 extracting: file3
 extracting: file4
[root@mylinserver chnadmin]# ls
demo.zip  file1  file2  file3  file4
[root@mylinserver chnadmin]# unzip demo.zip -d /opt
Archive:  demo.zip
 extracting: /opt/file1
 extracting: /opt/file2
 extracting: /opt/file3
 extracting: /opt/file4
[root@mylinserver chnadmin]# cd /opt/
[root@mylinserver opt]# pwd
/opt
[root@mylinserver opt]# ls
file1  file2  file3  file4  rh
[root@mylinserver opt]#
```

- To ensure what are the port numbers running in this server along with PID (Process ID),
- **'netstat -ntlp'**

```
root@mylinserver:/opt
[root@mylinserver opt]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4567/sshd
tcp6       0      0 :::111                  :::*                    LISTEN      1/systemd
tcp6       0      0 :::22                   :::*                    LISTEN      4567/sshd
[root@mylinserver opt]#
```

- To stop the firewall or any service service,
- **'service <service name> stop'**

```
root@mylinserver:/opt
[root@mylinserver opt]# service firewalld stop
Redirecting to /bin/systemctl stop  firewalld.service
[root@mylinserver opt]#
```

- To ensure the status of the service,
- **'service <service name> status'**

```
root@mylinserver:/opt
[root@mylinserver opt]# service firewalld status
Redirecting to /bin/systemctl status  firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Tue 2018-02-27 15:11:28 UTC; 1min 28s ago
     Docs: man:firewalld(1)
  Process: 591 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
 Main PID: 591 (code=exited, status=0/SUCCESS)

Feb 27 13:42:40 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Feb 27 13:42:42 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Feb 27 15:11:27 mylinserver systemd[1]: Stopping firewalld - dynamic firewall daemon...
Feb 27 15:11:28 mylinserver systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@mylinserver opt]#
```

- To download any software / file / folder from internet,
- **'wget <download URL>'**

```
root@mylinserver:/opt
[root@mylinserver opt]# wget http://www-eu.apache.org/dist/tomcat/tomcat-7/v7.0.85/bin/apache-tomcat-7.0.85.tar.gz
--2018-02-27 15:15:32--
Resolving www-eu.apache.org (www-eu.apache.org)... 195.154.151.36, 2001:bc8:2142:300::
Connecting to www-eu.apache.org (www-eu.apache.org)|195.154.151.36|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9037227 (8.6M) [application/x-gzip]
Saving to: 'apache-tomcat-7.0.85.tar.gz'

100%[===========================================================================================>] 9,037,227   6.33MB/s   in 1.4s

2018-02-27 15:15:34 (6.33 MB/s) - 'apache-tomcat-7.0.85.tar.gz' saved [9037227/9037227]

[root@mylinserver opt]# ls
apache-tomcat-7.0.85.tar.gz  file1  file2  file3  file4  zh
[root@mylinserver opt]#
```

- To extract the tar file,
- **'tar xvzf <filename.tar.gz>'**

```
root@mylinserver:/opt
[root@mylinserver opt]# ls
apache-tomcat-7.0.85.tar.gz  file1  file2  file3  file4  rh
[root@mylinserver opt]# tar xvzf apache-tomcat-7.0.85.tar.gz
apache-tomcat-7.0.85/webapps/manager/WEB-INF/jsp/401.jsp
apache-tomcat-7.0.85/webapps/manager/WEB-INF/jsp/403.jsp
apache-tomcat-7.0.85/webapps/manager/WEB-INF/jsp/404.jsp
apache-tomcat-7.0.85/webapps/manager/WEB-INF/jsp/sessionDetail.jsp
apache-tomcat-7.0.85/webapps/manager/WEB-INF/jsp/sessionsList.jsp
apache-tomcat-7.0.85/webapps/manager/WEB-INF/web.xml
apache-tomcat-7.0.85/webapps/manager/images/add.gif
apache-tomcat-7.0.85/webapps/manager/images/asf-logo.svg
apache-tomcat-7.0.85/webapps/manager/images/code.gif
apache-tomcat-7.0.85/webapps/manager/images/design.gif
apache-tomcat-7.0.85/webapps/manager/images/docs.gif
apache-tomcat-7.0.85/webapps/manager/images/fix.gif
apache-tomcat-7.0.85/webapps/manager/images/tomcat.gif
apache-tomcat-7.0.85/webapps/manager/images/update.gif
apache-tomcat-7.0.85/webapps/manager/images/void.gif
apache-tomcat-7.0.85/webapps/manager/index.jsp
apache-tomcat-7.0.85/webapps/manager/status.xsd
apache-tomcat-7.0.85/webapps/manager/xform.xsl
[root@mylinserver opt]# ls
apache-tomcat-7.0.85  apache-tomcat-7.0.85.tar.gz  file1  file2  file3  file4  rh
```

- To provide all permission to files / folders,
- **'chmod -R 777 <file / folder name>'**

```
root@mylinserver:/opt
[root@mylinserver opt]# chmod -R 777 apache-tomcat-7.0.85
[root@mylinserver opt]# ls
apache-tomcat-7.0.85  apache-tomcat-7.0.85.tar.gz  file1  file2  file3  file4  rh
[root@mylinserver opt]#
```

- To start the Tomcat Service,
- **'./startup.sh'**

```
root@mylinserver:/opt/apache-tomcat-7.0.85/bin
[root@mylinserver bin]# pwd
/opt/apache-tomcat-7.0.85/bin
[root@mylinserver bin]# ./startup.sh
Using CATALINA_BASE:   /opt/apache-tomcat-7.0.85
Using CATALINA_HOME:   /opt/apache-tomcat-7.0.85
Using CATALINA_TMPDIR: /opt/apache-tomcat-7.0.85/temp
Using JRE_HOME:        /
Using CLASSPATH:       /opt/apache-tomcat-7.0.85/bin/bootstrap.jar:/opt/apache-tomcat-7.0.85/bin/tomcat-juli.jar
Tomcat started.
[root@mylinserver bin]#
```

- To see the Kernel details,
- **'uname -a'**

```
root@mylinserver:/opt/apache-tomcat-7.0.85/bin
[root@mylinserver bin]# uname -a
Linux mylinserver 3.10.0-514.28.1.el7.x86_64 #1 SMP Fri Jul 7 12:58:19 EDT 2017 x86_64 x86_64 x86_64 GNU/Linux
[root@mylinserver bin]#
```

- To get the OS name and version,
- **'cat /etc/redhat-release'**

```
root@mylinserver:/opt/apache-tomcat-7.0.85/bin
[root@mylinserver bin]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.3 (Maipo)
[root@mylinserver bin]#
```

- To create a new username and the password,
- **'useradd <username>'**
- **'passwd <username>'**

```
root@mylinserver:/home
[root@mylinserver bin]# useradd saravanan
[root@mylinserver bin]# passwd saravanan
Changing password for user saravanan.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@mylinserver bin]# cd /home/
[root@mylinserver home]# ls
chnadmin  saravanan
[root@mylinserver home]#
```

- To restart the server,
- **'reboot'**

```
PuTTY (inactive)
[root@mylinserver bin]# useradd saravanan
[root@mylinserver bin]# passwd saravanan
Changing password for user saravanan.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@mylinserver bin]# cd /home/
[root@mylinserver home]# ls
chnadmin  sample  saravanan
[root@mylinserver home]# reboot
```

PuTTY Fatal Error

Server unexpectedly closed network connection

OK

- To know more Linux commands, refer the below given URL's
- https://www-uxsup.csx.cam.ac.uk/pub/doc/suse/suse9.0/userguide-9.0/ch24s04.html
- https://www.guru99.com/must-know-linux-commands.html
- https://drive.google.com/file/d/1f_AFv6TjV_mu9WbXdHIXJX2aOXxi9N4D/view?usp=sharing

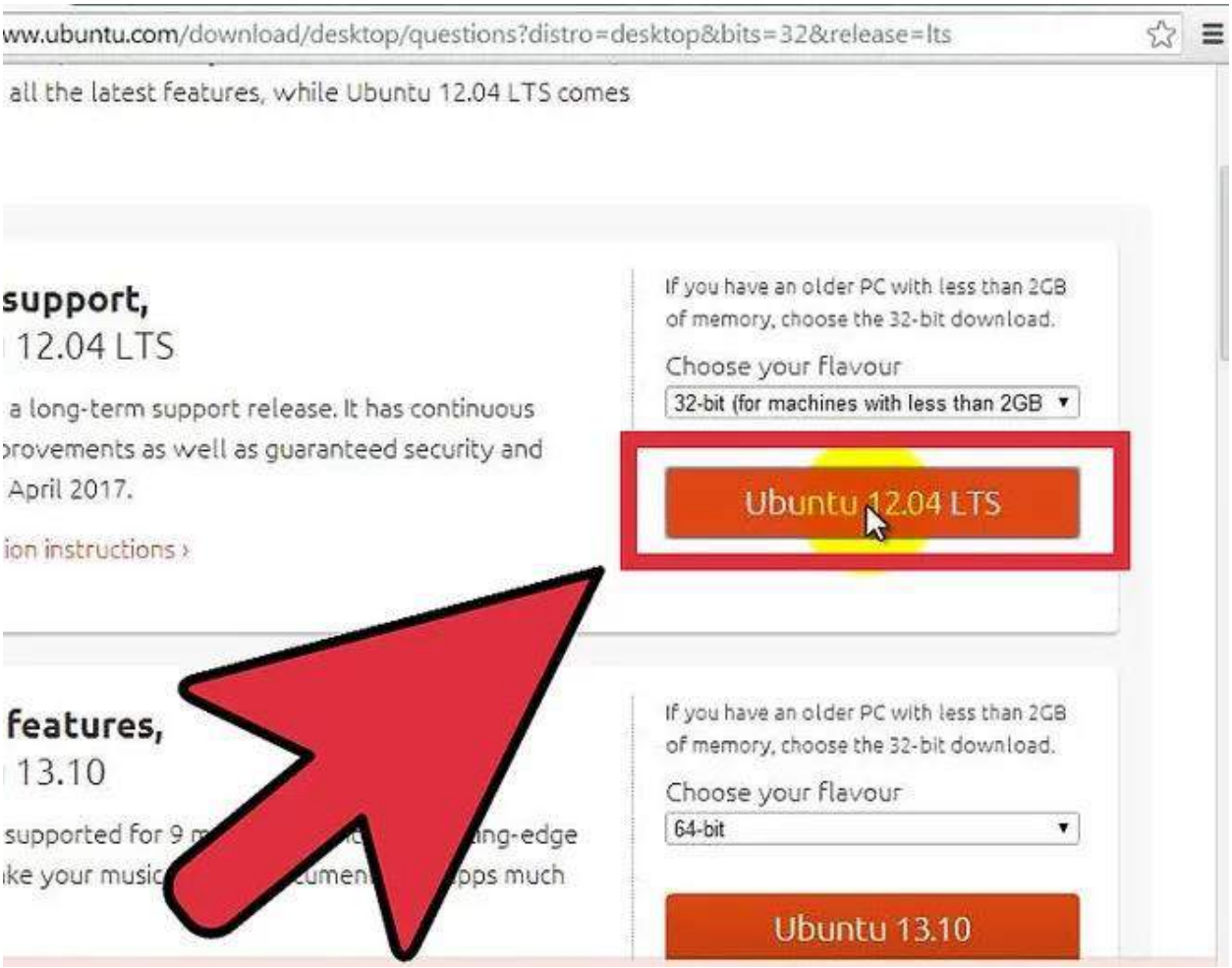
Installation and Initialization:

Installation:

- If you're new to Linux, consider trying a lightweight and easy to use distribution, such as Ubuntu, Lubuntu, etcetera. Linux distributions (known as "distros") are typically available for free to download in ISO

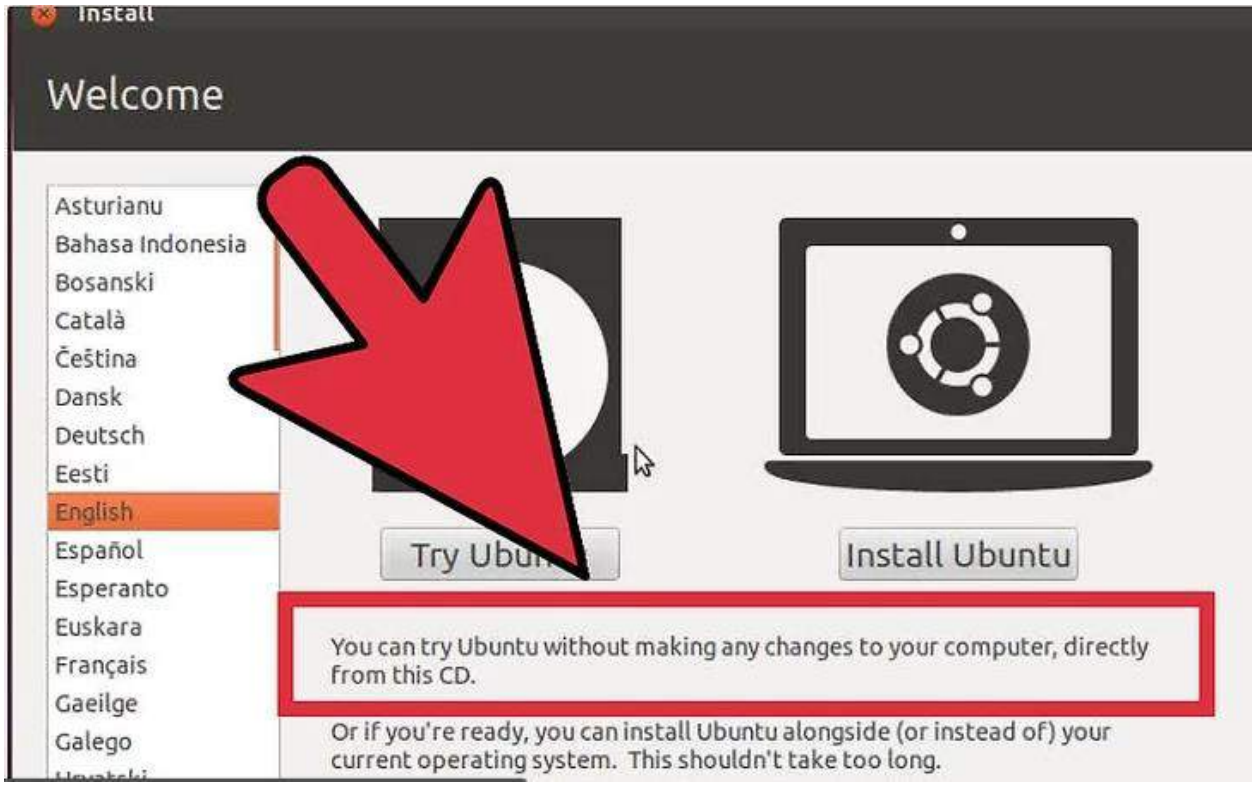
format. You can find the ISO for the distribution of your choice at the distribution's website. This format needs to be burned to a CD or USB stick before you can use it to install Linux. This will create a Live CD or Live USB.

- A Live CD or Live USB is a disk that you can boot into, and often contains a preview version of the operating system that can be run directly from the CD or USB stick
- Install an image burning program or use your system's built-in burning tool if you are using Windows 7, 8, or Mac OS X. Pen Drive Linux and UNetBootin are two popular tools for burning ISO files to USB sticks.

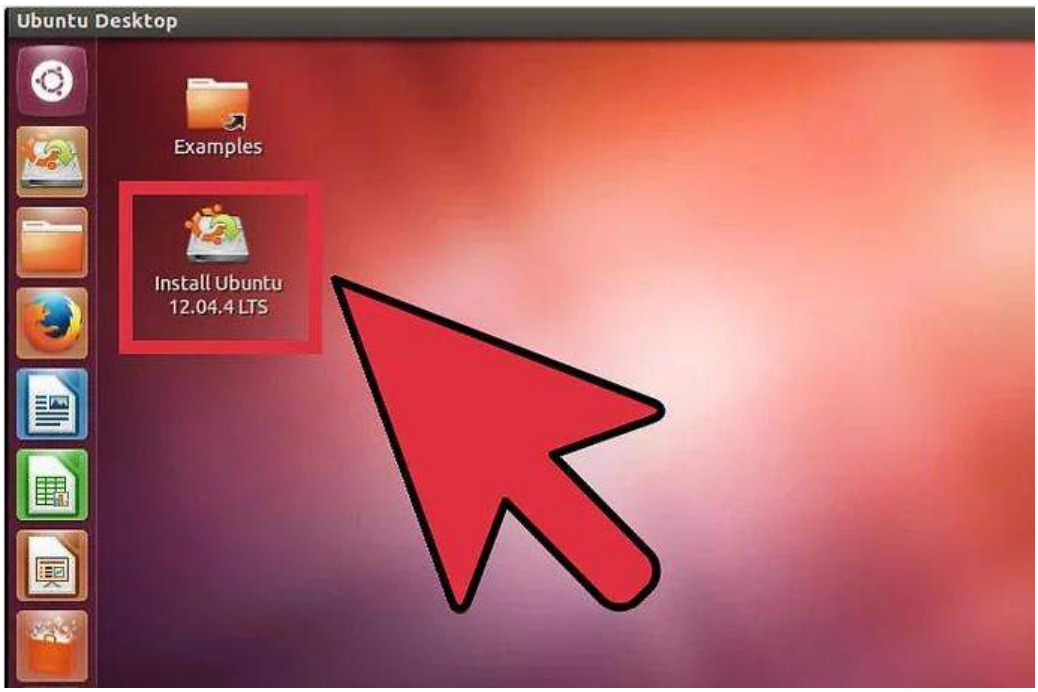


- Most computers are set to boot into the hard drive first, which means you will need to change some settings to boot from your newly-burned CD or USB. Start by rebooting the computer.
- Once the computer reboots, press the key used to enter the boot menu. The key for your system will be displayed on the same screen as the manufacturer's logo. Typical keys include F12, F2, or Del.
- For Windows 8 users, hold the Shift key and click restart. This will load the Advanced Startup Options, where you can boot from CD.
- For Windows 10 users, go to advanced boot in settings and click "Restart Now."
- If your computer doesn't give you direct access to the boot menu from the manufacturer's splash screen, it's most likely hidden in the BIOS menu. You can access the BIOS menu in the same way that you would get to the boot menu. At the manufacturer splash screen, the key should be listed in one of the bottom corners.

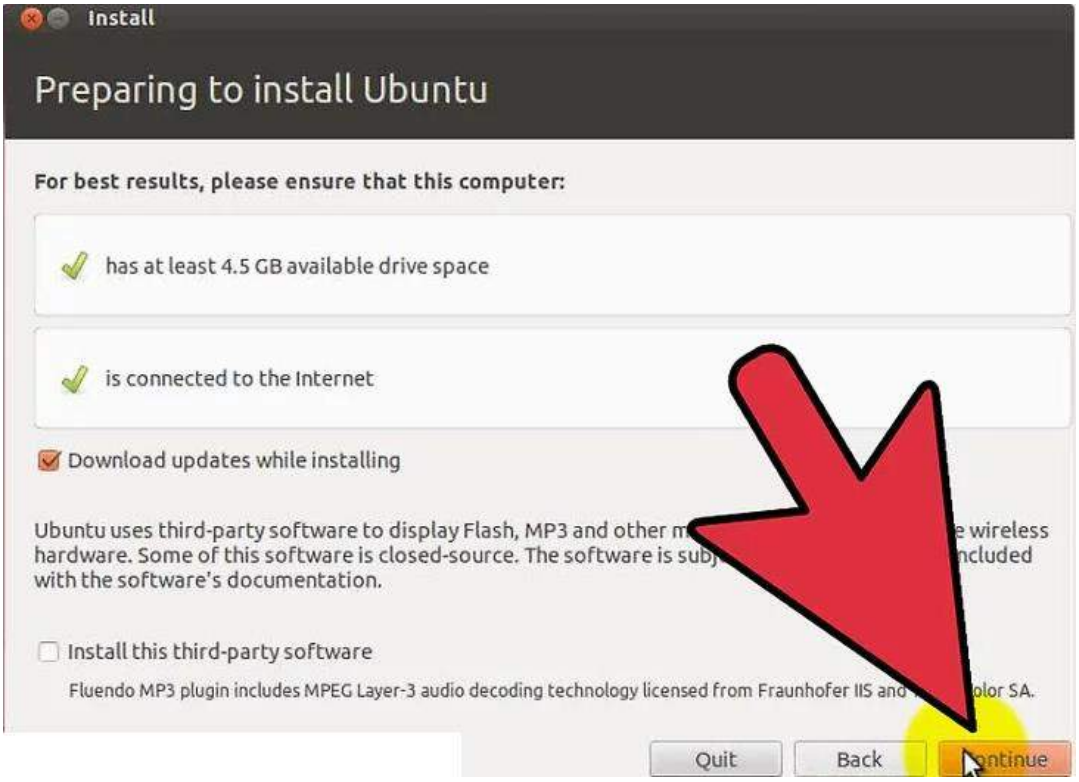
- Once you're in the boot menu, select your live CD or USB. Once you've changed the settings, save and exit the BIOS setup or boot menu. Your computer will continue with the boot process.



- Most Live CDs and USBs can launch a "live environment", giving you the ability to test it out before making the switch. You won't be able to create files, but you can navigate around the interface and decide if it's right for you.

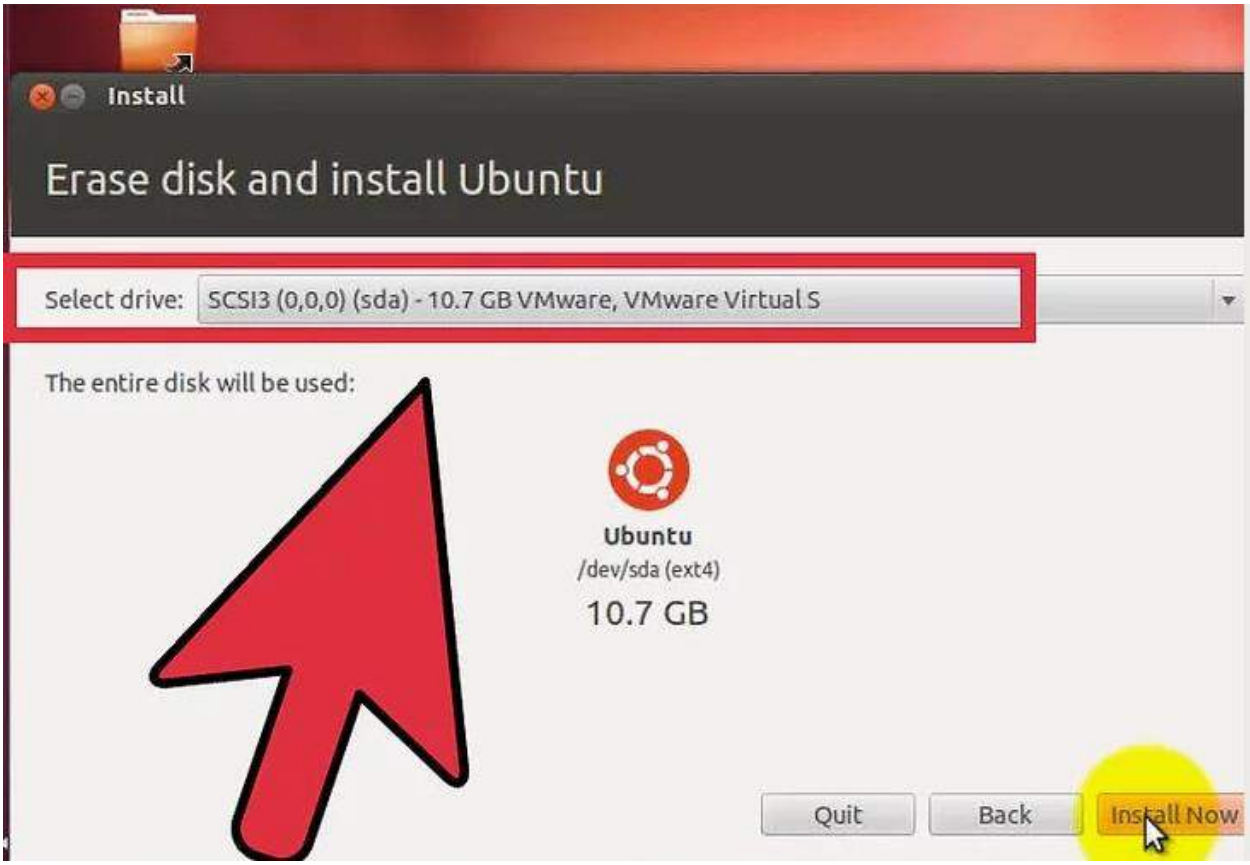


- If you're trying out the distro, you can launch the installation from the application on the desktop. If you decided not to try out the distribution, you can start the installation from the boot menu.
- You will be asked to configure some basic options, such as language, keyboard layout, and time zone.

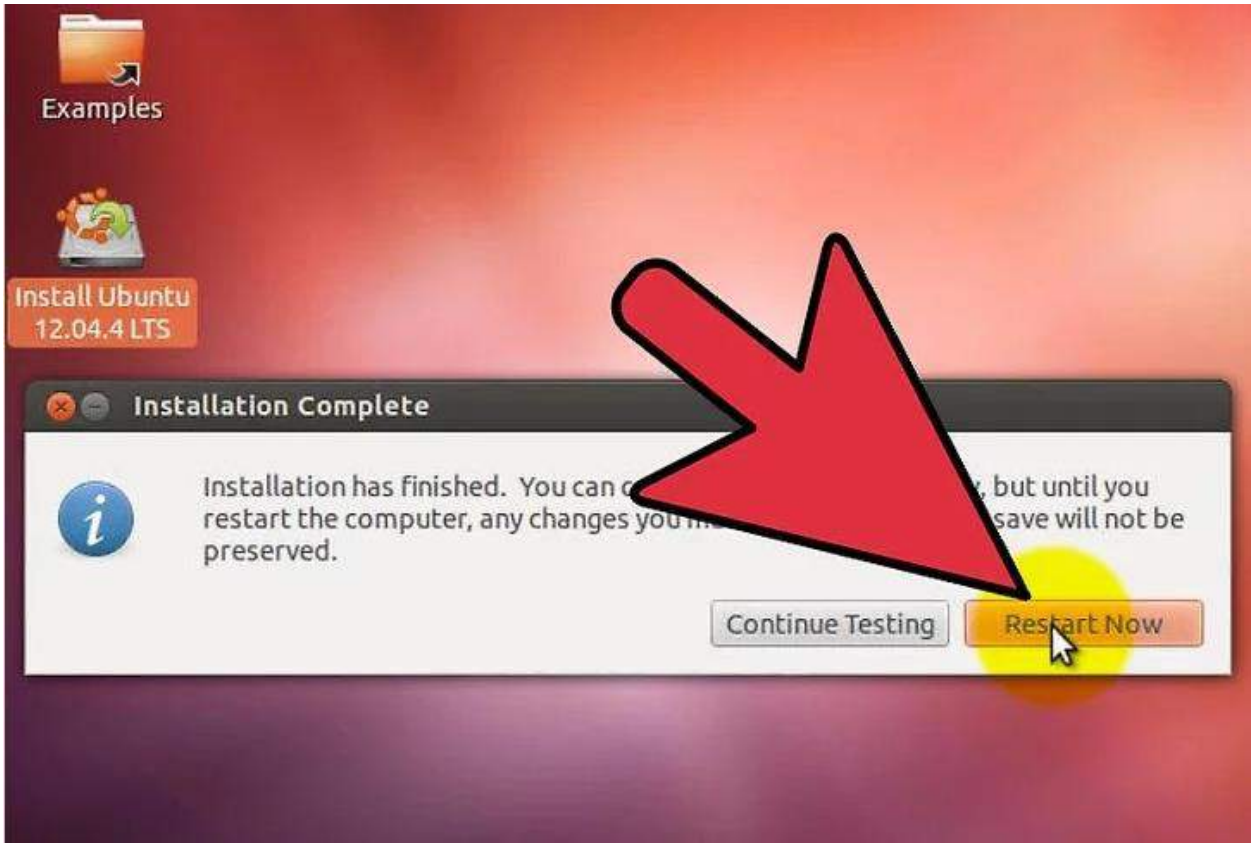


- You will need to create login information to install Linux. A password will be required to log into your account and preform administrative tasks.

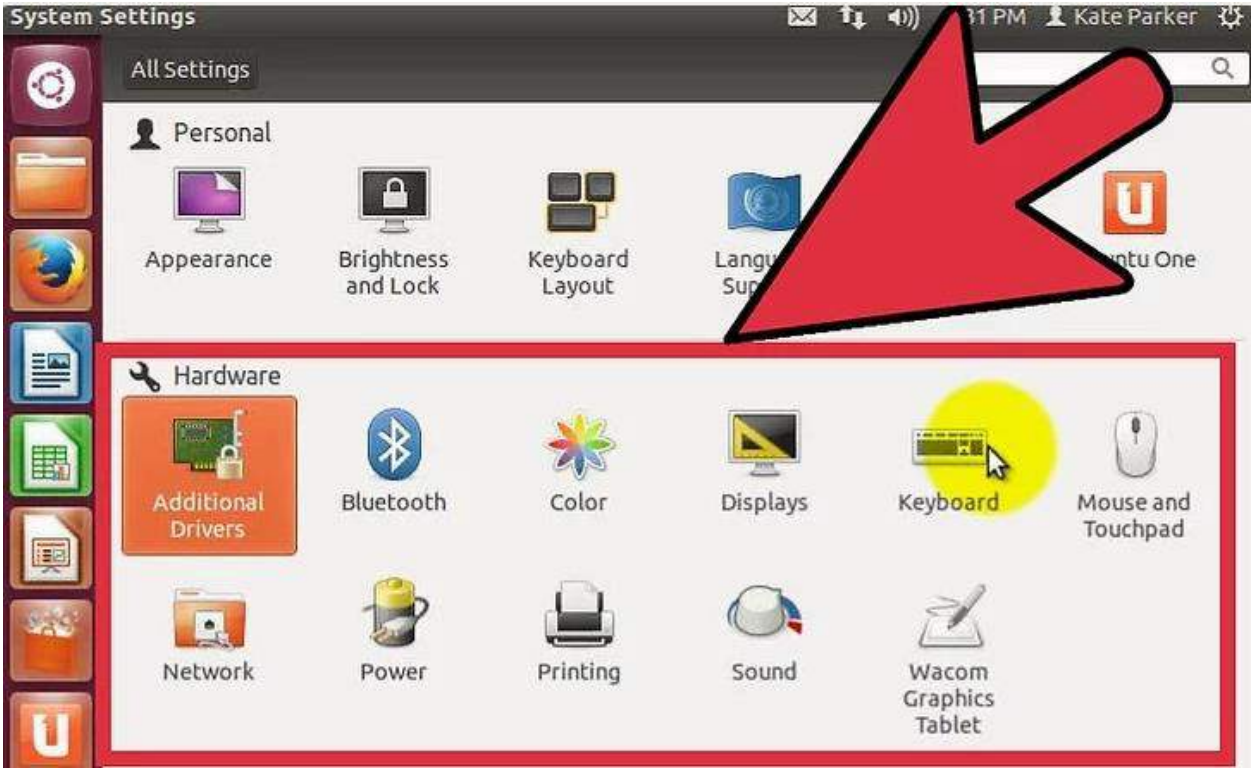
- Linux needs to be installed on a separate partition from any other operating systems on your computer if you intend dual booting Linux with another OS. A partition is a portion of the hard drive that is formatted specifically for that operating system. You can skip this step if you don't plan on dual booting.
- Distros such as Ubuntu will set a recommended partition automatically. You can then adjust this manually yourself. Most Linux installations require at least 20 GB, so be sure to set aside enough room for both the Linux operating system and any other programs you may install and files you may create.
- If the installation process does not give you automatic partitions, make sure that the partition you create is formatted as Ext4. If the copy of Linux you are installing is the only operating system on the computer, you will most likely have to manually set your partition size.



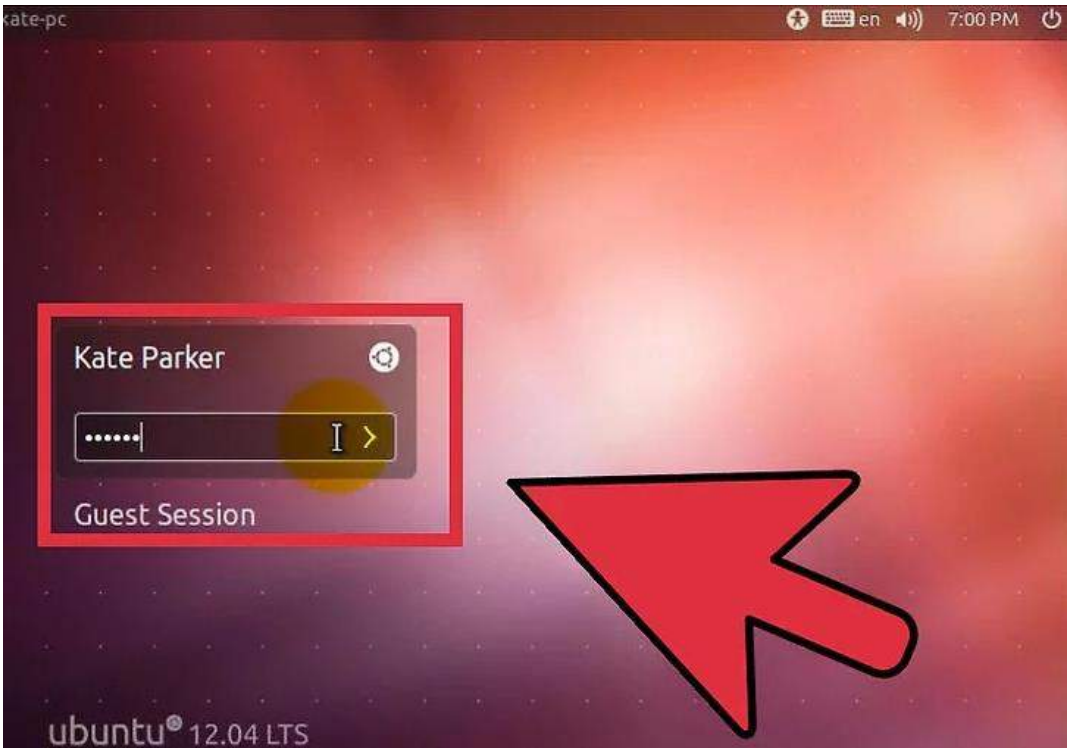
- Once the installation is finished, your computer will reboot. You will see a new screen when your computer boots up called “GNU GRUB”. This is a boot loader that handles Linux installations. Pick your new Linux distro from the list. This screen may not show up if you only have one operating system on your computer. If this screen isn't being presented to you automatically, then you can get it back by hitting shift right after the manufacturer splash screen.
- If you install multiple distros on your computer, they will all be listed here.



- Most hardware should work out of the box with your Linux distro, though you may need to download some additional drivers to get everything working.
- Some hardware requires proprietary drivers to work correctly in Linux. This is most common with graphics cards. There is typically an open source driver that will work, but to get the most out of your graphics cards you will need to download the proprietary drivers from the manufacturer.
- In Ubuntu, you can download proprietary drivers through the System Settings menu. Select the Additional Drivers option, and then select the graphics driver from the list. Other distros have specific methods for obtaining extra drivers.
- You can find other drivers from this list as well, such as Wi-Fi drivers.



- Once your installation is complete and you've verified that your hardware is working, you're ready to start using Linux. Most distros come with several popular programs installed, and you can download many more from their respective file repositories.



Initialization:

- **Power Supply & SMPS**
- One of the main component of a computer is SMPS (Switching Mode Power Supply). The primary objective of this component is to provide the perfect required voltage level to the motherboard and other computer components. Computer internals work in DC, however the power supply we have at home and other places are AC. SMPS converts AC to DC and maintain the required voltage level so that the computer can work flawlessly.
- But the main task performed by SMPS, is to inform about the good power supply. As I told if the voltage is more/ or is less, in both the conditions a computer cannot work. As soon as you supply power to the computer, the SMPS checks the voltage level's its providing to the motherboard. If the power signal level is perfect, then SMPS will send a POWER GOOD signal to the motherboard timer.
- On receiving this POWER GOOD signal from SMPS, the motherboard timer will stop sending reset signal to the CPU. Which means the power level is good and the computer can boot.
- **Bootstrapping**
- Something must be programmed by default, so that the CPU knows where to search for instructions.
- This is an address location in the ROM. This address location is almost always constant in X86 based computers. The address location is FFFF:0000h.
- This address location is the last region of the ROM. It only contains one instruction. The instruction is to jump to another memory address location. This JUMP command will tell the location of the BIOS program in the ROM.
- This is how the computer will come to know where the BIOS program is located.
- **The Role of BIOS in booting process**
- The word booting comes from another word called bootstrapping. The computer knows how to bring itself up, when you press the start button, because of the instructions that are fed to a program called as BIOS. BIOS stands for Basic Input Output System. The most important use of BIOS during the booting process is POST. POST stands for Power on Self-Test. It’s a series of tests conducted by the bios, which confirms the proper functioning of different hardware components attached to the computer.
- POST is very important thing to have before the Operating system is loaded. Just imagine if you have a faulty hard drive or faulty memory, sometimes these things can cause data loss. POST checks and confirms the integrity of the following hardware components.
    - Timer IC's
    - DMA controllers
    - CPU
    - Video ROM
- A full POST check will confirm the integrity of the following devices as well.
    - Motherboard
    - Keyboard
    - Printer port
    - Hard Drive etc.
- If you are doing a warm start (which means you did a reset of a running machine, most of the times reset button is the small one near the power button on the CPU), a full POST check will not be conducted by the BIOS. However, if you are doing a Cold Start, which means you have applied the power now, it will conduct a full POST.
- BIOS determines whether it’s a cold or warm start, by looking at a flag in a predefined memory location. Once the POST completes, the BIOS will inform you about any problems it found with the help of beep codes (through system speaker). Different number of beep codes have different meaning.
- There are two things that people often get confused with. Its CMOS & BIOS. CMOS & BIOS are two completely different things in the computer motherboard. CMOS is a small memory RAM chip that's present in the motherboard. This RAM is different from the computers main RAM chip (which are replaceable memory chips.

- These days RAM chips are available in the range of Gigabytes.). Unlike the main RAM chip, CMOS RAM does not flush its memory when a computer is turned off. It remembers all the configuration with the help of a battery called CMOS battery.
- Removing a CMOS battery will make the CMOS to forget all the configuration you have saved previously.
- This is the reason you can unlock a computer that's protected with a CMOS password, by simply removing the CMOS battery.
- Also removing the CMOS battery will make the operating system to show you wrong time. Because system time consistency is maintained in CMOS settings.
- So, it’s always advisable to replace your CMOS battery at regular intervals, for proper functioning of the computer.
- Normally people say that we have modified BIOS settings. But it’s completely wrong. What they modified is in fact CMOS settings. CMOS settings is the place where you modify the boot order etc.
- Bios settings cannot be altered by the user. It requires a flash program provided by the manufacturer.
- So, let’s get back to our booting process. Once the POST check is completed successfully, BIOS will look CMOS settings to know what the boot order is. Boot order is nothing but a user defined order which tells where to look for the operating system.
- The order will be something like the below.
    - CD ROM
    - HARD DISK
    - USB
    - Floppy DISK
- The above shown order means that the BIOS will look at CD ROM first to check whether an OS can be loaded from there, if it does not find a bootable disk in the CD ROM, it will look check whether a bootable OS is there in the hard disk, then USB and then Floppy disk.
- Let's assume that you don’t have a bootable CD in your CD ROM drive, then the BIOS will turn to HARD disk.
- **MBR and GRUB**
- Now as you don't have any bootable CD in your CD ROM Drive, the bios will look at the second device from the boot order settings. The second device is your Hard Disk.
- BIOS is programmed to look at a permanent location on the hard disk to complete its task. This location is called a Boot sector. This is nothing but the first sector of your hard disk. This area is sometimes called as MBR (Master Boot Record). This is the location that contains the program that will help our computer to load the operating system. As soon as bios finds a valid MBR, it will load the entire content of MBR to RAM, and then further execution is done by the content of MBR.
- This first sector of the hard disk is only of 512 bytes. Yeah, it’s too small an area for an entire boot loader program to fit in. Hence most of the operating system store only the first stage of their boot loader program in here. Only the first 440 bytes from the total of 512 bytes is used by the first stage boot loader, the remaining part is used to store partition table information.
- Read: What is MBR and GPT Partition Table
- As the title of this article says, "Linux Booting process", we will be having grub stage one in the first 440 bytes of the MBR. I would suggest reading the below article to understand grub and its details.
- Read: Grub tutorial
- You can take an entire dump/backup of your MBR in Linux with the help of the following command.

```
root@ubuntu-dev:~# dd if=/dev/sda of=mbr bs=512 count=1
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000134061 s, 3.8 MB/s
```

- What the above command does is to simply dump the contents of your first sector which of 512 bytes to a file named mbr. bs in the above command stands for block size. And count means to dump only the first sector (the dump will start from the beginning of the hard disk, and the size is 512 bytes)

```
root@ubuntu-dev:~# file mbr.bin
mbr.bin: x86 boot sector; partition 1: ID=0x83, active, starthead 32, startsector 2048, 19451904 secto
```

- **mbr.bin: x86 boot sector; partition 1: ID=0x83, active, starthead 32, startsector 2048, 19451904 sectors; partition 2: ID=0x5, starthead 254, startsector 19455998, 2093058 sectors, code offset 0x63**
- I have only two partitions on the system, that's why its showing partition 1 & partition 2. The MBR contains of the following things to summarize. From the partition table shown in the above mbr dump output, Grub stage 1 in the MBR will look for a partition with active flag set on it. Please remember the fact that there can only be one active partition from the 4. If you see my partition table output above, partition 1 is having an active flag.
    - First stage grub
    - Partition table information
    - Error messages
    - Magic Number
- The fourth point is a Magic Number of 2 bytes. This magic number serves as a method of verification for the MBR. This 2-byte magic number will contain values that will be something like AA55. A different magic number indicates a corrupted MBR or invalid MBR.
- The primary job of the stage 1 bootloader is to load the second stage boot loader. The second stage boot loader is the stage 2 grub, that does the job of loading the kernel and other initrd image files (we will come to that part in some time). GRUB (Grand Unified Boot Loader) is the combined name given to different stages of grub.
- Now there is a little surprise that am going to reveal. There are not two stages of grub. But there are three stages of grub in total. I will explain you the reason behind this. The three stages are mentioned below.
    - GRUB Stage 1
    - GRUB Stage 1.5
    - Grub Stage 2
- Now from where does this stage 1.5 came. The hard disk sectors are counted form 0 to the last sector. As explained previously the first sector (sector 0) contains the GRUB stage 1. Normally partitions will not start before sector 63. So, partitions will start form sector number 63. Hence, we have sectors form 1-63 free. This space is used for storing GRUB stage 1.5. This free space between MBR and the beginning of the partitions is called as MBR GAP.
- Now you might think what the requirement of an additional stage in grub is. If you are a Linux guy, you might have already configured grub configuration file. If you remember the configuration, it contains the kernel file location and name, its partition. Now how will the grub access those kernel files without the file system drivers?
- Grub Stage 1.5 located in the MBR GAP (sector 1 to 63 before the beginning of the first partition) basically contains the drivers for reading file systems. So, grub stage 1 will load grub stage 1.5 to the RAM and will pass the control to it.
- Now grub stage 1.5 will load the file system drivers and once the file system drivers are loaded, it can now access /boot/grub/grub.conf file which contains other details about kernel path and initrd path etc.
- Now this is the point where you are presented with a beautiful TUI (Terminal user interface), where you can select your operating system kernel and press enter to boot it.
- **Loading the Kernel Image**
- Like GRUB, kernel is also loaded in stages. A Linux kernel is responsible for handling Process management, Memory Management, Users, Inter process communication etc. I must say kernel is never used by a user. What the kernel does is to maintain a good environment for programs to run. Yeah, we use kernel through different programs.
- Kernel is a compressed image file. The location of this compressed kernel image is specified in the grub 2 configuration file. It’s basically an executable bzImage file.
- Now you need to have a lot of drivers and modules to access underlying hardware and other stuff. For example, if you have RAID configured on your / partition how will you mount it without knowing the programs or think how you will include a kernel module or how to remove a kernel module. All these

things required different set of programs and code. Including all these codes inside the kernel will make it a larger file image.

- But our kernel image file needs to be smaller, that's the reason its compressed image file. So, most of these drivers and tools along with a small similar root file system feel is given by initrd. Initrd is sometimes called as initial root file system. This is used by the kernel before the real root file system is mounted. Initrd is available in the form of an image like the kernel image file. Let's see what's the content of this initrd image file. You can find the initrd image file and the kernel image file in the /boot directory.

```
[root@localhost initrd]# mv initramfs-2.6.32-358.14.1.el6.x86_64.img initramfs-2.6.32-358.14.1.el6.x86_64.gz

[root@localhost initrd]# gunzip initramfs-2.6.32-358.14.1.el6.x86_64.gz

[root@localhost initrd]# cpio -id < initramfs-2.6.32-358.14.1.el6.x86_64
90587 blocks
[root@localhost initrd]# ls
bin                 initqueue                           mount        sysroot
cmdline             initqueue-finished                  pre-pivot    tmp
dev                 initqueue-settled                   pre-trigger  usr
dracut-004-303.el6  initqueue-timeout                   pre-udev     var
emergency           initramfs-2.6.32-358.14.1.el6.x86_64 proc
etc                 lib                                 sbin
init                lib64                               sys
```

- If you see the above commands, we have first uncompressed the initrd image file, then we can view the contents of that file with the help of cpio command.
- Now you can see the contents of initrd image file. There are folders that are very much like our Linux directory structure. There is /etc/, /lib, and some necessary commands in /sbin etc. It’s a small root file system that the kernel loads as a temporary root file system before the real root file system is loaded.
- Loading and unloading of kernel modules is done with the help of programs like insmod, and rmmod present in the initrd image.
- Now as the kernel is loaded into the memory, the execution begins by checking the processor family and architecture. The kernel conducts a lot of hard ware specific operations and the first user space program it executes is /sbin/init.
- As this is the first program executed by the kernel, it has got a process id number of 1. The process id number 1 for init was not kept intentionally, but it was due to the fact that it is the first process executed by the kernel. Now as soon as the kernel executes the init process, it will look at the /etc/inittab configuration file to see the default run level.
- There are different run level's in linux.
- Run-Level
    - 0 - System Halt/Shut Down
    - 1 - Single User Mode
    - 2 - Multiuser Mode Without Networking
    - 3 - Full Multiuser Mode
    - 4 - Unused
    - 5 - GUI/X11
    - 6 - Reboot
- The /etc/inittab file contains the default run level like the one shown below.

```
1  id:3:initdefault:
```

- Now that means, we have a run level 3 as the default run level. Once this is identified, then run level specific programs are started by the kernel. This is the reason you have the following directories.

```
[root@localhost]# cd /etc/rc.d/
[root@localhost rc.d]# ll
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 init.d
-rwxr-xr-x. 1 root root  2617 Jul 24 08:53 rc
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc0.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc1.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc2.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc3.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc4.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc5.d
drwxr-xr-x. 2 root root  4096 Oct  8 00:50 rc6.d
-rwxr-xr-x. 1 root root   499 Aug 13 10:55 rc.local
-rwxr-xr-x. 1 root root 19216 Jul 24 08:53 rc.sysinit
```

- The folders rc0.d, rc1.d, rc2.d etc contains run level specific programs that will be executed depending upon the default run level you have in your inittab configuration file.
- Let's see what the contents inside these run level folders are.

```
[root@localhost rc3.d]# ls
K01numad        K80kdump              S13cpuspeed         S28autofs
K01smartd       K84wpa_supplicant     S13irqbalance       S50choose_repo
K02oddjobd      K86cgred              S13rpcbind          S50cloud-init-local
K10psacct       K87restorecond        S15mdmonitor        S50mcelogd
```

- If you see the files inside these run level specific folders, they either begin with S or they begin with K. The files are also numbered. Now files with an S at starting will be executed during the startup process, and files that begins with K, will be killed during shutdown process.
- The number after either S or K is the sequence with which these will be executed.
- Once the kernel has started all programs in your desired run level directory. You will get a login screen to log inside your booted system. Hope this article was helpful and easy to understand. Please let us know in case anybody finds a mistake in this article, so that we can correct it.

Boot and Package Management:

- Refer the below given URL to download and for more information about Boot and Package Management.
- https://linode.com/docs/tools-reference/linux-package-management/
- https://drive.google.com/file/d/1_0uWZY65vlFzvJof-OJxomWcU-ETAEaA/view?usp=sharing

User Administration:

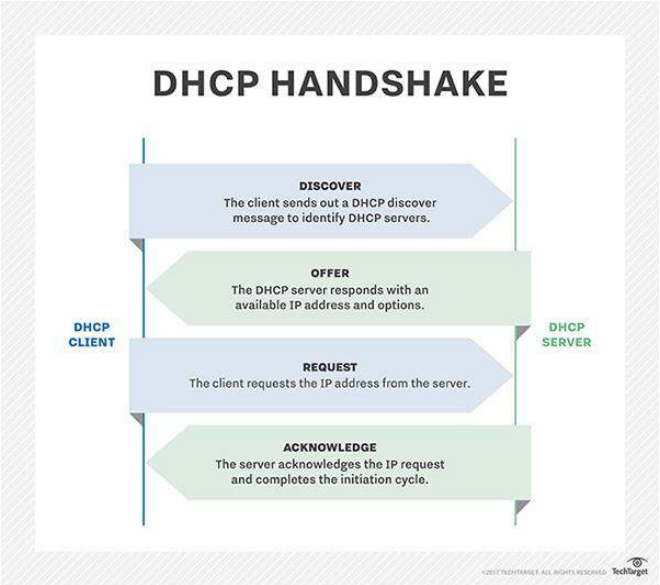
- Download the file using below given URL to know about the commands to create a User and Groups.
- https://drive.google.com/file/d/1y7lNY6ePIZvL88f-Dxd5wWJ-CzfdTwbZ/view?usp=sharing

Service Protocols:

- We could see below mentioned Service Protocols in detail.

Dynamic Host Configuration Protocol (DHCP):

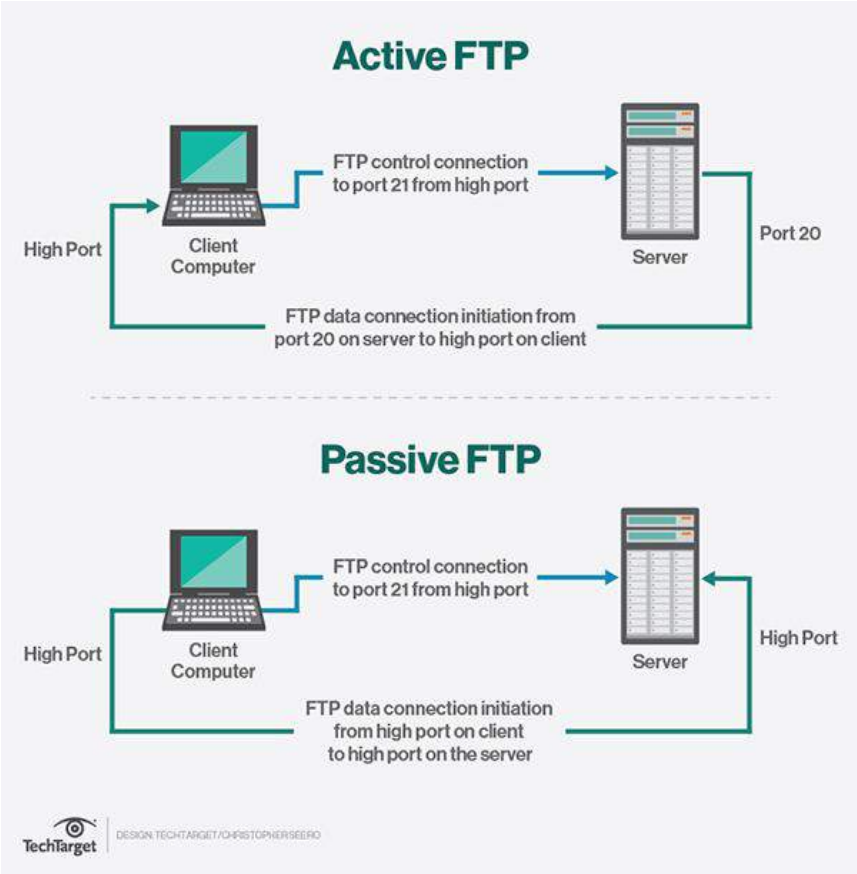
- DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks as well as large enterprise networks.



- Refer below given URL for more information.
- http://searchnetworking.techtarget.com/definition/DHCP

File Transfer Protocol (FTP):

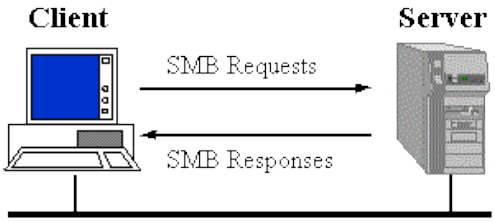
- The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
- FTP is built on a client-server model architecture and uses separate control and data base line kali Linux 1 bor <amd. mn> connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead; it is technologically different.
- FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.



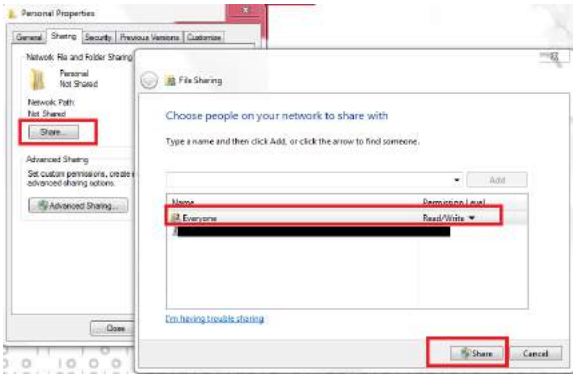
- Refer below given URL for more information.
- http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol

Samba (SMB):

- SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.
- SMB is a client server, request-response protocol. The below diagram illustrates the way in which SMB works. The only exception to the request-response nature of SMB (that is, where the client makes requests and the server sends back responses) is when the client has requested opportunistic locks (oplocks) and the server subsequently must break an already granted oplock because another client has requested a file open with a mode that is incompatible with the granted oplock. In this case, the server sends an unsolicited message to the client signaling the oplock break.
- Servers make file systems and other resources (printers, mailslots, named pipes, APIs) available to clients on the network. Client computers may have their own hard disks, but they also want access to the shared file systems and printers on the servers.
- Clients connect to servers using TCP/IP (NetBIOS over TCP/IP as specified in RFC1001 and RFC1002), NetBEUI or IPX/SPX. Once they have established a connection, clients can then send commands (SMBs) to the server that allow them to access shares, open files, read and write files, and generally do all the sort of things that you want to do with a file system. However, in the case of SMB, these things are done over the network.



- To install Samba on Linux Server, create one Ubuntu Server and do the following steps.
- sudo -s
- apt-get update
- apt-get install samba
- vi /etc/samba/smb.conf
- Insert the below content at the bottom of the file.
  [share]
  comment = Ubuntu File Server Share
  path = /opt/samba/share
  browsable = yes
  guest ok = yes
  read only = no
  create mask = 0755
- Save the file.
- Esc + :wq
- cd /opt
- mkdir samba
- cd samba
- mkdir share
- cd share
- chown nobody.nogroup /opt/samba/share/
- touch sample.txt
- vi /etc/init/nmbd.conf
  # install -o root -g root -m 755 -d /var/run/samba
  NMBD_DISABLED=`testparm -s --parameter-name='disable netbios' 2>/dev/null`
  # ["x$NMBD_DISABLED" = xYes] && { stop; exit 0; }
- Save the file.
- Esc + :wq
- service smbd restart
- service nmbd restart
- After this installation you can able to use this share path both Windows and Linux. Use any Windows Server and type the below content to access this shared folder which is available in Linux.
- \\<Ubuntu IP>\share
- To Access in Linux,
- Smb://<Ubuntu IP>/share
- If you want to share the files and folders using NFS between Windows to Windows, you could open 445 port number and proceed to share after giving permissions to that folder which you would like to share.

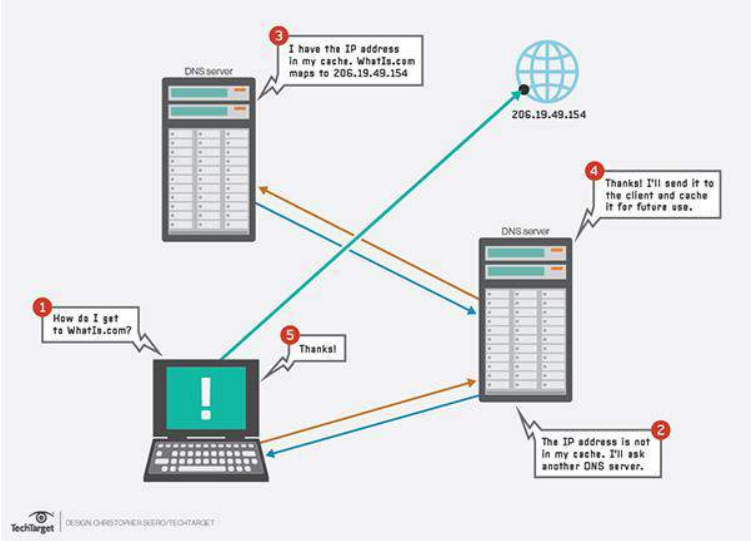


Apache:

- Apache could act as a Web Server as well as Application Server. If you require your application to be deployed in Apache, it can be possible by placing an Application Bundle in www folder which could be accessed like http://<ServerIP>/Application Context.
- Majority of the users, using an Apache as a Web Server to be balancing the load of an Application from multiple request from an end user.
- Apache load balancer is an open source server application traffic distribution solution that, according to recent statistics, has been utilized in over 100,000 web sites. One of its main attractions for providing high availability to web applications is its customizability which allows it to be programmed to operate in many different modes depending upon the unique requirements of a given environment. These modes are configured using the Multiprocessing Modules (MPMs). To create your Apache load balancer, you will need to have the apache module mod proxy and the mod proxy balancer which are readily available for download. The Apache Software Foundation provides support for its user community along with other open source applications.
- While native Apache load balancer can meet the needs of some implementations, the programming knowledge and granular manipulation required to optimize it results in it not being suitable for every scenario. For this reason, dedicated proprietary hardware/virtual load balancers such as the KEMP Loadmaster are often leveraged to provide load balancing and application delivery services for enterprise websites and applications.

Domain Name System (DNS):

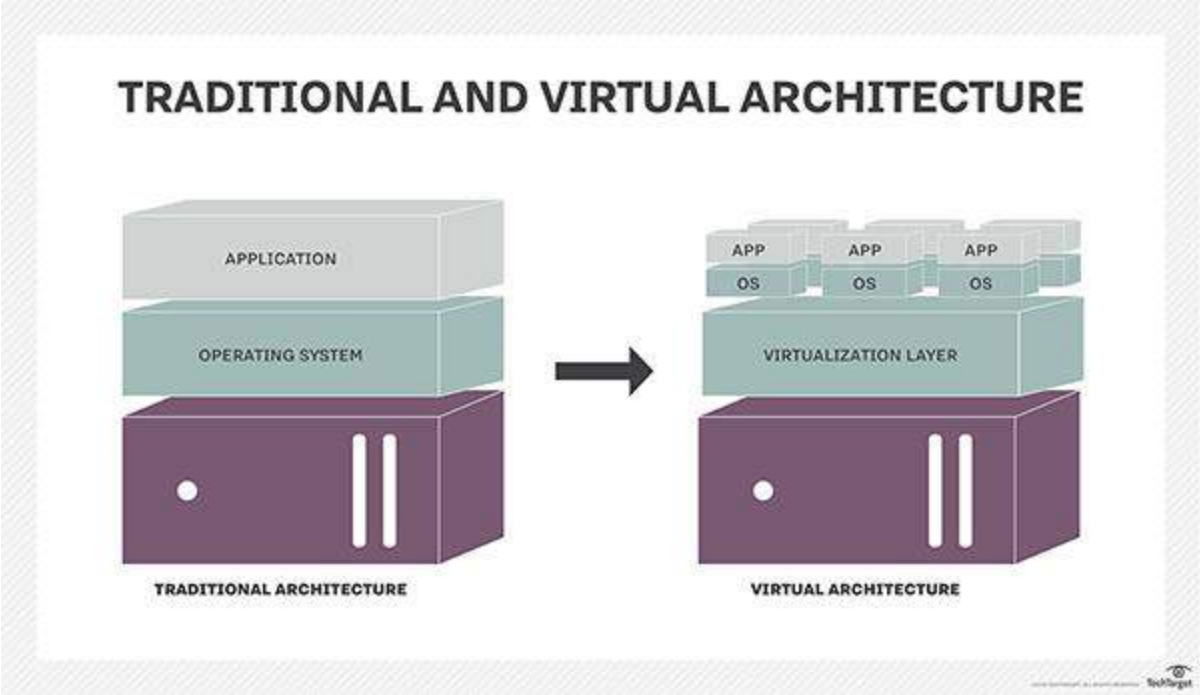
- The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types TechTarget.com into a web browser, a server behind the scenes will map that name to the IP address 206.19.49.149.

- 

- To promote efficiency, servers can cache the answers they receive for a set amount of time. This allows them to respond more quickly the next time a request for the same lookup comes in. For example, if everyone in an office needs to access the same training video on a website on the same day, the local DNS server will ordinarily only have to resolve the name once, and then it can serve all the other requests out of its cache.
- Refer the below given URL for more information.
- http://searchnetworking.techtarget.com/definition/domain-name-system

Virtualization:

- Virtualization describes a technology in which an application, guest operating system or data storage is abstracted away from the true underlying hardware or software. A key use of virtualization technology is server virtualization, which uses a software layer called a hypervisor to emulate the underlying hardware. This often includes the CPU's memory, I/O and network traffic. The guest operating system, normally interacting with true hardware, is now doing so with a software emulation of that hardware, and often the guest operating system has no idea it's on virtualized hardware. While the performance of this virtual system is not equal to the performance of the operating system running on true hardware, the concept of virtualization works because most guest operating systems and applications don't need the full use of the underlying hardware. This allows for greater flexibility, control and isolation by removing the dependency on a given hardware platform. While initially meant for server virtualization, the concept of virtualization has spread to applications, networks, data and desktops.



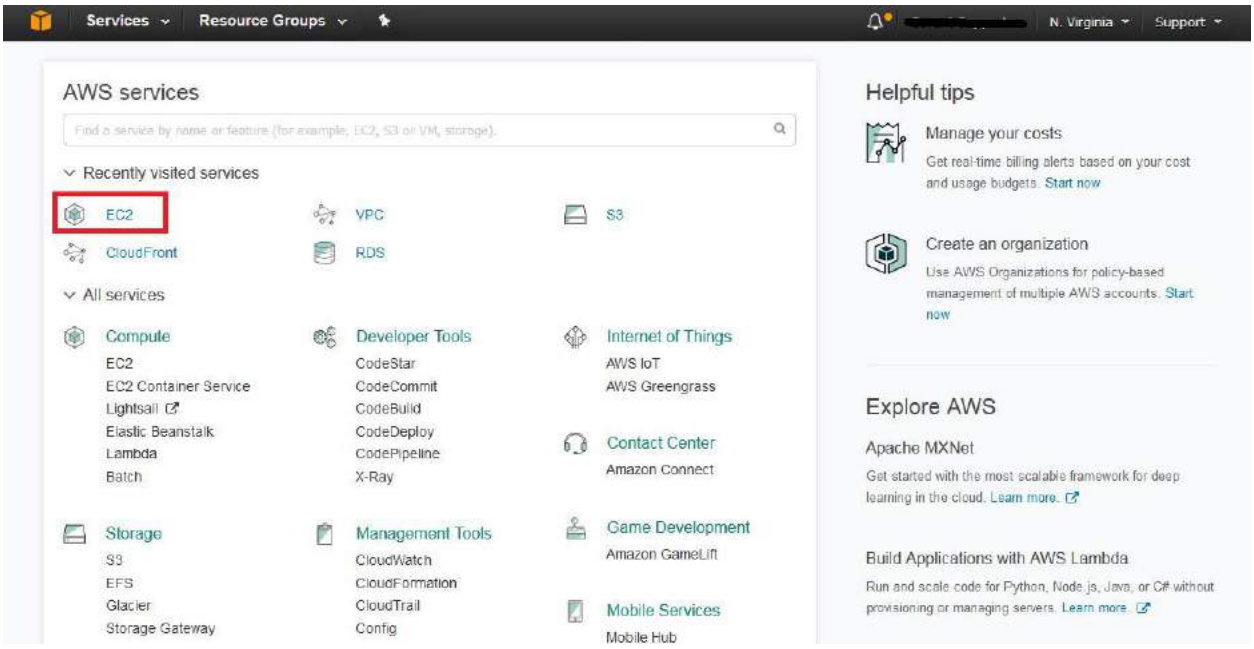
- Refer the below given URL for more information.
- http://searchservervirtualization.techtarget.com/definition/virtualization
- **Types of Virtualization:**
- Network virtualization
- Storage virtualization
- Server virtualization
- Data virtualization
- Desktop virtualization
- Application virtualization

AWS Overview

- In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. One of the key benefits of cloud computing is the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with your business. With the cloud, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly spin up hundreds or thousands of servers in minutes and deliver results faster.
- Today, AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.

EC2 (Elastic Compute Cloud):

- After creation of new account, sign in to AWS Console using the credentials which has been used for account creation.
- Once logged into AWS account, first screen would be Dashboard Screen as like shown below.
- EC2 is divided into two Types:
- Classic – Servers would be running in different network.
- VPC (Virtual **Private Cloud)** – Servers would be running in same network.

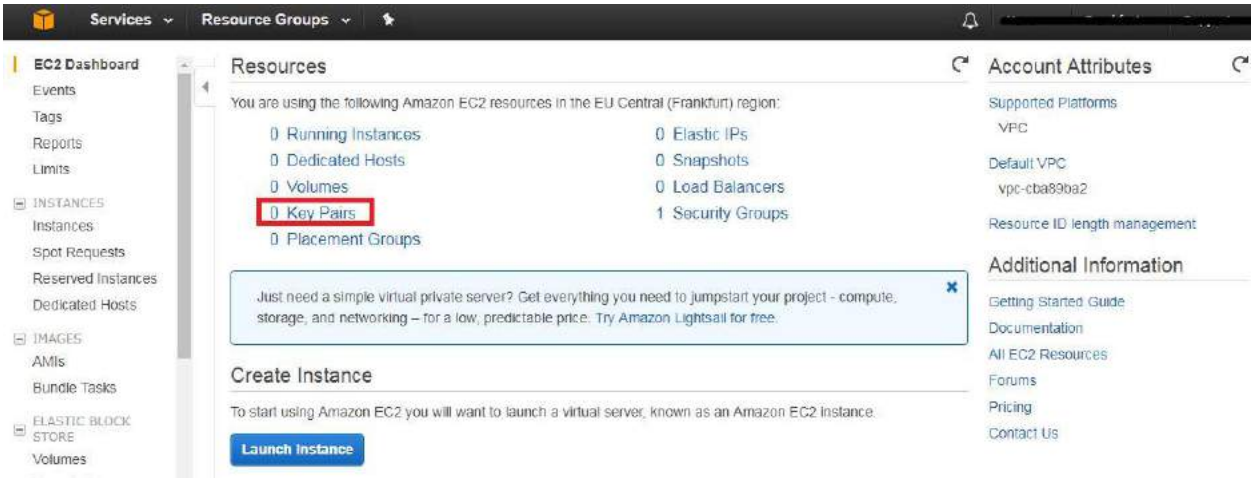


- Under EC2, find the below given sub modules.

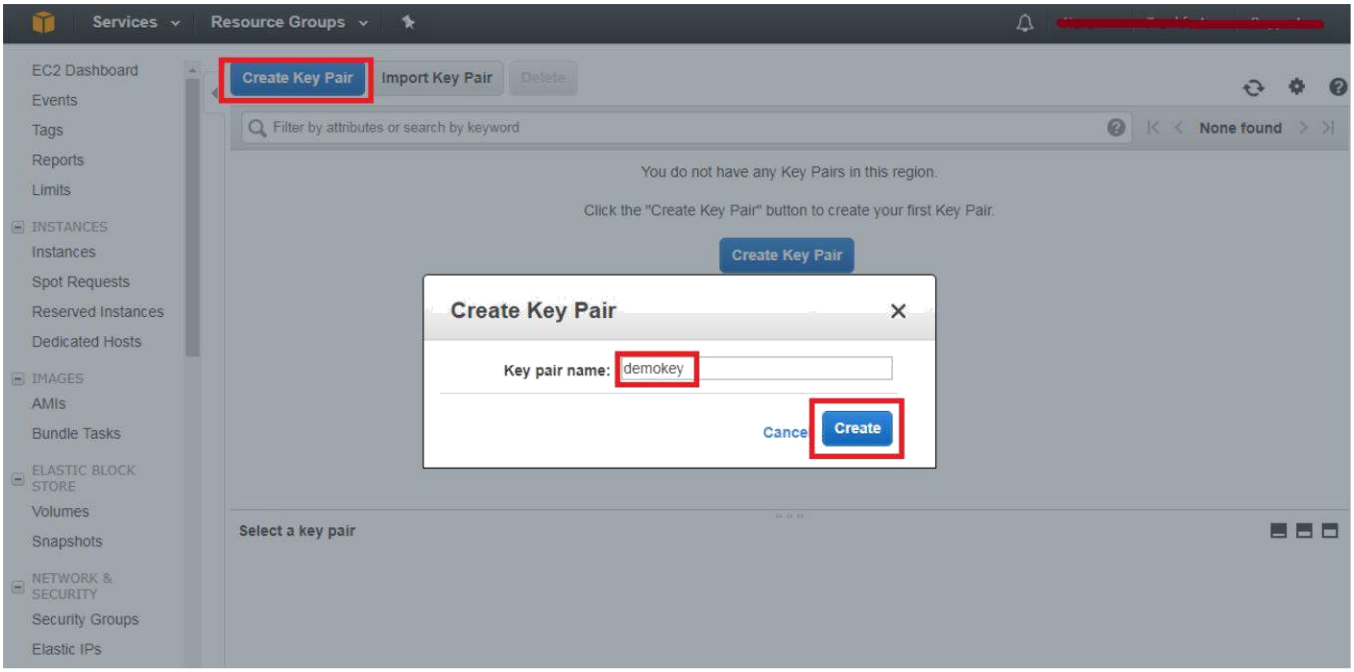
- **Instances** – Servers can be created in Windows as well as in Linux Platform.
- **KeyPairs** – It is used to get the password for Windows Servers and converting into PPK file for authenticating Linux Servers.
- **AMI's** – Amazon Machine Images would help to capture an image of the server as it is and new server can be launched from this captured image at any point of time.
- **Elastic IP's** – Elastic IP addresses are used to reserve the IP address as a Static One and it wouldn't be changed even if we stop and Start the servers.
- **Security Groups** – It is used to open respective port numbers to be communicable from created server. It has Custom / My IP and Anywhere.
- **Placement Groups** - A placement group is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.
- **Dedicated Hosts** - An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Windows Server, Microsoft SQL Server, SUSE, Linux Enterprise Server, and so on.

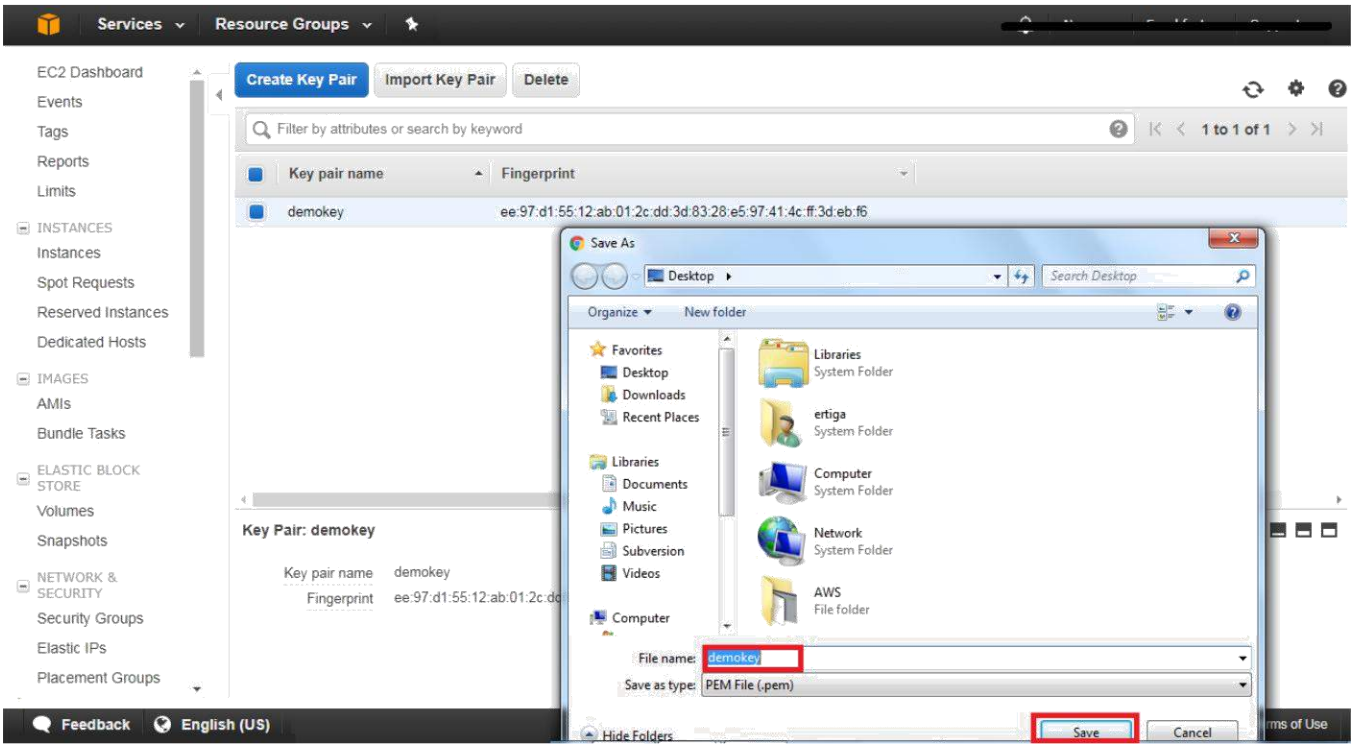
KeyPairs:

- Navigate to EC2 Dashboard, Click on KeyPairs Section.



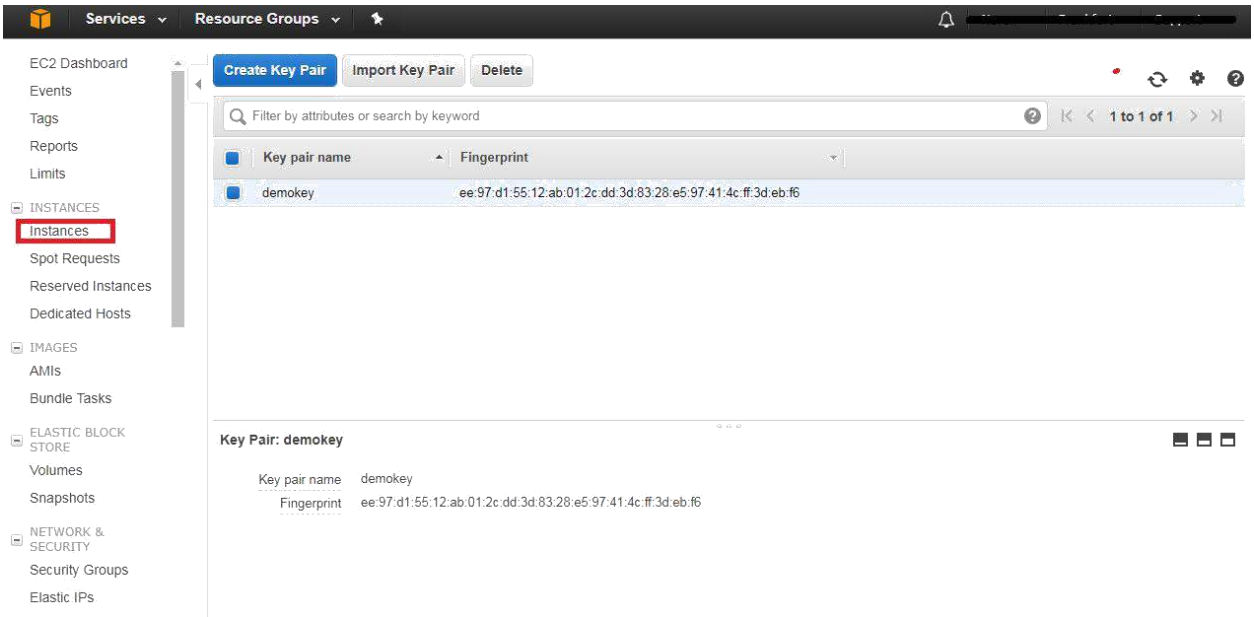
- Click on Create Key Pair and provide any name for the key pair.
- After providing a name, click on Create and download the KeyPair file which can be used for authenticating both Windows and Linux Servers.
- Find the below given screenshots for your easy reference.



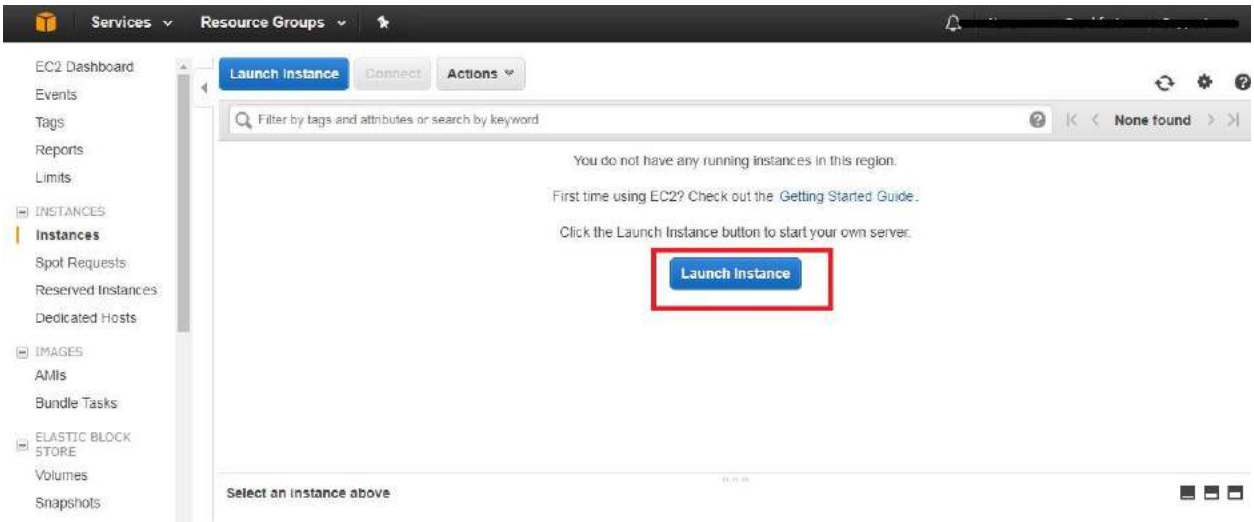


Instances:

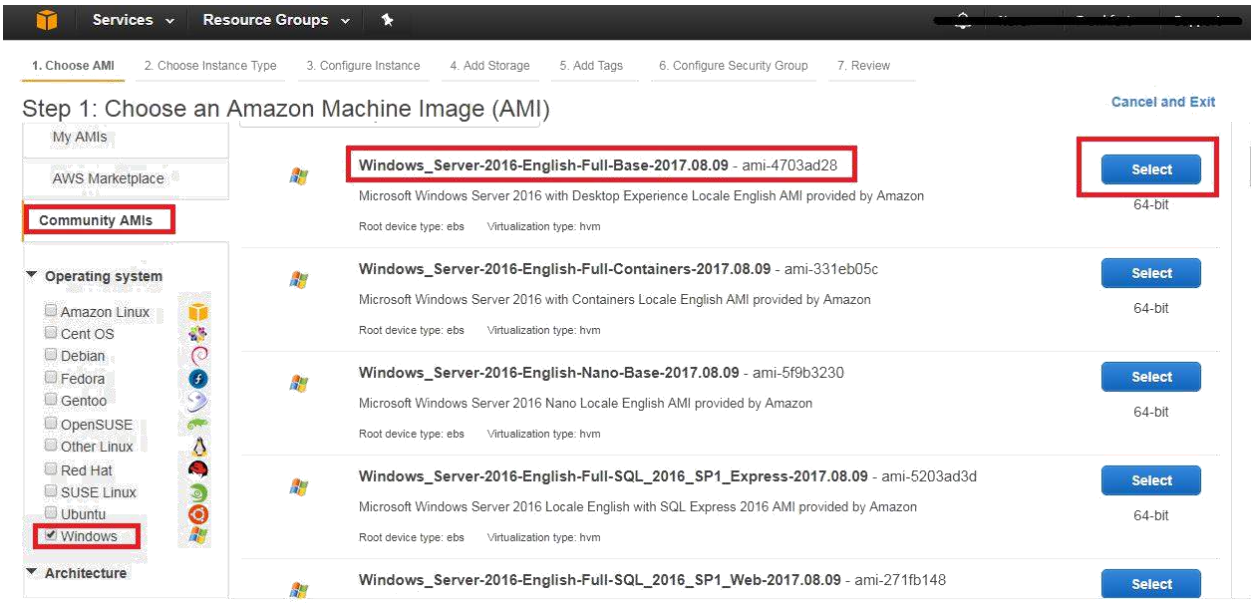
- After creating a KeyPair file, navigate to Instances as like below screenshot



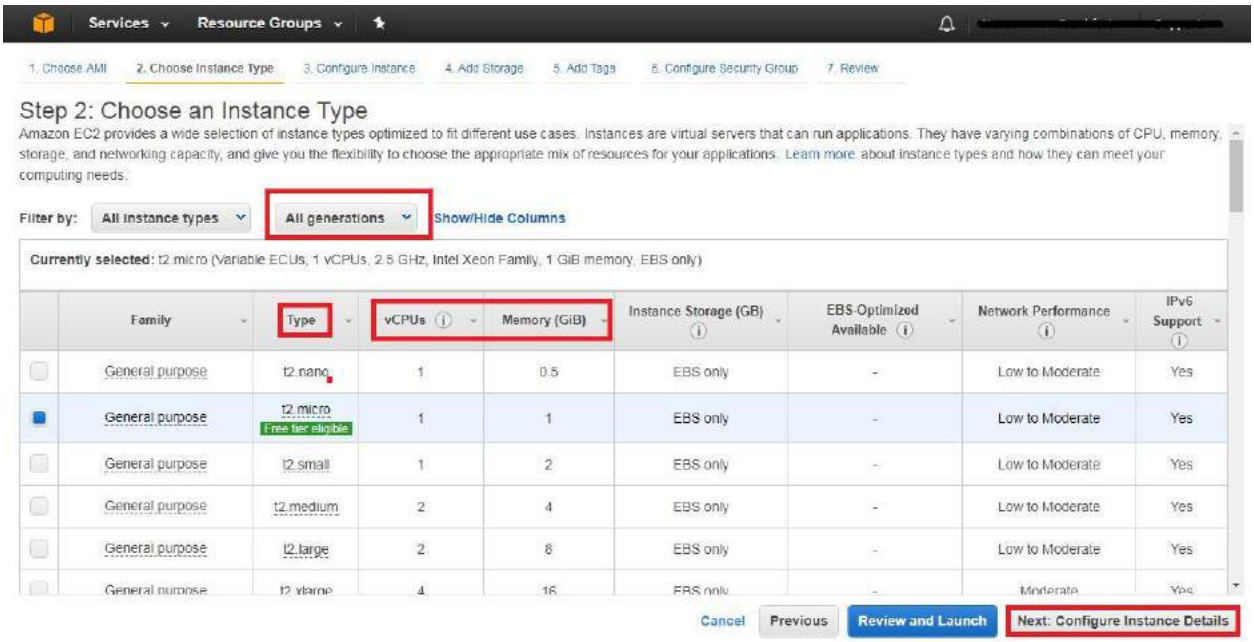
- Click on Launch Instances for creating a new server in EC2 Classic as like below screenshot.



- Navigate to Community AMI, Select an Operating System and AMI to create a new server as like given below.
- My AMIs is an option, where you could find the list of AMI which was created in your account.
- AWS Marketplace is another option to select any kind of IaaS / SaaS / PaaS from third parties who pushed their items in marketplaces.

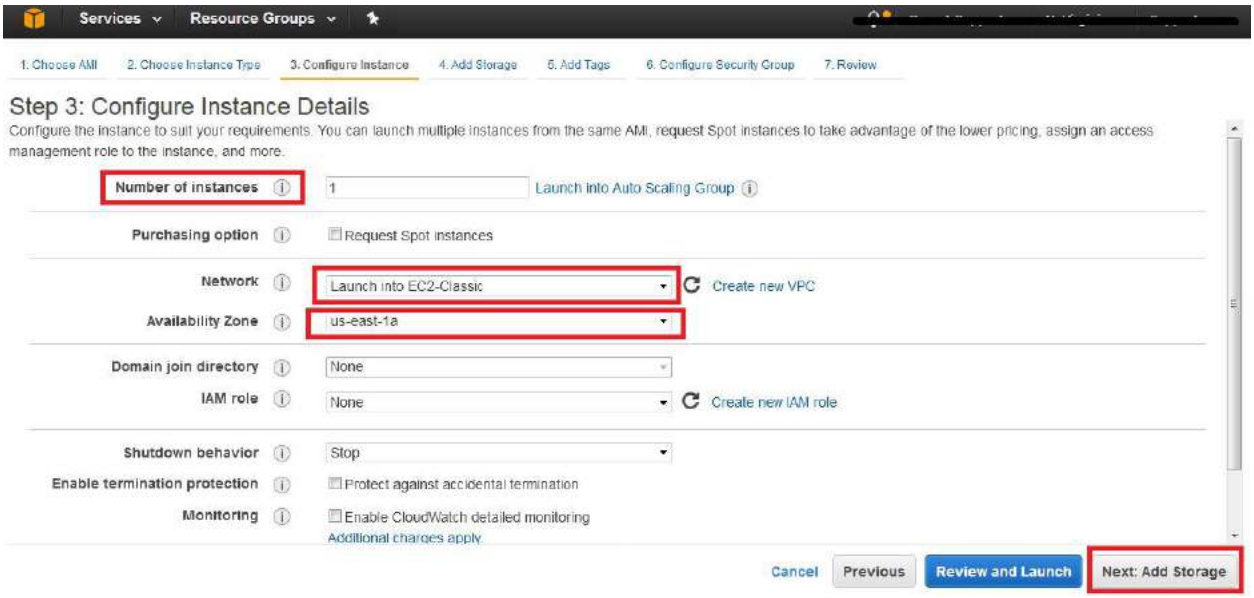


- After Selecting an Operating System, need to choose the configurations based on application requirements.
- Some Instance Flavors are supported only for VPC, some are supported only for Classic and few flavors are supported for both VPC and EC2.



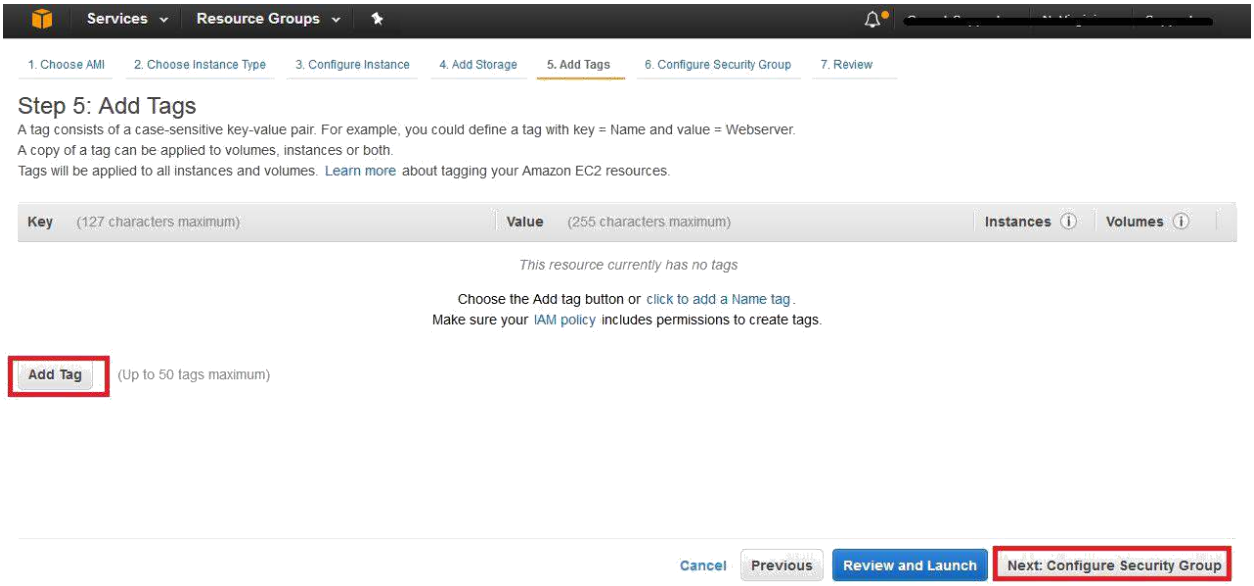
- After selecting an instance flavor, choose the network of instance whether to launch in EC2 Classic or VPC. For demo purpose, am launching an instance in EC2 Classic by choosing an instance flavor m3.medium (1 vCPUs & 3.75GB RAM).

- Availability Zone – It is said as to be, under one specific region, availability zones would be categorized. For Example, Under Chennai we are naming it as North / South Chennai.

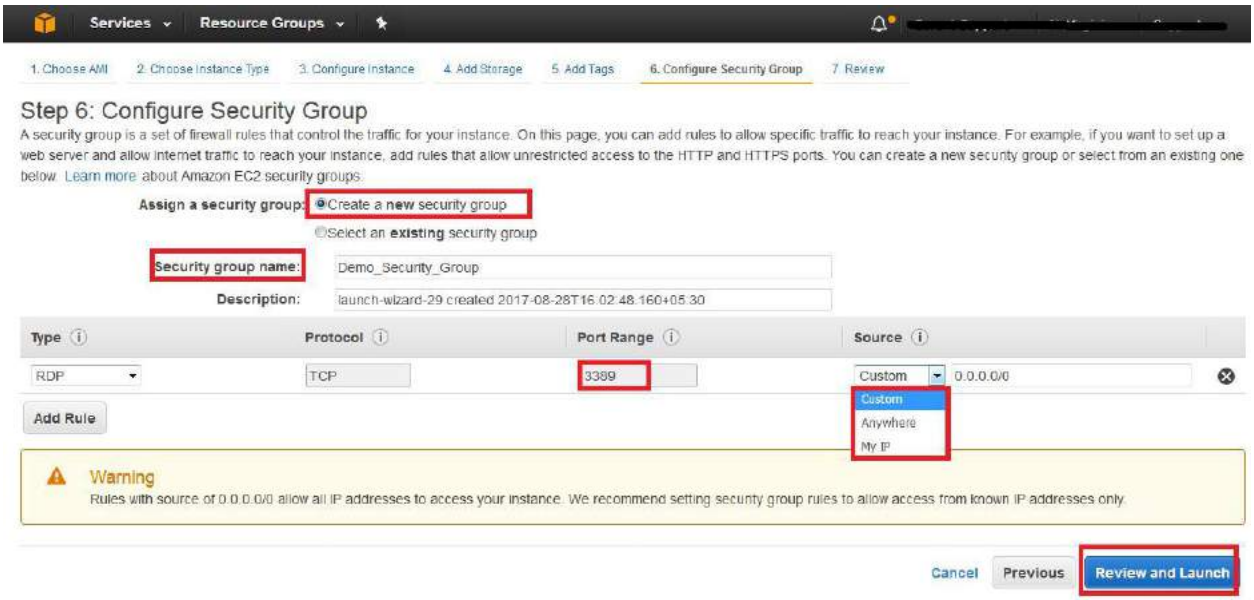


- Provided the necessary Storage Space which is required on the server. In this, Root would be acting as C Drive and if any additional volume required on the server like D / E drive, you can select Add Volume to add the same. Find the below screenshot which gives you a clear information.

- Tags – Addition of Tags is for user reference. If we are maintaining huge amount of servers like 300 to 400 +, to get clear information on each server and each key pair, you could provide the tag name or else, it is not mandatory to provide the same. Refer the below screenshot for more information.

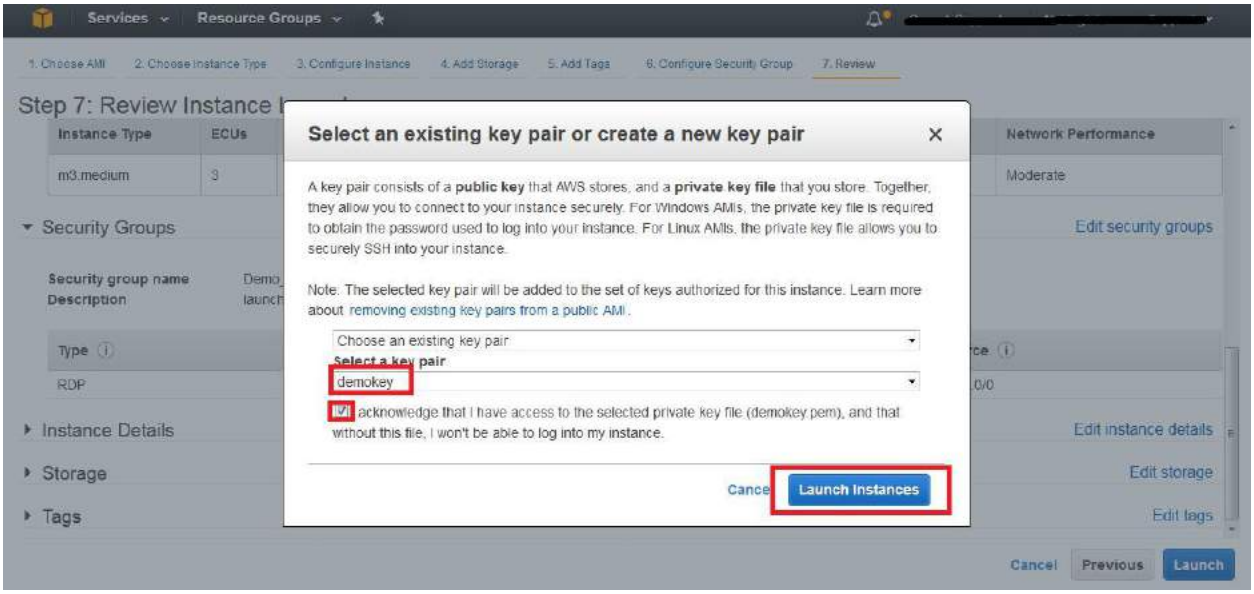


- In Security Group, you can open the necessary ports which are respective to your application. By default, RDP port 3389 for Windows and SSH 22 Ports for Linux needs to be opened for taking the remote control of newly launching server.
- If Custom is chosen in Source, port will be communicable only to the subnet which you had provided.
- If Anywhere is chosen, it can be communicable across the globe.
- If MyIP is chosen, port will be communicable only to your computer.

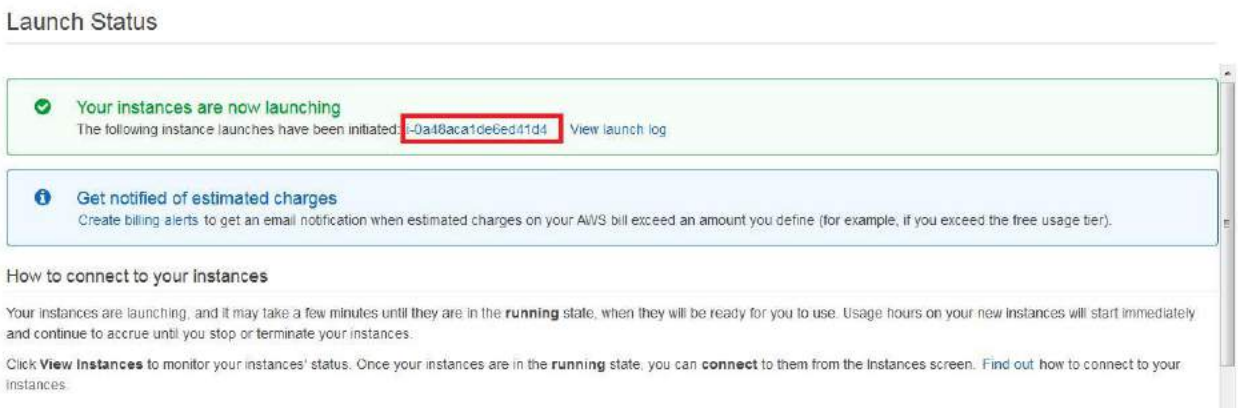


- Click on Review and Launch to choose a created KeyPair. After Selecting the KeyPair, acknowledge to terms and conditions which is provided by AWS as like given below.

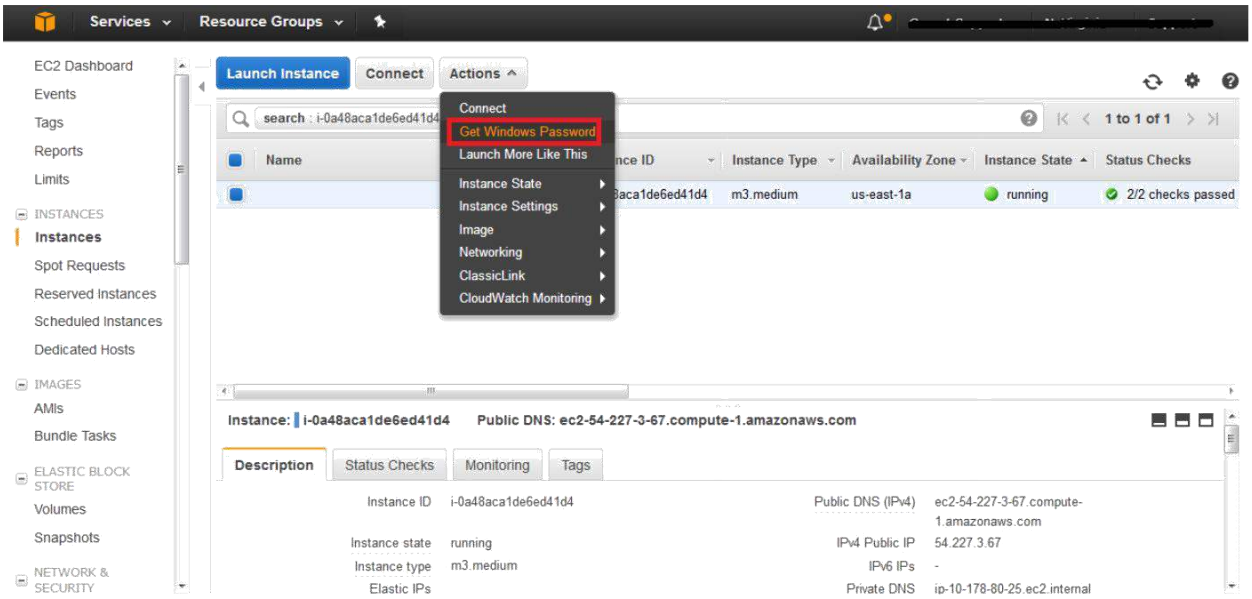
- After clicking on Launch Instances, a new server would be provisioned with configurations which have been selected above.

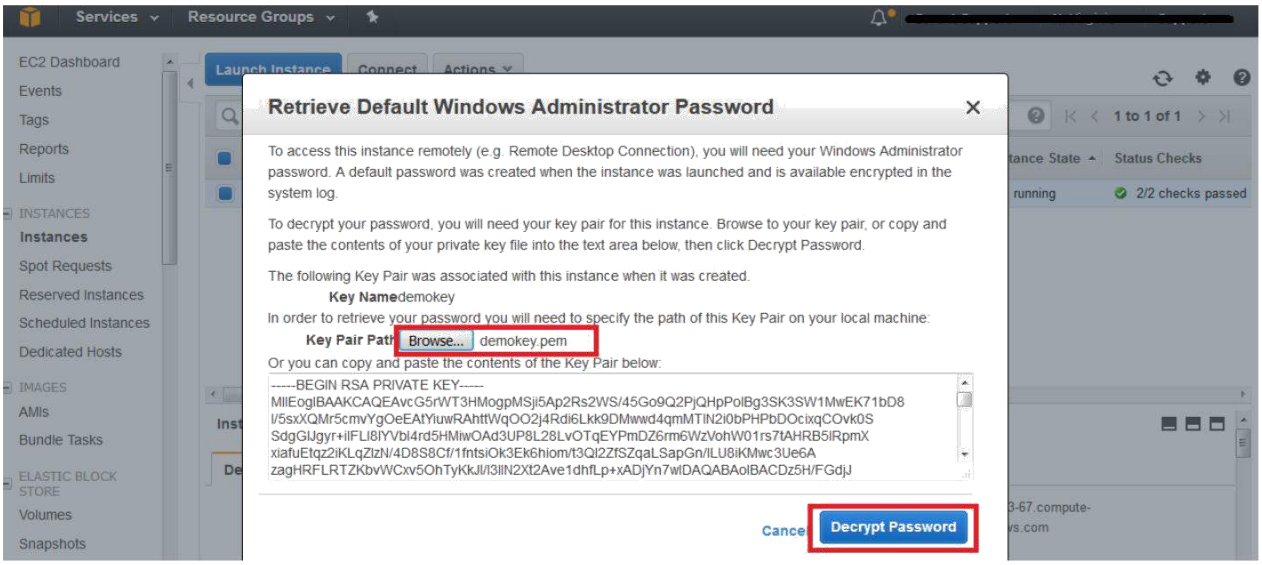


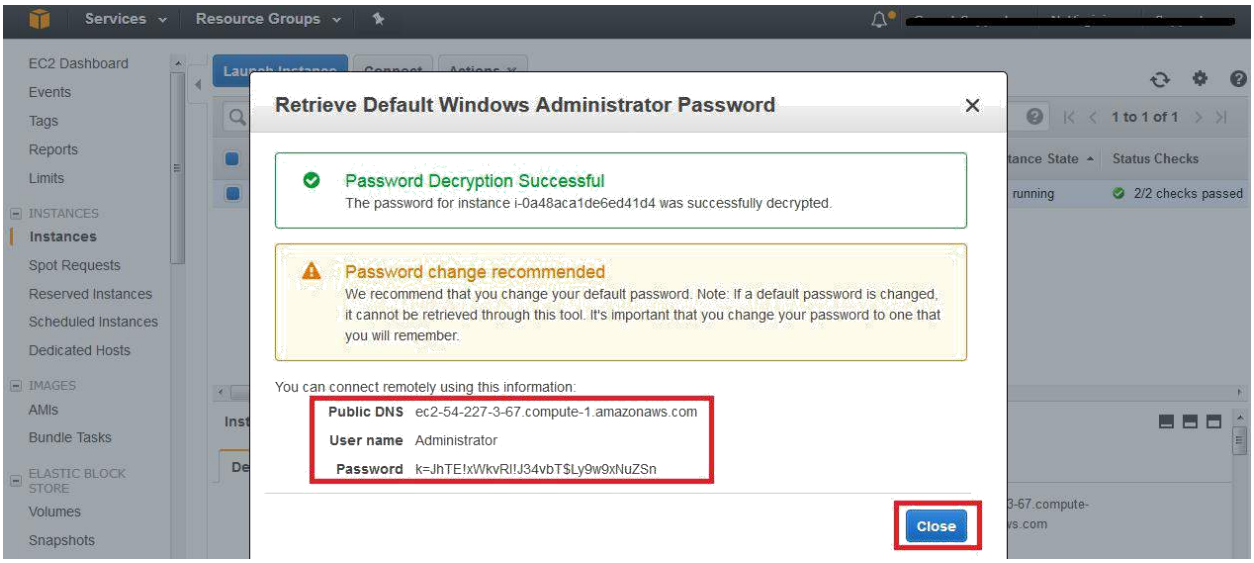
- Instance provisioning is in progress and click on Instance ID to view the status of instance as like given below.



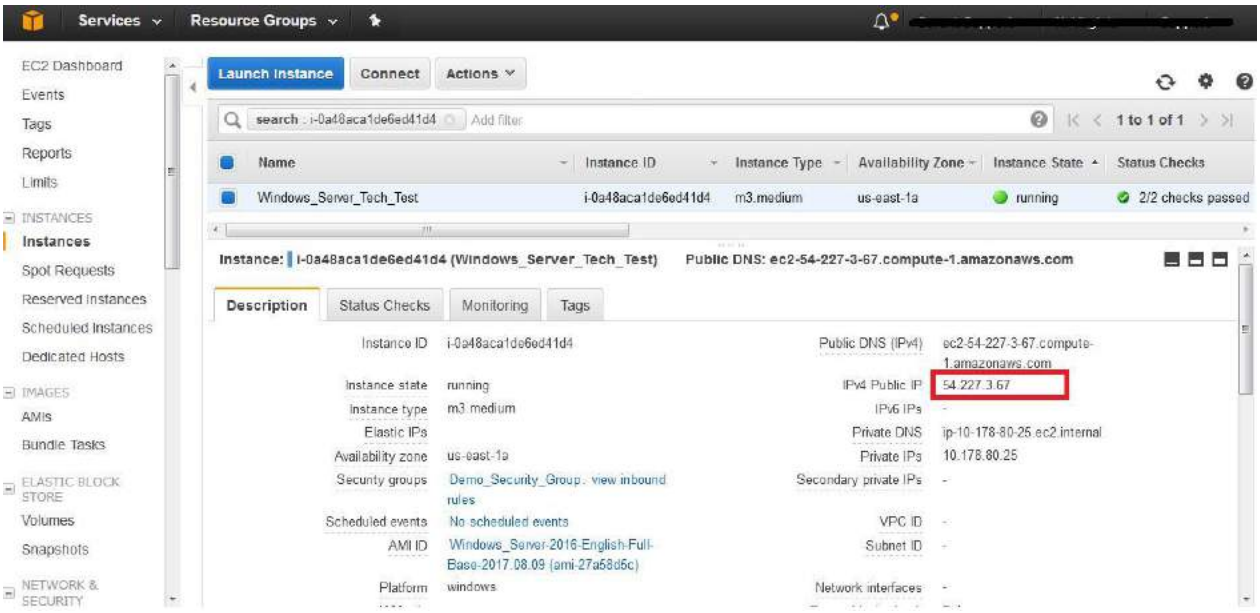
- Click on Actions >> Get Windows Password to get an authentication of newly launched server as like shown below.
- Once you click on Get Windows Password, upload the Key Pair file, which has been used during server creation, and click on decrypt password.
- Save an authentication in notepad file, which would helpful, while logging into newly launched server.


Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Launch Instance
Connect
Actions
Connect
Get Windows Password
Launch More Like This
Instance State
Instance Settings
Image
Networking
ClassicLink
CloudWatch Monitoring
search : i-0a48aca1de6ed41d4
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
m3.medium
us-east-1a
running
2/2 checks passed
Instance: i-0a48aca1de6ed41d4
Public DNS: ec2-54-227-3-67.compute-1.amazonaws.com
Description
Status Checks
Monitoring
Tags
Instance ID
i-0a48aca1de6ed41d4
Instance state
running
Instance type
m3.medium
Elastic IPs
Public DNS (IPv4)
ec2-54-227-3-67.compute-1.amazonaws.com
IPv4 Public IP
54.227.3.67
IPv6 IPs
-
Private DNS
ip-10-178-80-25.ec2.internal


Services
Resource Groups
Retrieve Default Windows Administrator Password
To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.
To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.
The following Key Pair was associated with this instance when it was created.
Key Name demokey
In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:
Key Pair Path
Browse...
demokey.pem
Or you can copy and paste the contents of the Key Pair below:
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvcG5rWT3HMogpMSji5Ap2Rs2WS/45Go9Q2PjQHpPolBg3SK3SW1MwEK71bD8
I/5sxXQMr5cmvYgOeEAtYiuwRAhttWqOO2j4Rdi6Lkk9DMwwd4qmMTIN2i0bPHPbDOcixqCOvk0S
SdgGIJgyr+iIFLI8IYVbI4rd5HMiwOAd3UP8L28LvOTqEYPmDZ6rm6WzVohW01rs7tAHRB5IRpmX
xiafuEtqz2iKLqZlzN/4D8S8Cf/1fntsiOk3Ek6hiom/t3QI2ZfSZqaLSapGn/ILU8iKMwc3Ue6A
zagHRFLRTZKbvWCxv5OhTyKkJI/I3IIN2Xt2Ave1dhfLp+xADjYn7wIDAQABAoIBACDz5H/FGdjJ
Cancel
Decrypt Password

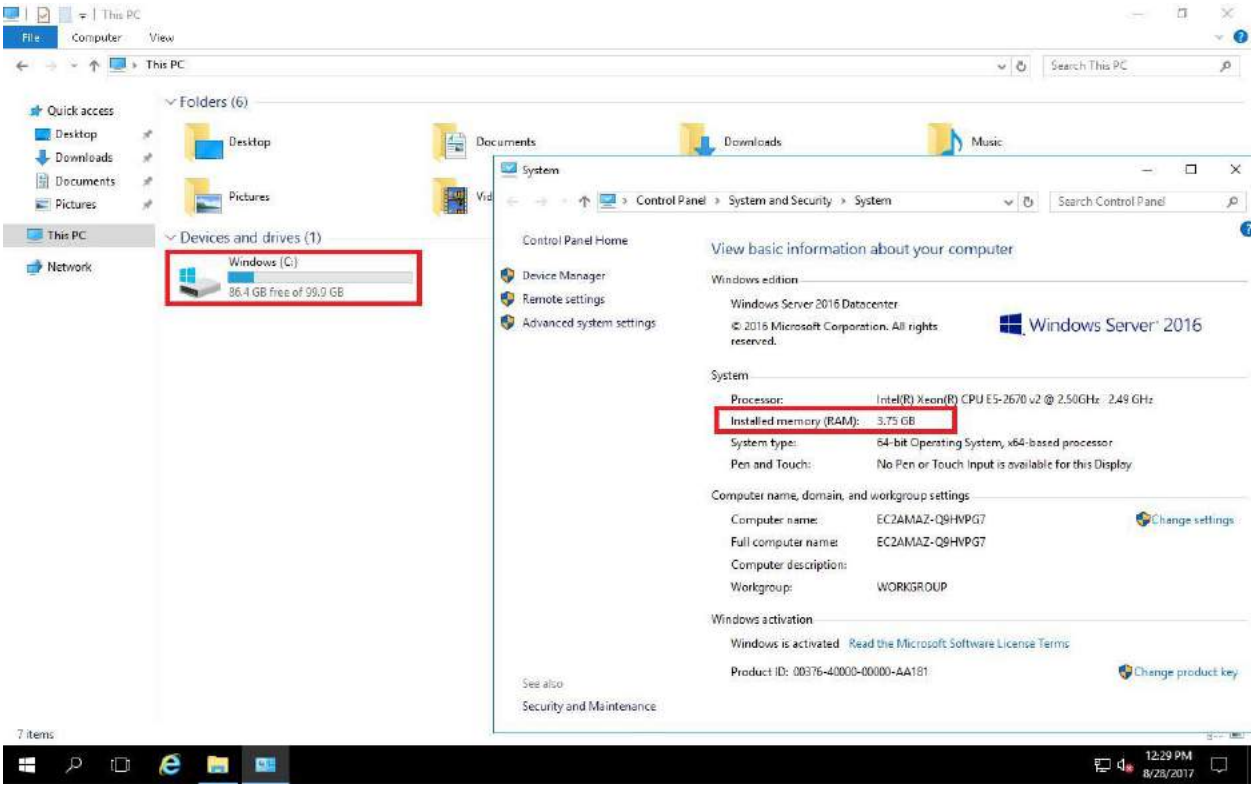


- After generating the password, Copy the Public IP address to take the RDP of the launched server.



- Click on Start Menu in your PC, type Remote Desktop Connection for taking RDP of the server.
- Provide the IP address, Username and the password of created server to logging into the same.

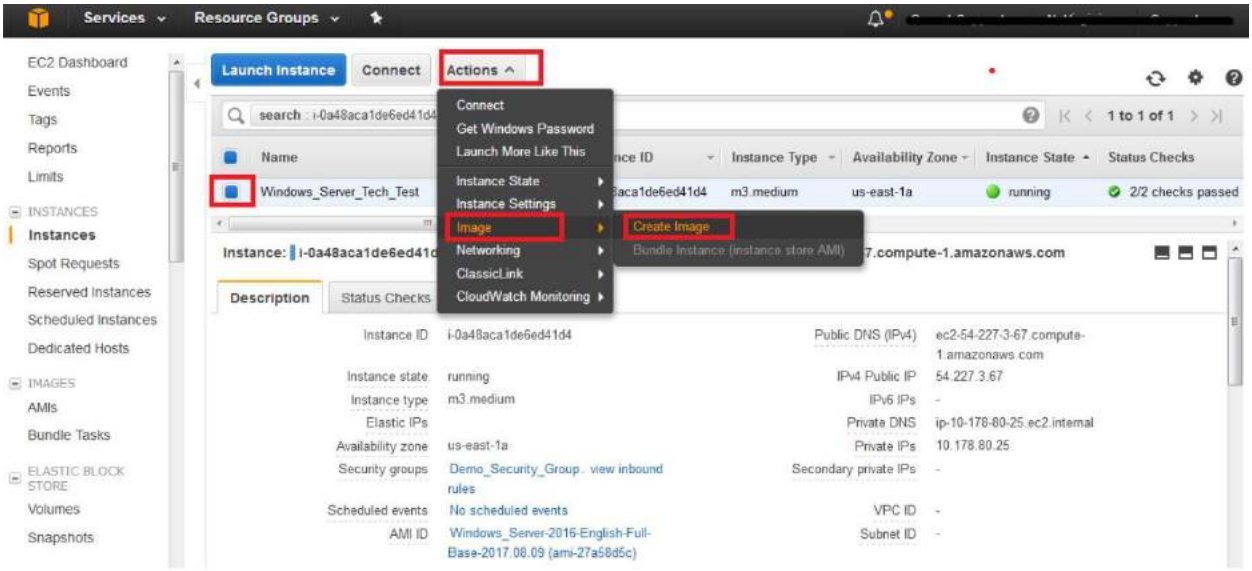
- After logged into the server, ensure the Hard Disk Size and RAM which is available on created server just to confirm whether an instance has been launched from chosen instance flavor as shown below.

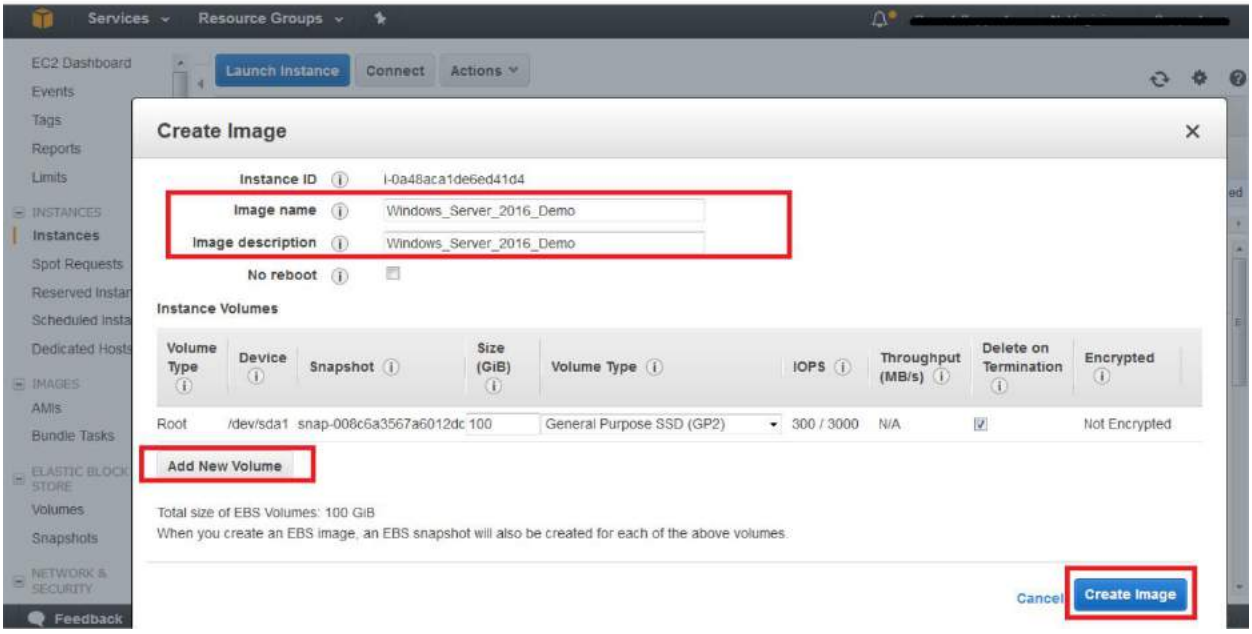


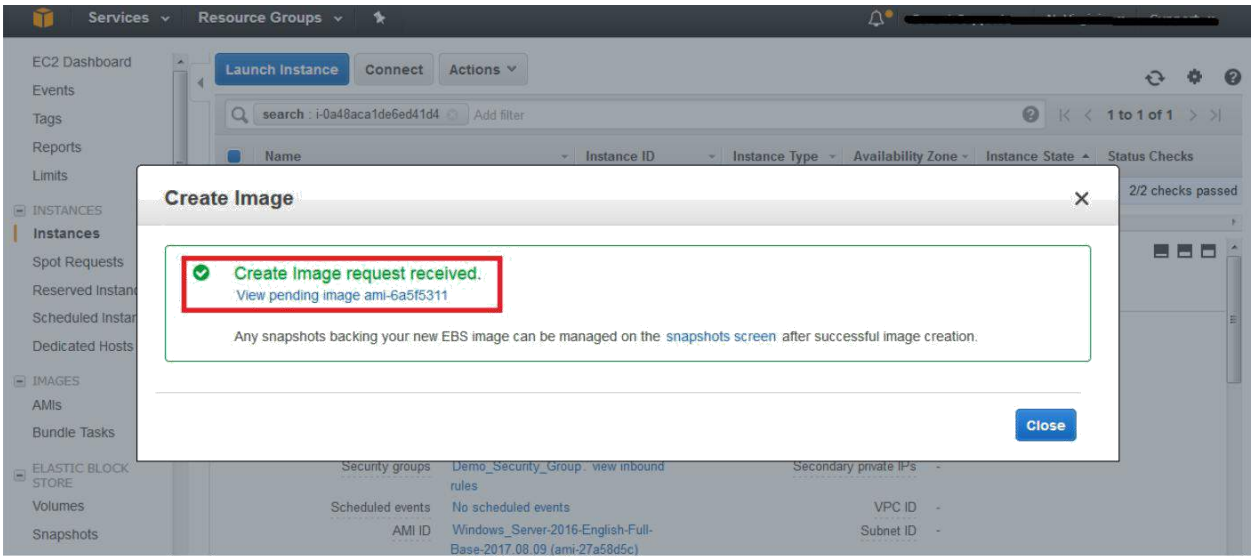
AMIs (Amazon Machine Image):

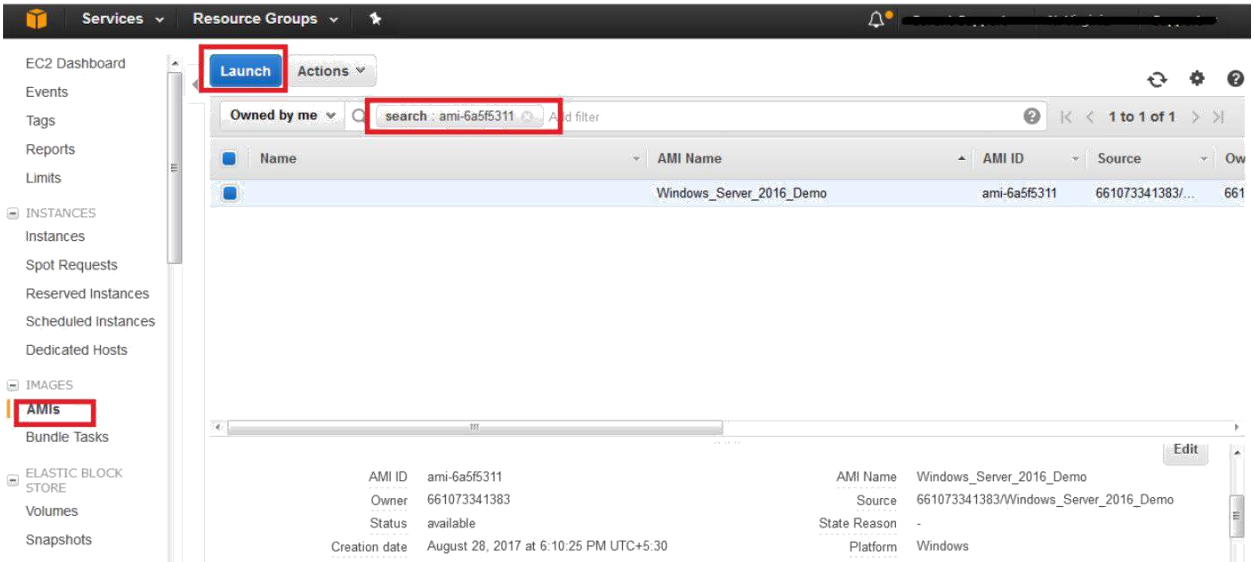
- Amazon Machine Image used to capture a server as an image and it can be launched any time whenever we would require.

- Same kind of instance as like it was while taking an image, would be launched in AWS if we click on create a new instance from captured image.
- Select an instance which you would like to capture it as an image. Click on Actions >> Image >> Create Image
- Provide an image name and description of the same. If required to add any additional volume, click on Add Volume to add any additional storage.
- After Clicking on Create Image, AMI ID would be generated.
- Image creation would take 15 to 20 mins of time. Once an image is created, you would be able to launch multiple instances from the captured image.
- Once an Image has been created, new instance can be created by clicking on Launch Instance, followed by same steps for creating a new server.





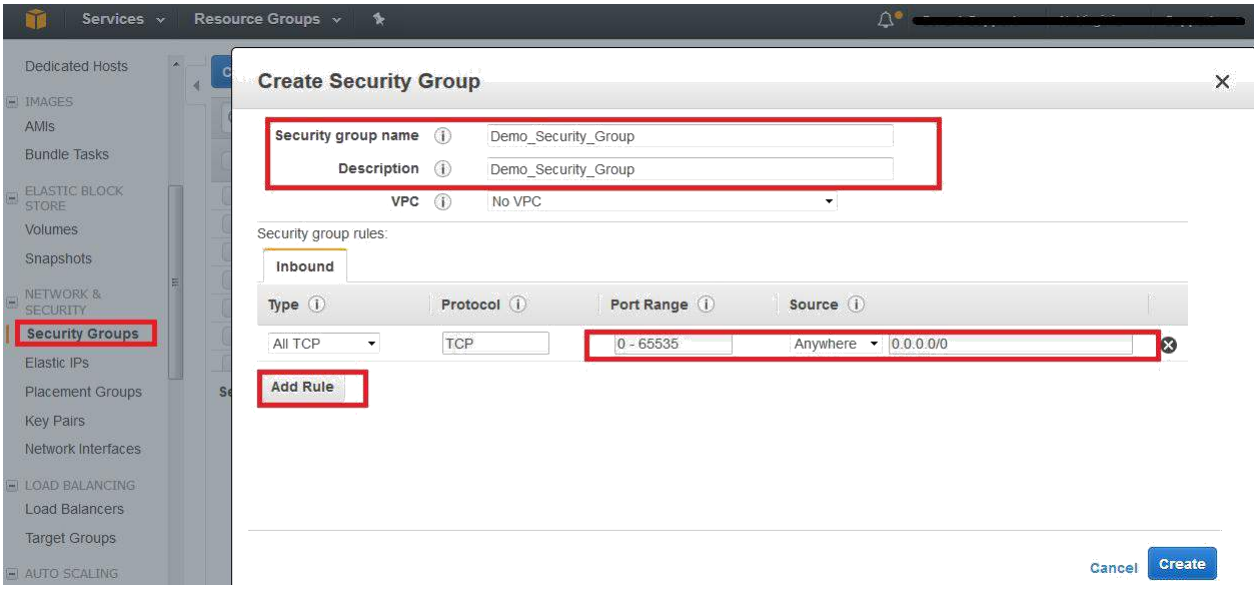




- If new server has been launched from captured image, same credentials of original server needs to be used, in which you have been captured it as an image.

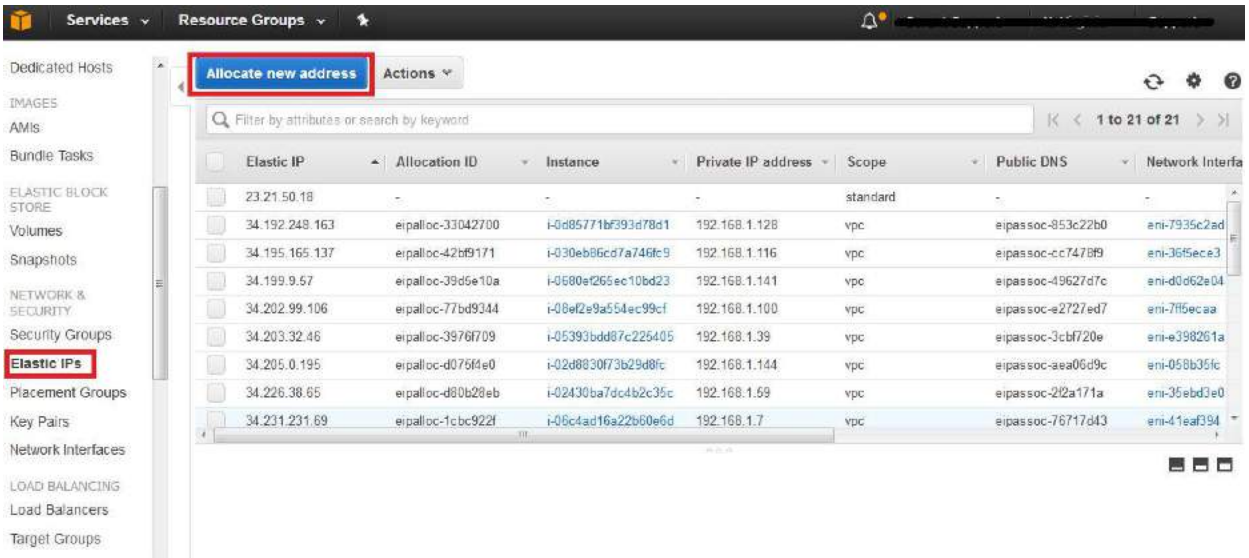
Security Groups:

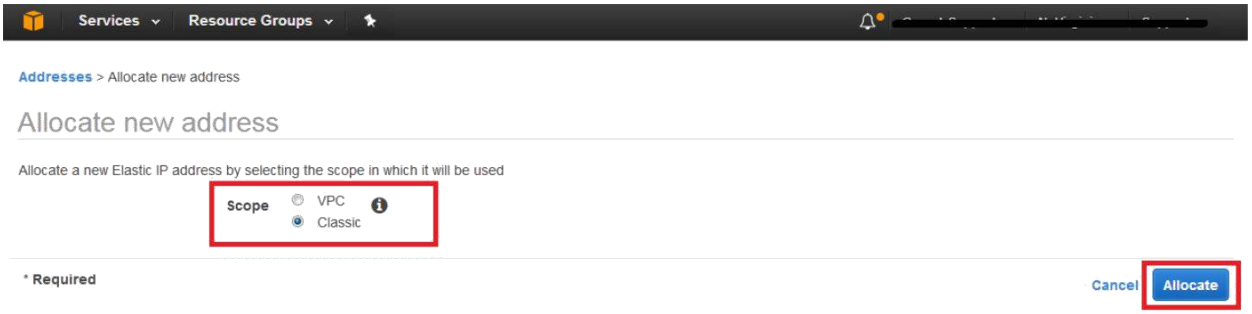
- In Security Group, you can open the necessary ports which are respective to your application. By default, RDP port 3389 for Windows and SSH 22 Ports for Linux needs to be opened for taking the remote control of newly launching server.
- If Custom is chosen in Source, particular port will be communicable only to the subnet which you had provided.
- If Anywhere is chosen, it can be communicable across the globe.
- If MyIP is chosen, particular port will be communicable only to your computer.

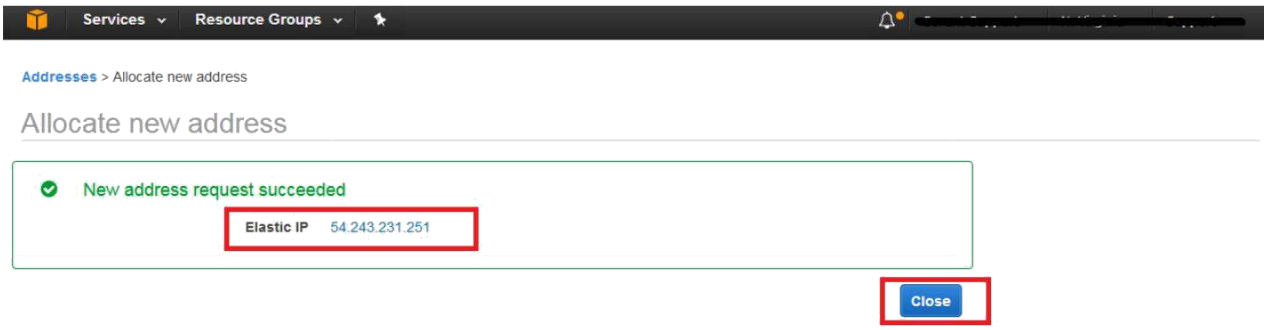


Elastic IP Address:

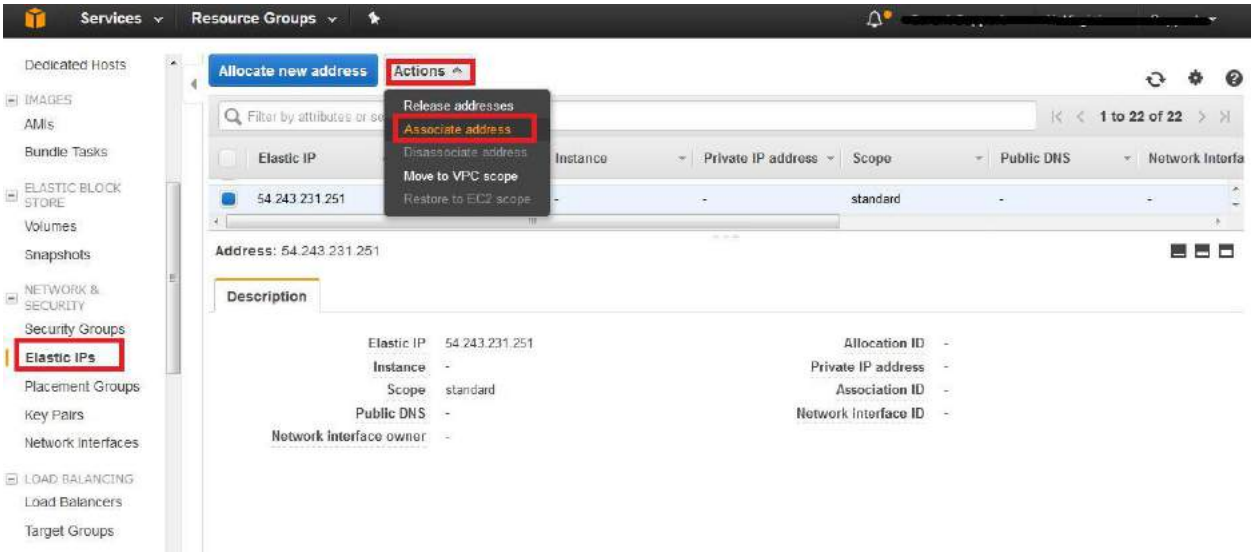
- Elastic IP address is used to reserve any specific IP address, so that it wouldn't be changed even if we stop and start the server.
- Once the server has been created, before deploying any application or sharing the server to end user, create a new Elastic IP Address and associate the same to the server which you have been created.
- Choose an elastic IP to be created for Classic or VPC and click on Associate.

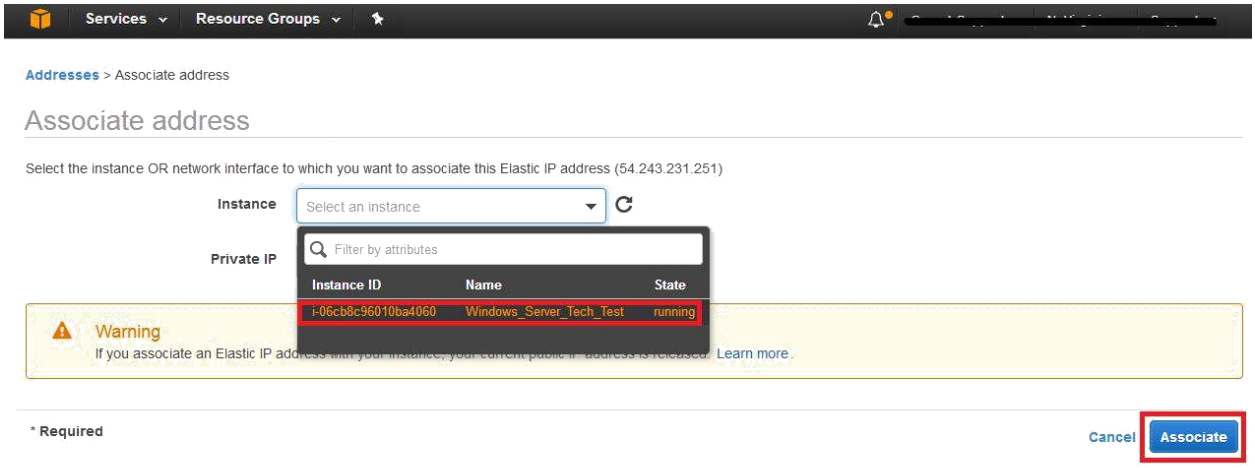






- After creation of new IP address, associate the same to newly created server as like
- shown below.





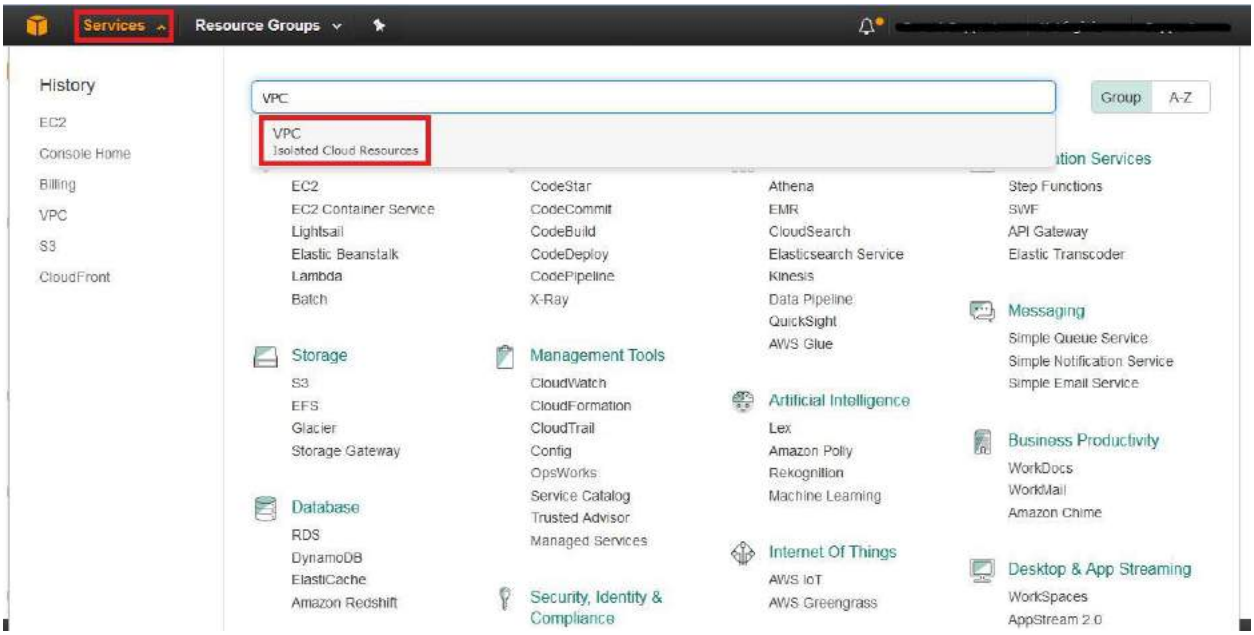
- After Assigning Elastic IP Address, you would be able to take the RDP of launched server with newly created IP address. Use the same credentials which has been used earlier.

Advantages on EC2 Instances:

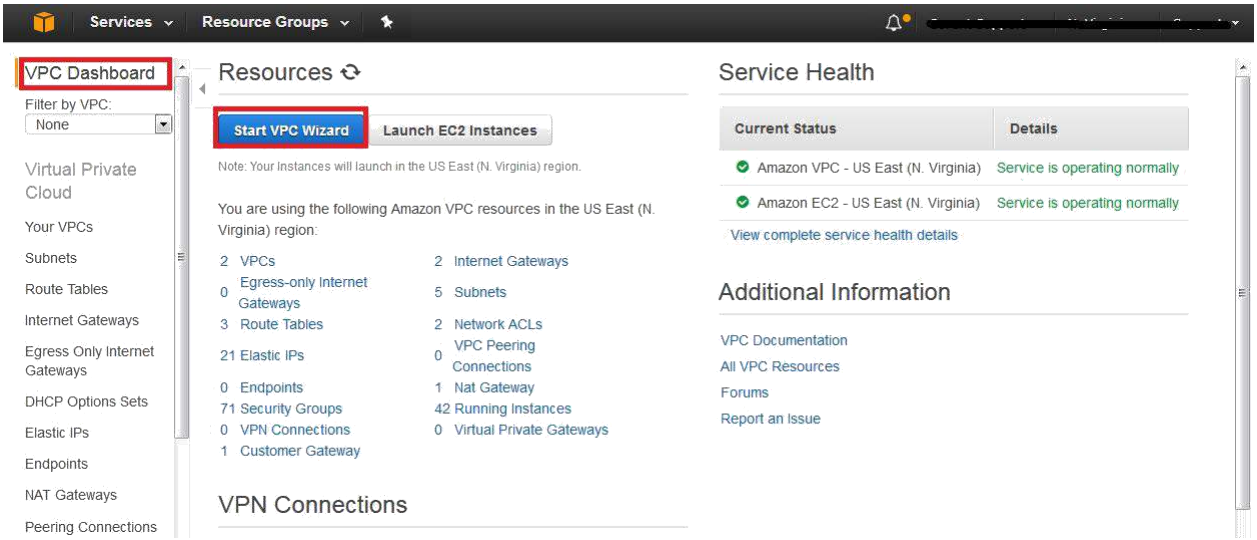
- Virtual Machines will be maintained by AWS.
- Time & Cost Saving.
- Power Supply.
- No possibility on disaster.
- Data will be secured.

Amazon VPC (Virtual Private Cloud):

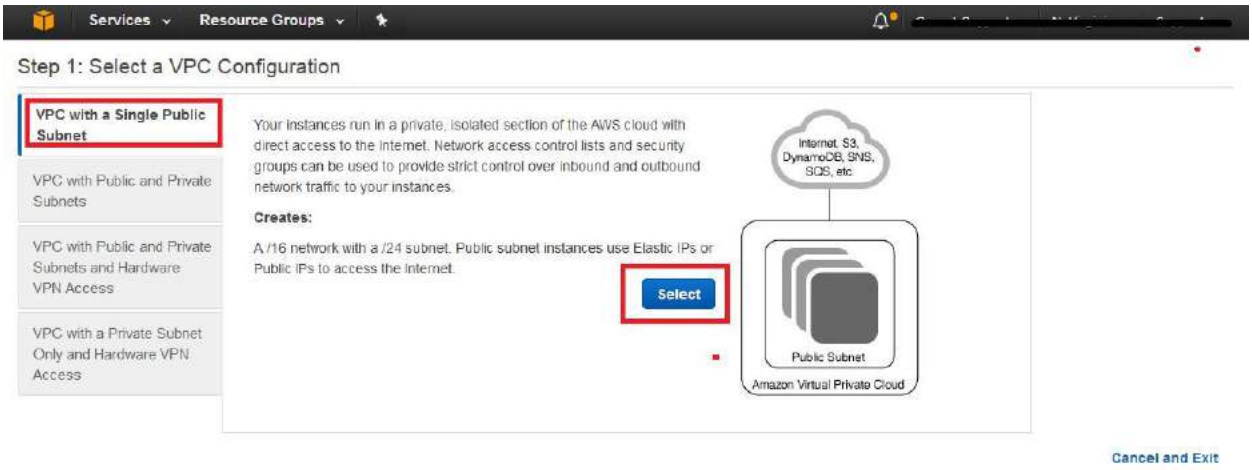
- Navigate to Services and Type VPC in search box.
- Choose the VPC for creating the same as like shown below.



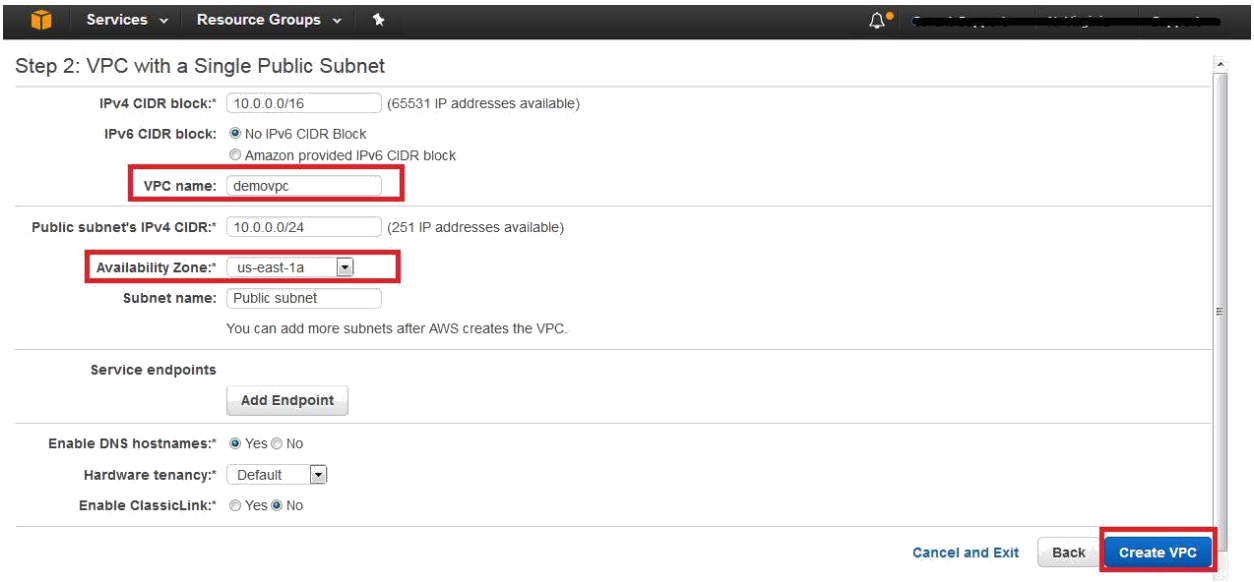
- After selecting VPC, dashboard screen will appear. Click on Start VPC Wizard to create a new VPC as like shown below.



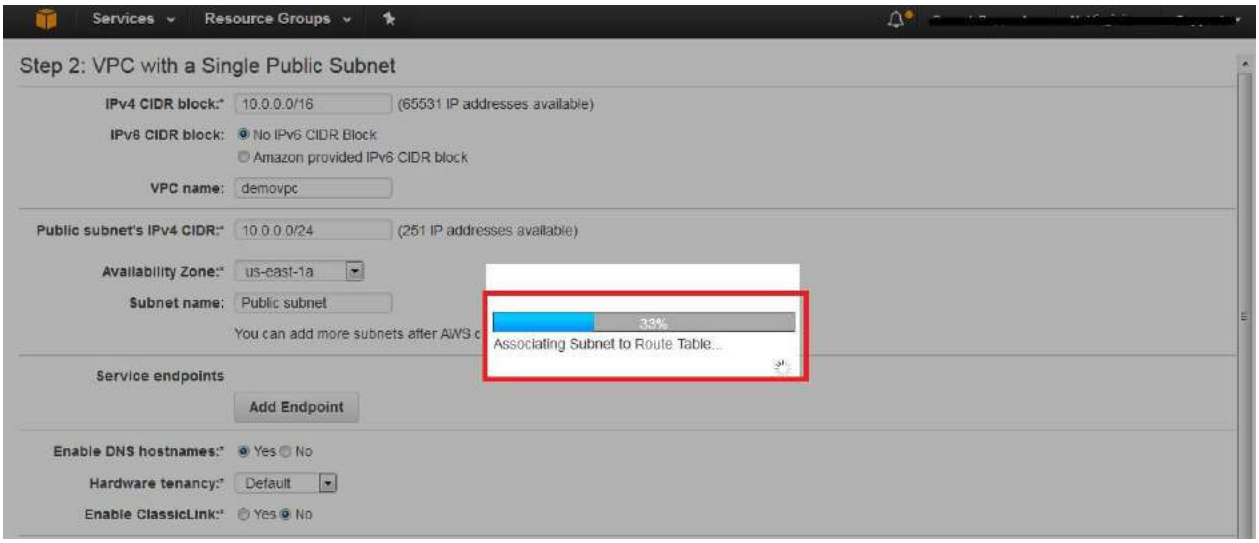
- Select a VPC Configuration based on your requirement and click on Select as shown below.



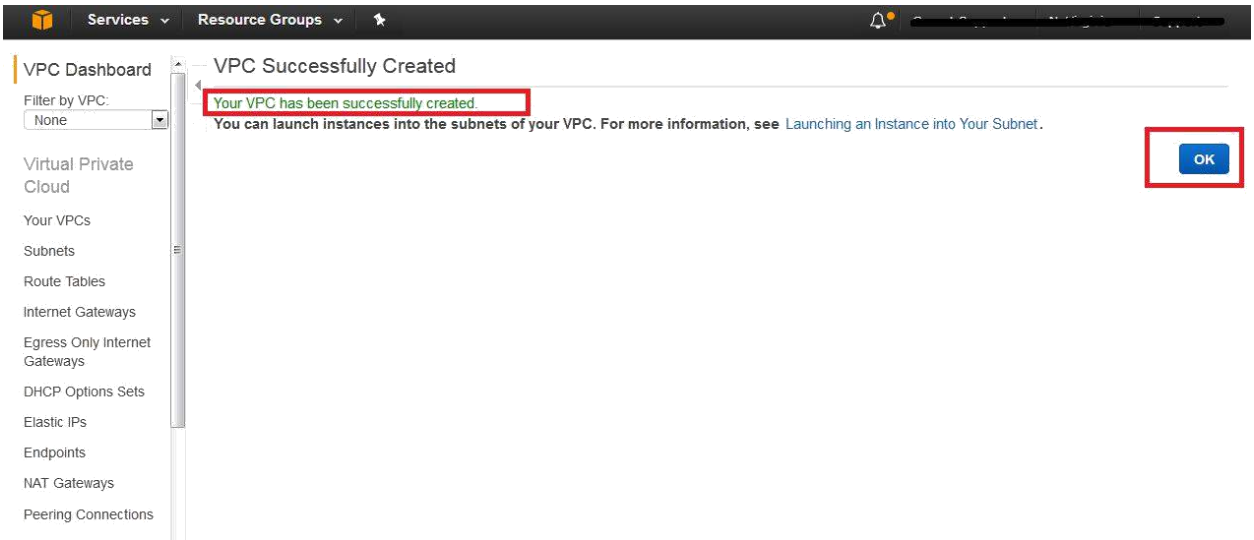
- If you require a VPC with one Subnet which has public access, you could choose first
- option. If you require both Public and Private Subnet, choose the second option. If
- you require both with Hardware VPN access, 3rd option can be chosen. If you would require only Private connection, 4th Option can be chosen and that Private Subnet would be accessible with VPN. Architecture diagram of 4 options can be seen in right side of the page.
- After selecting the configuration, provide the VPC name and choose the Availability Zone as like shown below.



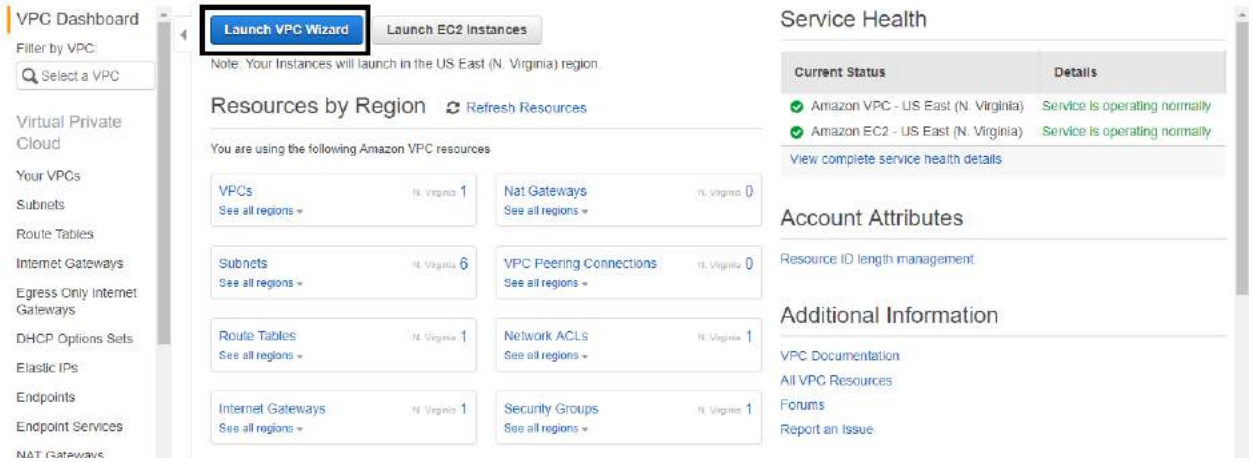
- After clicking on Create VPC, a new VPC wizard would be created along with Subnet & internet gateway as like shown below.



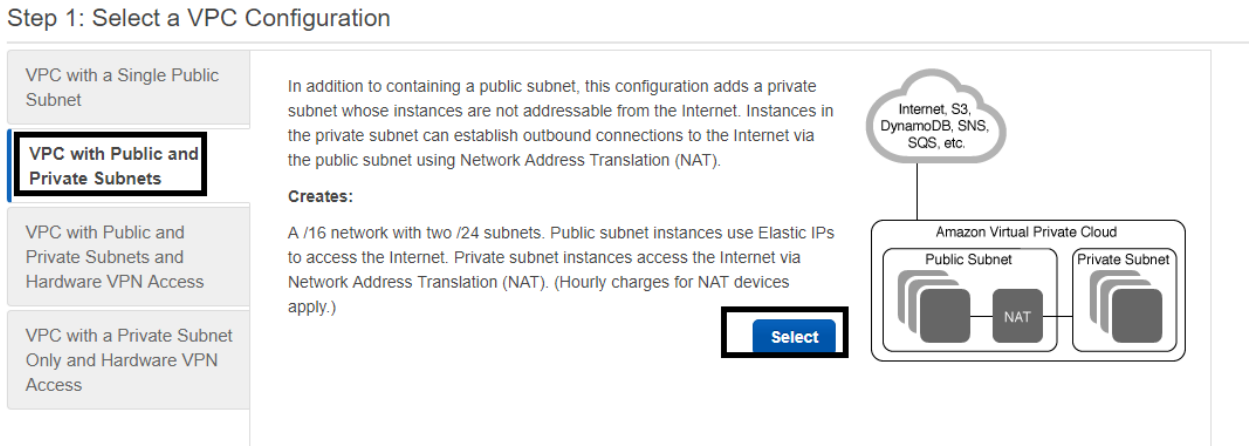
- After creation of VPC, proceed to launch a new server under EC2 VPC. Creation of new server is similar like as we seen earlier.



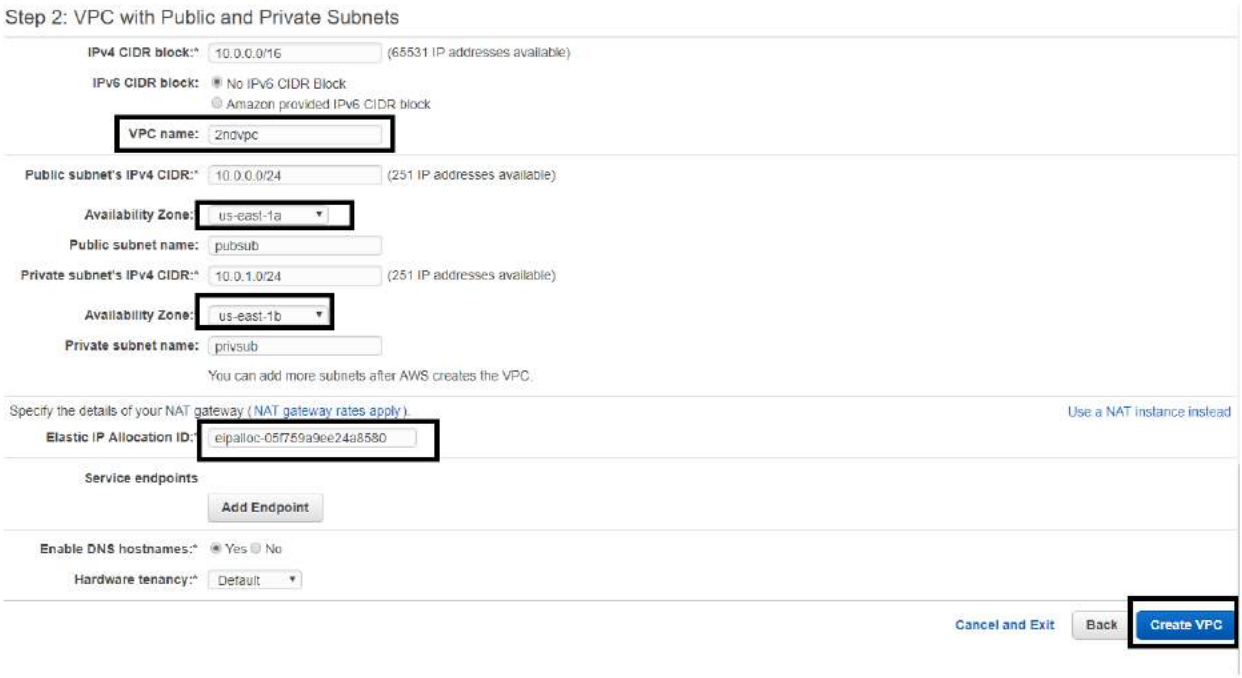
- Second VPC could be created using below screenshots.



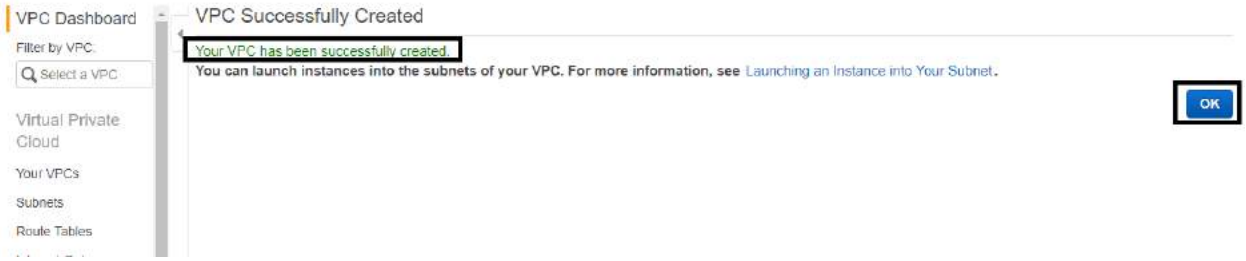
- Choose the second option of VPC whereas, one Public Subnet and One Private Subnet will be created.



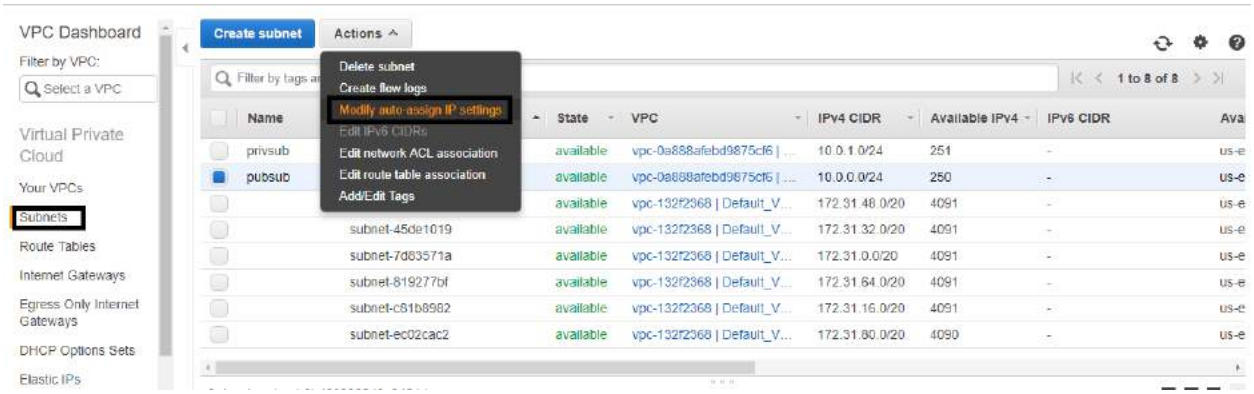
- Provide the name of the VPC, Subnets and choose the Availability zone to click on next. Since it is a second VPC, we would require one NAT (elastic IP address) which will be acting as a bridge to communicate between Public & Private Subnet.



- VPC has been created successfully.

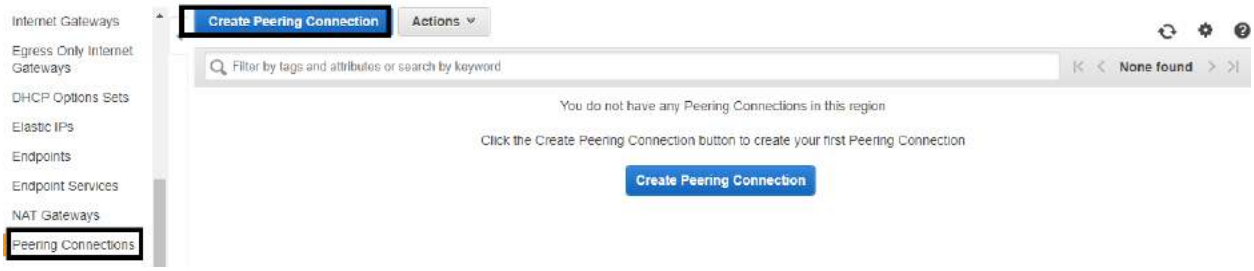


- To enable a public IP for the subnets, click on Actions and choose modify auto-assign IP.

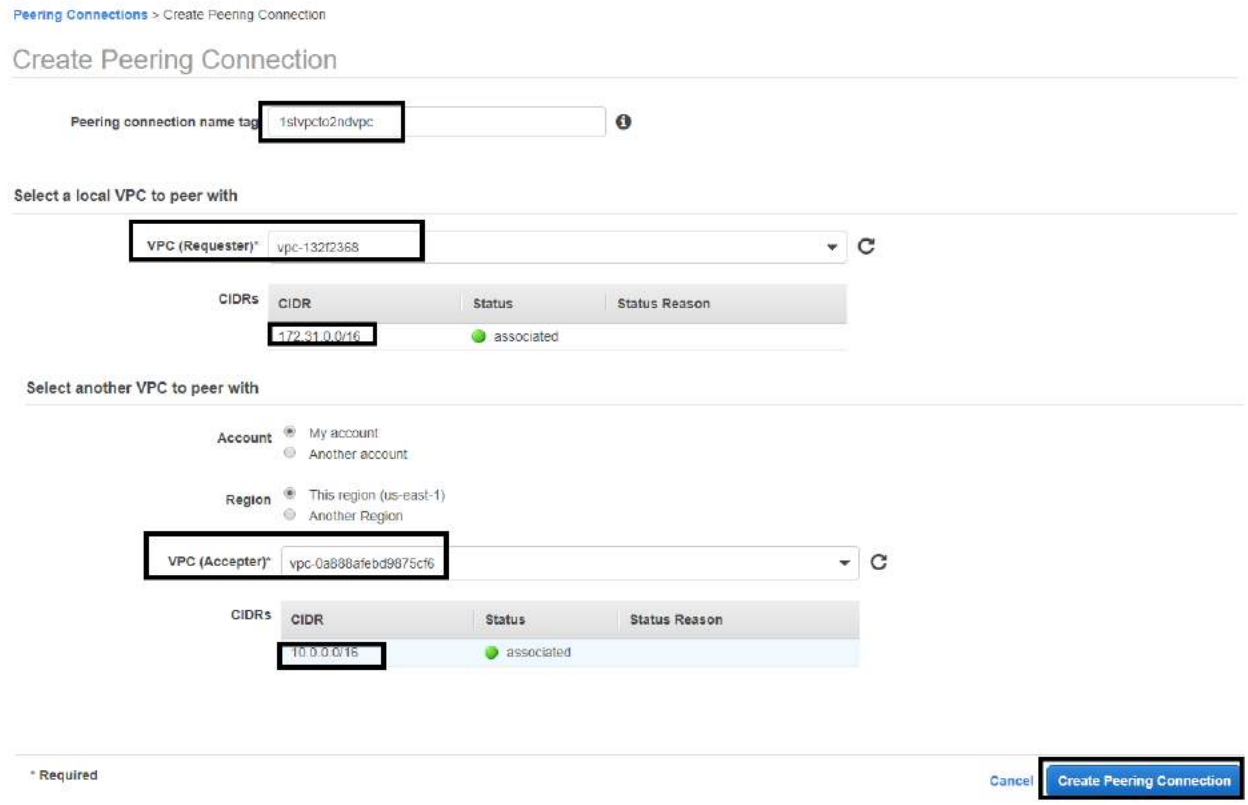


- Enable the IP option and click on Okay.

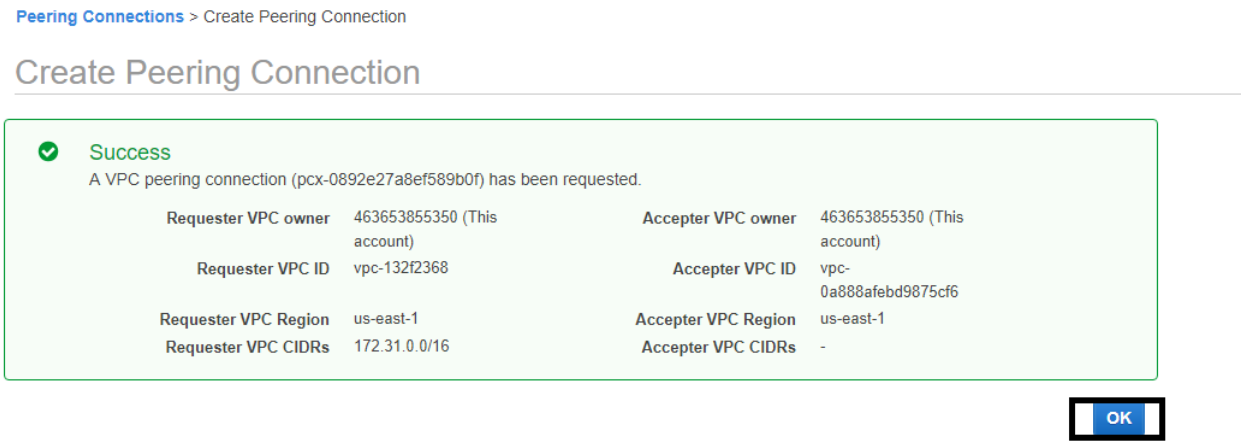
- To create a peering connection between Two VPC on same region or on different region or on different AWS accounts, Select peering connection and click on Create Peering connection.



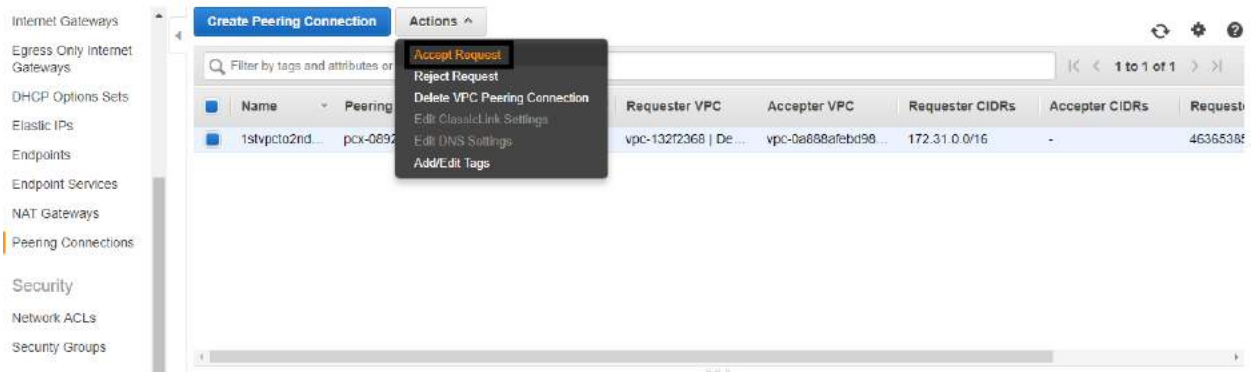
- Provide the Peering name, select the source VPC and target VPC to establish a connection.

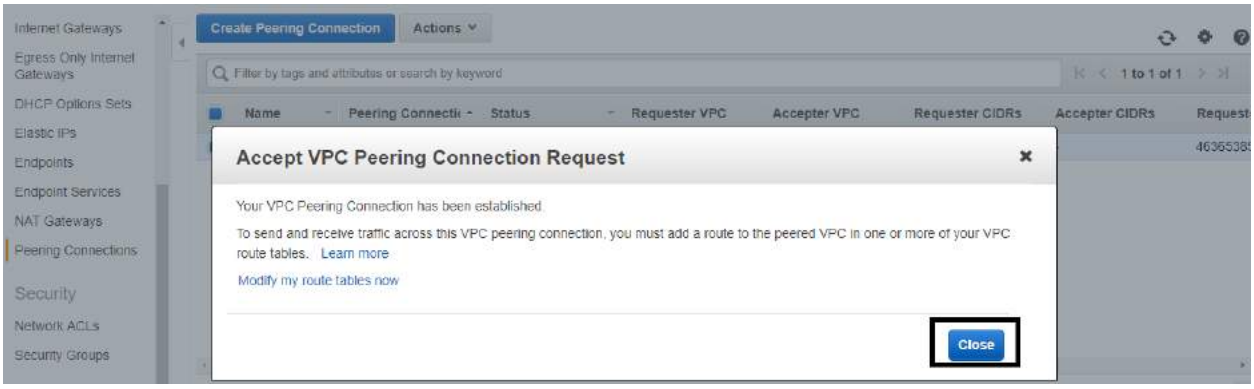


- Peering connection has been created successfully.

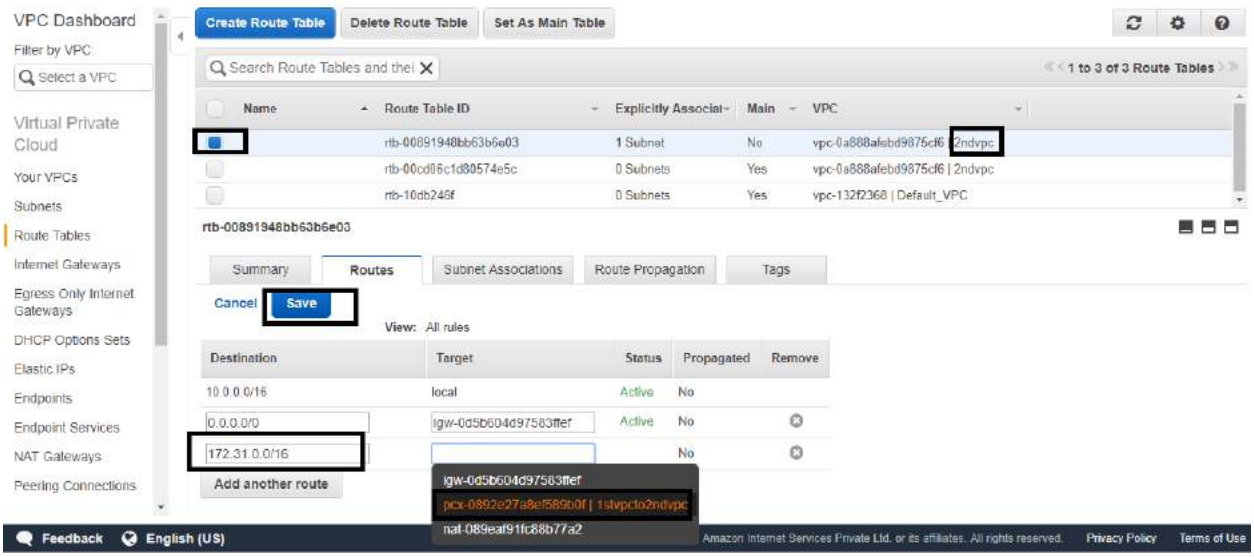


- Click on Actions and accept the request.

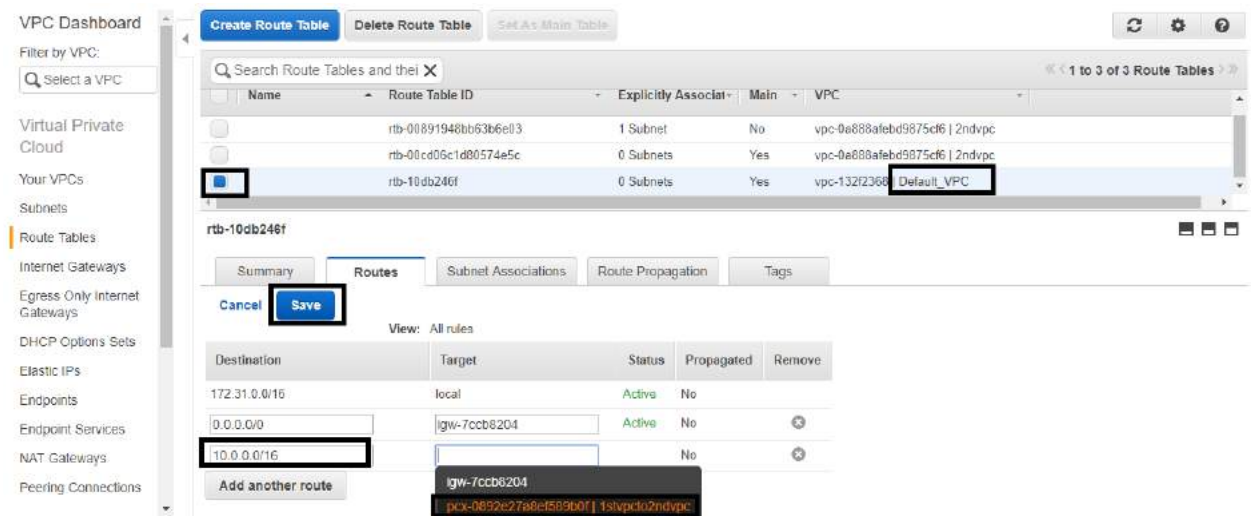




- Navigate to Route Tables, select the route table is being used for 2nd VPC to add an Address Space of 1st VPC using peering connection.

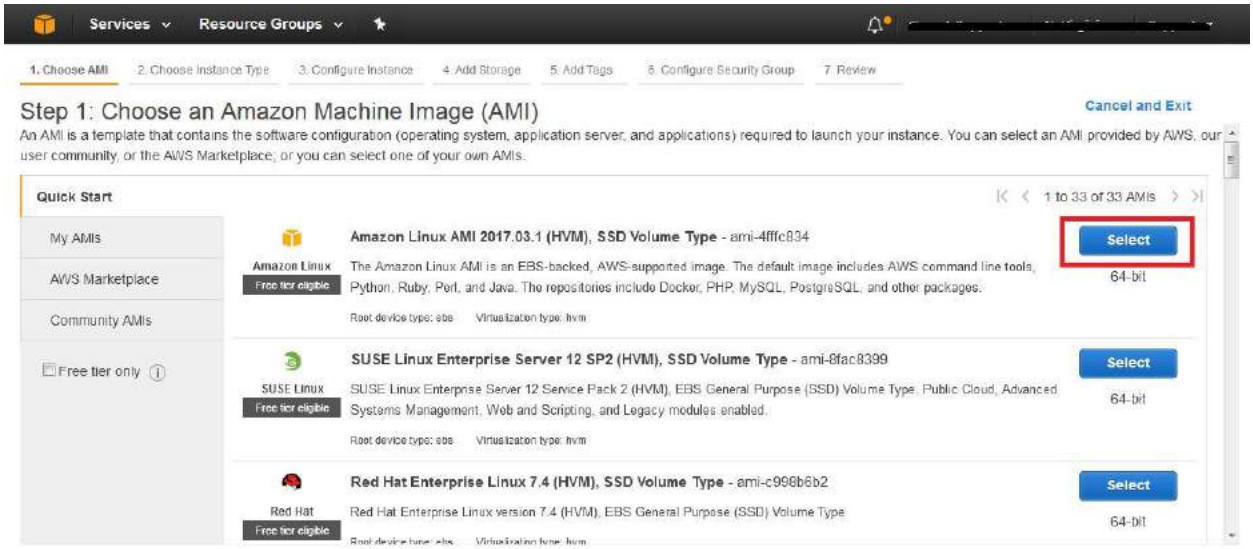


- Similarly, select the route table is being used for 1st VPC to add an address space of 2nd VPC using peering connection.

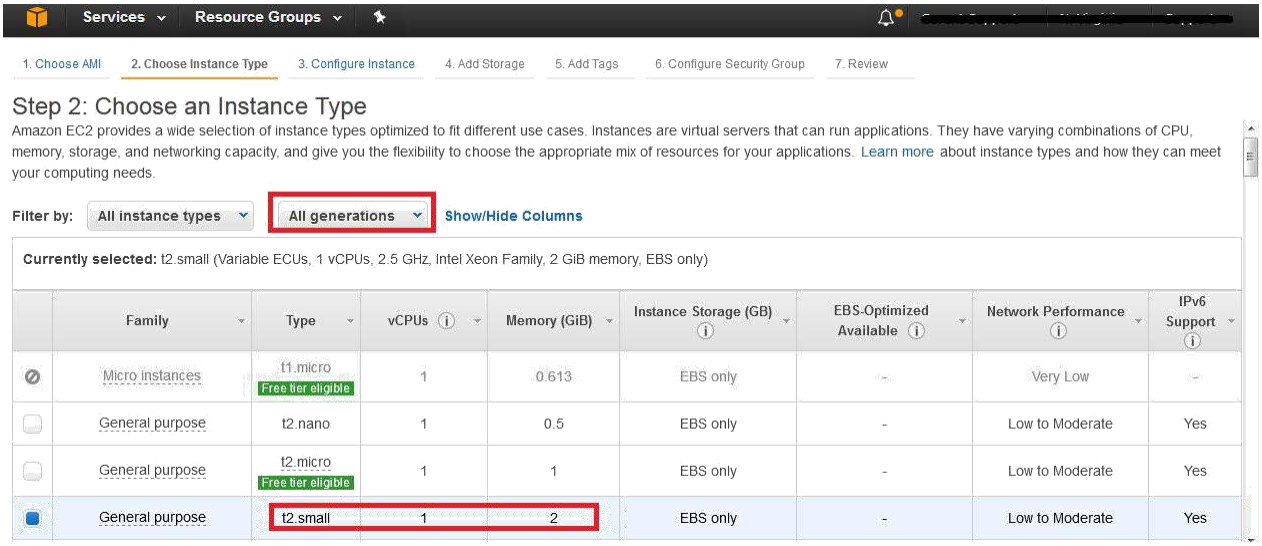


- Now, connection has been established between two VPC where it could communicate using private IP address each.

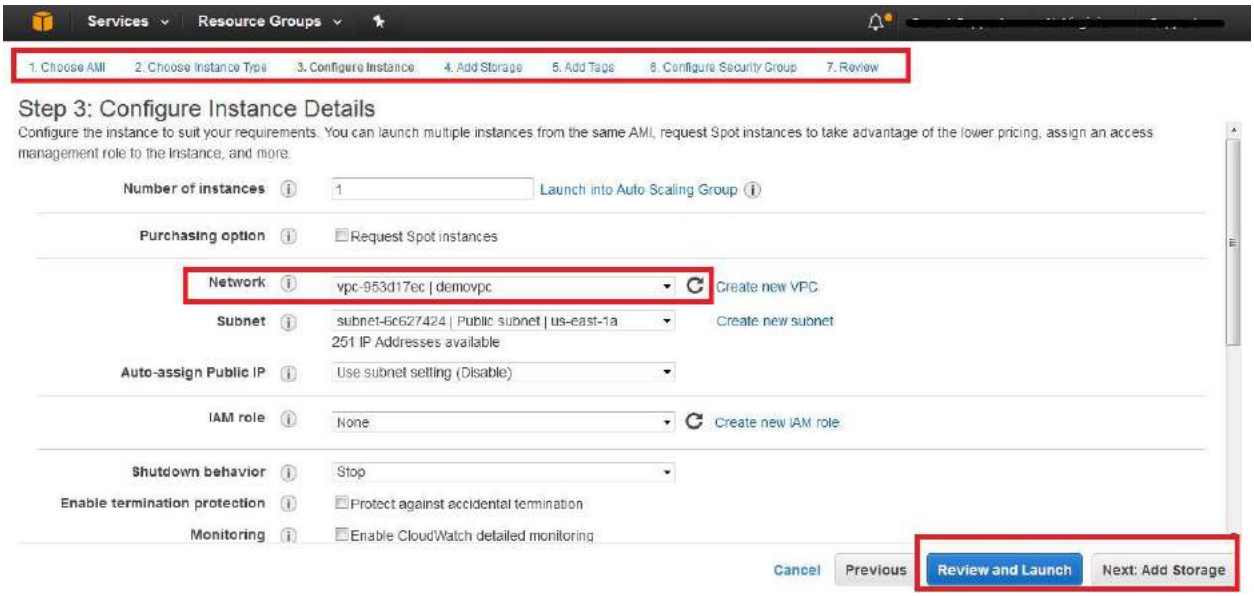
- After creation of VPC, navigate to EC2 for launching a new server and choose any operating system based on your requirement.
- Launching of new server is same like we seen in EC2 Classic method.
- Whatever Operating System and its version available in EC2 Classic would be available in EC2 VPC as well.
- Only difference between Classic and VPC is, instances would be running in same subnet if we launch in VPC and it would be running in different subnet if we launch in Classic.
- Some Instance Flavor supports only for VPC, some flavors supports only for Classic and few supports for both the model.
- Launch Linux Server as like shown below.



- Choose any instance flavor as per requirement as shown below. Please select the instance flavor which supports for VPC or it supports for both model.

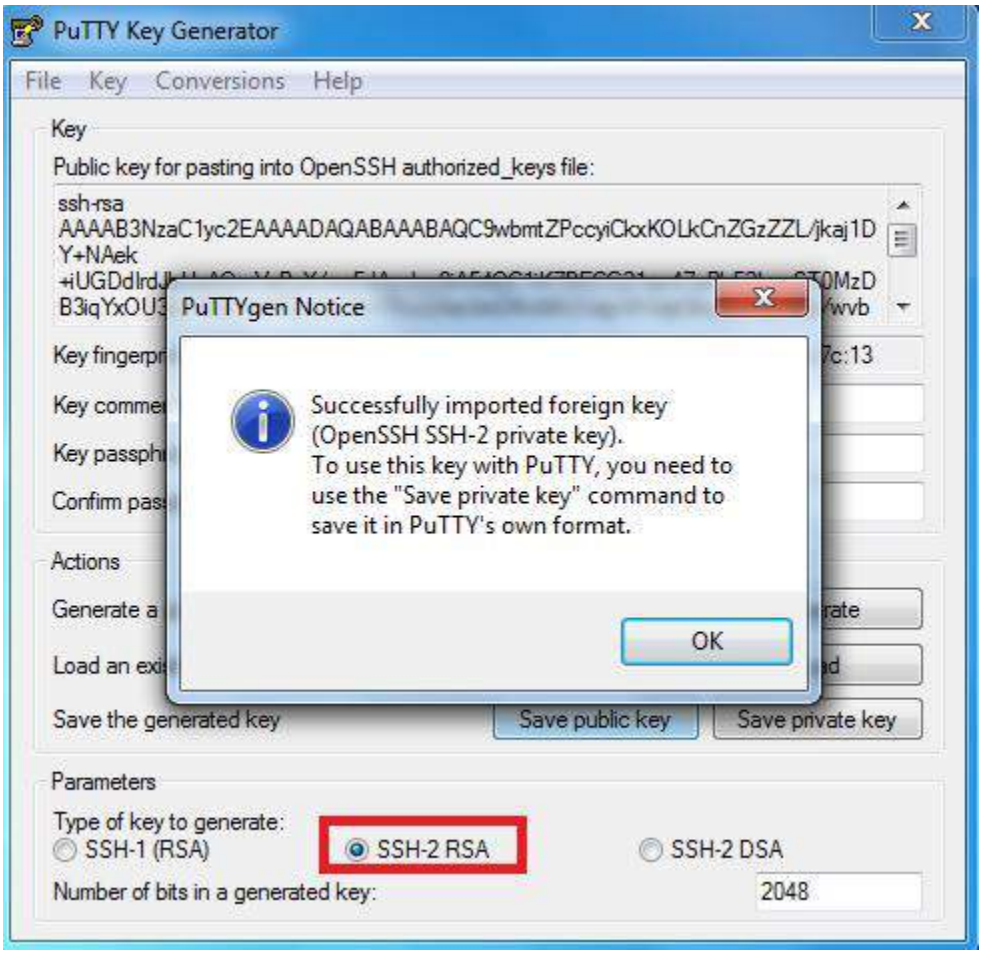


- After choosing an instance flavor, choose the network model as VPC. The VPC name which has been used will be displayed in this screen. Select the same and proceed to launch instances. Apart from these changes, steps to launch an instance are same for both Classic and VPC model.
- If EC2 Classic is in disabled state on Network tab, chosen instance flavor doesn't support for EC2 classic model and vice versa for EC2 VPC.

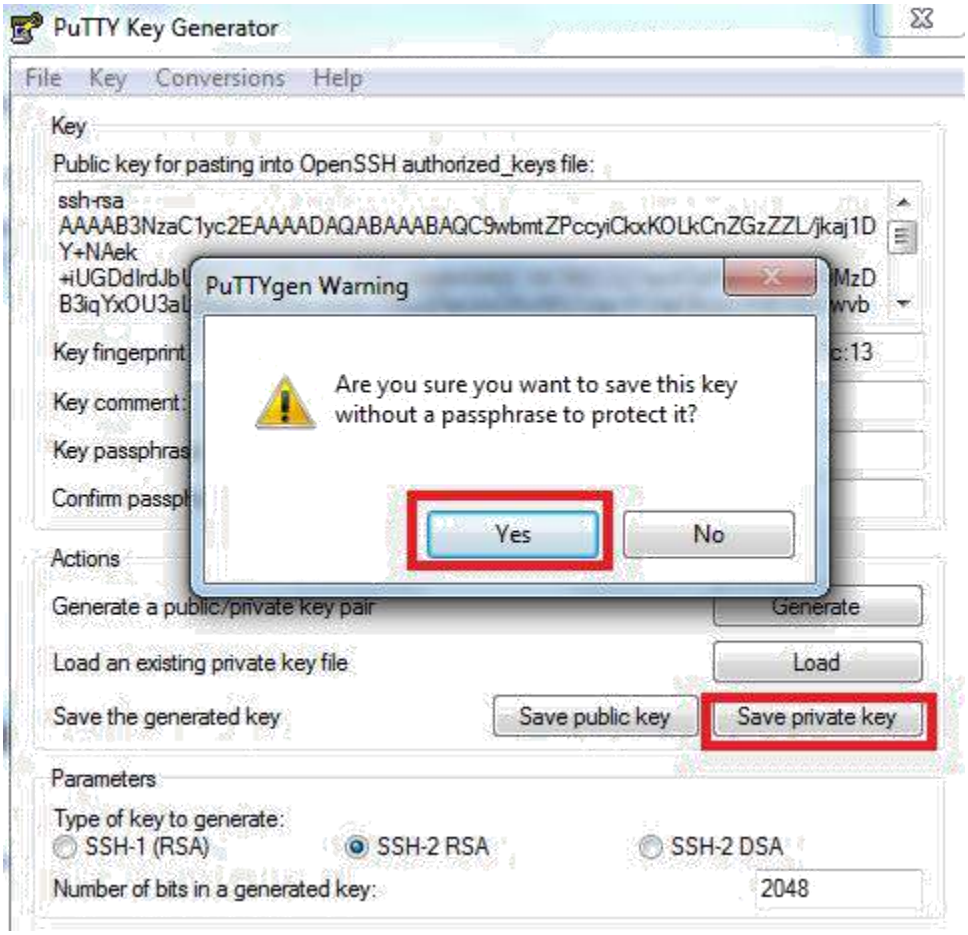


- Once Linux Server has been created under a VPC, we need to convert the KeyPair which is in PEM file to PPK format using PuttyGen tool.
- For Windows Server, we could use the KeyPair which has been created in AWS directly to get the random password after uploading and for Linux we need to go in this method.
- This method for Linux needs to be followed for both (Classic & VPC).
- Download the PuttyGen tool by clicking the below link.
- http://download.freedownloadmanager.org/Windows-PC/PuTTYGen/FREE-0.63.html

- Once PuttyGen download completes, open the file and import the KeyPair file which has been created earlier.
- After importing, choose the parameter as SSH-2 RSA for converting into PPK file as shown below.



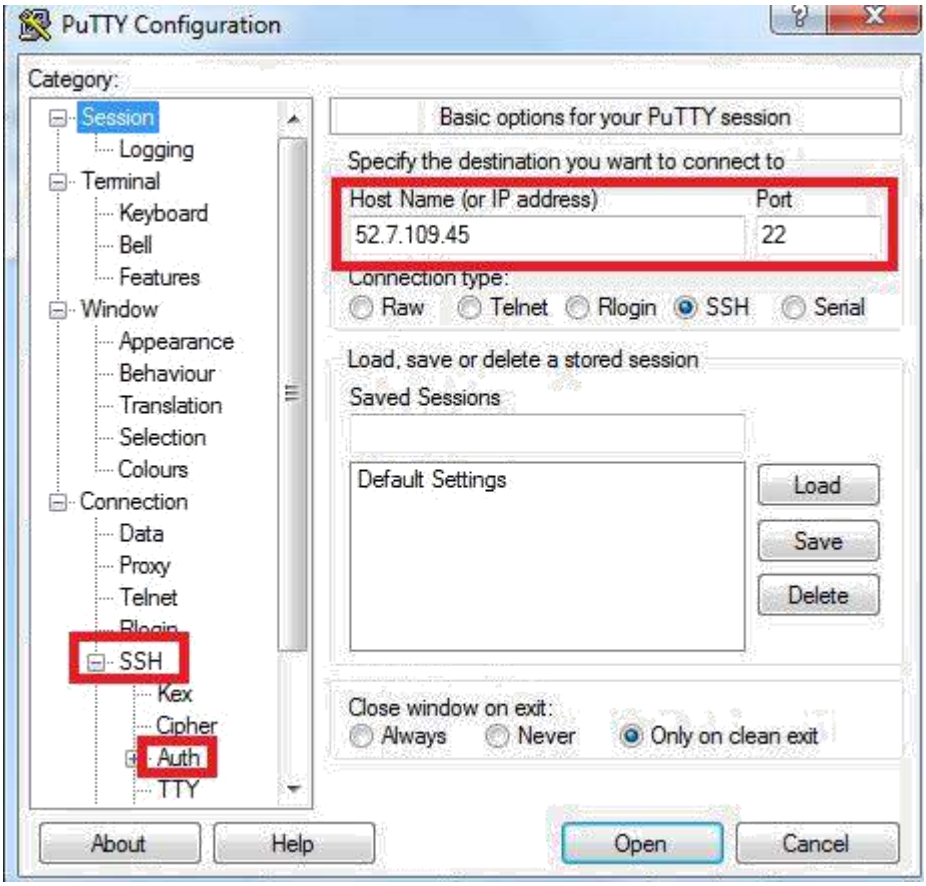
- Click on Save Private Key and choose an option as Yes as like shown below.

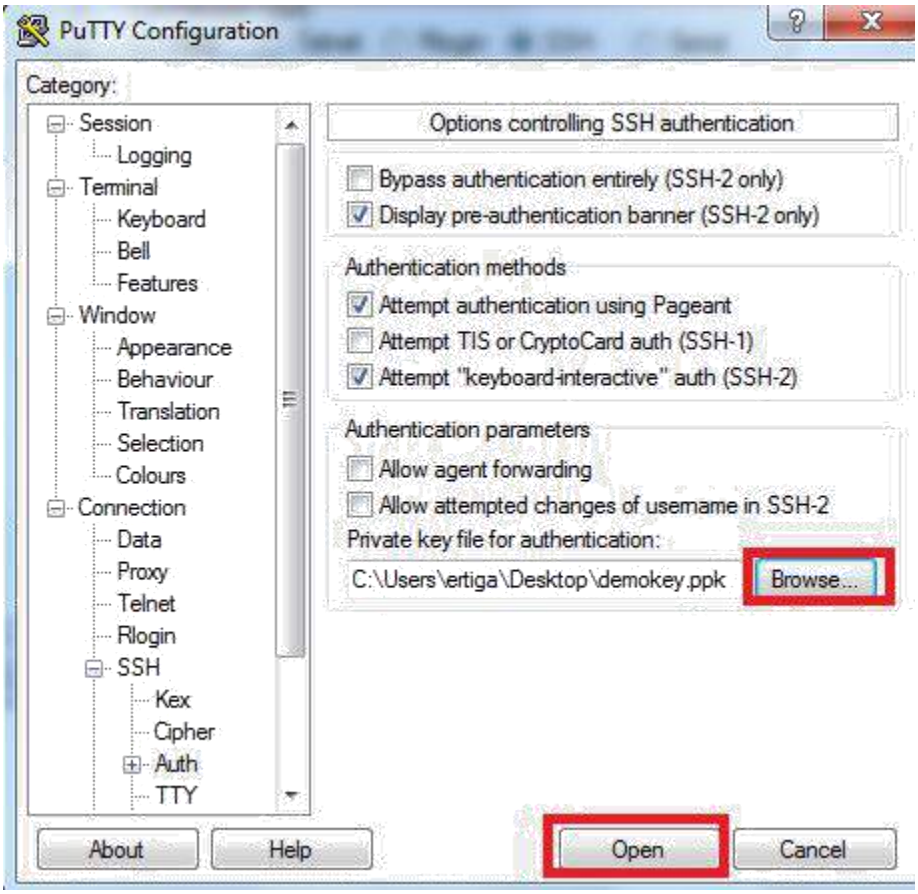


- Save the PPK file by providing any name as per your wish and this PPK file is used to authenticating Linux servers which has been created under VPC / Classic.

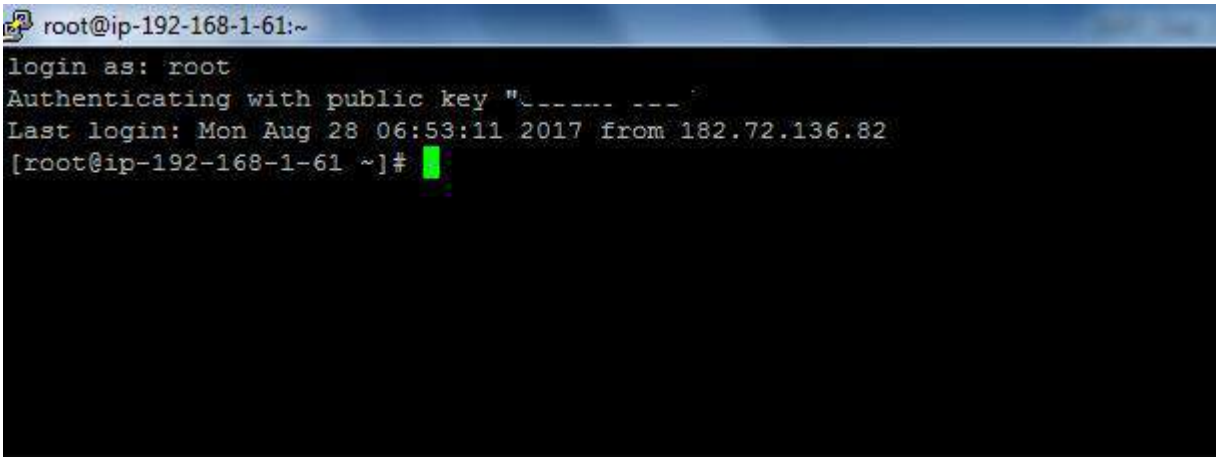
- demokey.ppk

- After creation of PPK file, download the Putty tool for taking SSH of Linux Server. Putty can be downloaded by clicking on below link.
- https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe
- Once download gets completed, open the Putty File to provide the IP address of Linux server and upload the newly generated PPK file for authenticating the same by clicking on Auth under SSH as shown below.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Cipher
Auth
TTY
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
52.7.109.45
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
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
Help
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Cipher
Auth
TTY
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:
C:\Users\ertiga\Desktop\demokey.ppk
Browse...
About
Help
Open
Cancel

- After uploading the PPK file, click on open to take the SSH of created Linux server.
- By default, username of Linux platform which is available in AWS would be, ec2-user / root.
- If ec2-user is not working, try with root as a username.



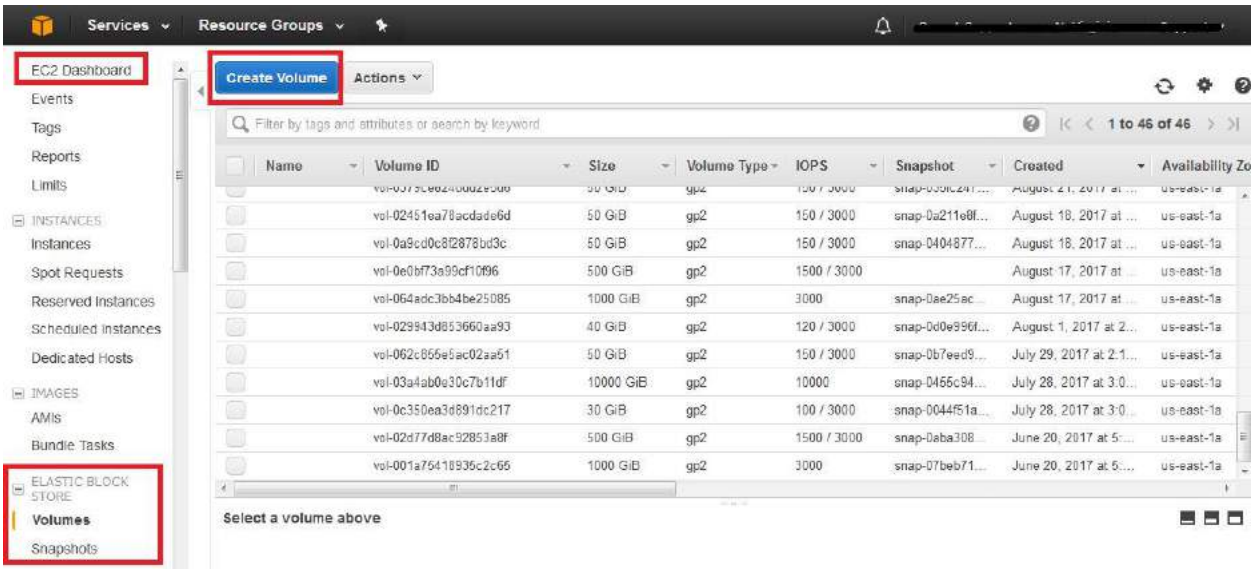
- These are the steps to create a new server in EC2 VPC and Classic.

Advantages on VPC:

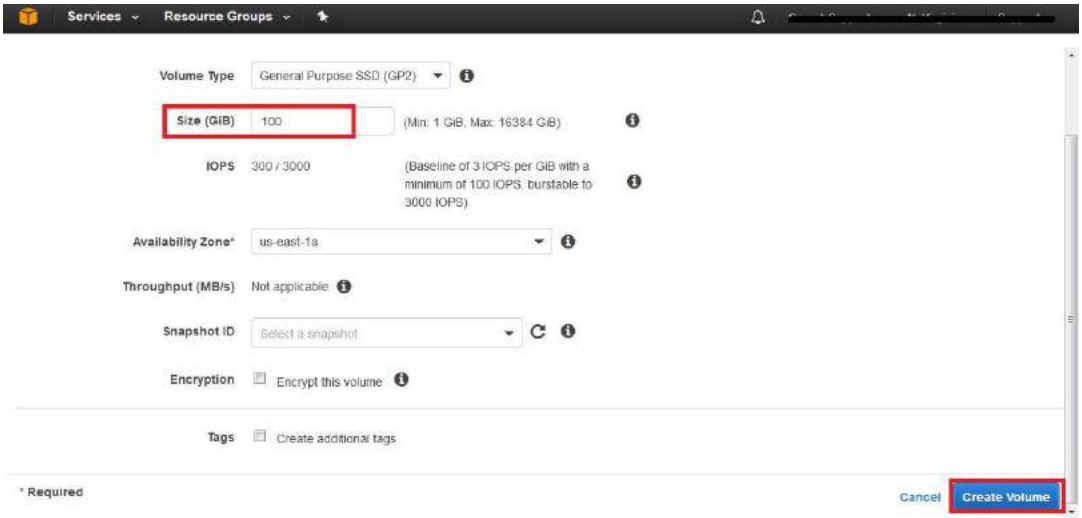
- All the Virtual Machines will be running in the same network, so that communication between VM will be faster.
- Easier Data Synchronization between VM running in different Subnets.
- Able to connect On-Premises Server to the VPC.

EBS (Elastic Block Store):

- EBS has categorized into two types.
- **Volumes** – It would help you to add / attach a new volume of data into created server.
- **Snapshot** – This would help you to capture the snapshot of added volume and create a new volume from captured snapshot. Once a new volume has been created, it can be attached to any server which is running in EC2.
- To add a new Volume, click on EC2 under Services and Choose Create Volume option under Elastic Block Store.

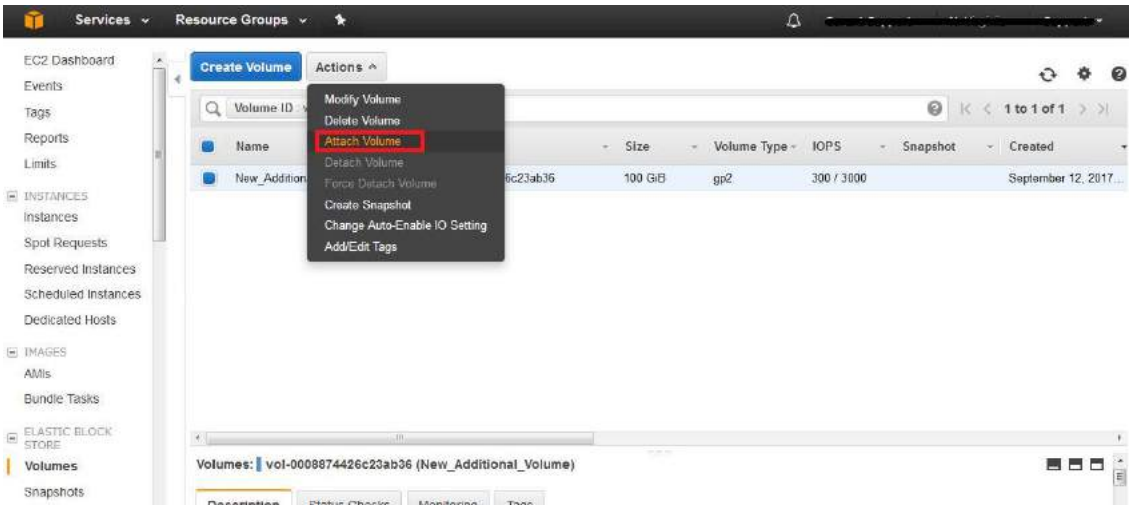


- Provide the size of the volume which is required to add it in the server and click on create volume.

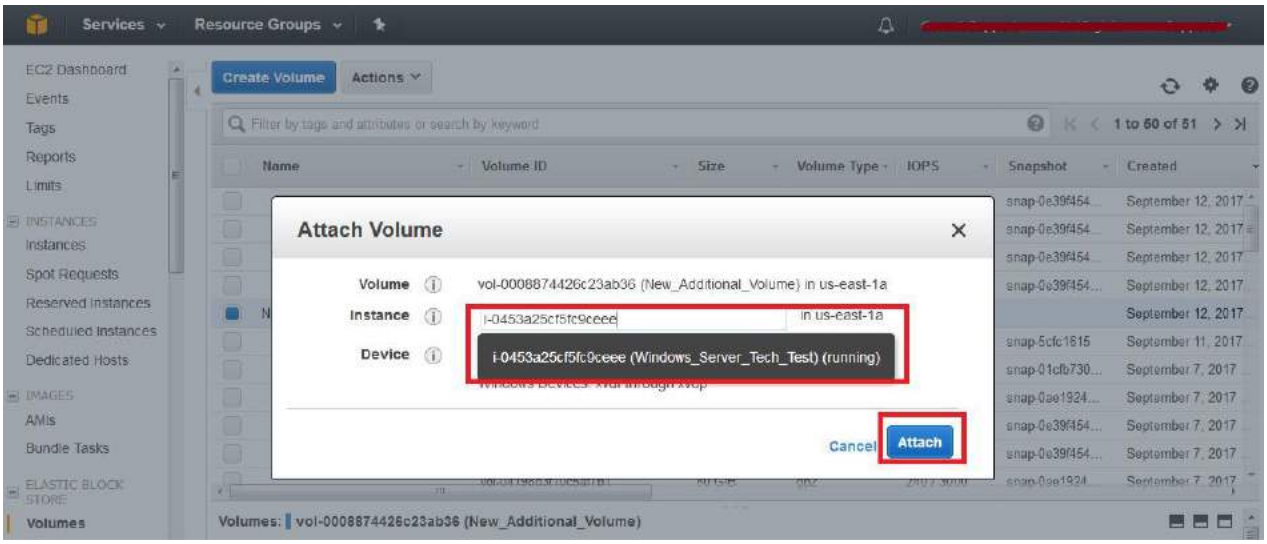


- Once the volume is created, Volume ID will be generated. Click on Volume ID to view the created volume.

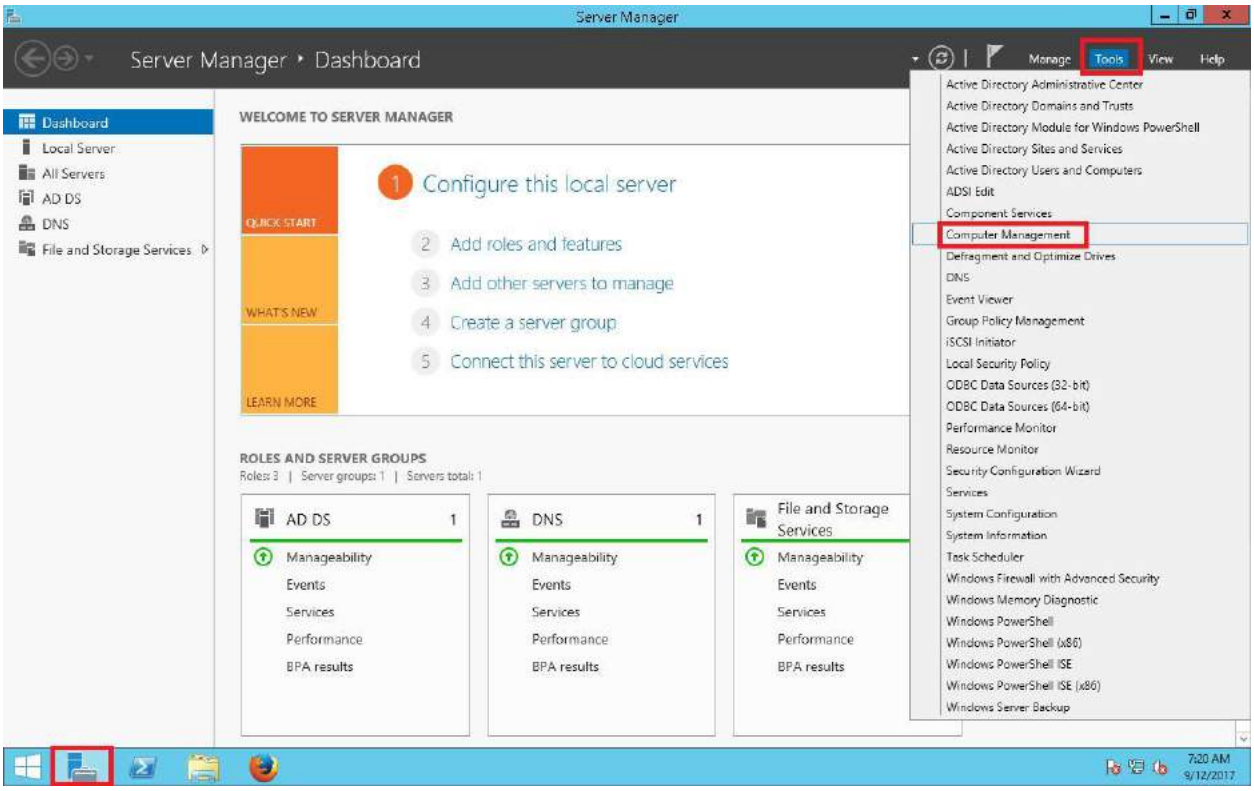
- Created Volume name can be modified by clicking on edit option. After choosing the volume to attach into the server, click on **Actions >> Attach Volumes** as like shown below.

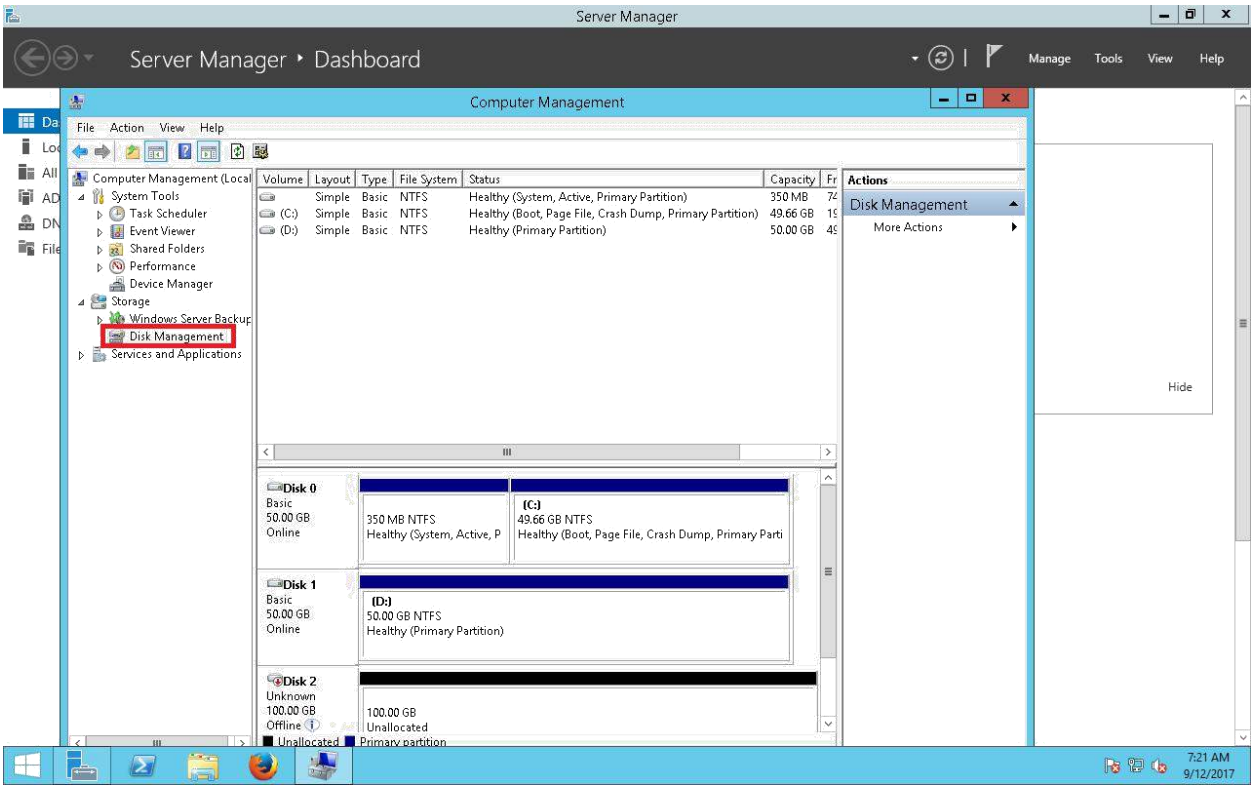


- After clicking on Attach volume, choose the server which has been created in EC2 and click on Attach. Volumes can be attached to any kind of server, whether it is Windows or Linux. No restrictions of adding new volumes and attaching on server.

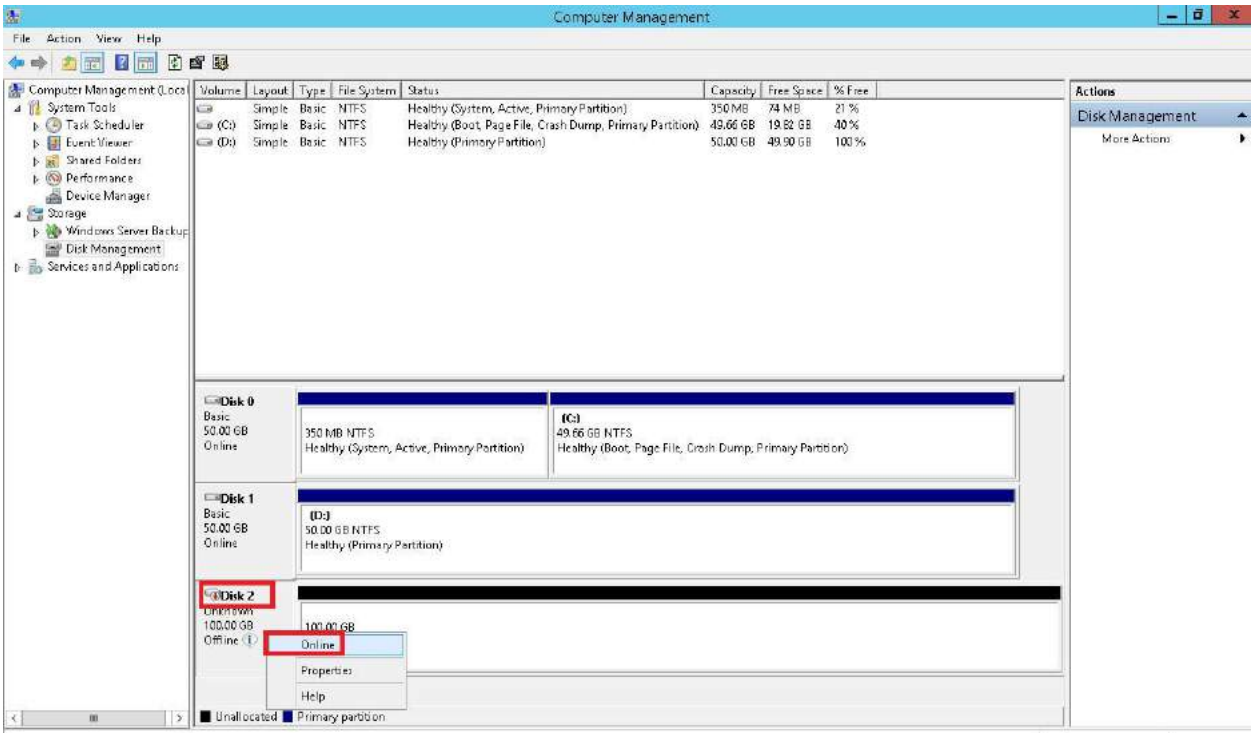


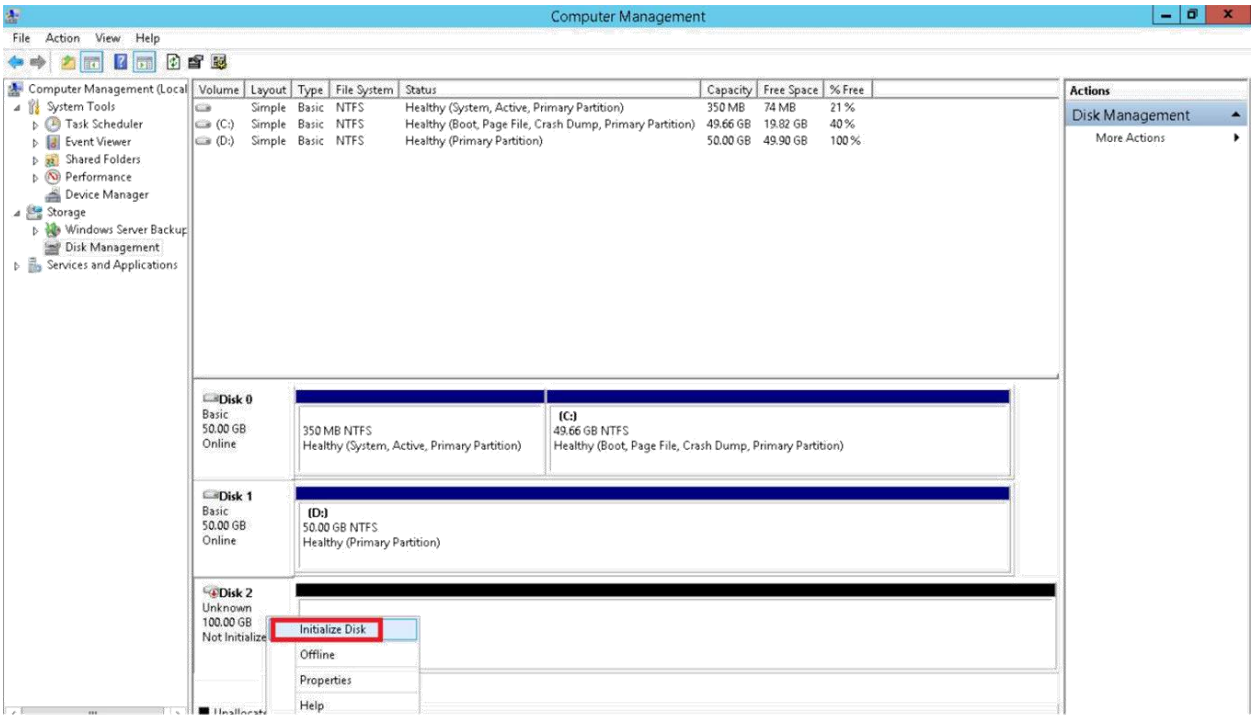
- After attaching the new volume in server, it would be attached. We need to mount the volume into the server. To mount it, we need to log in to the server in which we had attached the volume. Once you logged into the server using RDP, navigate to **Server Manager >> Tools >> Computer Management >> Disk Management** as like shown below.

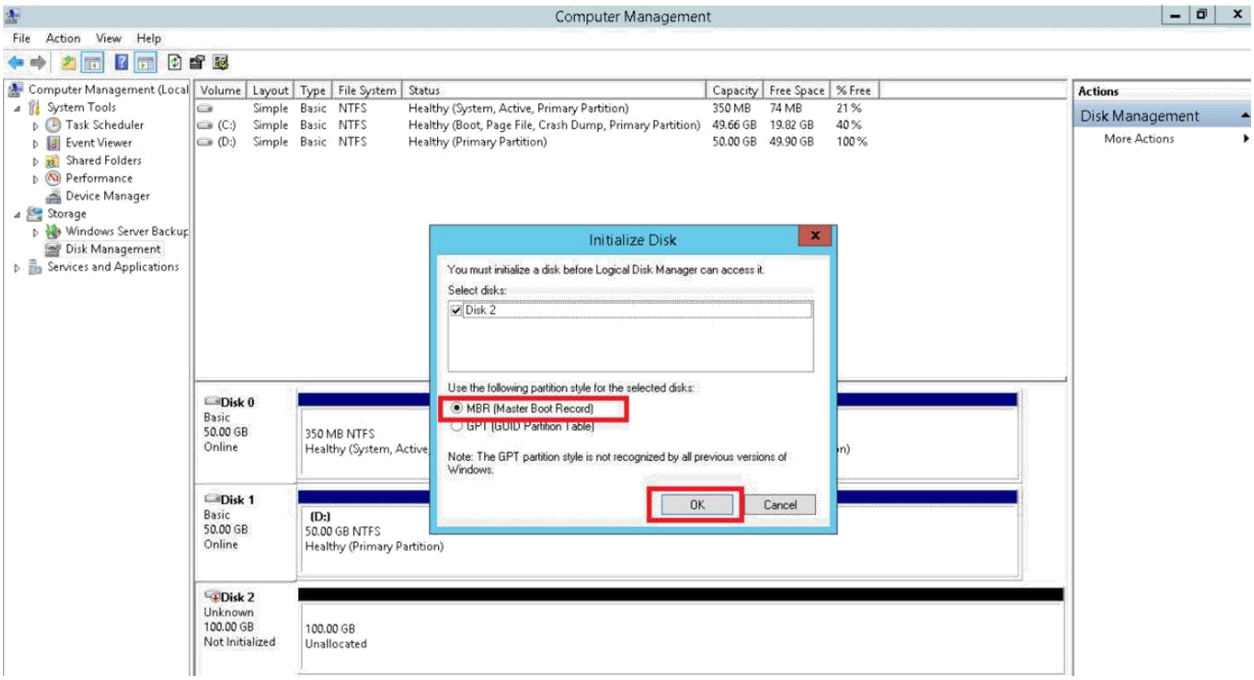




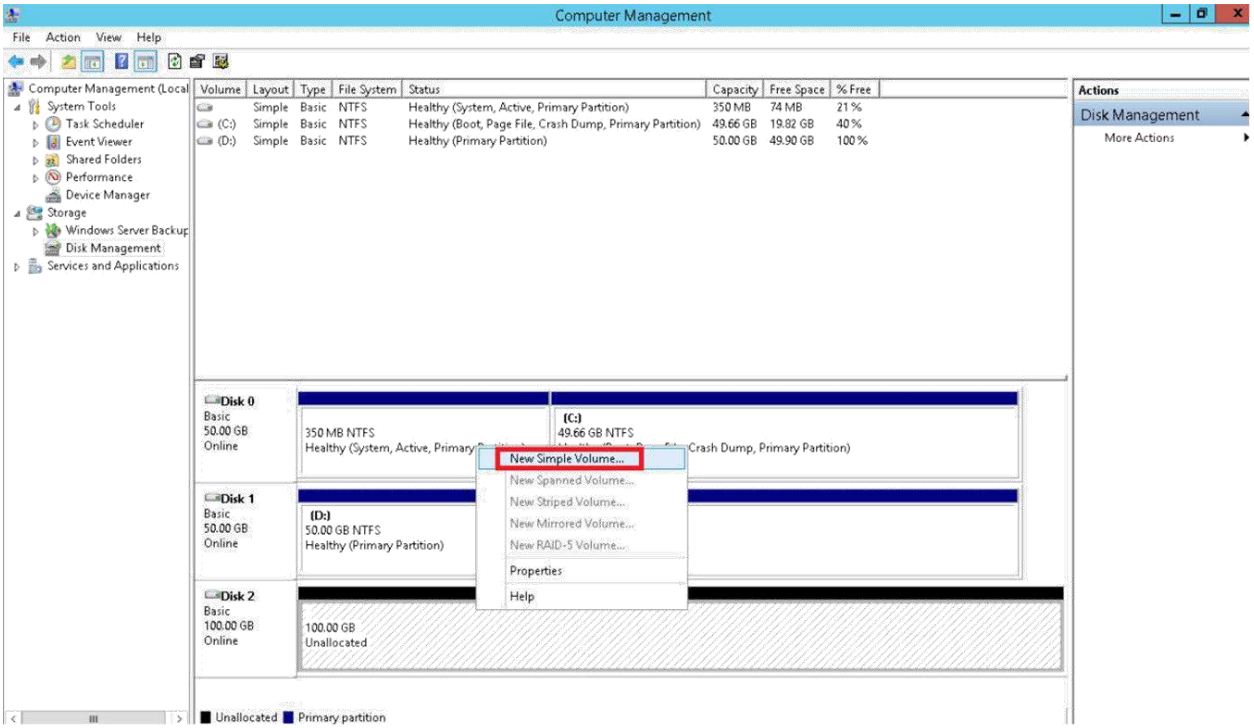
- After navigating to Disk Management, you would be able to view added volume inside the server. To mount the same, right click on Disk 2 which is shown below and make it as Online. Once it came to online, right click again for initializing the disk by choosing MBR (Master Boot Record).

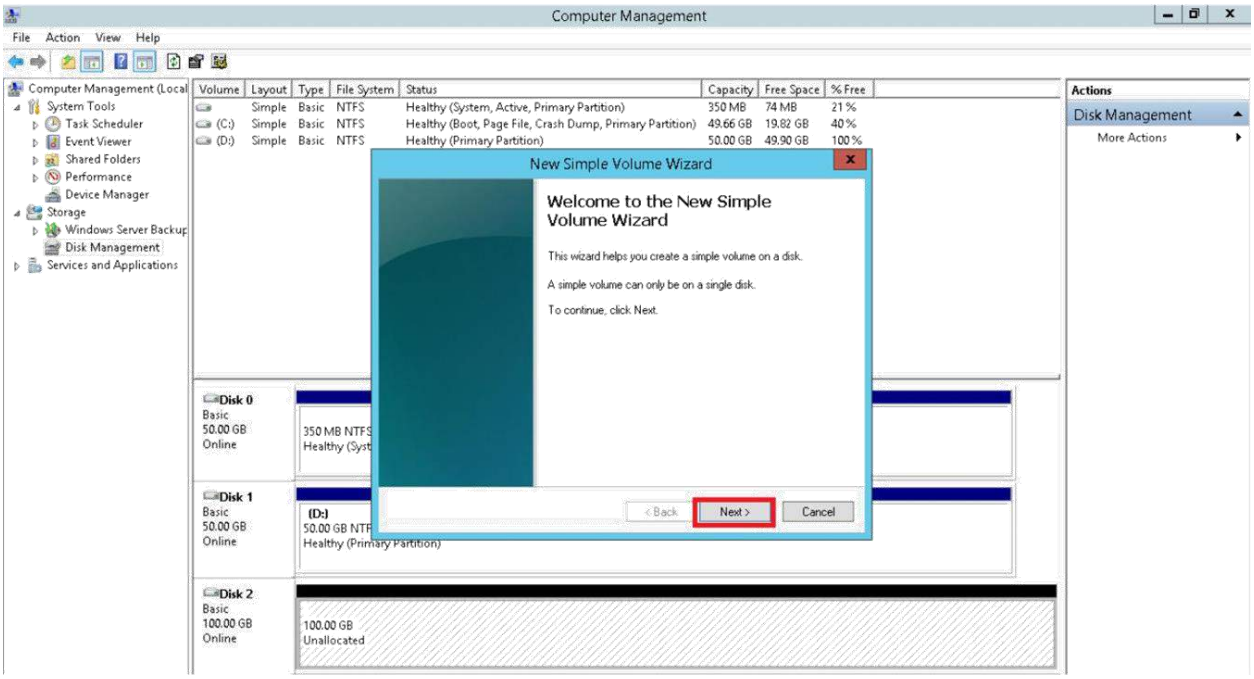




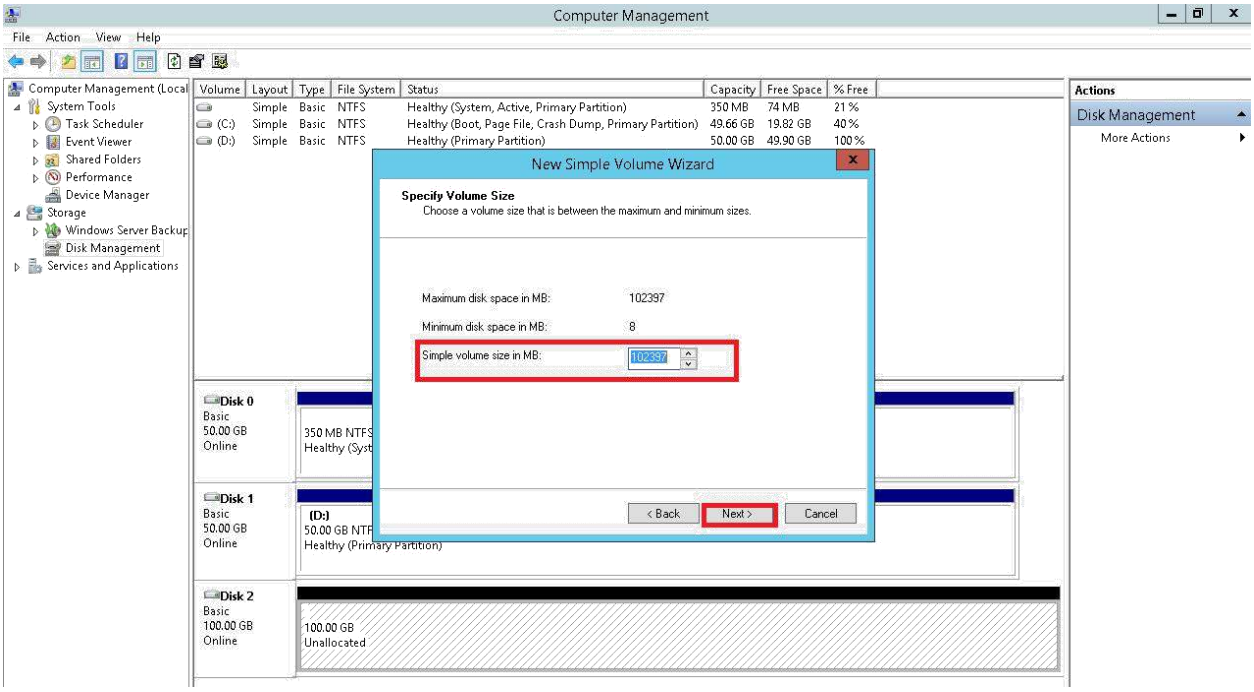


- Once the disk has been initialized, right click on unallocated section and choose New Simple
- Volume for mounting the disk into server. Click on Next

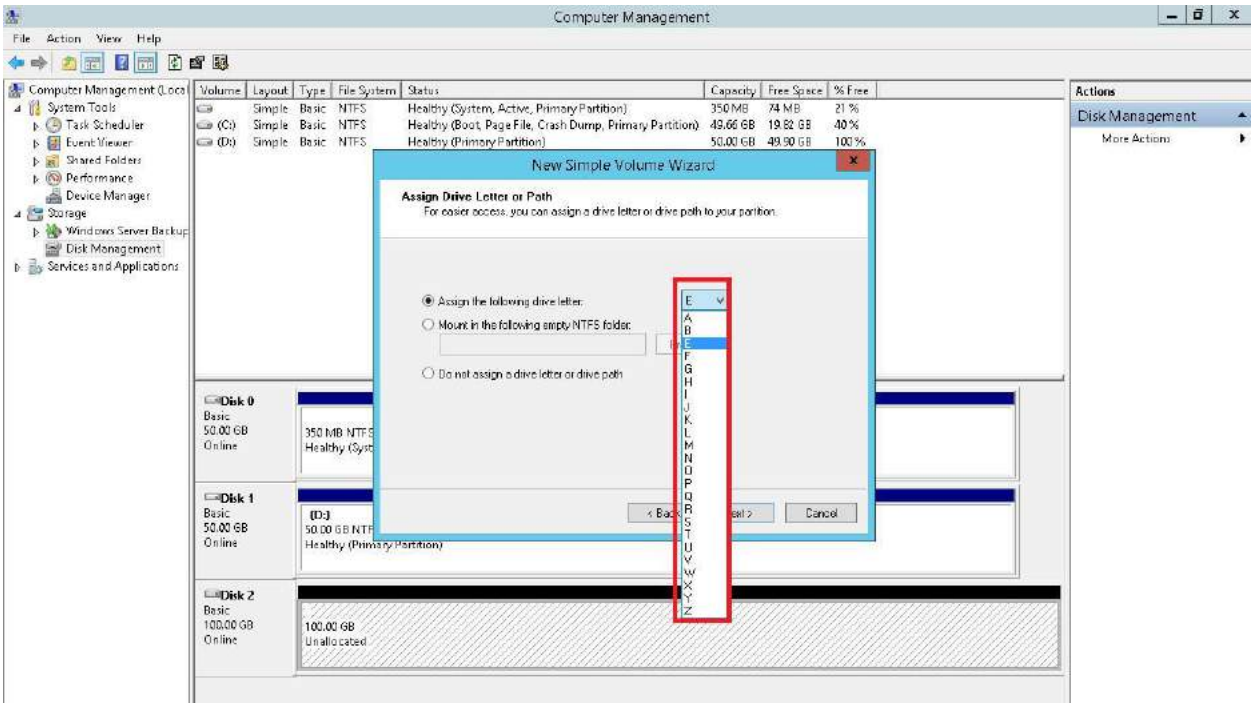




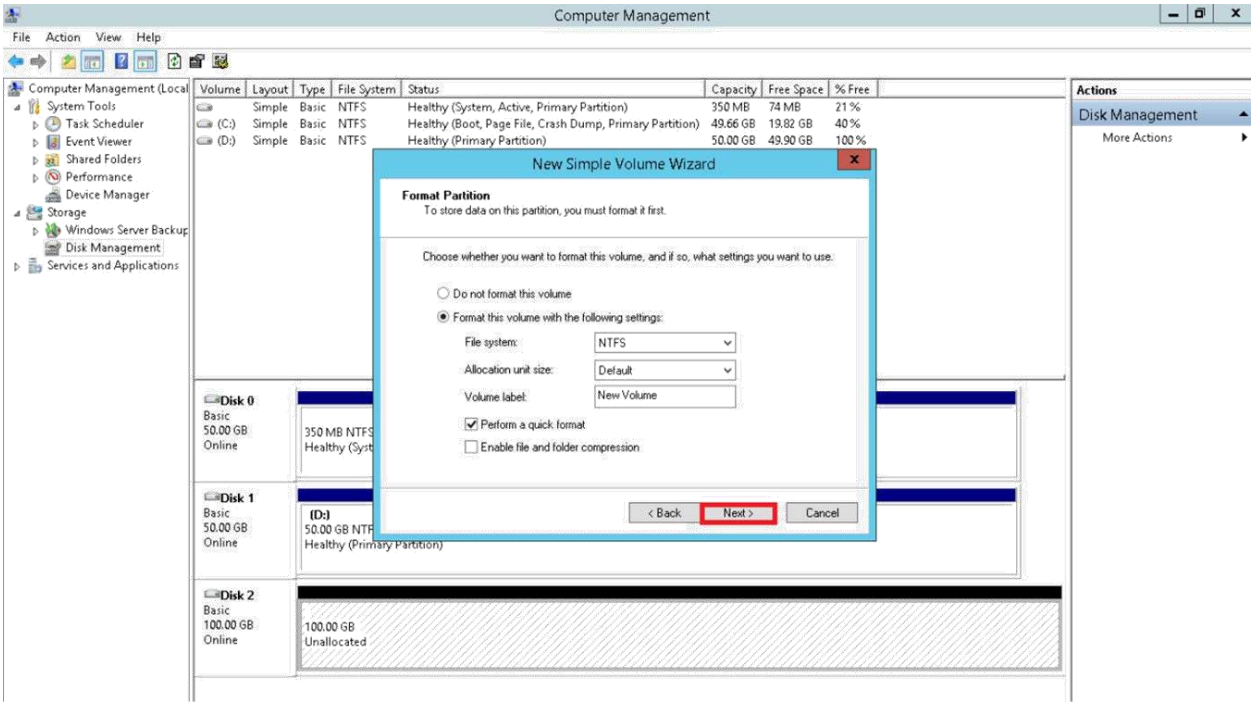
- If you want to partition the volume into two different drives, it can be possible by providing certain amount of size in the volume instead of using all size. Once the certain size has been segregated, again we need to follow the same steps for creating another Simple Volume in a different drive by right clicking on unallocated section.

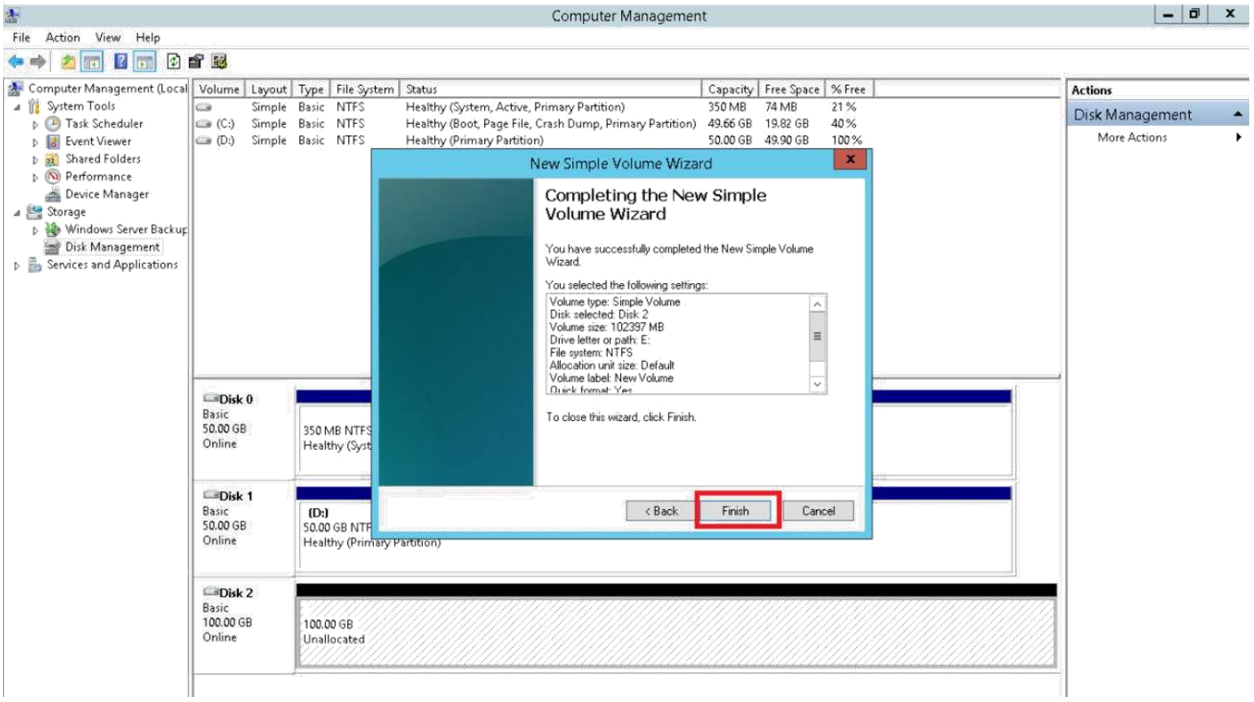


- Choose the letter of the drive which you wish and click on Next as like shown below.

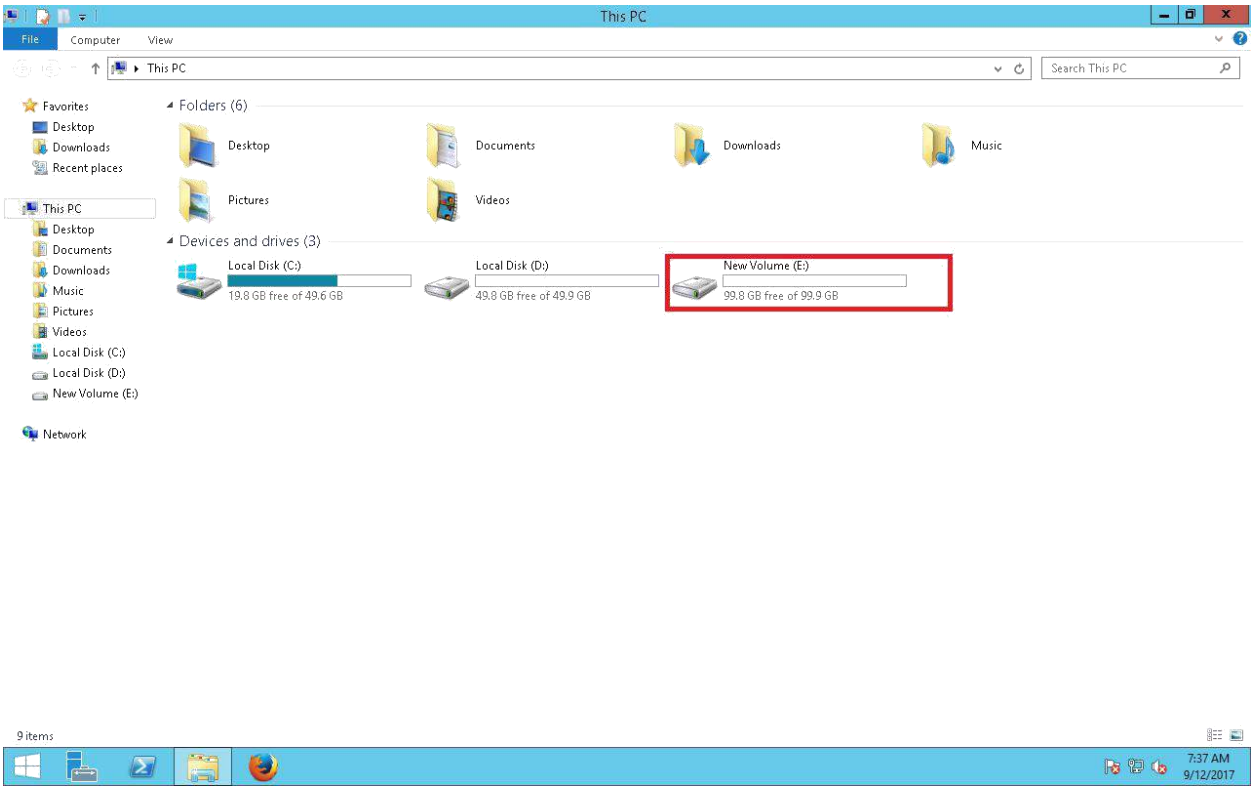


- If you want to change any file system, it can be possible by choosing in the drop down under File System. After choosing the file system, click on Next and Finish.

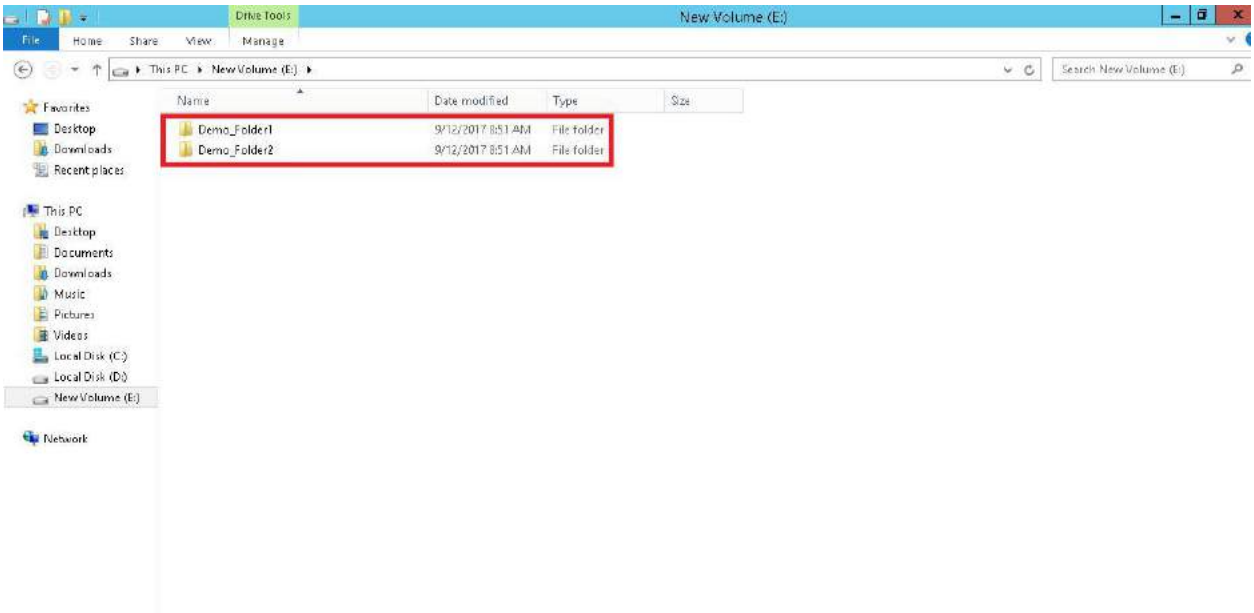




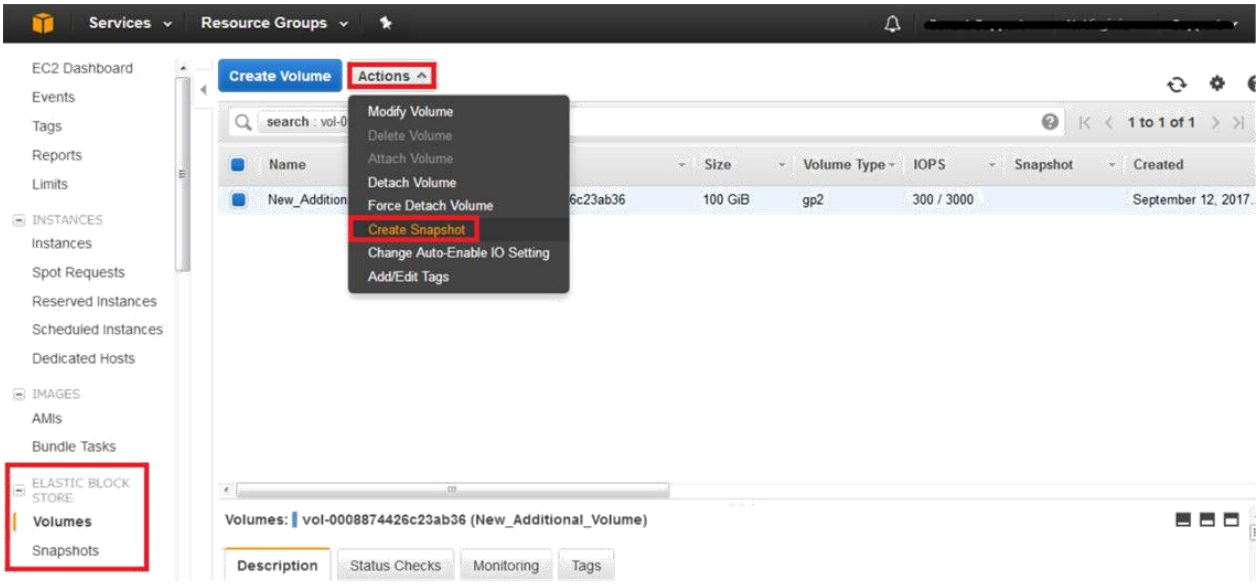
- Attached volume has been mounted in the server which is running under EC2 and the same is
- available in My Computer as like shown below.

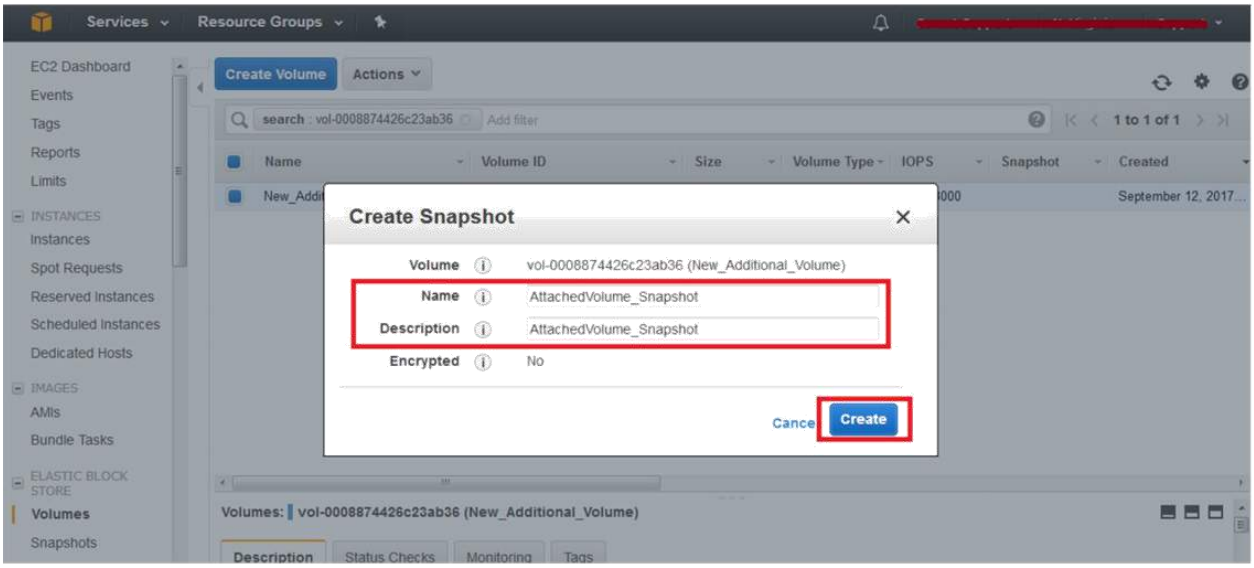


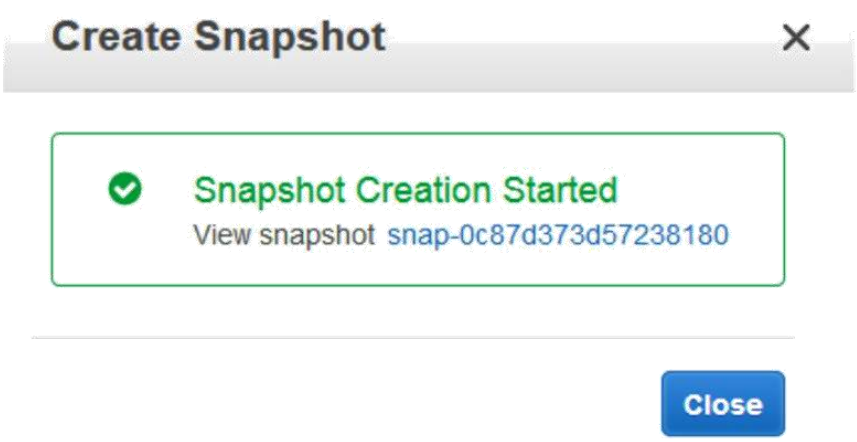
- Create / copy any files and paste it in an attached drive as like shown below.



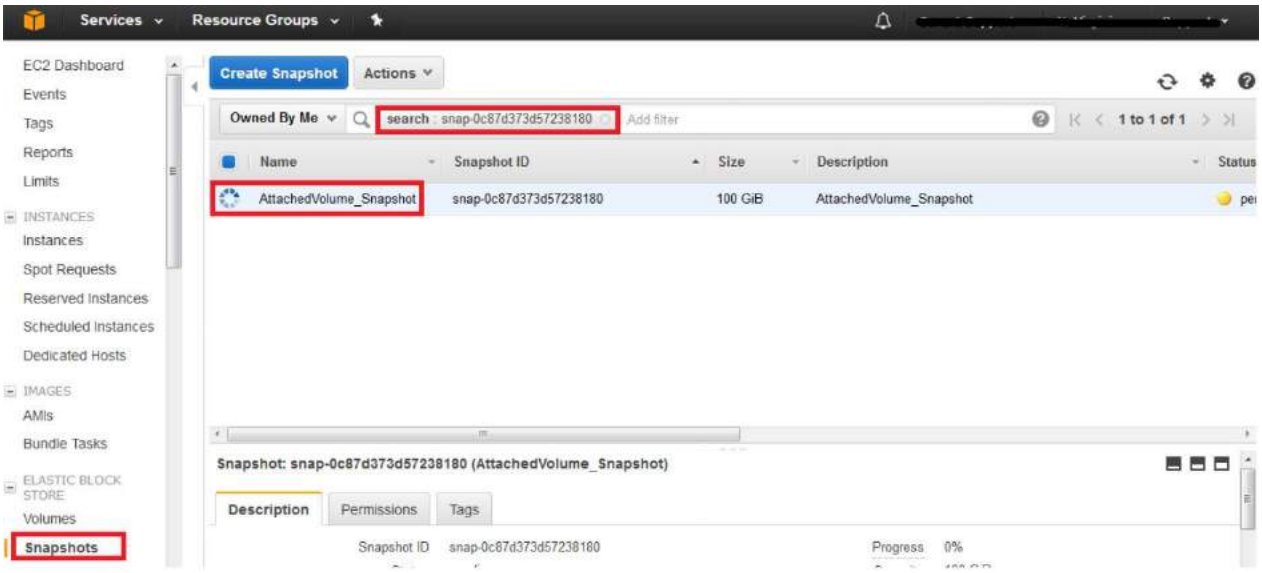
- After pasting the files, proceed to create a Snapshot by providing Snapshot name and description on AWS, so that a new snapshot would be created along with pasted files in an attached drive.

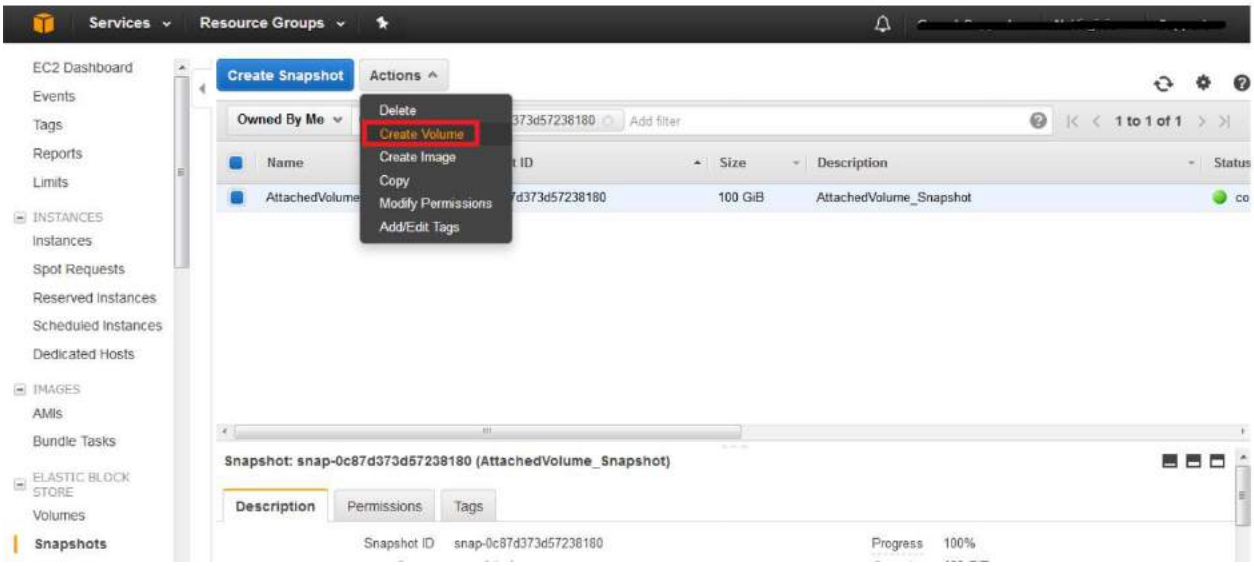

Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Create Volume
Actions
Modify Volume
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Create Snapshot
Change Auto-Enable IO Setting
Add/Edit Tags
1 to 1 of 1
Name
Size
Volume Type
IOPS
Snapshot
Created
New_Addition
100 GiB
gp2
300 / 3000
September 12, 2017
Volumes: vol-0008874426c23ab36 (New_Additional_Volume)
Description
Status Checks
Monitoring
Tags

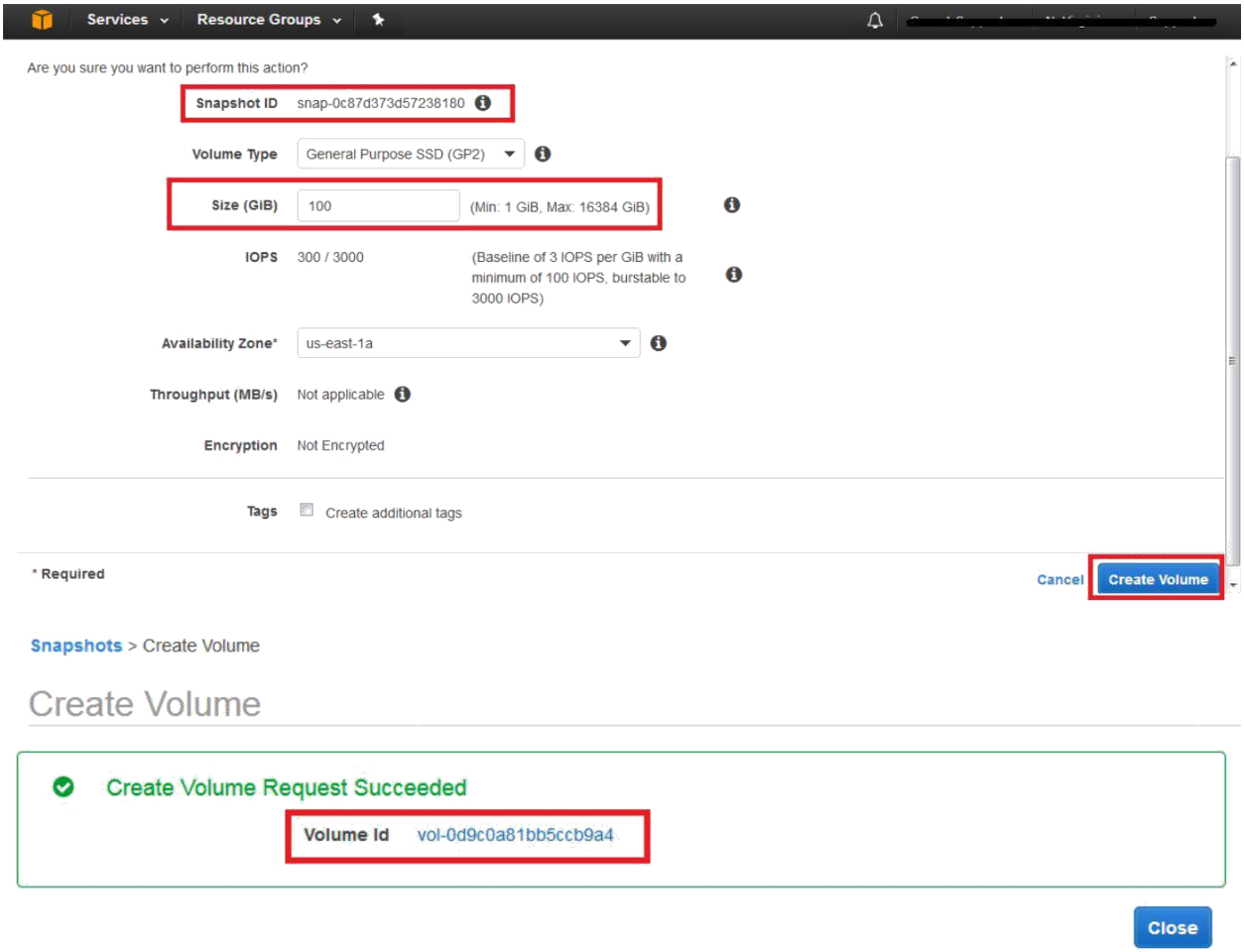

Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Create Volume
Actions
search : vol-0008874426c23ab36
Add filter
1 to 1 of 1
Name
Volume ID
Size
Volume Type
IOPS
Snapshot
Created
September 12, 2017
Create Snapshot
Volume
vol-0008874426c23ab36 (New_Additional_Volume)
Name
AttachedVolume_Snapshot
Description
AttachedVolume_Snapshot
Encrypted
No
Cancel
Create
Volumes: vol-0008874426c23ab36 (New_Additional_Volume)
Description
Status Checks
Monitoring
Tags


Create Snapshot
Snapshot Creation Started
View snapshot snap-0c87d373d57238180
Close

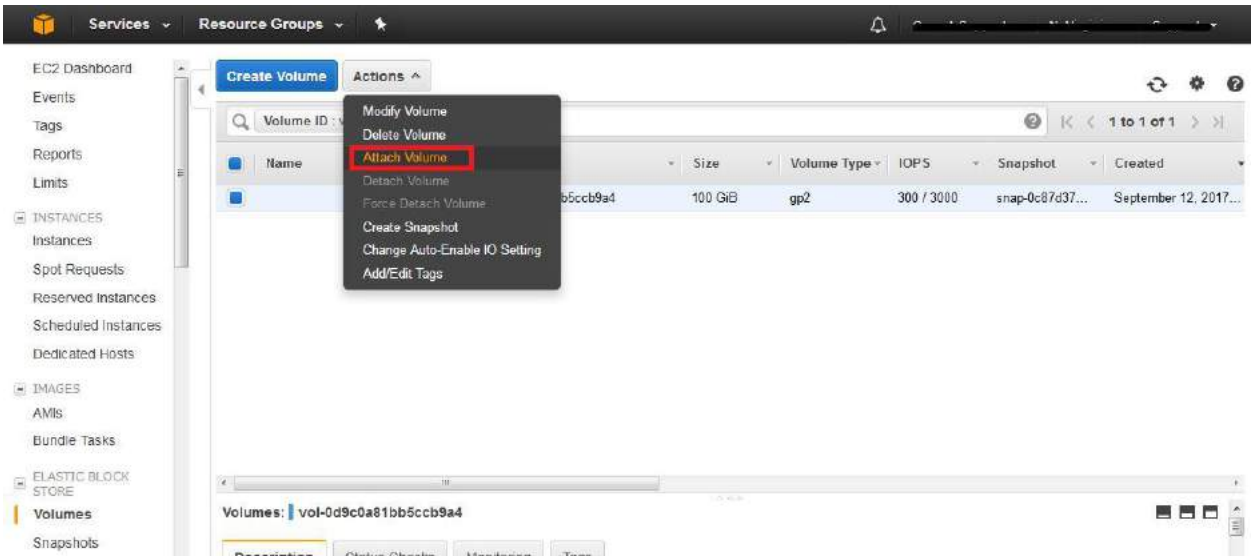
- Once you click on above snapshot ID, you would be able to see the creation of snapshot. Once the snapshot gets created, you would be able to create a new volume as like shown below.

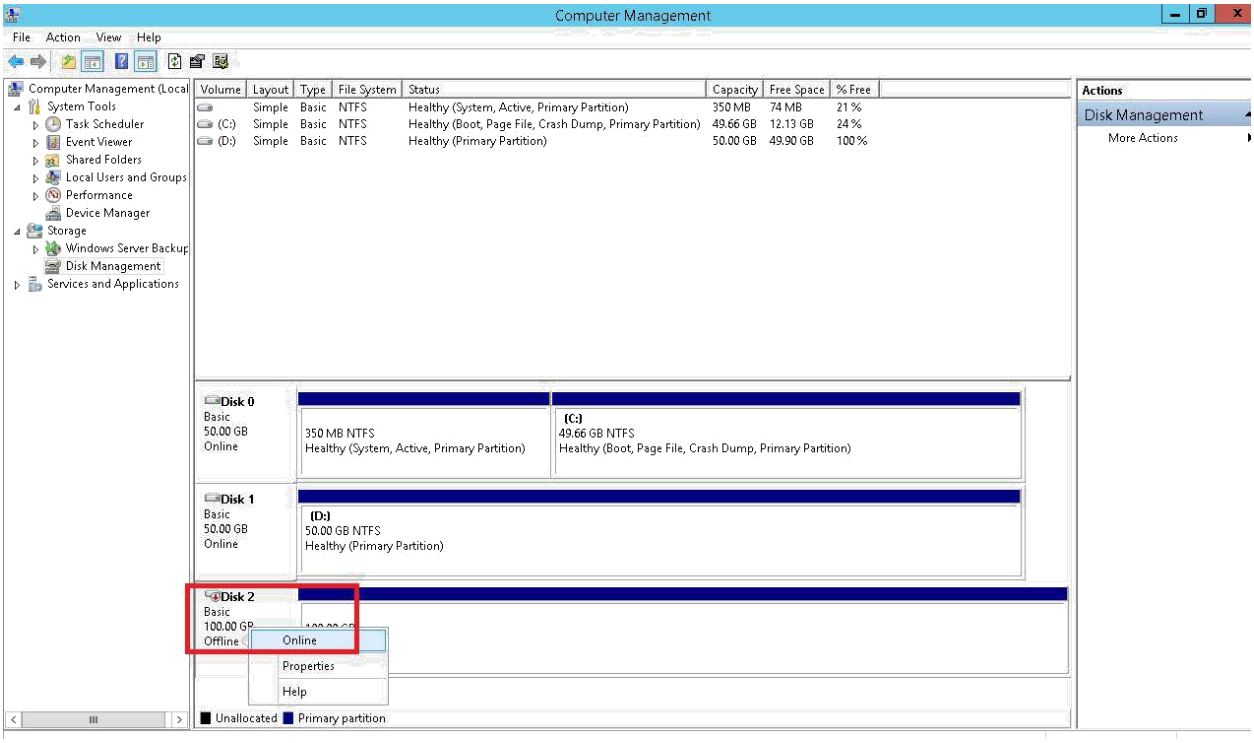




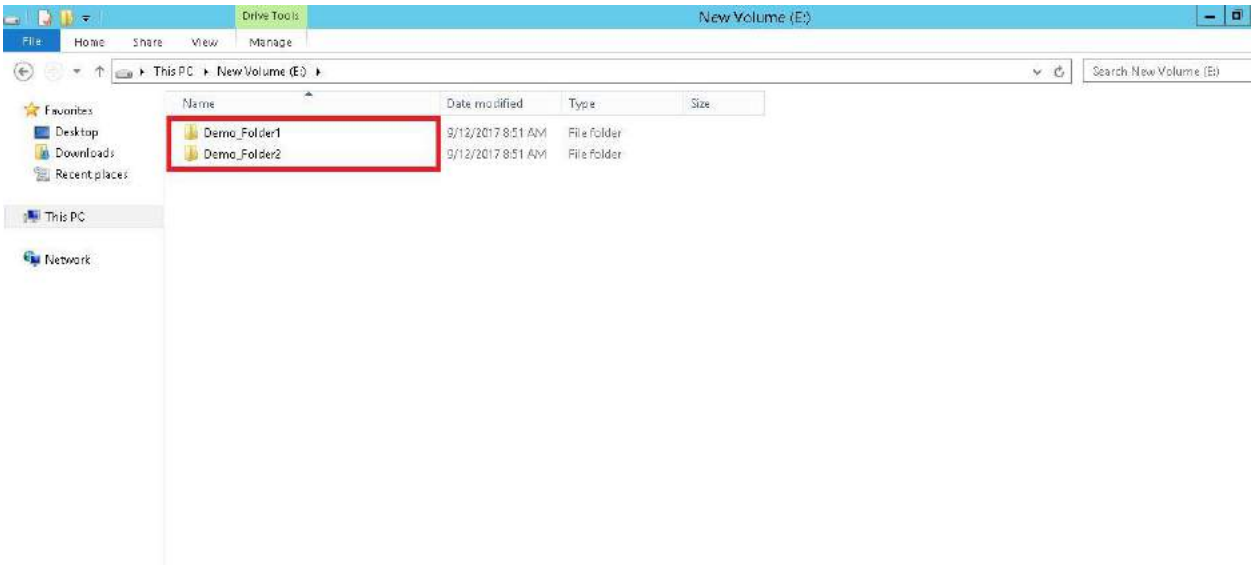


- Once the volume is created, click on Volume ID which would navigate to the Volume which is being created. After proceeding, click on attach a volume in any other available server under EC2. Follow the same steps which have been performed earlier to attach a new volume in a server as well as mounting of attached volume inside the server.





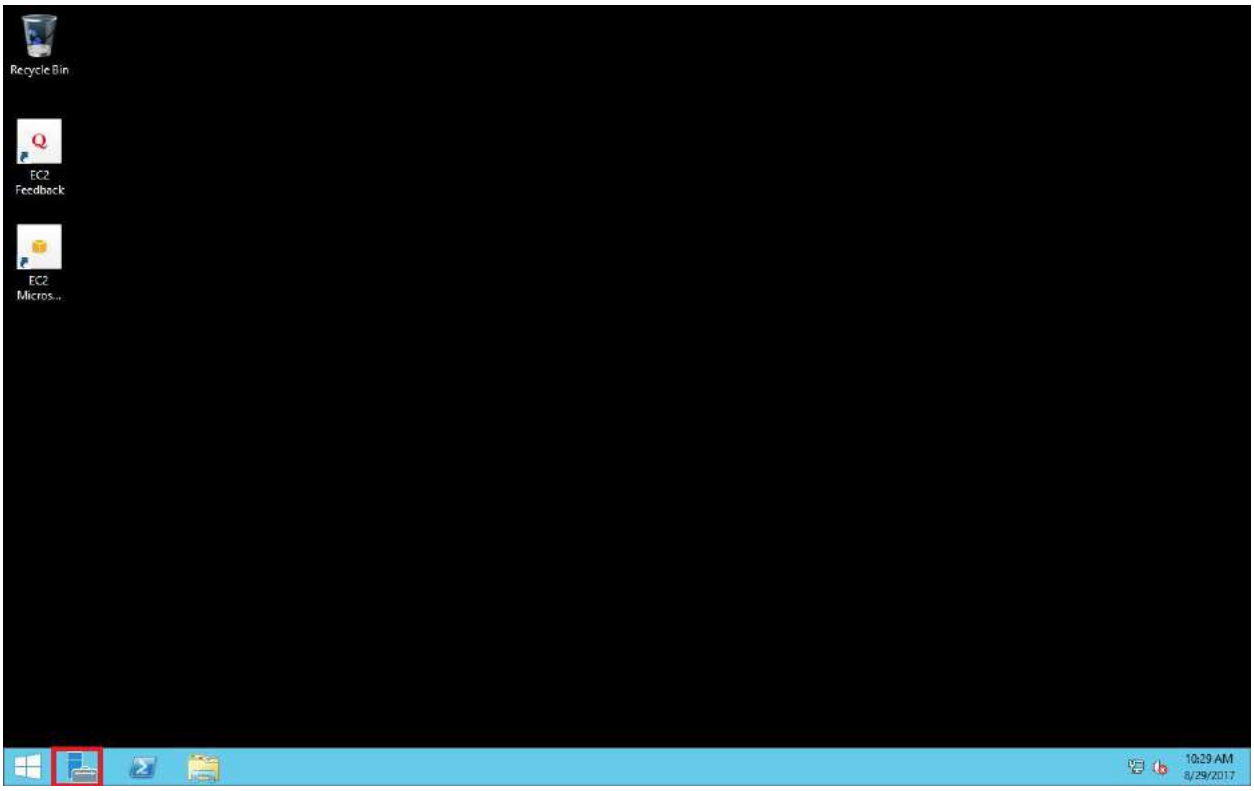
- Same folders would be found in newly attached volume in another server as like shown below.

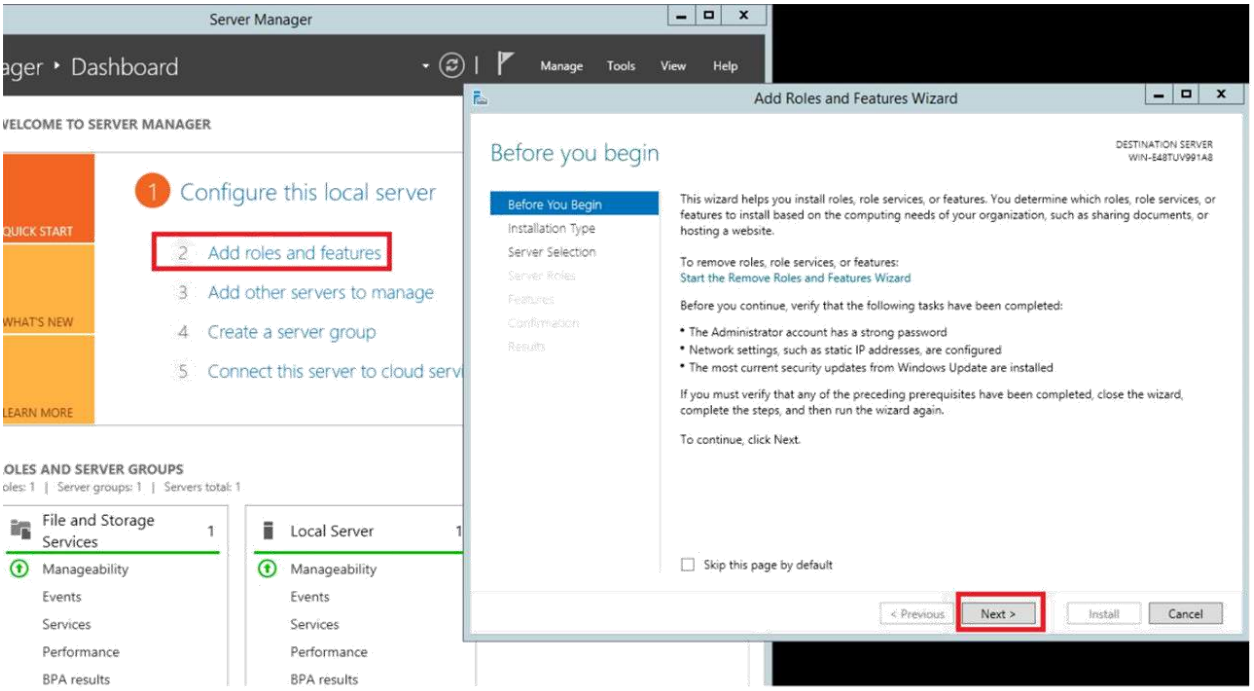


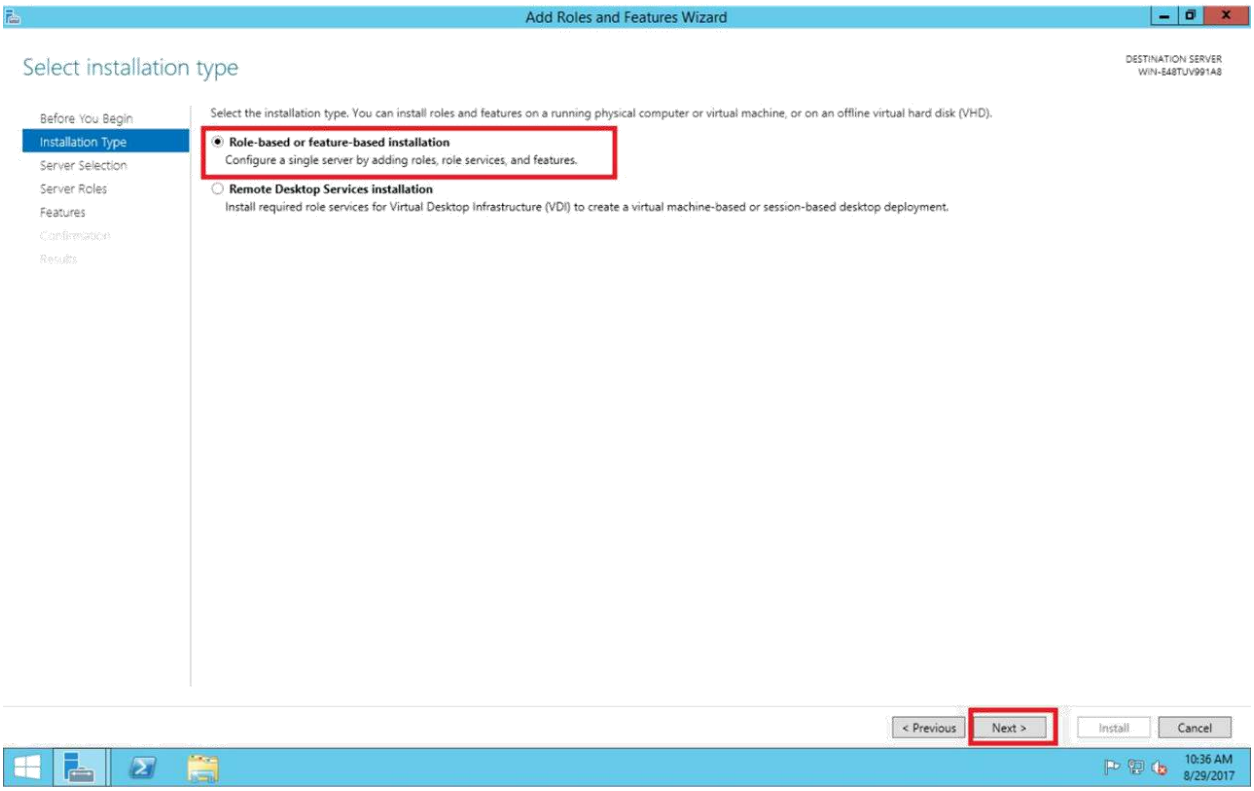
- This snapshot can be used to take the C Drive as a Snapshot and from that, it can be created as an AMI. So, whatever OS available in C Drive would be launched if we click on Launch Instance under the created image which is in AMI.
- Hence, the combinations of Volumes and Snapshot would be said as to be Elastic Block Store.

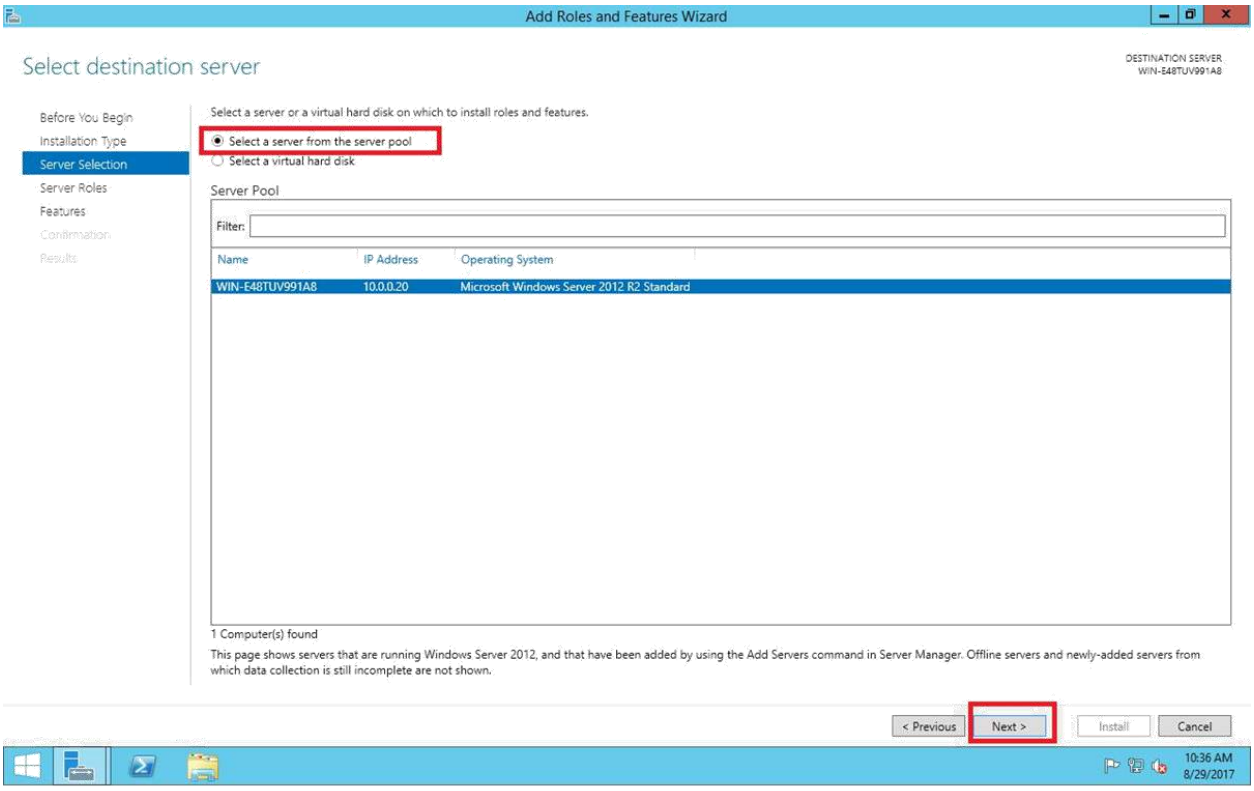
ELB (Elastic Load Balancer):

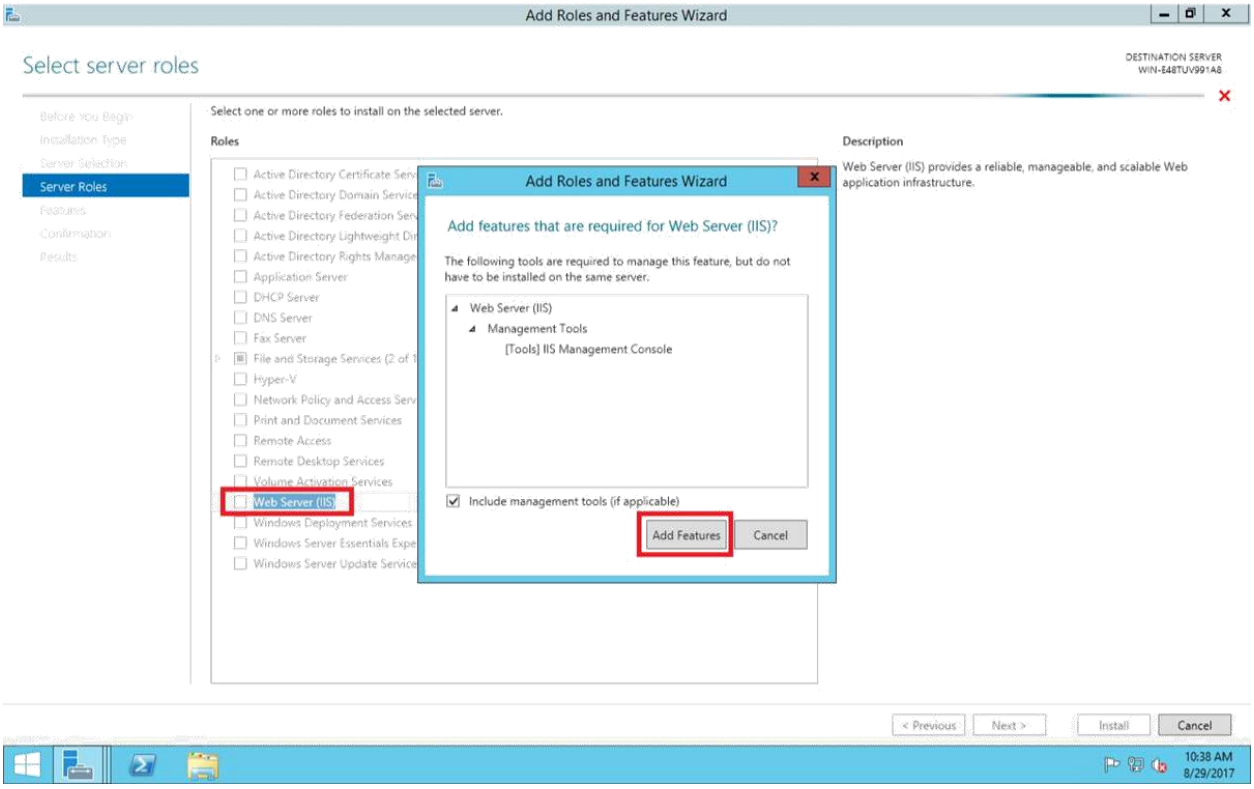
- Load Balancer is used to balance the load from 'N' number of users accessing any web-based application simultaneously.
- If any web application is running on two node architecture which is Application to be running on one server and database to be running on another server, it wouldn't be able to provide a stable accessibility of application all the times since number of users would be accessing the same application in parallel.
- When an application is being accessed by many users simultaneously, obviously server performance would be slower which would give a more business impact.
- To avoid such circumstances, Load Balancer comes into the picture to handle many application servers when number of users accessing an application simultaneously.
- Instead of setting up a Load Balancer in separate server, AWS providing it as PaaS service which is named as ELB (Elastic Load Balancer).
- Before getting started with ELB, create two Windows servers in a same VPC. Make sure, that VPC is available in two different Availability zones to provide higher availability of Load Balancer. EC2 Classic Servers also can be used for ELB and recommended way to use VPC servers to get end to end communication within servers without any delay.
- Launch these two servers by opening 3389 and 80 port number in security group which needs to be accessible globally by choosing anywhere option.
- After launching a new server, log into the same for installing IIS Web Server. Make sure to install IIS on both the servers. Steps to install IIS web server would be shown in below screenshot.
- Click on **Server Manager** >> **Roles and Features** >> Next >> Choose **Role Based or Feature Based Installation** >> Next >> Choose **Select a Server from the Server pool** >> Next >> Choose **Web Server IIS** >> click on **Add Features** >> Next >> Next >> Next >> Install >> Close.
- Installation of IIS would take around 5 minutes of time. Install IIS on both the servers which are running under same VPC and open default port number of IIS 80 on both the servers.




Server Manager
ager ▸ Dashboard
Manage
Tools
View
Help
VELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud servi
OLES AND SERVER GROUPS
oles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-E48TUV991A8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-E48TUV991A8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
10:36 AM
8/29/2017


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-E48TUV991A8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-E48TUV991A8
10.0.0.20
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
10:36 AM
8/29/2017


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-E48TUV991A8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Serv
Active Directory Domain Service
Active Directory Federation Serv
Active Directory Lightweight Di
Active Directory Rights Manage
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (2 of 1
Hyper-V
Network Policy and Access Serv
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Expe
Windows Server Update Service
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
10:38 AM
8/29/2017

Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-E48TUV991A8

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- [ ] .NET Framework 3.5 Features
- [x] .NET Framework 4.5 Features (2 of 7 installed)
- [ ] Background Intelligent Transfer Service (BITS)
- [ ] BitLocker Drive Encryption
- [ ] BitLocker Network Unlock
- [ ] BranchCache
- [ ] Client for NFS
- [ ] Data Center Bridging
- [ ] Direct Play
- [ ] Enhanced Storage
- [ ] Failover Clustering
- [ ] Group Policy Management
- [ ] IIS Hostable Web Core
- [ ] Ink and Handwriting Services
- [ ] Internet Printing Client
- [ ] IP Address Management (IPAM) Server
- [ ] iSNS Server service
- [ ] LPR Port Monitor
- [ ] Management OData IIS Extension
- [ ] Media Foundation
- [ ] Message Queuing
- [ ] Multipath I/O
- [ ] Network Load Balancing
- [ ] Peer Name Resolution Protocol
- [ ] Quality Windows Audio Video Experience

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous | Next > | Install | Cancel

10:40 AM
8/29/2017

Add Roles and Features Wizard

Web Server Role (IIS)

DESTINATION SERVER
WIN-E48TUV991A8

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, and Windows Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

< Previous | Next > | Install | Cancel

10:41 AM
8/29/2017

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-E48TUV991A8

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
- Role Services
- Confirmation
- Results

Select the role services to install for Web Server (IIS)

Role services

- [x] Web Server
  - [x] Common HTTP Features
    - [x] Default Document
    - [x] Directory Browsing
    - [x] HTTP Errors
    - [x] Static Content
    - [ ] HTTP Redirection
    - [ ] WebDAV Publishing
  - [x] Health and Diagnostics
    - [x] HTTP Logging
    - [ ] Custom Logging
    - [ ] Logging Tools
    - [ ] ODBC Logging
    - [ ] Request Monitor
    - [ ] Tracing
  - [x] Performance
    - [x] Static Content Compression
    - [ ] Dynamic Content Compression
  - [x] Security
    - [x] Request Filtering
    - [ ] Basic Authentication
    - [ ] Centralized SSL Certificate Support
    - [ ] Client Certificate Mapping Authentication
    - [ ] Digest Authentication
    - [ ] IIS Client Certificate Mapping Authentication

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

< Previous | Next > | Install | Cancel

10:42 AM
8/29/2017

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
WIN-E48TUV991A8

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
- Role Services
- Confirmation
- Results

To install the following roles, role services, or features on selected server, click Install.

[ ] Restart the destination server automatically if required

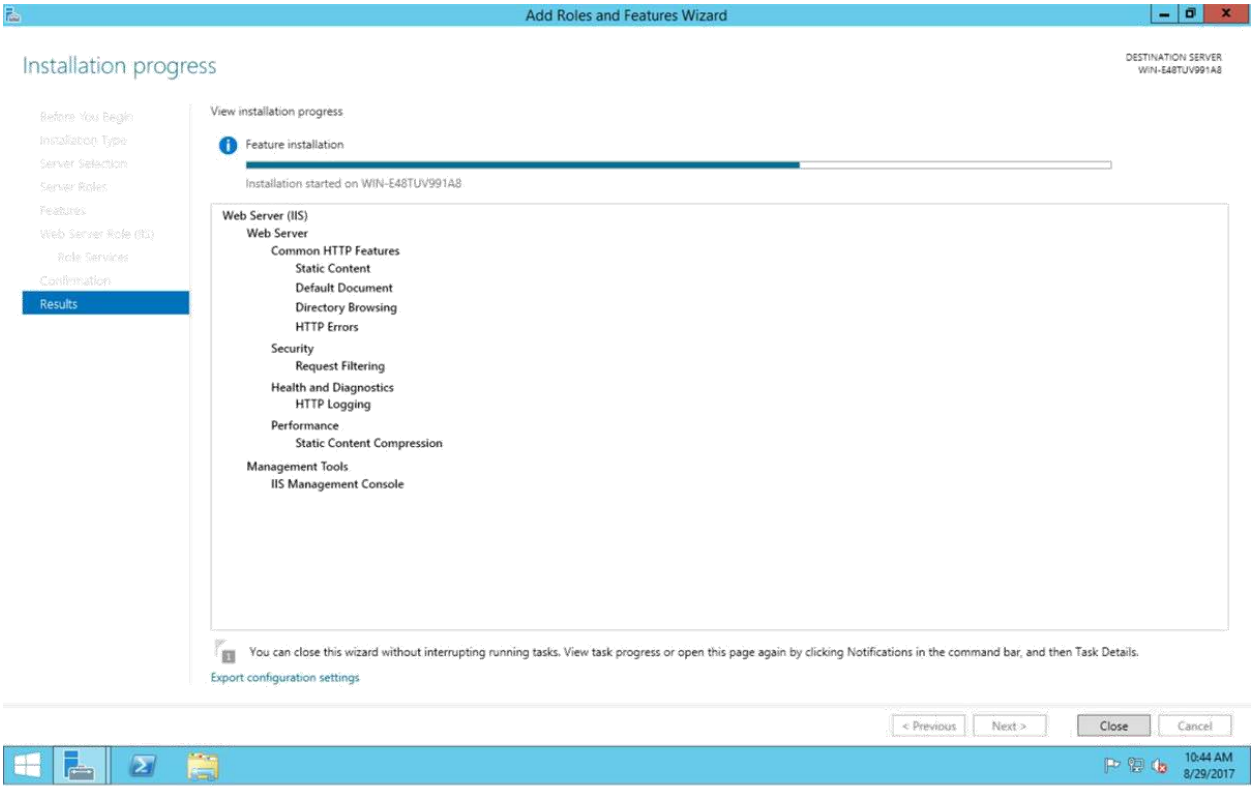
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

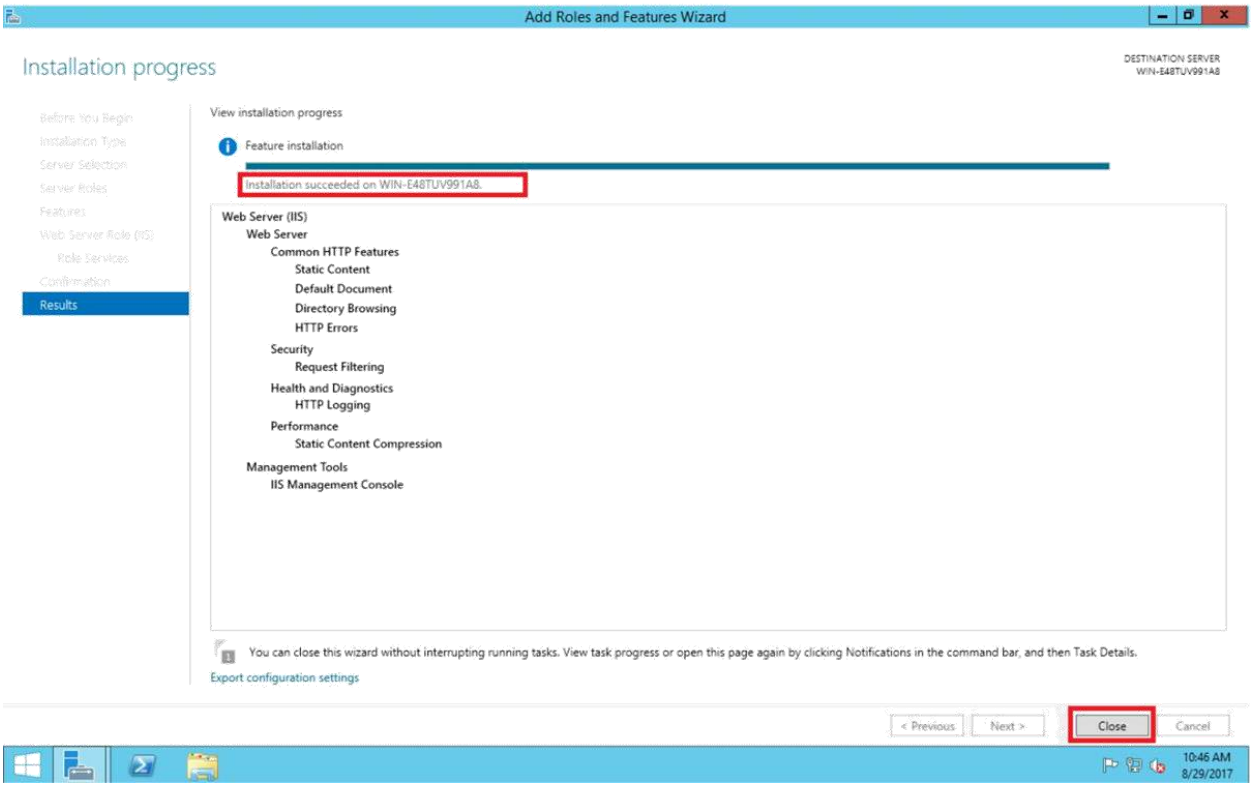
- Web Server (IIS)
  - Web Server
    - Common HTTP Features
      - Static Content
      - Default Document
      - Directory Browsing
      - HTTP Errors
    - Security
      - Request Filtering
    - Health and Diagnostics
      - HTTP Logging
    - Performance
      - Static Content Compression
  - Management Tools
    - IIS Management Console

Export configuration settings
Specify an alternate source path

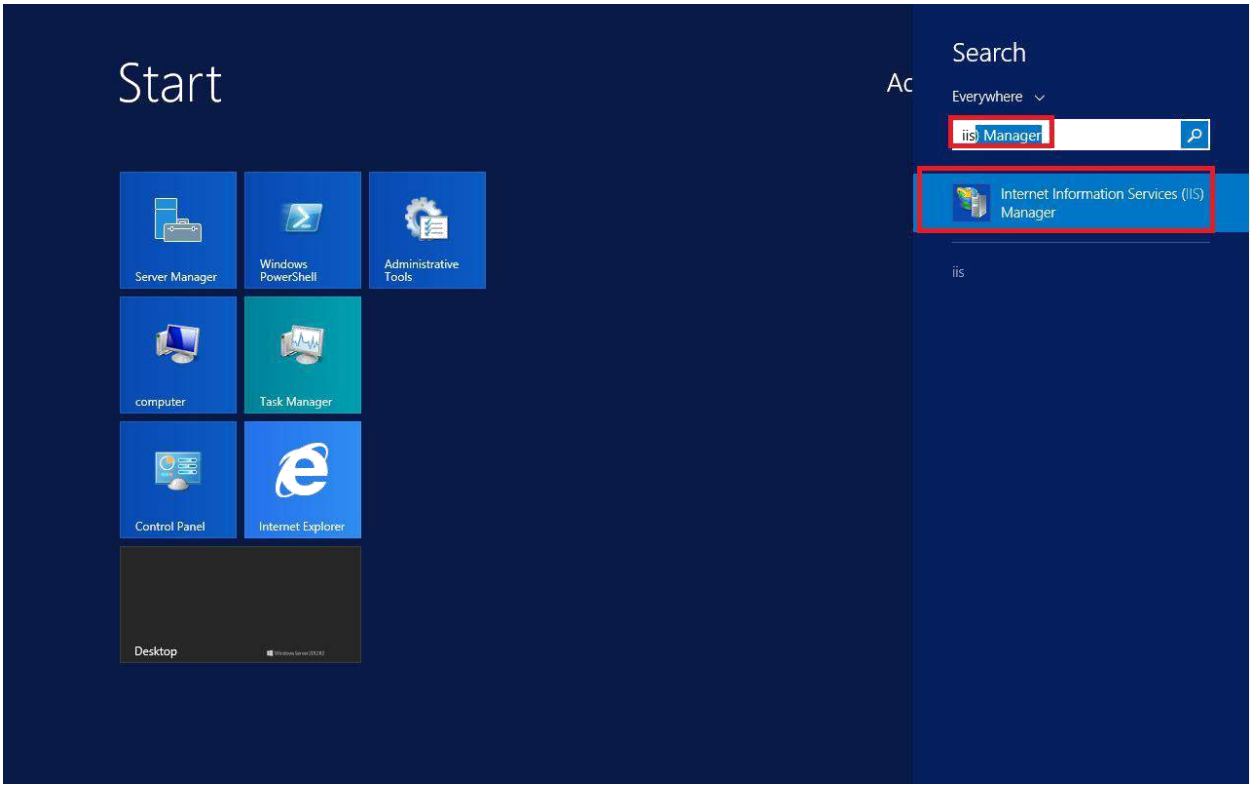
< Previous | Next > | Install | Cancel

10:43 AM
8/29/2017

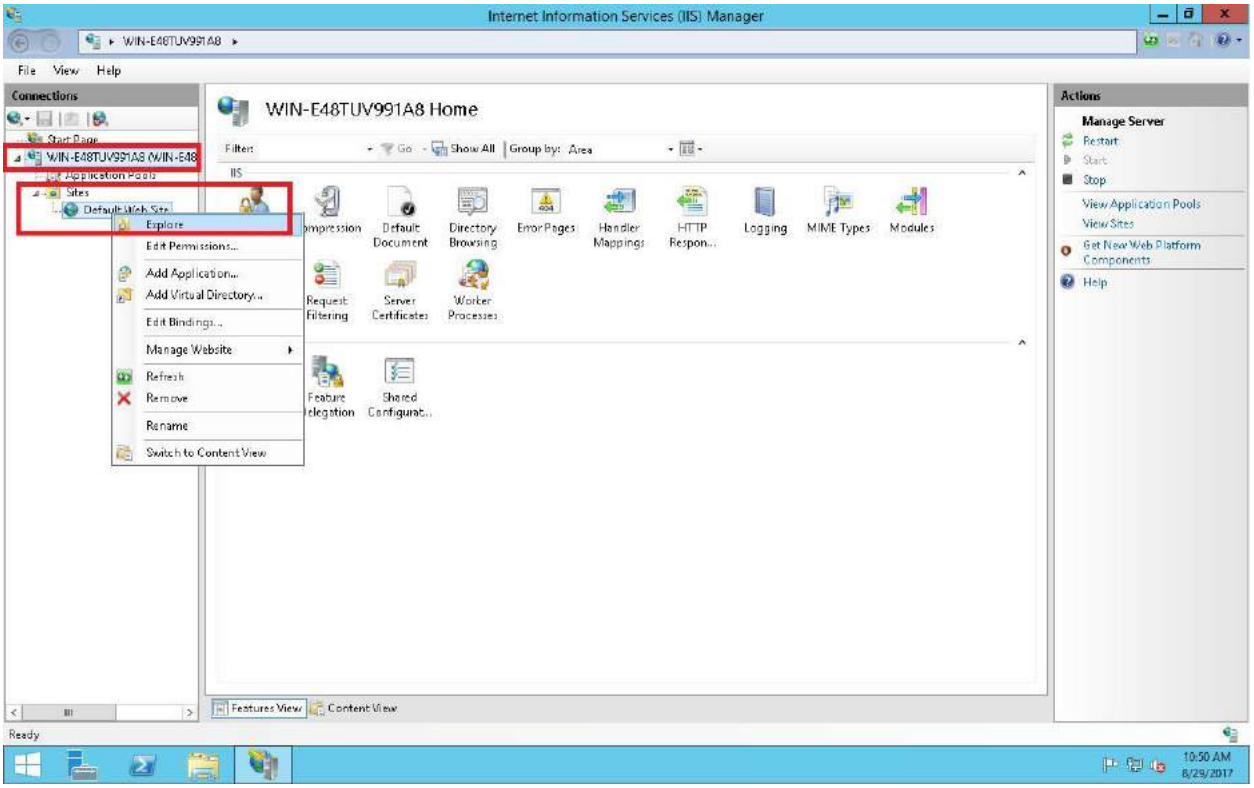




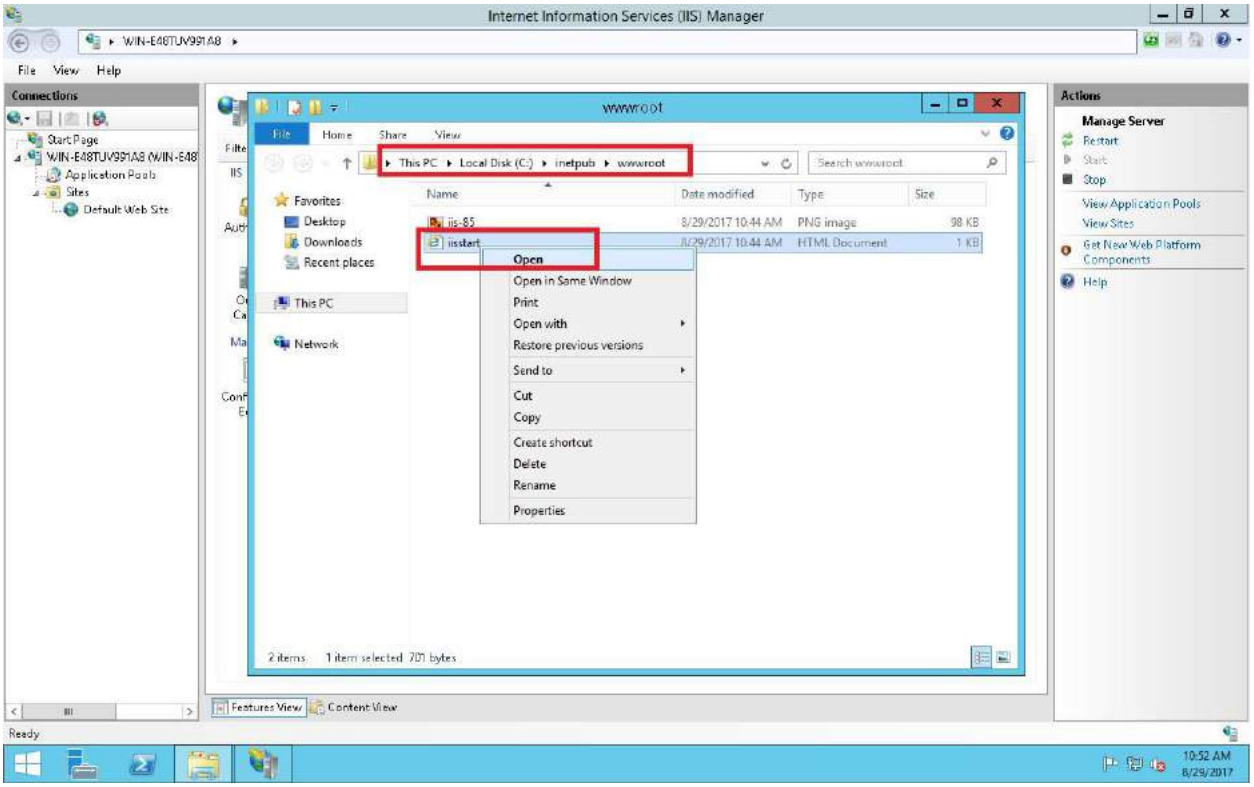
- Once IIS installation gets completed, change the home screen to wordings for easy identification as shown below. To do so, follow the below steps.
- Navigate to IIS by clicking on Windows Logo button and type IIS in search box.



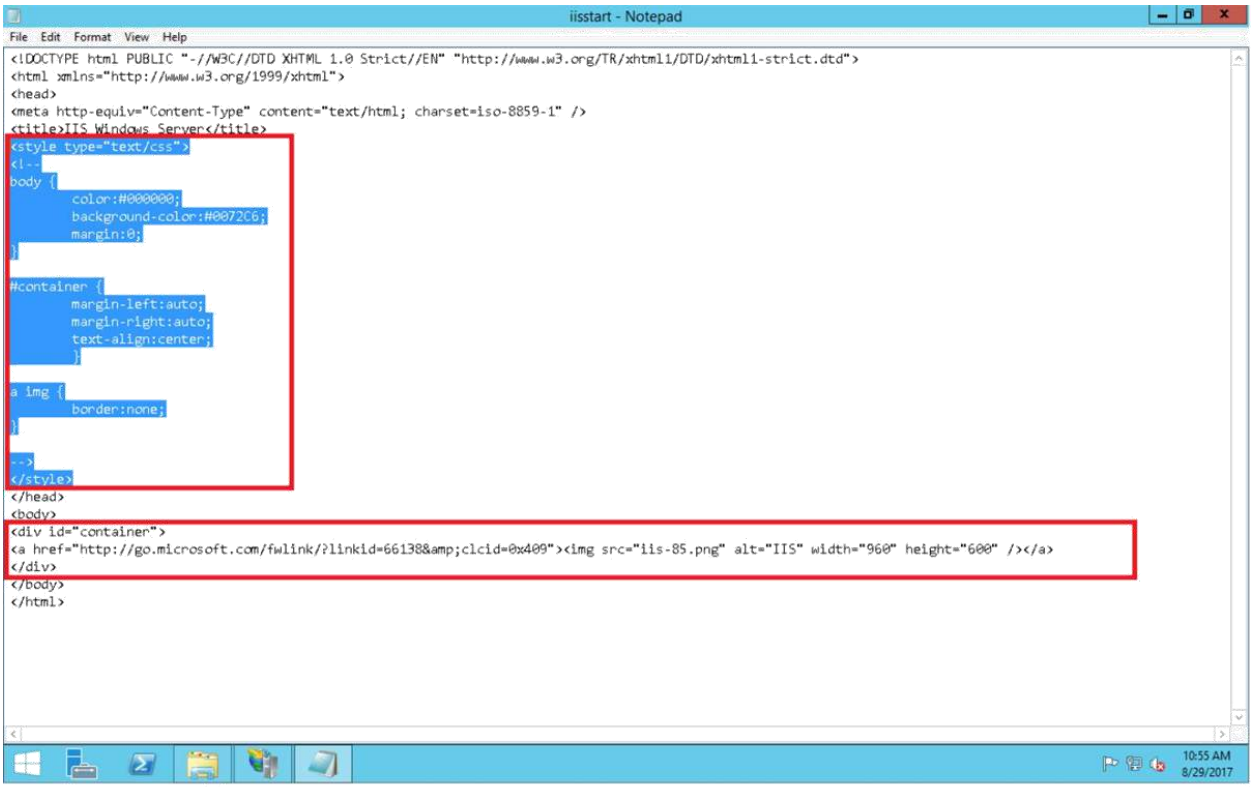
- After navigating to IIS, right click default web site and choose an option explore.

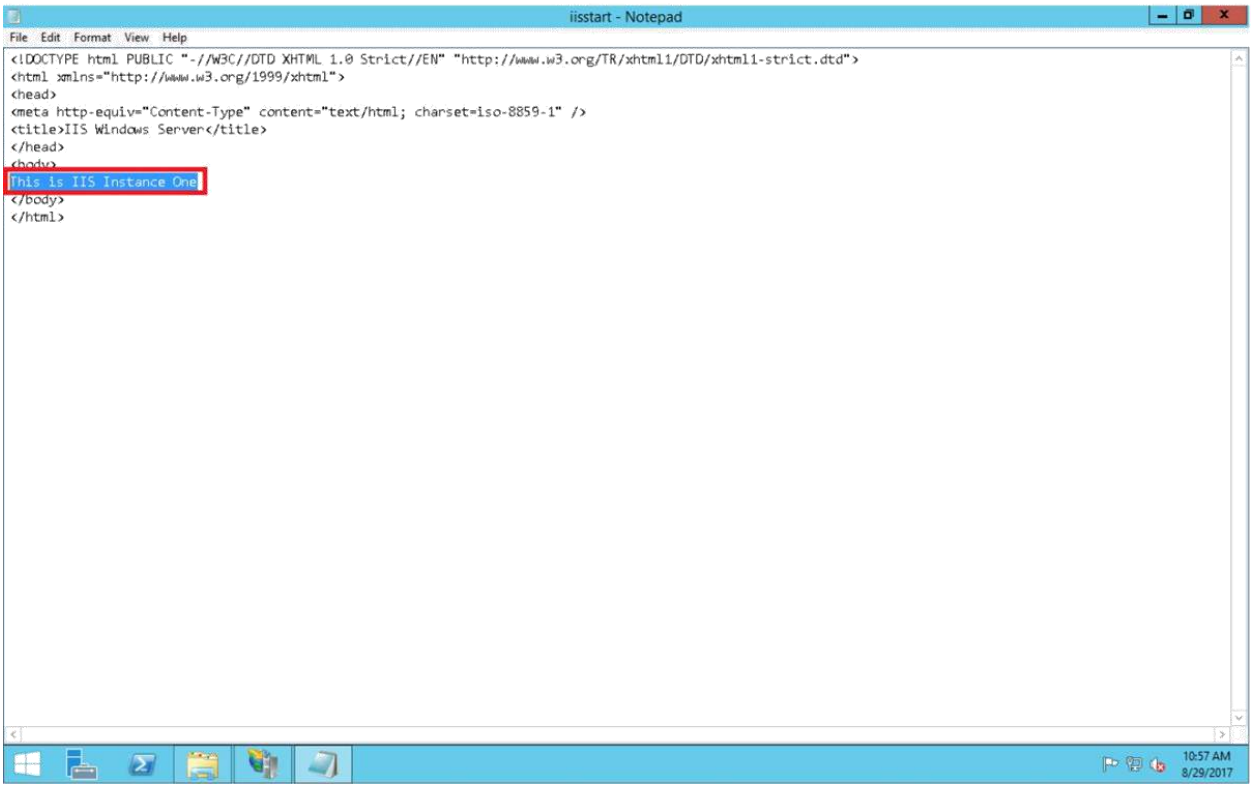


- After exploring the folder, right click on iisstart HTML document to open the document in notepad to change the wordings of IIS home screen.

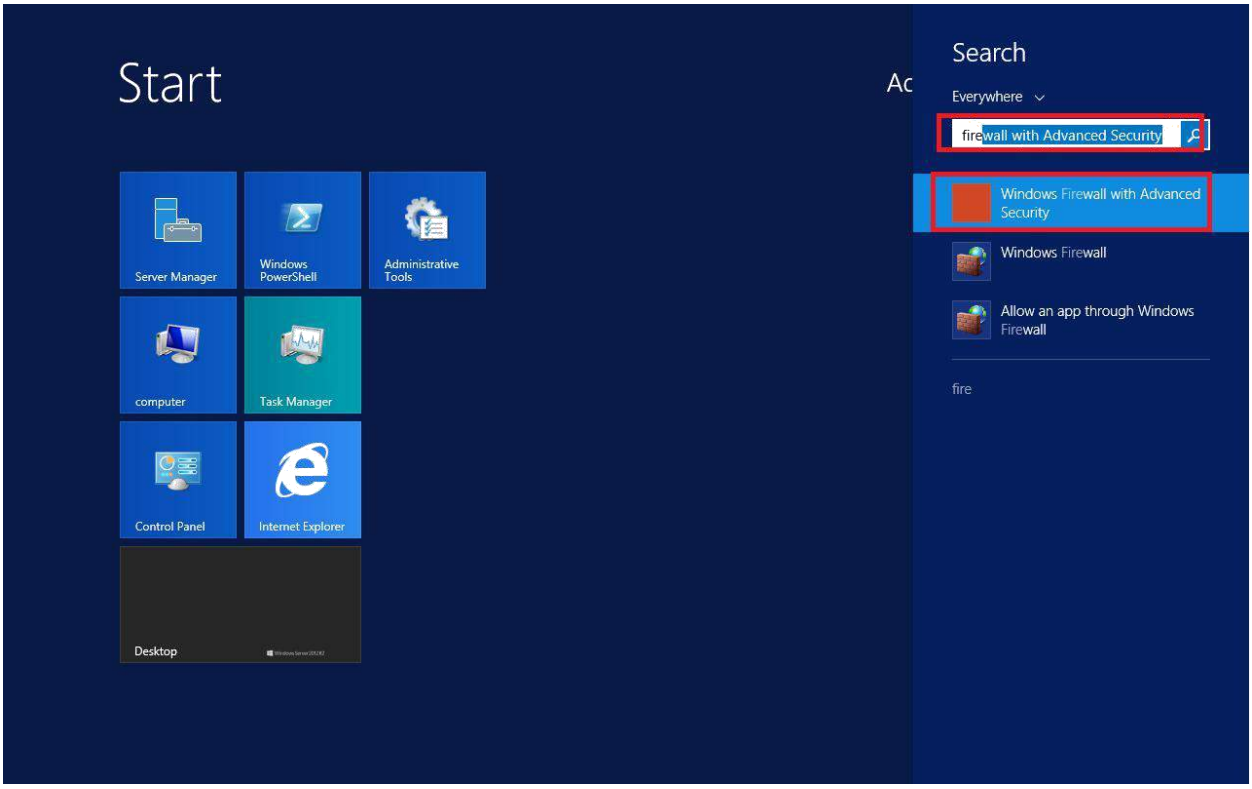


- After opening the HTML file, delete the below highlighted values and type the following as showing in the below screen.

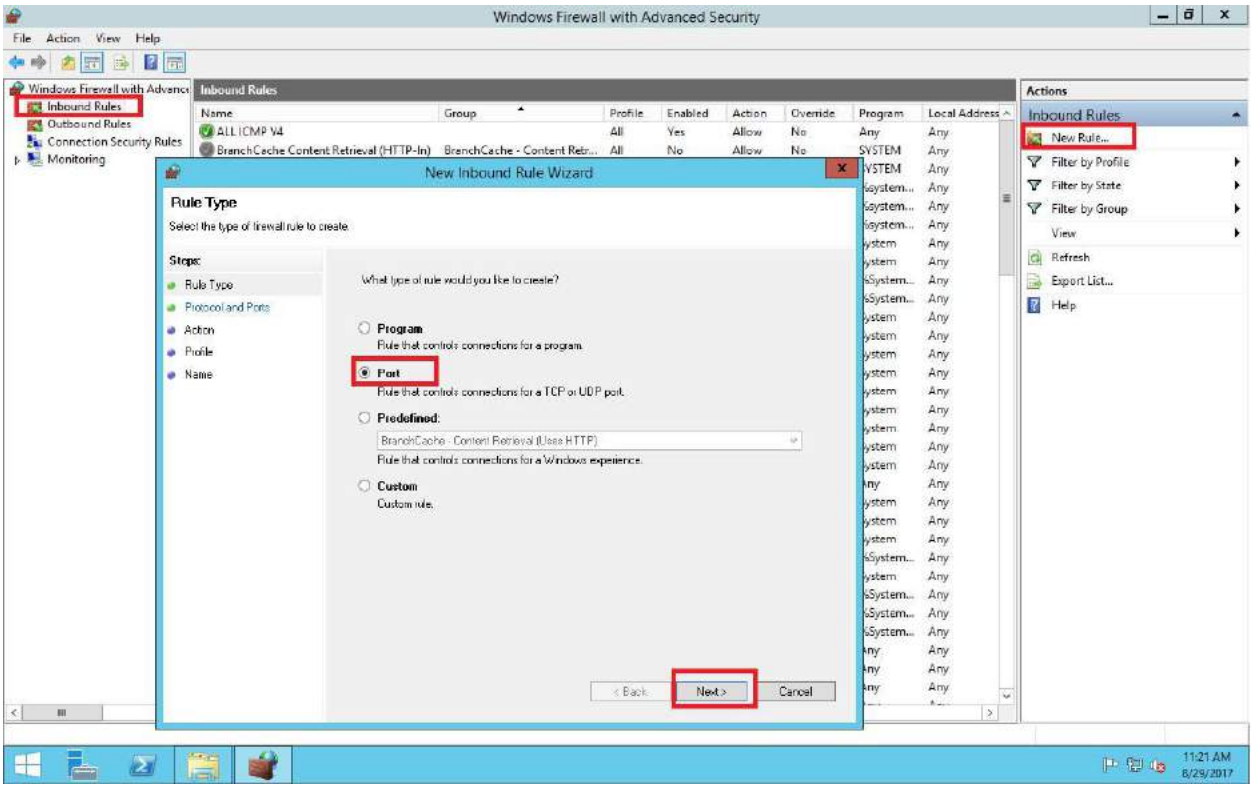




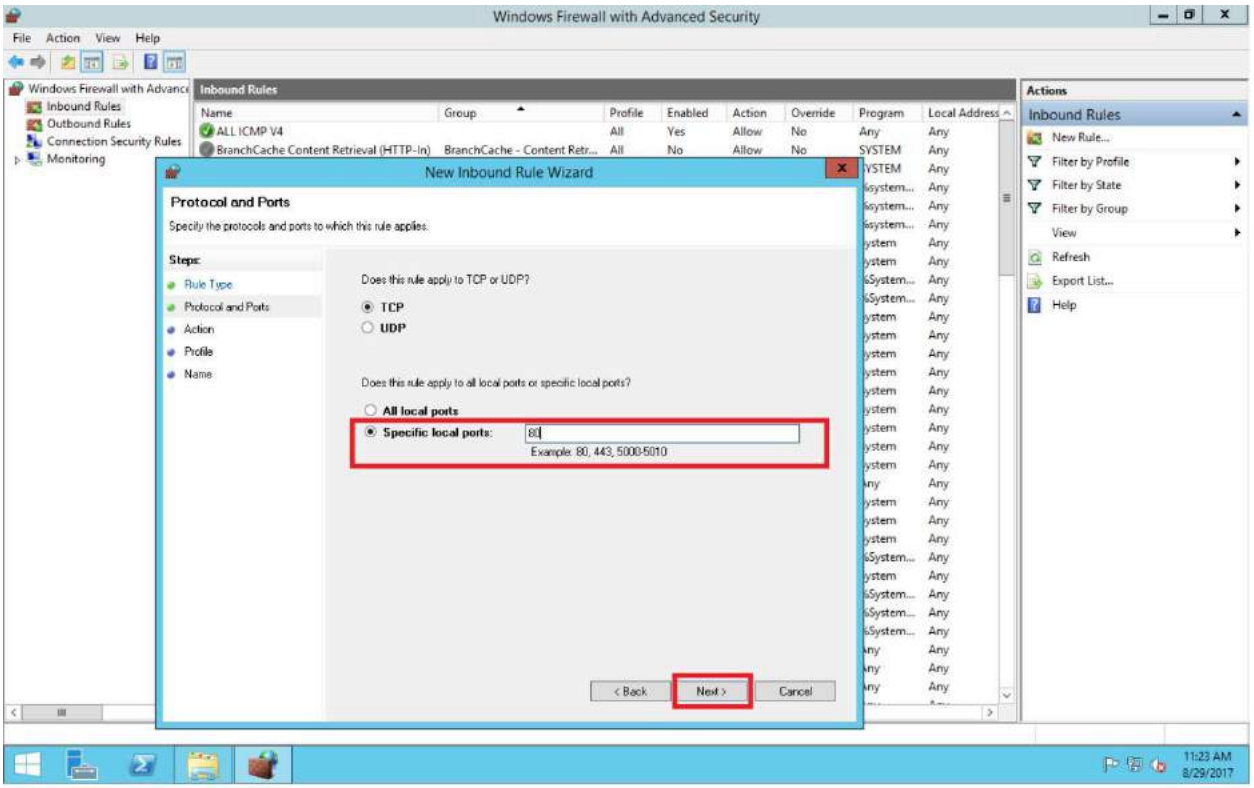
- After changing in HTML document, need to open default IIS port number 80 in an inbound firewall rule inside the servers.

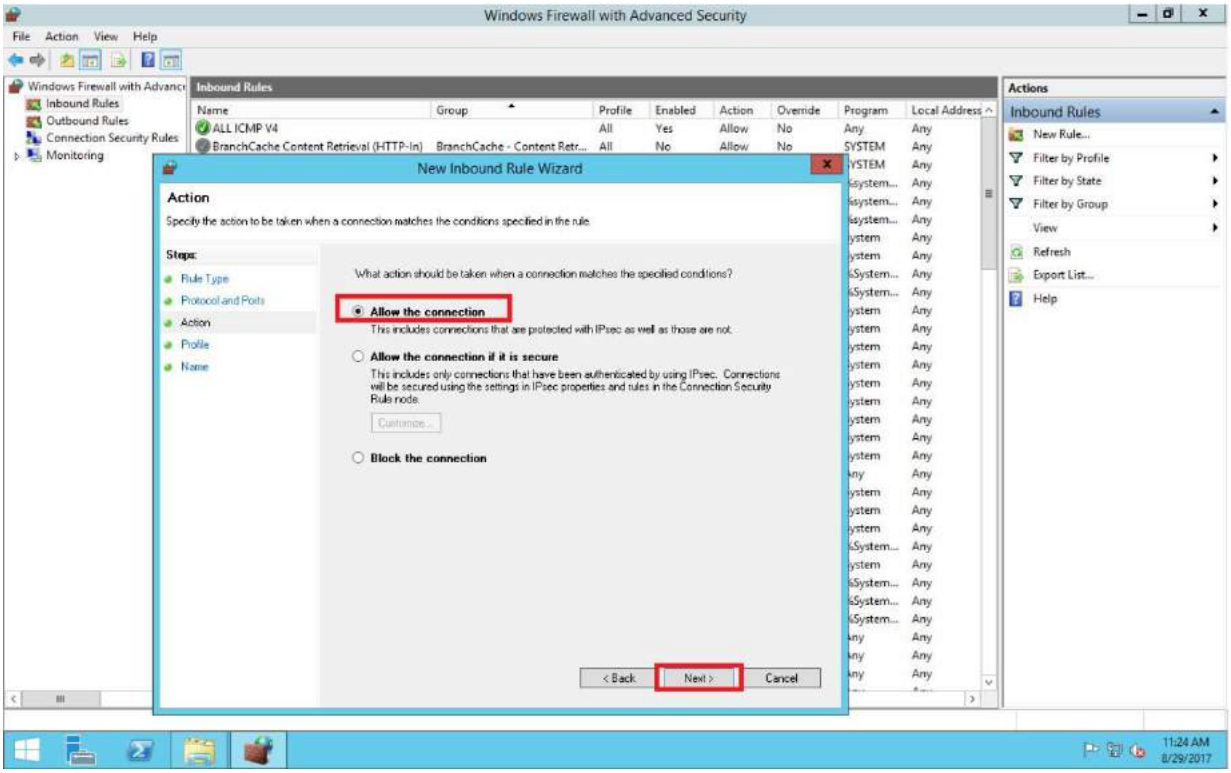


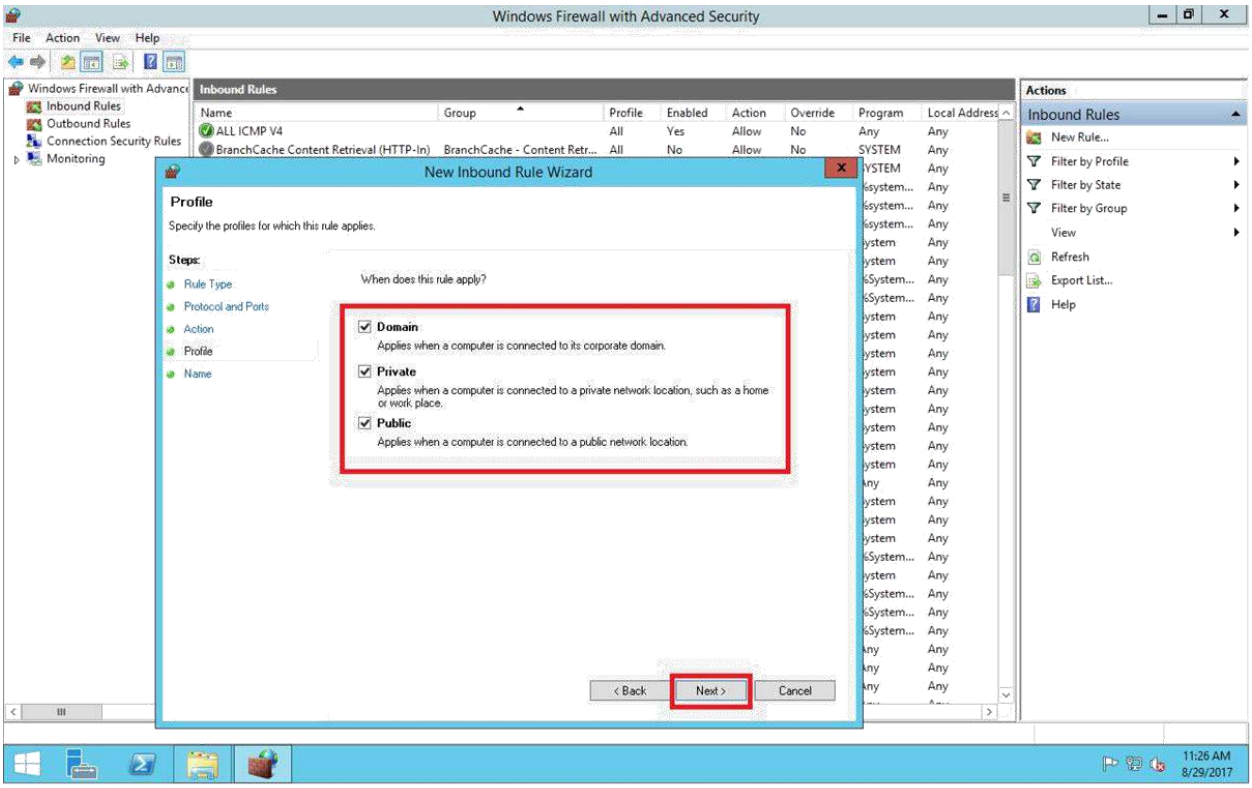
- After clicking on Windows Firewall with Advanced Security, choose Inbound Rules >> New Rule >> Port >> Next

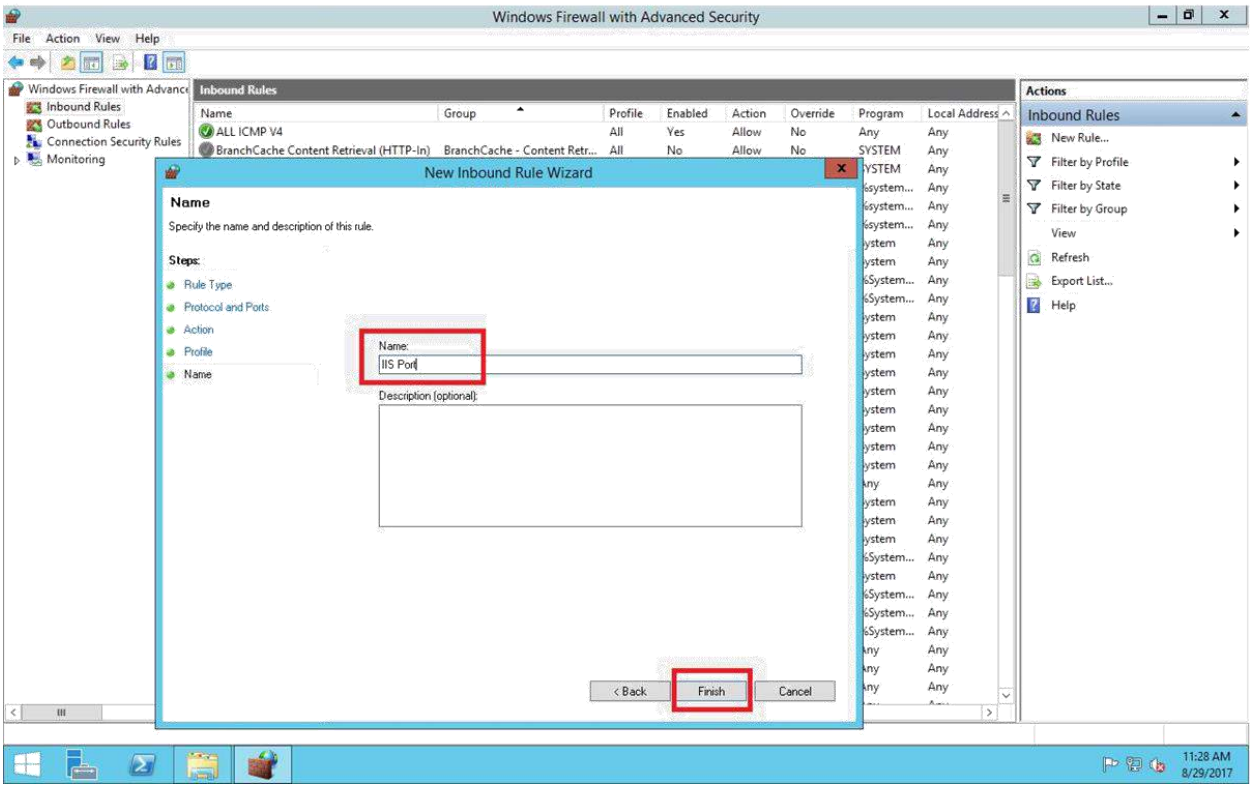


- Provide the port number as **80** which is default port number of IIS and click on Next >> Select **Allow the connection** >> Next >> Select **Domain, Public & Private** option >> Next >> **Provide any name as per your wish** >> Finish.



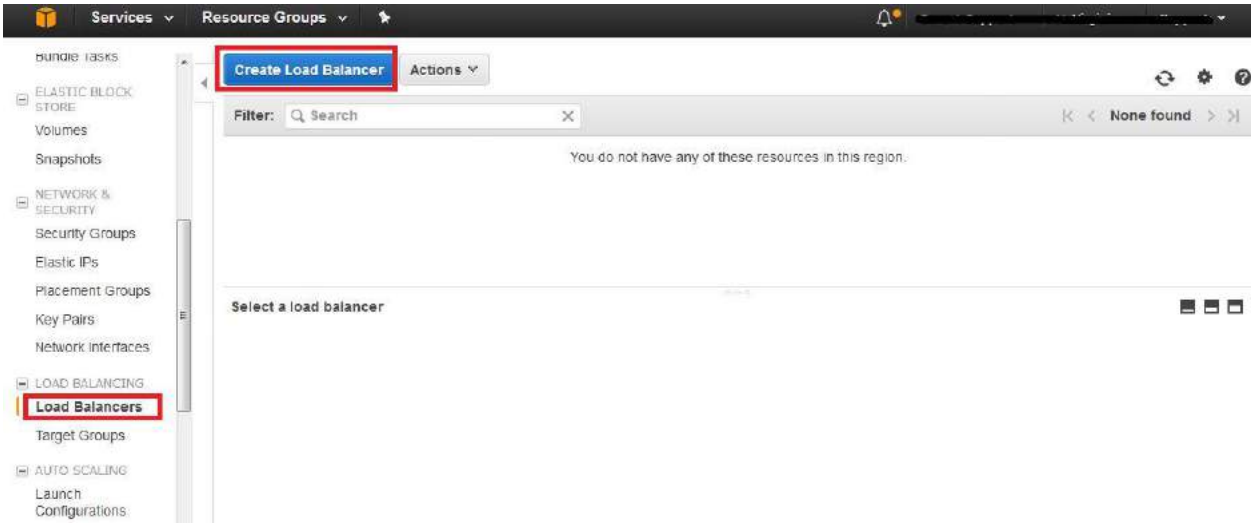



Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
ALL ICMP V4
BranchCache Content Retrieval (HTTP-In)
BranchCache - Content Retr...
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
11:26 AM
8/29/2017

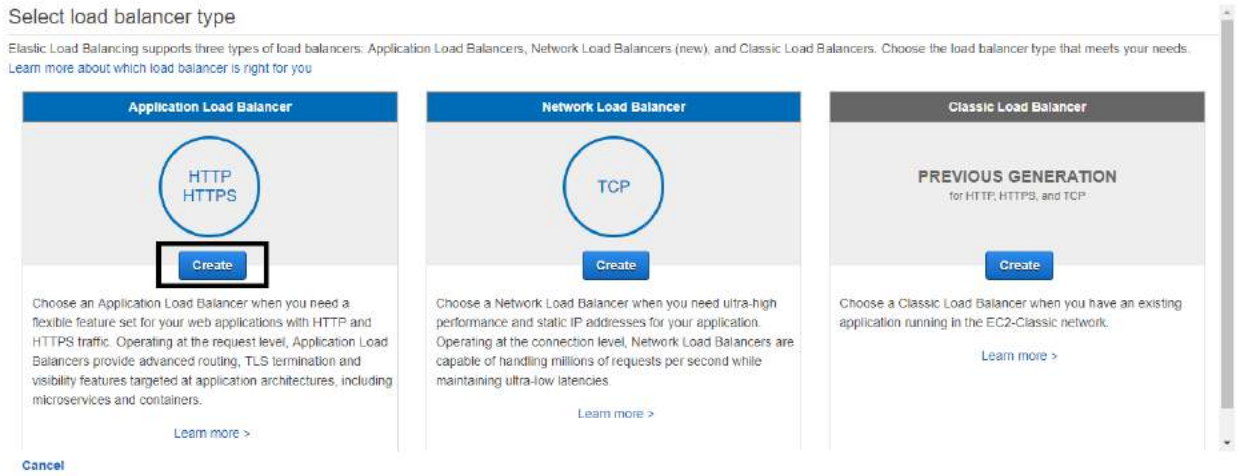

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
ALL ICMP V4
BranchCache Content Retrieval (HTTP-In)
BranchCache - Content Retr...
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
IIS Port
Description (optional):
< Back
Finish
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
11:28 AM
8/29/2017

- Access IIS by providing the server IP address in any browser in your computer as like shown below.
- Ensure the same on both the servers whether IIS is being accessible globally.

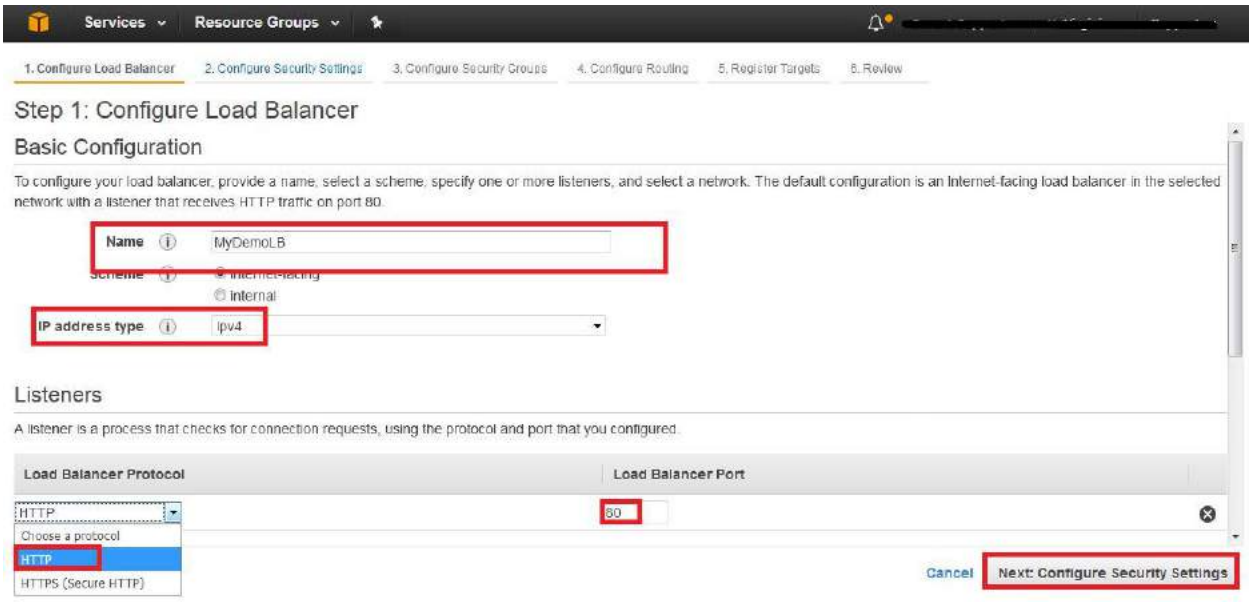
- After installing IIS and opening 80 port numbers on both the servers, we can get started with ELB by creating a new Load balancer in AWS.
- Select Services >> EC2 >> Load Balancers >> Click on Create Load Balancer

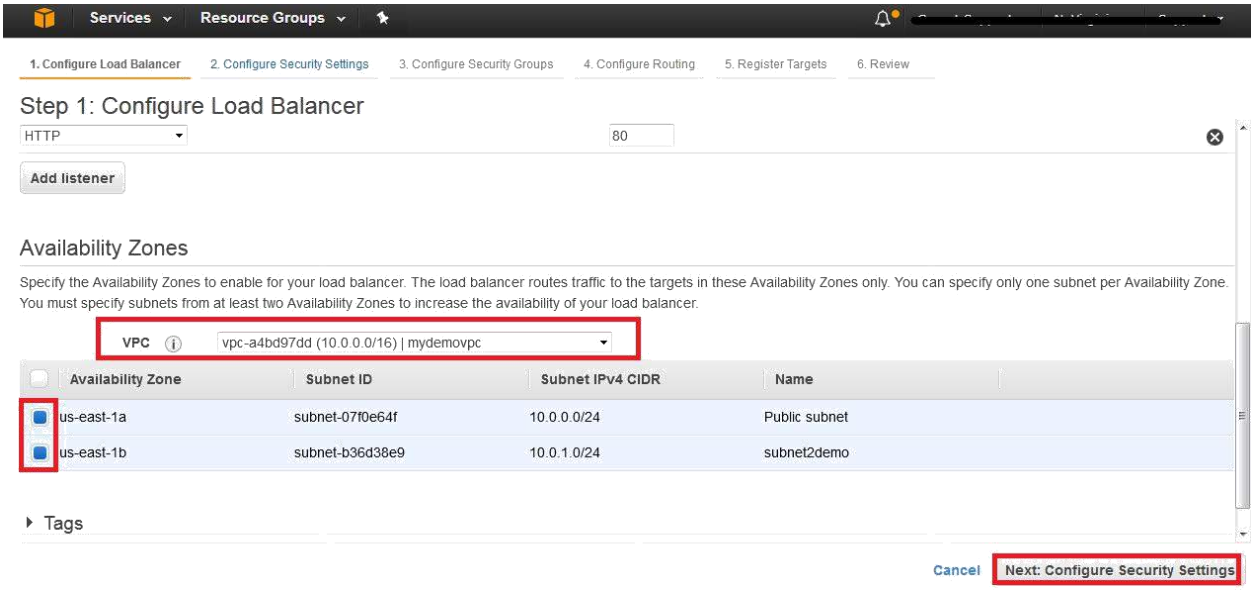


- There are three types of Elastic Load Balancing.
- **Application Load Balancer** – It makes routing decisions on application layer (HTTPS / HTTP) and it routes to one or more ports on each instance which is running on EC2. It supports for both EC2 Classic & VPC.
- **Classic Load Balancer** – It makes routing decision on Transport (TCP) and Application layer (HTTPS / HTTP) and it is supported for both Classic & VPC. Based on the requirement, you can choose any one type.
- **Network Load Balancer** - It makes routing decision only on Transport (TCP) and it is a new feature which has ultra-performance where it can handle 1000 request per second. Based on the requirement, you can choose any one type.

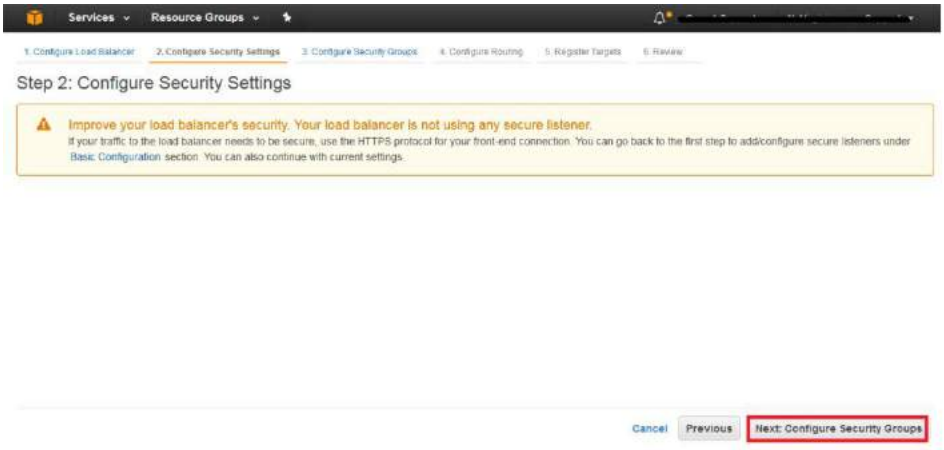


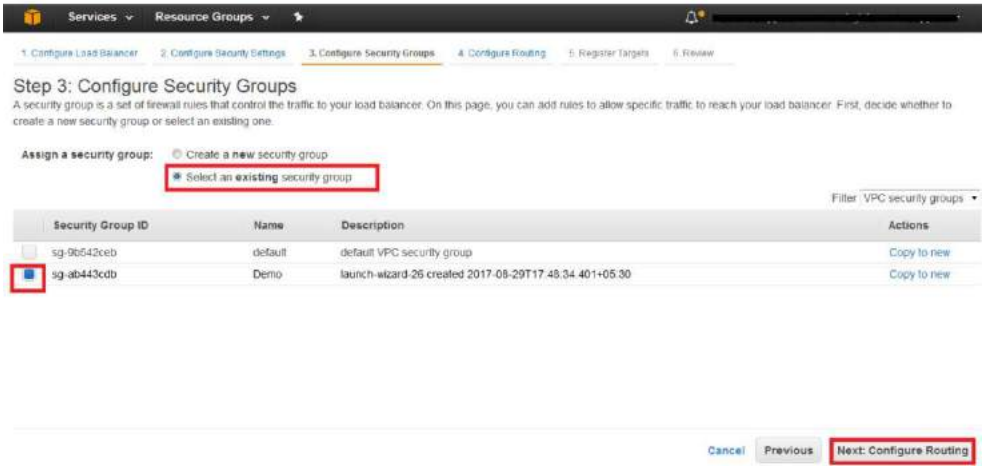
- Provide a LB Name as you wish, choose IP Address type as ipv4 and provide the Listener port based on your application need. You can choose any protocol HTTP or HTTPS and if you are selecting HTTPS, you would require to create a SSL certificates and the same must be uploaded to Certificate Manager in AWS Account. https://console.aws.amazon.com/acm/home?region=us-east-1#/firstrun/ . Moving down, you need to select your already created VPC and choose the Availability zone under the same VPC. We must select at least two Availability zone.



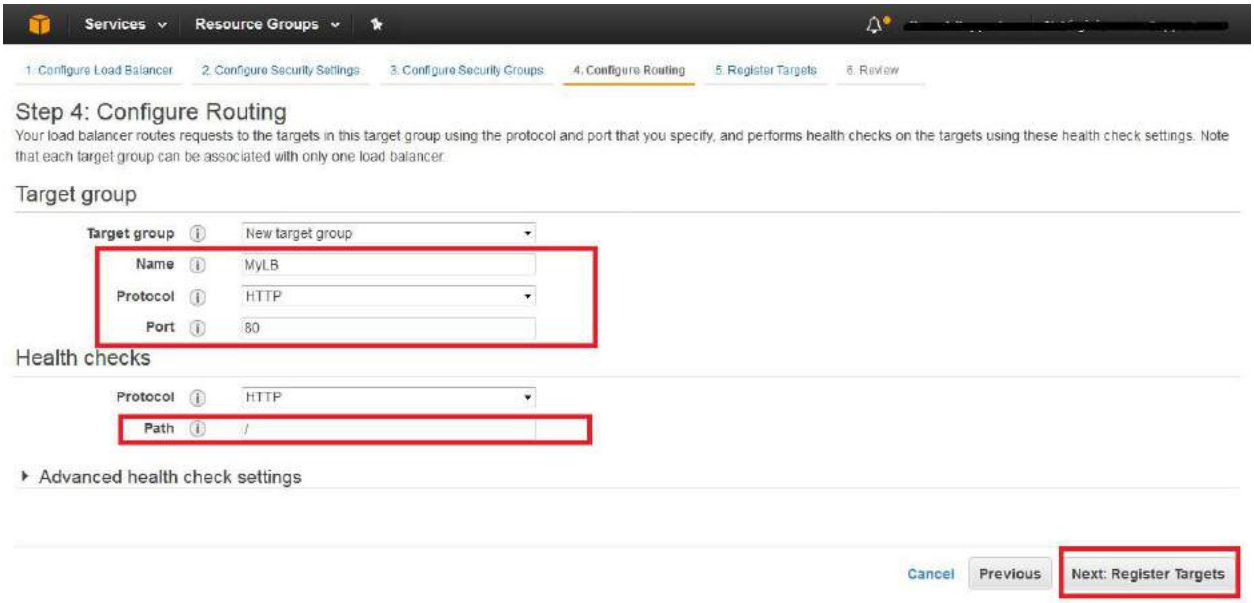


- Navigate to Security Settings to open the LB port which needs to be accessible globally. If you have an existing security group and the same can be used.

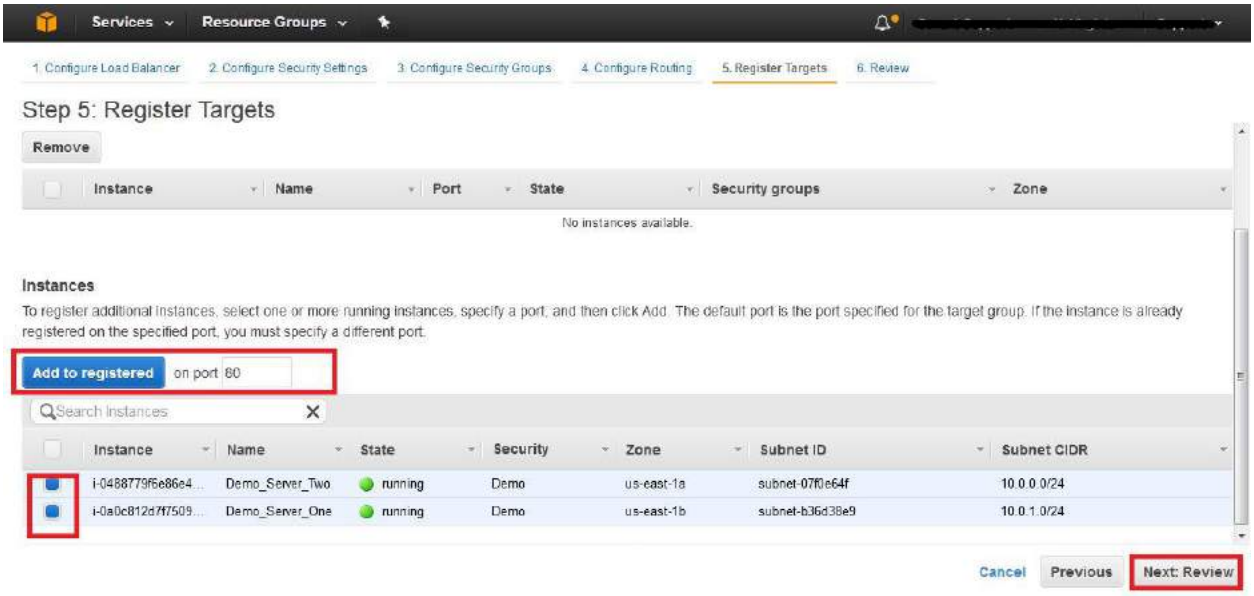




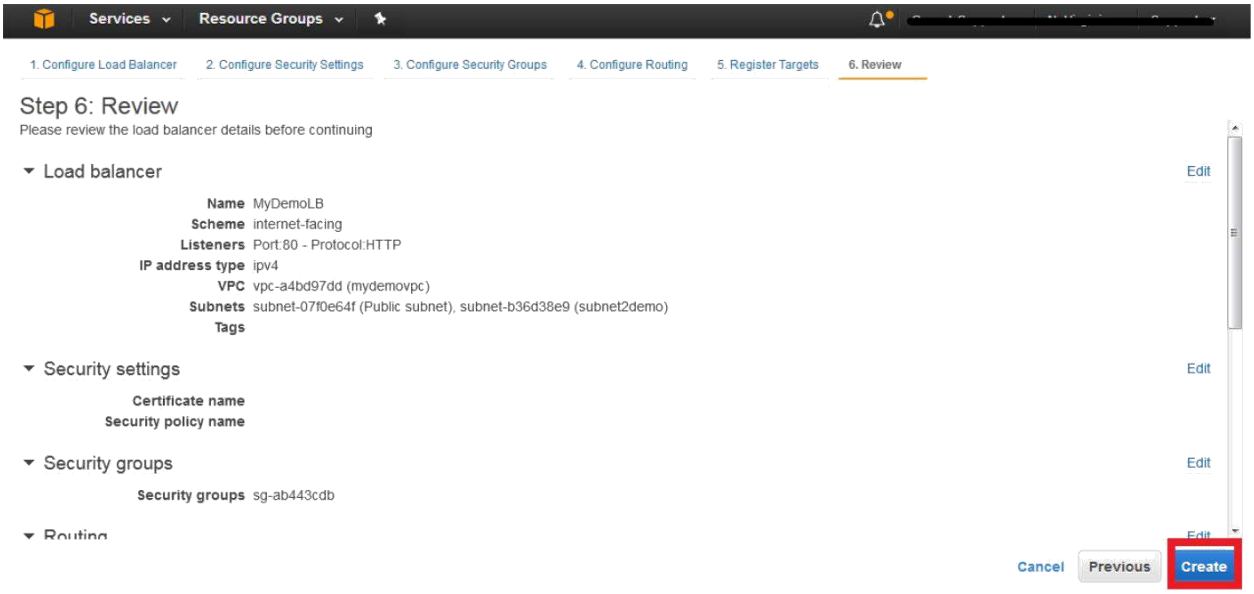
- Provide the Target Group name, choose the protocol, and provide the port number and context of your application as like shown below.



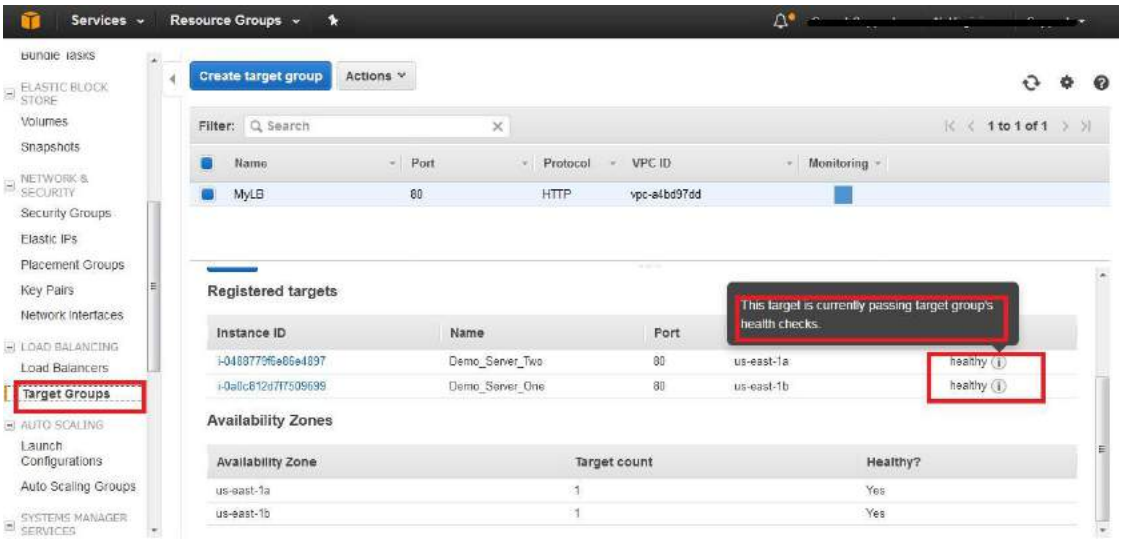
- Choose an application instances which is running under same VPC to connect it to Load Balancer by mentioning the port number in which application is being running up.



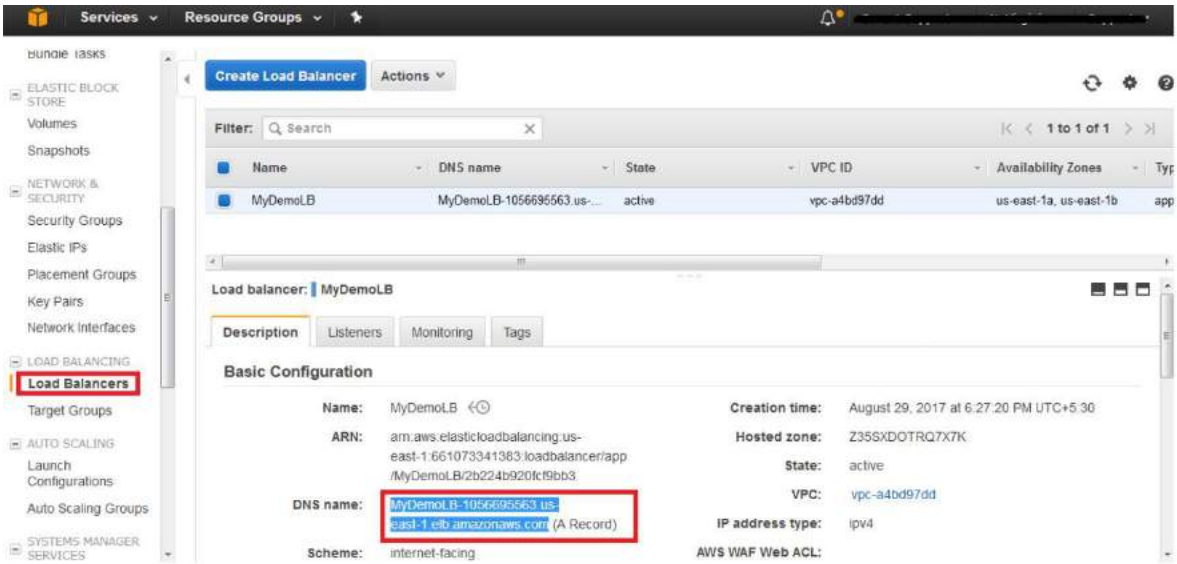
- Review the Summary of Load Balancer creation and click on create and close the page.



- Navigate to Target Groups to ensure the health status of added application instances whether it has been mapped to Load Balancer properly as like shown below. The Status needs to be changed as Healthy as like shown below.

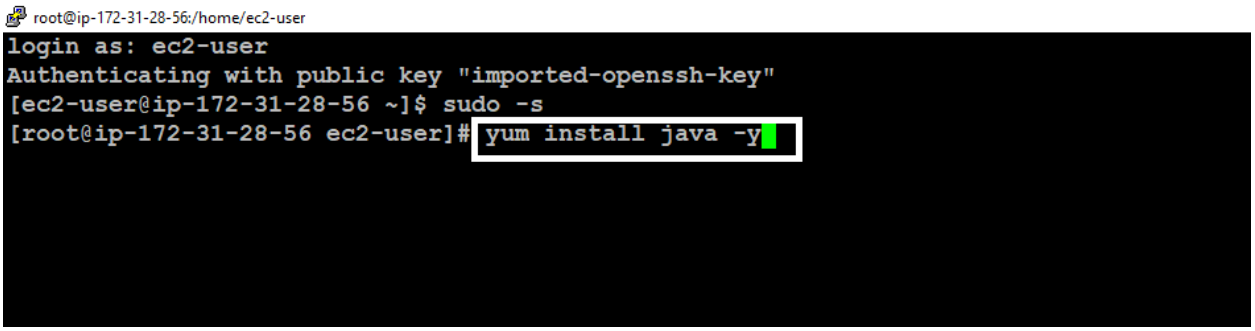


- Once the status has been changed to healthy, navigate back to Load Balancer to copy the domain name and access it in any of the web browser. Hence, application servers are balanced with load balancer. Creation of Load Balancer for both Classic and Application are similar except few steps.



Network Load Balancer:

- Create a two Linux Server for installing Tomcat in 8080 TCP port before creating a Network Load Balancer.
- After creation of Linux Server, login to the same and install Java on that EC2 instance using the below command.



- Followed by install wget using below command.

```
  libXcomposite.x86_64 0:0.4.4-4.1.el7                libXext.x86_64 0:1.3.3-3.el7
  libXfont.x86_64 0:1.5.2-1.el7                       libXi.x86_64 0:1.7.9-1.el7
  libXrender.x86_64 0:0.9.10-1.el7                    libXtst.x86_64 0:1.2.3-1.el7
  libfontenc.x86_64 0:1.1.3-3.el7                     libjpeg-turbo.x86_64 0:1.2.90-5.el7
  libpng.x86_64 2:1.5.13-7.el7_2                      libxcb.x86_64 0:1.12-1.el7
  lksctp-tools.x86_64 0:1.0.17-2.el7                  python-javapackages.noarch 0:3.4.1-11.el7
  stix-fonts.noarch 0:1.1.0-5.el7                     ttmkfdir.x86_64 0:3.0.9-42.el7
  tzdata-java.noarch 0:2018e-3.el7                    xorg-x11-font-utils.x86_64 1:7.5-20.el7
  xorg-x11-fonts-Type1.noarch 0:7.5-9.el7

Dependency Updated:
  nspr.x86_64 0:4.19.0-1.el7_5                  nss.x86_64 0:3.36.0-5.el7_5           nss-softokn.x86_64 0:3.36.0-5.el7_5
  nss-softokn-freebl.x86_64 0:3.36.0-5.el7_5    nss-sysinit.x86_64 0:3.36.0-5.el7_5   nss-tools.x86_64 0:3.36.0-5.el7_5
  nss-util.x86_64 0:3.36.0-1.el7_5

Complete!
[root@ip-172-31-28-56 ec2-user]# yum install wget -y
```

- Get the download URL of Apache 8.0.32 version Tomcat and download on the created EC2 Instance.

```
Total download size: 547 k
Installed size: 2.0 M
Downloading packages:
wget-1.14-15.el7_4.1.x86_64.rpm                                                          | 547 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : wget-1.14-15.el7_4.1.x86_64                                                                  1/1
  Verifying  : wget-1.14-15.el7_4.1.x86_64                                                                  1/1

Installed:
  wget.x86_64 0:1.14-15.el7_4.1

Complete!
[root@ip-172-31-28-56 ec2-user]# wget http://redrockdigimark.com/apachemirror/tomcat/tomcat-8/v8.5.32/bin/apache-tomcat-8
5.32.tar.gz
```

- Extract the tar file using the below command.

```
root@ip-172-31-28-56:/home/ec2-user
[root@ip-172-31-28-56 ec2-user]# ls
apache-tomcat-8.5.32.tar.gz
[root@ip-172-31-28-56 ec2-user]# tar -xvzf apache-tomcat-8.5.32.tar.gz
```

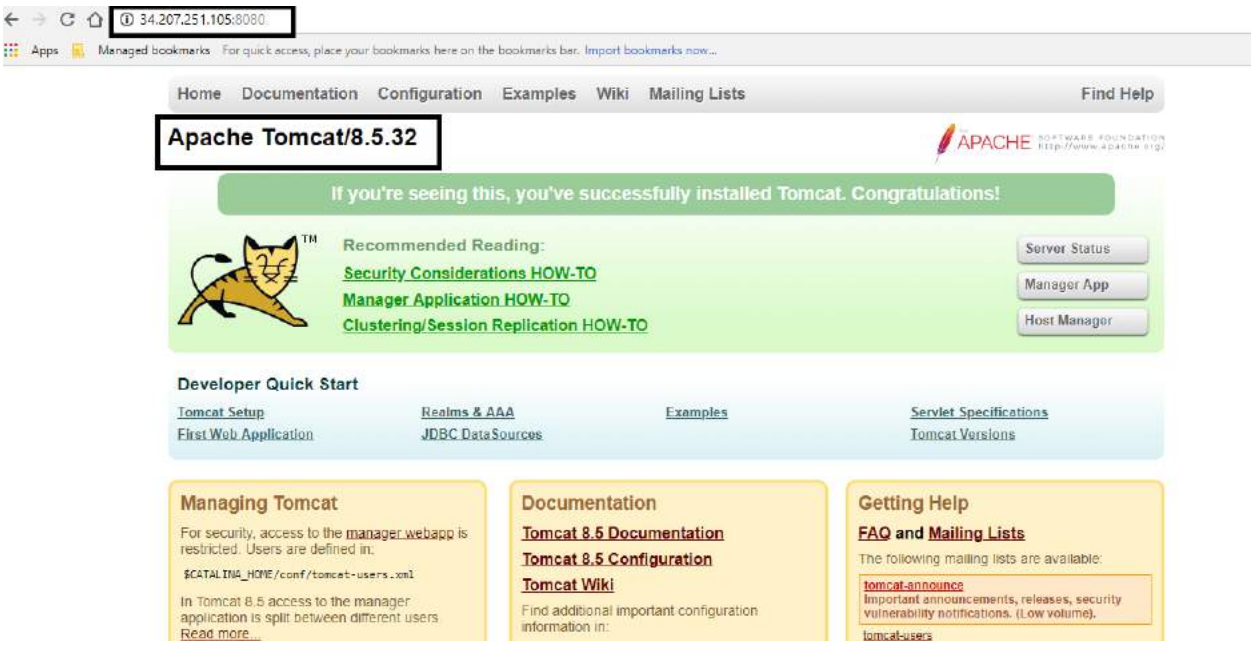
- Provide the permission for extracted folder.

```
root@ip-172-31-28-56:/home/ec2-user
[root@ip-172-31-28-56 ec2-user]# ls
apache-tomcat-8.5.32  apache-tomcat-8.5.32.tar.gz
[root@ip-172-31-28-56 ec2-user]# chmod -R 766 apache-tomcat-8.5.32
```

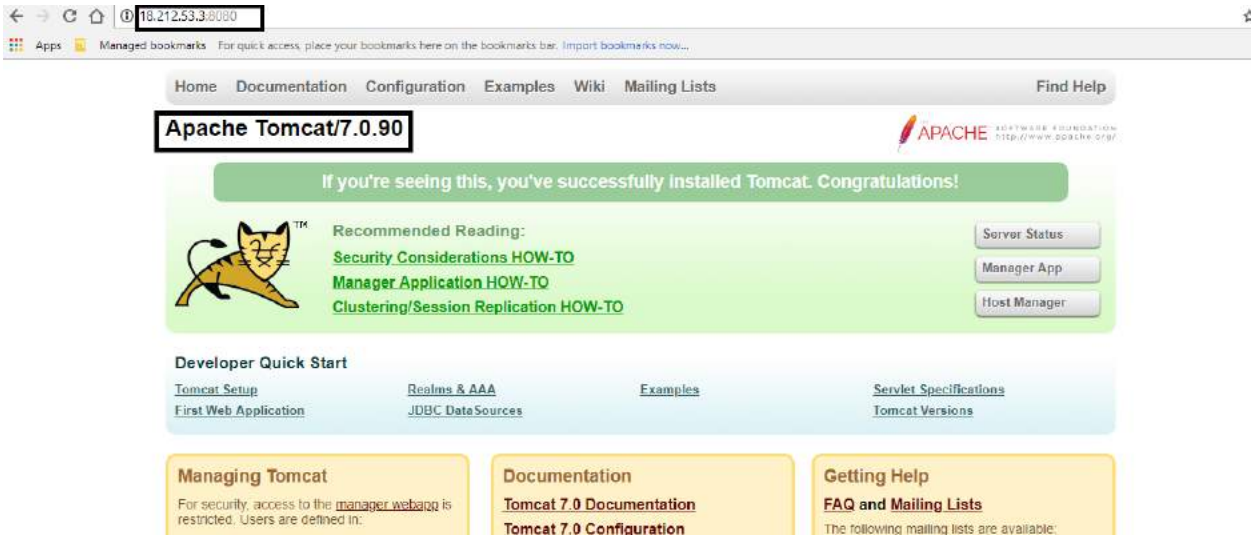
- Navigate to bin folder and start the Tomcat using below command.

```
root@ip-172-31-28-56:/home/ec2-user/apache-tomcat-8.5.32/bin
[root@ip-172-31-28-56 ec2-user]# ls
apache-tomcat-8.5.32  apache-tomcat-8.5.32.tar.gz
[root@ip-172-31-28-56 ec2-user]# chmod -R 766 apache-tomcat-8.5.32
[root@ip-172-31-28-56 ec2-user]# cd apache-tomcat-8.5.32/bin/
[root@ip-172-31-28-56 bin]# ./startup.sh
Using CATALINA_BASE:   /home/ec2-user/apache-tomcat-8.5.32
Using CATALINA_HOME:   /home/ec2-user/apache-tomcat-8.5.32
Using CATALINA_TMPDIR: /home/ec2-user/apache-tomcat-8.5.32/temp
Using JRE_HOME:        /
Using CLASSPATH:       /home/ec2-user/apache-tomcat-8.5.32/bin/bootstrap.jar:/home/ec2-user/apache-tomcat-8.5.32/bin/to
t-juli.jar
Tomcat started.
[root@ip-172-31-28-56 bin]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1070/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1026/master
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN      1281/java
tcp6       0      0 :::8009                 :::*                    LISTEN      1281/java
tcp6       0      0 :::8080                 :::*                    LISTEN      1281/java
tcp6       0      0 :::22                   :::*                    LISTEN      1070/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1026/master
[root@ip-172-31-28-56 bin]#
```

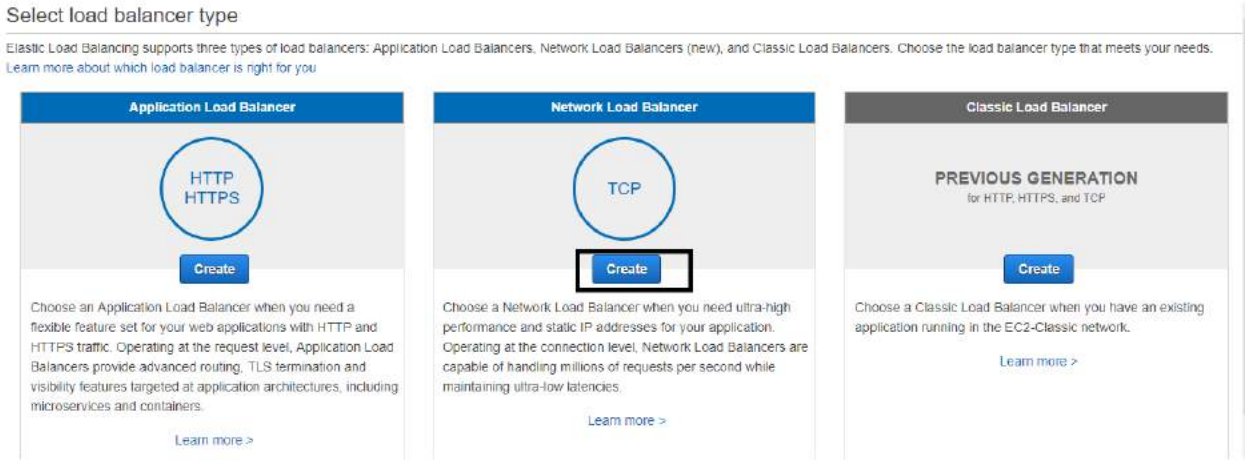
- Access the Tomcat in a browser by providing EC2 instance IP Address along with port number as like shown below.



- Similarly do the same steps in another Linux EC2 instance and install 7.0.90 version of Tomcat to show the differences between two Tomcats while accessing Network Load Balancer.



- After ensuring Tomcat is working fine on both the Linux VM, proceed to create a Network Load Balancer.



- Provide the name and front end port number, followed by select the VPC along with Availability zones where those two Linux EC2 instances are running.

1. Configure Load Balancer | 2. Configure Routing | 3. Register Targets | 4. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.

Name: mynetworklb

Scheme: internet-facing / internal

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
TCP	443

Add listener

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.

Click here to manage your Elastic IPs.

VPC: vpc-132f2368 (172.31.0.0/16) | Default_VPC (default)

Availability Zone	Subnet ID	Subnet IPv4 CIDR	Elastic IP	Name
us-east-1a	subnet-ec02cac2	172.31.80.0/20		
us-east-1b	subnet-c81b8982	172.31.16.0/20		
us-east-1c	subnet-45de1019	172.31.32.0/20		
us-east-1d	subnet-7d83571a	172.31.0.0/20		
us-east-1e	subnet-819277bf	172.31.64.0/20		

Cancel | Next: Configure Routing

- Provide the backend port numbers to ensure the health status of two instances.

1. Configure Load Balancer | 2. Configure Routing | 3. Register Targets | 4. Review

Step 2: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group: New target group

Name: tomcatservers

Protocol: TCP

Port: 8080

Target type: instance

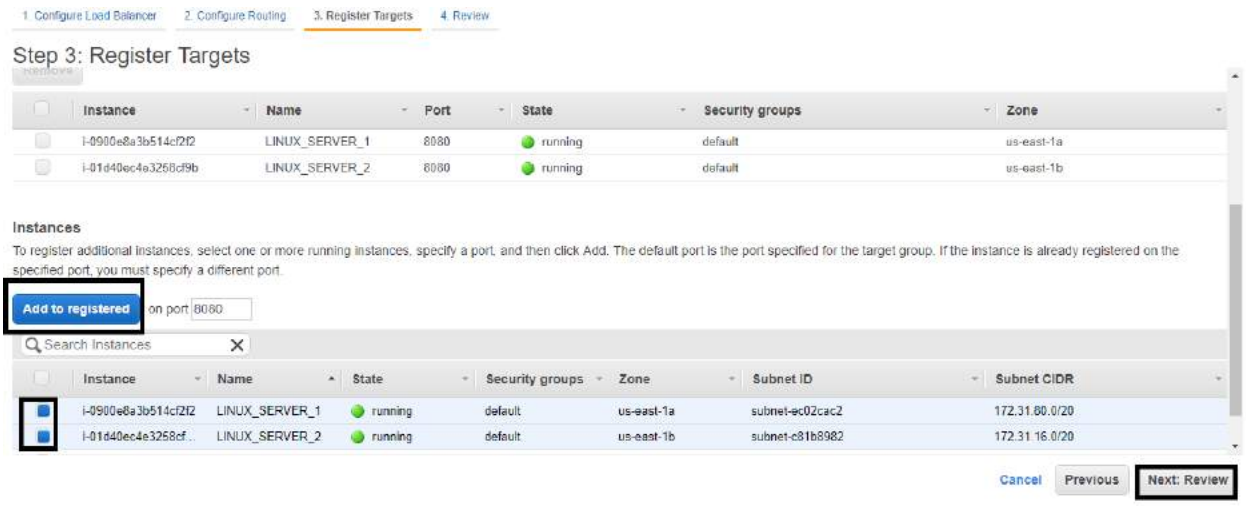
Health checks

Protocol: TCP

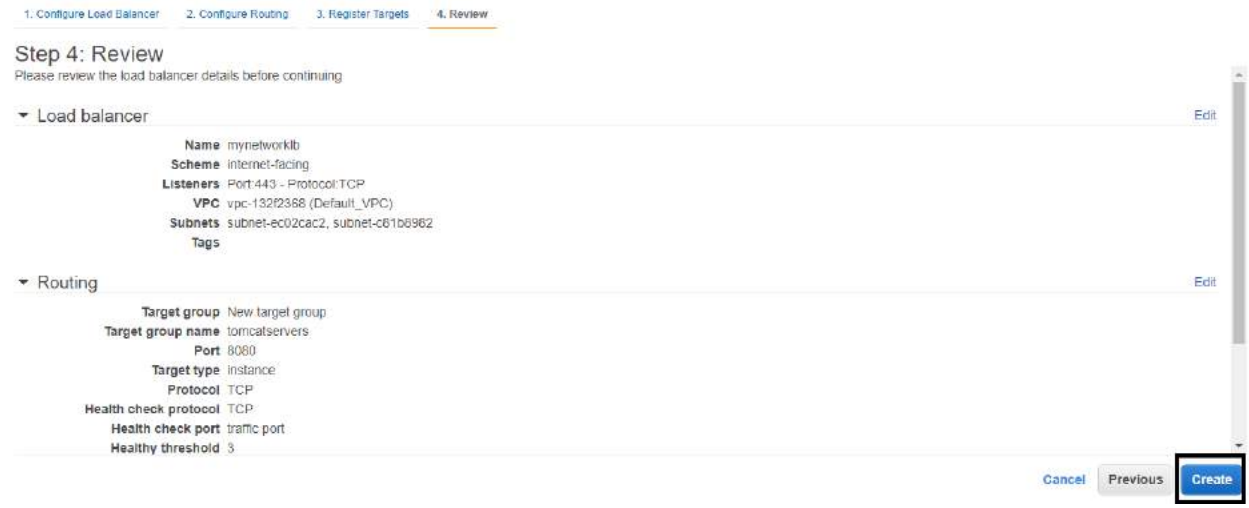
Advanced health check settings

Cancel | Previous | Next: Register Targets

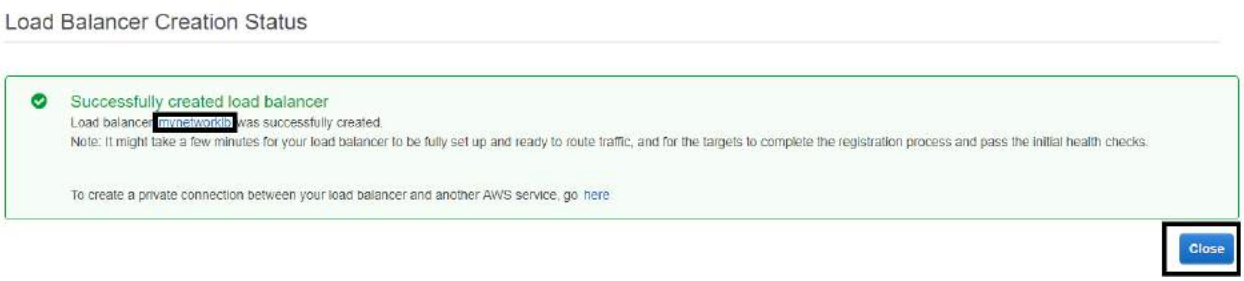
- Select the EC2 instances in which Tomcat are running and click on Add to registered.

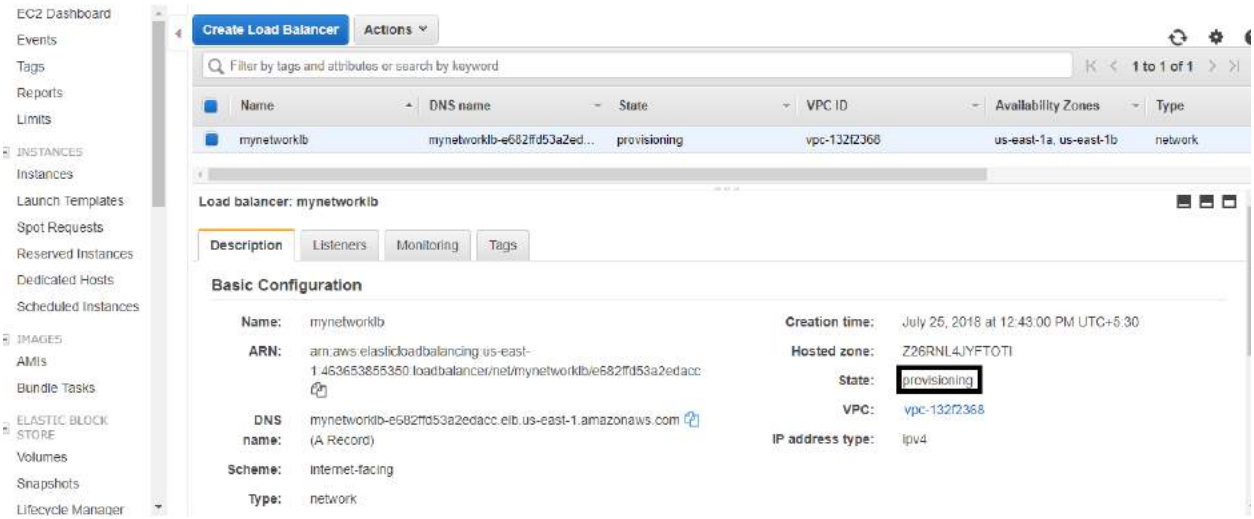


- Review the options which has been selected and click on create.

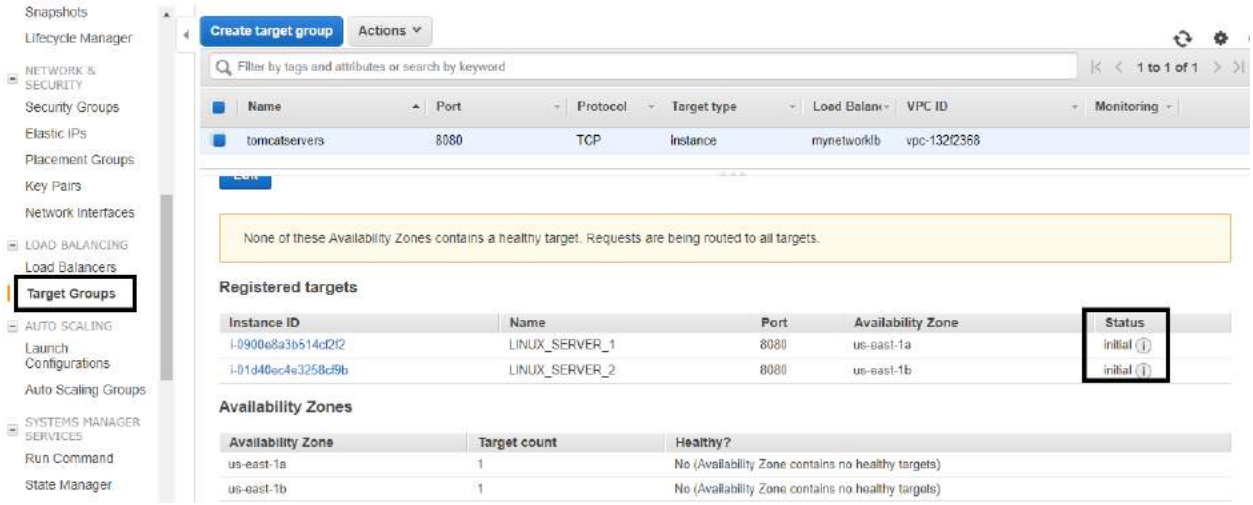


- Network Load Balancer creation is in progress and this would take around 6-8 minutes of time.

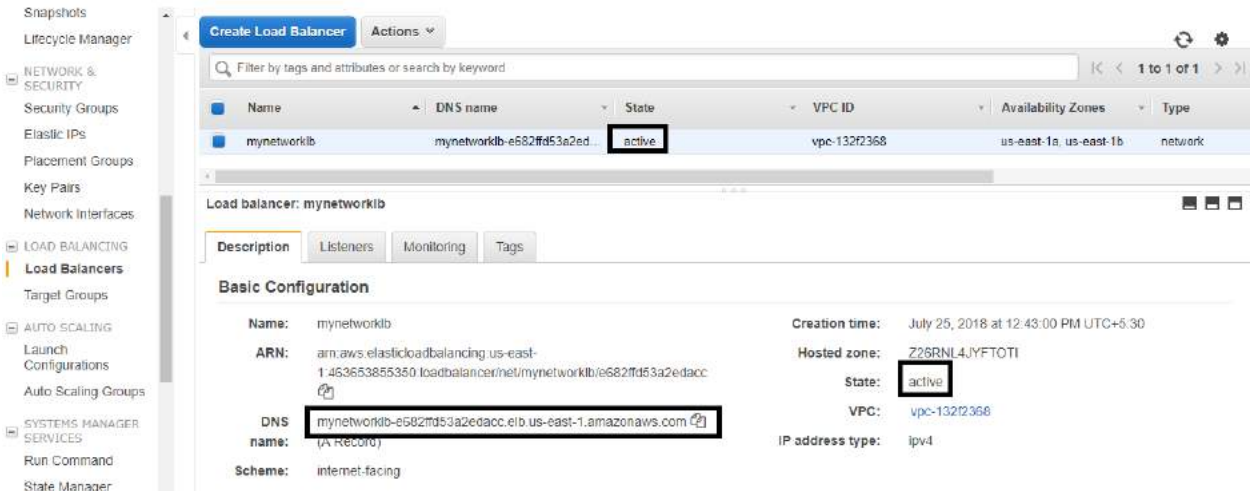




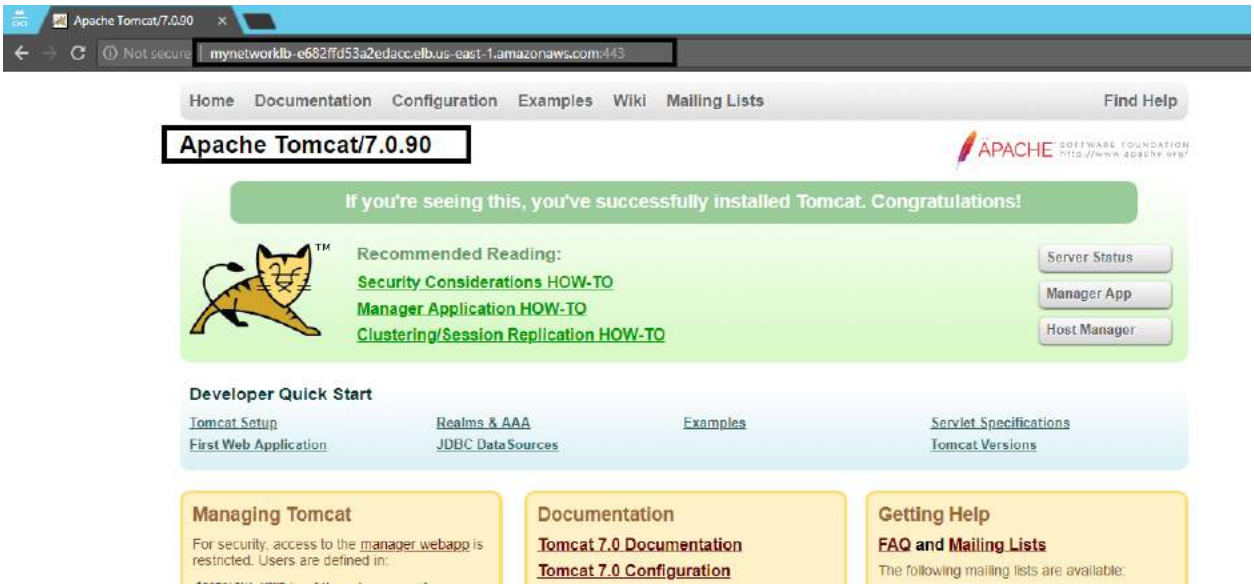
- Click on Target Groups to ensure EC2 instances are added In back end of Load Balancer.

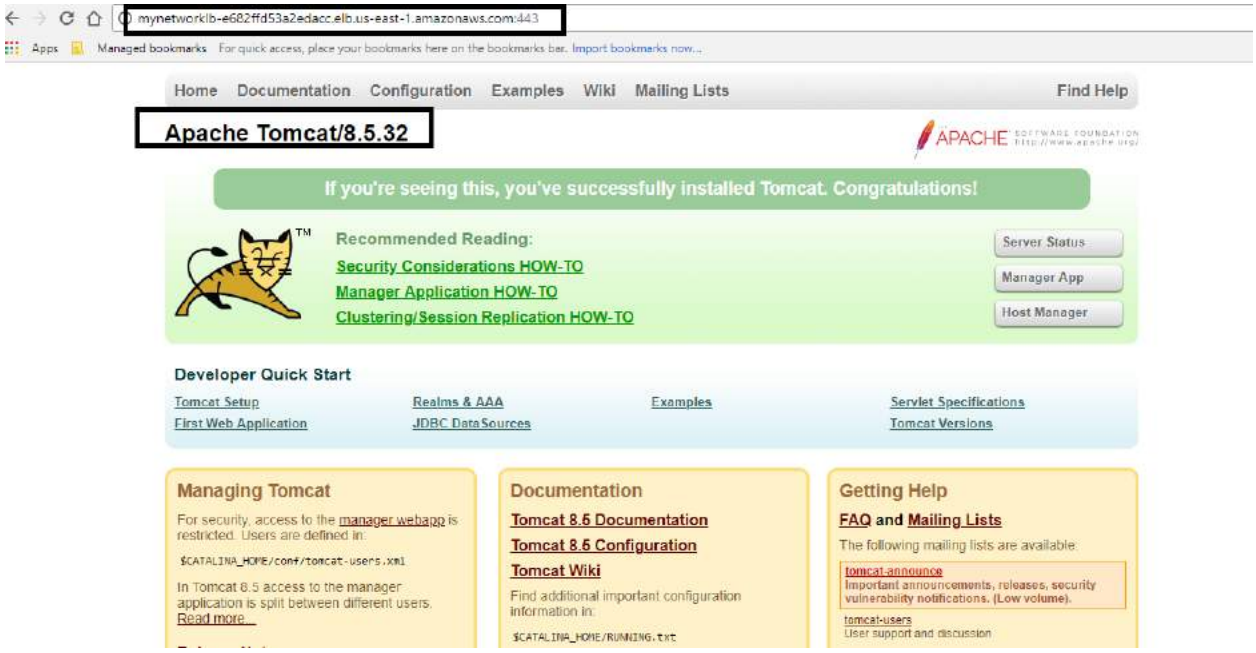


- Now, the Network Load Balancer has been created and copy the DNS name to access it.



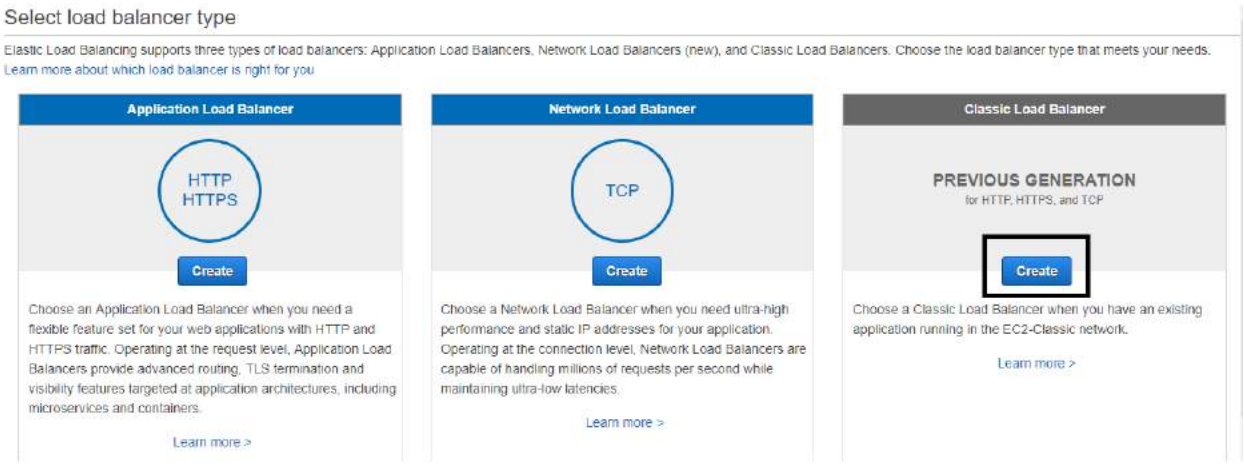
- Open the browser and start accessing using copied DNS URL.
- You need to provide the 443 port number since it is configured as a TCP not as HTTPS. This Network Load balancer routes through Round Robin mechanism and open another computer to ensure it is routed to another Tomcat EC2 instance.



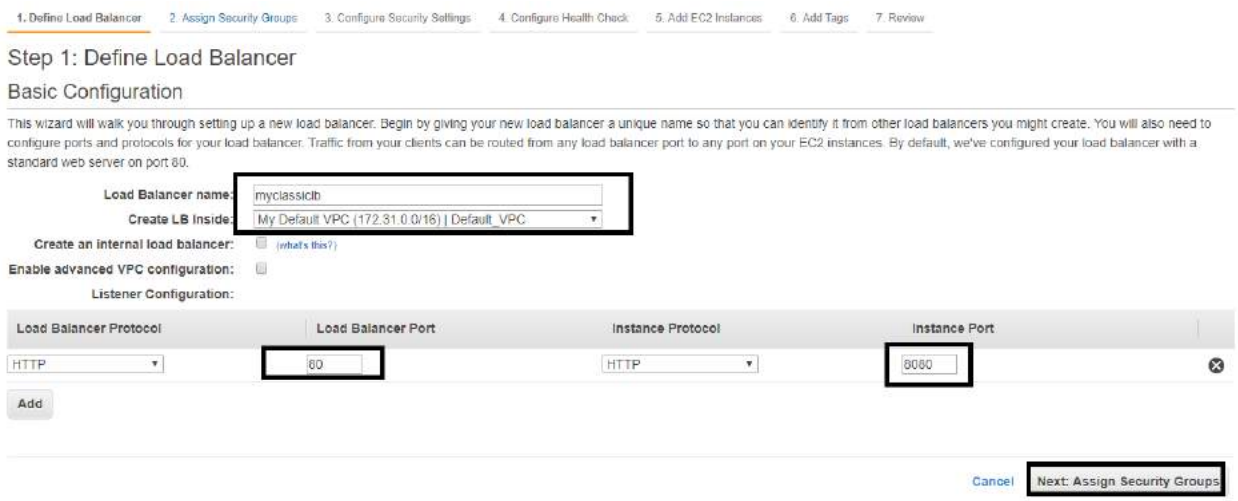


Classic Load Balancer:

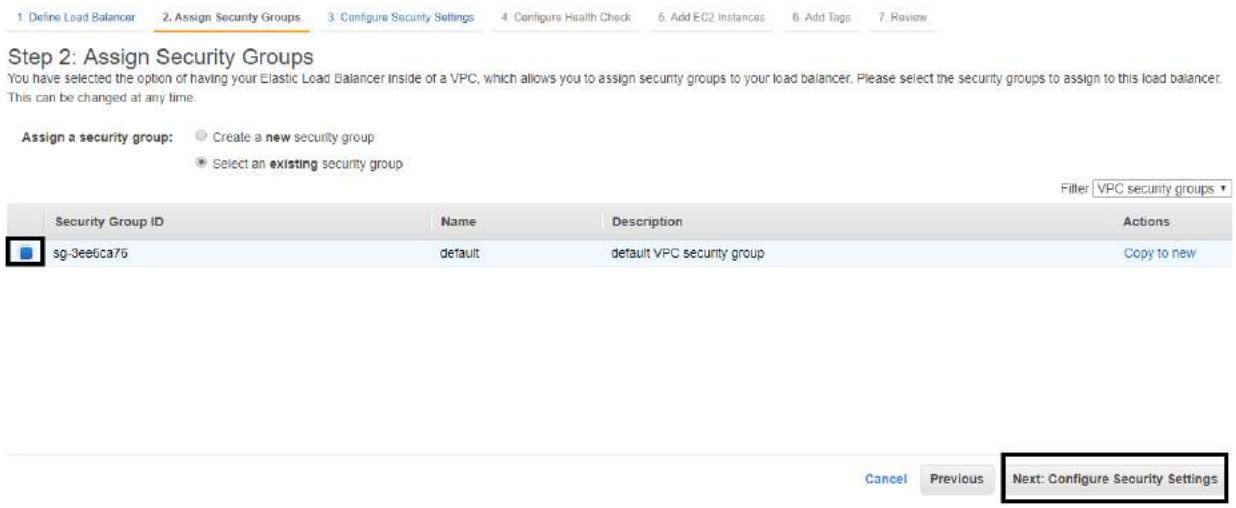
- Create a two Linux Server for installing Tomcat in 8080 TCP port before creating a Classic Load Balancer.
- To create Linux Machine and installing Java & Tomcat, follow the same steps which we followed in Network Load Balancer.
- After configuring with Tomcat installation in Linux EC2 instance, follow the below steps to create a Classic Load Balancer.



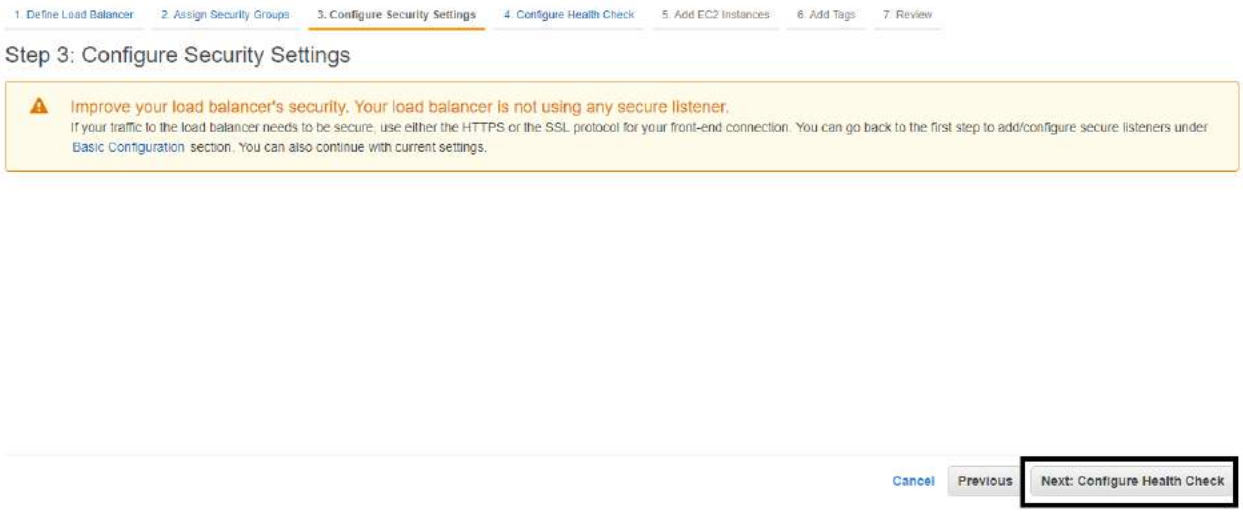
- Provide the name, front end and backend port number to proceed with next steps.



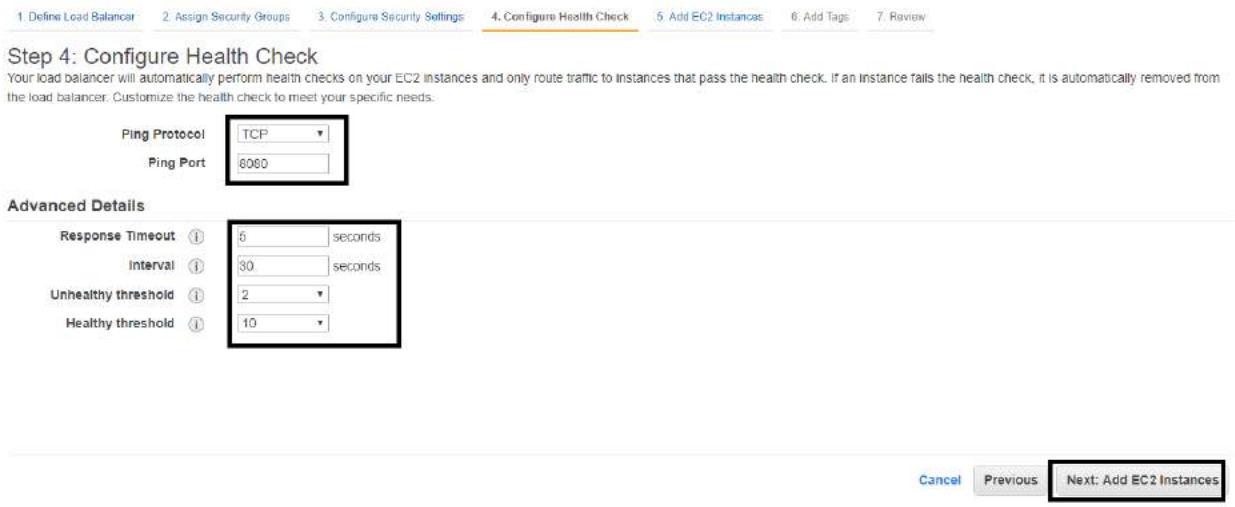
- Select the security group and make sure front end and backend port number has opened in an inbound rules.



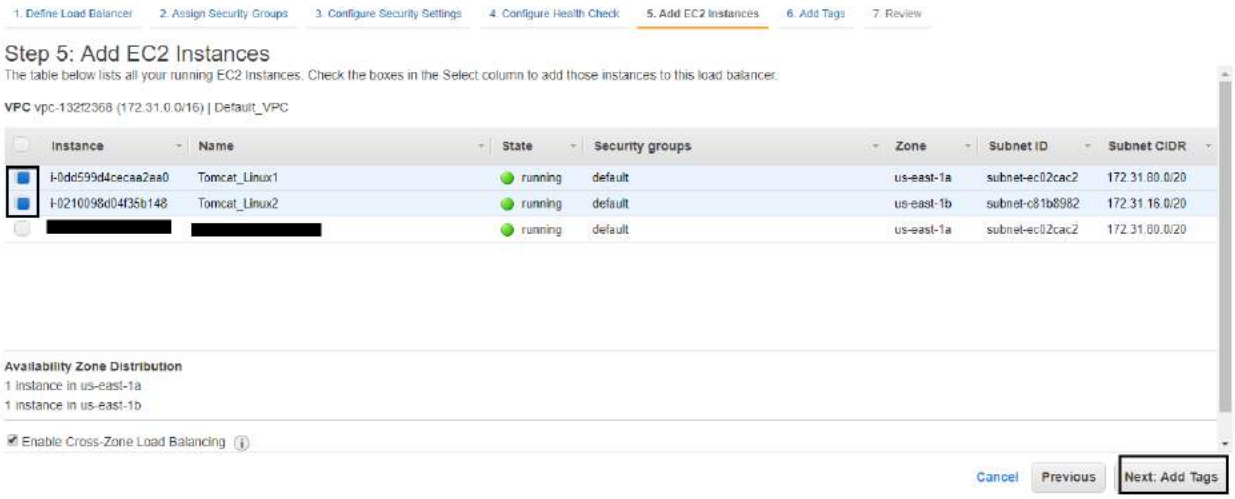
- If you are choosing the front end port as HTTPS, you supposed to upload the SSL certificate in this below section.



- Choose the backend protocol as TCP and mention the port number.



- Add an EC2 instances in which tomcat are running.



- If keys and Tags are required you could add it.

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 6: Add Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key	Value

Create Tag

Cancel | Previous | Review and Create

- Review every option which has been chosen and proceed with creation.

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 7: Review

Please review the load balancer details before continuing

Define Load Balancer

Edit load balancer definition

Load Balancer name: myclassiclb
Scheme: internet-facing
Port Configuration: 80 (HTTP) forwarding to 8080 (HTTP)

Configure Health Check

Edit health check

Ping Target: TCP:8080
Timeout: 5 seconds
Interval: 30 seconds
Unhealthy threshold: 2
Healthy threshold: 10

Add EC2 Instances

Edit instances

Cross-Zone Load Balancing: Enabled
Connection Draining: Enabled, 300 seconds
Instances: i-0dd599d4cecaa2aa0 (Tomcat_Linux1), i-0210096d04f35b148 (Tomcat_Linux2)

Cancel | Previous | Create

Load Balancer Creation Status

Successfully created load balancer
Load balancer myclassiclb was successfully created.
Note: It may take a few minutes for your instances to become active in the new load balancer.

Close

- Backend instance mapping to Classic Load Balancer are in progress.

Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations

Create Load Balancer | Actions

Filter by tags and attributes or search by keyword | 1 to 1 of 1

Name	DNS name	State	VPC ID	Availability Zones	Type
myclassiclb	myclassiclb-1792119327.us-...		vpc-132f2368	us-east-1a, us-east-1b,...	classic

Load balancer: myclassiclb

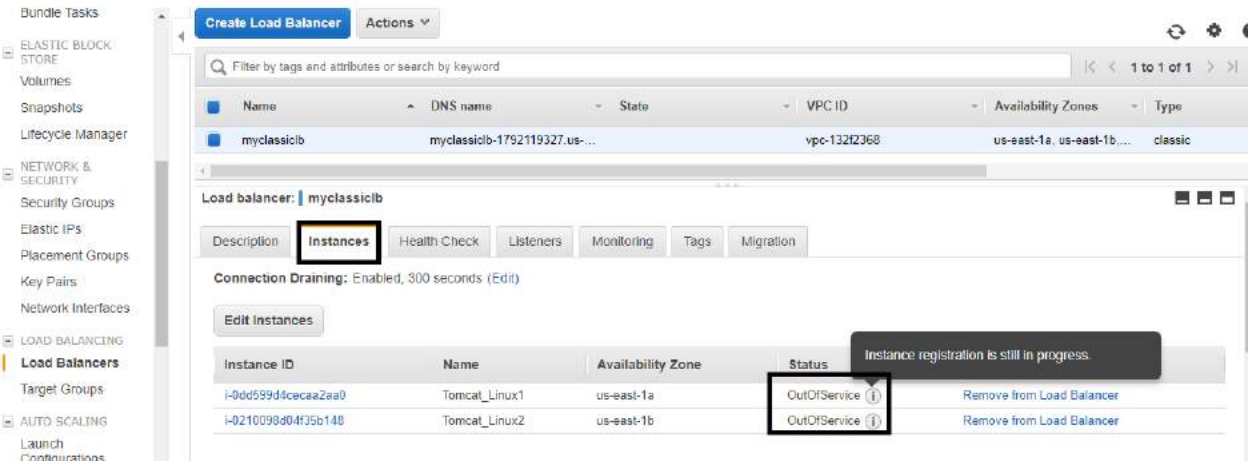
Description | Instances | Health Check | Listeners | Monitoring | Tags | Migration

Basic Configuration

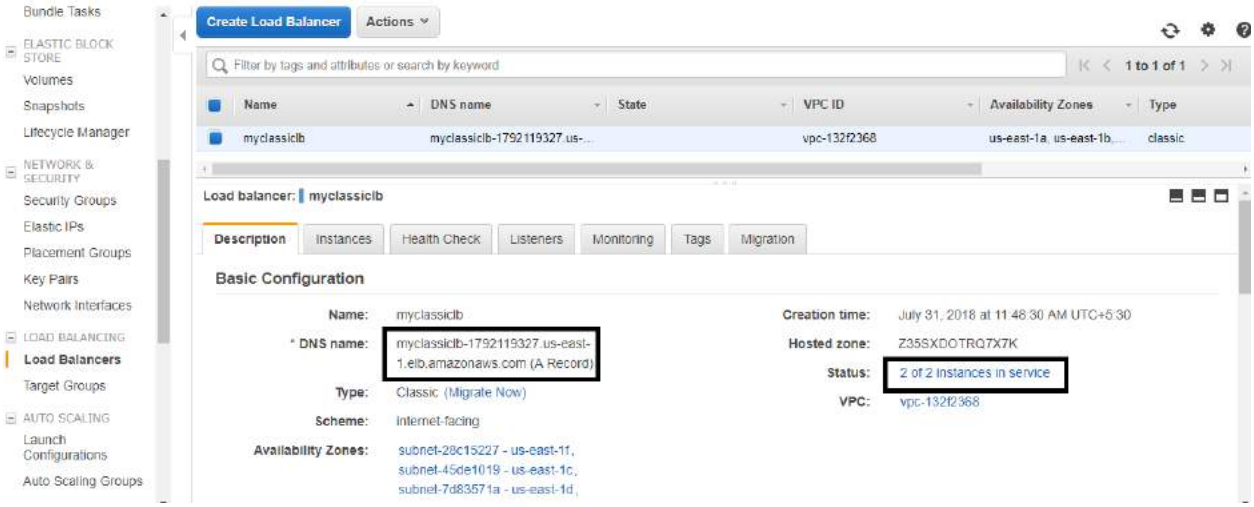
Name: myclassiclb
*** DNS name:** myclassiclb-1792119327.us-east-1.elb.amazonaws.com (A Record)
Type: Classic (Migrate Now)
Scheme: internet-facing
Availability Zones: subnet-28c15227 - us-east-1f, subnet-45de1019 - us-east-1c,

Creation time: July 31, 2018 at 11:46:30 AM UTC+5:30
Hosted zone: Z35SXDOTRQ7X7K
Status: 0 of 2 instances in service
VPC: vpc-132f2368

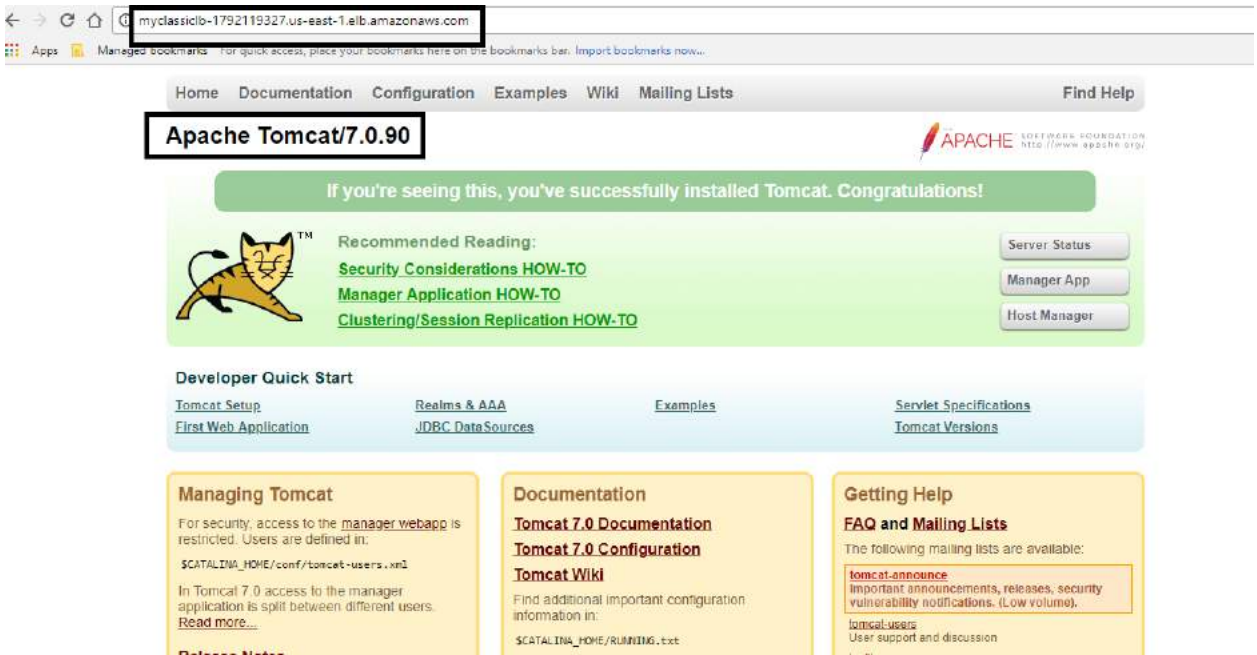
- EC2 instance mapping to LB are in progress and currently Classic Load Balancer are ensuring the health status of both the EC2 instances.



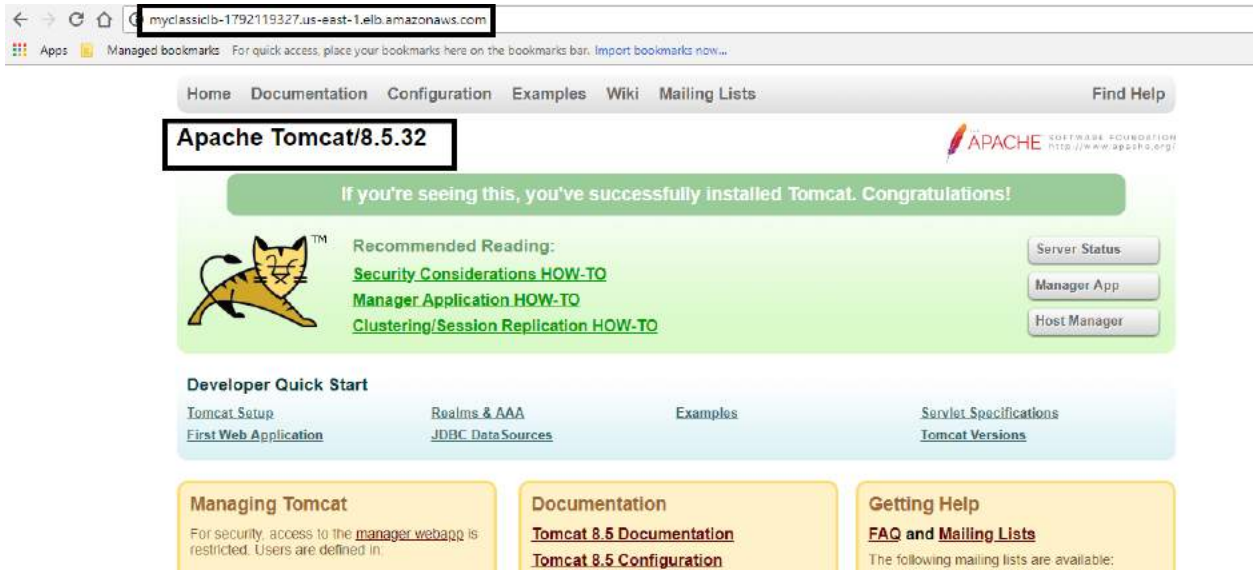
- Both an EC2 instances are mapped successfully to Classic Load Balancer and copy the DNS to access the Load Balancer.



- Accessing the URL in a browser and Tomcat Home Page is working fine.



- Both an EC2 instances are working fine when we are accessing from Classic Load Balancer URL.



Advantages of Elastic Load Balancer:

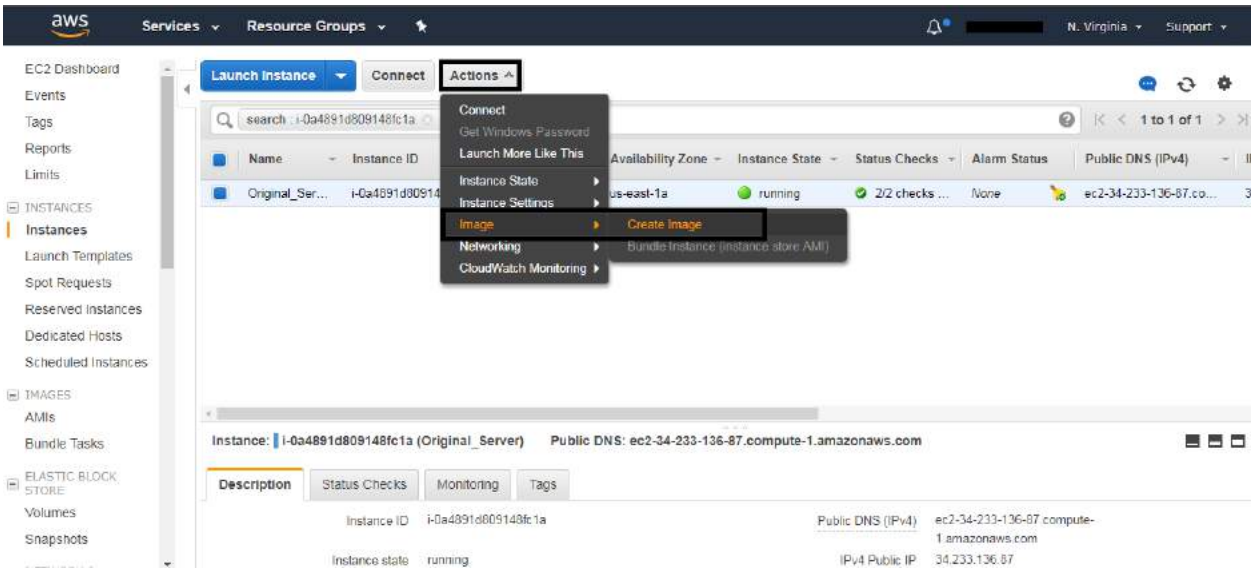
- Virtual Machine cost would be saved.
- Could expect 100% availability since it is functioning as managed service.
- No possibilities on crash or restarting the services as we do in normal Apache Load Balancer VM.
- Easily can include / exclude application servers from this ELB.
- Could handle millions of request within a second.

Auto-Scaling:

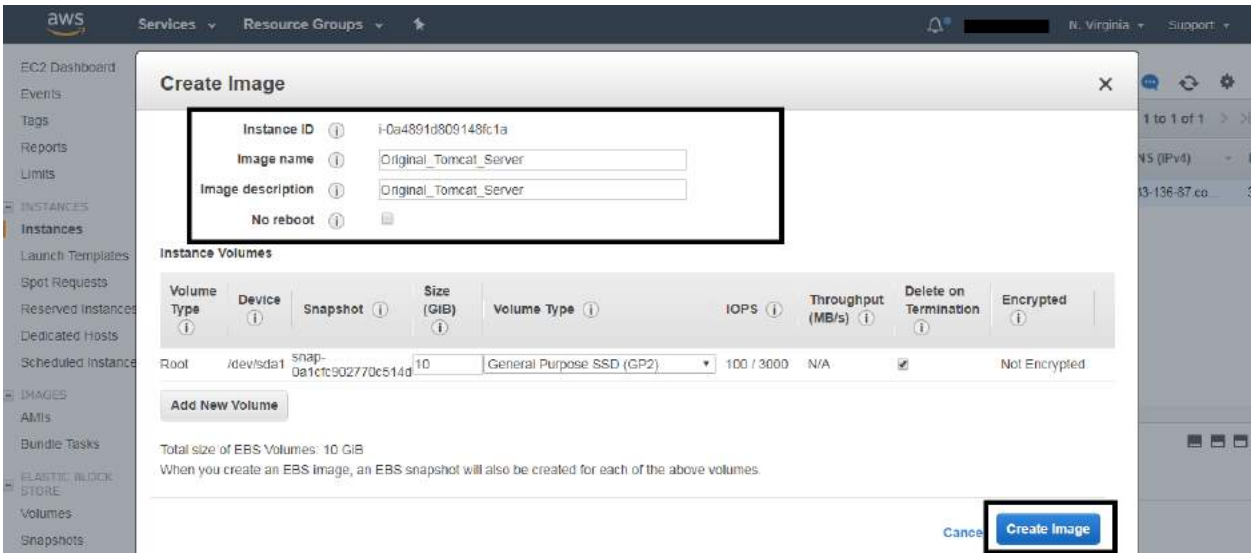
- Create a new EC2 instance in VPC.
- Install IIS or Apache Tomcat based on Operating System or as per your requirement. If it is IIS installation refer the above Elastic Load Balancer Steps for IIS installation.
- Start the Web Server and access from outside of the server by opening the port in Security Group.
- If it is Tomcat Web Server, enable it by default in Service whenever it starts up after rebooting.
- Install Java using below command.
- yum install java -y
- yum install java-1.8.0-openjdk-devel -y
- Open this text file and type the below commands.
- vi /etc/profile
  export JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk/
  export JAVA_PATH=/usr/lib/jvm/java-1.8.0-openjdk/bin
- Follow the below steps to enable the Tomcat service to startup by default whenever server booting up.
- chmod -R 777 apache-tomcat-7.0.82
- cd apache-tomcat-7.0.82/
- chmod -R 777 *.*
- sudo vi /etc/systemd/system/tomcat.service
  [Unit]
  Description=Apache Tomcat Web Application Container
  After=syslog.target network.target
  [Service]
  Type=forking
  Environment=JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk/bin

Environment=CATALINA_PID=/home/ec2-user/apache-tomcat-8.5.28/temp/tomcat.pid
Environment=CATALINA_HOME=/home/ec2-user/apache-tomcat-8.5.28/
Environment=CATALINA_BASE=/home/ec2-user/apache-tomcat-8.5.28/
Environment='CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC'
Environment='JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom'
ExecStart=/home/ec2-user/apache-tomcat-8.5.28/bin/startup.sh
ExecStop=/bin/kill -15 $MAINPID
User=root
Group=root
[Install]
WantedBy=multi-user.target

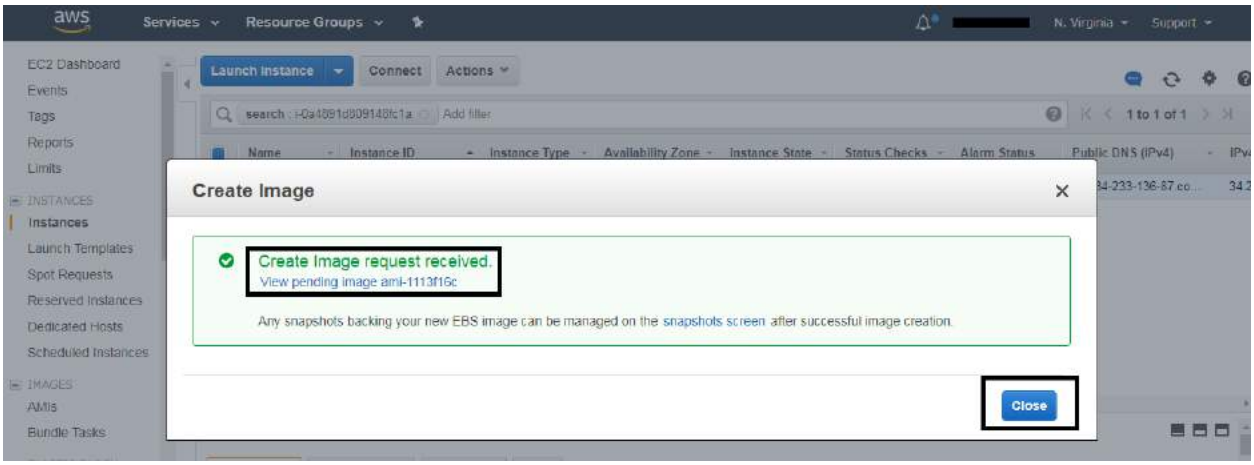
- Start the Apache Tomcat by navigate to bin and execute./startup.sh
- Provide the below command to ensure 8080 ports is running up.
- netstat -ntlp
- sudo systemctl start tomcat.service
- sudo systemctl enable tomcat.service
- Once the tomcat is started, ensure this has been added to OS Services by restarting the server.
- After the Server has booted up, ensure it by netstat -ntlp whether Tomcat Port number is running up without starting it manually.
- If it is working fine, capture that server as an AMI as like below given screenshot.



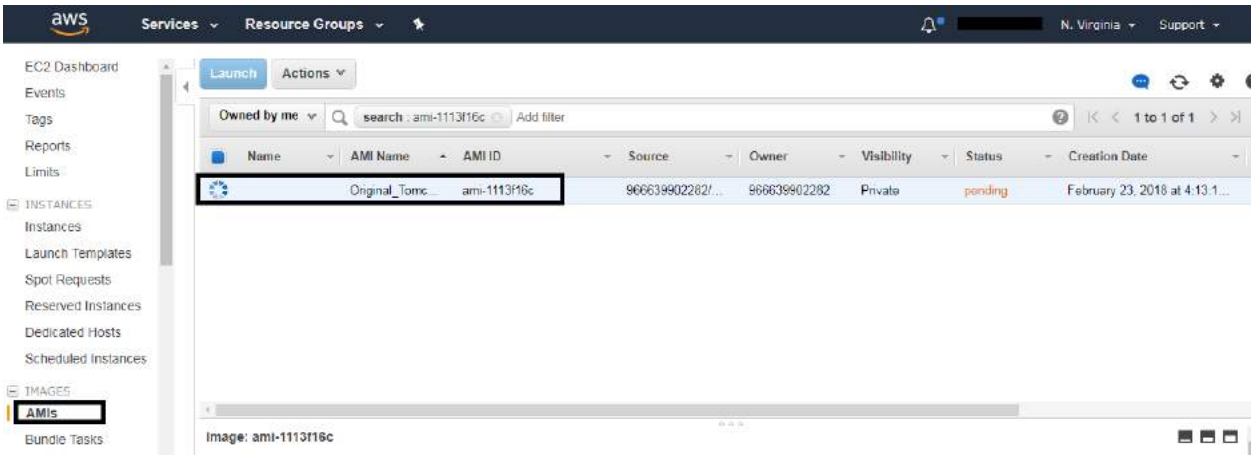
- Provide an AMI Name and click on Create Image.



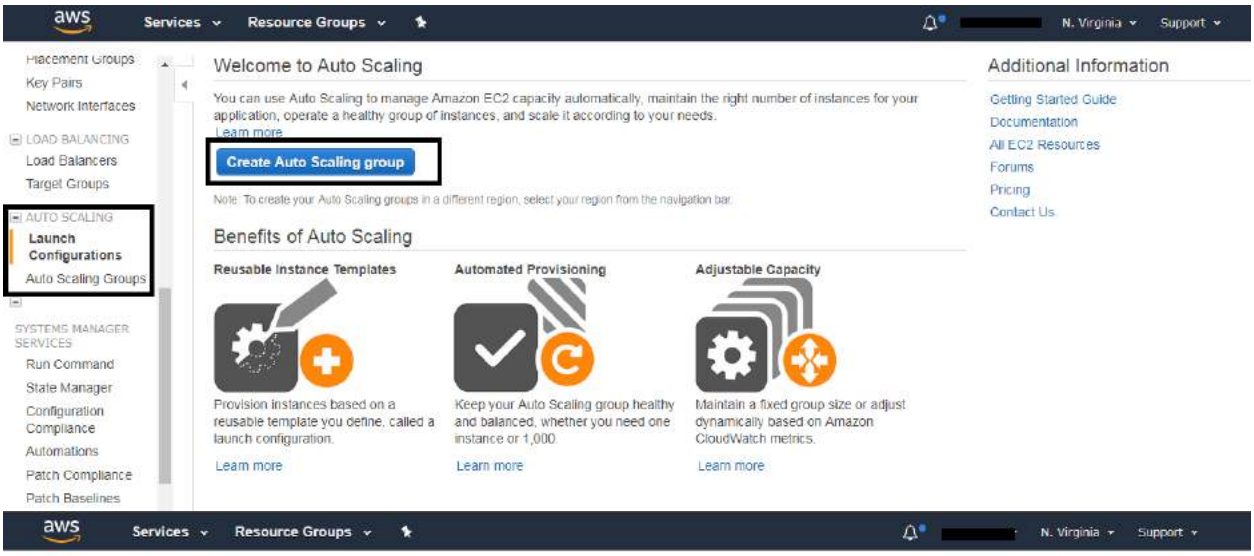
- Make a note of AMI ID and click on the same.

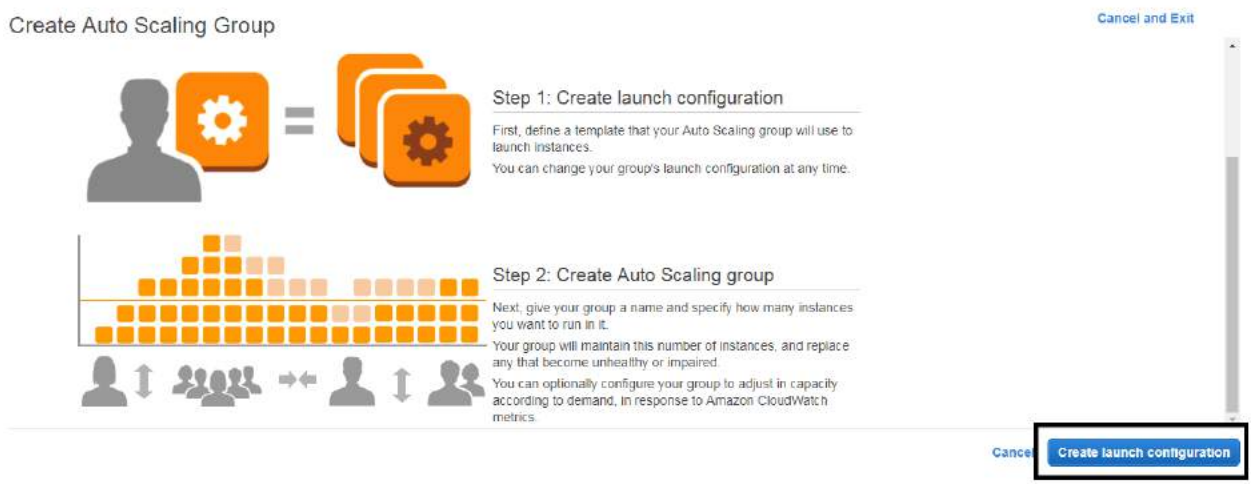


- AMI creation is in progress. It would take 5-7 minutes depends upon root volume size.

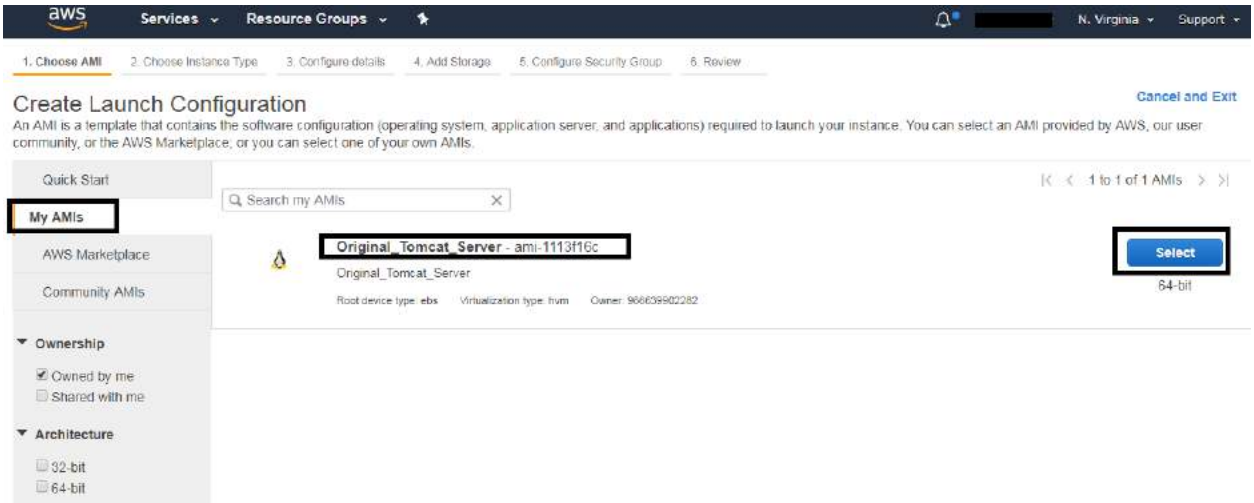


- Once an AMI is created, navigate to Auto Scaling Group and Click on Launch Configurations.

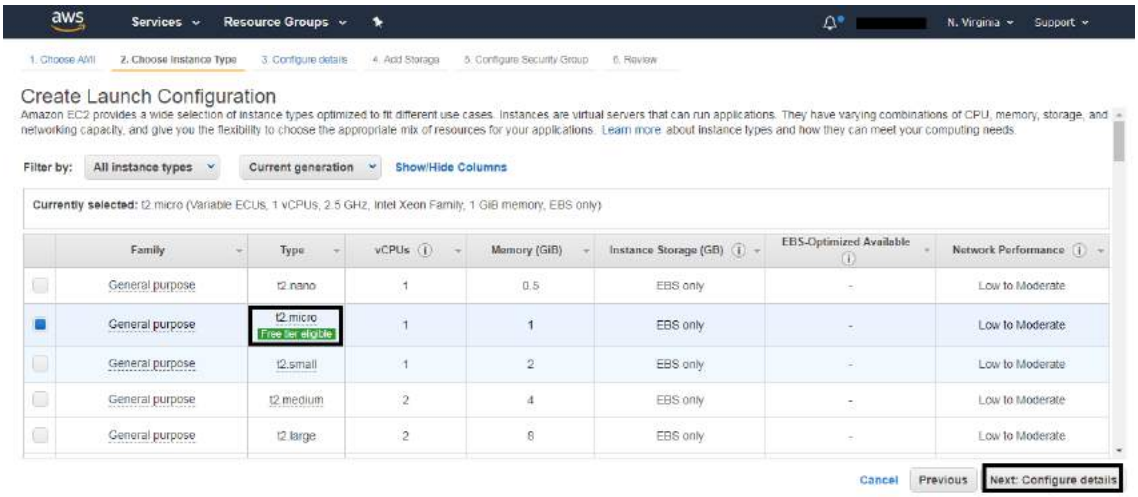




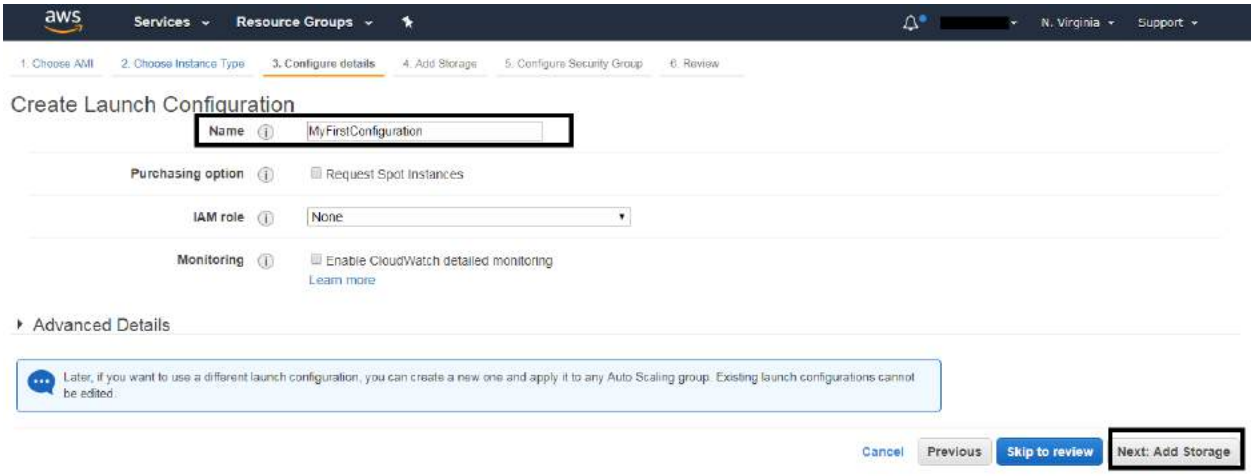
- Select your captured AMI and click on next.



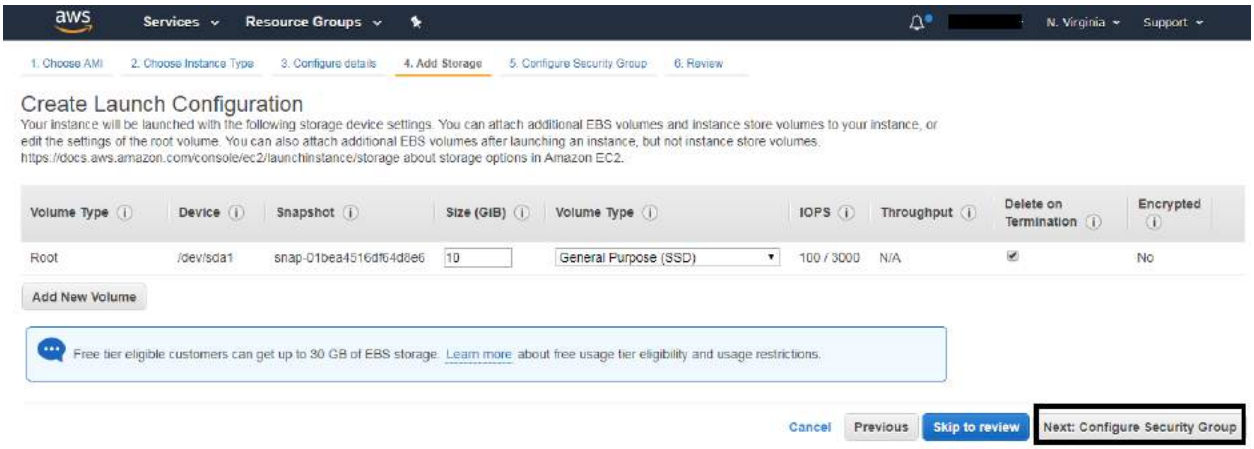
- Instance type can be changed based on application usage.



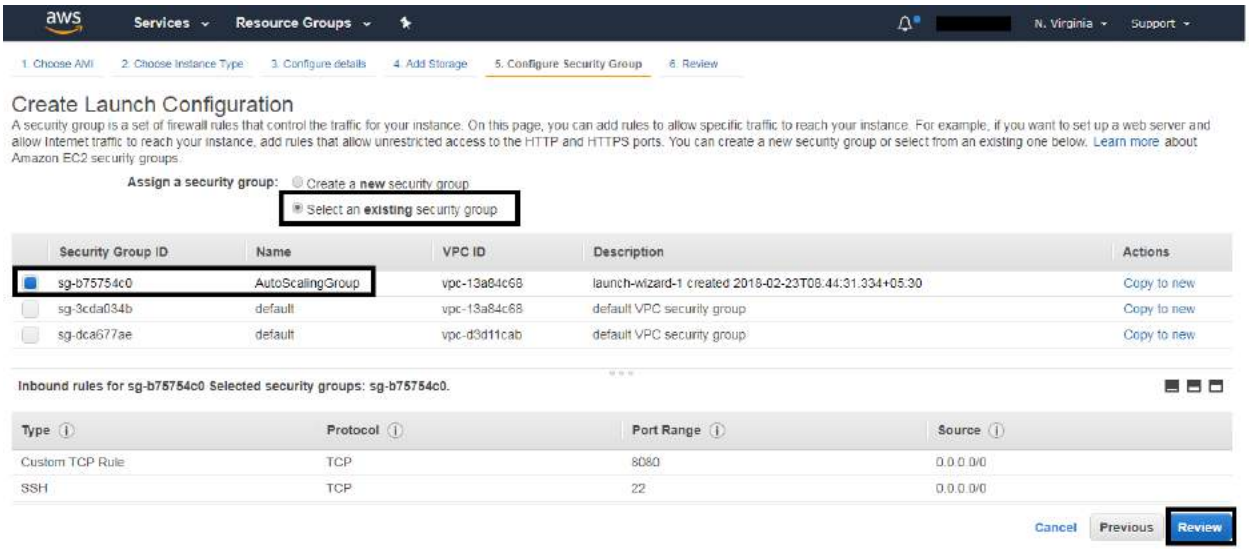
- Provide the configuration name and remaining options can be default values.



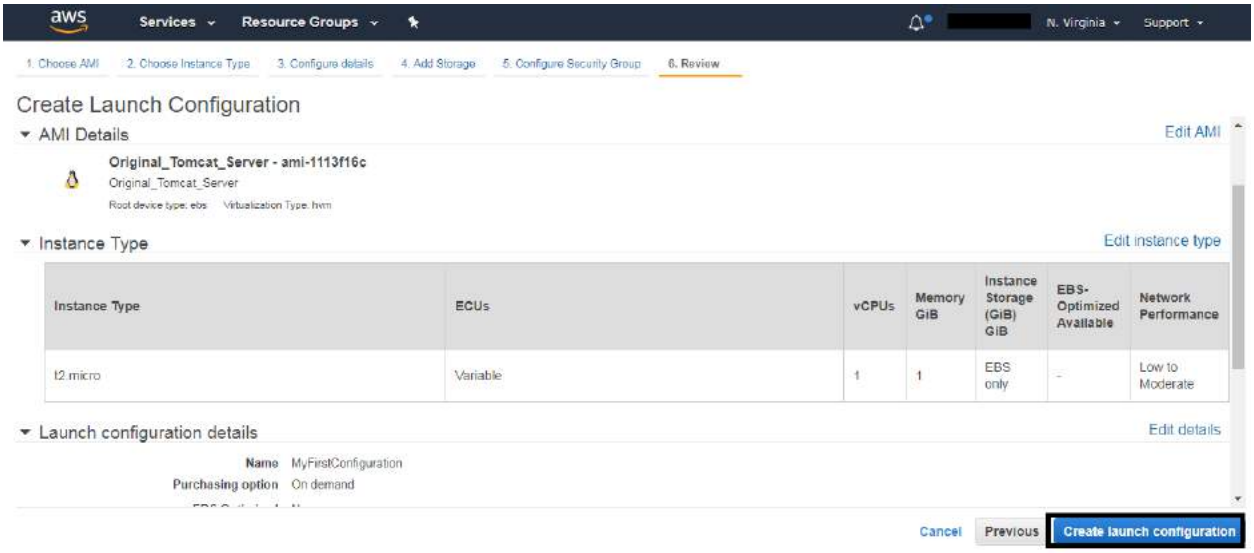
- If storage needs to be added, it can be increased in this section and click on Security Group.

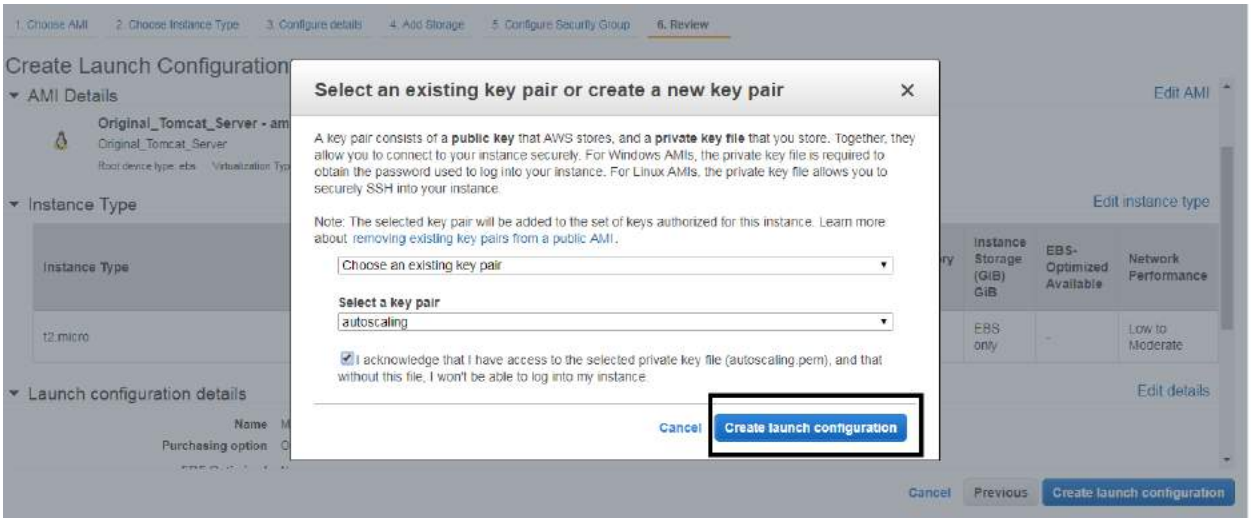


- Choose an Existing Security Group and click on Review.

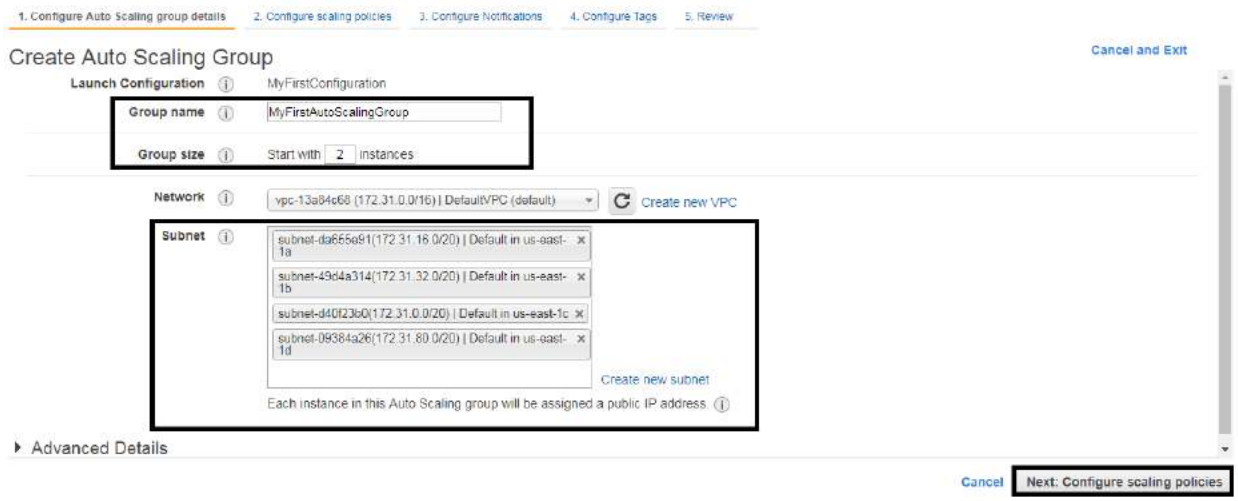


- Click on Create Launch Configuration and select the Key Pair of Instances, then it redirects to Auto Scaling Creation.

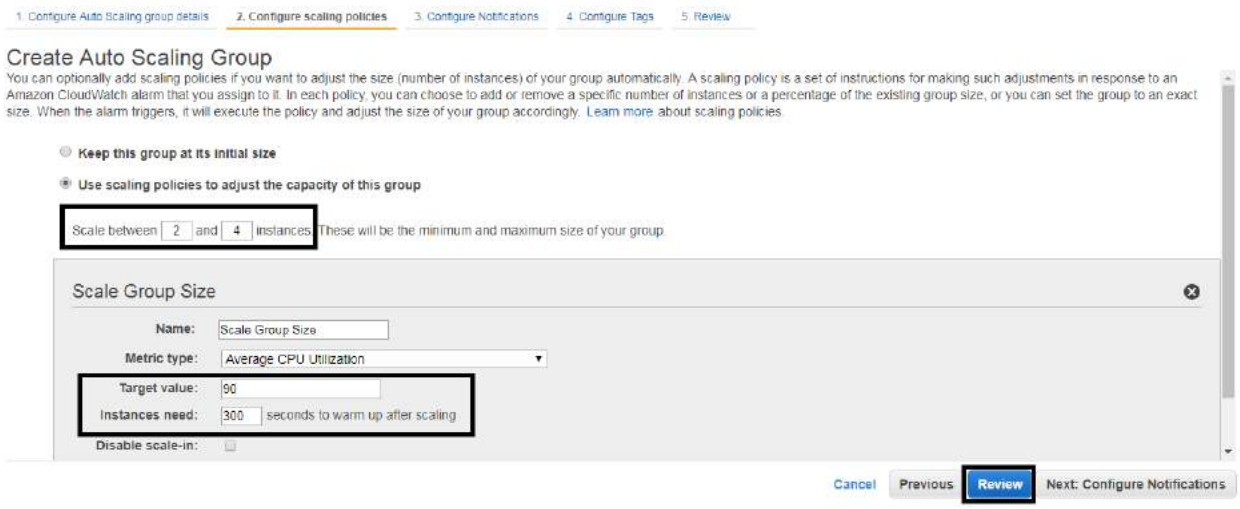




- Provide the Auto Scaling Group Name and provide the count of instances which would require for your application. The instance count which has been provided would be the minimum value and provided count of instances would be always in running state. It can be changed in future depends upon the load. Choose the VPC and Subnet to proceed with Scaling policies.



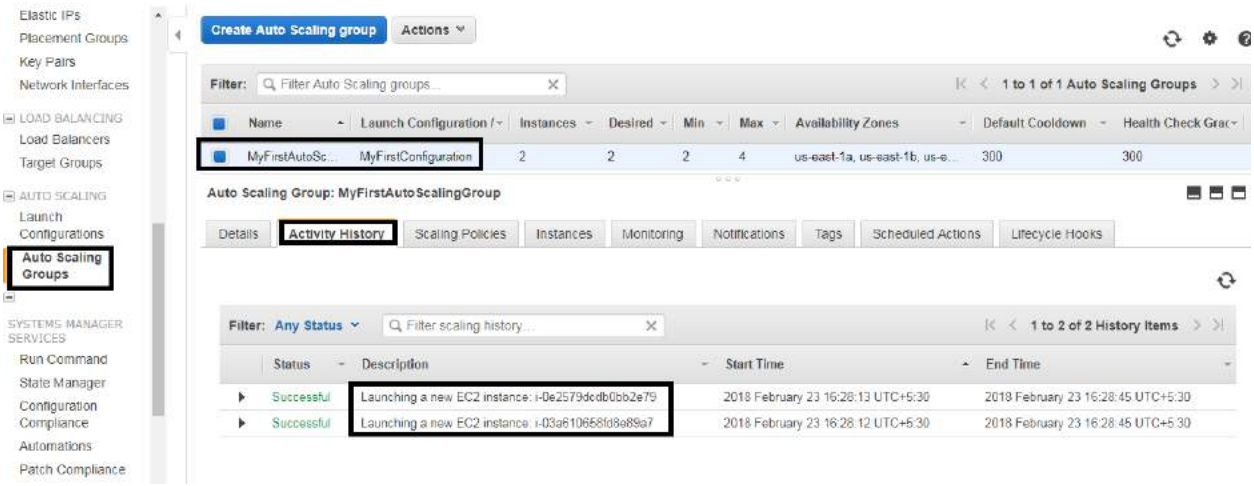
- You can set the maximum count of Instances, which needs to be provisioned on the load, and the same can be modified any time after the creation of Auto Scaling Group. Here, scaling policies are based on the CPU Utilization and provide value is 90%. So, if CPU crosses 90 % on the minimum count of 2 Instances, Maximum value count of instances would get provisioned.



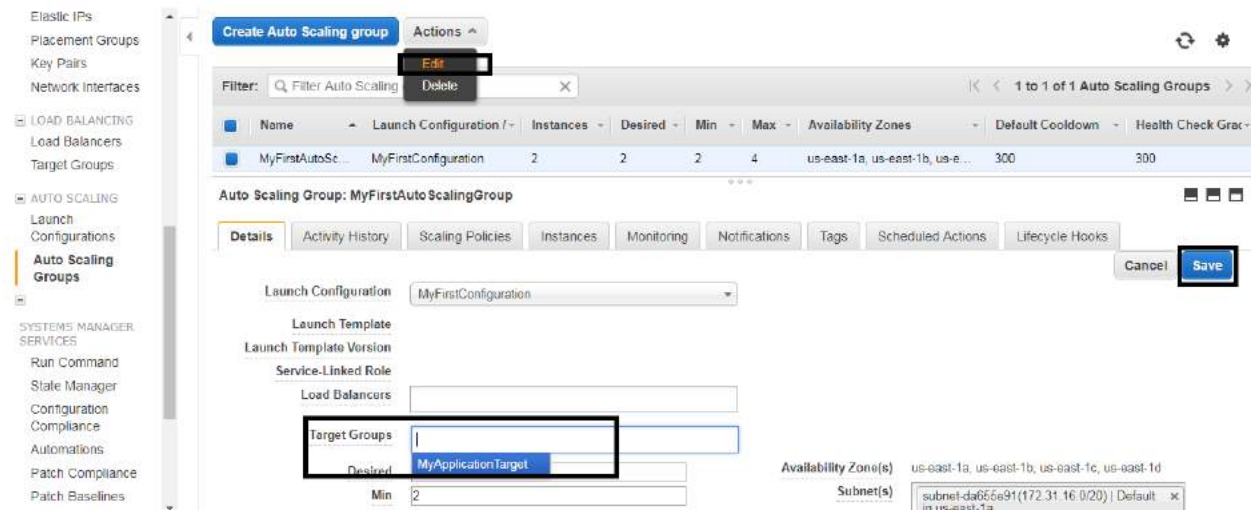
- Click on Review if you do not want any notifications during Instance Provisioning / De-Provisioning.
- Create an Auto Scaling Group.

- Auto Scaling Group is being created.

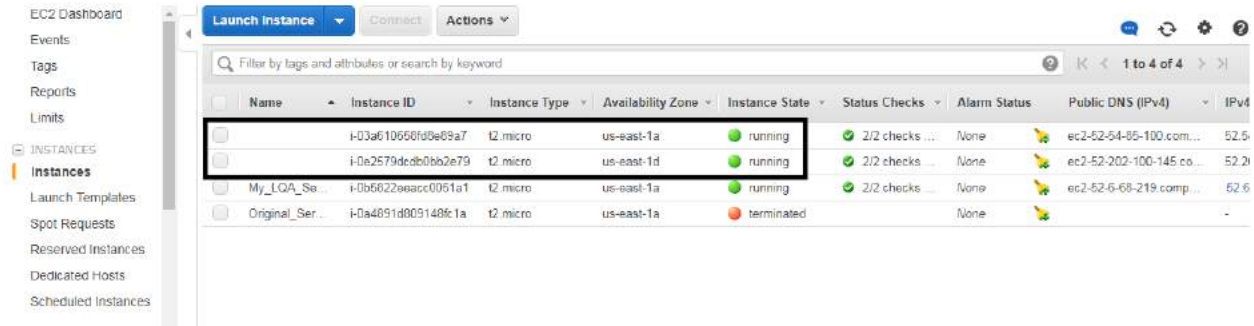
- During this creation, proceed to create Application / Classic / Network Load Balancer based on the requirement along with Target Group. Map the initial Minimum instances in Target Groups.
- Auto Scaling Group Instances creation is in progress and the status of the same can be found in Activity History section.



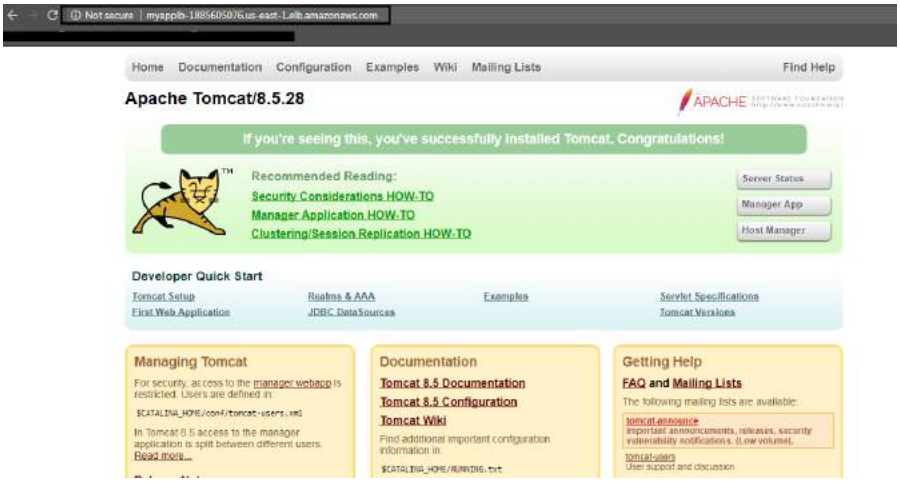
- After / during the creation of Auto Scaling Group, click on Actions >> Edit to map the Target Group of Load Balancer into Auto Scaling Group. Once it has been mapped, click on Save. Hence, whenever load increases on the application, based on the defined scaling Policies new instances would gets provisioned automatically without any manual work and the created instances would be mapped automatically to Load Balancer since we have been mapped the Target Group to Auto Scaling Group.



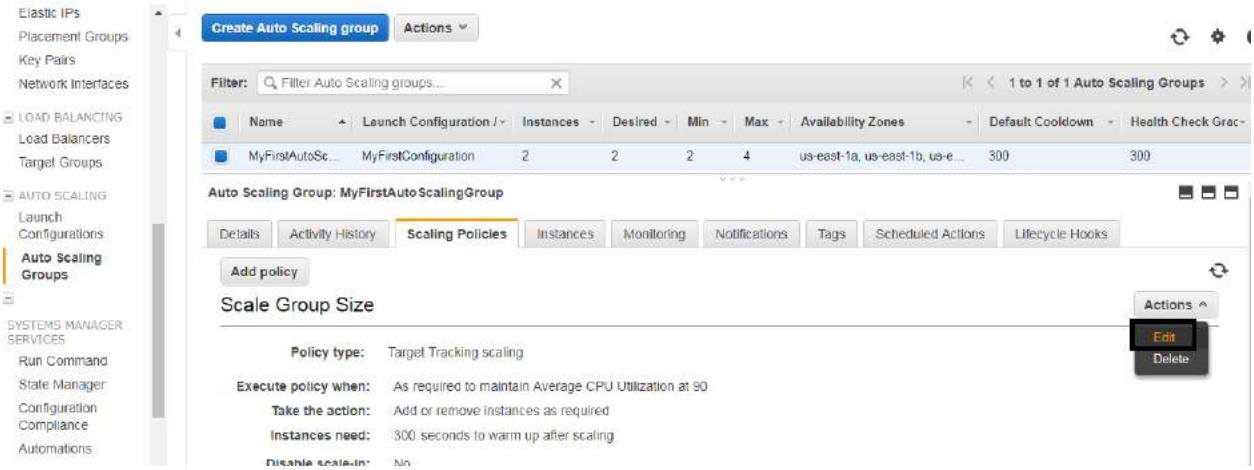
- Instances provisioned can be found in EC2 section.

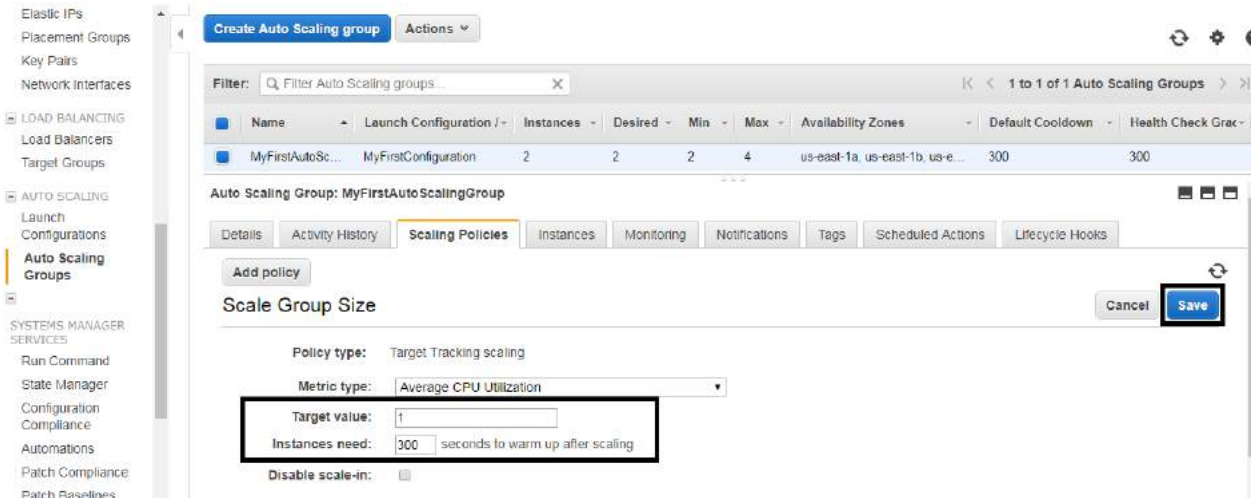


- Now, application is being accessed in Two instances using Load Balancer.

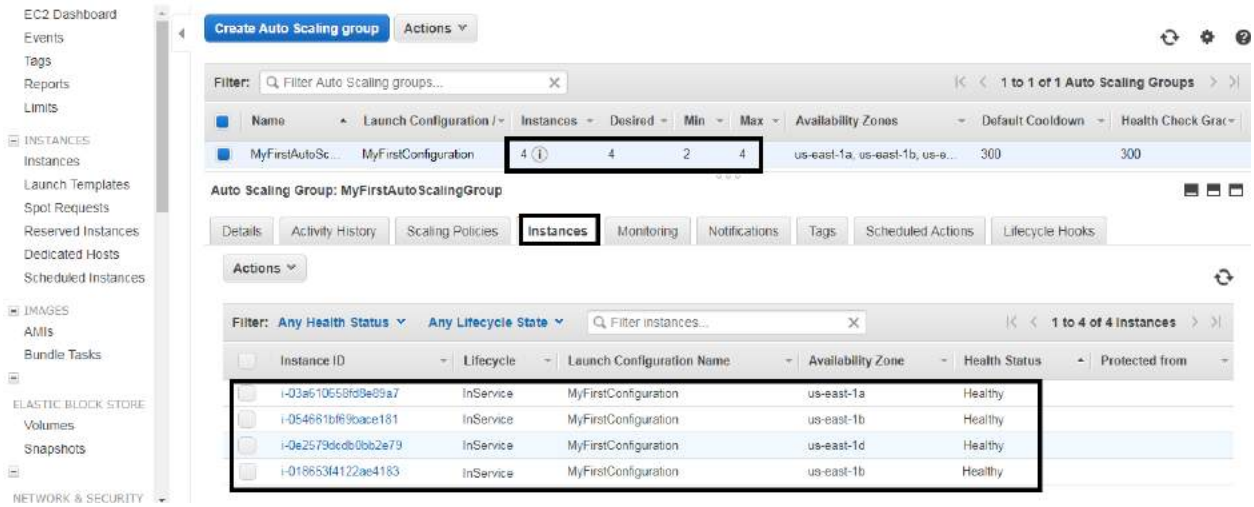


- Scaling Policies can be modified any time, so to ensure Scale Out is working fine, am proceeding to change the scaling policies to 1% of CPU utilization.

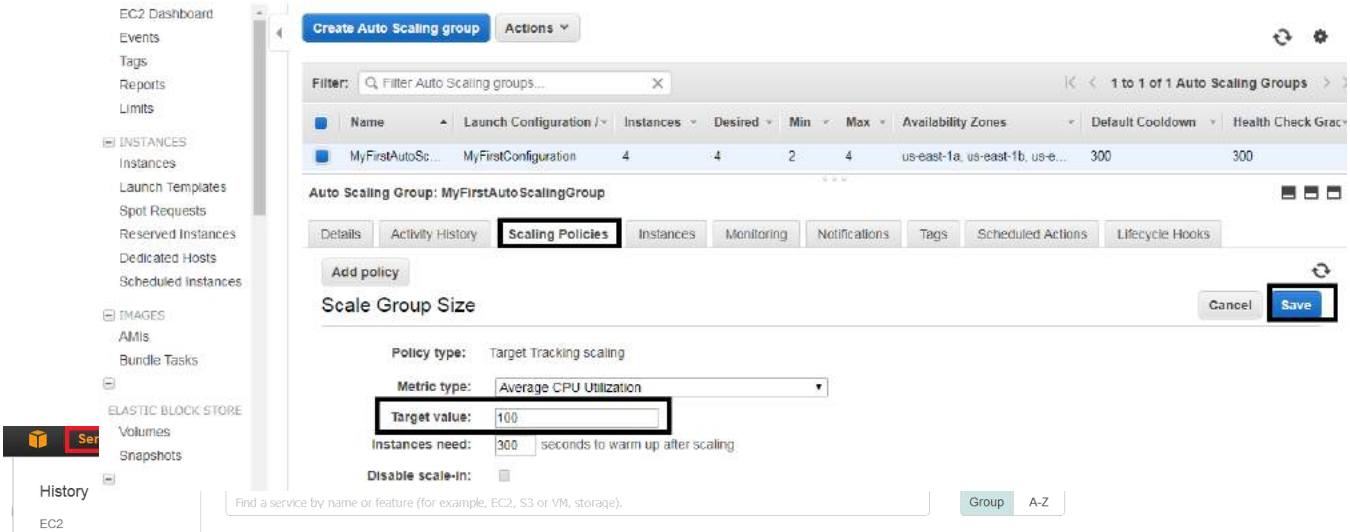




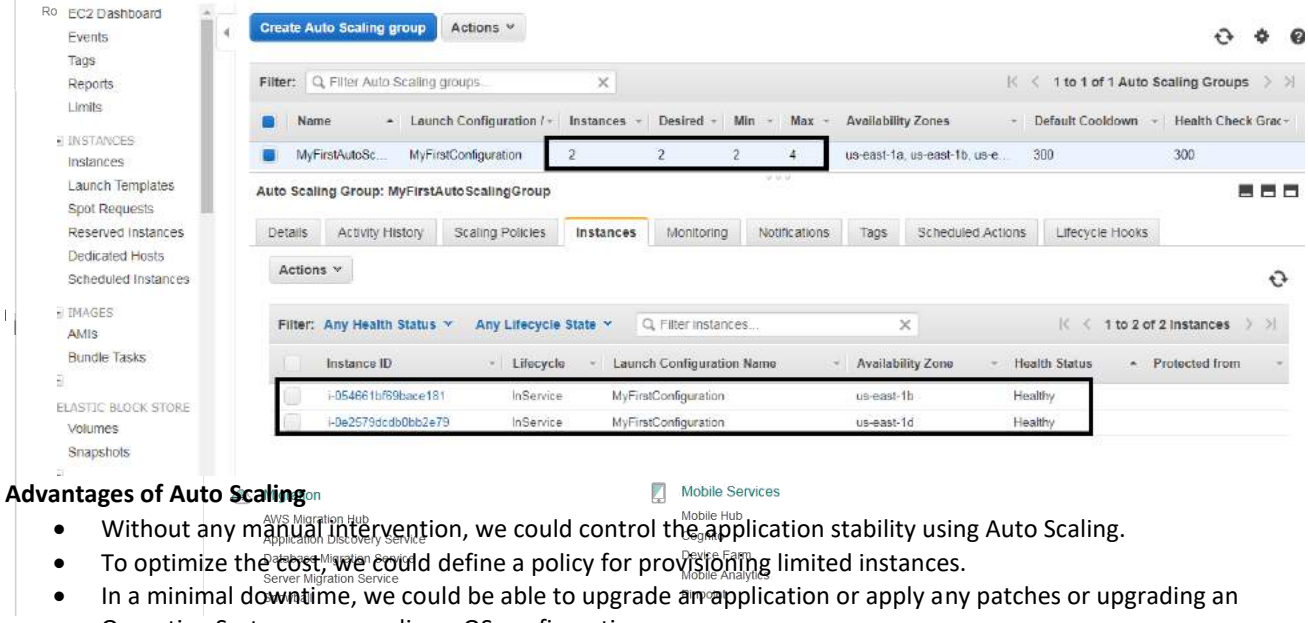
- Once the Scaling policies has been modified, instances would start to provision automatically by defined scaling policies and the same can be seen in Instances section.



- To ensure Scale In, am again changing the Scaling Policies to 100% of CPU utilization.



- Based on the scaling Policies, instances have been reduced to 2 instances which is the default count which has been set for this Auto Scaling Group.



Advantages of Auto Scaling

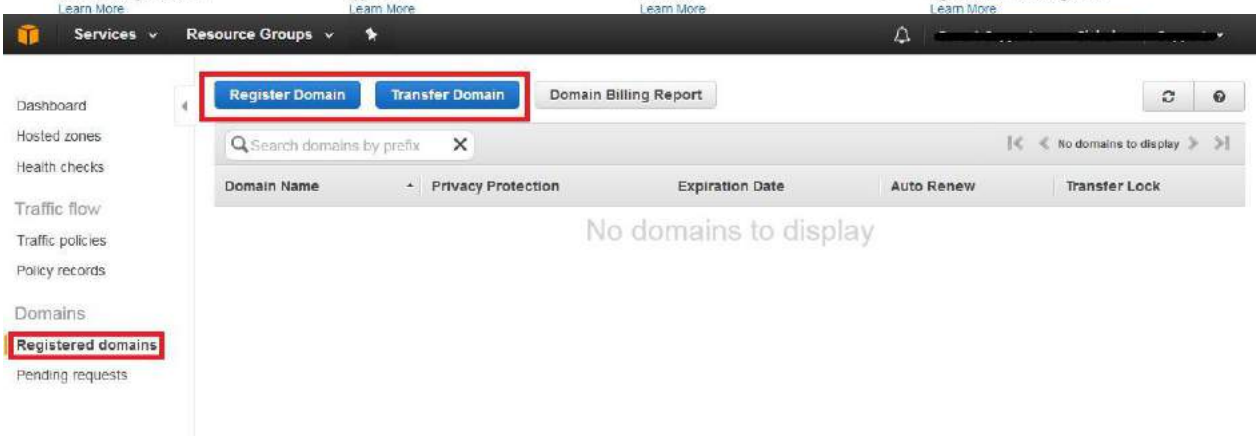
- Without any manual intervention, we could control the application stability using Auto Scaling.
- To optimize the cost, we could define a policy for provisioning limited instances.
- In a minimal downtime, we could be able to upgrade an application or apply any patches or upgrading an Operating System or upgrading a OS configuration.

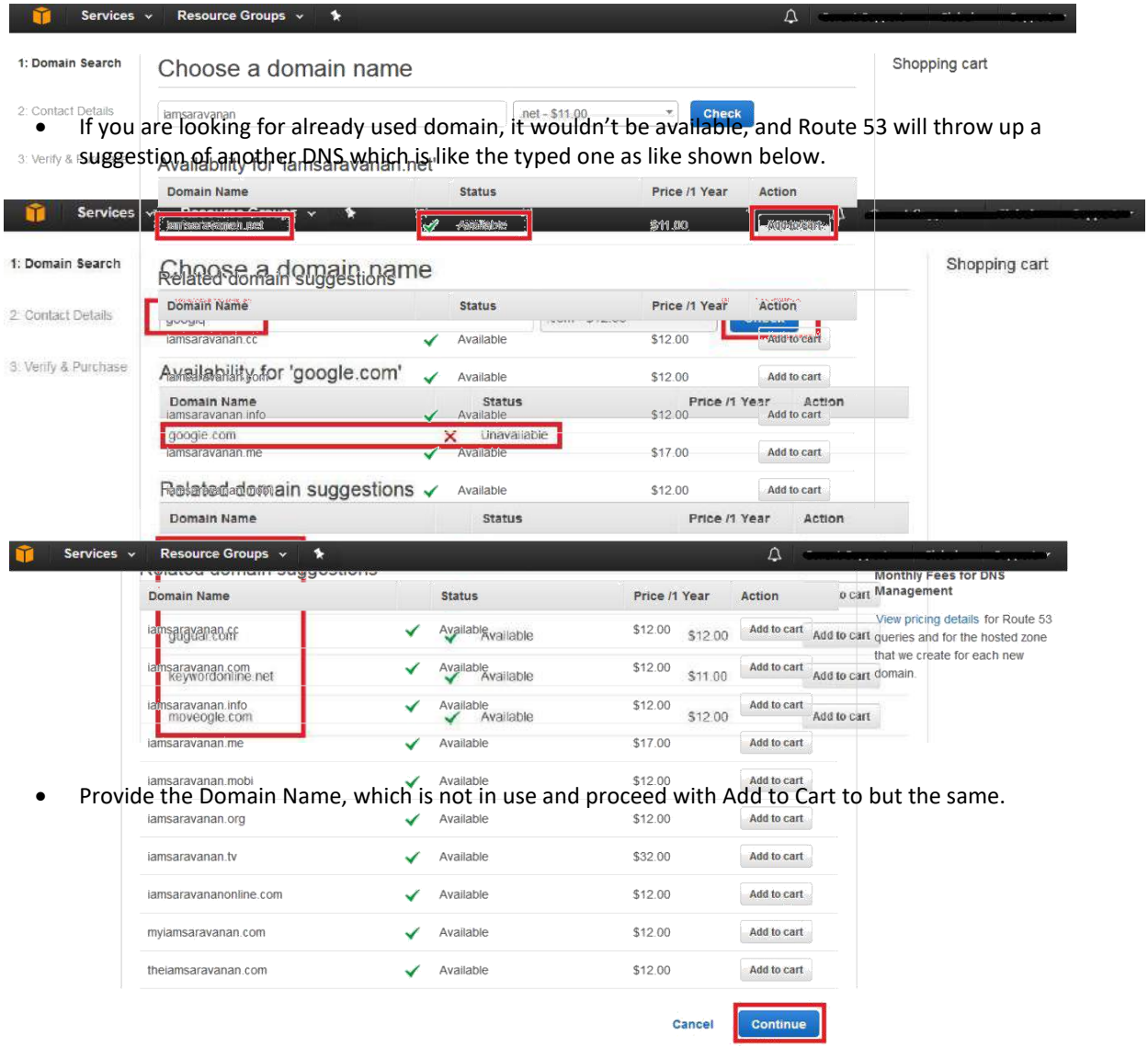
Route 53:

- Route 53 is being used to register a new domain name service / hosting an existing domain to any of the EC2 instances, transferring a domain and managing the DNS.
- To Register a new Domain, navigate to Services, choose Route 53 under Network and Content Delivery option as like shown below.

- For Registering a new domain, you can click on Get started now under Domain Registration.

- Followed by, click on Register domain for buying a new DNS which can be used for your application. If you have an existing domain, you can click on transfer, which would transfer an existing domain name to AWS Route 53.

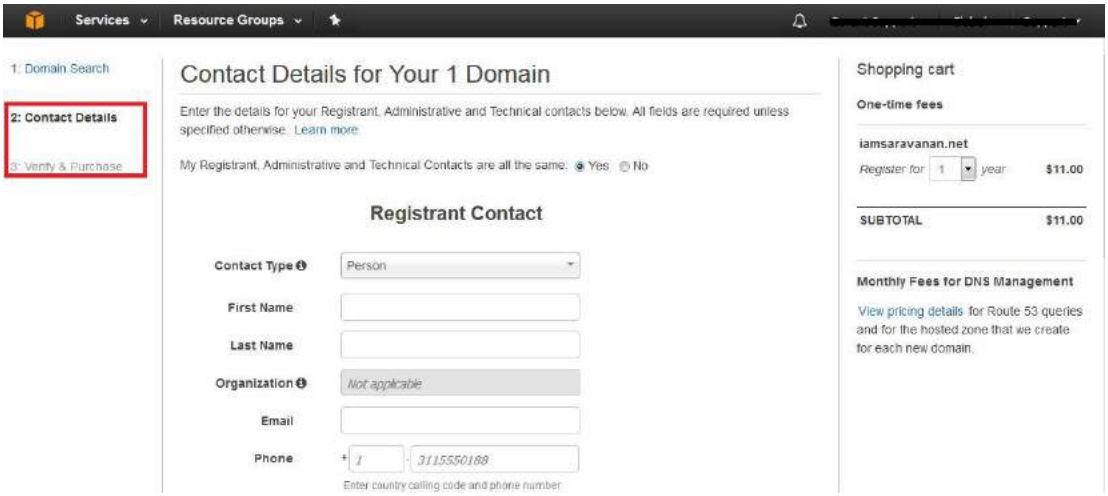




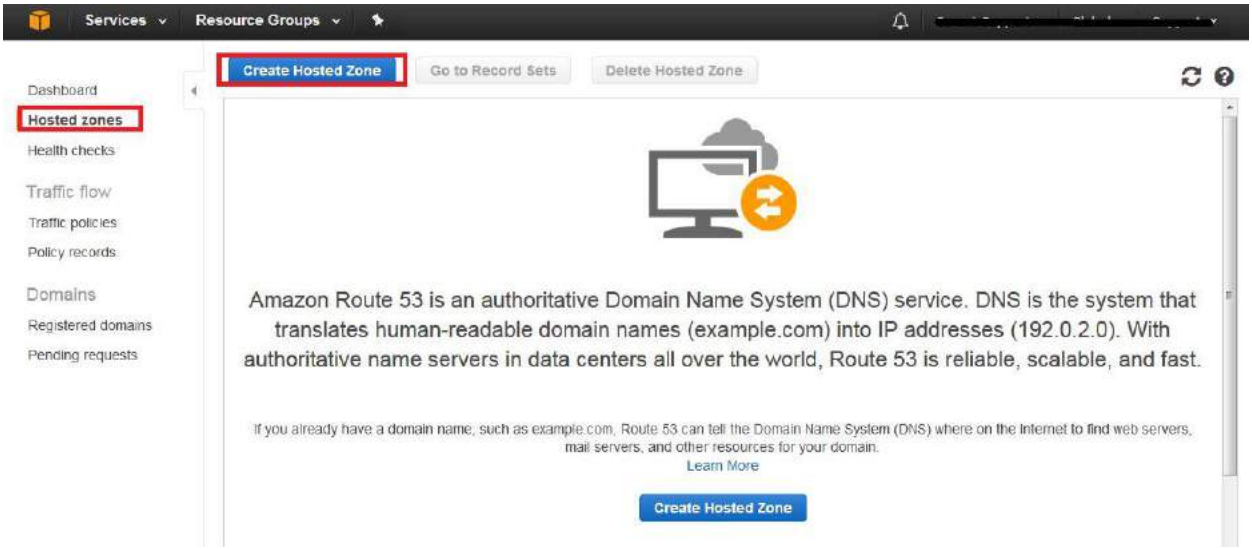
- If you are looking for already used domain, it wouldn't be available, and Route 53 will throw up a suggestion of another DNS which is like the typed one as like shown below.

- Provide the Domain Name, which is not in use and proceed with Add to Cart to but the same.

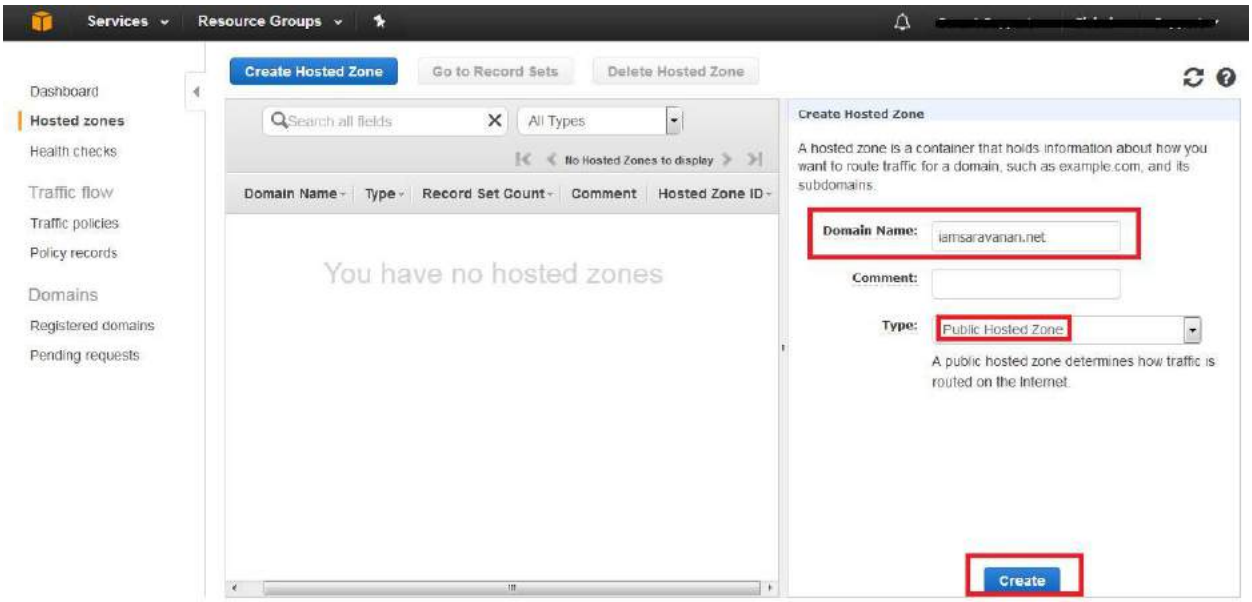
- Proceed to purchase a DNS by providing basic information as like shown below.



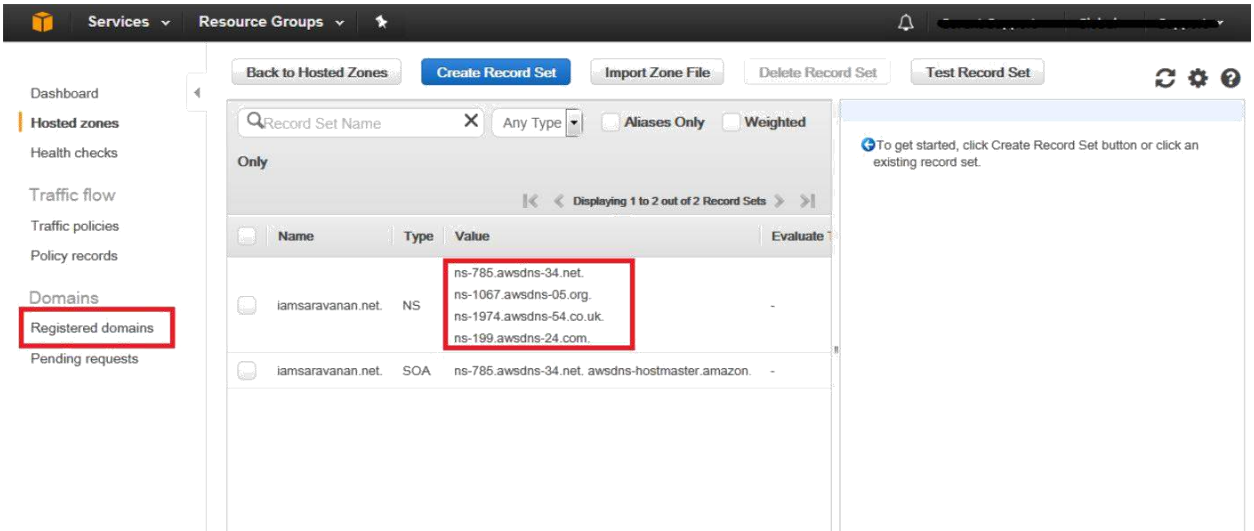
- Click on Hosted Zone for mapping an existing / registered domain name. After clicking on hosted zone, navigate to create Hosted zone as like shown below. Reason for creating a hosted zone is, it doesn't connect automatically to the domain name. Hence, we would be denoting for owner of the domain and DNS provider will be denoting for hosted zones.

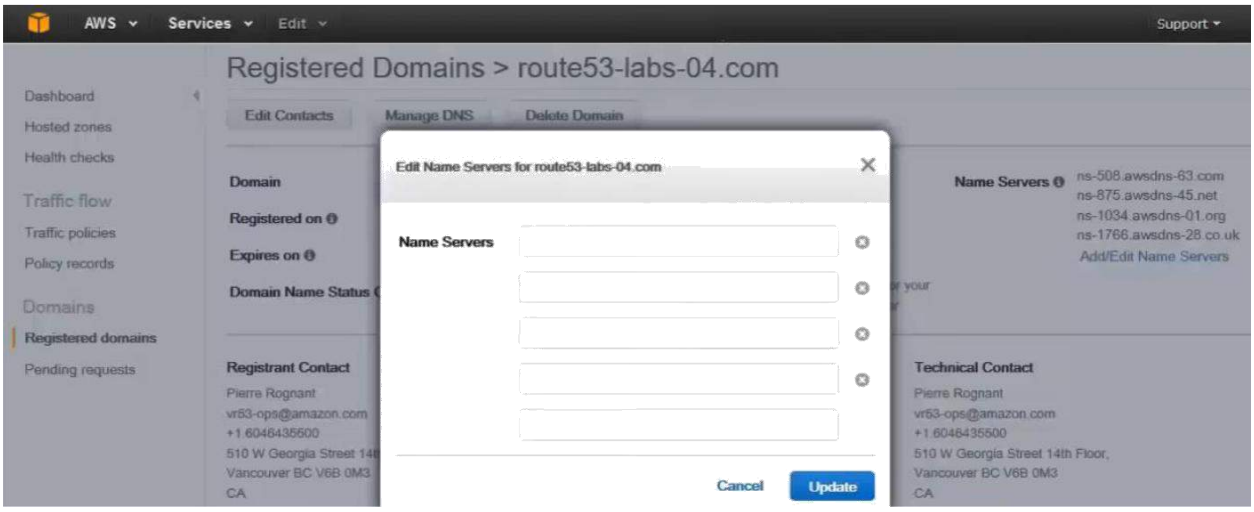


- Provide an existing / registered domain name and choose the type as public hosted zone.

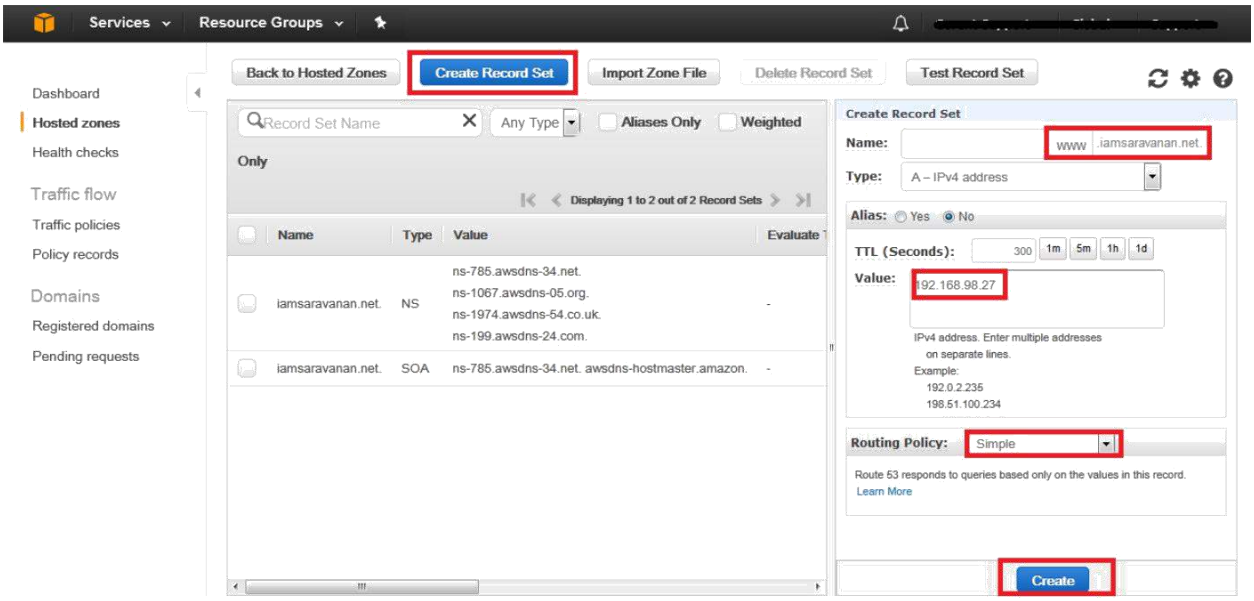


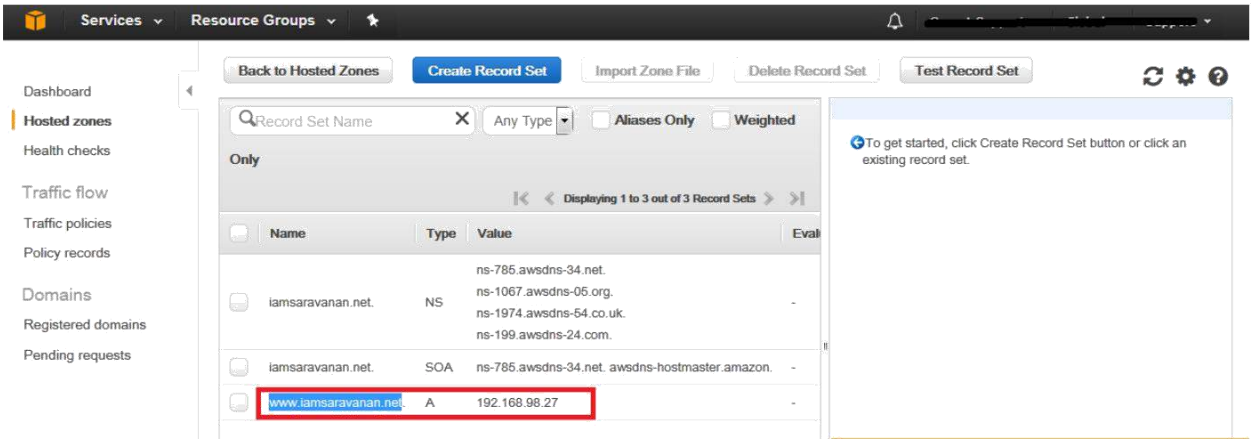
- After creation of hosted zone, 4 NS values (nameservers) would be generated. We need to map these 4 values in a registered domain. Advantages of mapping these 4 values (nameservers) in a registered domain are the actual DNS which would routes to these 4 values to give an output to end users.





- Once you have been updated these 4 values, proceed to create a new DNS record for the domain using the IP address of my web server.
- After creating a new record, you would be able to access the application using the domain name instead of IP address.



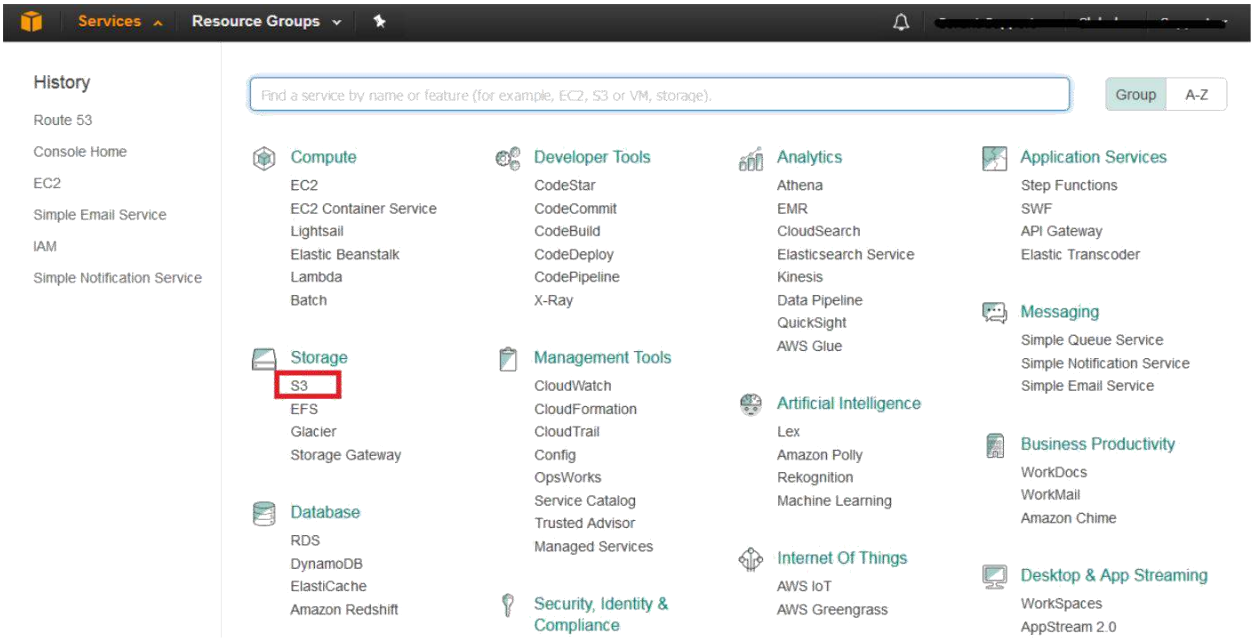


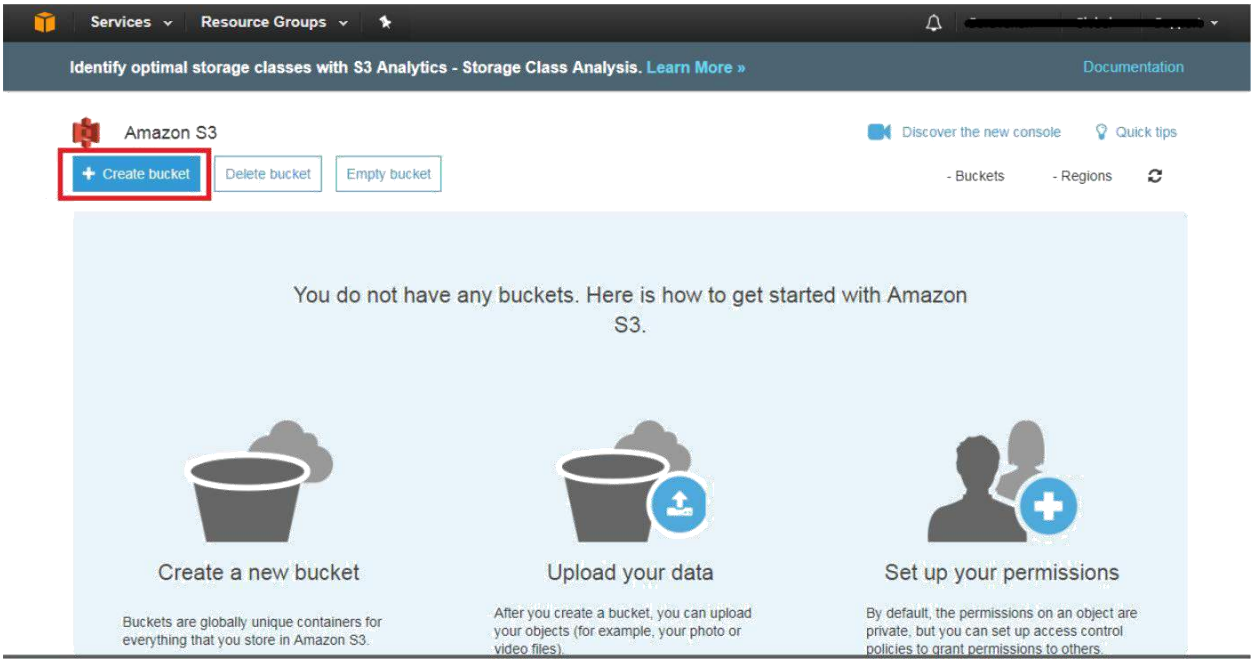
Advantages of Route53:

- Domain Name could be easily purchased and transferred from another domain provider.
- Easily host a zone by creating new record sets.

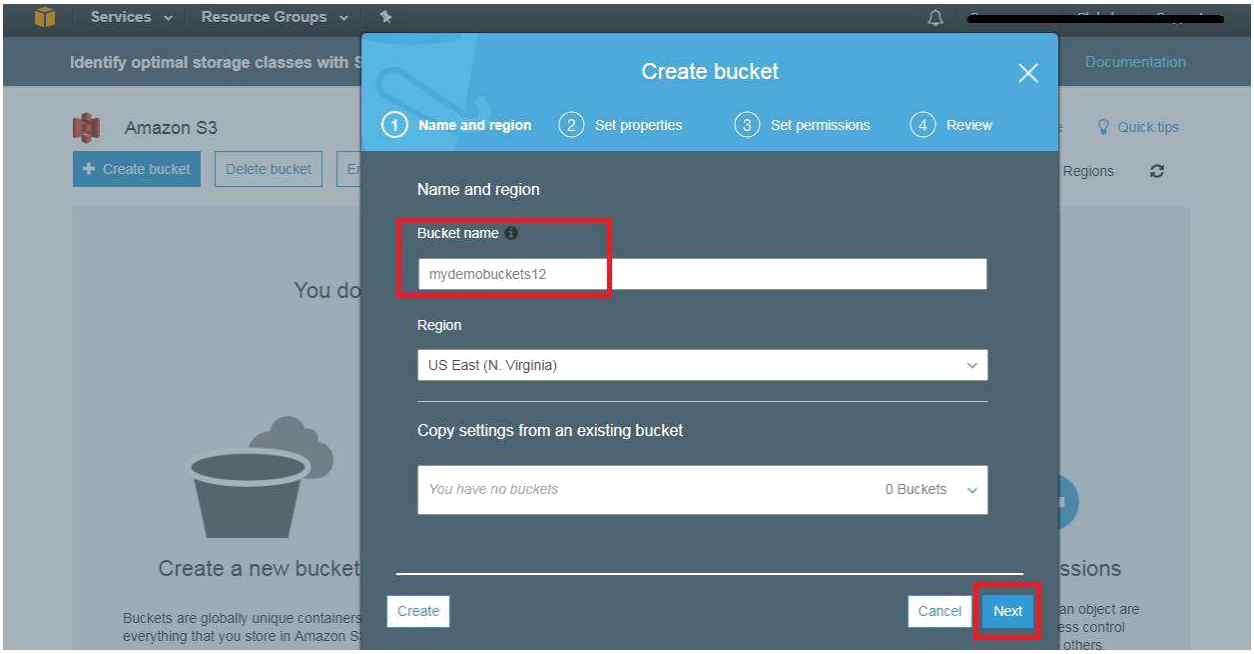
S3 (Simple Storage Service):

- AWS S3 is abbreviated as Simple Storage Service. S3 makes it simple and practical to collect, store, and analyze data - regardless of format – all at massive scale. S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices.
- Click on Services and Select S3 for creating a new bucket as like shown below.

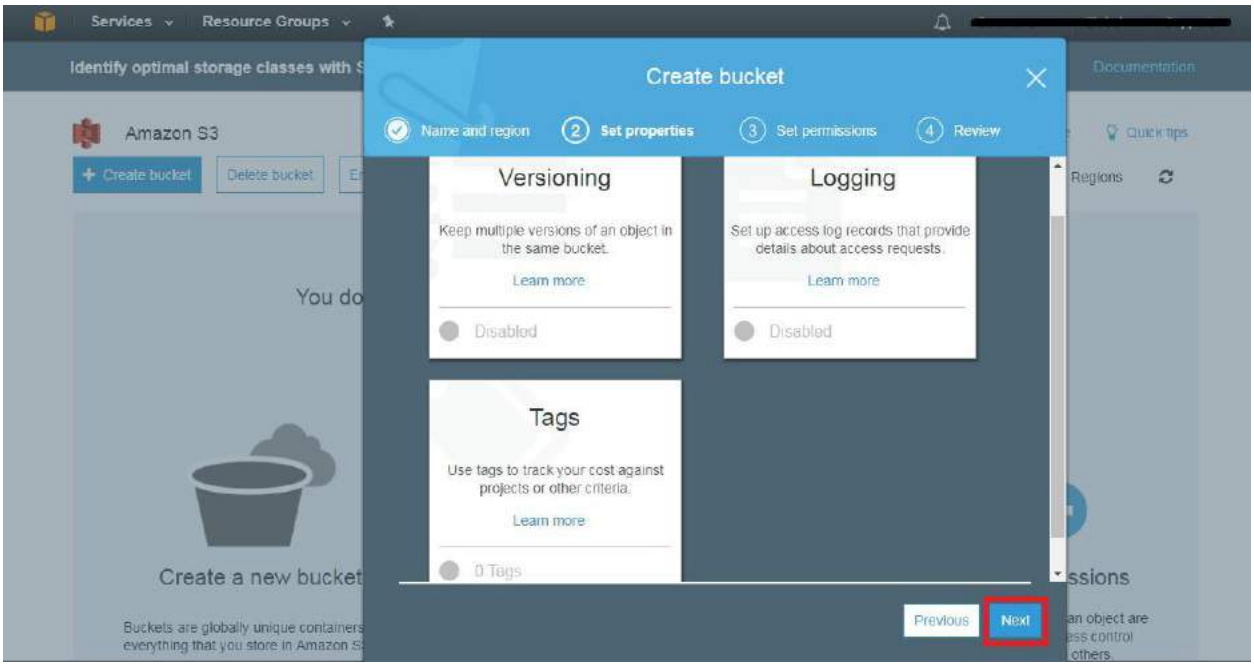




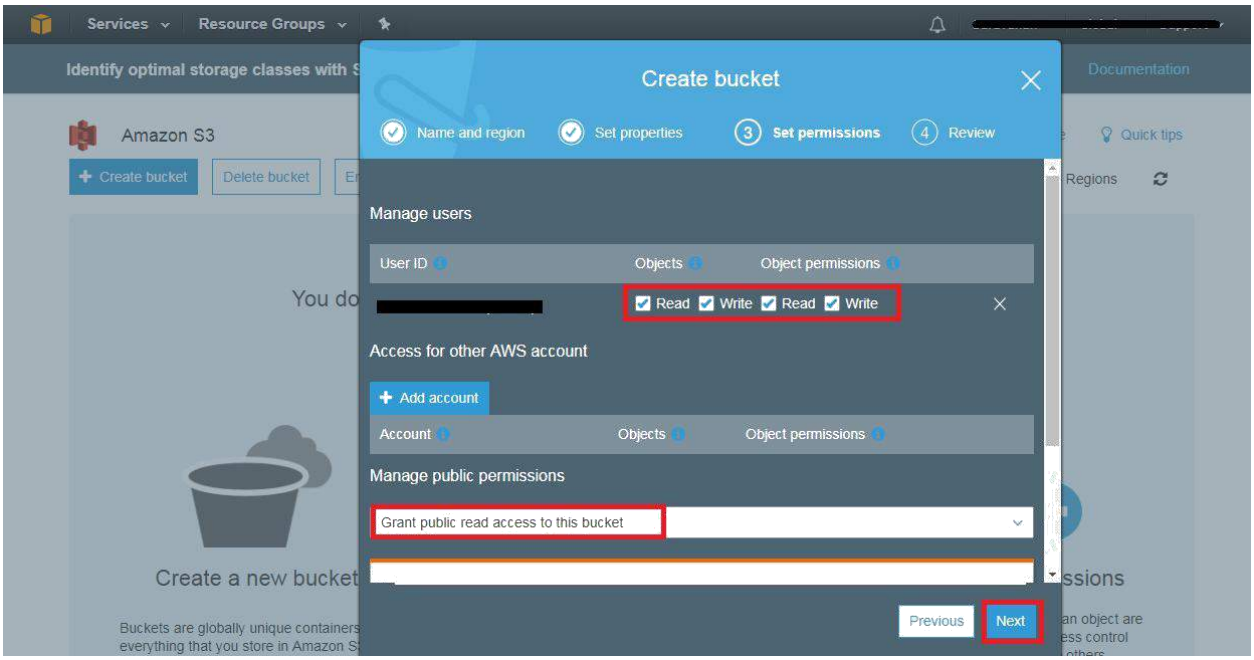
- Provide the name for bucket and click on Next as like shown below.



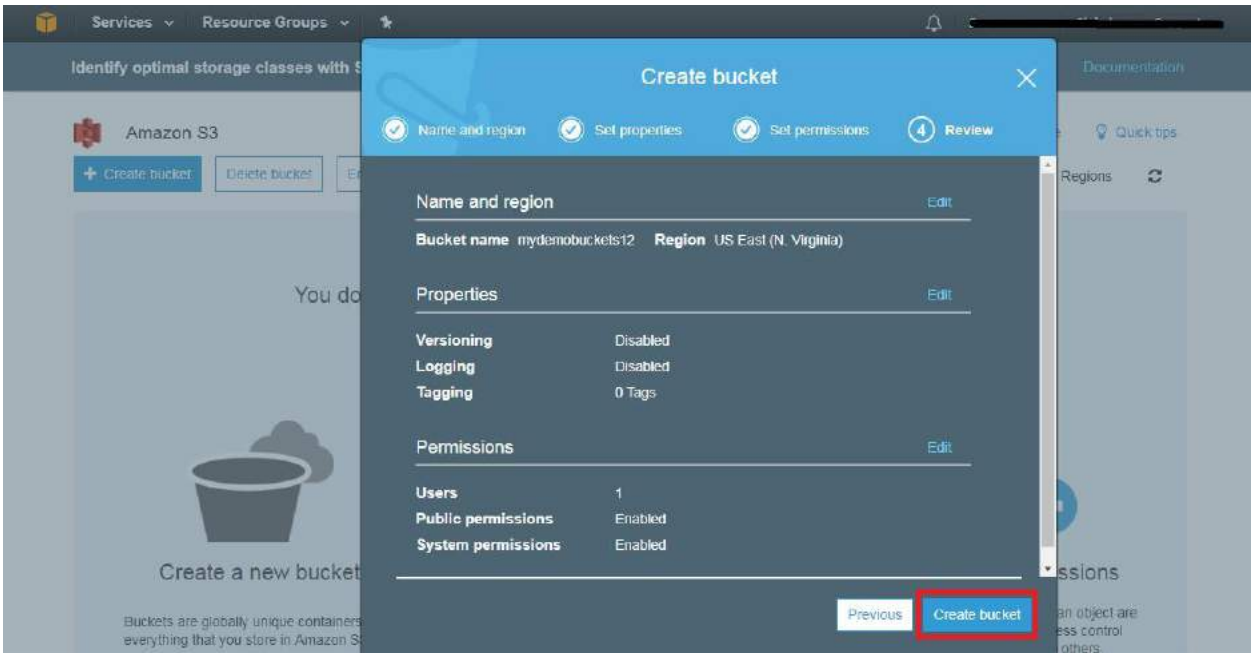
- Versioning is to maintain the list of versions of data which you are uploading to the bucket. Logging gives you a log files for each transactions / activity which you are doing in the S3 bucket which has been created. Tag Names is just to maintain an identity of bunch of data which you have been uploaded in the bucket. If required enable these three modules and click on next.



- Provide the permissions to access the created bucket. It can be provided based on the requirement, so that you can proceed to assign the respective privileges as like shown below.

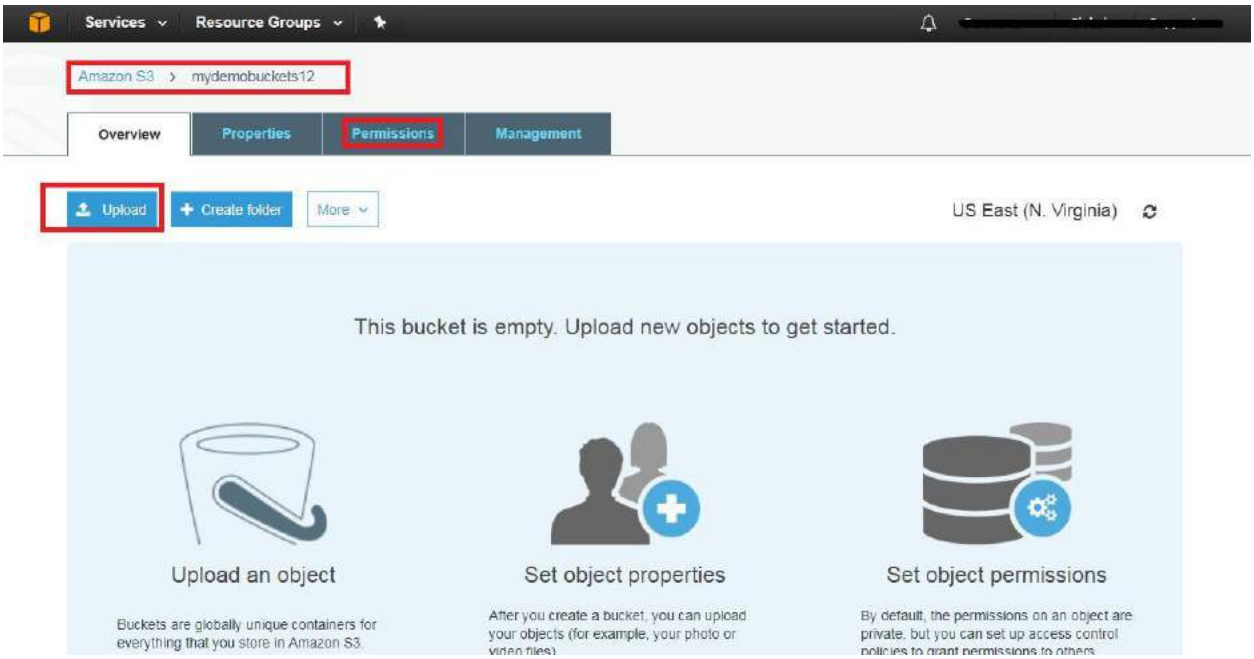


- Review the list of items which has been mapped / chosen and proceed to create bucket as like shown below.

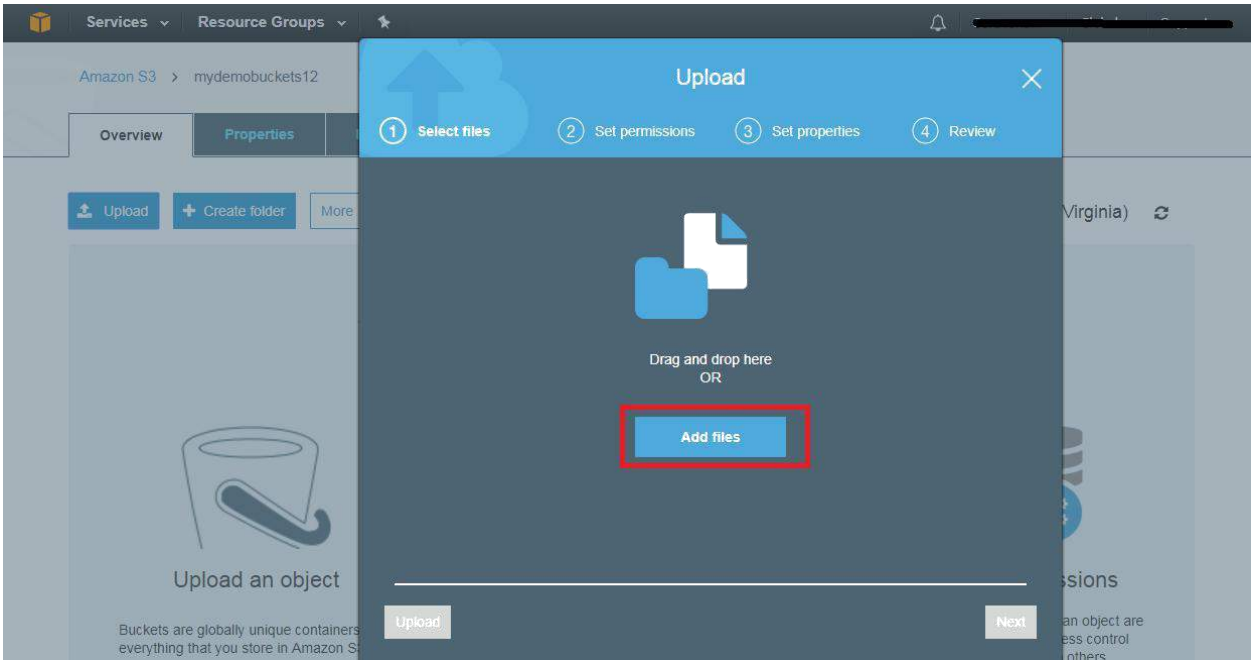


- Created buckets can be viewed in the bucket list. Proceed to click on respective bucket for uploading the data files inside the bucket.

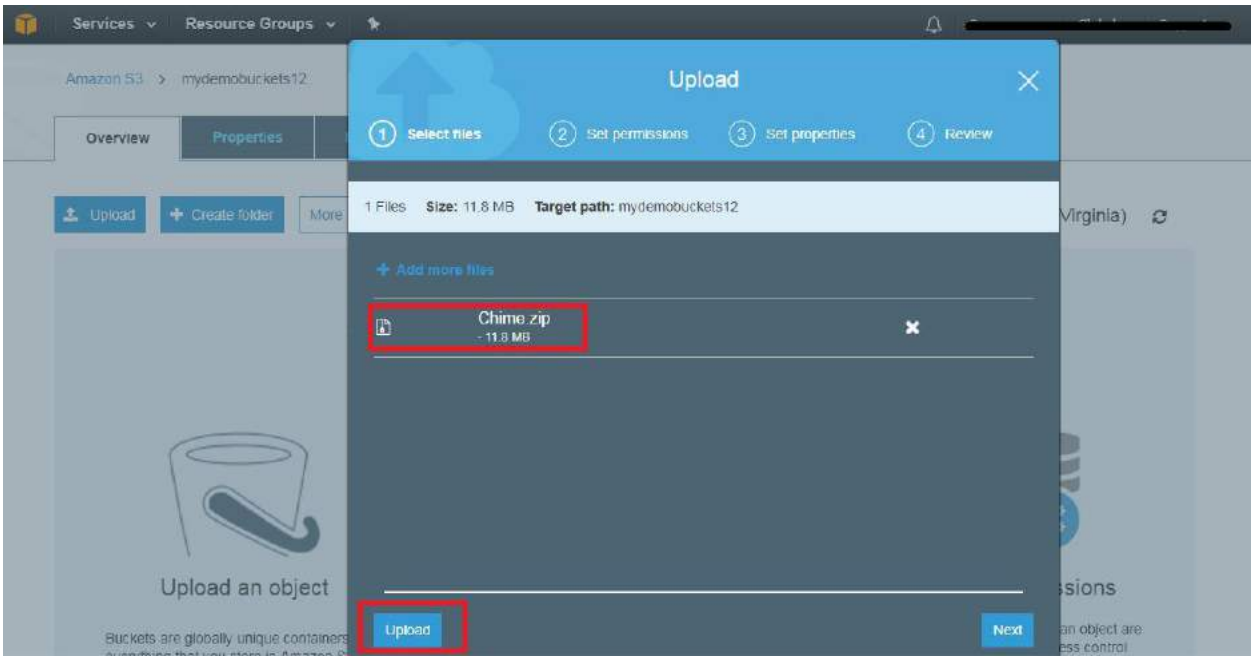
- Proceed to click on Upload button for uploading any kind of data into the created bucket. If any permission needs to be edited after the creation of bucket, that can be possible by clicking on permissions tab and change the privileges.

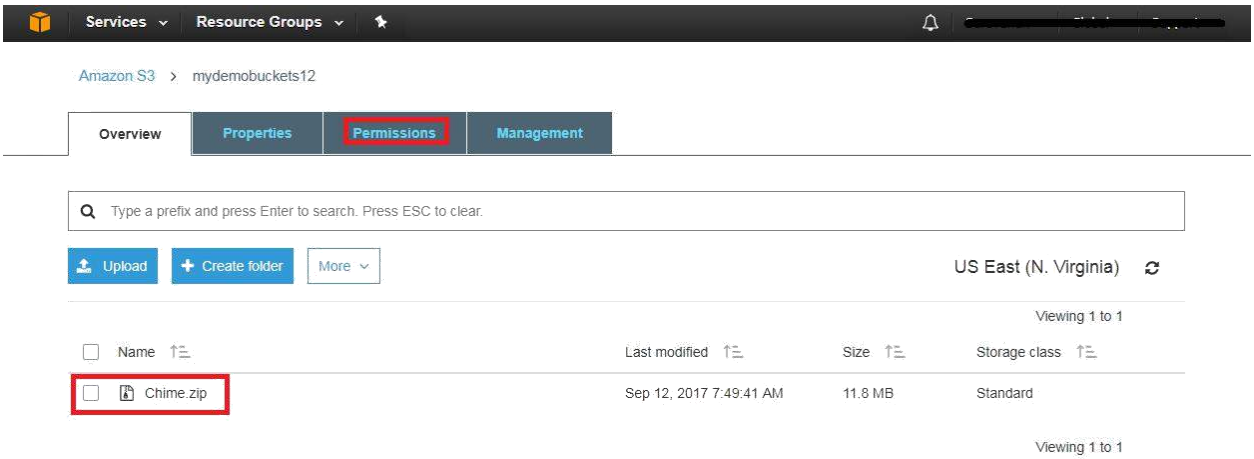


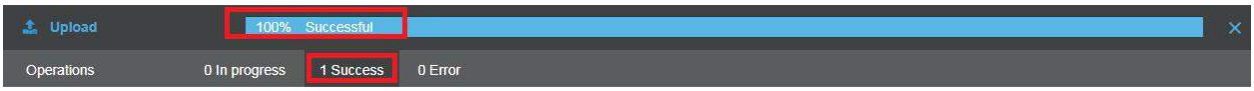
- Click on Add files for choosing the data files from your PC to upload it into S3 bucket as like shown below.



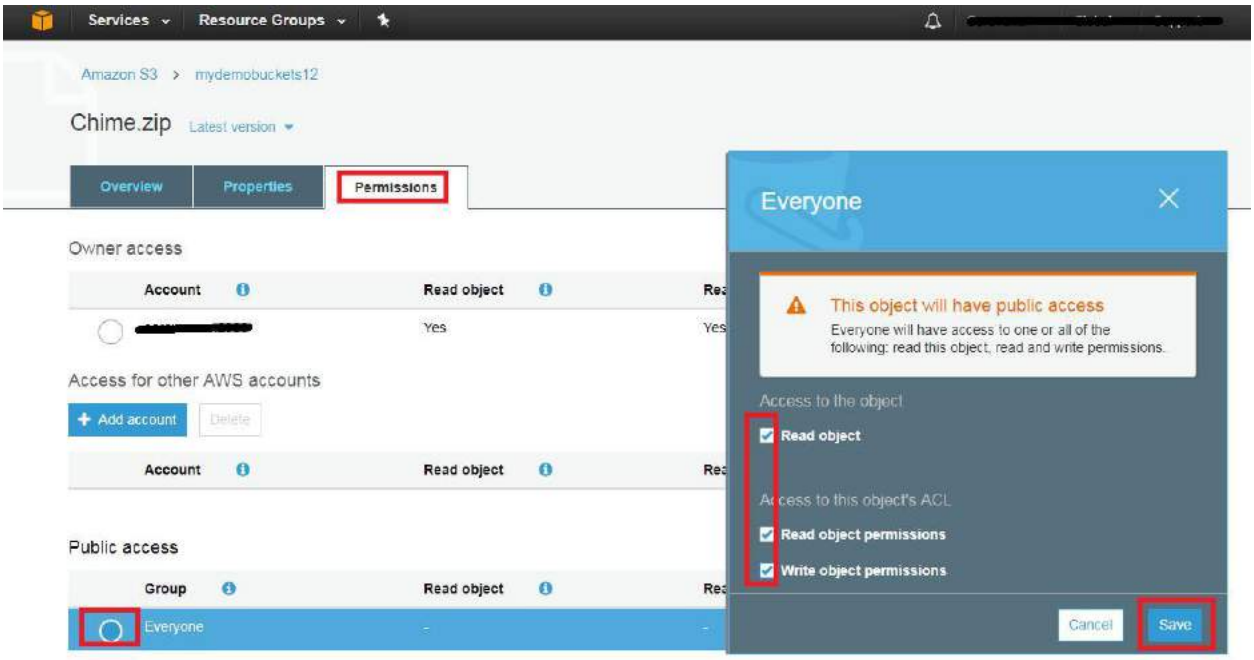
- After choosing the file, click on Upload Option for start the upload activities of chosen data file. During this upload screen, you can provide the permission of the data that can be able to read / write the same on Set Permissions Tab. Permission can be provided even after uploading the data into bucket. Once the upload gets completed, it would be placed under the bucket which has been created in S3 as like shown below.



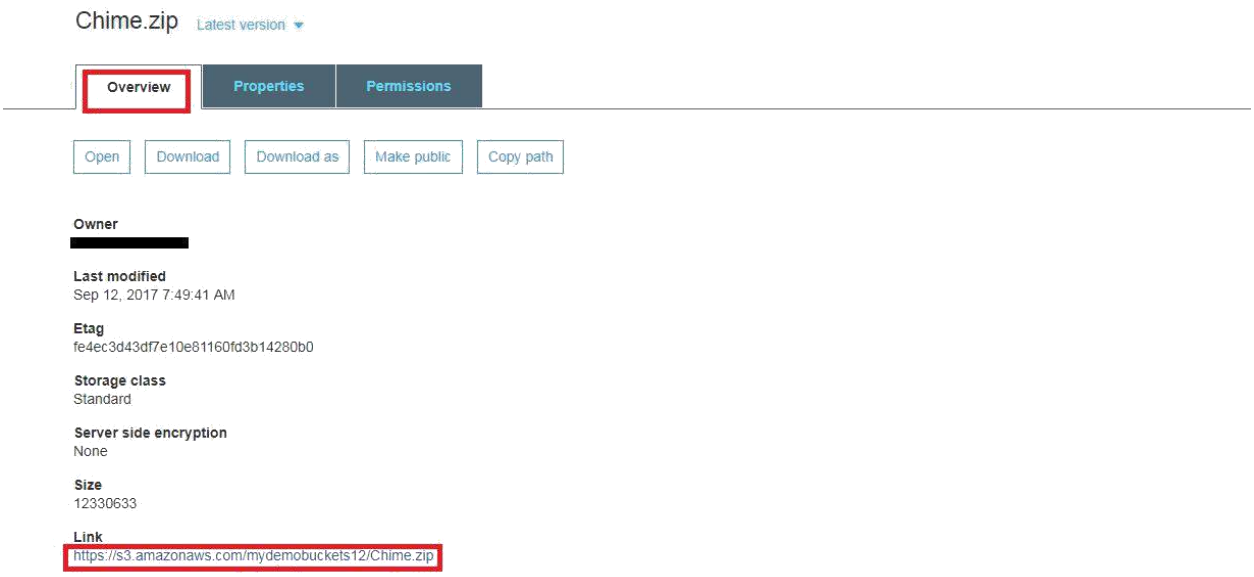




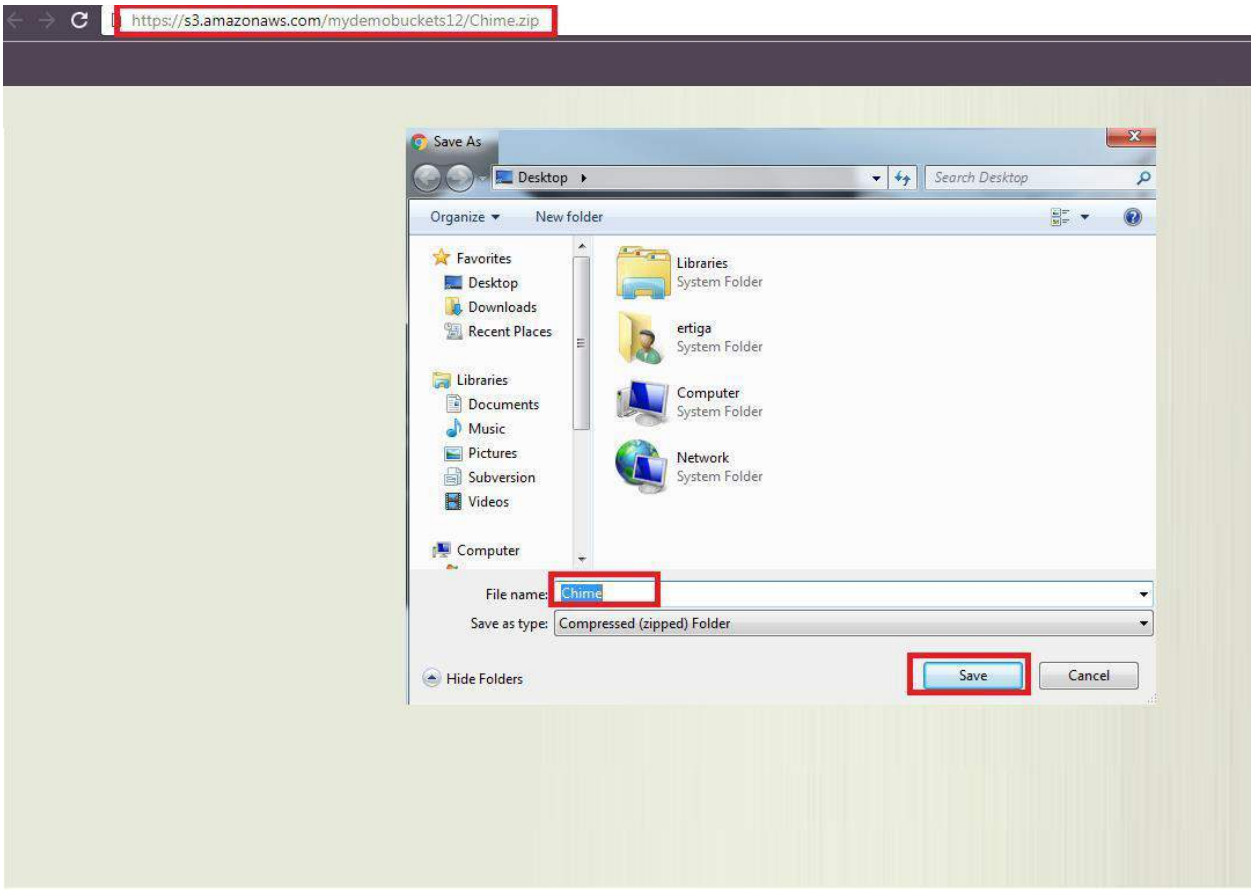
- Navigate to Permissions Tab as like shown in above screenshot and choose everyone option to provide a grant all access to everyone across the globe, which can be able to download the uploaded data file into S3 bucket as like shown below.



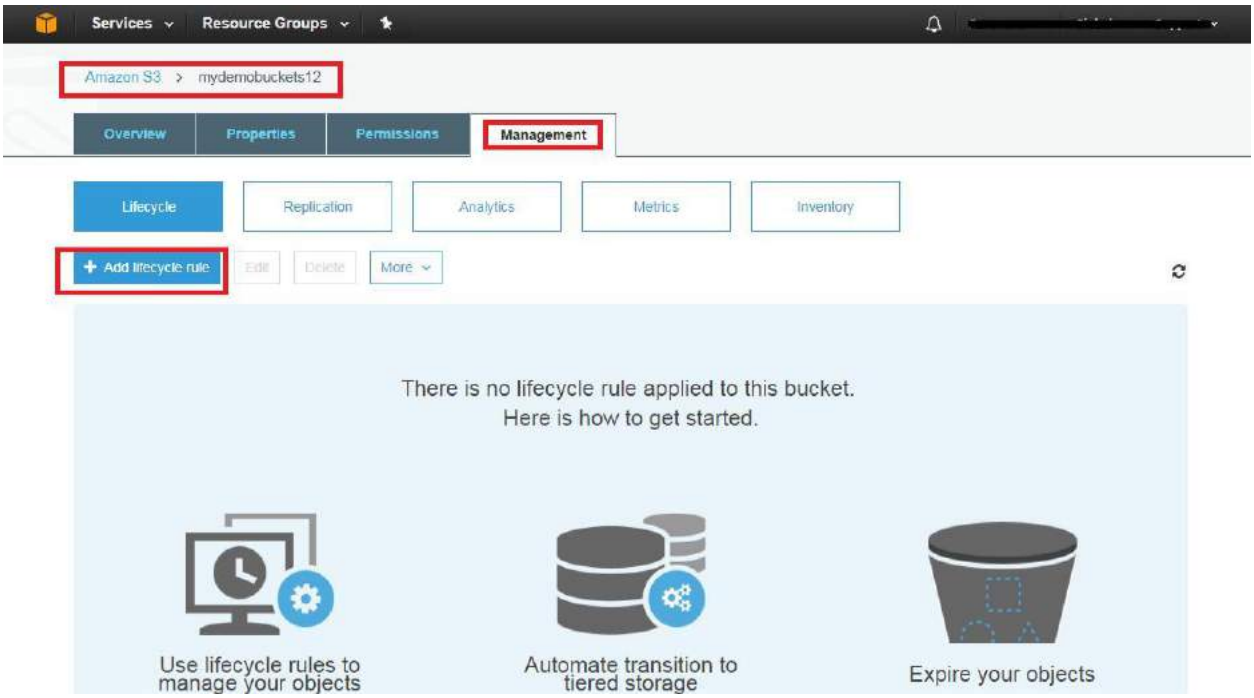
- After providing the permissions, navigate to Overview tab for copying the URL to download the uploaded data.



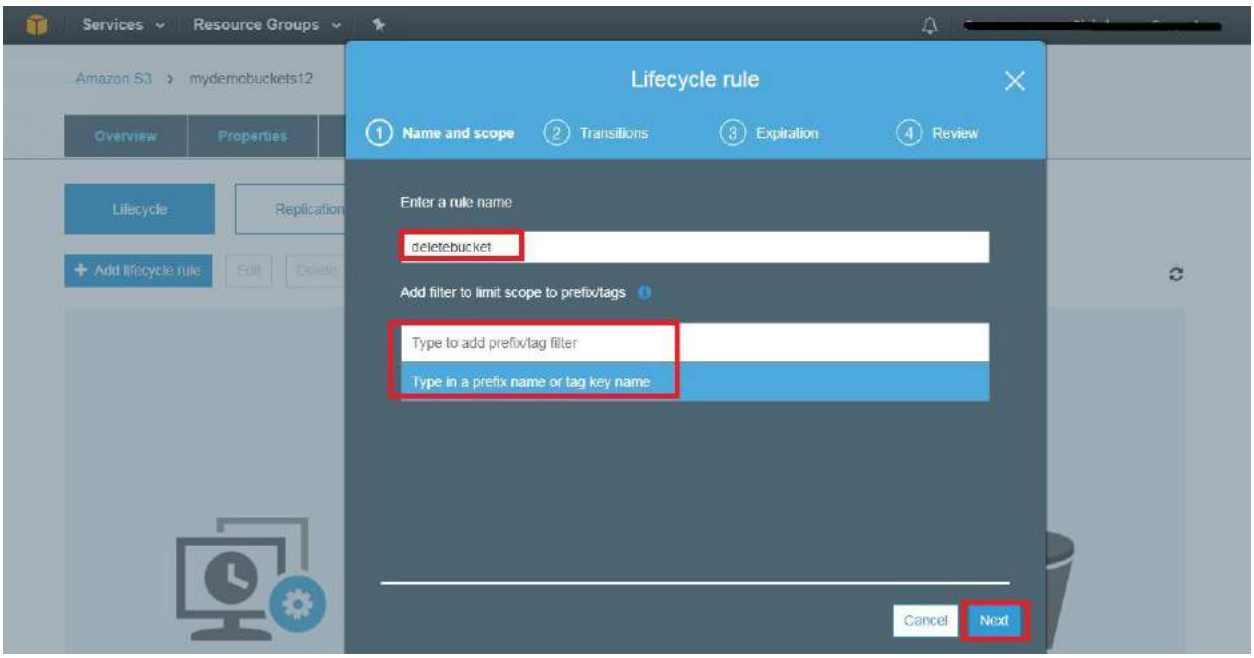
- Paste the copied URL in any of the browser and ensure it is downloading as expected.



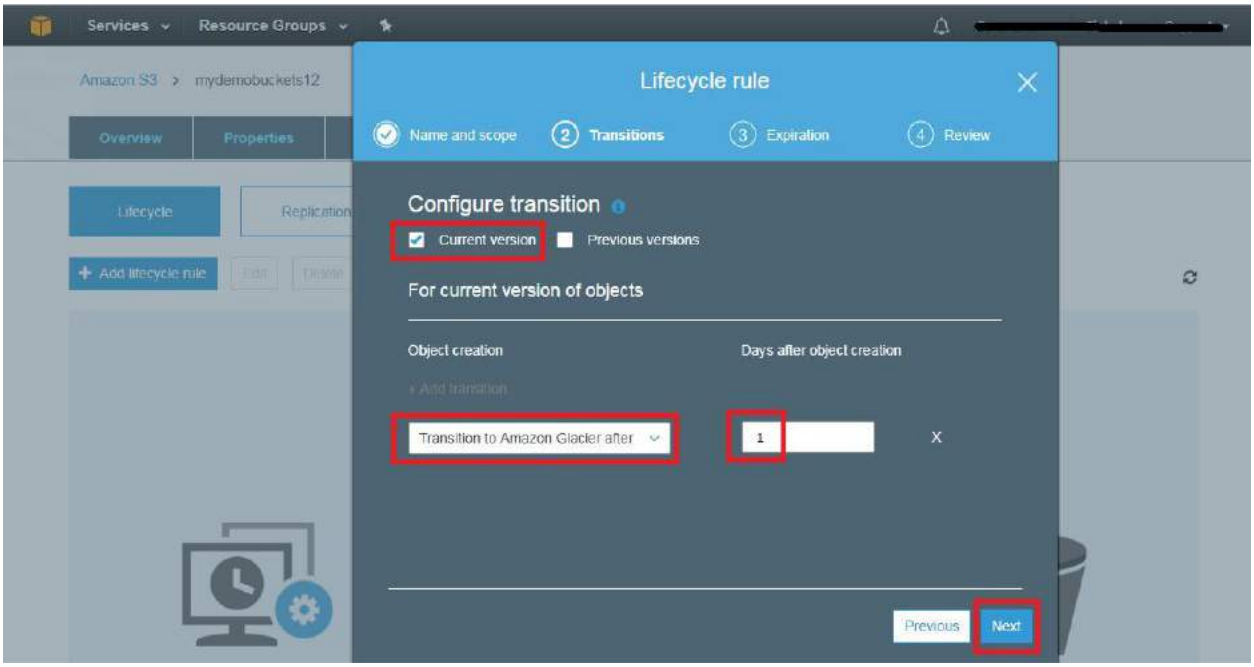
- We would be able to set the process for archiving the uploaded data automatically to Glacier by creating a new Lifecycle rule as like shown below. To do that, we need to navigate to Management and choose the Add Lifecycle rule.



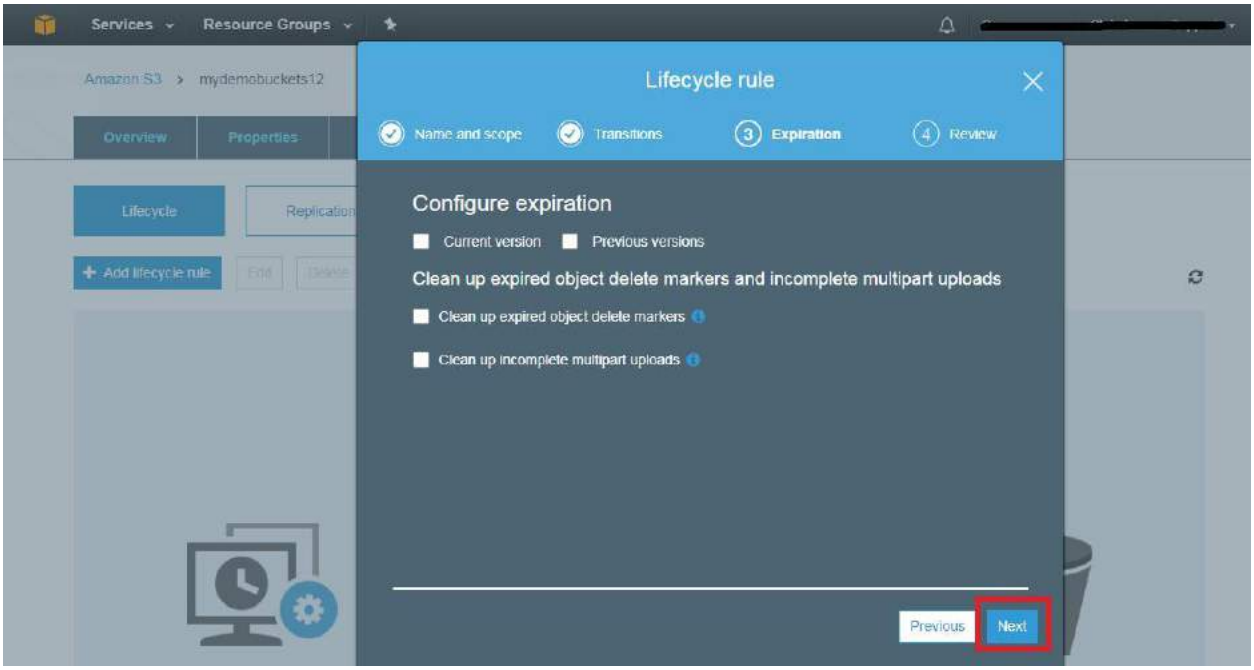
- Provide the rule name and if you want to archive the complete bucket, you no need to provide any name on prefix section and if you want to delete any particular data inside the bucket, we need to specify the data file name in prefix section. Then click on next.



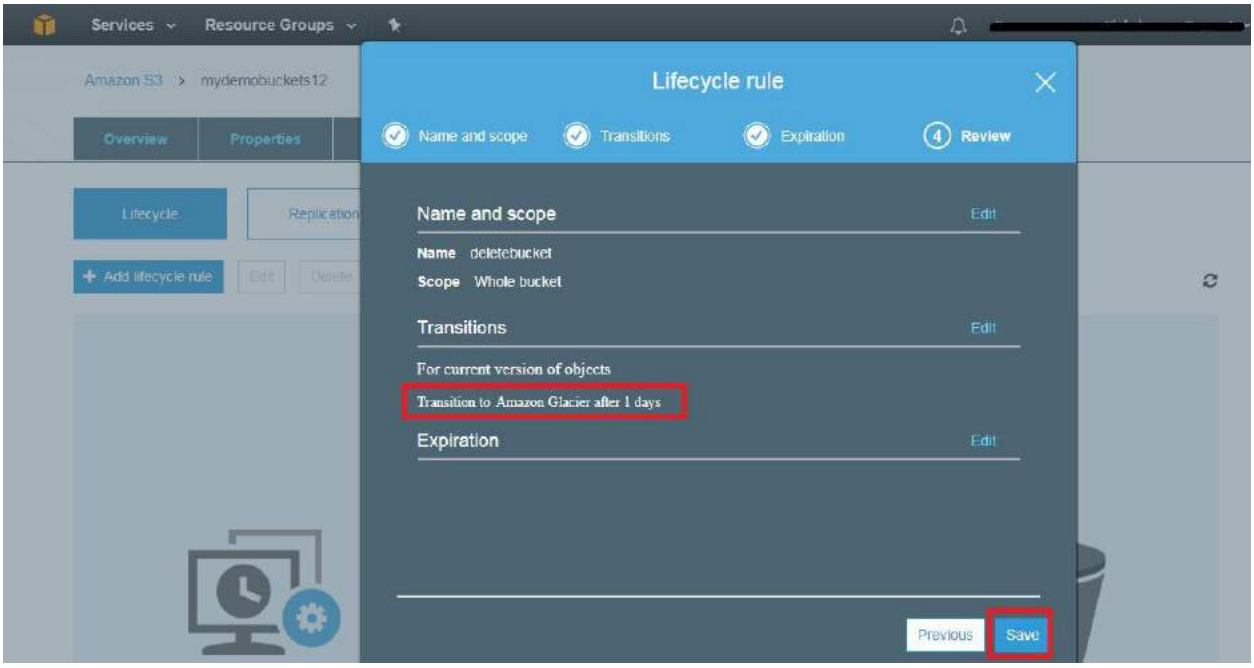
- You can select the current version of bucket which needs to be archived to Glacier after mentioning number of days. Also, these data can be moved to STANDARD_IA storage class when you know those objects are infrequently accessed. It can be done by choosing the drop down.



- Uploaded data files can be expired and once it has been expired, it would be deleted from S3 bucket. Also, if you want to clean up the data which has been failed to upload, it can be done by selecting Clean up Expired Object and Incomplete multipart uploads.
- Please find the below URL to download some sample scripts for uploading / synchronizing the data from EC2 instances to S3.
- https://drive.google.com/file/d/1oycnSFUvTc_1Js-NCwm_6CRqdNMAeV8V/view?usp=sharing



- Review the added content and click on save for archiving the data after a day and it would be under Glacier.



Advantages of S3:

- Any file or data with a large amount of size could be easily accessible / downloaded from anywhere.
- We could use this S3 as common repository for automation scripts as we are doing in GitHub and Chef Server.
- Backup of an Artifacts could be saved in S3 bucket and same could be retrieved in a minimal time.
- Uploaded data could be archived or Expired automatically based on the policy which we set during uploading.
- S3 Buckets are acting as an interface to export or import a data from end user to AWS resources like (DynamoDB, RDS, etc.)
- Elastic Beanstalk using this S3 bucket for transferring the data to instances.

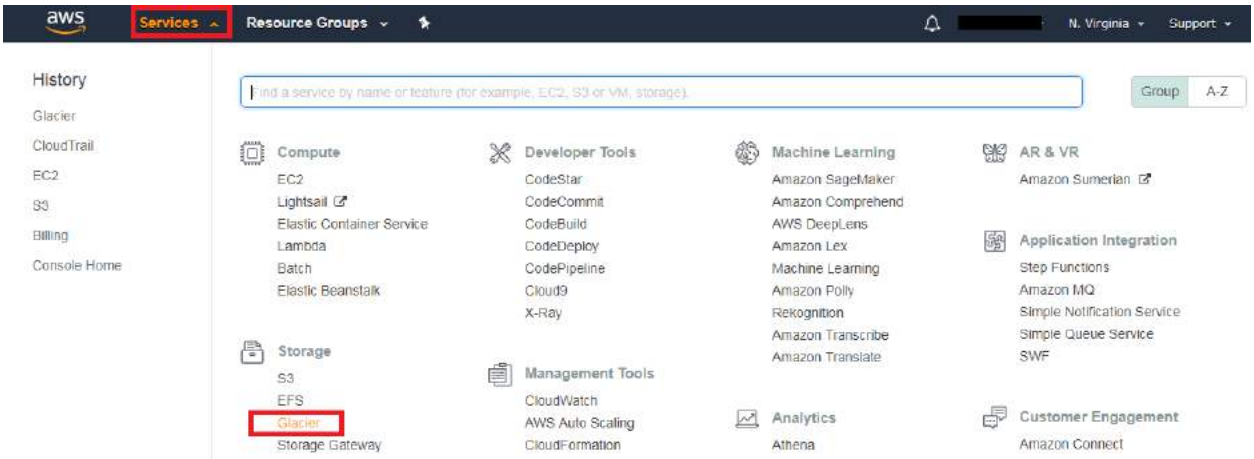
Glacier:

- Data is stored in Amazon Glacier in "archives." An archive can be comprised of any data such as photos, videos, or documents. You can upload a single file as an archive or aggregate multiple files into a TAR or ZIP file and upload as one archive.

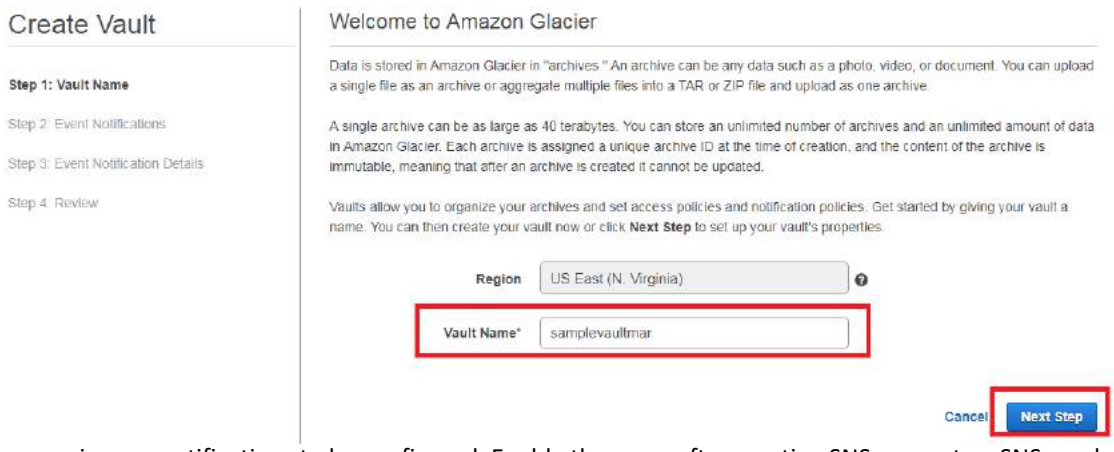
- A single archive can be as large as 40 terabytes. You can store an unlimited number of archives and an unlimited amount of data in Amazon Glacier. Each archive is assigned a unique archive ID at the time of creation, and the content of the archive is immutable, meaning that after an archive is created it cannot be updated.

- Amazon Glacier uses "vaults" as containers to store archives. You can view a list of your vaults in the AWS Management Console and use the AWS SDKs to perform a variety of vault operations such as create vault, delete vault, lock vault, list vault metadata, retrieve vault inventory, tag vaults for filtering and configure vault notifications. You can also set access policies for each vault to grant or deny specific activities to users. Under a single AWS account, you can have up to 1000 vaults.

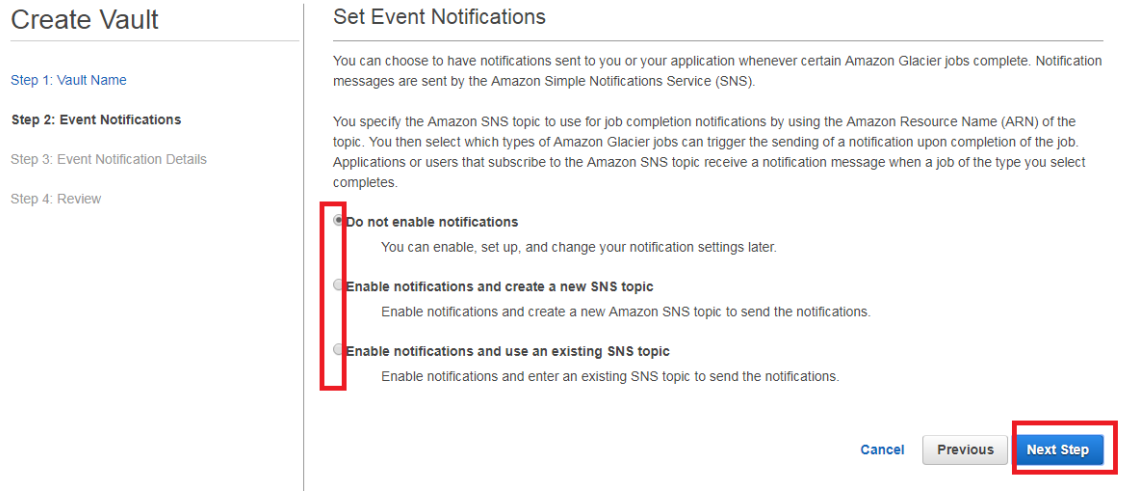
- Click on Services and Choose Glacier.



- Provide the Vault Name and Choose the region

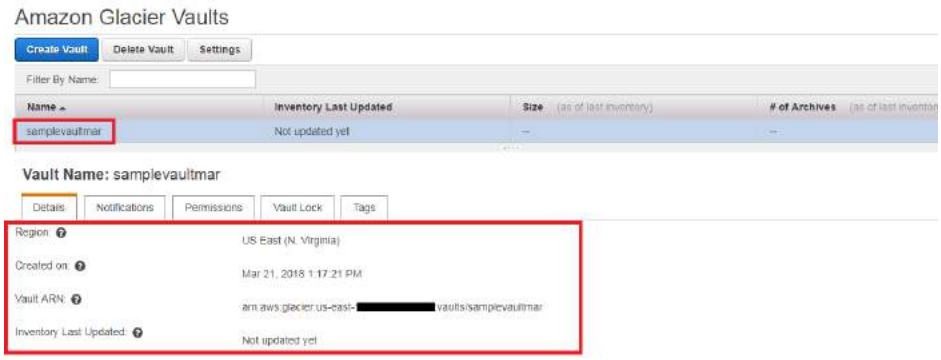


- If you require any notifications to be configured, Enable the same after creating SNS or create a SNS newly by here itself.

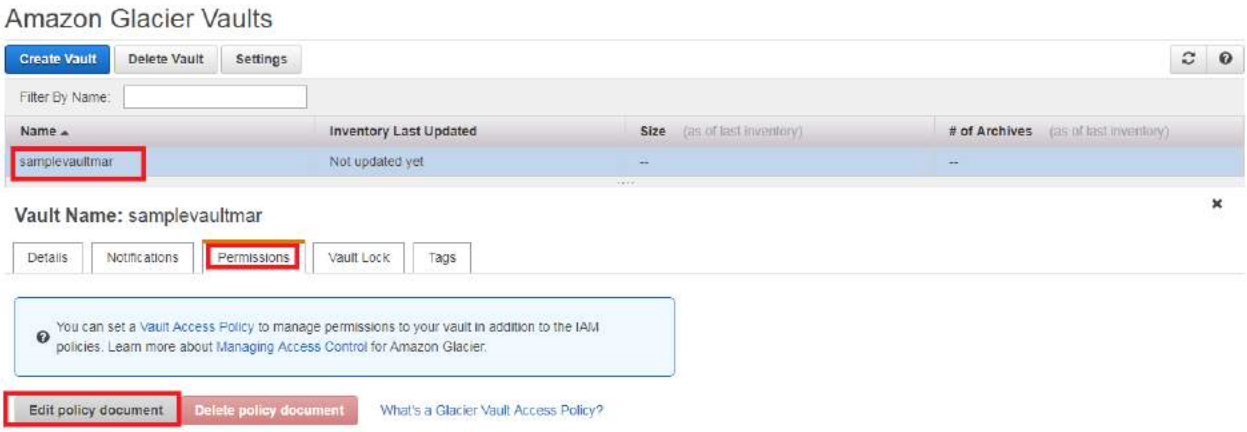


- Procced to review the values which has been provided and click on Submit.

- Once the Vault has created, we would be able to get an ARN.

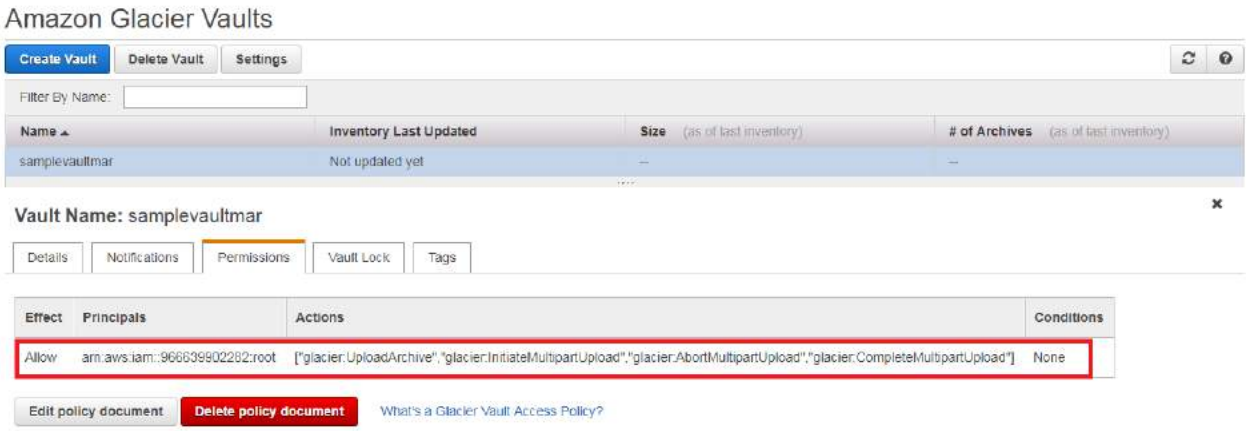


- To provide a permission to this vault, navigate to permission option.

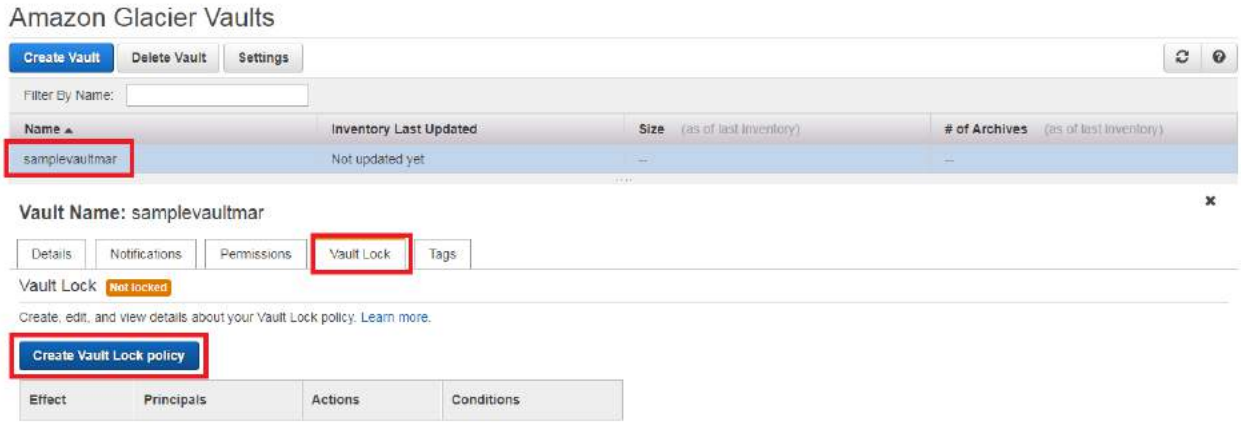


- Copy this entire code and provide a permission to upload any data to this Glacier.

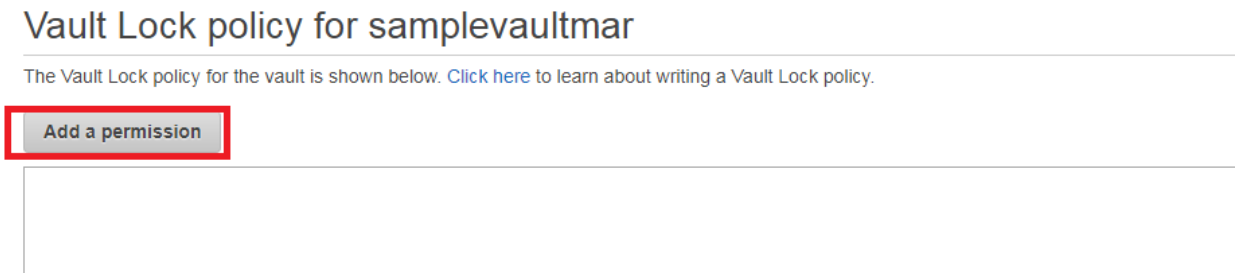
- Once the permission has been created, we would be able to see the same.



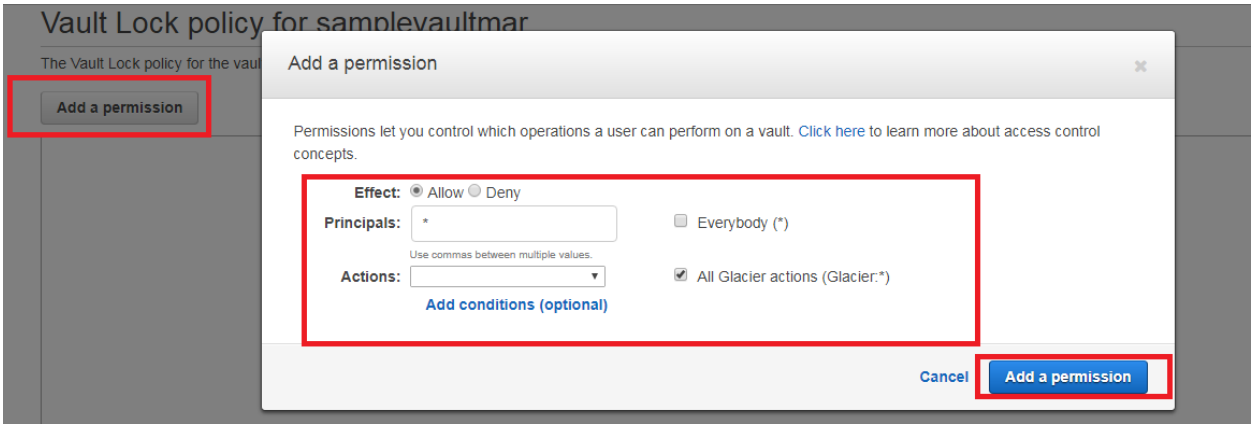
- Now, navigate to Vault Lock.



- Click on Add Permission to provide an access to this Vault.

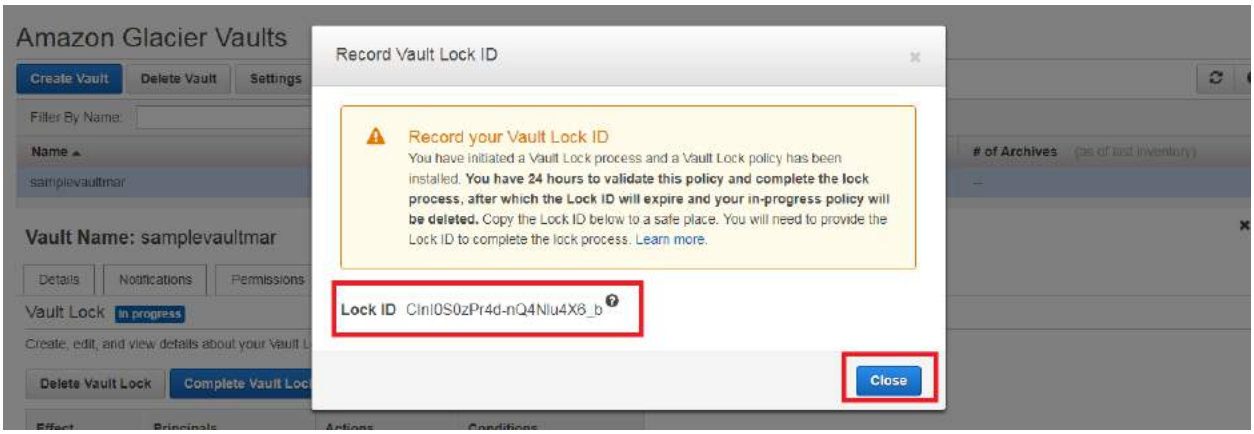


- Choose Allow Option, Provide * in Principals and All Glacier Actions as given below.

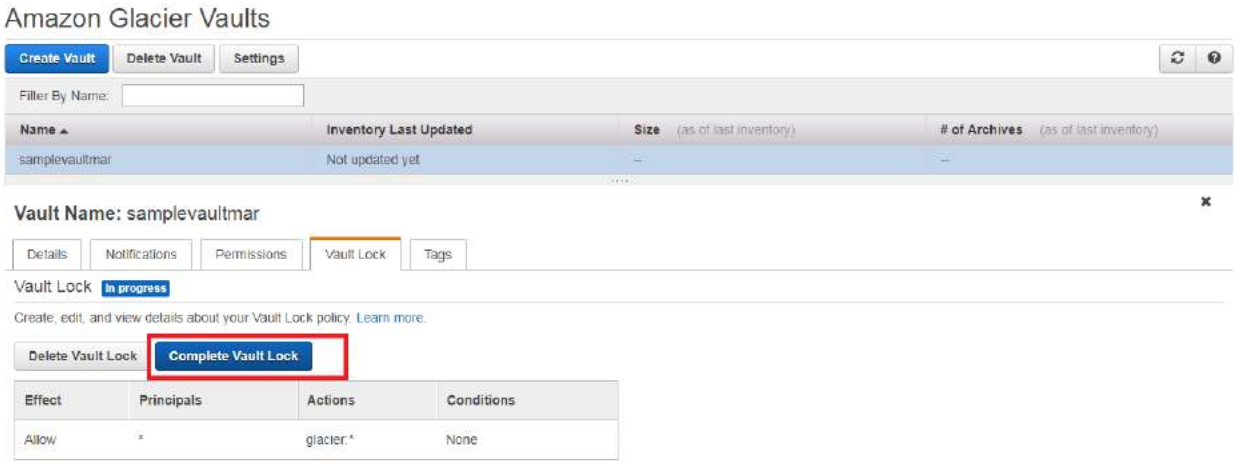


- Automatically, code will be generated if we give it in UI level.

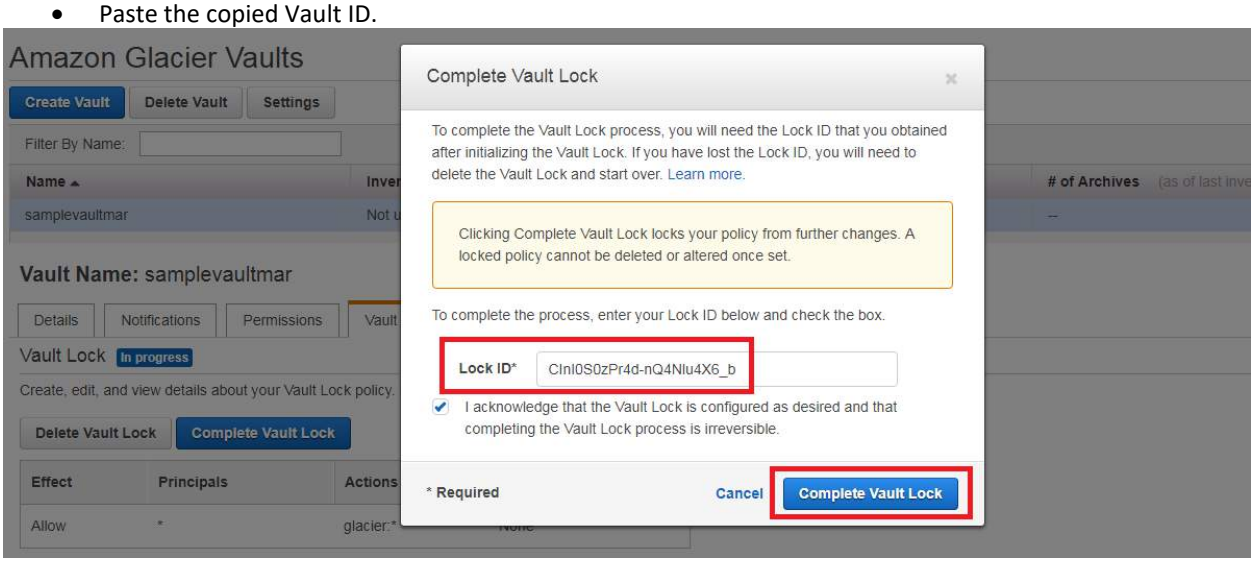
- Once you click on Initialize, Vault ID will be generated. Need to record this Vault ID in this created Vault.



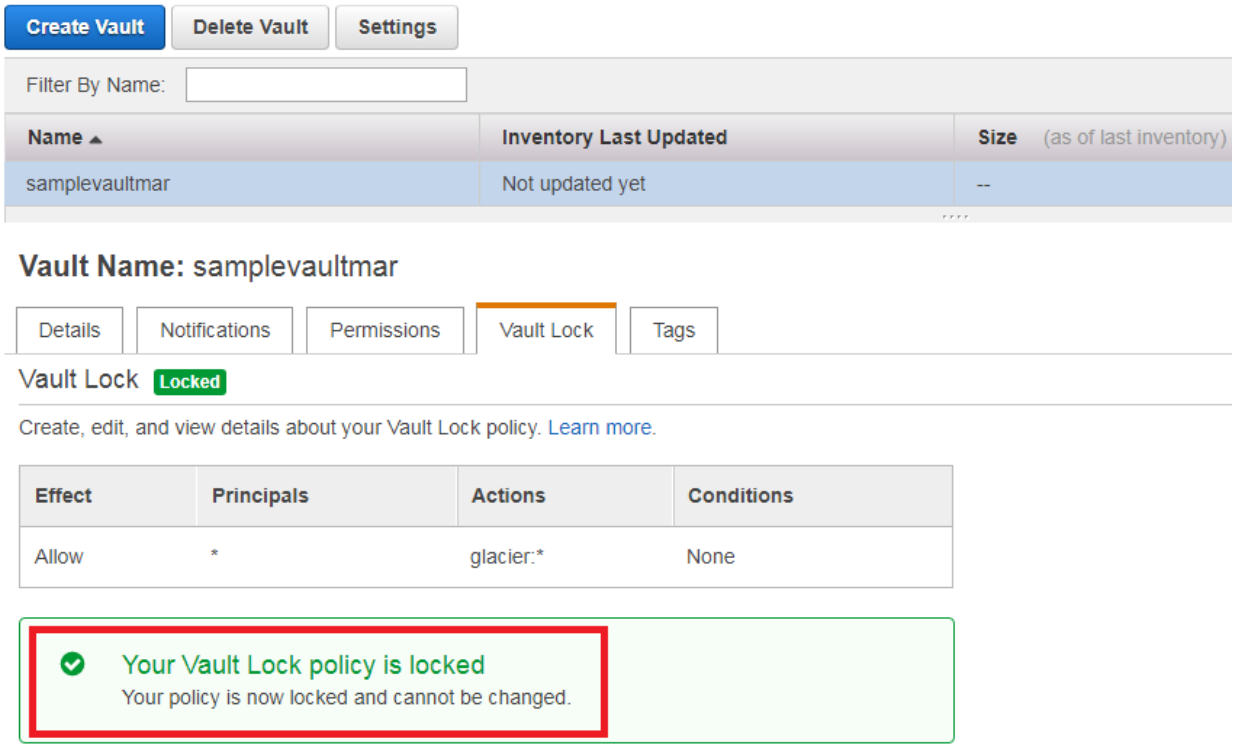
- Copy that Lock ID and click on Complete Vault Lock.



- Paste the copied Vault ID.

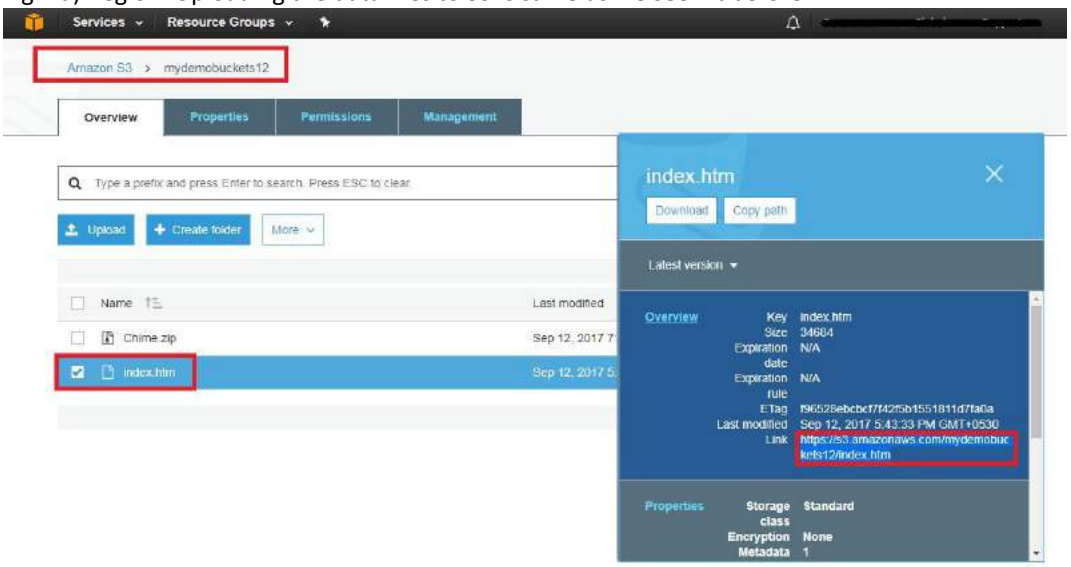


- Created Vault has been locked and now we would be able to do any actions on this created vault using CLI or Portal or SDK.

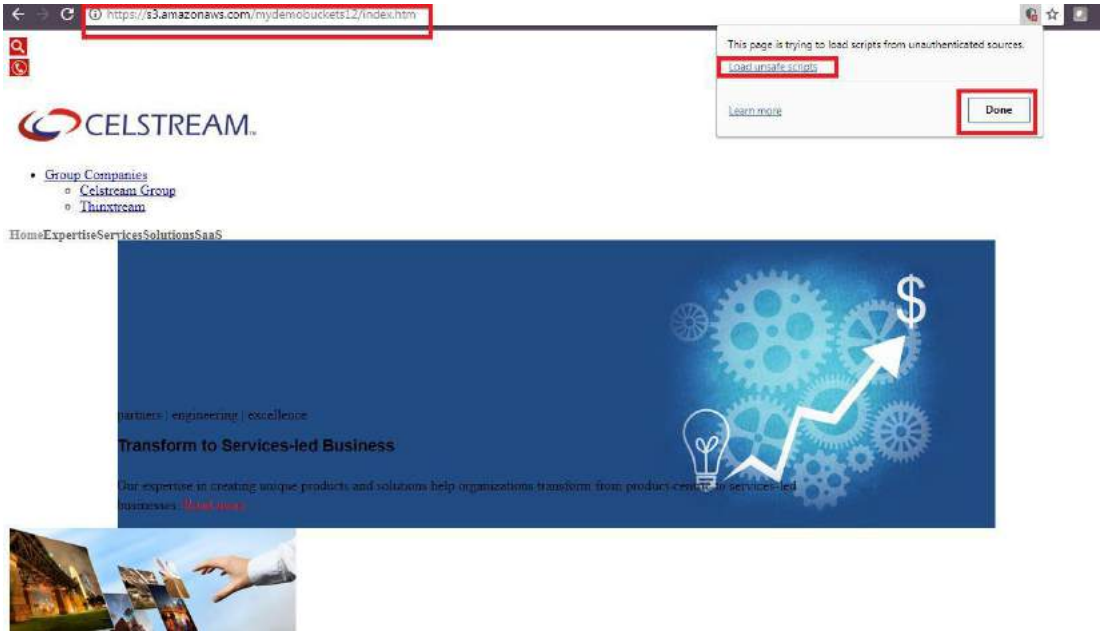


CloudFront:

- Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as.html, CSS, php, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately. If the content is not in that edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.
- Before we are getting started with CloudFront, we can upload one website in S3 Bucket in US-East (Virginia) Region. Uploading the data files to S3 is same as we seen it before.

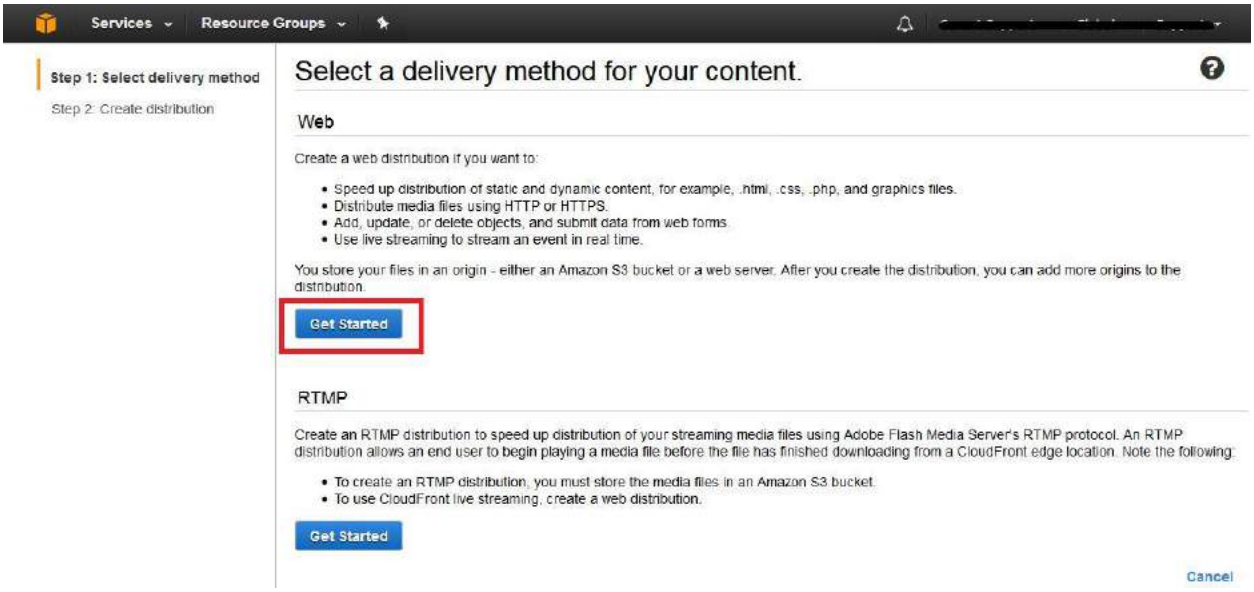


- Once you have been completed to upload the file, try to access it any of the browser by copying the URL. When you are accessing it from S3 bucket, browser is asking to load all the images separately and loading of this website would take some time since we are accessing it from Chennai.



- After you are clicking on to load scripts, a website would be displayed properly with all the contents on the same as like shown below. Hence, we could see some delay in accessing this sample mocked website from Chennai Region when this source file is available in Virginia region under S3 bucket.

- Now, we can get started with CloudFront by mapping this S3 bucket data and try to access the same in a browser by using CloudFront domain name. CloudFront providing two types to delivering the content to end users.
- **Web –** If you are using HTTP / HTTPS protocol or any kind of live streaming application, you can use Web method to deliver the content to end users.
- **RTMP –** It is used to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location.



- After choosing the Web, we need to select the source file in which you would like to distribute the content across the globe. It is also said to be Edge Locations and we can select either S3 Bucket or Web Server or ELB as an origin in which source file is available.
- If you would like to apply any patches or remove anything from the source file after creating a CloudFront distribution, that can be possible by selecting Get, Head, Options, Put, Post, Patch and Delete option under allowed HTTP methods as like shown below. Once you done this, if you make any changes in source file which is available in S3 bucket, it would be reflected to all edge locations which has been created using CloudFront.
- Apart from these, remaining values would be default values and proceed to create distribution.
- To deploy a CloudFront it would take around 15 to 20 minutes since it is distributing across the globe. Once the CloudFront has been created, the status would be changed to Deployed as like shown below.

Services Resource Groups

Step 1: Select delivery method

Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name: mydemobuckets12.s3.amazonaws.com

Origin Path: — Amazon S3 Buckets — mydemobuckets12.s3.amazonaws.com

Origin ID: S3-mydemobuckets12

Restrict Bucket Access: Yes / No

Origin Custom Headers: Header Name | Value

Default Cache Behavior Settings

Path Pattern: Default (*)

Viewer Protocol Policy: HTTP and HTTPS / Redirect HTTP to HTTPS / HTTPS Only

Allowed HTTP Methods: GET, HEAD / GET, HEAD, OPTIONS / GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Services Resource Groups

Distributions

What's New

Reports & Analytics

Cache Statistics

Monitoring and Alarms

Popular Objects

Top Referrers

Usage

Viewers

Private Content

How-to Guide

Origin Access Identity

CloudFront Distributions

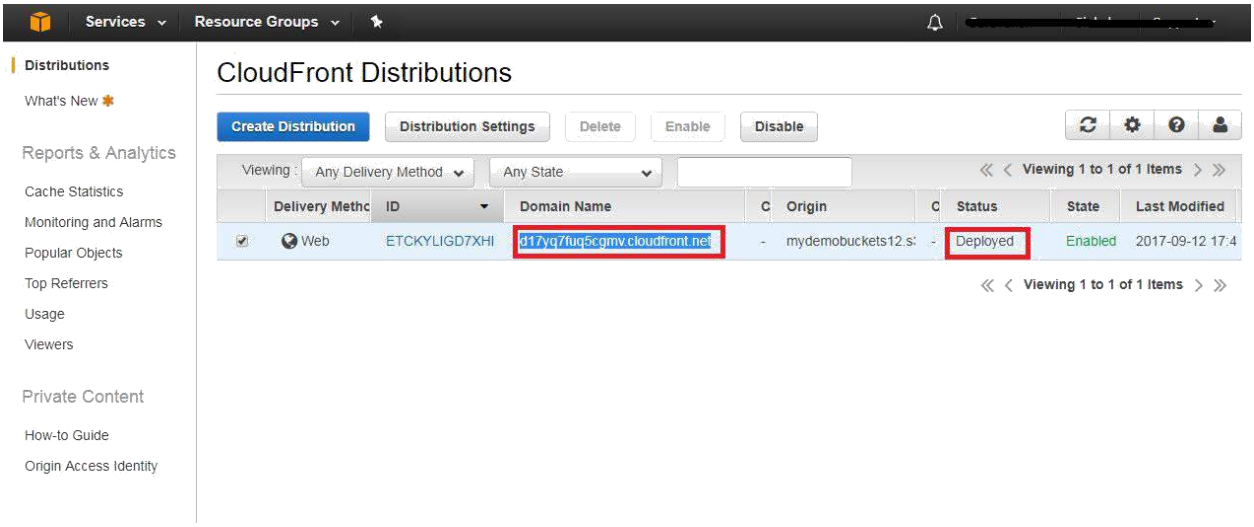
Create Distribution | Distribution Settings | Delete | Enable | Disable

Viewing: Any Delivery Method | Any State

Viewing 1 to 1 of 1 Items

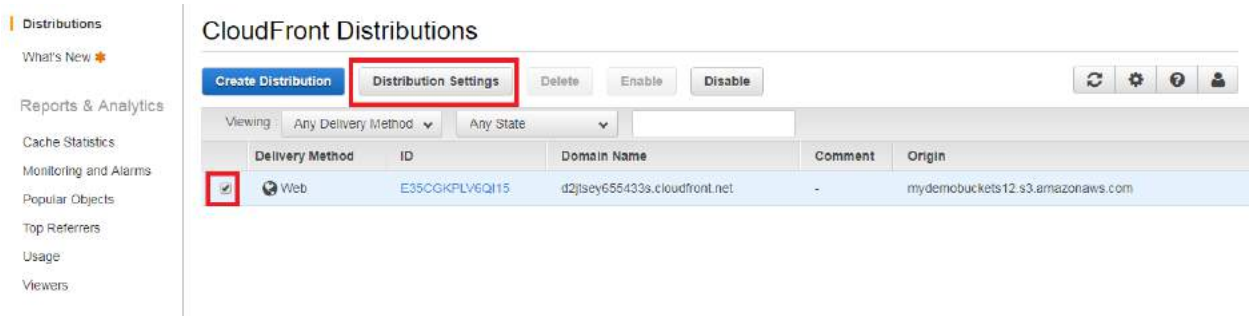
Delivery Methc	ID	Domain Name	C	Origin	C	Status	State	Last Modified
Web	ETCKYLIGD7XHI	d17yq7fuq5cgmv.cloudfront.net	-	mydemobuckets12.s:	-	In Progress	Enabled	2017-09-12 17:4

Viewing 1 to 1 of 1 Items

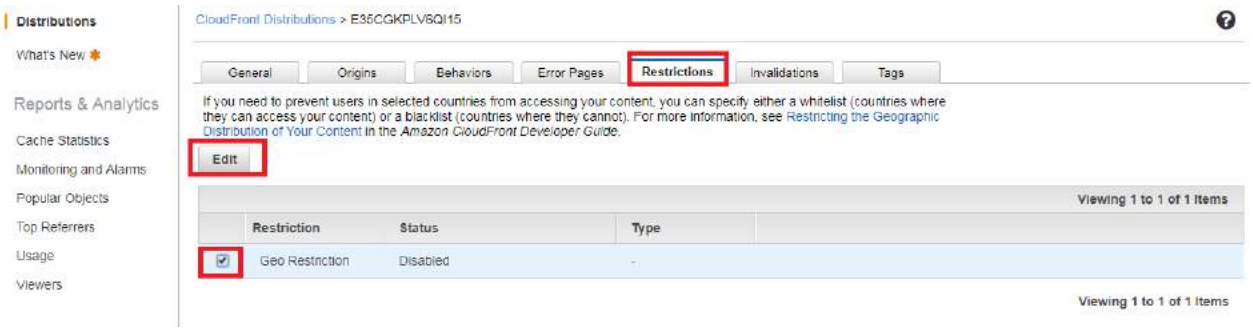


- Copy the domain name and access it in any of the browser to see the difference between accessing the website from S3 bucket and from CloudFront. You can able to see some low latency while accessing it from CloudFront.

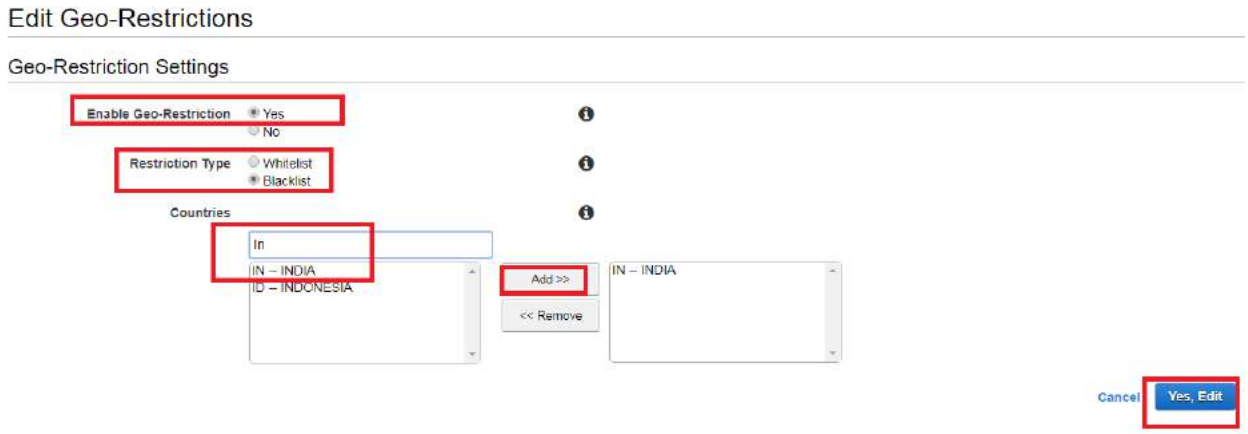
- If you want to restrict this access to any specific country, that could be possible by selecting the cloud front which you want to restrict and click on Distribution settings.



- Choose the restrictions option, click on Geo-Restriction and choose edit option.



- Click on Yes for enabling a Geo-Restriction and choose the type as blacklist. Then choose the country from which you want to restrict this access.



- Restriction to access this Cloud Front URL from India has been enabled successfully.

- Now, when we try to access it from India, it will throw an error message by AWS as like shown below.

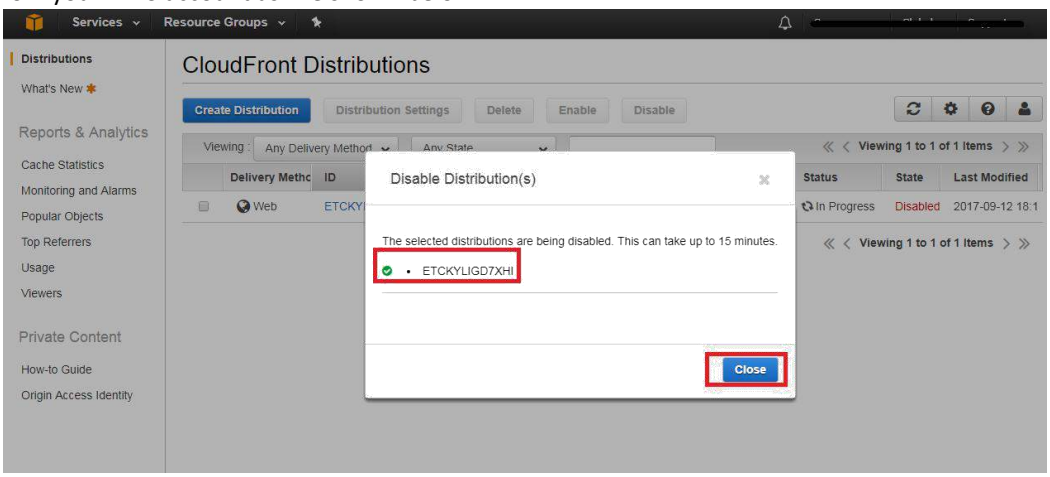
403 ERROR

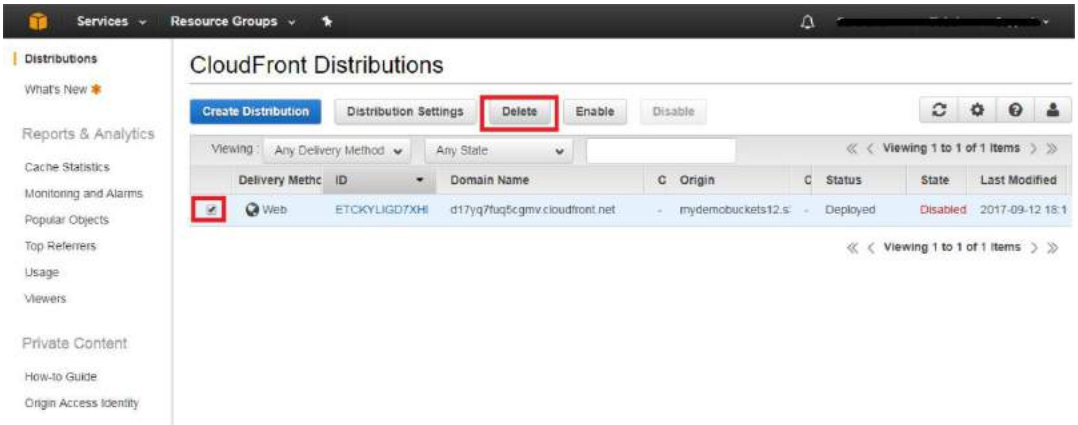
The request could not be satisfied.

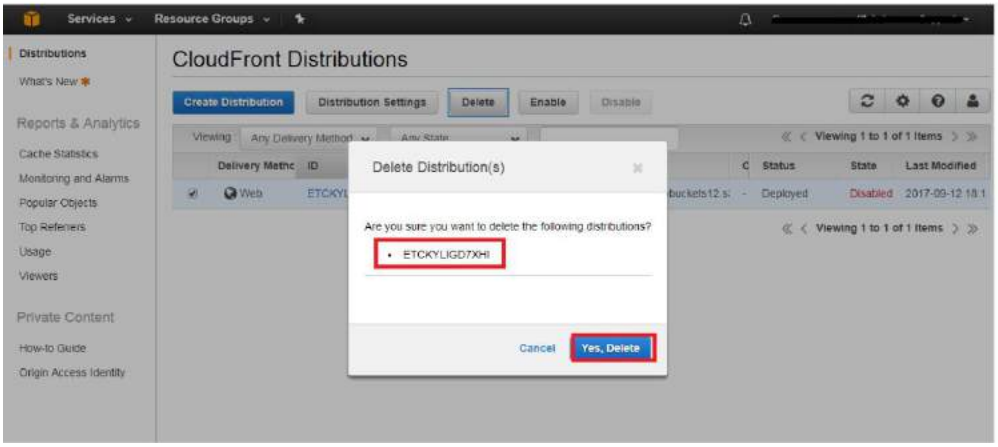
The Amazon CloudFront distribution is configured to block access from your country.

```
Generated by cloudfront (CloudFront)
Request ID: fmrhA95jIi3BDa8dVcICdCVtX1cvvFKOw0jzV2d_ReQdjzhVA9TOVQ==
```

- For deleting the created CloudFront, you need to disable it by selecting created CloudFront as like shown below. For disabling this CloudFront, it would take some time to disable since it would be turning off in all the edge location which is across the globe.
- Once disable is completed, select the CloudFront and click on Delete which would be completely removed from your AWS account as like shown below.





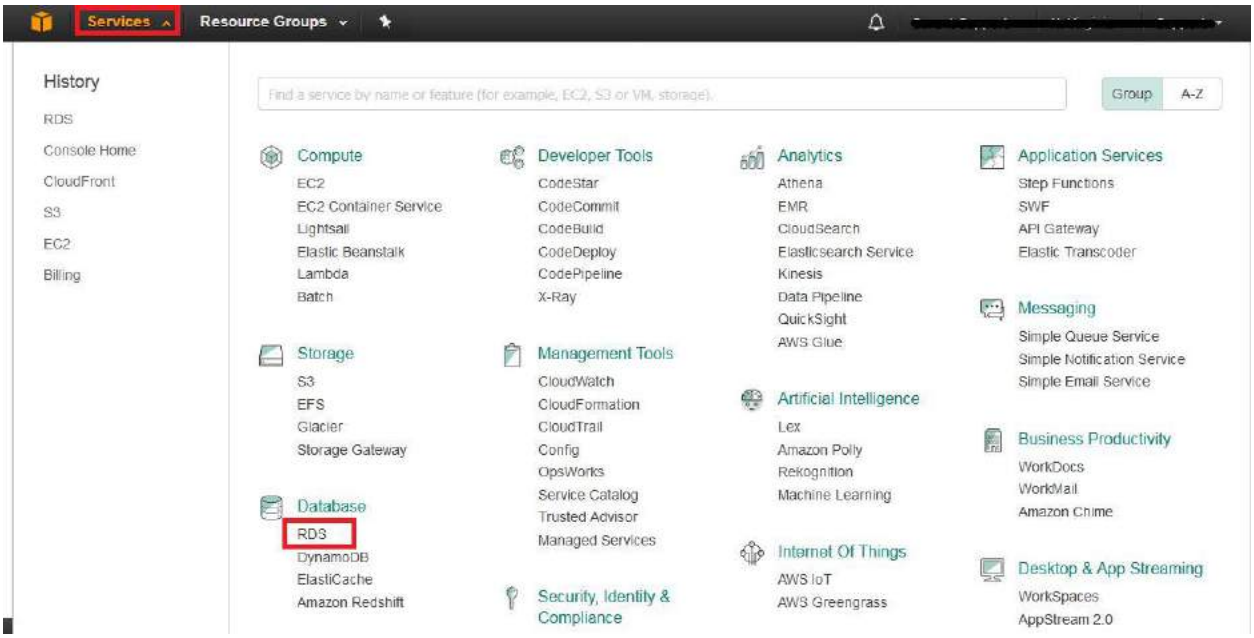


Advantages of Cloud Front:

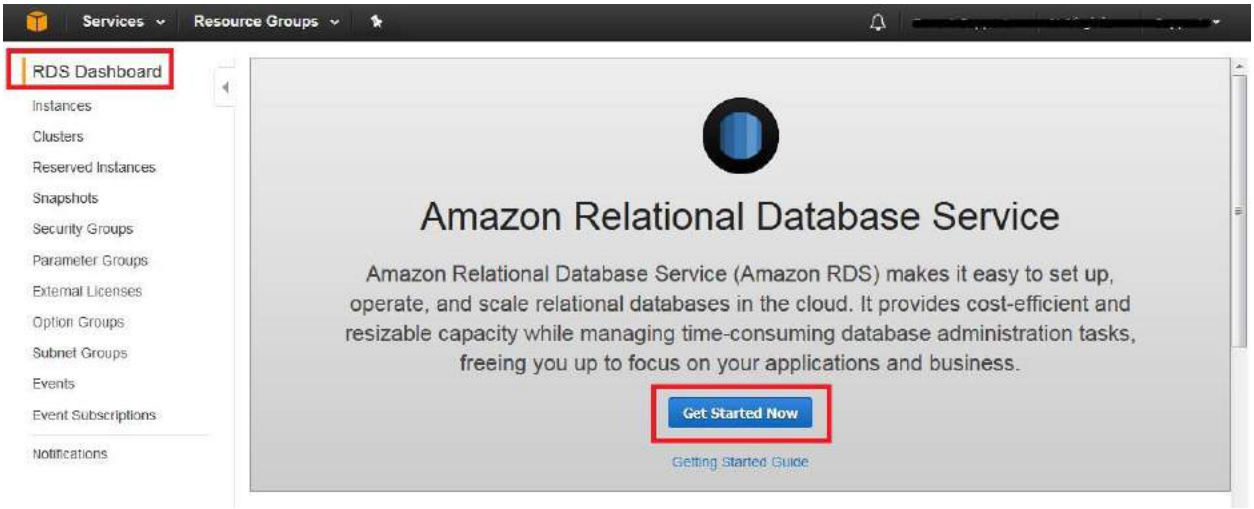
- With a minimal effort and cost, we could distribute our application across the globe as well as specific to regions.
- Cloud Front could be able to restrict an access to specific country.

RDS (Relational Database Service):

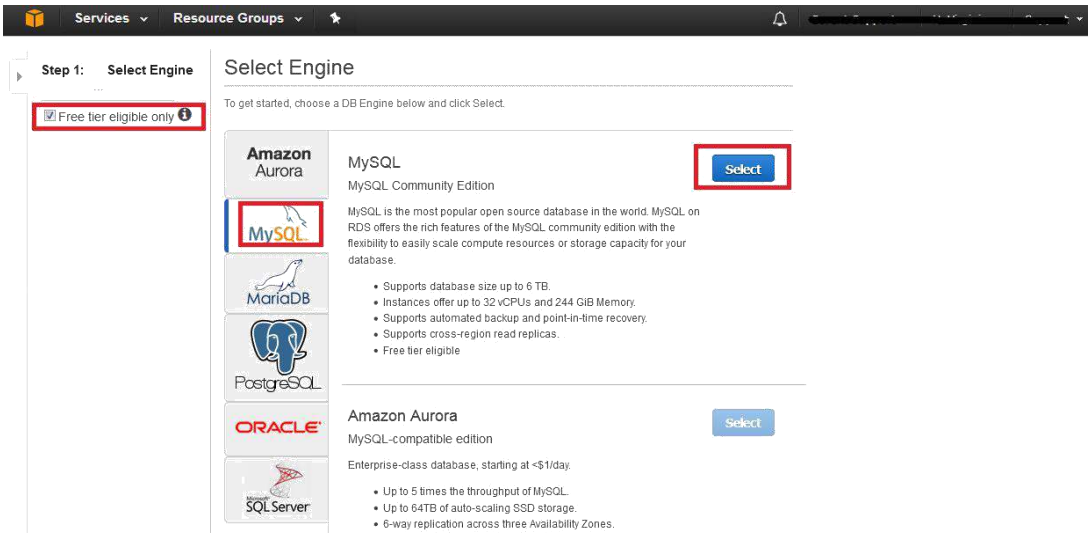
- RDS is a kind of PaaS which is available in AWS. If you are using two servers in your On-Premises like Application Server (Tomcat) and Database Server (MySQL). Consider, you are doing the migration of these two environments to AWS cloud and instead creating a new Database Server under EC2, I can able to use this RDS which is available in AWS.
- This would helpful to reduce the VM cost for Database and, RDS helps to take the back up of database automatically.
- Navigate to Services and Click on RDS under Database section as like shown below.



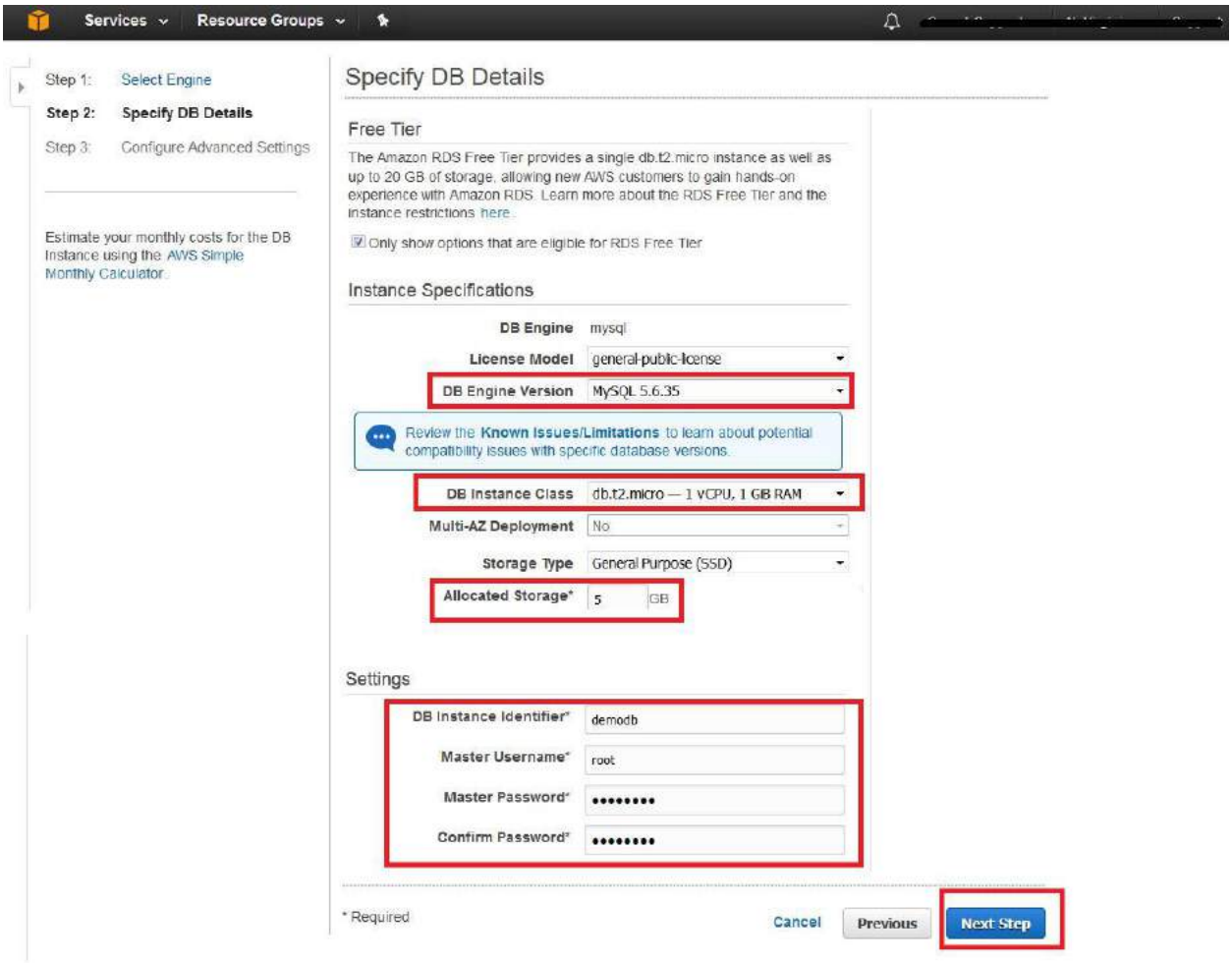
- Click on Get Started Now for creating a new RDS.



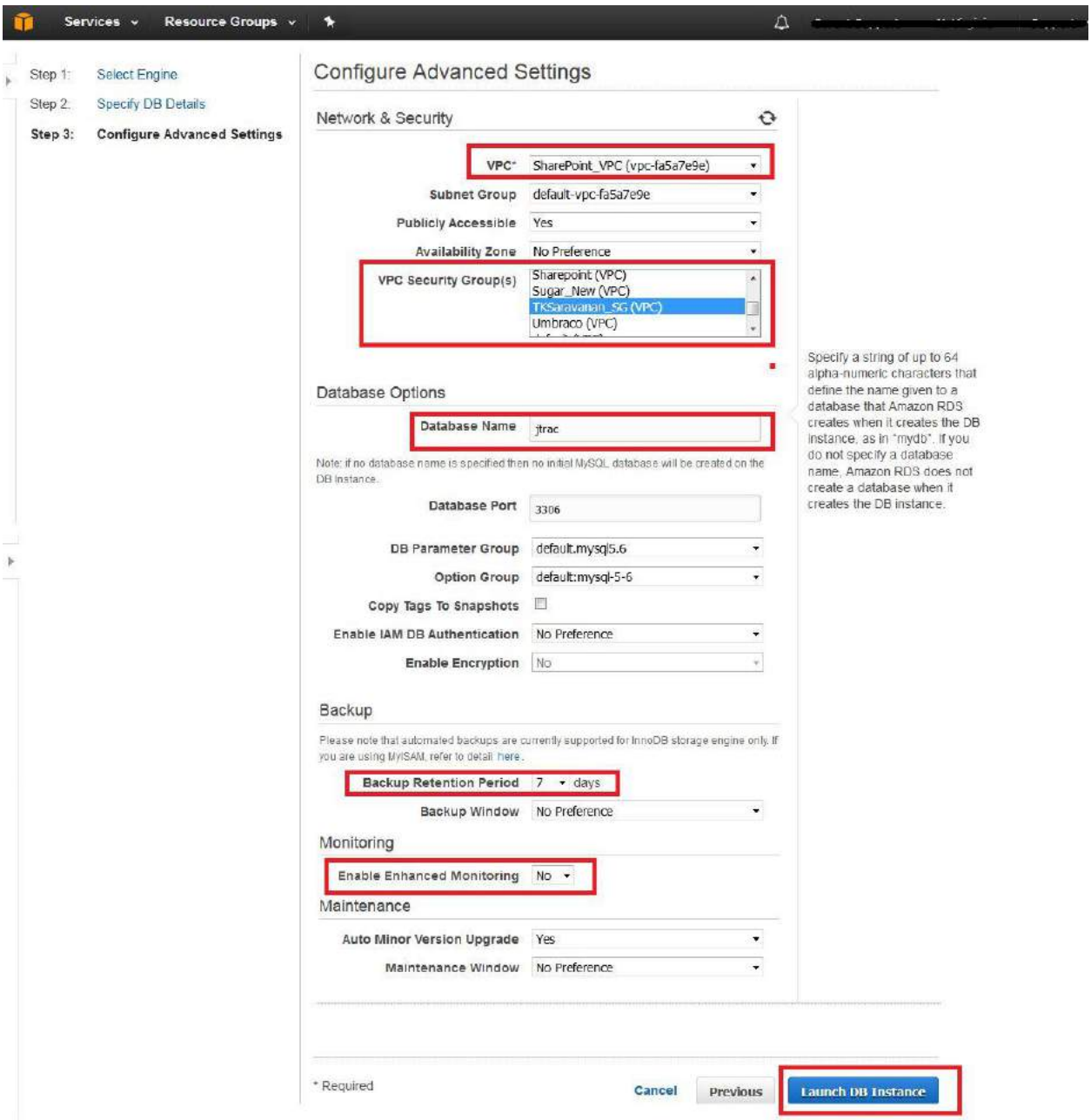
- As a free-tier, choose MySQL database and proceed with next screen.



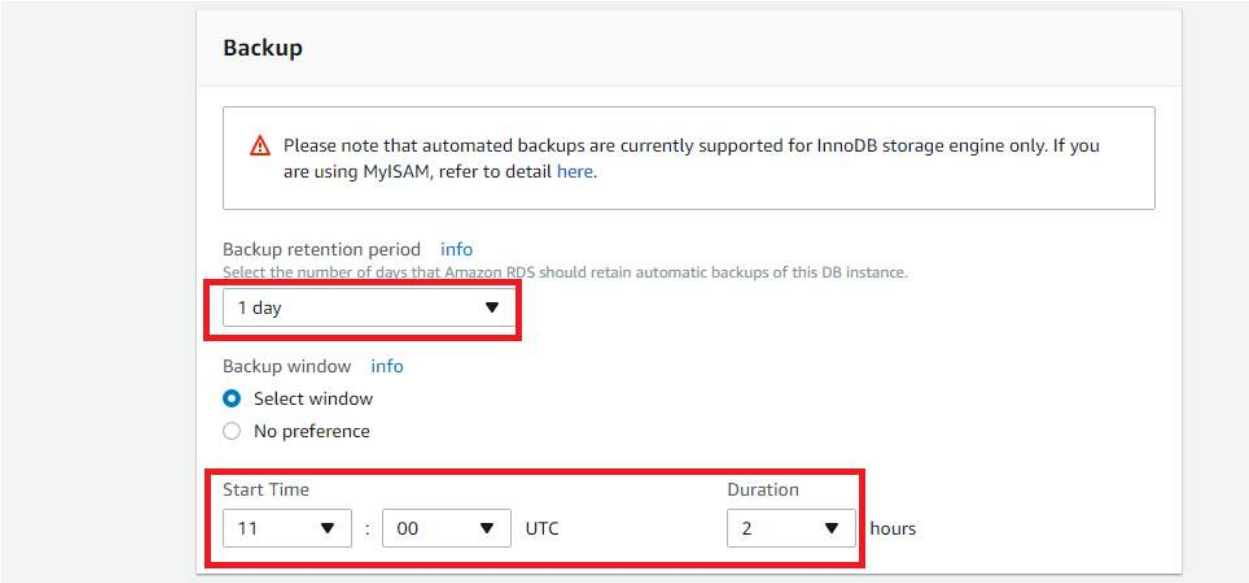
- Choose the MySQL version, configuration, provide RDS name, username & password of MySQL as like shown below and proceed with next. If required choose Multi-AZ deployment to access this MySQL in different Availability zone which is kind of failover set-up.



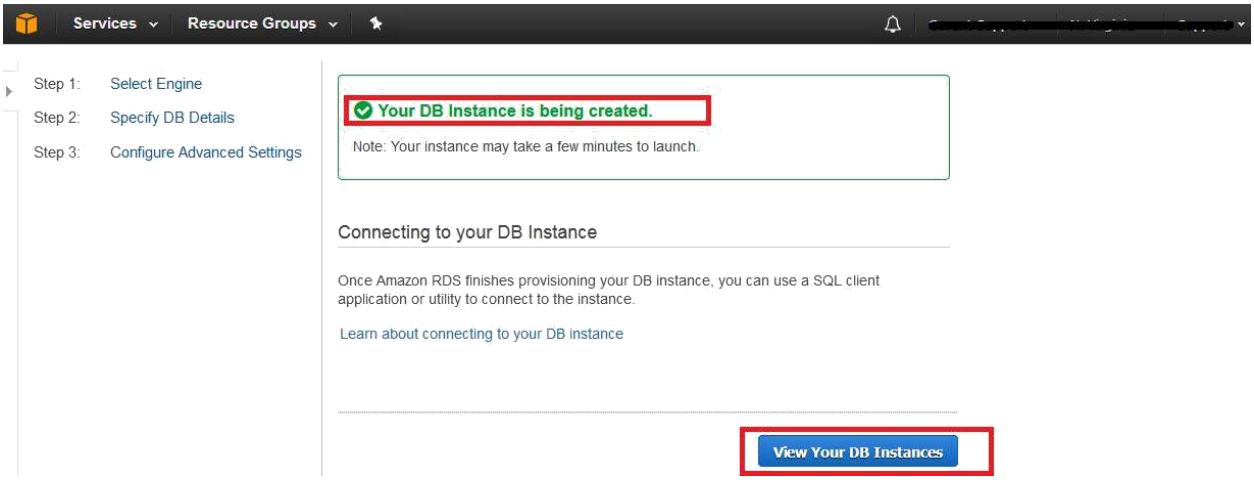
- We need to create this RDS under any VPC which has been created earlier, choose the Security Group which has 3306 MySQL port communicating globally, provide the database name based on your application, if required to take the backup, choose the frequency of the same and proceed with next steps as like shown below.
- Also, AWS providing an option to monitor the created RDS, so that you would be able to take an action immediately if any failover comes in.
- Finally click on Launch DB instances.



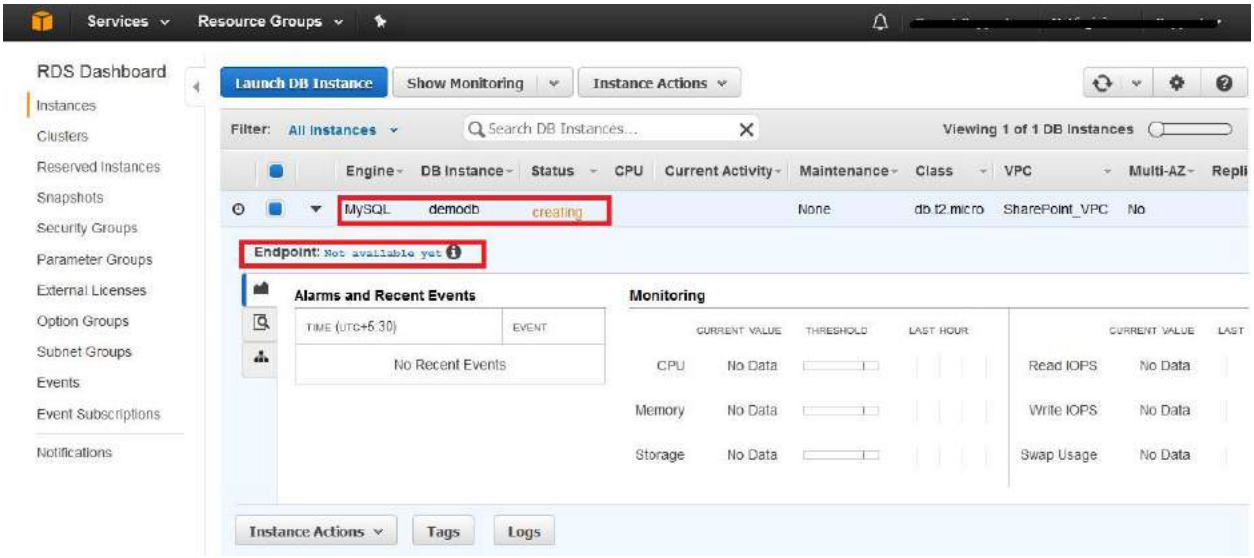
- If Database Backup is being required, you could specify the days and time which is being required to take a backup.



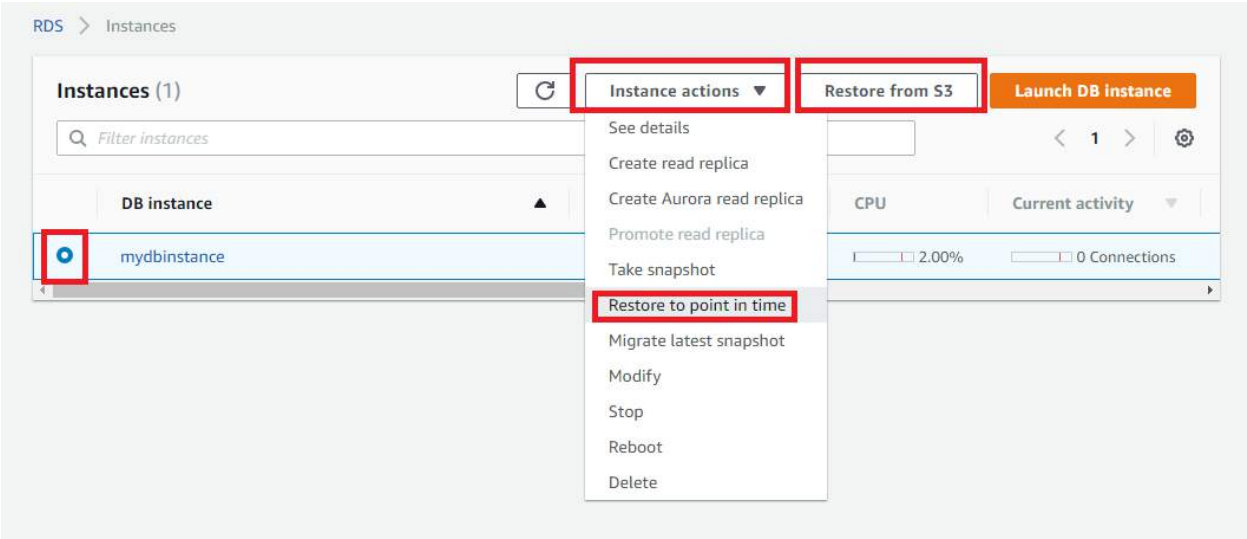
- Click on View your DB instances.



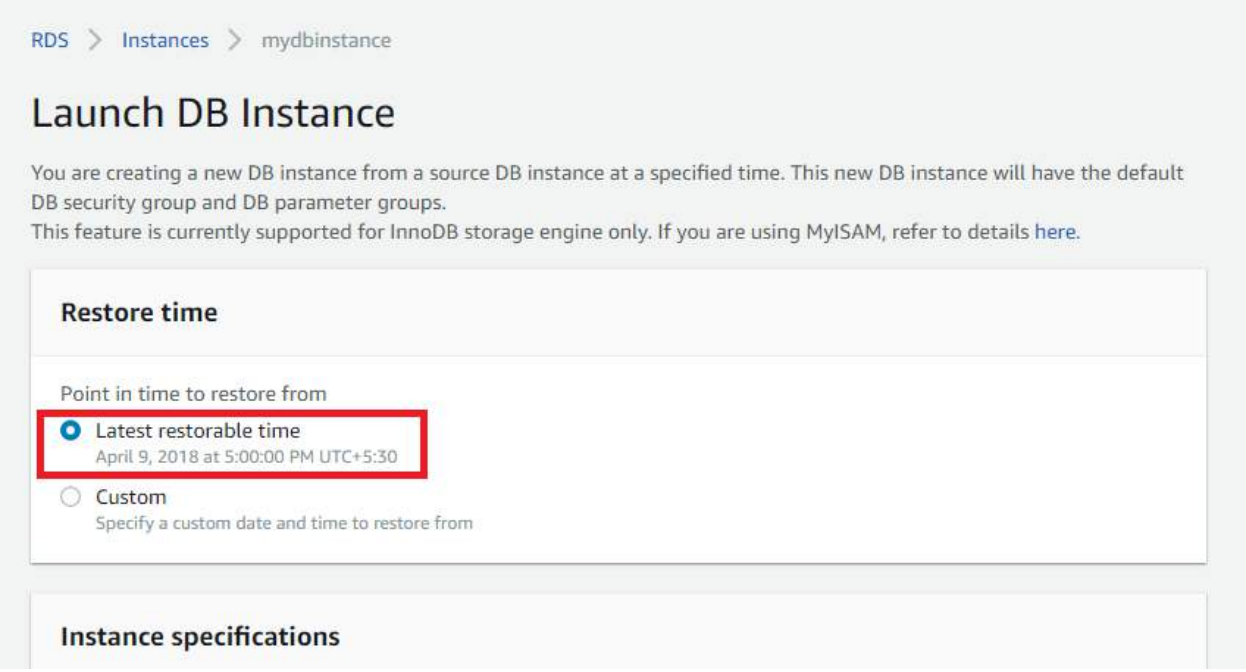
- MySQL is being created a generally it would take around 10 minutes of time.



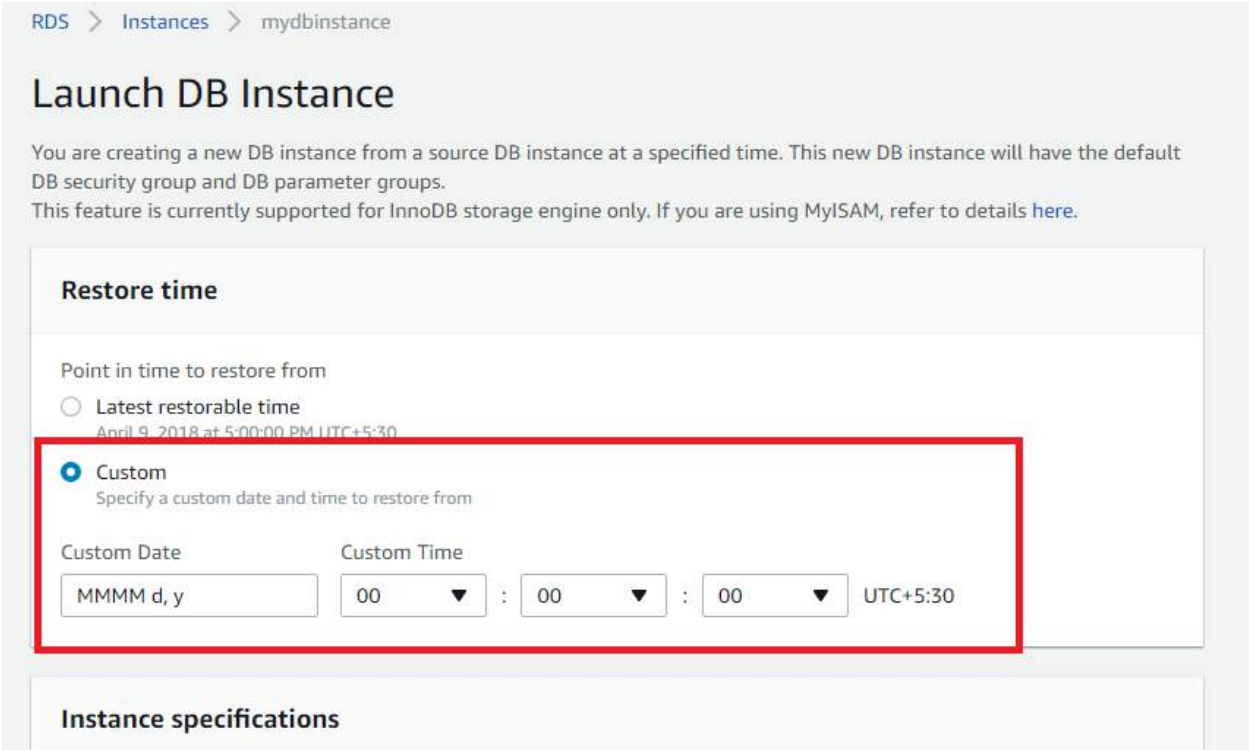
- After creation of this RDS Database, backup activity is being initiated and the same could be restored any given point of time. To do a restore of RDS, select an RDS instance which you want to take the back up and click on instance actions. Then choose to restore to point in time option.
- If you want to restore it from S3, same could be possible by providing the bucket name of the dump file it has been saved.



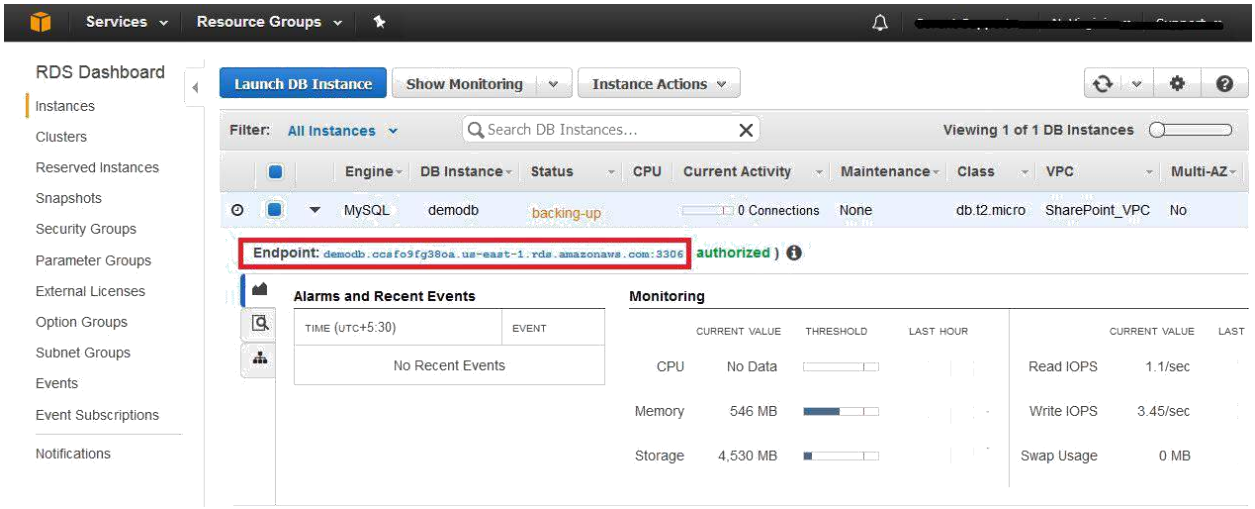
- There are two options to restore a database instance. Either you could provide the latest backup which has been taken.



- Or, custom time of the database instance backup could be specified by mentioning date and time. Followed by, new RDS instance would be created with the complete data of your existing database.

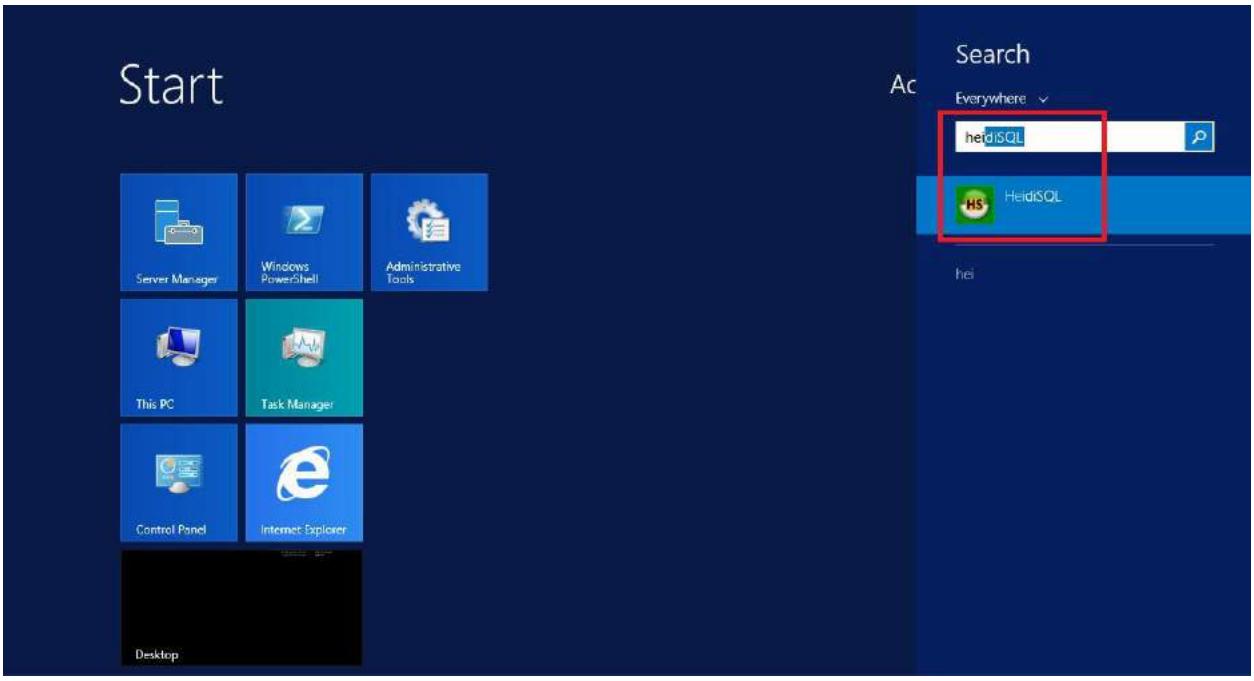


- Once the MySQL has been created, we need to copy this Endpoint URL which would be acting as an identity for this created MySQL in RDS.
- If we are using the MySQL in any of the server, we would be using IP address of the database server to configure inside the application in respective places. Since we are using this MySQL as a PaaS, we need to configure through Endpoint URL which is available in AWS.
- Make a note of this Endpoint URL, DB name, Username and the password of created MySQL, so that it would be easier to configure in application files.

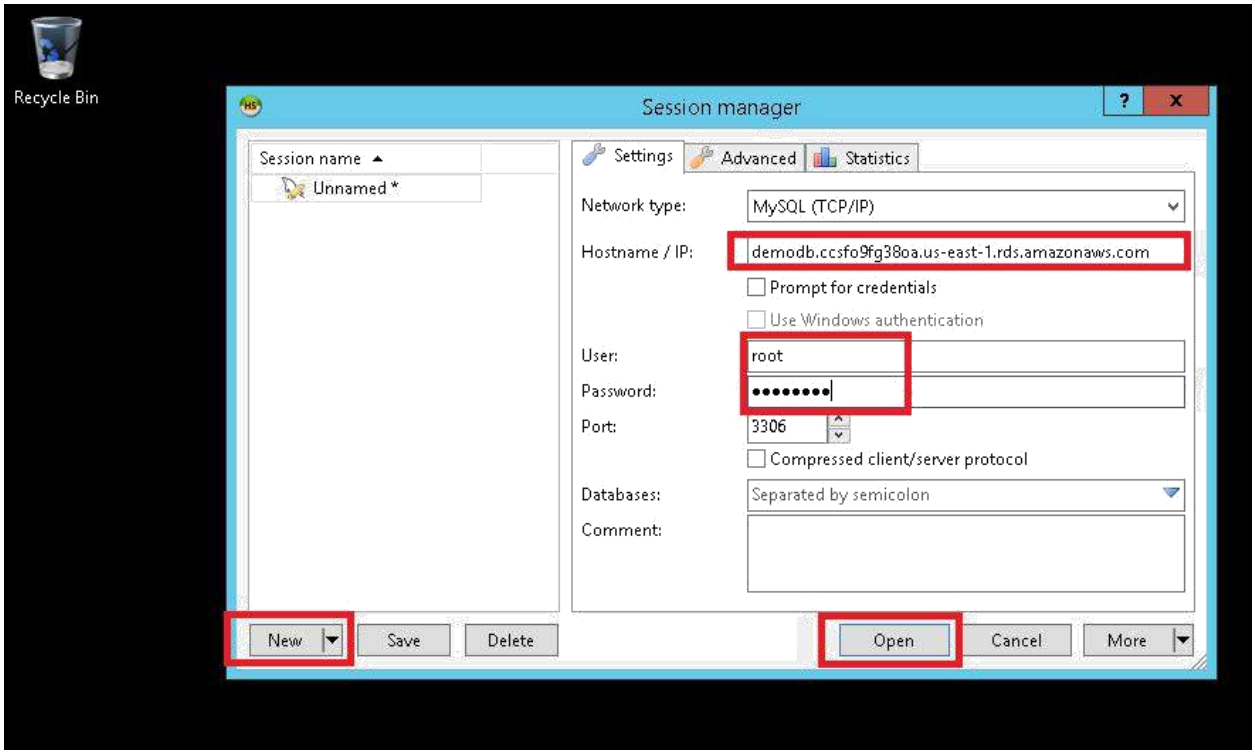


- Login to any of the server / your local PC to download and install HeidiSQL which is a kind of Client tool to connect to the created MySQL. Since this MySQL is running as a PaaS, we do not have an option to connect it without using any client tool. It is like taking a RDP of Windows Server using Remote Desktop Connection tool.
- HeidiSQL can be downloaded by clicking on below link.

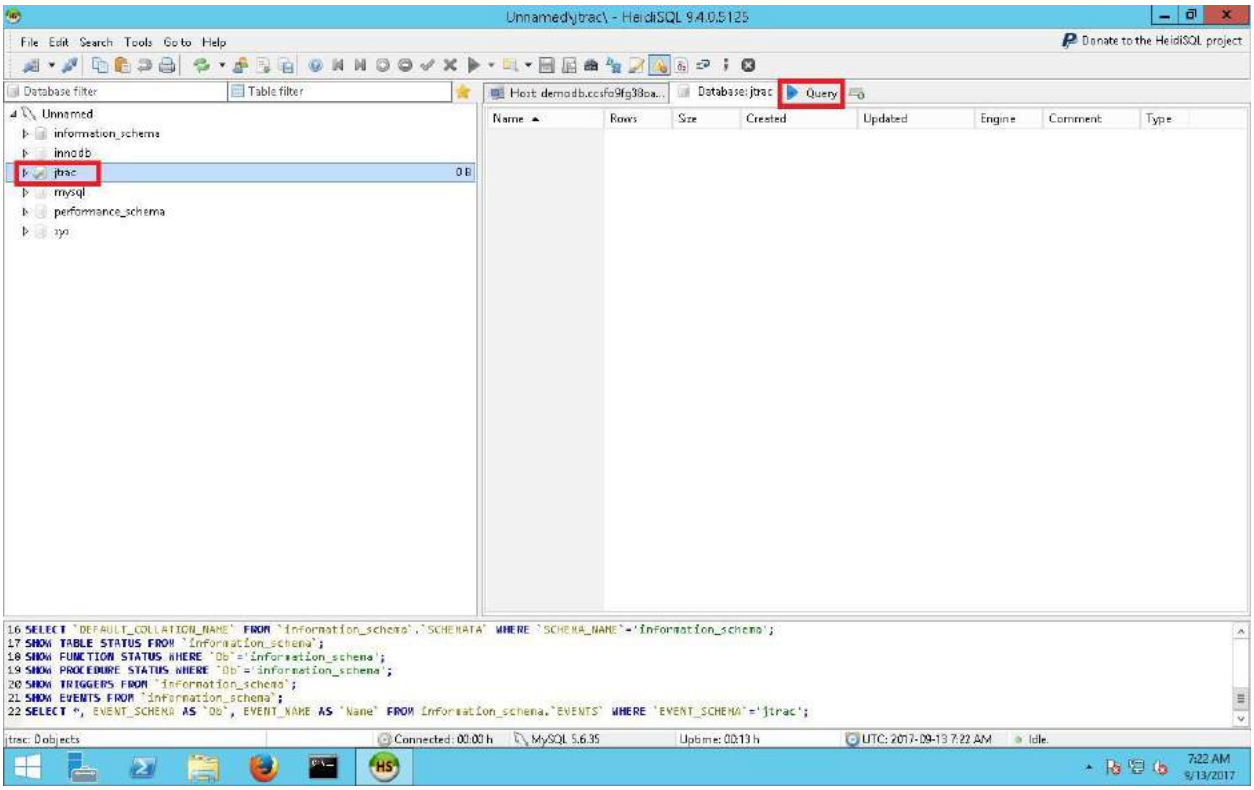
- https://www.heidisql.com/installers/HeidiSQL_9.4.0.5125_Setup.exe
- Once download gets completed, proceed to install the same as like installing general EXE applications. After installation, login to this HeidiSQL by clicking on Start Programs as like shown below.



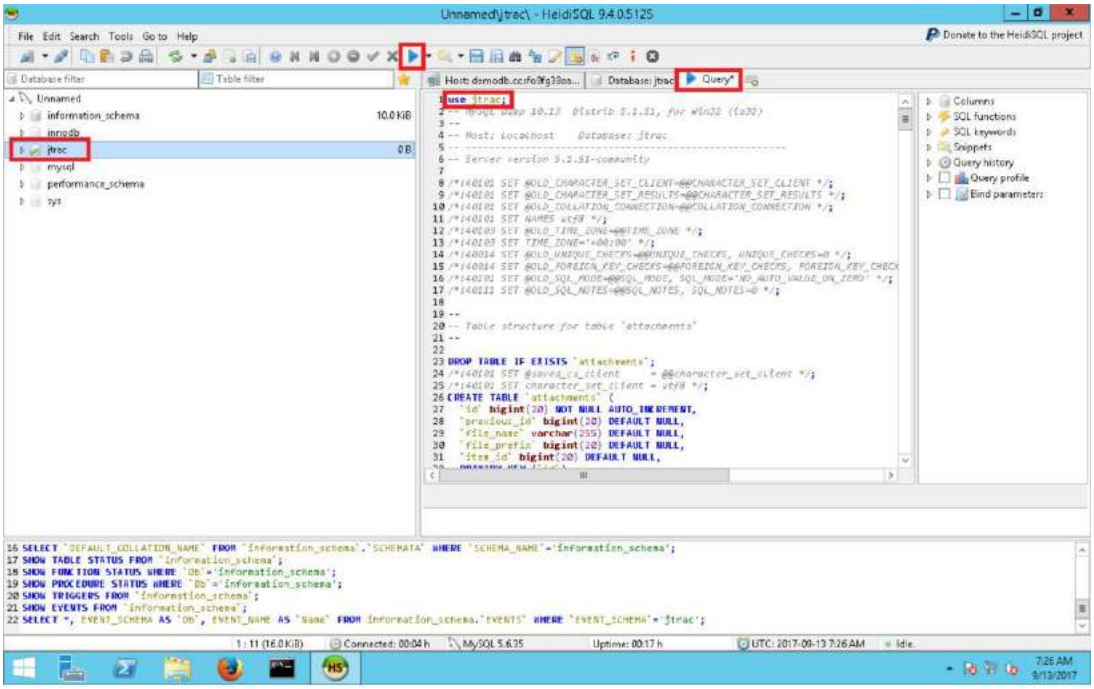
- Choose New, Provide Endpoint URL, username, password and the port number of created MySQL and click on Open.

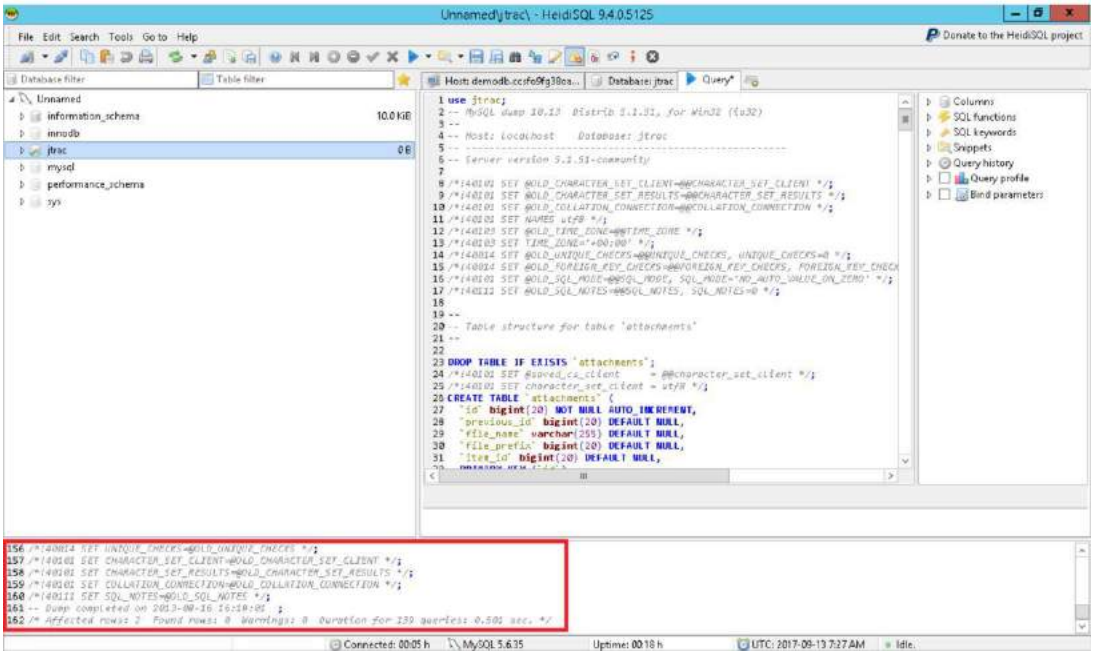


- After you opened the MySQL, you would be able to view the list of default databases which are available along with your created database.

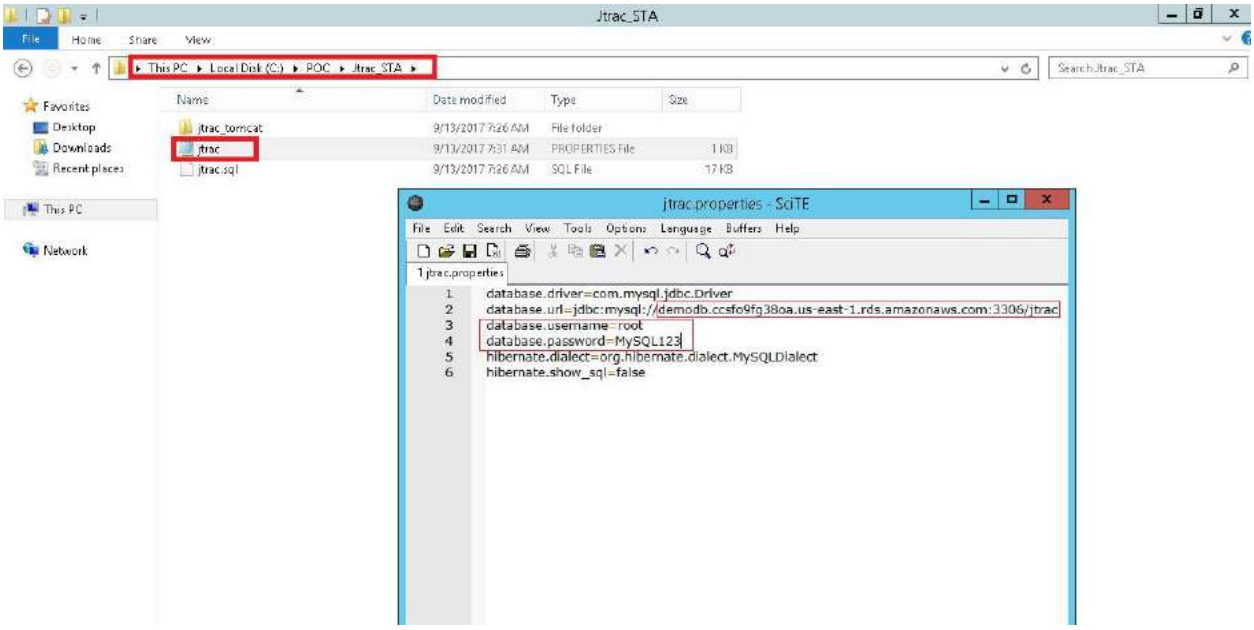


- We need to import jtrac.sql dump file under jtrac databases showing above. Jtrac.sql file can be found in the below given bundle after you are downloading it. Suggesting you download this bundle in any of the server or your local PC which would be acting as an Application server and extract the same. JTrac is a Java based application and we would require Java 1.6.24 version to deploy this in any server / PC.
- https://drive.google.com/file/d/1o0xpBF_qqFuLJ-qq-VwuiUjfoBX7Ht4q/view?usp=sharing
- Copy the complete Query by opening jtrac.sql file and paste it in HeidiSQL for importing the tables into the created MySQL RDS.

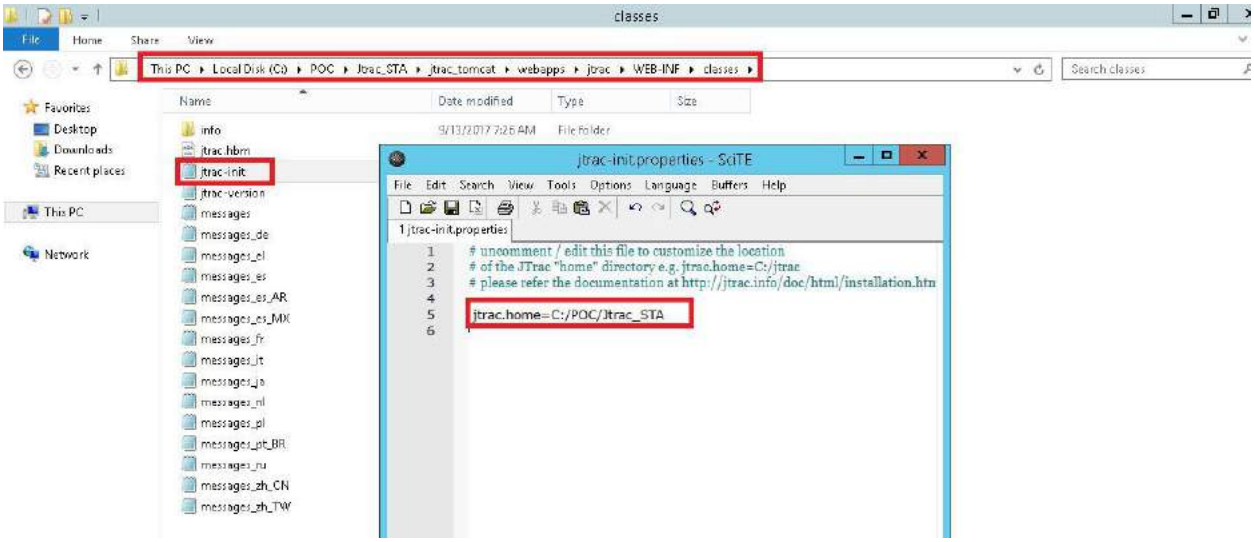




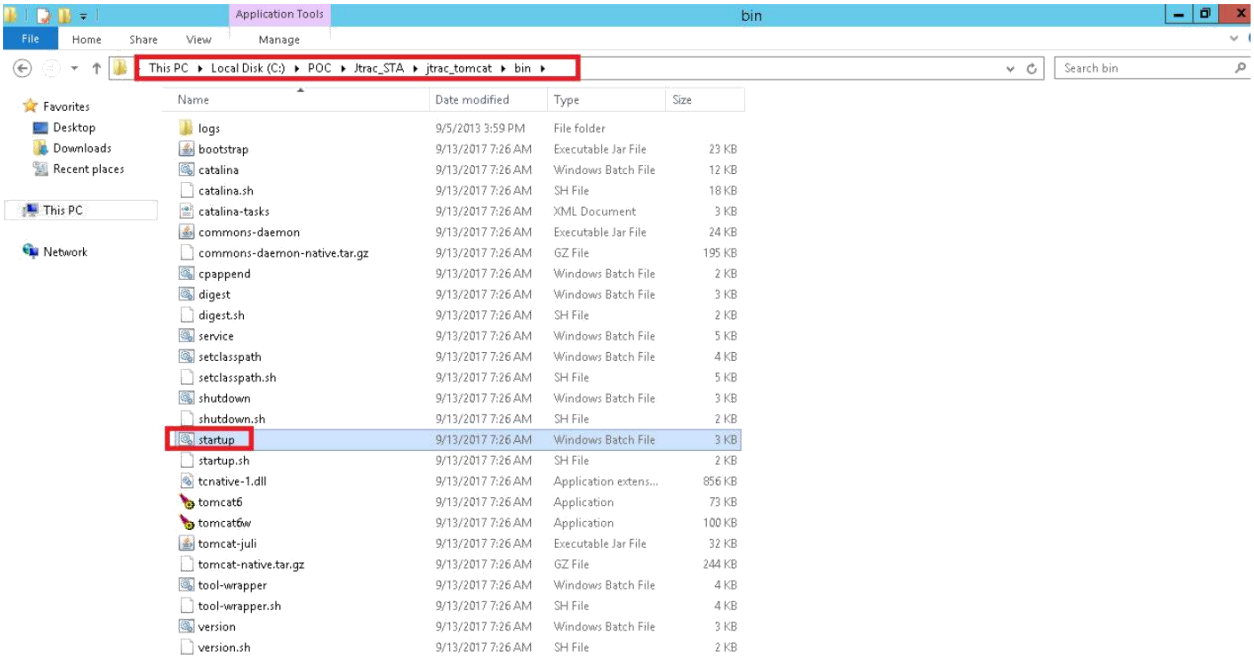
- Open Jtrac.Properties file which could be found in the bundle which you have downloaded and provide the MySQL details on the same as like shown below.

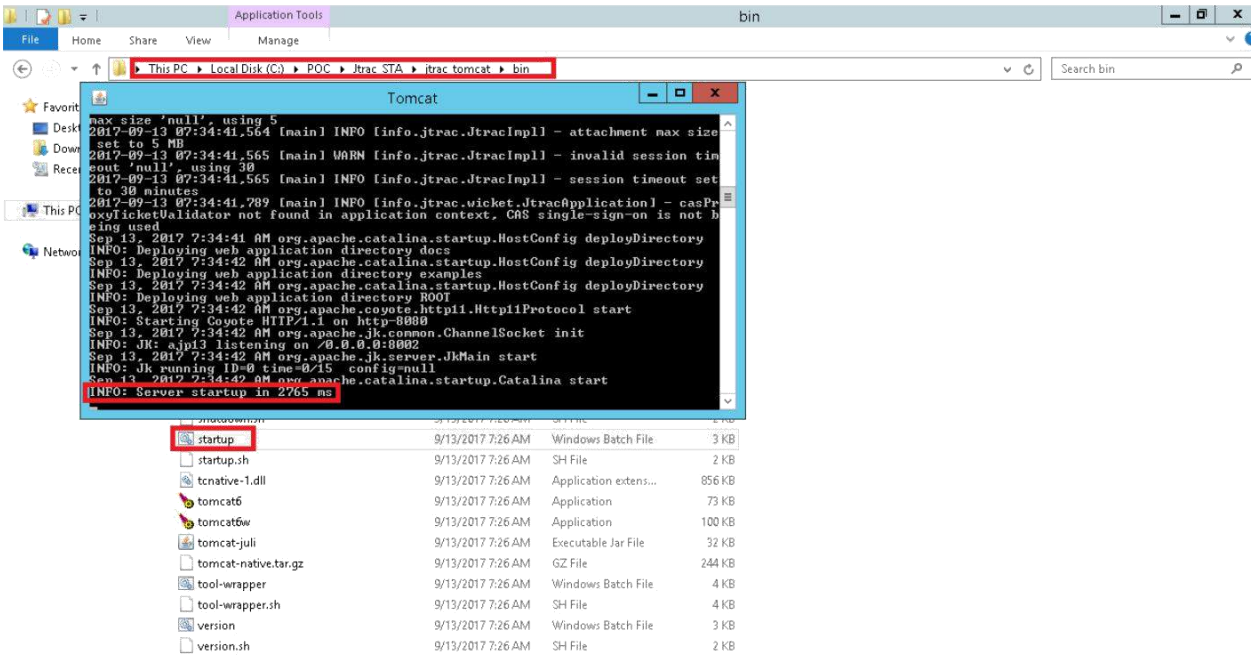


- Provide the Path location of this Jtrac.Properties file in jtrac-init.properties file which is shown below.

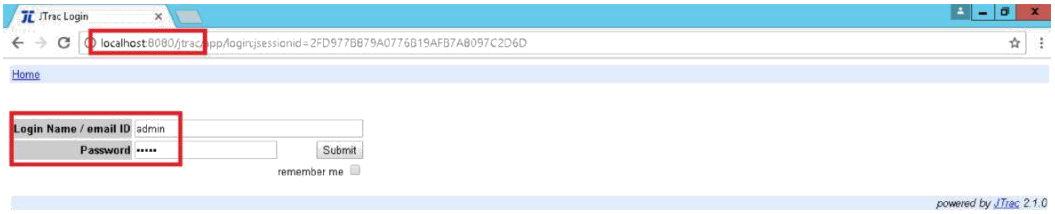


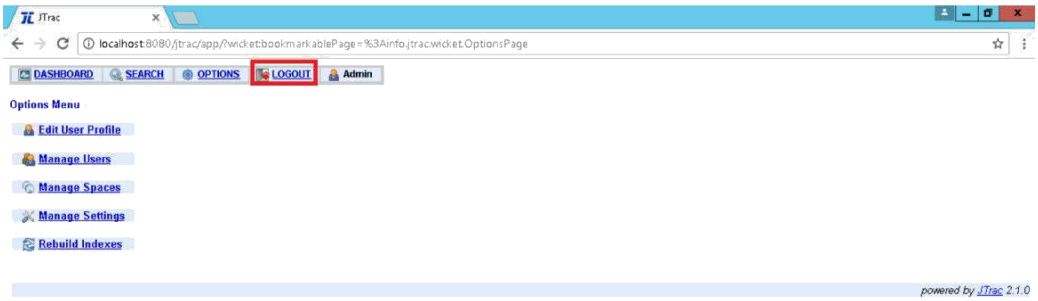
- Navigate to bin folder of Tomcat, start the same to ensure application is working fine as expected.



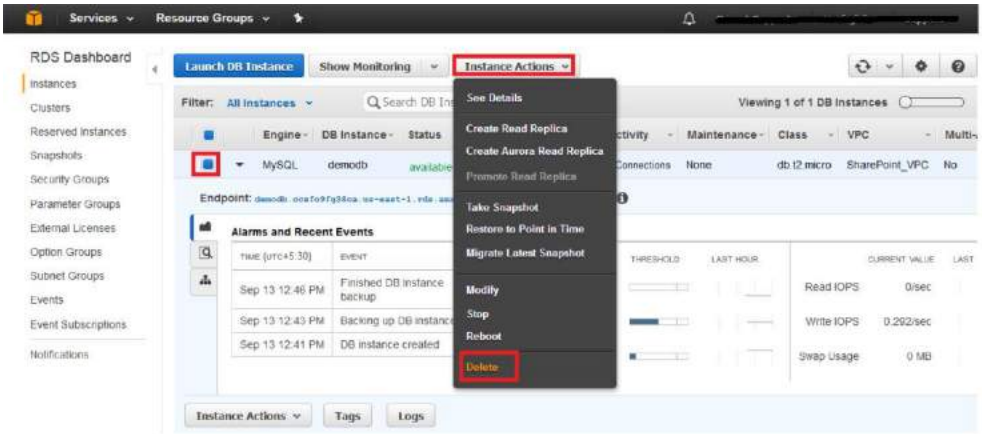


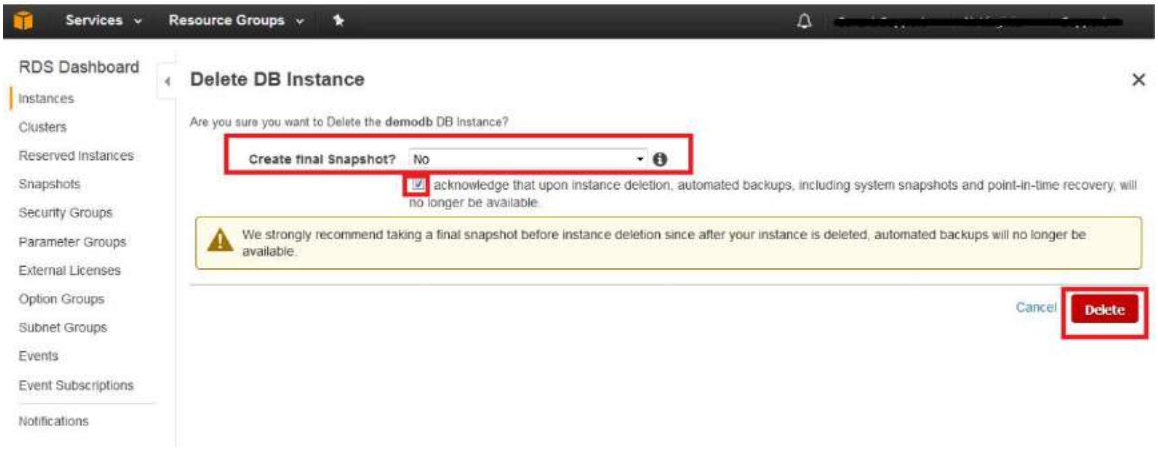
- Since this Jtrac application is accessing in 8080 protocol, access the same by providing localhost:8080/jtrac as like shown below. Login to the application by providing username and password as admin. Hence, application is accessible without any database server and by using the RDS service which is available in AWS portal.





- To delete the created RDS, select the MySQL which you have been created, navigate to instance actions and choose delete option. Choose No option in creation of Snapshot and confirm to delete the created RDS as like shown below.





Advantages of RDS:

- Instead of creating a new Instance and installing the respective databases (MySQL / MS-SQL / Oracle, etc.), we could easily create a new RDS instance with a minimal amount of time.
- This database maintained in RDS is safe and secured when compared to maintaining in an instance.
- This RDS could be able to take the backup automatically and the same could be restored any given point of time.
- To replicate the master and slave concept, AWS RDS providing an option to choose a replica set up which would be created in two different zones. If Master goes down, slave will be the master automatically.

Redshift:

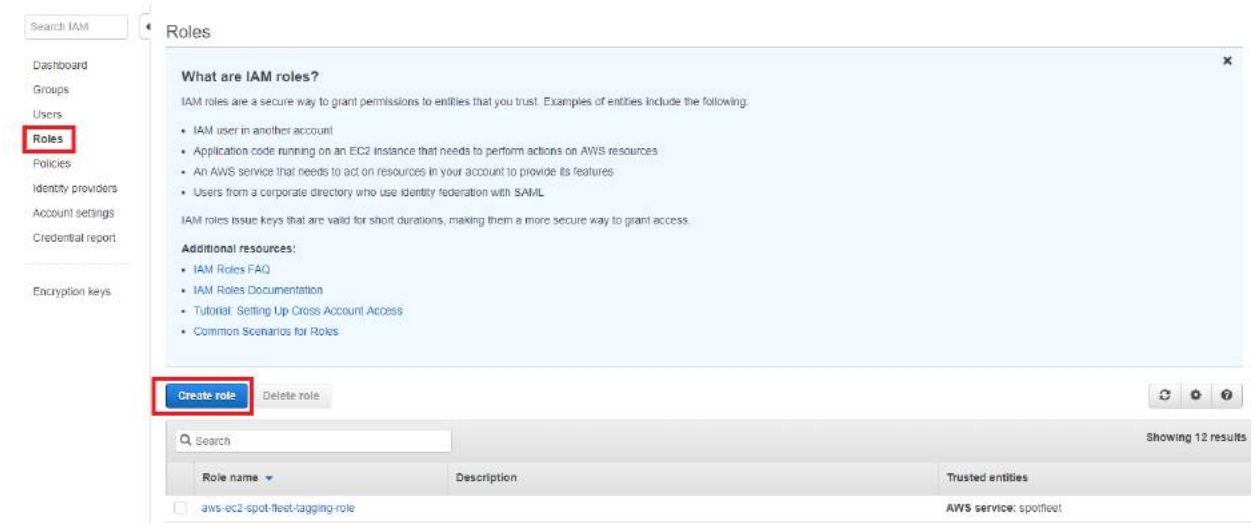
- Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools.
- It is optimized for datasets ranging from a few hundred gigabytes to a petabyte or more and costs less than $1,000 per terabyte per year, a tenth the cost of most traditional data warehousing solutions.
- There are six steps to be followed for verifying the Redshift.
- Step 1: Set Up Prerequisites
- Step 2: Create an IAM Role
- Step 3: Launch a Sample Amazon Redshift Cluster
- Step 4: Authorize Access to the Cluster
- Step 5: Connect to the Sample Cluster
- Step 6: Load Sample Data from Amazon S3

Step 1:

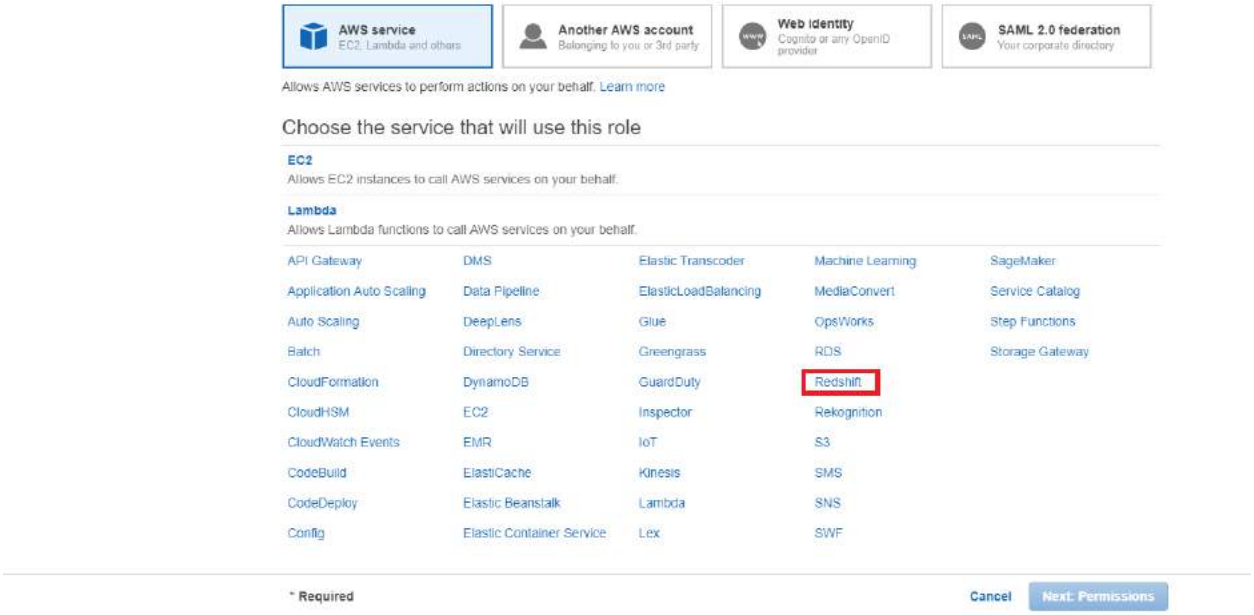
- We need to install SQL Workbench for connecting Redshift and the same could be downloaded from below given URL.
- https://drive.google.com/file/d/1QPS_EL4U5aw_bu_FauMaYJDvfuWyIq1j/view?usp=sharing
- After downloading, extract this zip file and place it in any location.
- Followed by, proceed to download the connectivity jar file from below given URL.
- https://drive.google.com/file/d/1BgTxsBlWQoGiUN9Vgq8-eSq9z2S-d_mQ/view?usp=sharing
- While opening this Workbench you supposed to choose the Redshift driver and you could refer upcoming screenshots.

Step 2:

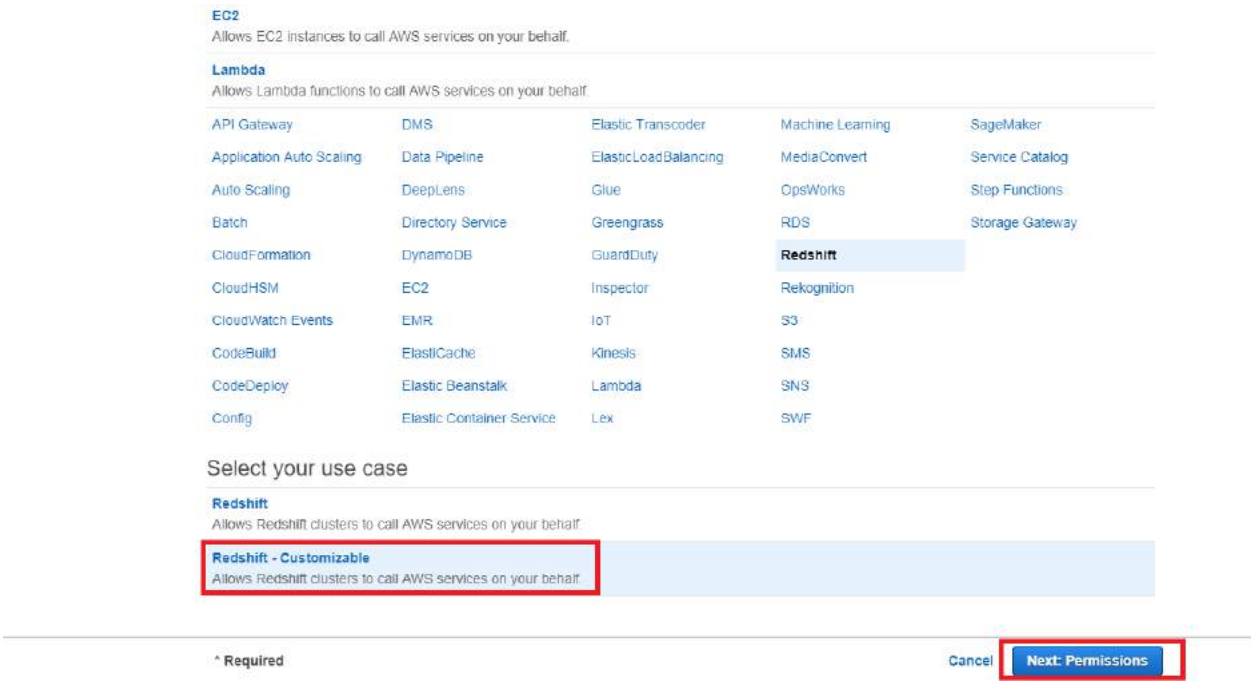
- Create a new IAM User and IAM role. To create a new IAM user, you could refer the IAM topic in the same document. Please make sure you have been chosen Redshift and S3 full access is being selected for this IAM user.
- For creating an IAM role, navigate to IAM options, choose an option as Roles, and click on Create Role.



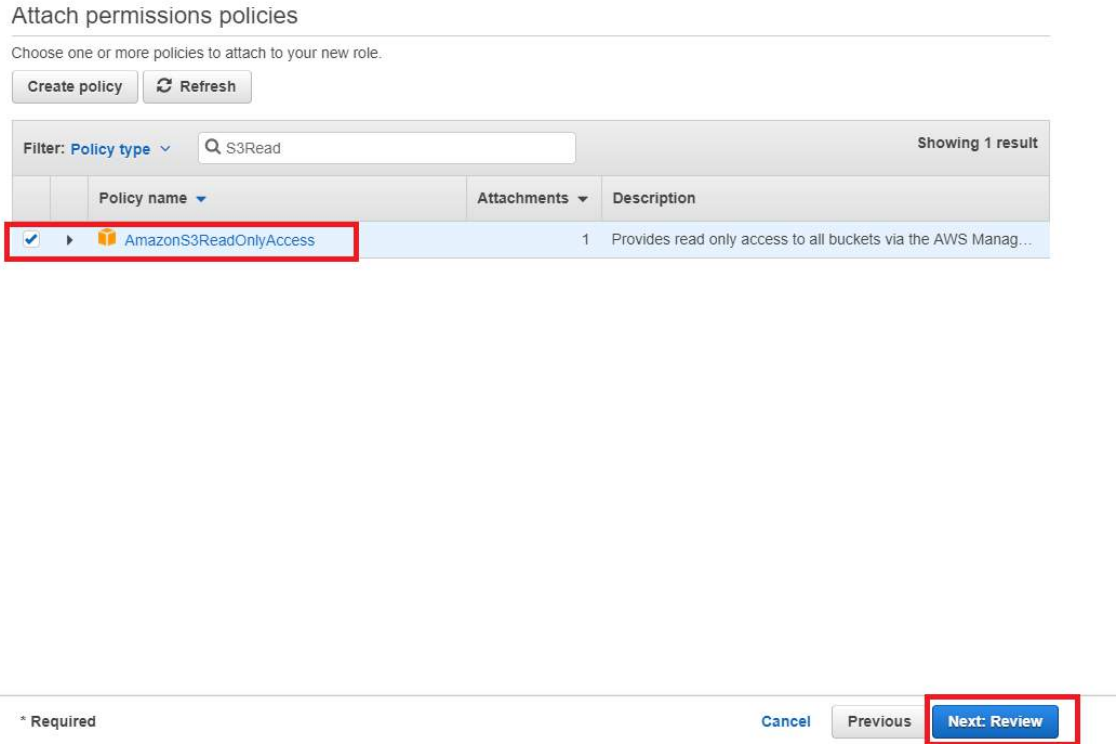
- Choose an Option as Redshift.



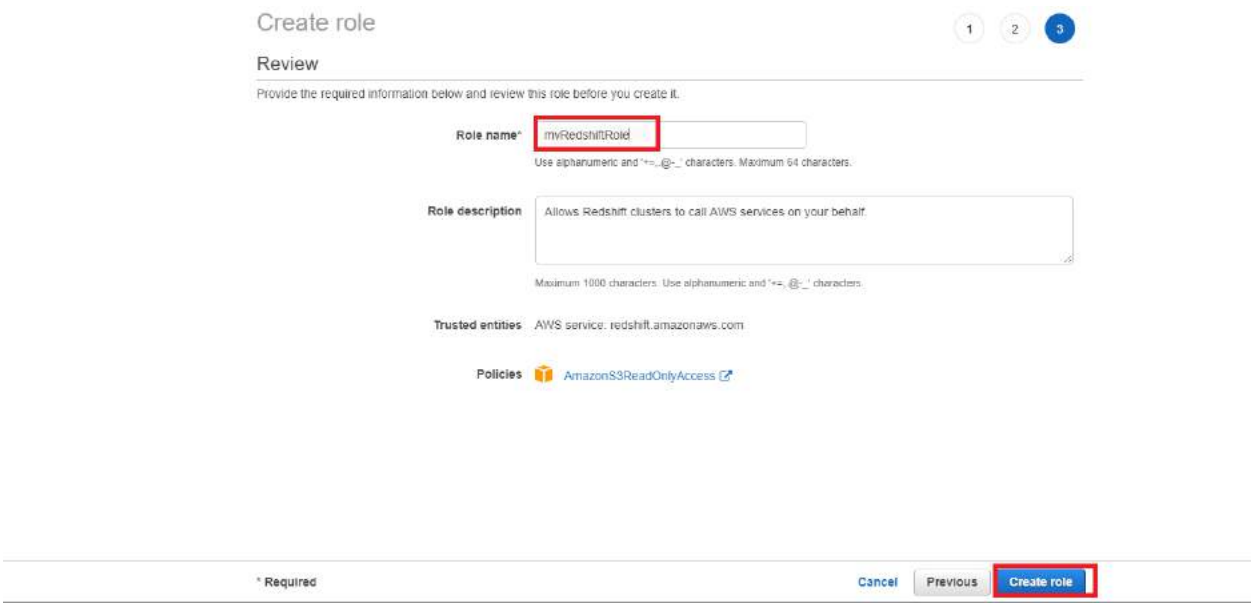
- Click on Redshift Customizable option.



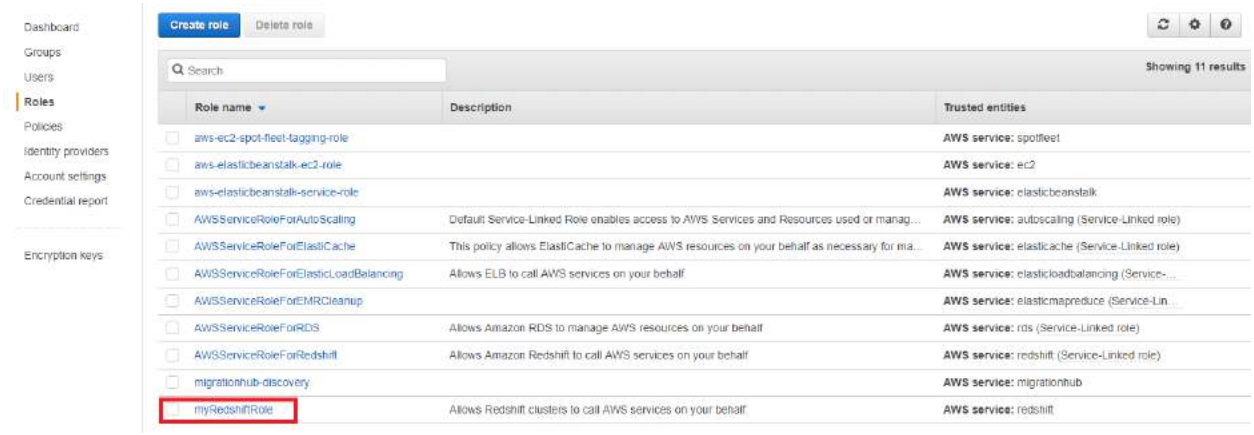
- We need to choose only S3 Read Only success through this IAM.



- Provide the name for this IAM role and click on create. After creating this IAM role, make a note of this ARN which would be used in future.

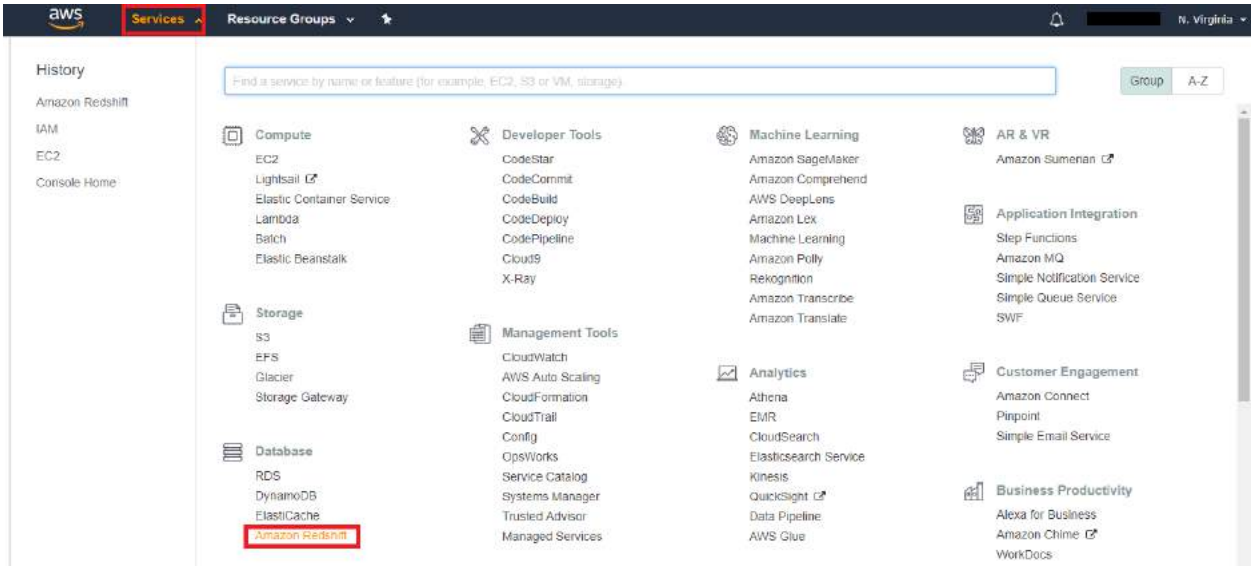


- New Redshift role has been created.

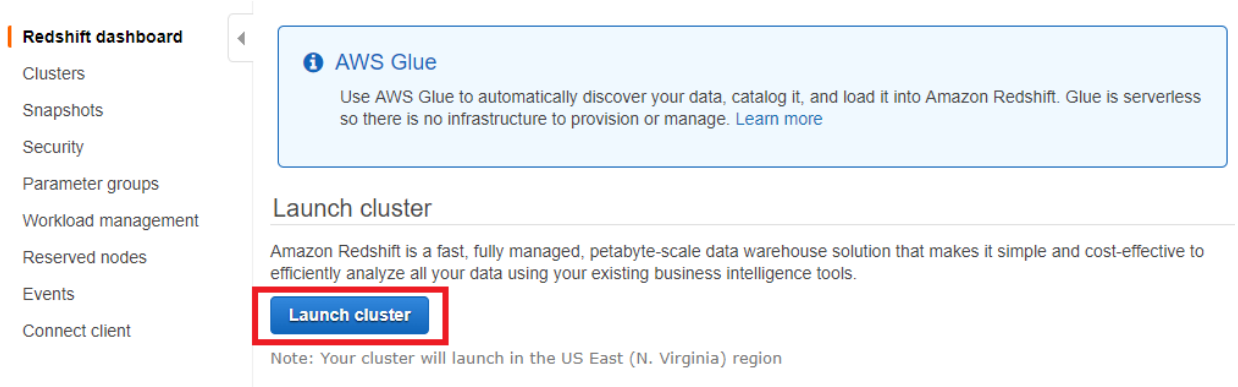


Step 3:

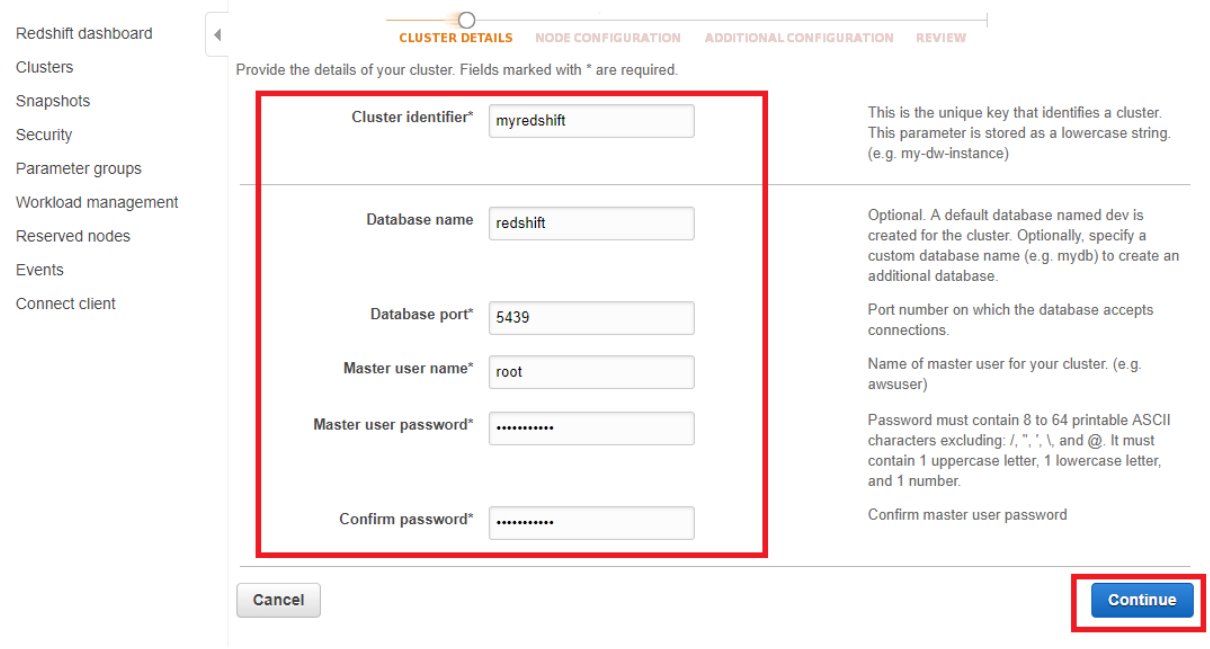
- Now, we could proceed to create a new Cluster. Select Services and choose Redshift option under the databases.



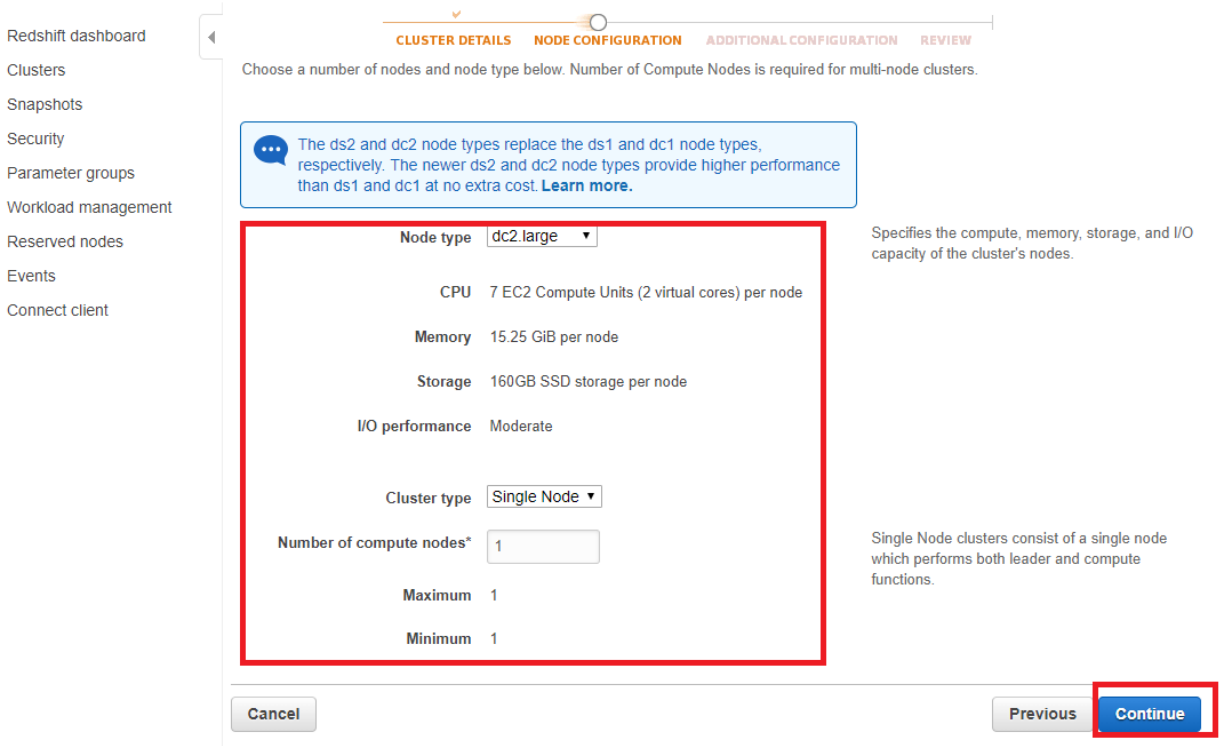
- Click on Launch Cluster.



- Provide the cluster name, username and the password along with DB name.



- Select the Node Type and make sure after validating the same it has deleted. If you want to replicate the set up, you can select the Node Type as Multiple from Single Node.



- Choose a VPC to launch it under, select the Security Group and Availability zone. Finally select an IAM role which has created in Step 2.

Redshift dashboard
Clusters
Snapshots
Security
Parameter groups
Workload management
Reserved nodes
Events
Connect client

CLUSTER DETAILS | NODE CONFIGURATION | ADDITIONAL CONFIGURATION | REVIEW

Provide the optional additional configuration details below.

Cluster parameter group default.redshift-1.0 — Parameter group to associate with this cluster.

Encrypt database None KMS HSM — Learn more about database encryption

Configure networking options:

Choose a VPC Default VPC (vpc-13a84c68) — The identifier of the VPC in which you want to create your cluster

Cluster subnet group default — Selected Cluster Subnet Group may limit the choice of Availability Zones

Publicly accessible Yes No — Select Yes if you want the cluster to be accessible from the public internet. Select No if you want it to be accessible only from within your private VPC network

Choose a public IP address Yes No — Select Yes if you want to select your own public IP address from a list of elastic IP (EIP) addresses that are already configured for your cluster's VPC. Select No if you want Amazon Redshift to provide an EIP for you instead.

Enhanced VPC Routing Yes No — Select Yes if you want to enable Enhanced VPC Routing. Learn more

Availability zone us-east-1a — The EC2 Availability Zone that the cluster will be created in.

Associate your cluster with one or more security groups.

VPC security groups default (sg-3cda034b) — List of VPC security groups to associate with this cluster.

Optionally, create a basic alarm for this cluster.

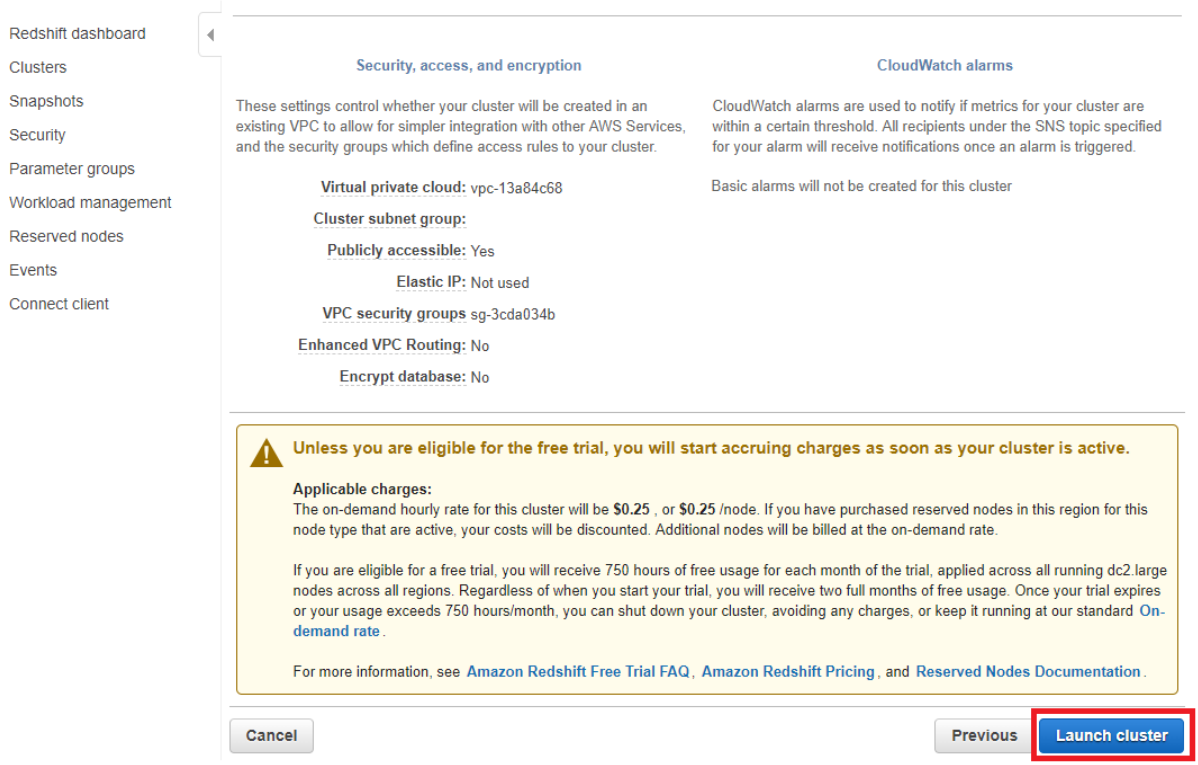
Create CloudWatch Alarm Yes No — Create a CloudWatch alarm to monitor the disk usage of your cluster.

Optionally, associate up to 10 IAM roles with this cluster.

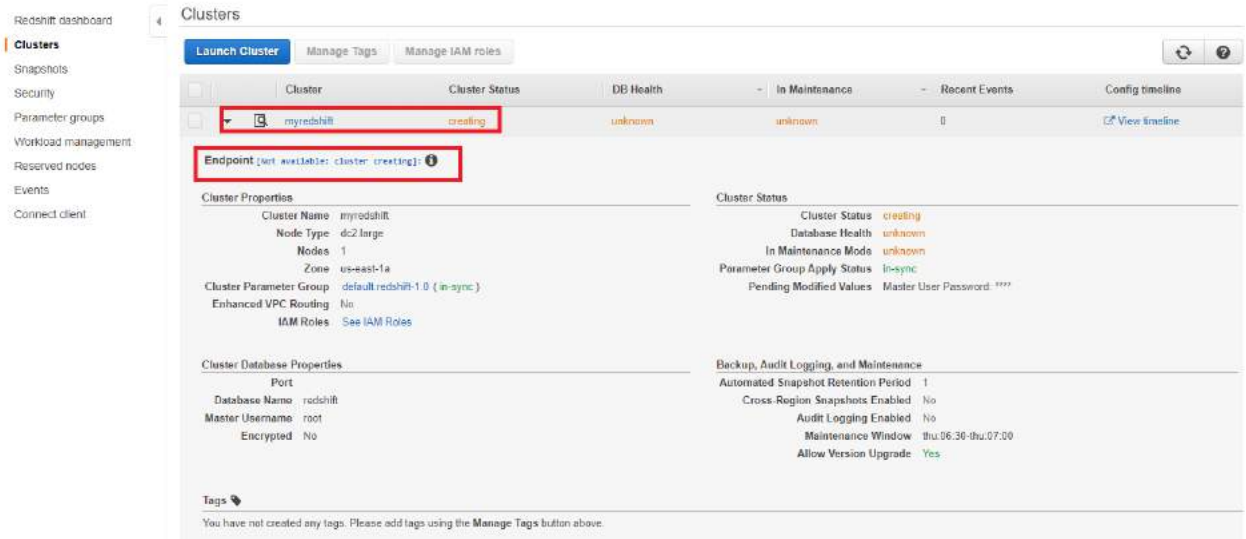
Available roles Choose a role
myRedshiftRole

Cancel | Previous | Continue

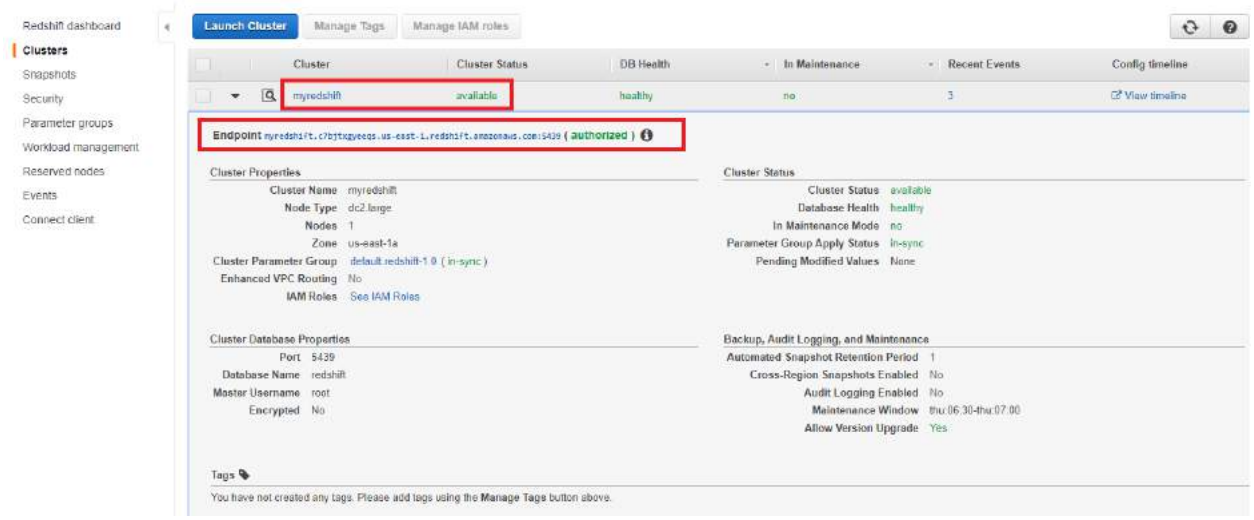
- Click on Launch Cluster after validating the selected items.



- Cluster creation is in progress which would take around 10-15 minutes of time.



- Cluster has been created successfully and you could make a note of this Endpoint URL.

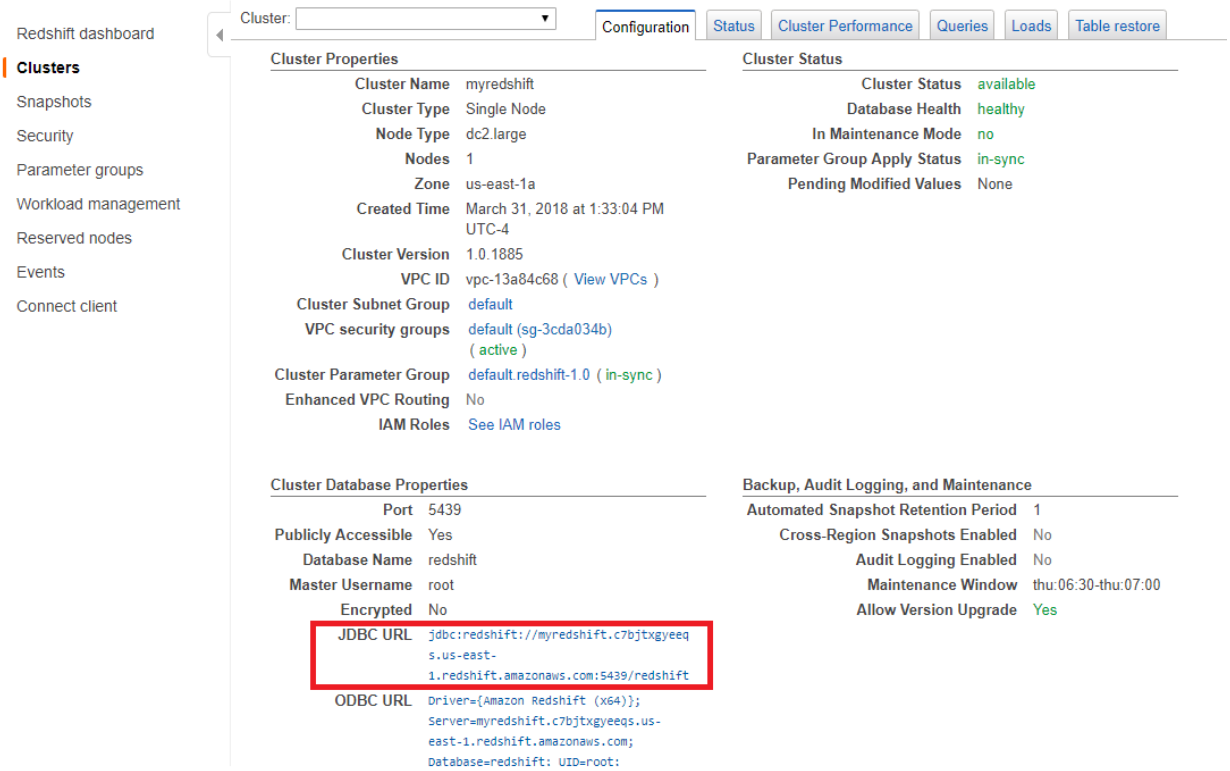


Step 4:

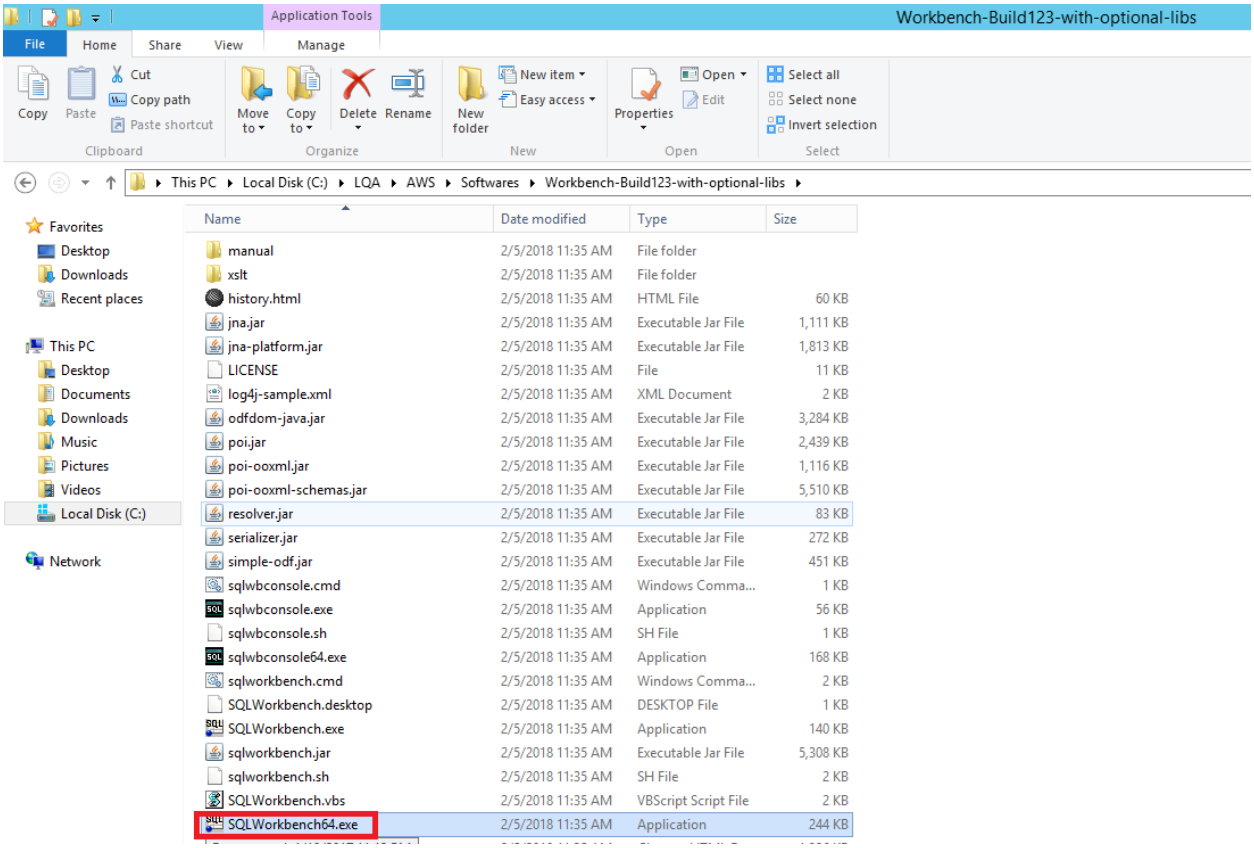
- Open the 5439 Redshift port number in the security group, which has been selected during Redshift Cluster provisioning.

Step 5:

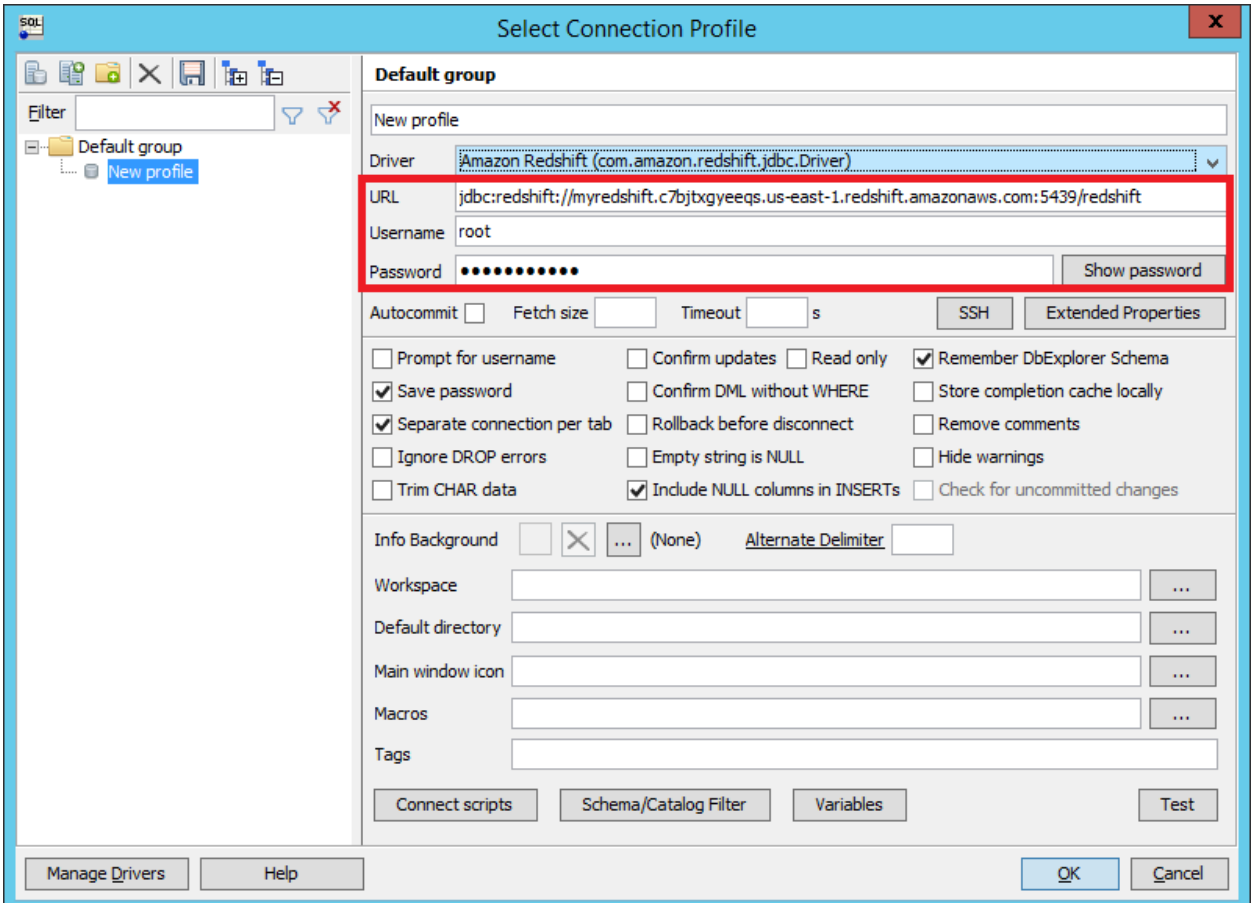
- Once the Redshift has been created, copy the JDBC URL and open the SQL Workbench.



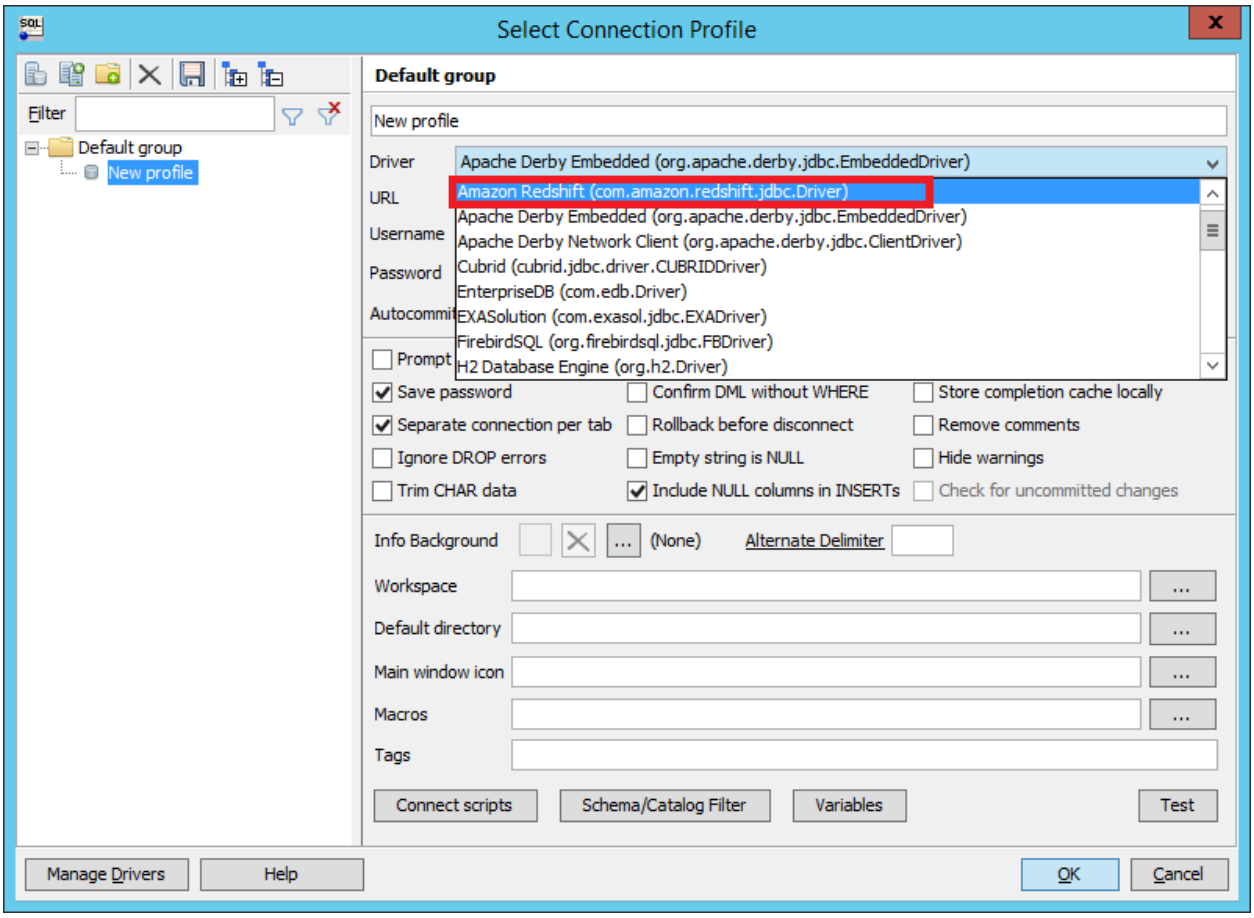
- Navigate to the folder where you have been downloaded Workbench and open the file depends on the system architecture.



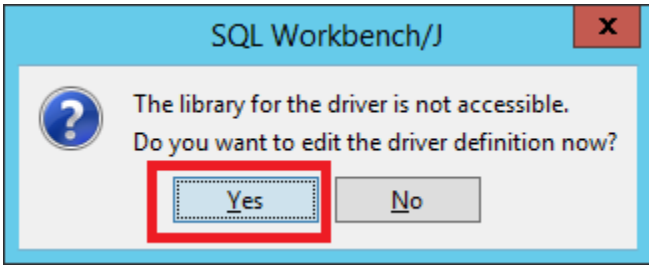
- Provide the JDBC URL, user name and the password.



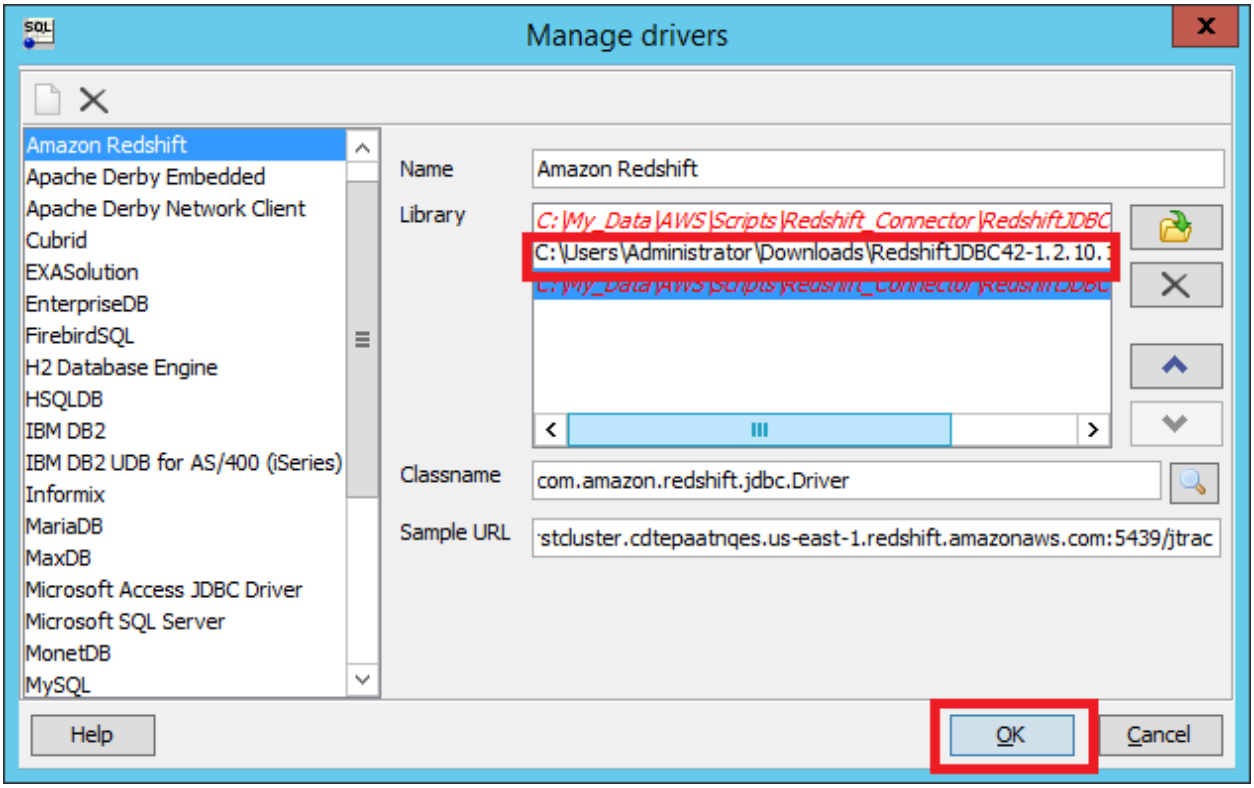
- Click on Drivers and select, Amazon Redshift.



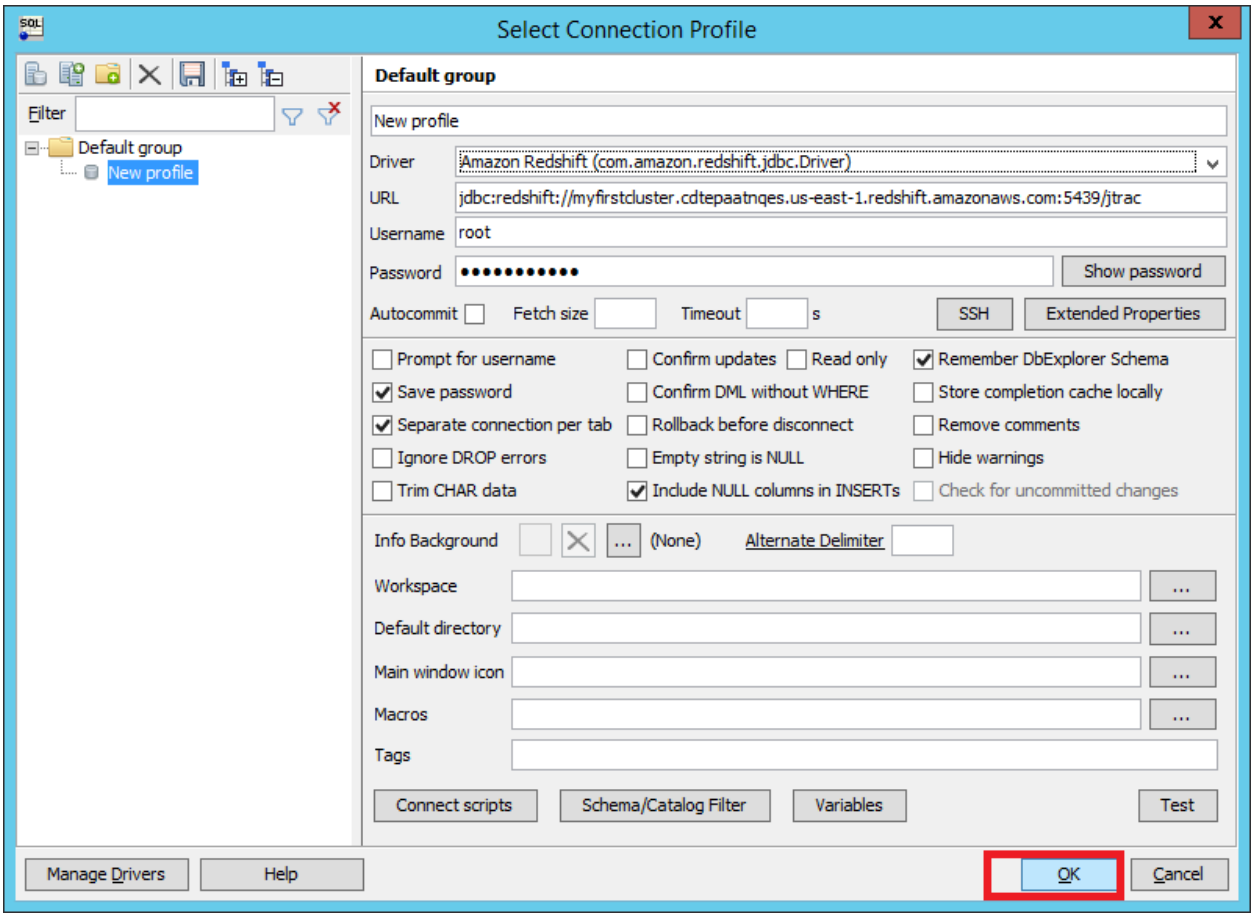
- Click on Yes.



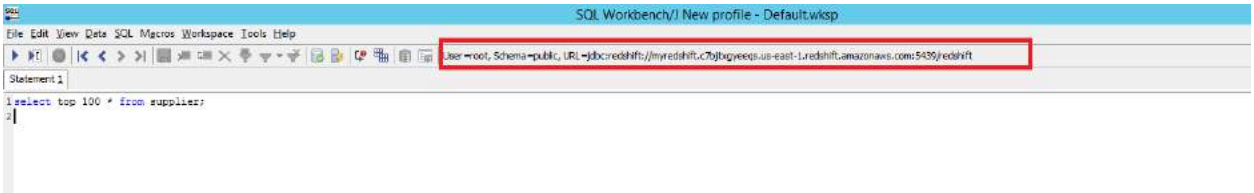
- Browse the location of connectivity jar which you have been downloaded and click on okay.



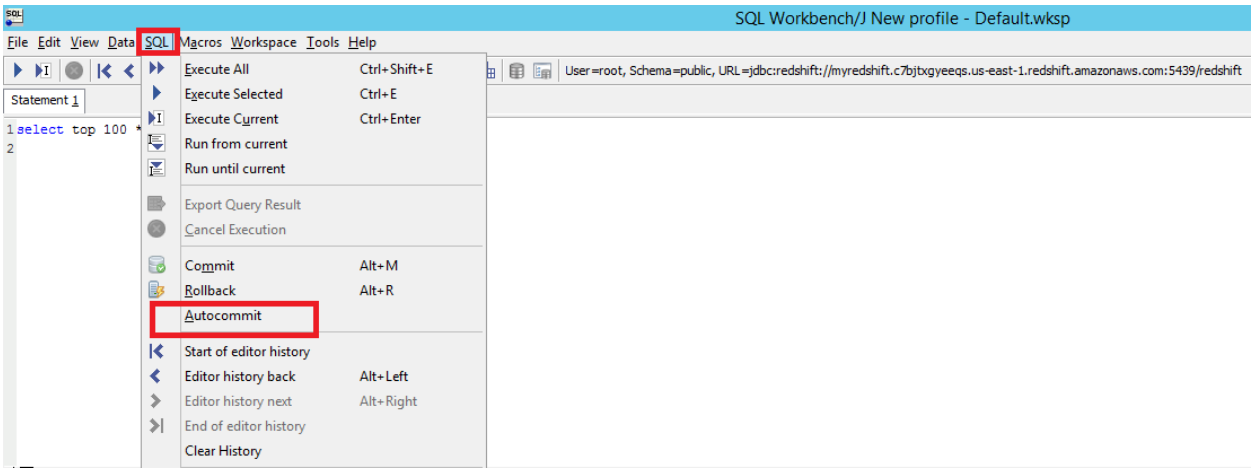
- After providing all the information, connect to Redshift database.



- Redshift has been connected successfully using workbench.



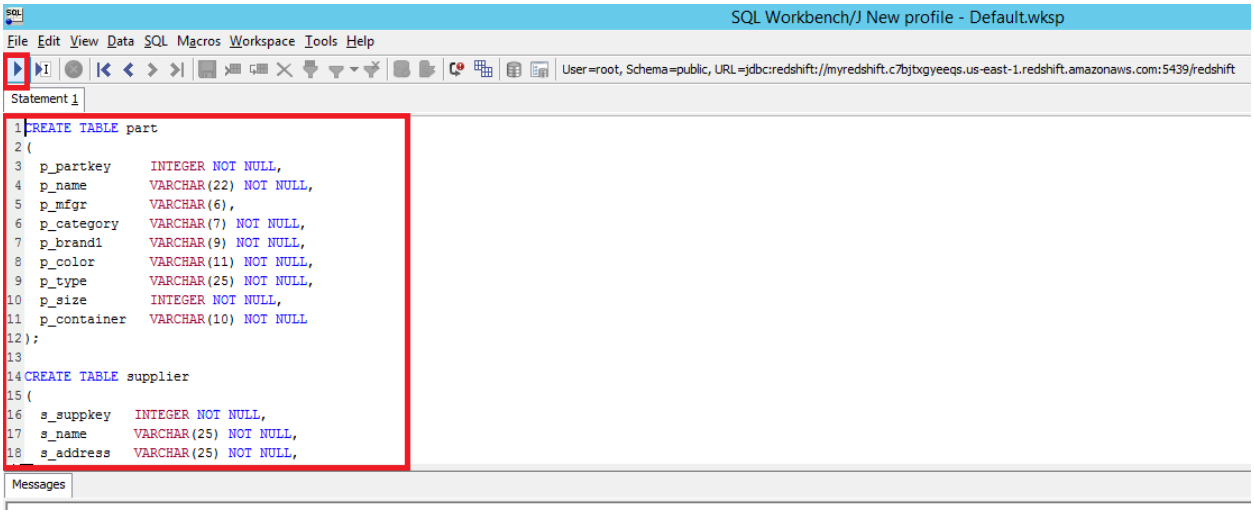
- Click on SQL option and select Auto Commit option before executing any commands.



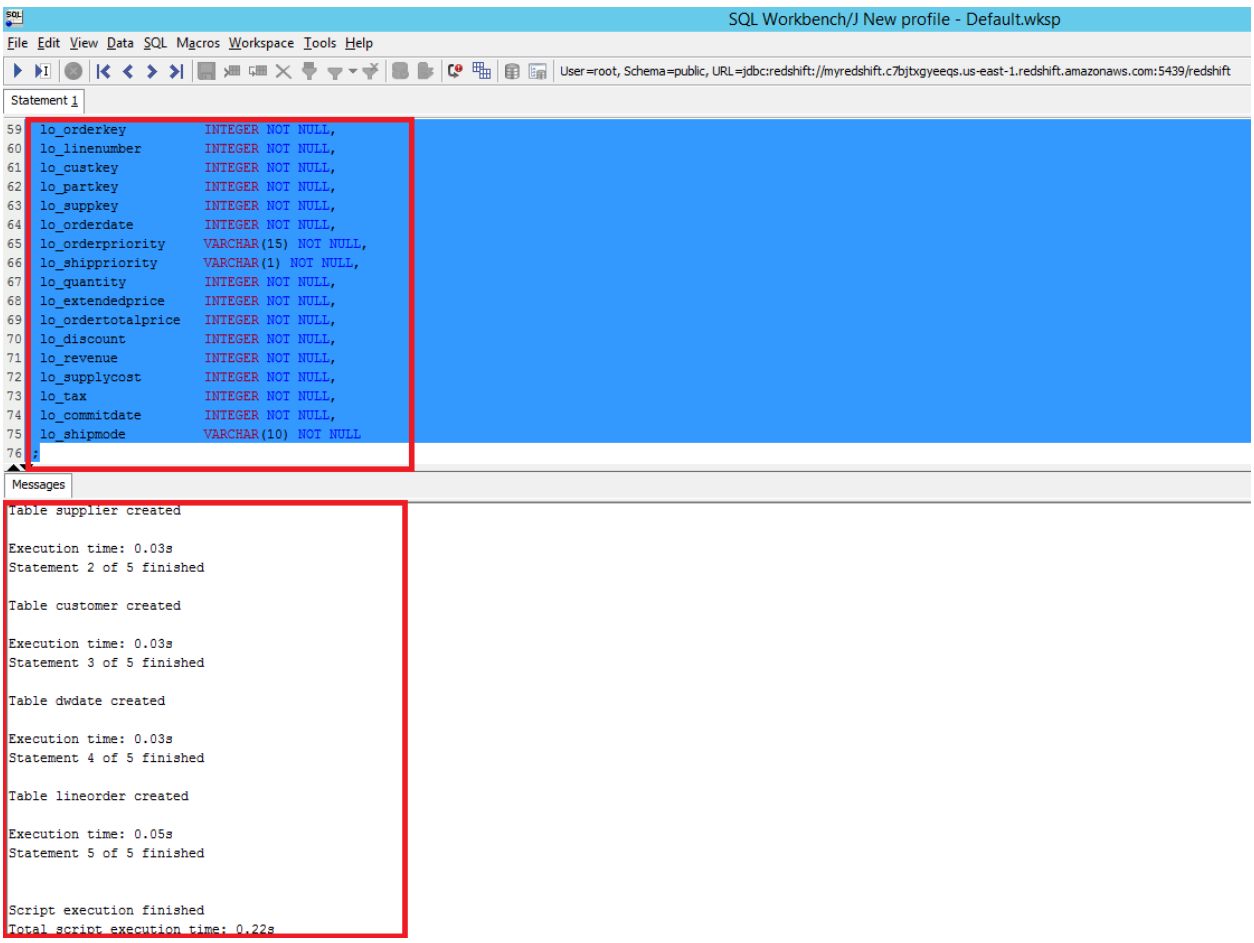
- Copy and paste the below content in Workbench and click on Play.

```
CREATE TABLE part
(
  p_partkey     INTEGER NOT NULL,
  p_name        VARCHAR(22) NOT NULL,
  p_mfgr        VARCHAR(6),
  p_category    VARCHAR(7) NOT NULL,
  p_brand1      VARCHAR(9) NOT NULL,
  p_color       VARCHAR(11) NOT NULL,
  p_type        VARCHAR(25) NOT NULL,
  p_size        INTEGER NOT NULL,
  p_container   VARCHAR(10) NOT NULL
);

CREATE TABLE supplier
(
  s_suppkey   INTEGER NOT NULL,
  s_name      VARCHAR(25) NOT NULL,
  s_address   VARCHAR(25) NOT NULL,
  s_city      VARCHAR(10) NOT NULL,
  s_nation    VARCHAR(15) NOT NULL,
  s_region    VARCHAR(12) NOT NULL,
  s_phone     VARCHAR(15) NOT NULL
);

CREATE TABLE customer
(
  c_custkey     INTEGER NOT NULL,
  c_name        VARCHAR(25) NOT NULL,
  c_address     VARCHAR(25) NOT NULL,
  c_city        VARCHAR(10) NOT NULL,
  c_nation      VARCHAR(15) NOT NULL,
  c_region      VARCHAR(12) NOT NULL,
  c_phone       VARCHAR(15) NOT NULL,
  c_mktsegment  VARCHAR(10) NOT NULL
);
```

```
CREATE TABLE dwdate
(
  d_datekey           INTEGER NOT NULL,
  d_date              VARCHAR(19) NOT NULL,
  d_dayofweek         VARCHAR(10) NOT NULL,
  d_month             VARCHAR(10) NOT NULL,
  d_year              INTEGER NOT NULL,
  d_yearmonthnum      INTEGER NOT NULL,
  d_yearmonth         VARCHAR(8) NOT NULL,
  d_daynuminweek      INTEGER NOT NULL,
  d_daynuminmonth     INTEGER NOT NULL,
  d_daynuminyear      INTEGER NOT NULL,
  d_monthnuminyear    INTEGER NOT NULL,
  d_weeknuminyear     INTEGER NOT NULL,
  d_sellingseason     VARCHAR(13) NOT NULL,
  d_lastdayinweekfl   VARCHAR(1) NOT NULL,
  d_lastdayinmonthfl  VARCHAR(1) NOT NULL,
  d_holidayfl         VARCHAR(1) NOT NULL,
  d_weekdayfl         VARCHAR(1) NOT NULL
);
CREATE TABLE lineorder
(
  lo_orderkey         INTEGER NOT NULL,
  lo_linenumber       INTEGER NOT NULL,
  lo_custkey          INTEGER NOT NULL,
  lo_partkey          INTEGER NOT NULL,
  lo_suppkey          INTEGER NOT NULL,
  lo_orderdate        INTEGER NOT NULL,
  lo_orderpriority    VARCHAR(15) NOT NULL,
  lo_shippriority     VARCHAR(1) NOT NULL,
  lo_quantity         INTEGER NOT NULL,
  lo_extendedprice    INTEGER NOT NULL,
  lo_ordertotalprice  INTEGER NOT NULL,
  lo_discount         INTEGER NOT NULL,
  lo_revenue          INTEGER NOT NULL,
  lo_supplycost       INTEGER NOT NULL,
  lo_tax              INTEGER NOT NULL,
  lo_commitdate       INTEGER NOT NULL,
  lo_shipmode         VARCHAR(10) NOT NULL
);
```



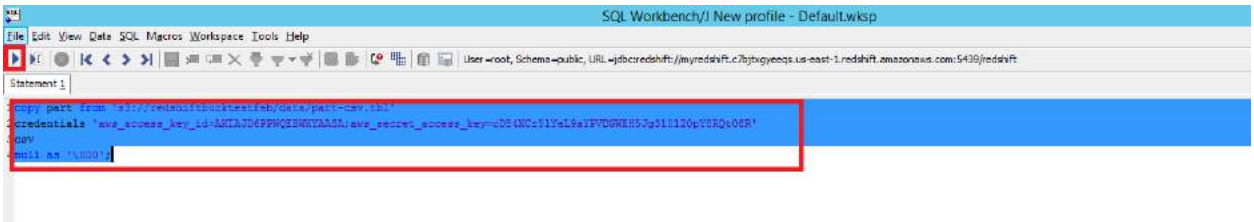
- Table have created successfully after executing.



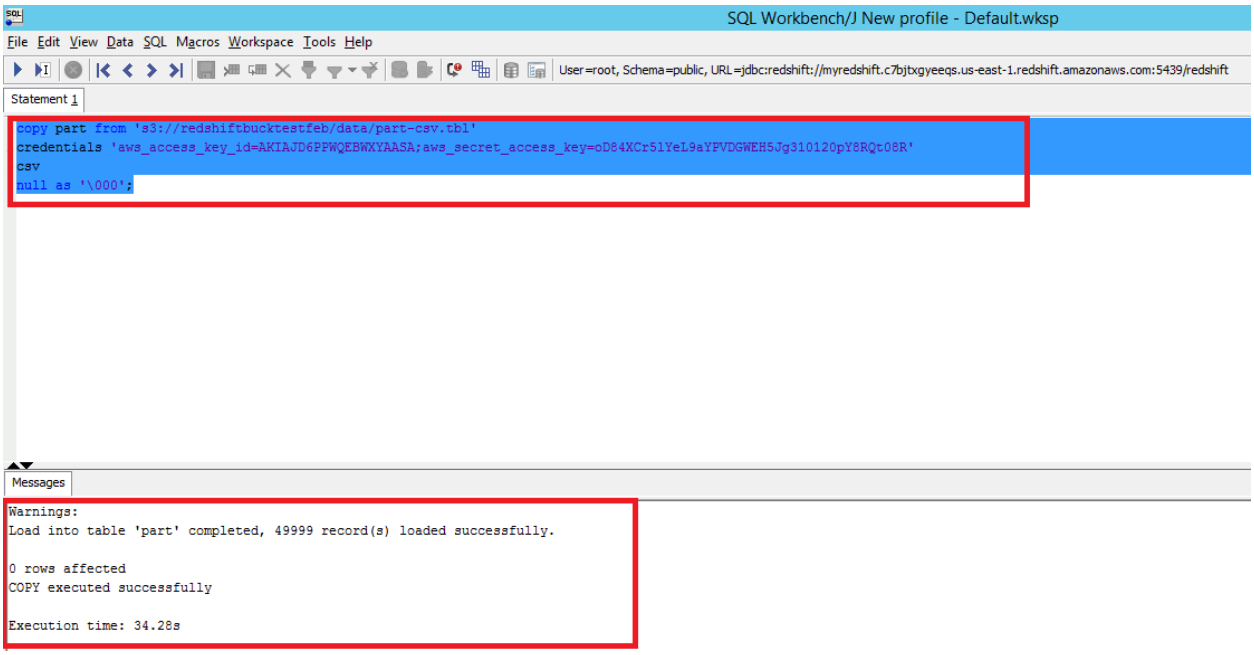
- Create one new S3 Bucket and upload all the files of sample data. Sample Data could be downloaded from the below given URL.
- https://drive.google.com/file/d/1iFcNqtrXjHP1q8ysrV6Wq5HWkjeJXj7t/view?usp=sharing

- After uploading all the files into S3 bucket, replace the bucket name, access key and secret key in upcoming commands which we are executing.

copy part from 's3://redshiftbucktestfeb/data/part-csv.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
csv
null as '\000';



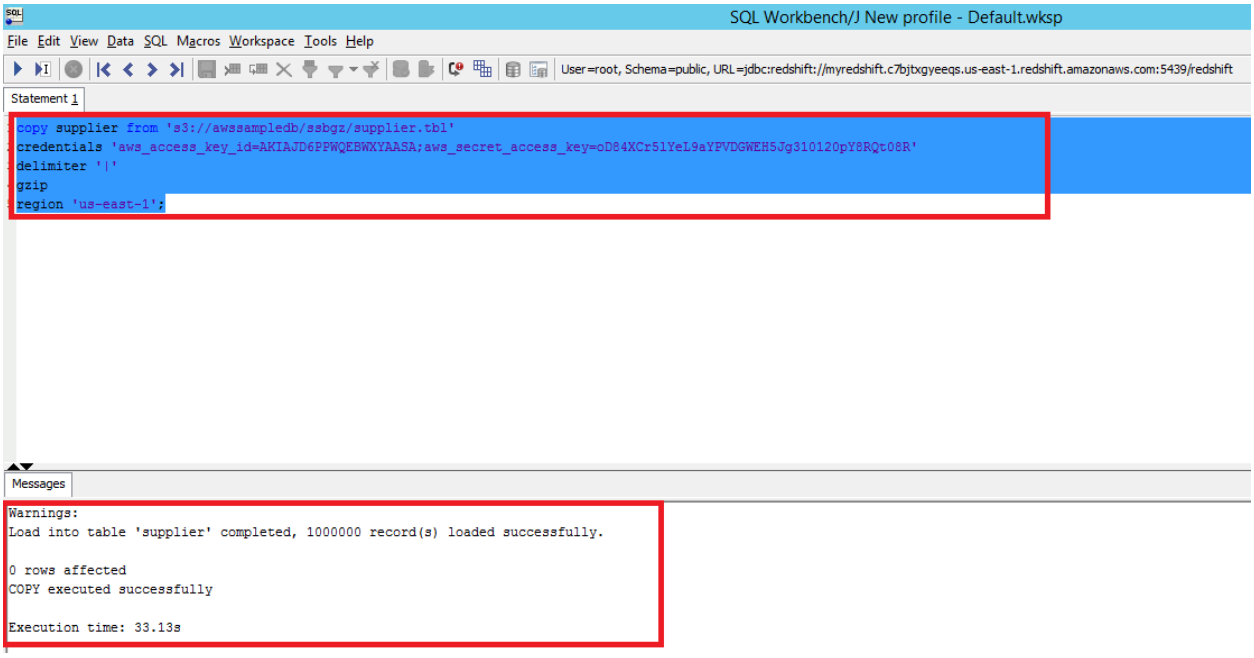
- Almost 50000 records are executed in this Redshift within 35 seconds of time.



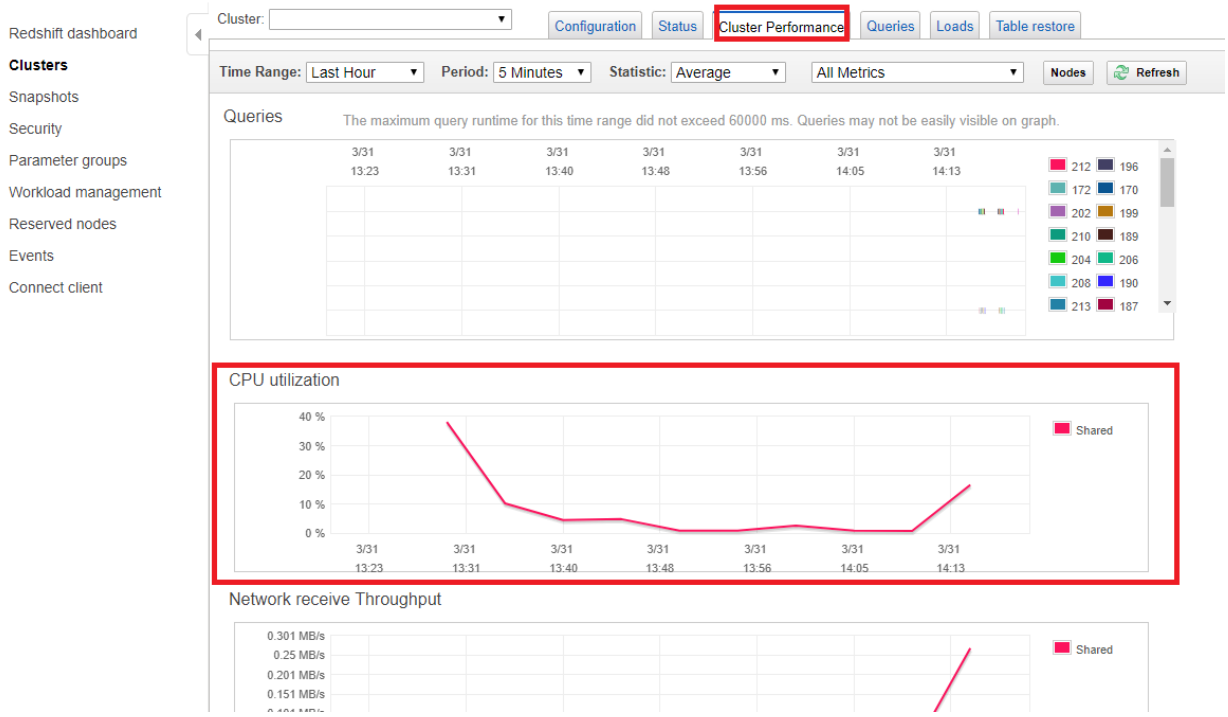
- Similarly, we are executing more commands to import huge volume of data into Redshift.

copy supplier from 's3://awssampledb/ssbgz/supplier.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
delimiter '|'
gzip
region 'us-east-1';

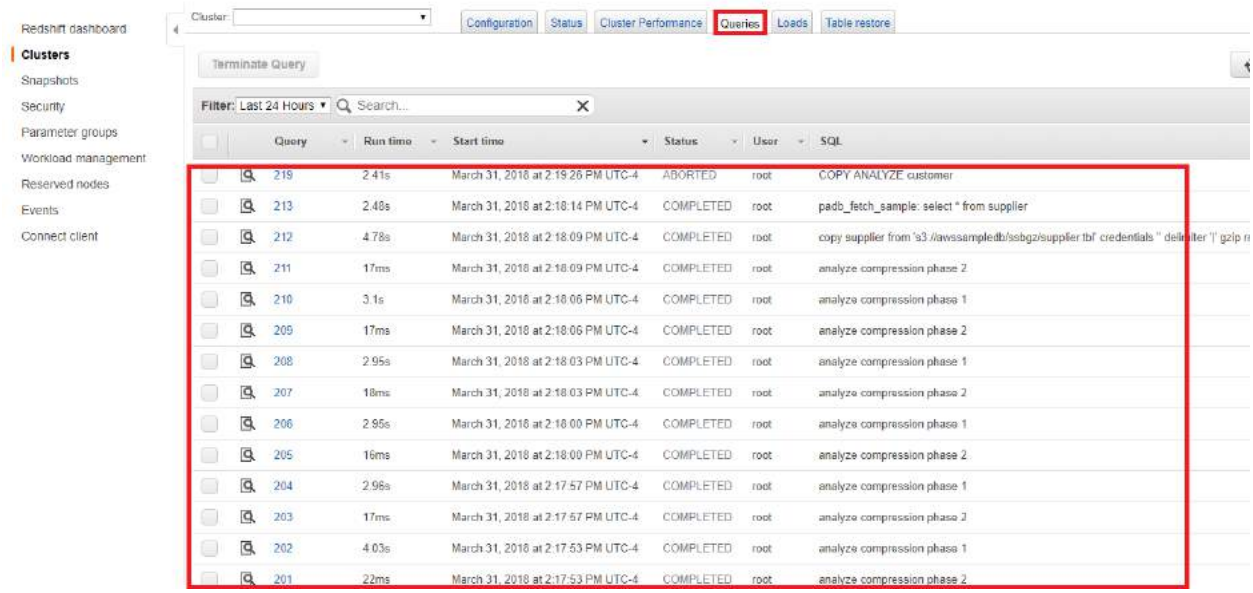
- Nearly 100000 records were executed in 33 seconds of time.



- Even though if we execute more volume of data, performance of this Redshift is same as like before without any slowness.



- Execution summary could be found in Queries tab.

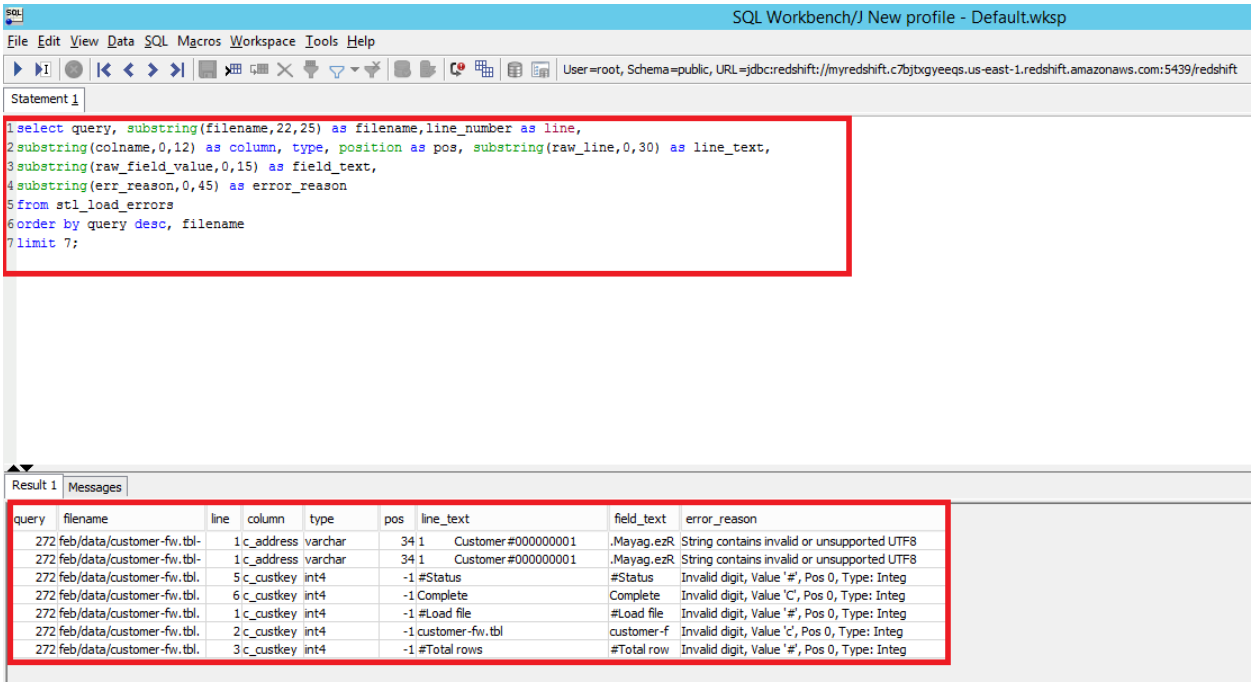


- As like before commands, execute the remaining commands in the Redshift Data warehouse.

```
copy customer from 's3://redshiftbucktestfeb/data/customer-fw.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
fixedwidth 'c_custkey:10, c_name:25, c_address:25, c_city:10, c_nation:15, c_region :12, c_phone:15,c_mktsegment:10'
maxerror 10;
```

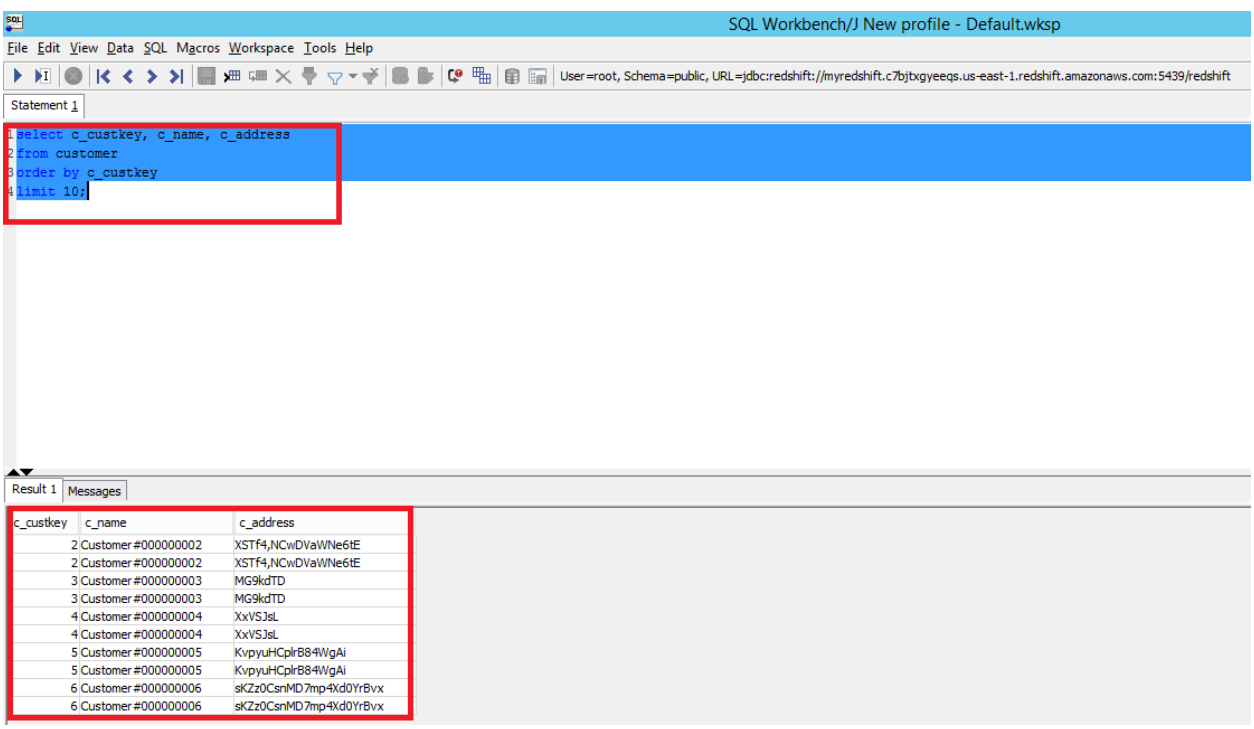
- To find the list of added data into Redshift, please use the below command to do the same.

```
select query, substring(filename,22,25) as filename,line_number as line,
substring(colname,0,12) as column, type, position as pos, substring(raw_line,0,30) as line_text,
substring(raw_field_value,0,15) as field_text,
substring(err_reason,0,45) as error_reason
from stl_load_errors
order by query desc, filename
limit 7;
```



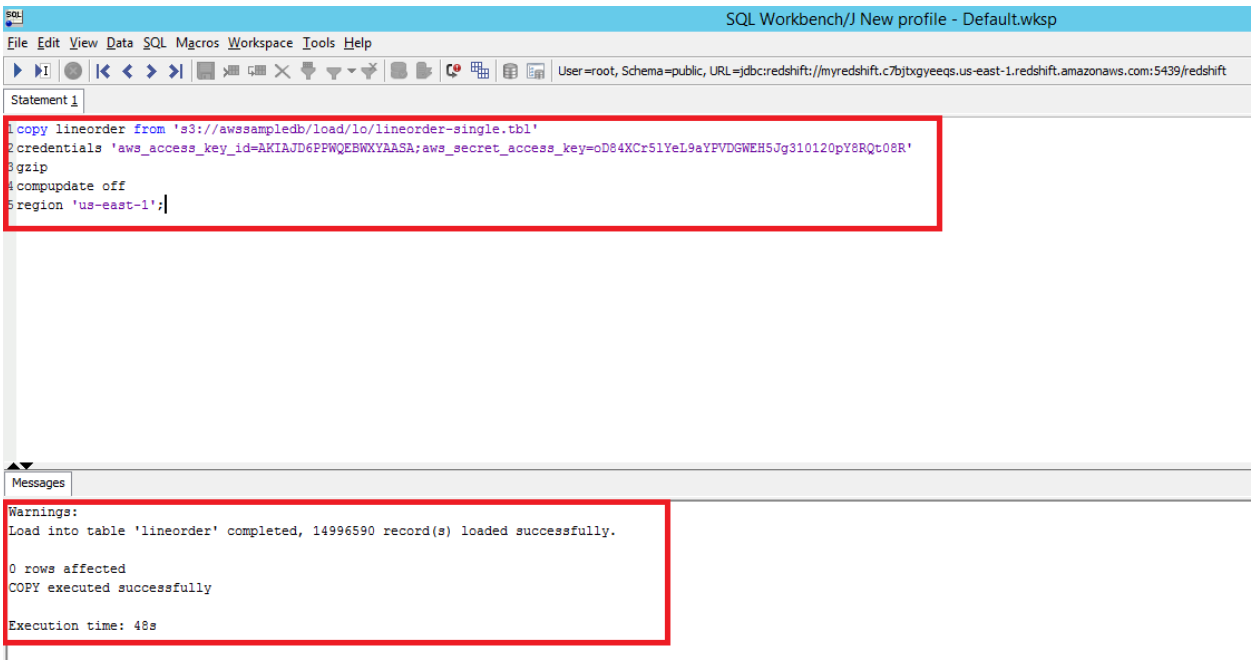
- Similarly, if you want to look into another table, execute the below command.

```
select c_custkey, c_name, c_address
from customer
order by c_custkey
limit 10;
```



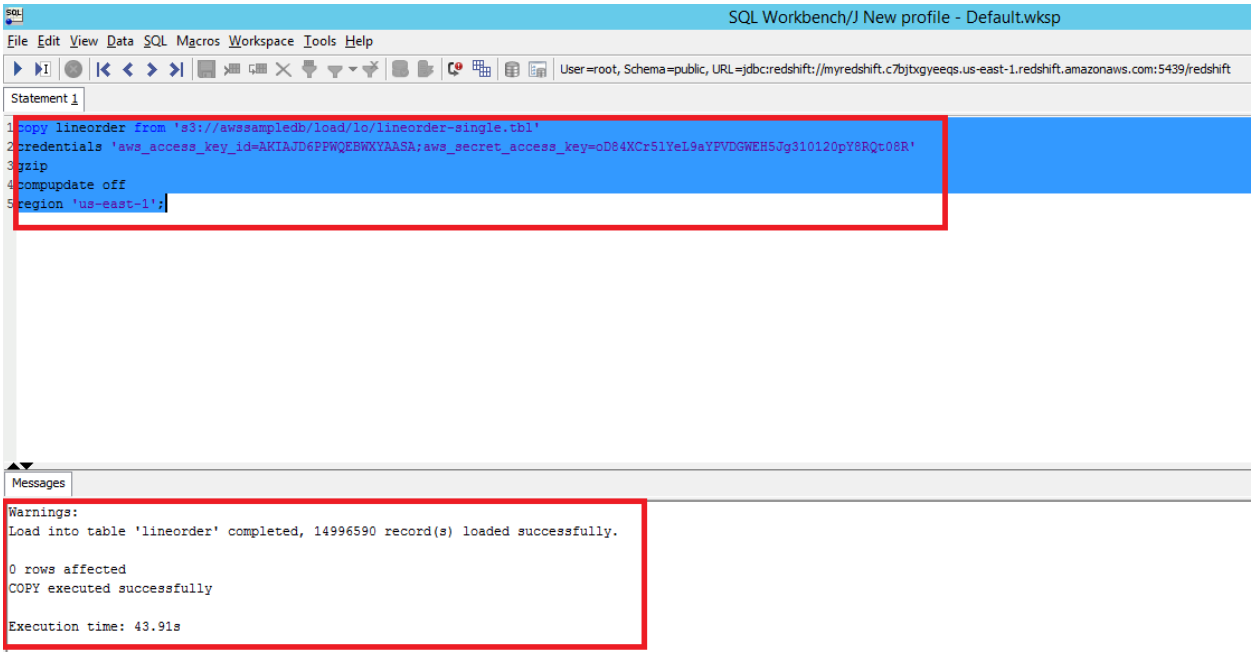
- Now, download customer-fw-manifest file from S3 bucket, change your bucket name and upload it back to s3 again.
- After uploading execute the below commands.

```
copy customer from 's3://redshiftbucktestfeb/data/customer-fw-manifest'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
fixedwidth 'c_custkey:10, c_name:25, c_address:25, c_city:10, c_nation:15, c_region :12, c_phone:15,c_mktsegment:10'
maxerror 10
acceptinvchars as '^'
manifest;
```



- Proceed to upload all the data to all the tables which you have been created using the below commands.

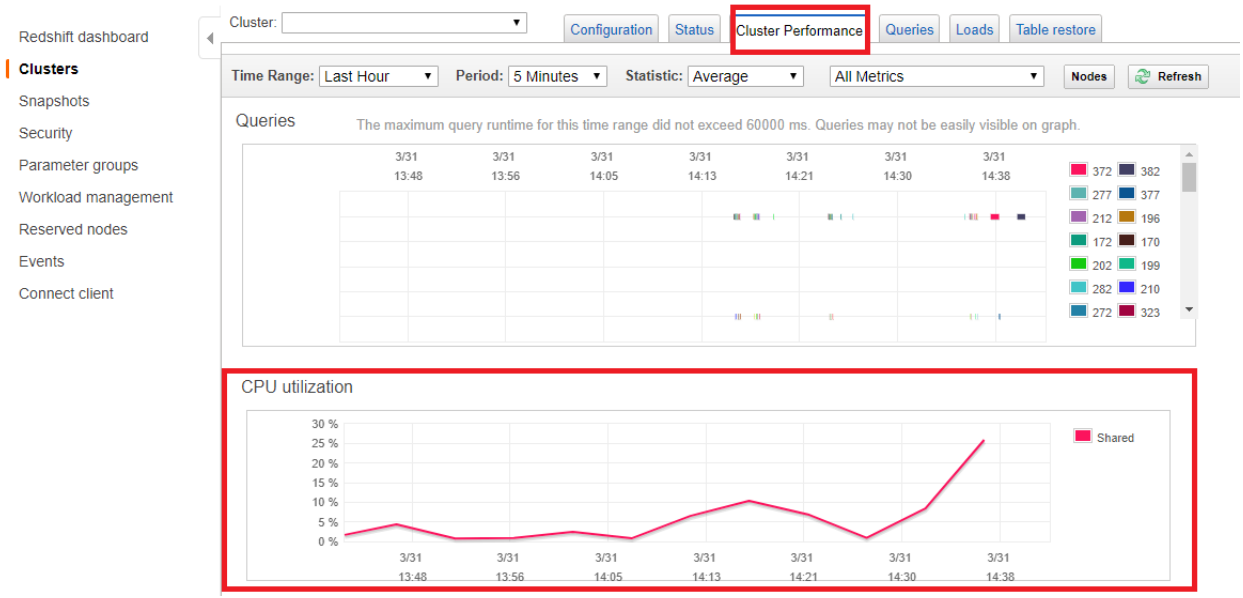
```
copy dwdate from 's3://redshiftbucktestfeb/data/dwdate-tab.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
delimiter '\t'
dateformat 'auto';

copy lineorder from 's3://awssampledb/load/lo/lineorder-single.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
gzip
compupdate off
region 'us-east-1';
```



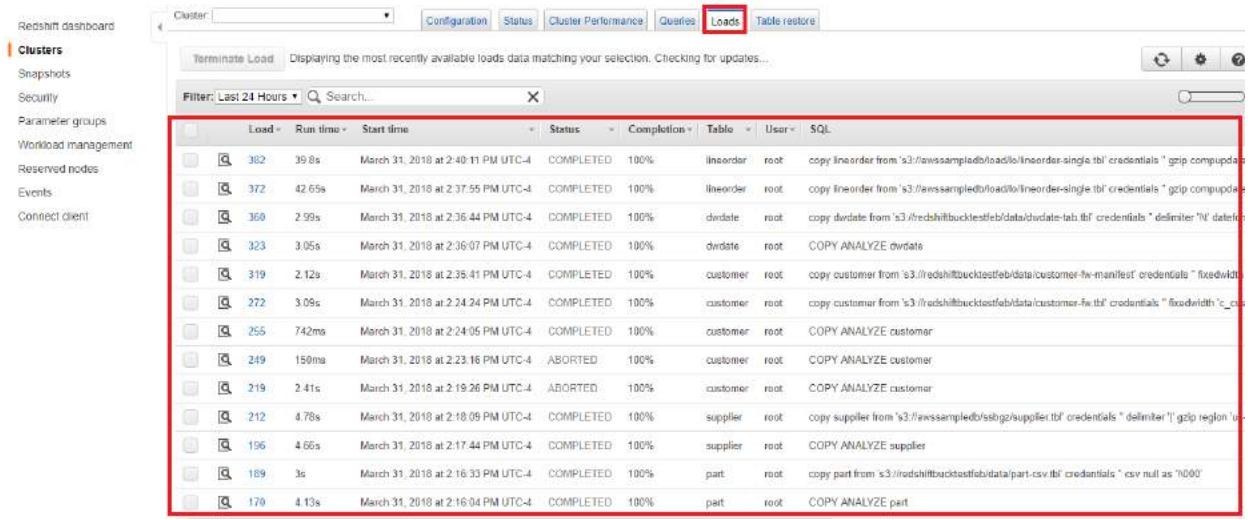
- Finally, we could import the data file to last table using the below command.

copy lineorder from 's3://awssampledb/load/lo/lineorder-multi.tbl'
credentials
'aws_access_key_id=AKIAJD6PPWQEBWXYAASA;aws_secret_access_key=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'
gzip
compupdate off
region 'us-east-1';

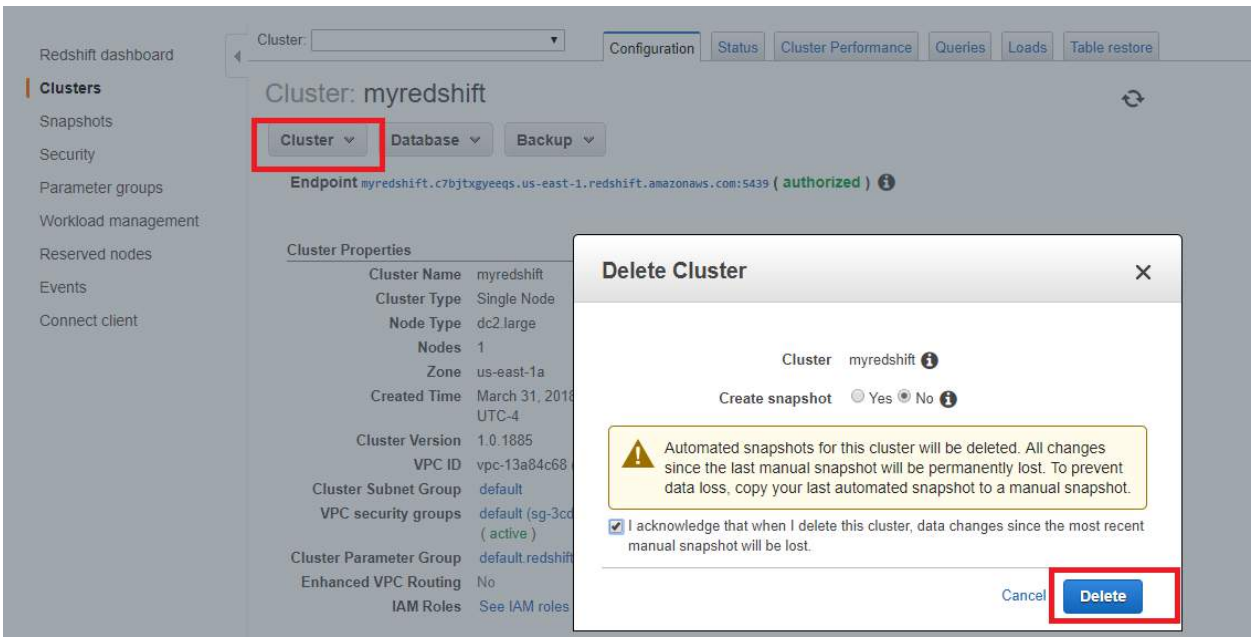
- Now, millions and millions of records has been added into this Redshift and even though, the performance of the same is stable.



- All the loaded data could be found in load menu,



- Click on Cluster and Select an option as delete & delete the Redshift database without taking a snapshot if there is no use in future.



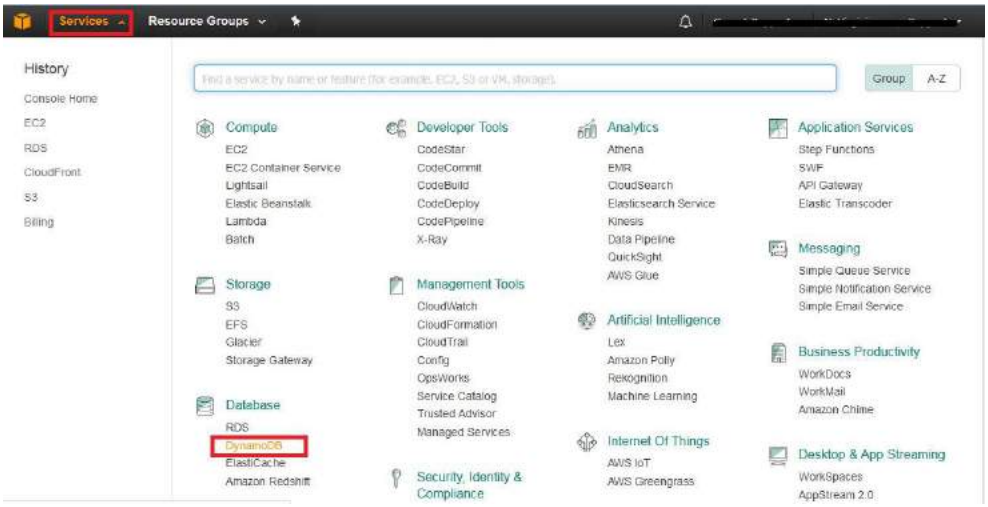
Advantages of Redshift:

- Massive Database
- Backing up
- Beyond Petabyte
- Saves Money
- Fasten Business Operation

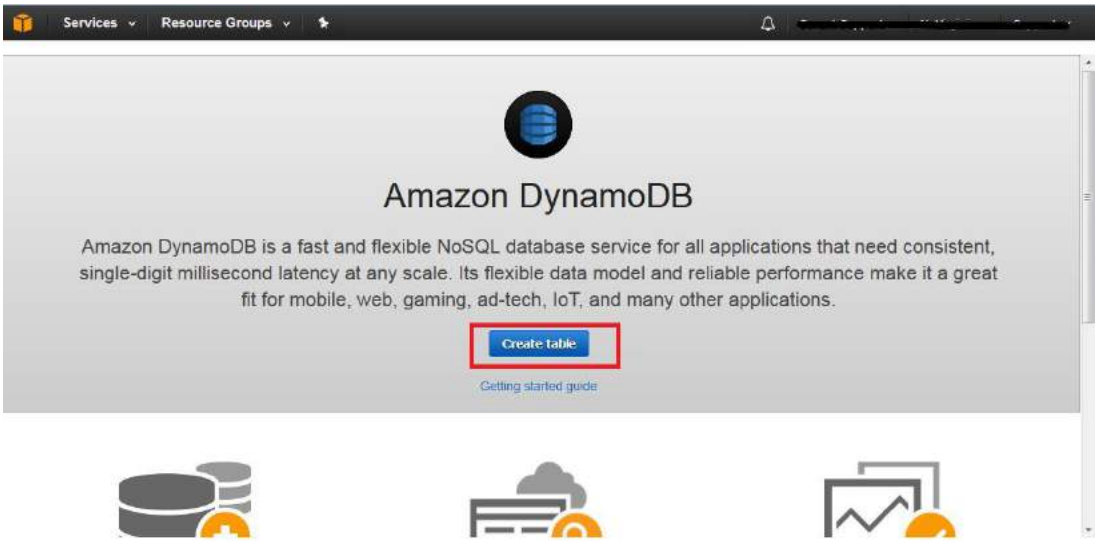
Refer the below given URL incase if you face more trouble in executing the above given queries.

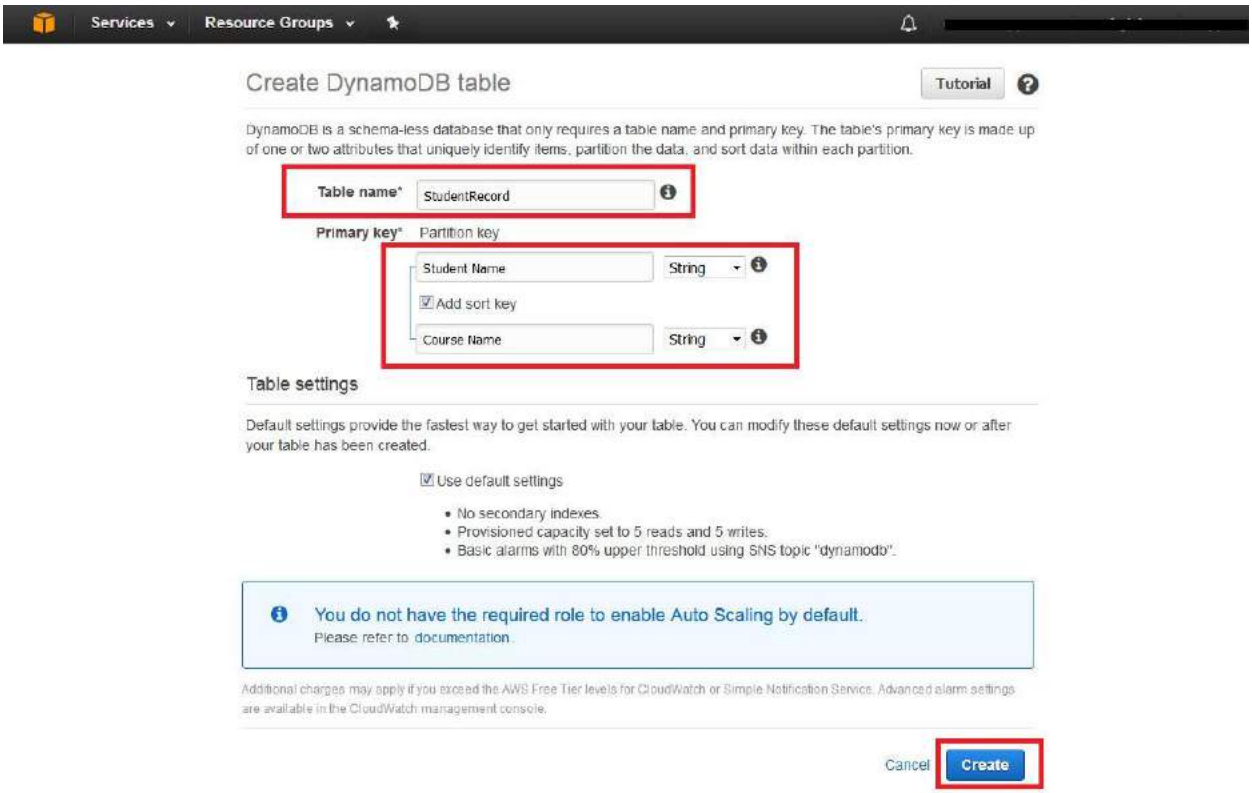
DynamoDB:

- Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity, makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.
- If you require only the table and instead of using Database, we can use DynamoDB, in which it contains only table to add your values, attributes and parameters.
- Navigate to Services and Choose DynamoDB under Database as like shown below.

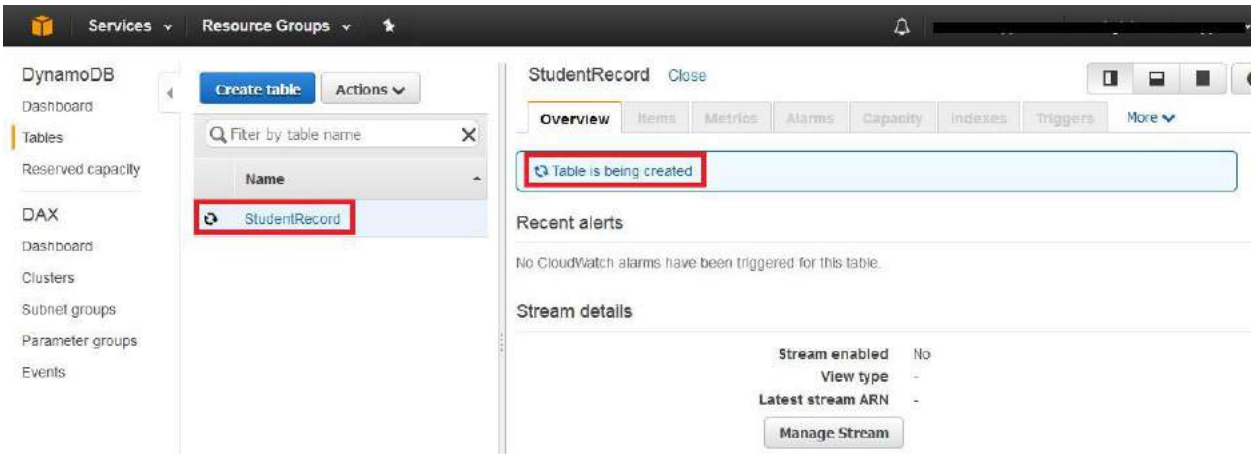


- Click on Create Table as like shown below.
- Provide the table name, Primary Key and add a sort key if required and click on create as like shown below.

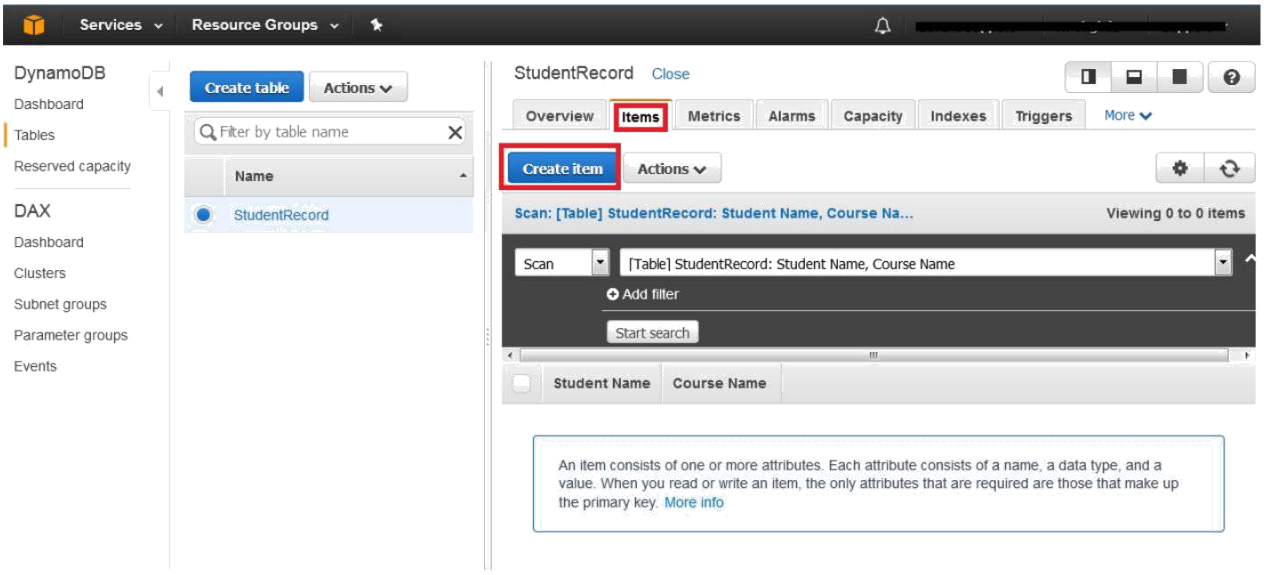


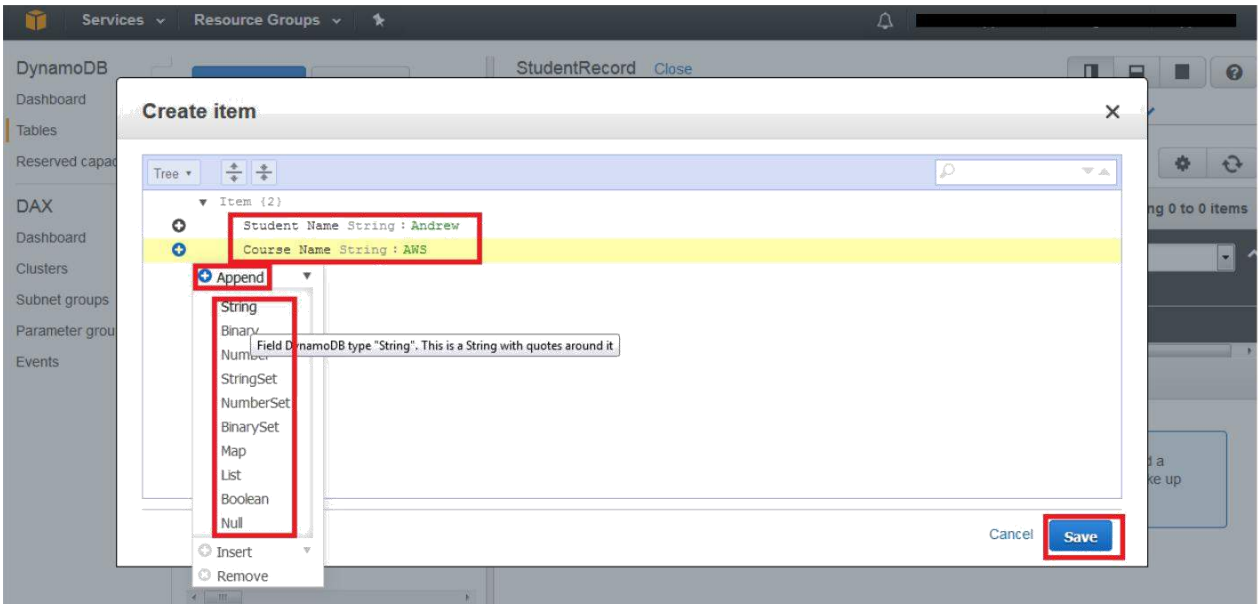


- Table is being created and generally, it would take within 5 minutes of time.

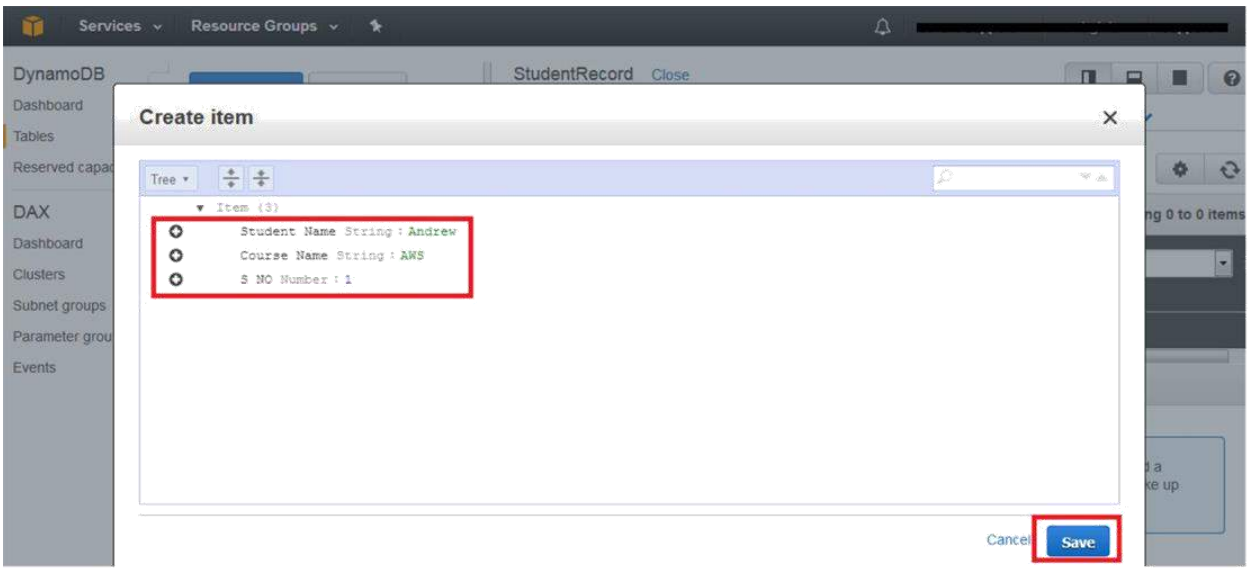


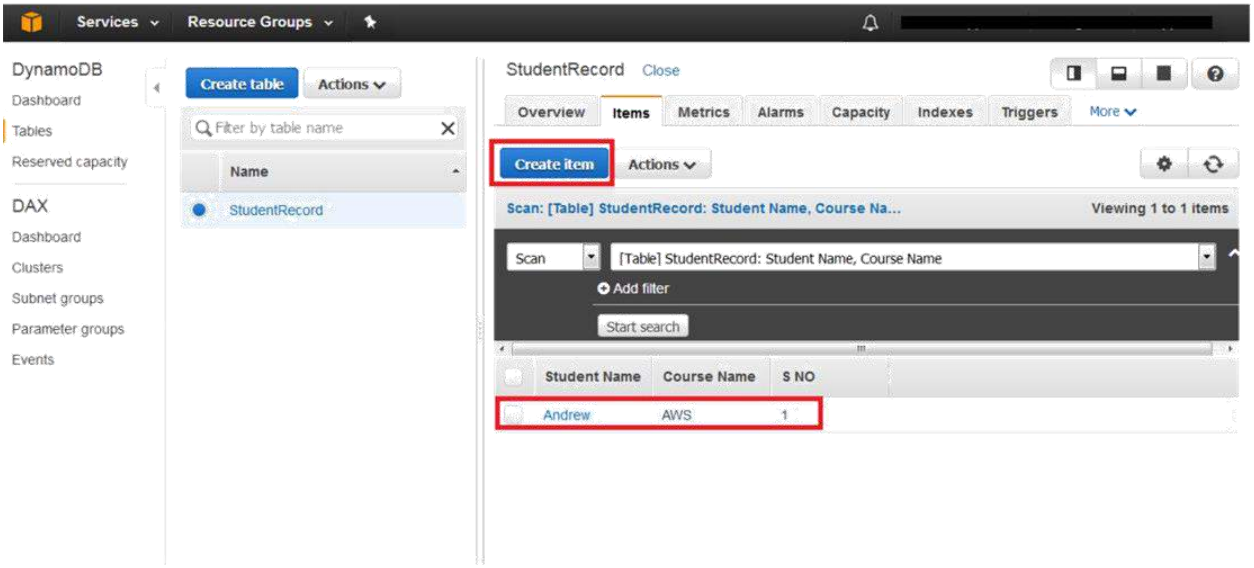
- Once the table is created, navigate to **Items >> Create Item** for adding the values and if required to add additional attributes, the same can be added as like shown below.

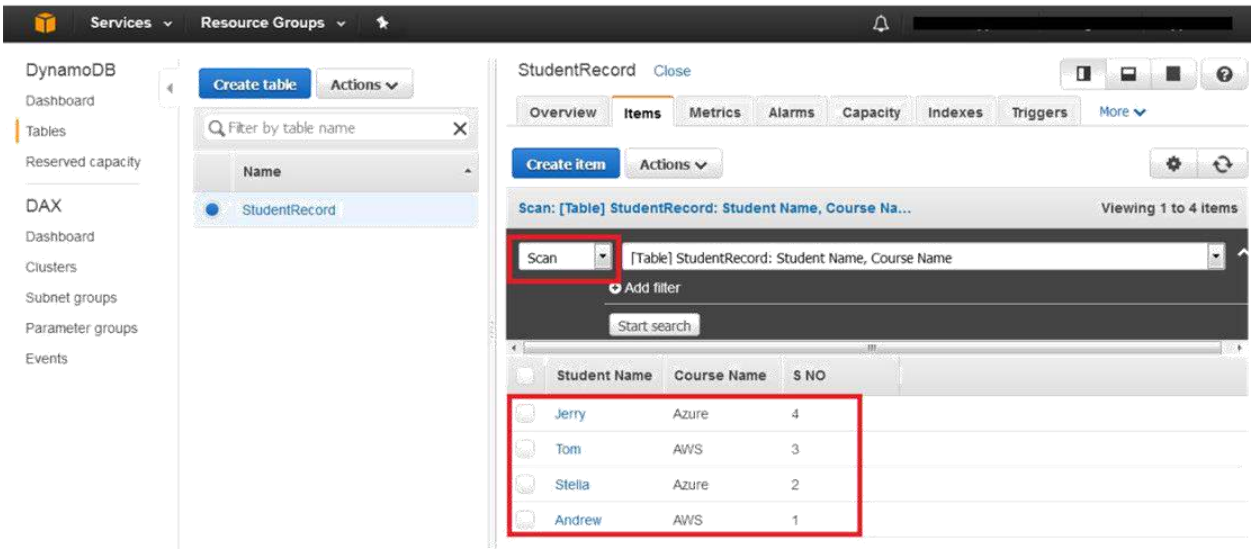

Services
Resource Groups
DynamoDB
Dashboard
Tables
Reserved capacity
DAX
Dashboard
Clusters
Subnet groups
Parameter groups
Events
Create table
Actions
Filter by table name
Name
StudentRecord
StudentRecord
Close
Overview
Items
Metrics
Alarms
Capacity
Indexes
Triggers
More
Create item
Actions
Scan: [Table] StudentRecord: Student Name, Course Na...
Viewing 0 to 0 items
Scan
[Table] StudentRecord: Student Name, Course Name
Add filter
Start search
Student Name
Course Name
An item consists of one or more attributes. Each attribute consists of a name, a data type, and a value. When you read or write an item, the only attributes that are required are those that make up the primary key. More info


Services
Resource Groups
DynamoDB
Dashboard
Tables
DAX
Dashboard
Clusters
Subnet groups
Events
StudentRecord
Close
Create item
Tree
Item {2}
Student Name String : Andrew
Course Name String : AWS
Append
String
Binary
StringSet
NumberSet
BinarySet
Map
List
Boolean
Null
Insert
Remove
Field DynamoDB type "String". This is a String with quotes around it
Cancel
Save

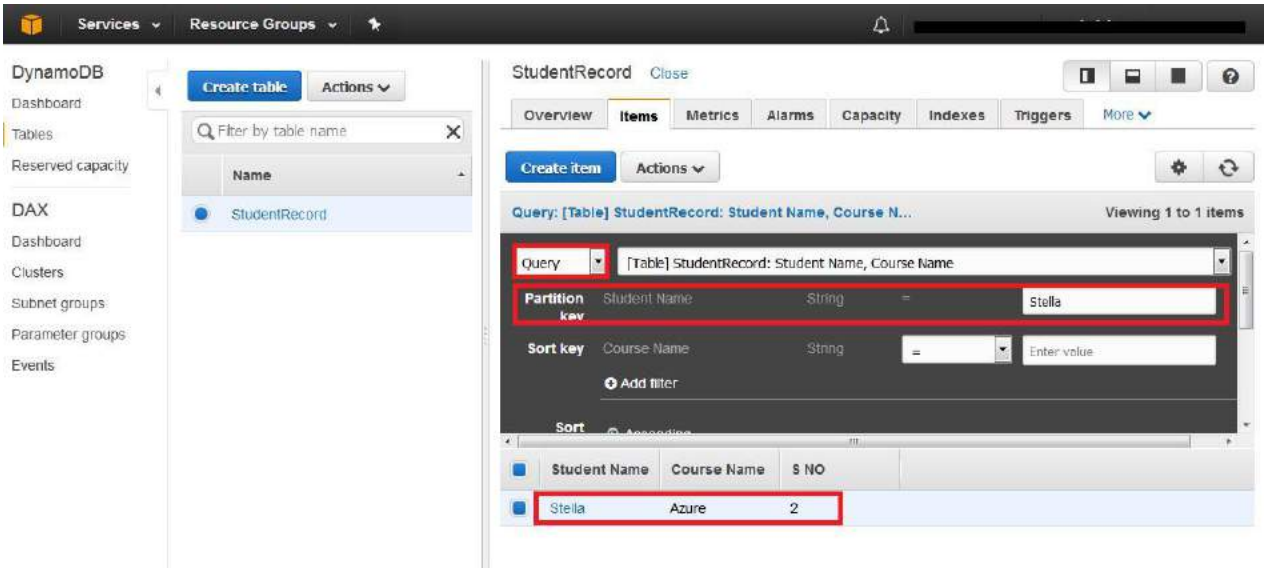
- After adding all the values, click on Save to add other items as like shown below.



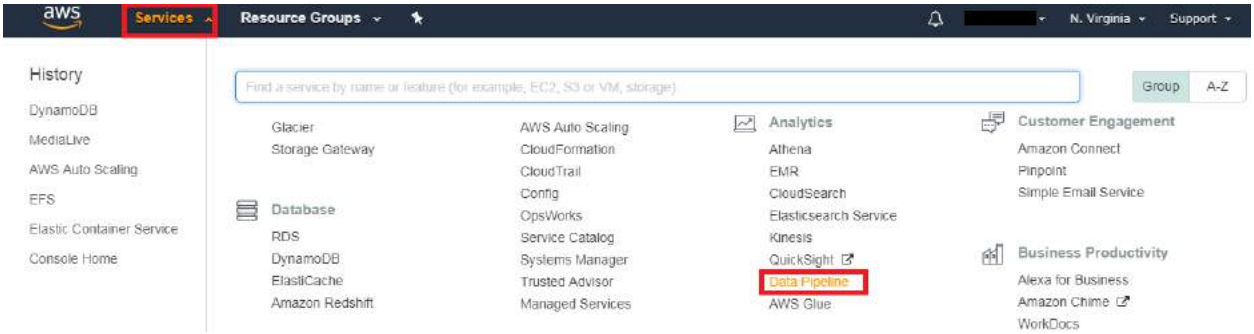




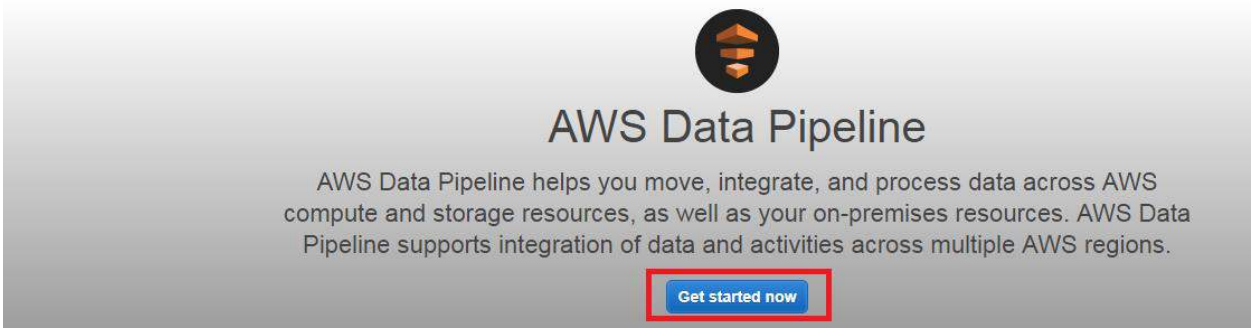
- Created items can be searched by changing the value to Query and type the necessary information to search in the created table as like shown below.



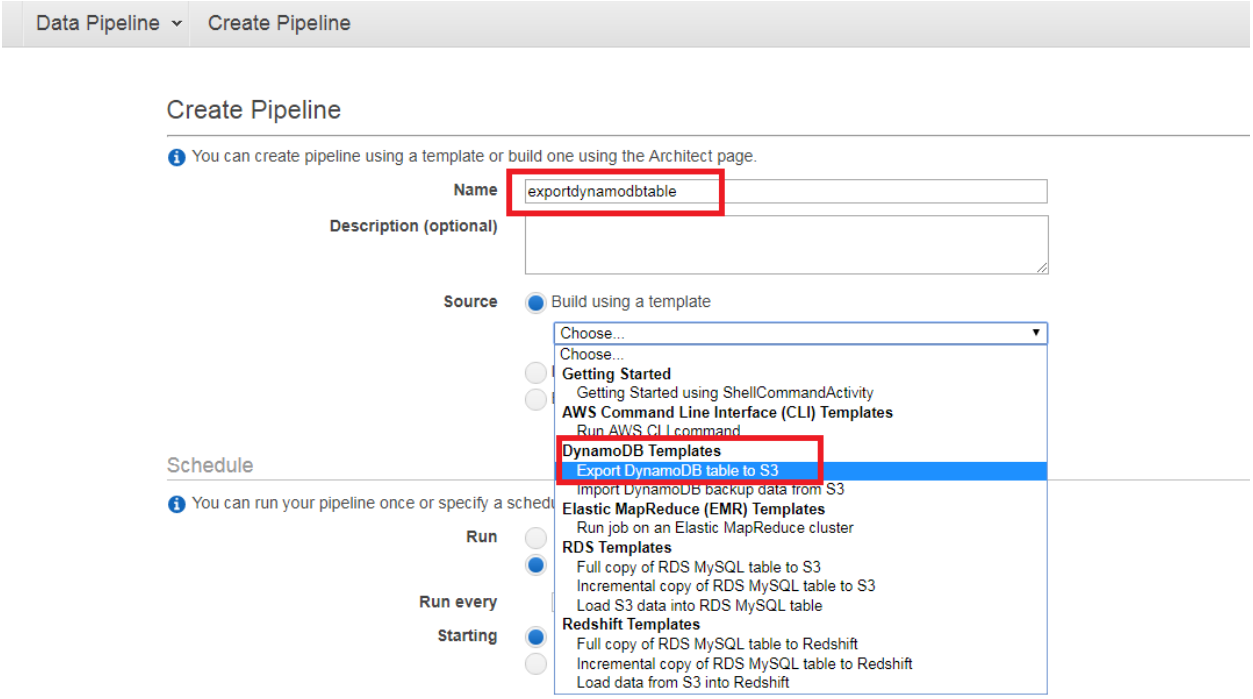
- Created tables can be downloaded using a Data Pipeline. To do that, navigate to Data pipeline from services.



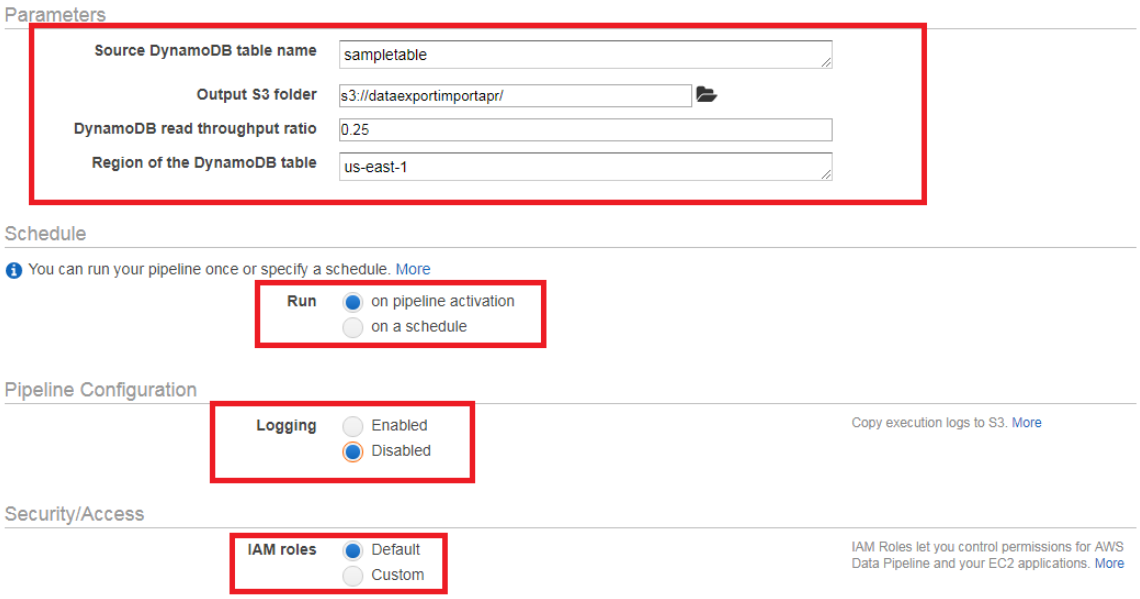
- Click on get started now.



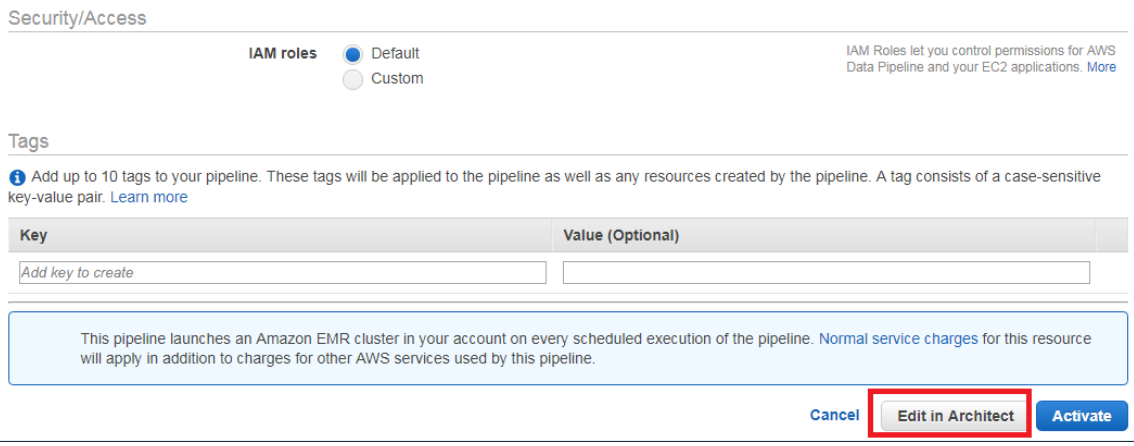
- Provide the name of the data pipeline and choose an existing template for exporting the table to S3.



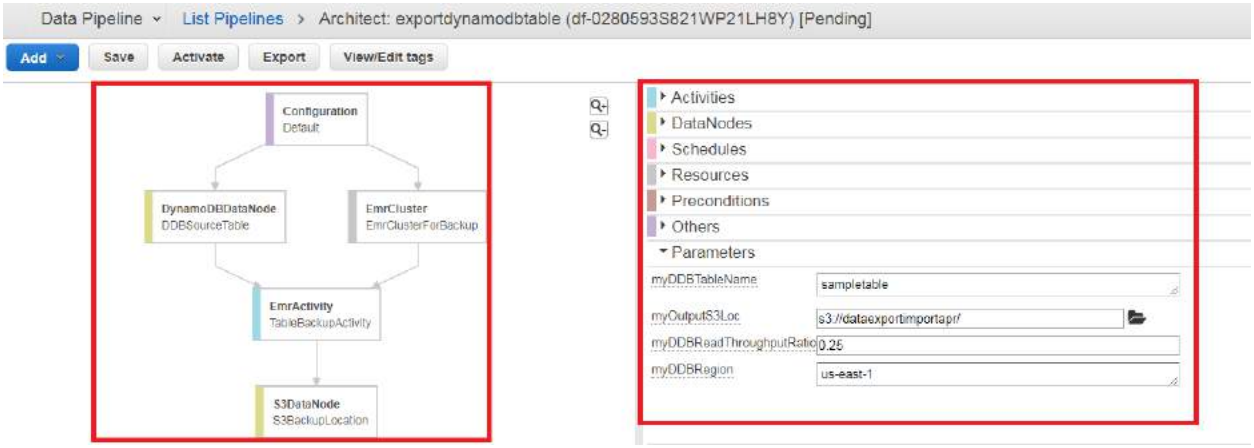
- Provide the table name which you need to export and choose the S3 bucket if you have existing one or create a new one, region of the table needs to be defined where it has been created. Choose on Pipeline activation and if the transaction logs is being required you could choose enable the logs.



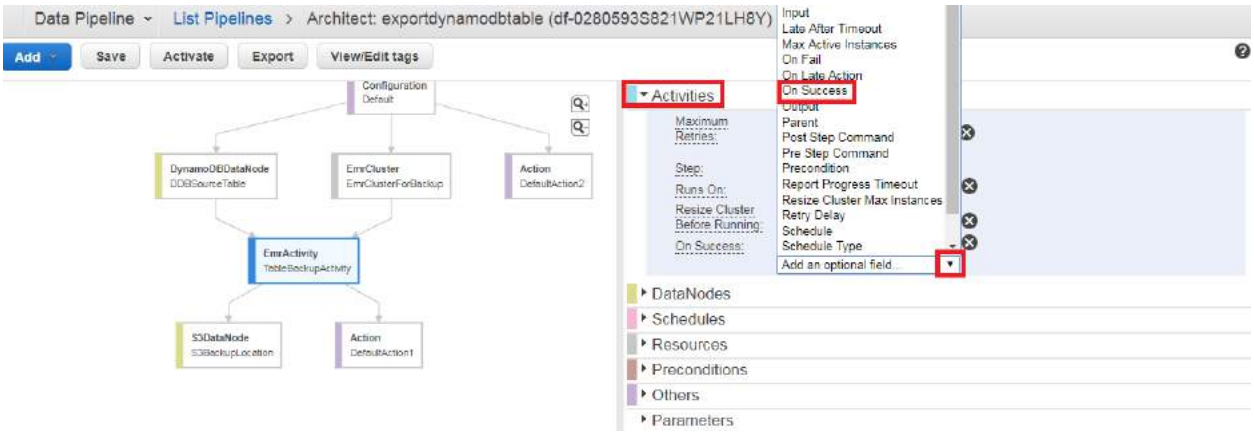
- Click on Edit in Architect for defining any alert rules for exporting the table like whether it has been successful or failed.



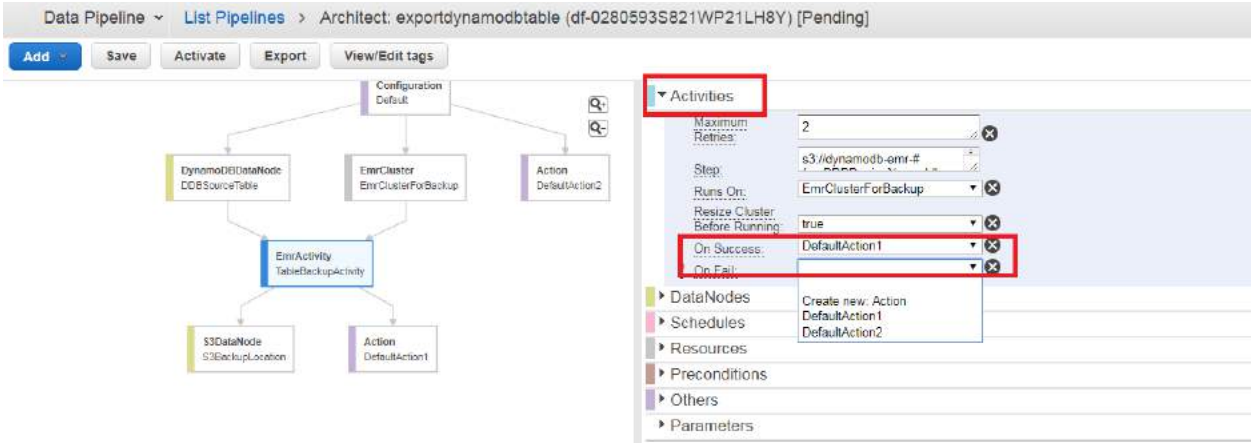
- Once you are done, it will be navigated to Pipeline list to see the created pipeline.



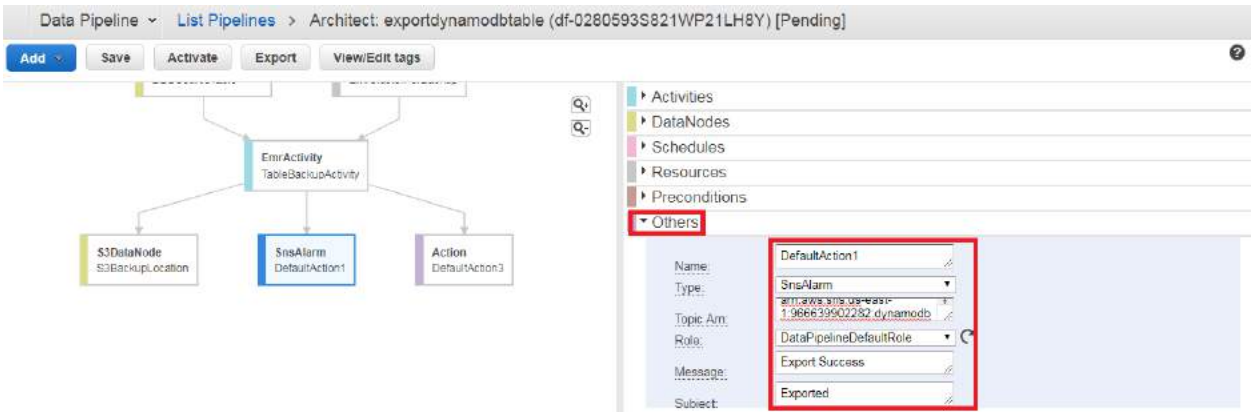
- Choose Activities Option for creating a new action item as Success and Fail.



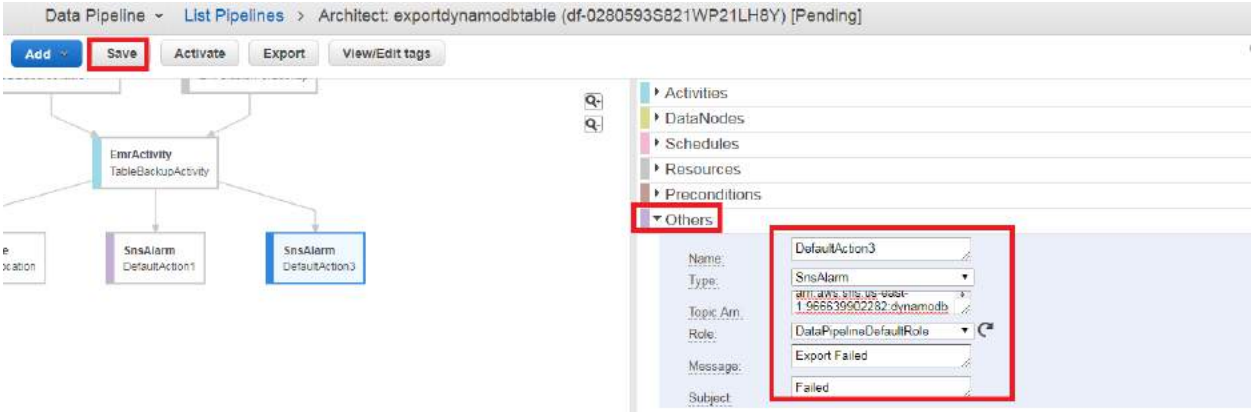
- Select create new action.



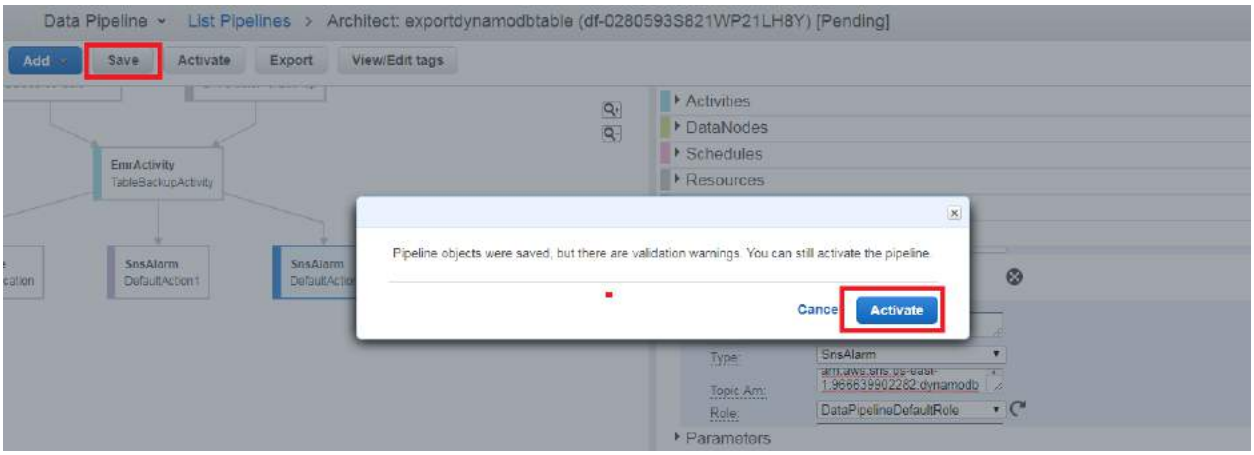
- Click on Others option for defining the SNS topic. SNS topic creation could be referred in below pages.



- Likewise, you need to do for both the action items which has been created in activities. Then click on Save.

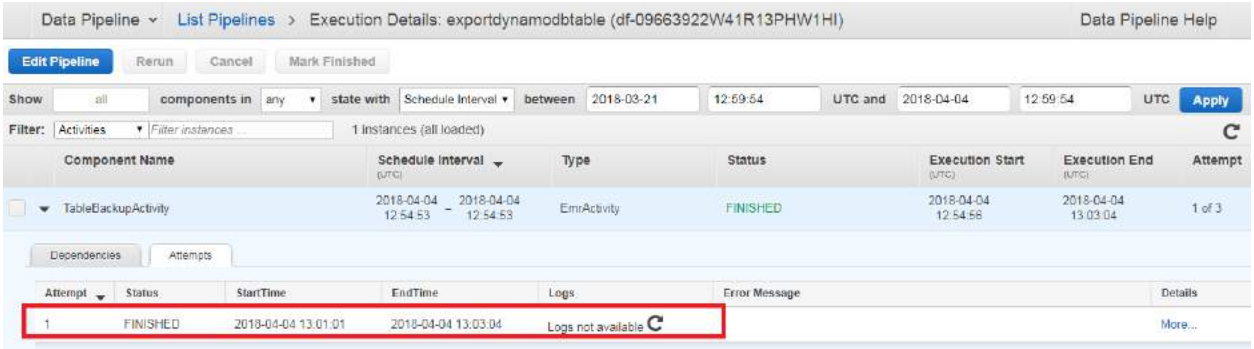


- It will prompt for activate and please proceed with that option.

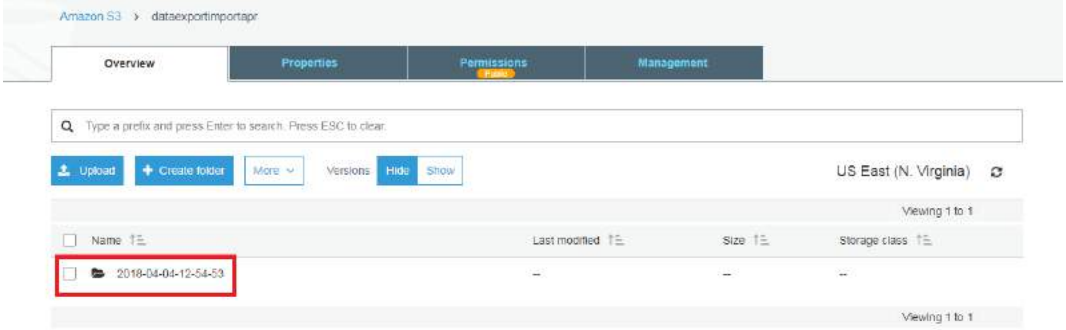


- Exporting the table is in progress. This would create an EC2 instance as an interface for exporting the table from DynamoDB to S3 bucket and the same will be deleted automatically after exporting the file. But please make sure to delete this pipeline once your testing activities gets completed. If required make sure all the instances has been terminated properly.

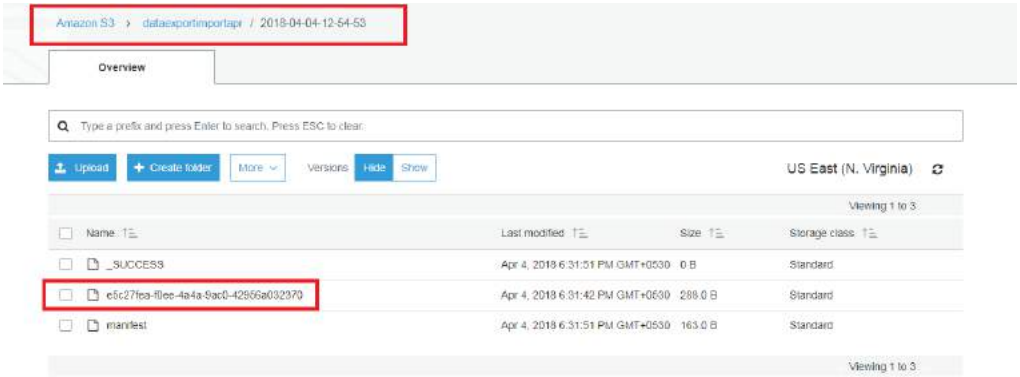
- Table export has been successful, and I have received an SMS on the same since I have been enabled SNS alerts for Phone Protocol.



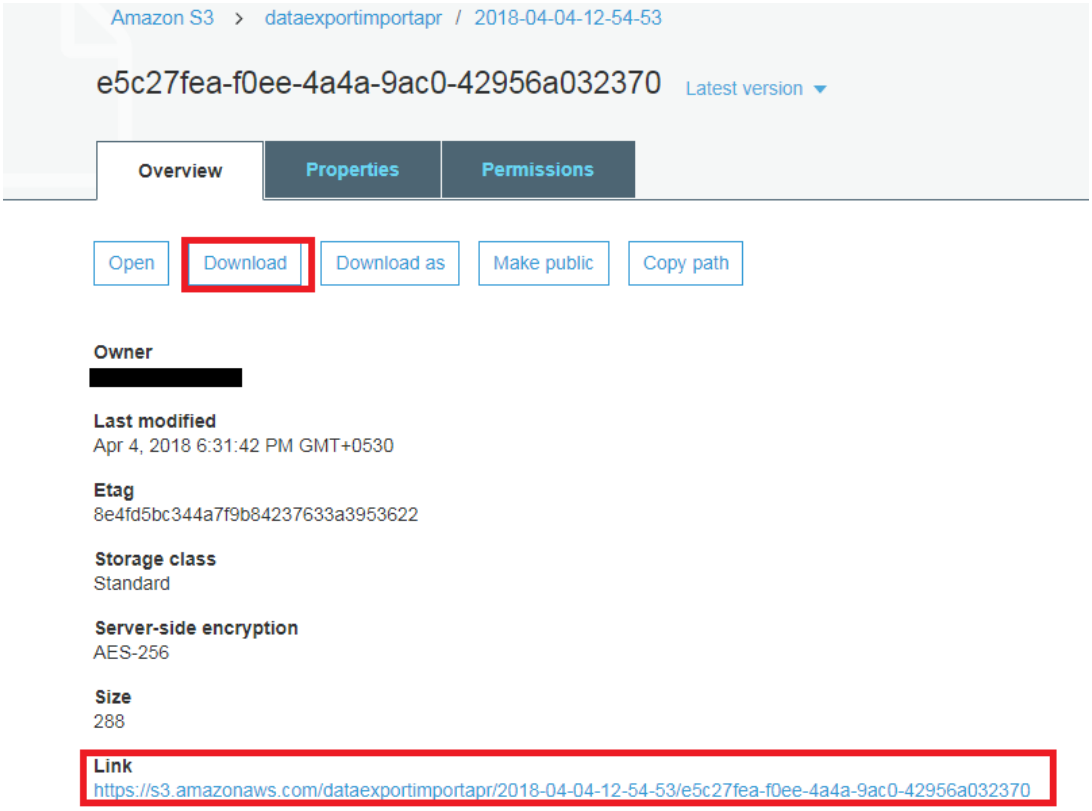
- Now, navigate to S3 bucket which has been used during pipeline creation.



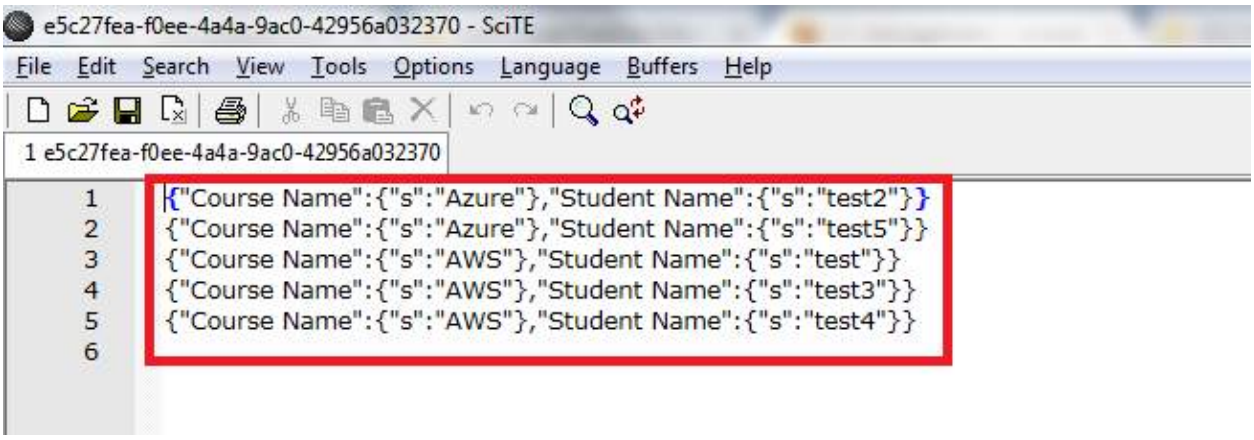
- Select the file which has been created and click on same



- Copy the link and download it or click on download option. If it is asking for permission, enable the same as make public access.



- Open the downloaded file in notepad or Scite to see the data which has been exported from DynamoDB using S3 and Data pipeline.

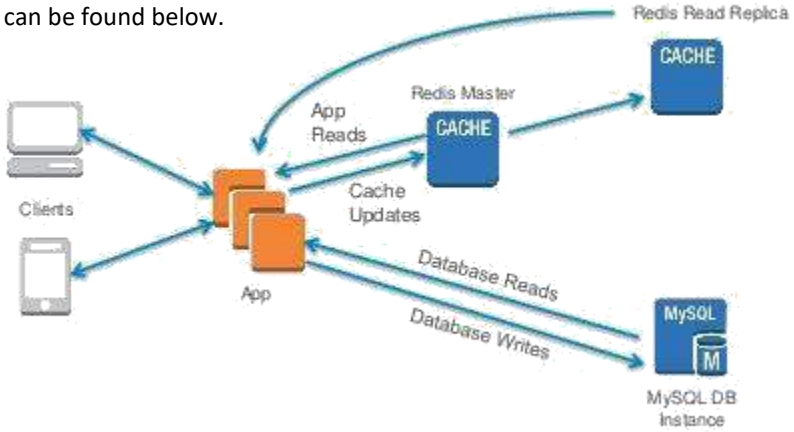


Advantages of DynamoDB:

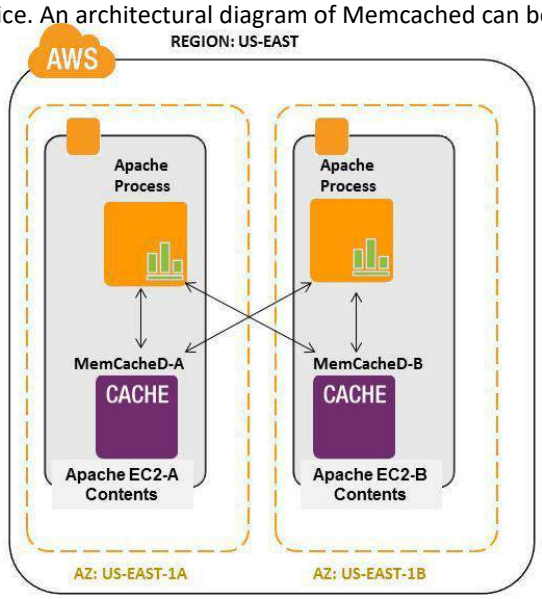
- Scalable – User can store unlimited amount of data.
- Distributed – DynamoDB scales horizontally by expanding a single table over multiple server
- Cost Effective – One-year free tier allows more than 40 million database operations/month and pricing is based on throughput (read/write per second) rather than storage
- Automatic data replication – All data items are stored on Solid State Disks (SSDs) and automatically replicated across multiple availability zones in a region
- Secure – DynamoDB uses proven secured methods to authenticate users and prevent unauthorized data access.

ElastiCache:

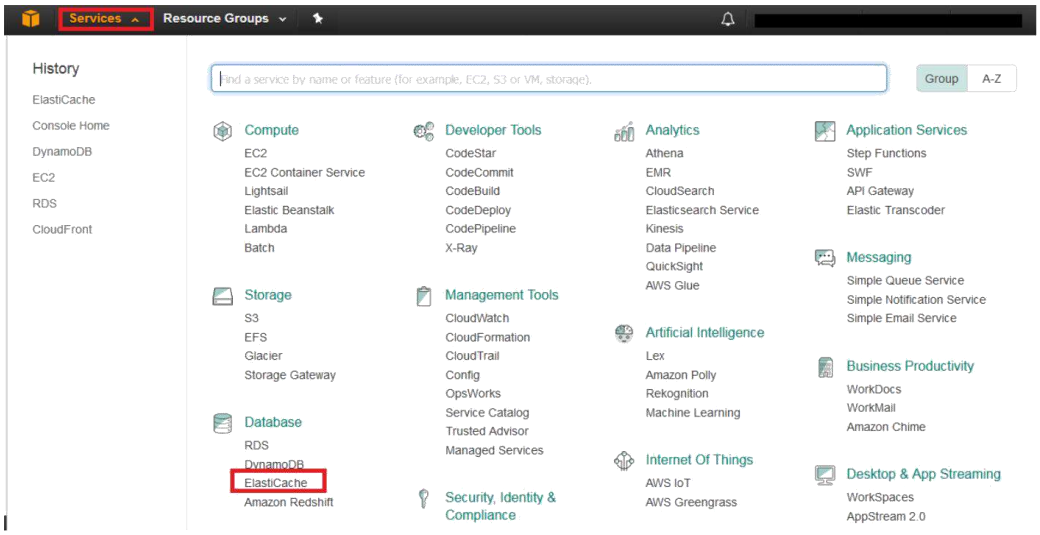
- Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.
- Amazon ElastiCache supports two open-source in-memory engines:
- **Redis -** a fast, open source, in-memory data store and cache. Amazon ElastiCache for Redis is a Redis-compatible in-memory service that delivers the ease-of-use and power of Redis along with the availability, reliability and performance suitable for the most demanding applications. Both single-node and up to 15-shard clusters are available, enabling scalability to up to 3.55 TB of in-memory data. ElastiCache for Redis is fully managed, scalable, and secure - making it an ideal candidate to power high-performance use cases such as Web, Mobile Apps, Gaming, Ad-Tech, and IoT. An architectural diagram of Redis cache can be found below.

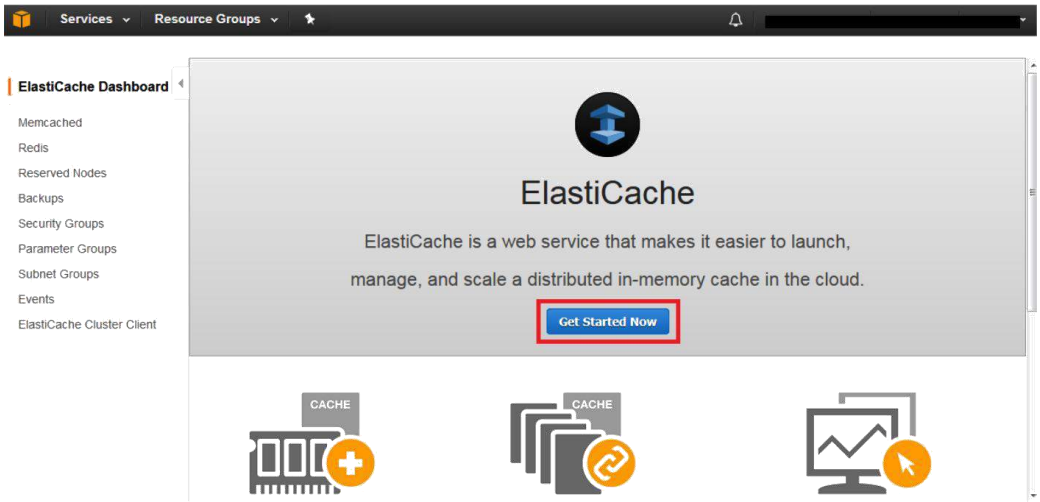


- **Memcached -** a widely adopted memory object caching system. ElastiCache is protocol compliant with Memcached, so popular tools that you use today with existing Memcached environments will work seamlessly with the service. An architectural diagram of Memcached can be found below.

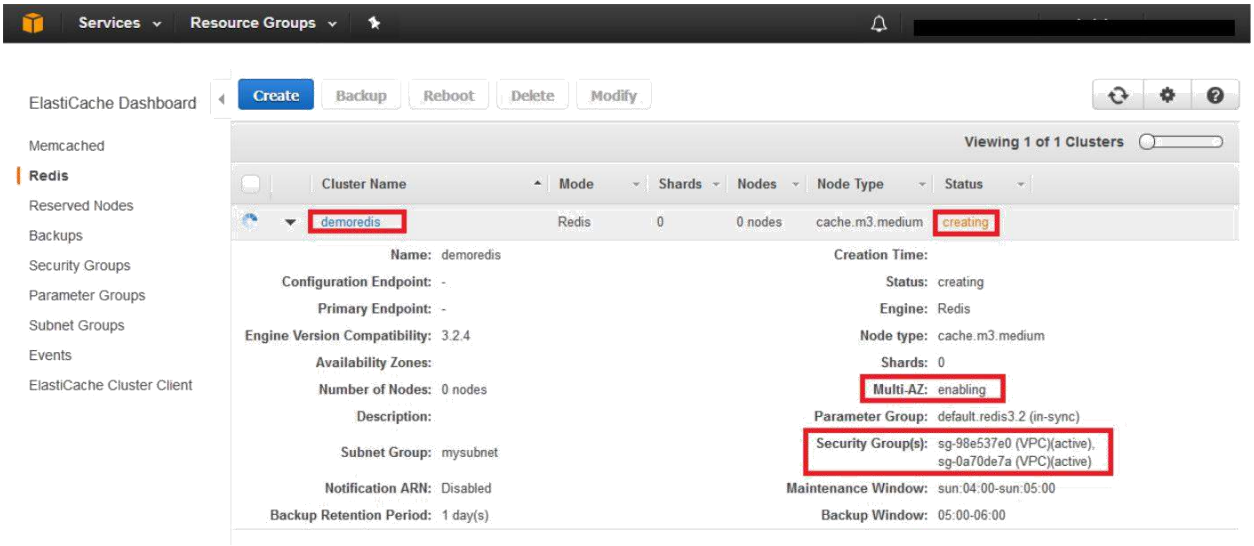


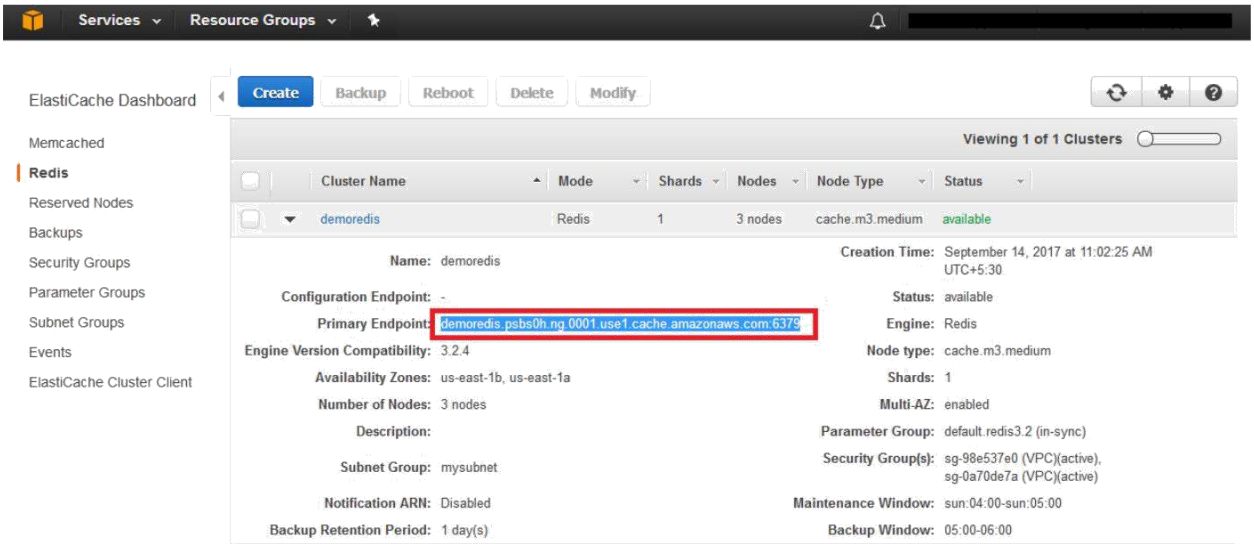
- Navigate to Services for ElastiCache and click on Get Started Now as like shown below.





- Choose the Redis for structure-based application, provide Name, Type, enable Multi-AZ with Auto Fail-Over, and choose the VPC if you have existing, select the Security Group which has 6379 port number is communicating globally.
- If required to take the back of created Redis, enable the same along with Frequency of back up and proceed to create the same.
- Generally, creation of cache would take around 5-10 minutes of time and once it is done, copy the Endpoint URL since it is acting as a service.





- Launch any Linux environment in EC2 under same VPC where this Redis has been created and install Telnet using the command "**yum install telnet**" which is like shown below.

```
root@localhost:/
[root@localhost /]# yum install telnet
Loaded plugins: fastestmirror, security
Determining fastest mirrors
base                                                                                                                    | 3.7 kB     00:00
extras                                                                                                                  | 3.4 kB     00:00
openlogic                                                                                                               | 2.9 kB     00:00
puppetlabs-deps                                                                                                         | 2.5 kB     00:00
puppetlabs-deps/primary_db                                                                                              |  27 kB     00:00
puppetlabs-products                                                                                                     | 2.5 kB     00:00
puppetlabs-products/primary_db                                                                                          | 170 kB     00:00
updates                                                                                                                 | 3.4 kB     00:00
updates/primary_db                                                                                                      | 3.6 MB     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package telnet.x86_64 1:0.17-48.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================================
 Package                          Arch                          Version                                  Repository                        Size
================================================================================================================================================
Installing:
 telnet                           x86_64                        1:0.17-48.el6                            base                              58 k

Transaction Summary
================================================================================================================================================
Install       1 Package(s)

Total download size: 58 k
Installed size: 109 k
Is this ok [y/N]: y
Downloading Packages:
telnet-0.17-48.el6.x86_64.rpm                                                                                           |  58 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : 1:telnet-0.17-48.el6.x86_64                                                                                                  1/1
  Verifying  : 1:telnet-0.17-48.el6.x86_64                                                                                                  1/1

Installed:
  telnet.x86_64 1:0.17-48.el6

Complete!
```

- After installing the telnet, copy the primary Endpoint and connect to Redis using the Linux environment which we have been created. After connecting to Redis cache, type the cache commands based on your application need. You can feed any information in the cache like database tables, procedures, triggers, functions, so that instead of communicating to Database server, cache will be giving the information if any user asked for it.

```
[root@ip-192-168-1-37 ~]# telnet demoredis.psbs0h.ng.0001.use1.cache.amazonaws.com 6379
Trying 192.168.0.99...
Connected to demoredis.psbs0h.ng.0001.use1.cache.amazonaws.com.
Escape character is '^]'.
set a 'HelloWord'
+OK
get a
$9
HelloWord
set b 'This is Testing Redis cache to find out how quick we get the content from database'
+OK
get b
$82
This is Testing Redis cache to find out how quick we get the content from database
```

- Delete the Redis Cache by selecting the same and choose Delete option like shown below.

- Find the below given URL to get more commands on Redis Cache.
- https://redis.io/commands

Advantages of ElastiCache:

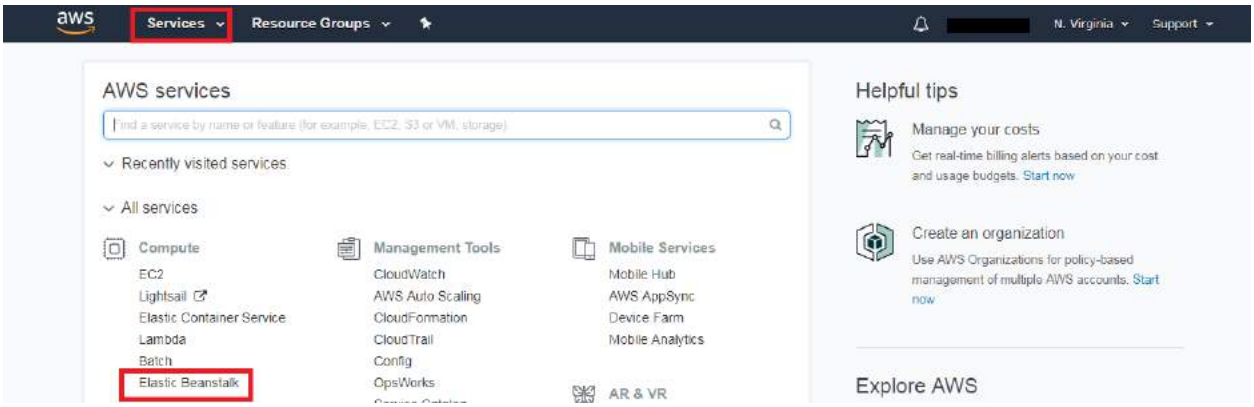
- Redis supports complex data types, such as strings, hashes, lists, and sets.
- Redis sorts or ranks in-memory data-sets.
- Redis provides persistence for your key store.
- Redis replicates the cache data from the primary to one or more read replicas for read intensive applications.
- Redis has automatic fail-over capabilities if the primary node fails.
- Redis has publish and subscribe (pub/sub) capabilities where the client is informed of events on the server.
- Redis has back-up and restore capabilities.
- Memcached is the simplest caching model.
- Memcached is helpful for people needing to run large nodes with multiple cores or threads.
- Memcached offers the ability to scale out/in, adding and removing nodes on-demand.
- Memcached handles partitioning data across multiple shards.
- Memcached handles cache objects, such as a database.
- Memcached may be necessary to support an existing Memcached cluster.

Elastic Beanstalk:

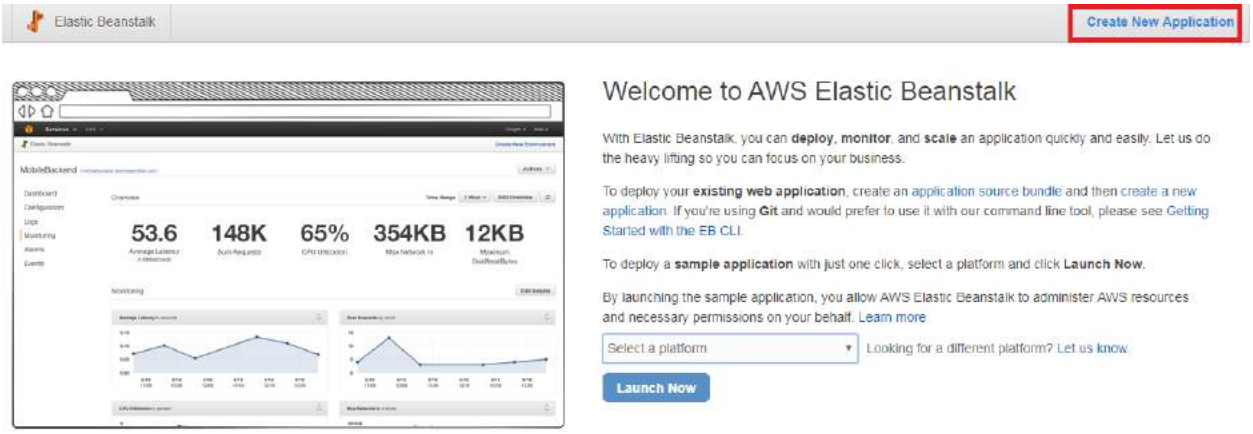
- With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

- Elastic Beanstalk supports applications developed in Java, PHP, .NET, Node.js, Python, and Ruby, as well as different container types for each language. A container defines the infrastructure and software stack to be used for a given environment. When you deploy your application, Elastic Beanstalk provisions one or more AWS resources, such as Amazon EC2 instances. The software stack that runs on your Amazon EC2 instances depends on the container type. For example, Elastic Beanstalk supports two container types for Node.js: a 32-bit Amazon Linux image and a 64-bit Amazon Linux image.

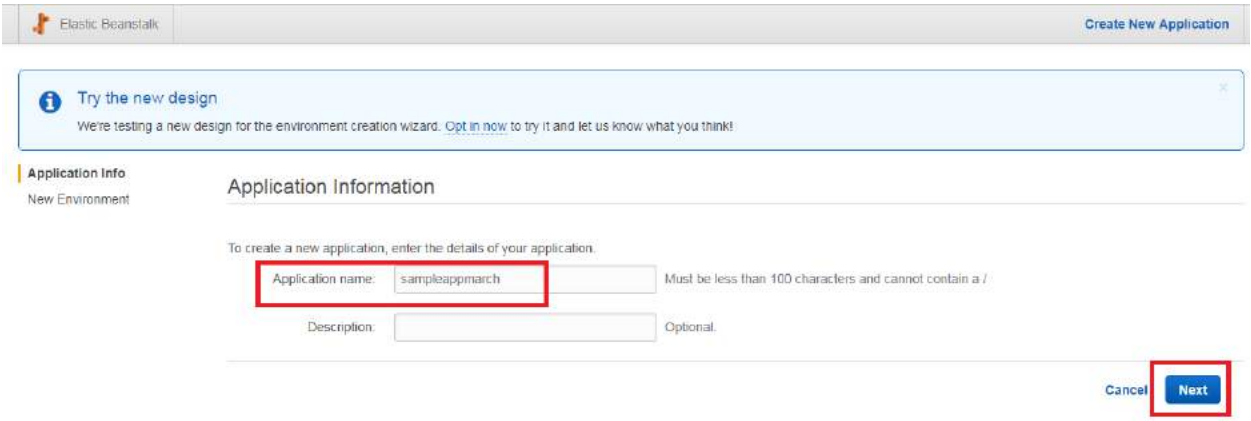
- Click on Services and choose Elastic Beanstalk.



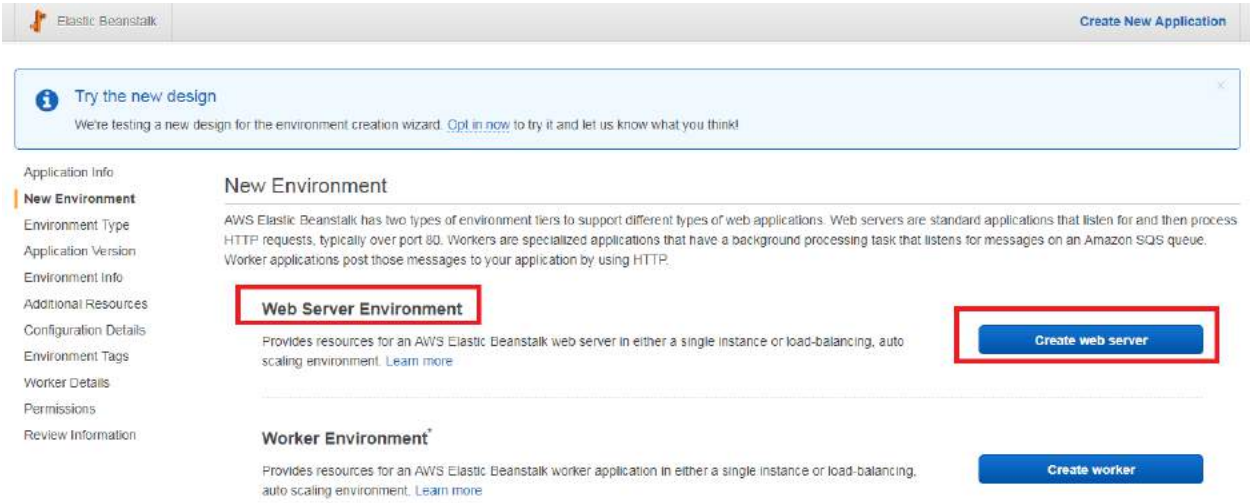
- Click on Create New Application to deploy it and test it. If you click on Select Platform Dropdown and choose the technology, environment would be launched by default values. If you want to choose your own environment, click on create new application.



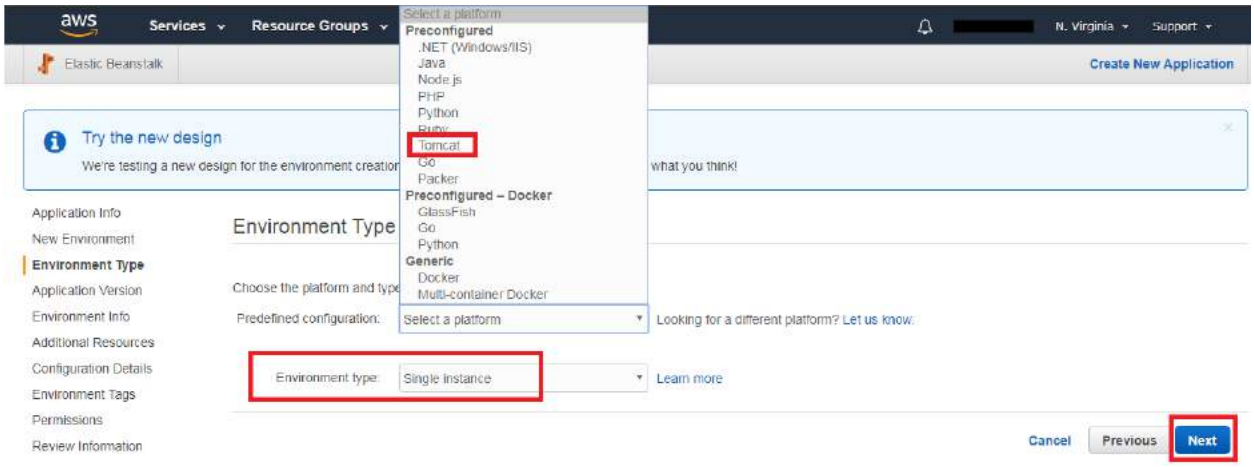
- Provide an Application Name and description if required and click on Next.



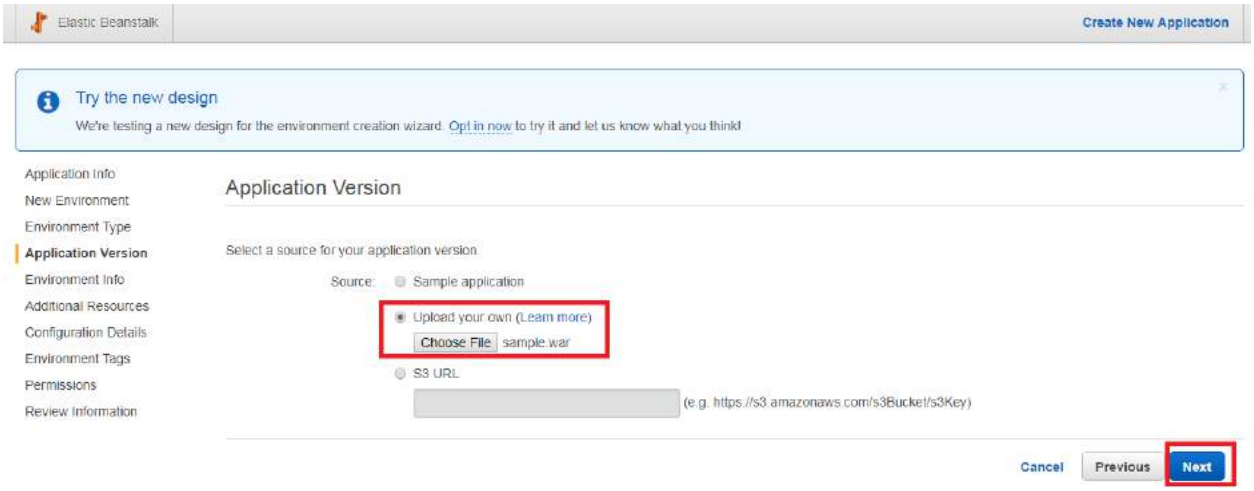
- If you are about to test an independent application in a browser, you could choose Web Server Environment. In case if your application requires any dependency tasks like messaging queue, you could choose Worker Environment.



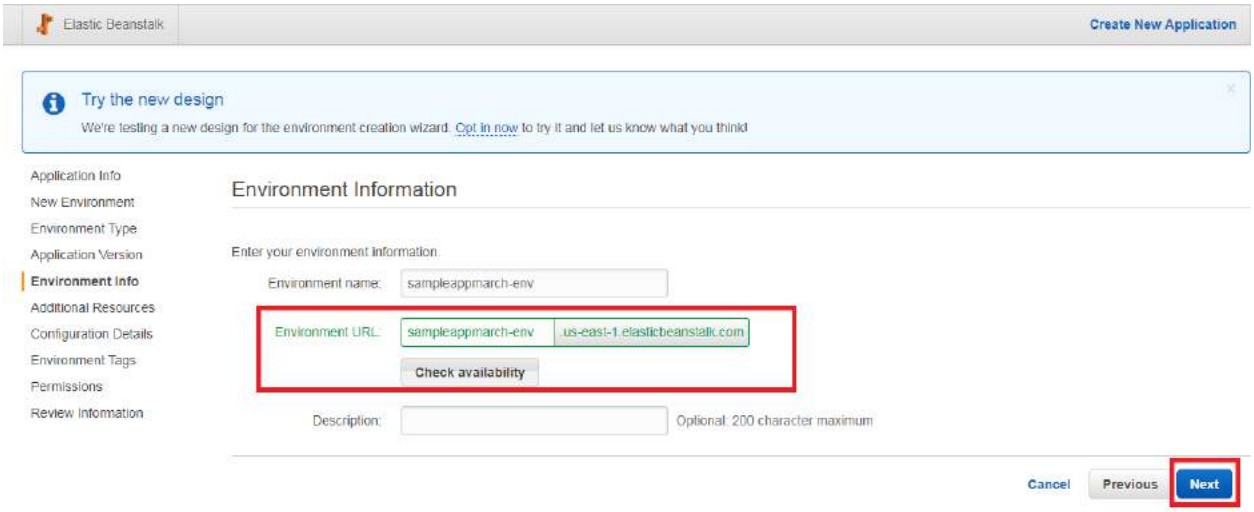
- Choose the Web Server / Technology which you would like to deploy and validate. If LB and Auto Scaling is required, you can change an Environment type.



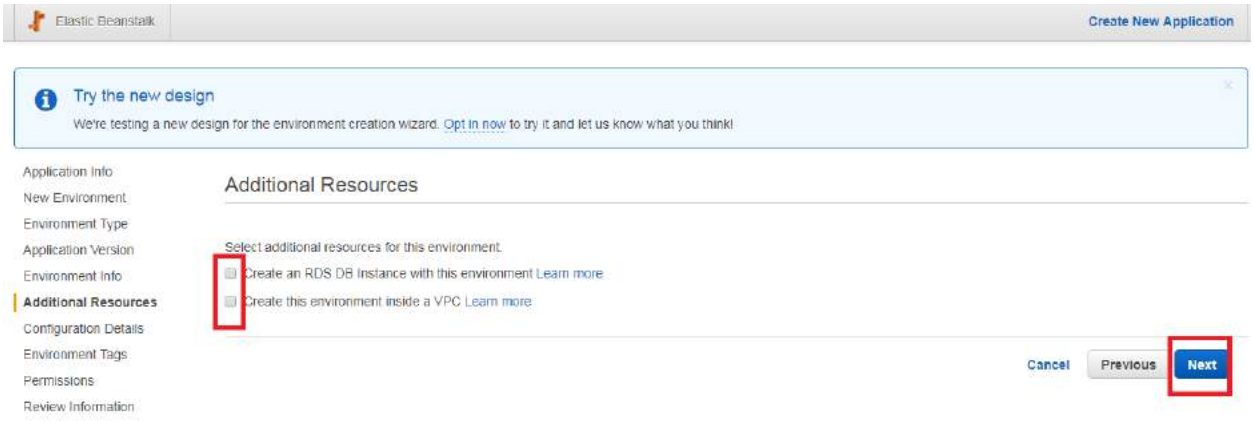
- Upload the sample war file of Tomcat which could be downloaded from Internet or from below given URL, since we have been chosen Tomcat as Web Server.
- https://drive.google.com/file/d/1GvMwXU-BqFK6Xkm3VUtVXhPjRJVnKoyH/view?usp=sharing



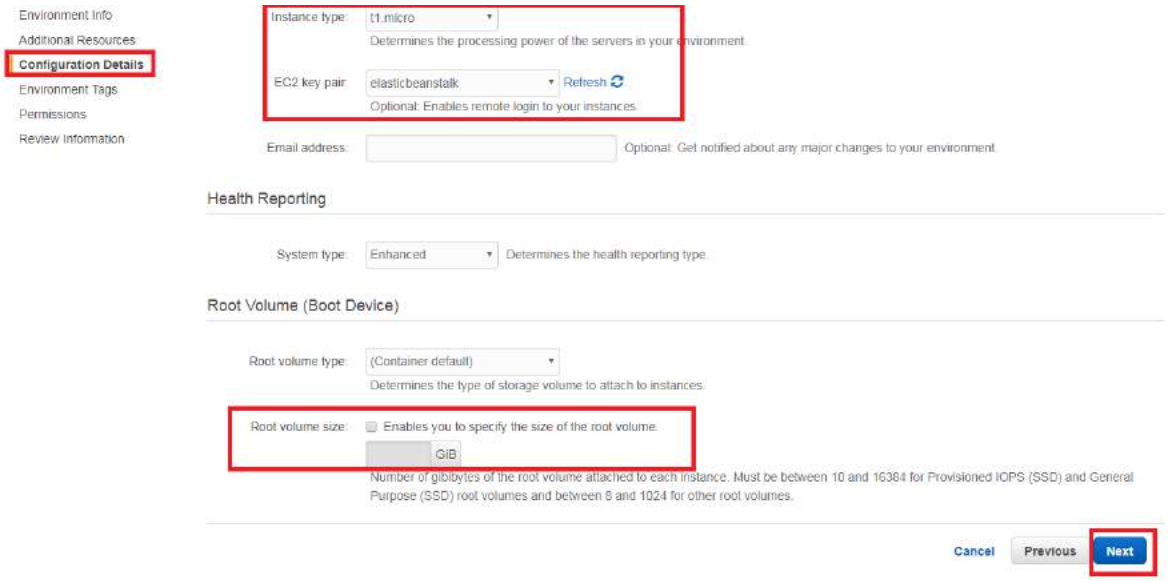
- Check for an URL whether it is available. If it is not, you supposed to change this URL name.



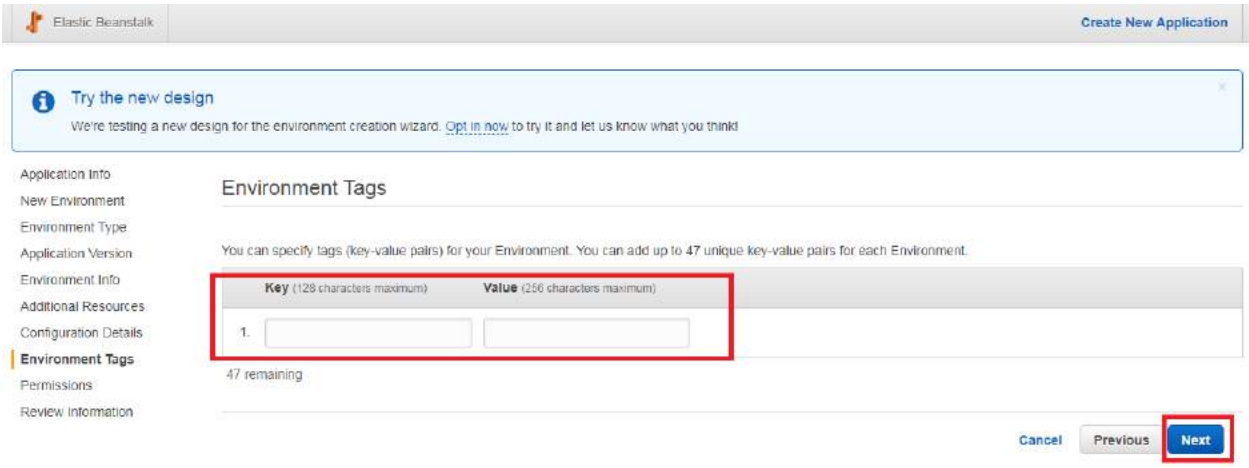
- If this application requires any Backend server like RDS, you could select the same.



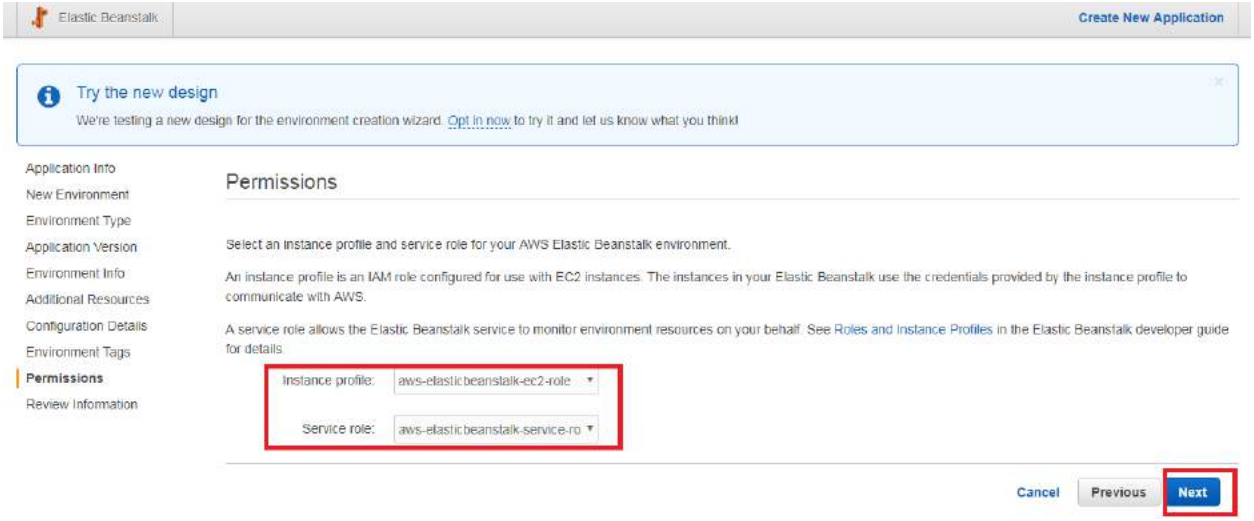
- Provide the instance type / configuration which is based on application functionality / performance and remaining could be default values unless any changes in HDD size / root volume of Web Server.



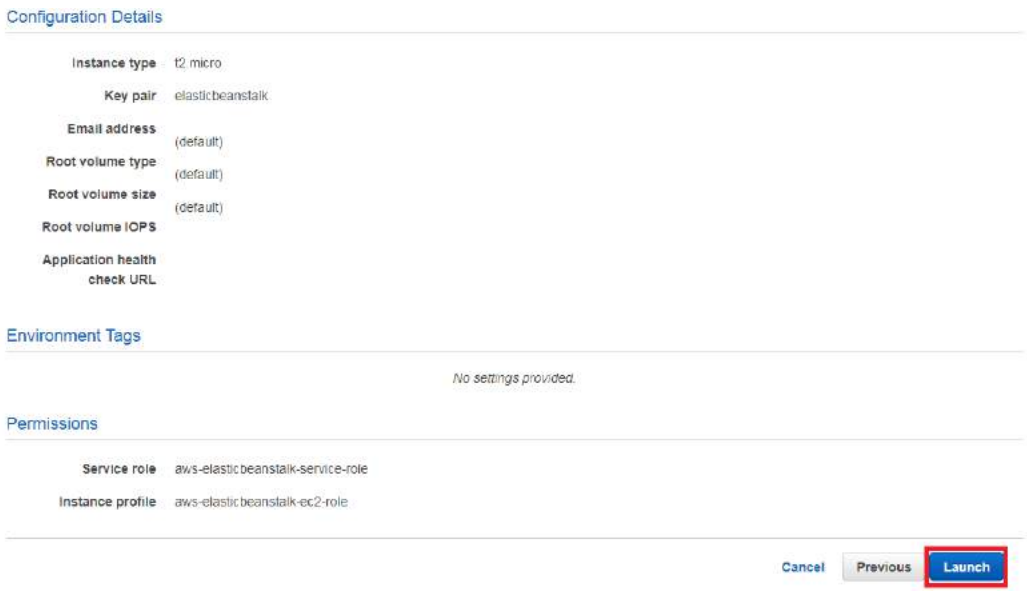
- Provide the tags if necessary.



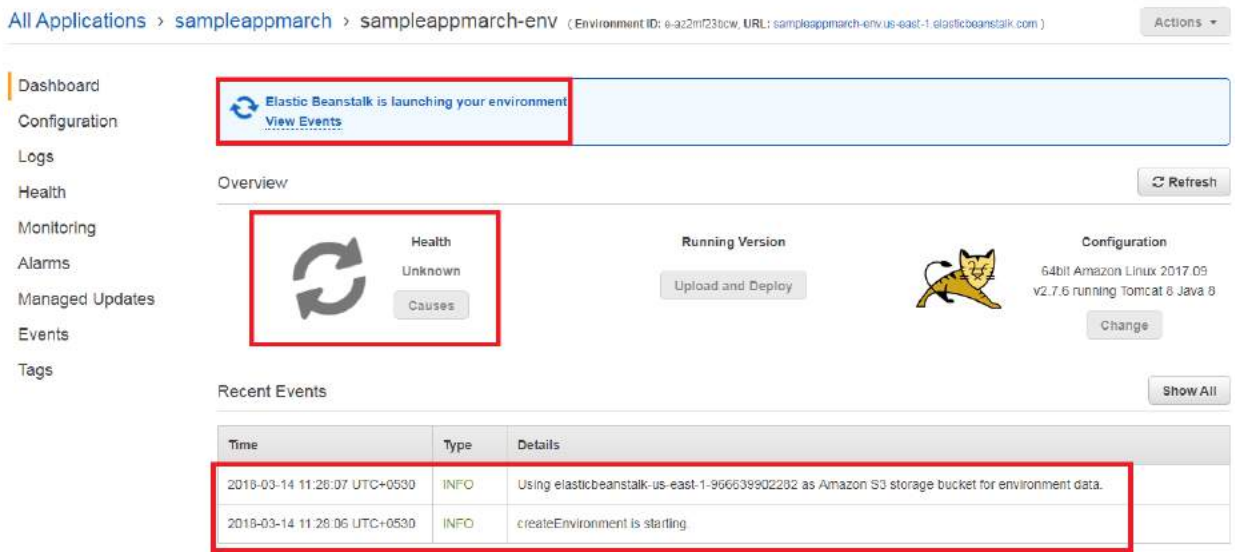
- By default, this role will be chosen to access S3 and to monitor the environment.



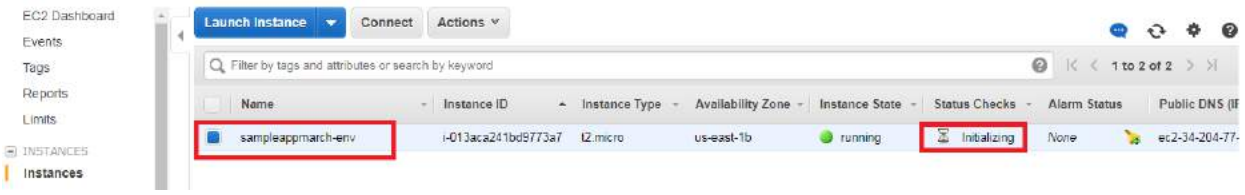
- Review the chosen items and click on Launch.

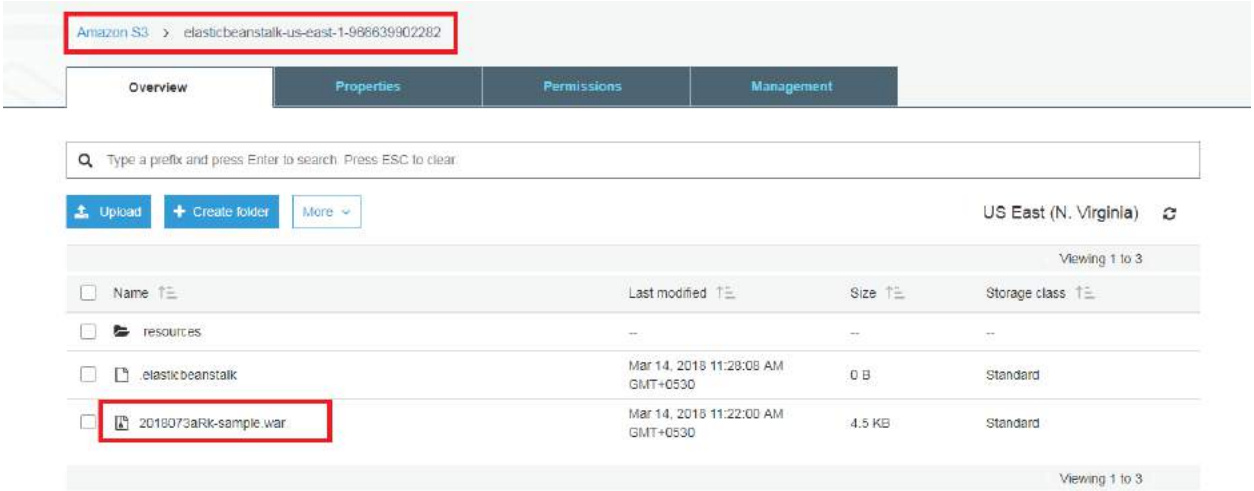


- Elastic Beanstalk provisioning is in progress and it would takes around 5-8 minutes of time. Status of provisioning each service can be visible in recent events.

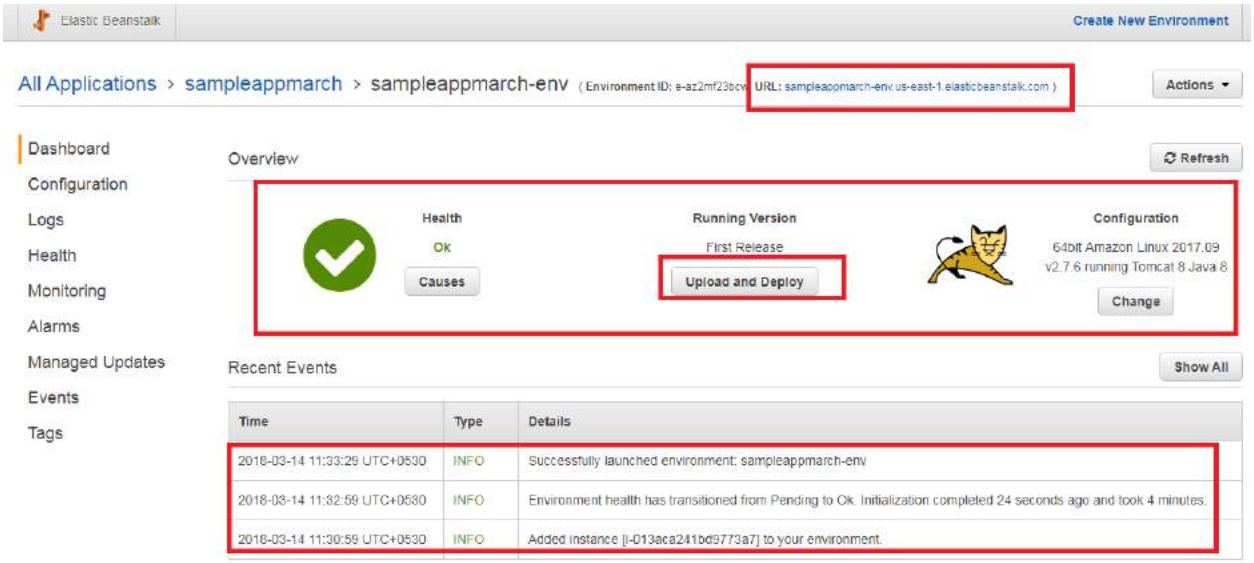


- Parallelly, EC2 instances are provisioning automatically along with S3 bucket creation.

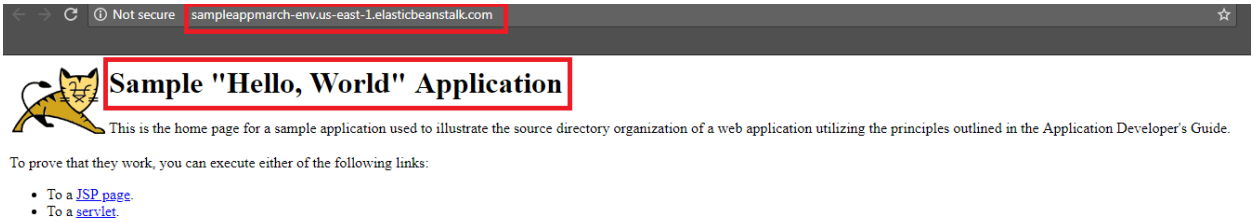




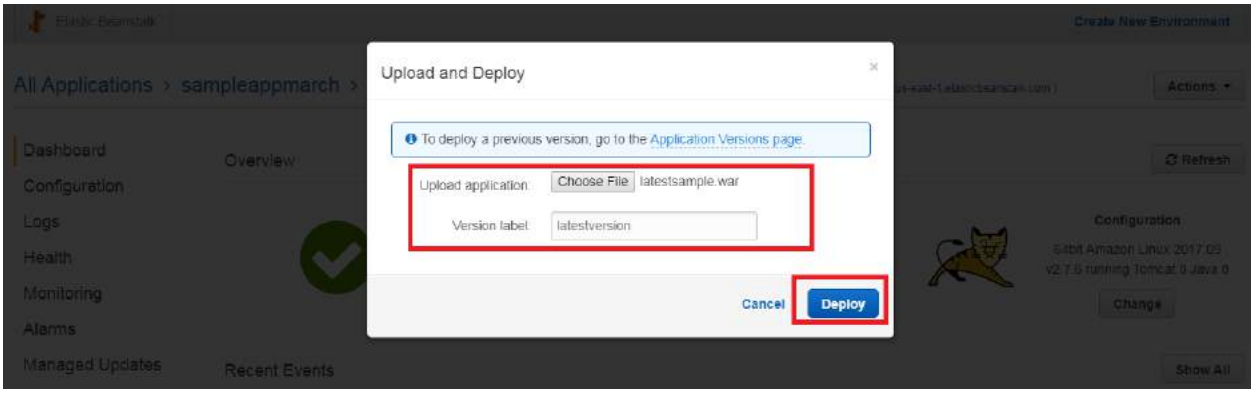
- Once the environment is being created, you could able to access an application using the URL.

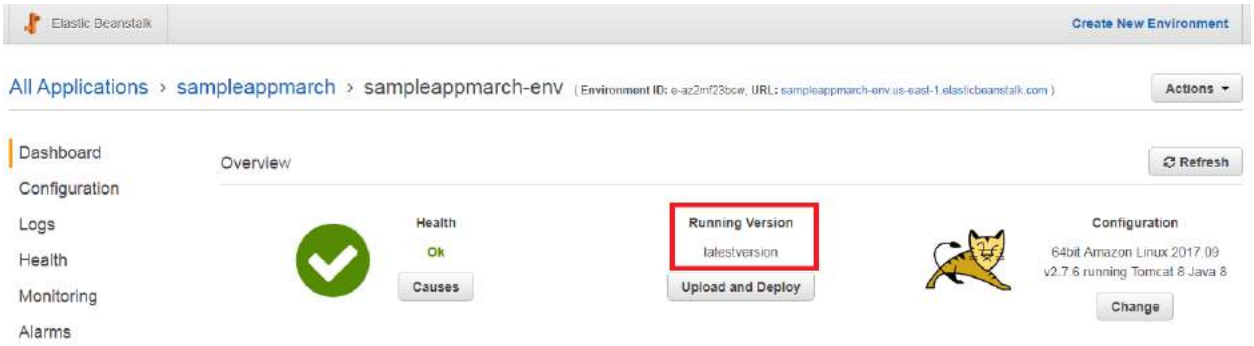


- Application is working fine as expected.

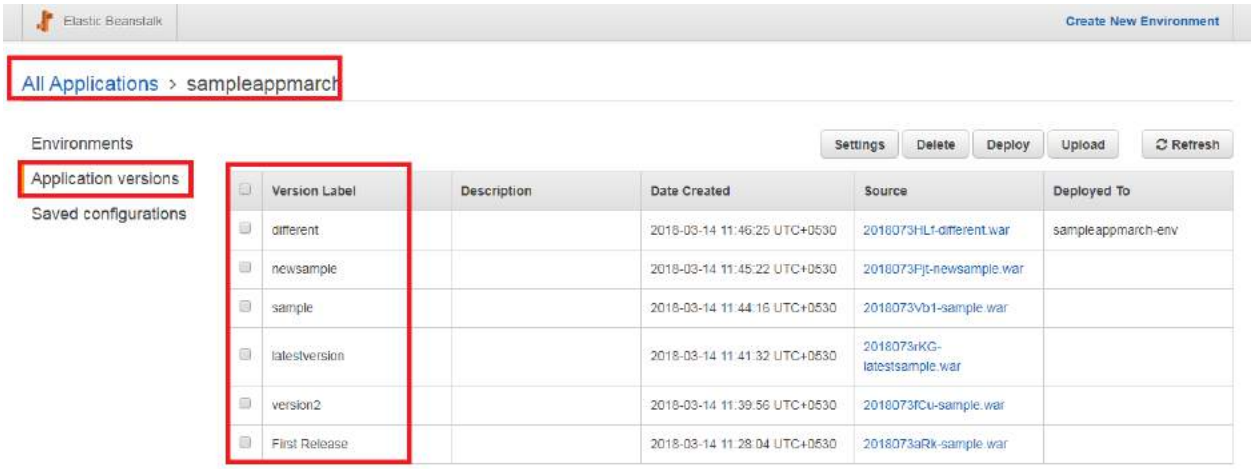


- In case of any version management / to test a new release, same can be done in this already created Beanstalk. Upload the latest version of war file with a different name and validate it with same URL.

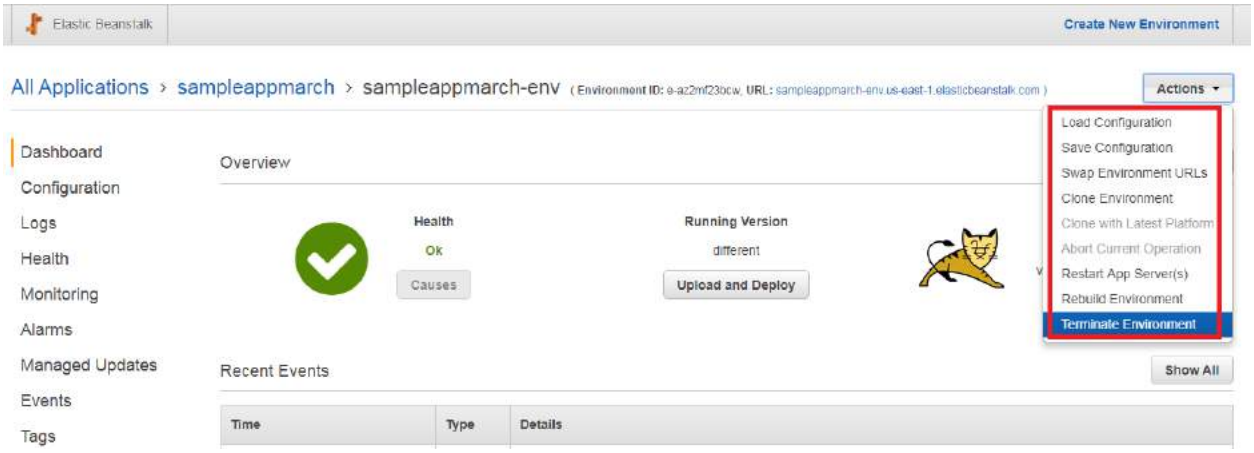




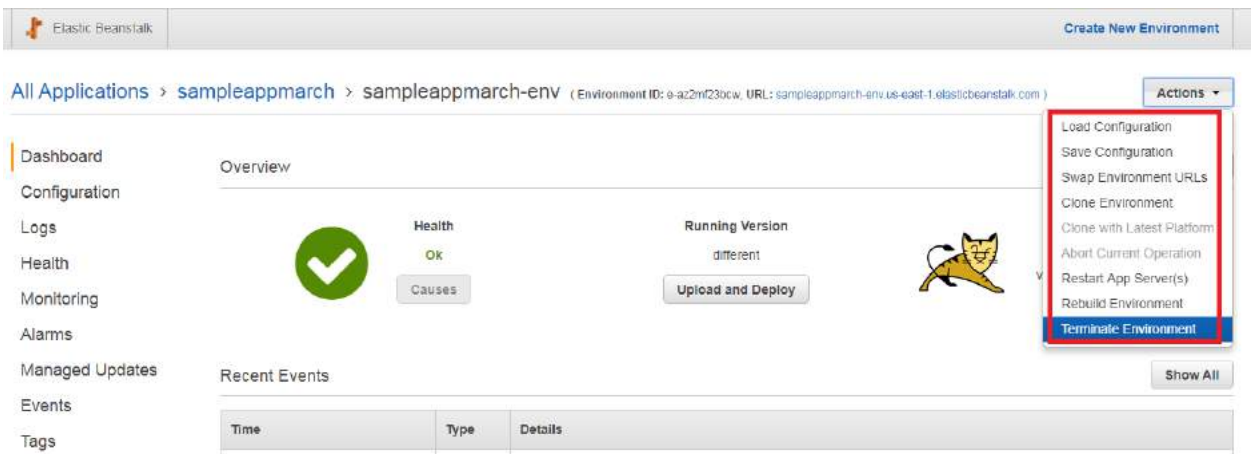
- To maintain a version management of list of uploaded war files, same be like below screenshot.



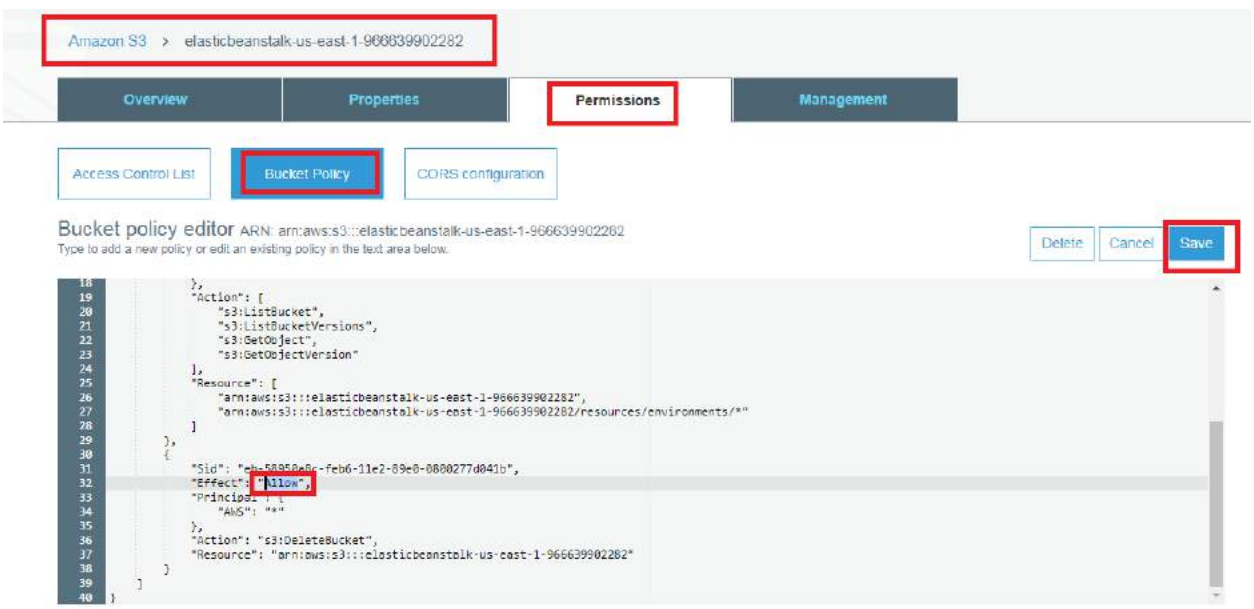
- Click on Actions and choose terminate environment to delete the created Elastic Beanstalk.



- Confirm the deletion by providing the name of Beanstalk.



- To delete the S3 bucket, you need to change the permission to Allow state as like given below.



Advantages of Elastic Beanstalk:

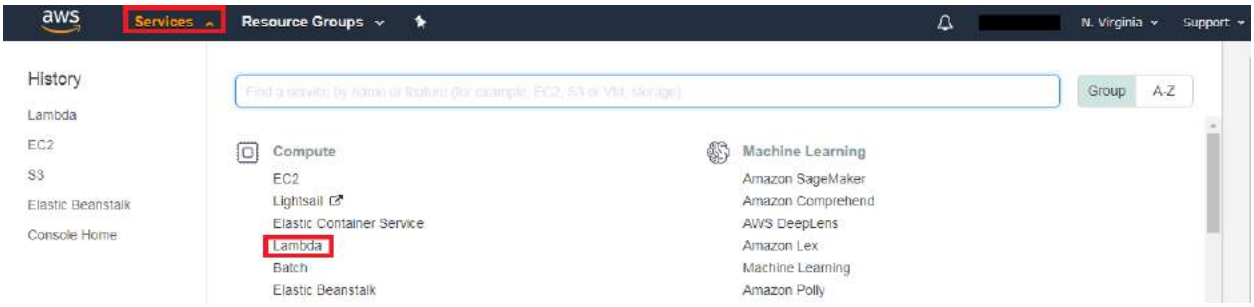
- Get the ability to deploy a variety of applications on AWS, coded in a variety of programming languages like PHP, Java, Python, Ruby, Node.js, and Go
- Support for web and application containers, including Docker.
- Selection of the most appropriate EC2 instance types that match the processing and memory requirements of your application.
- Support for both Linux and Windows Server based environments.
- Full control over the AWS resources that power your app, along with the complete ability to adjust the various configurations and settings right from the Elastic Beanstalk management console.
- Automatic scaling using Auto Scaling, with easy configuring of metrics and thresholds that determine when to add or remove instances from an environment.
- Immediate and direct troubleshooting via direct login access to Amazon EC2 instances.
- The ability to run your apps in multiple Availability Zones, thereby easily improving reliability.
- Enhanced security via enabling of the HTTPS protocol on the load balancer.
- Deployment of new versions to running environments using different deployment options.
- Effortless rollbacks to previous versions.
- Access to CloudWatch monitoring metrics like CPU utilization, request count, and latency.
- Ability to run other application components like memory caching, side by side in Amazon EC2.

Lambda:

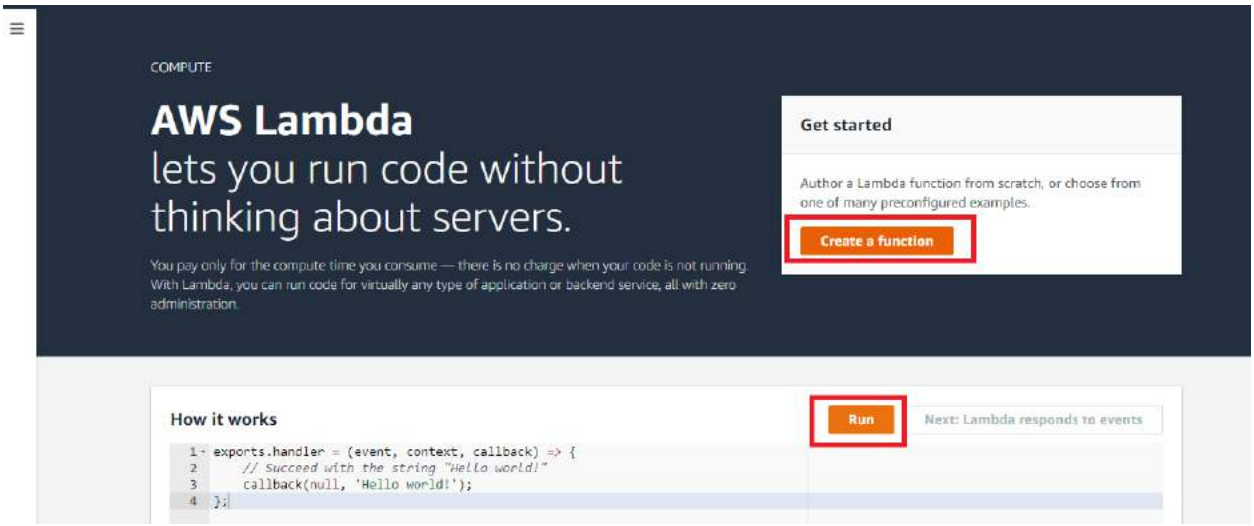
- AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging. All you need to do is supply your code in one of the languages that AWS Lambda supports (currently Node.js, Java, C#, Go and Python).

- You can use AWS Lambda to run your code in response to events, such as changes to data in an Amazon S3 bucket or an Amazon DynamoDB table; to run your code in response to HTTP requests using Amazon API Gateway; or invoke your code using API calls made using AWS SDKs. With these capabilities, you can use Lambda to easily build data processing triggers for AWS services like Amazon S3 and Amazon DynamoDB process streaming data stored in Kinesis or create your own back end that operates at AWS scale, performance, and security.

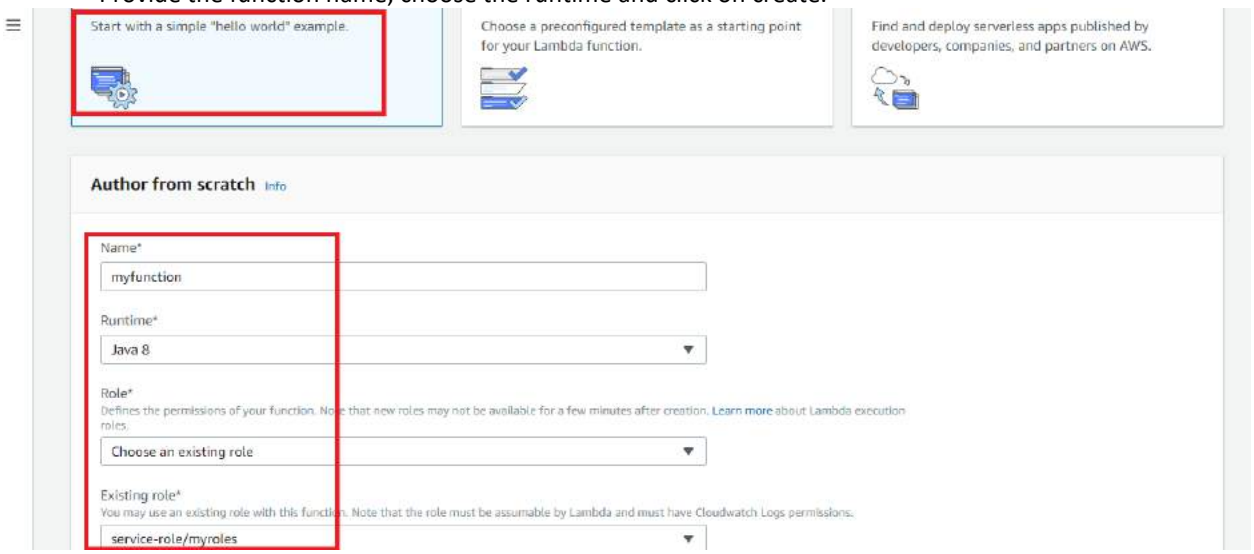
- Click on Services and select Lambda to create a new one.



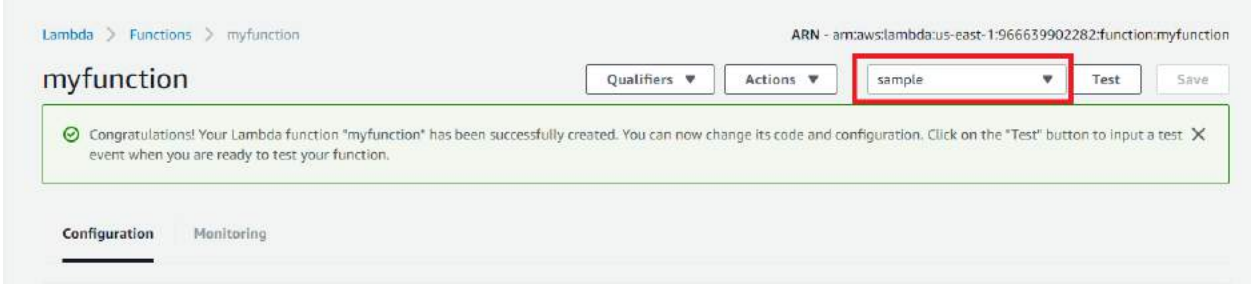
- If you want to run a sample code same can be validated if you click on Run and if you want to create a new function, select the same appropriately.



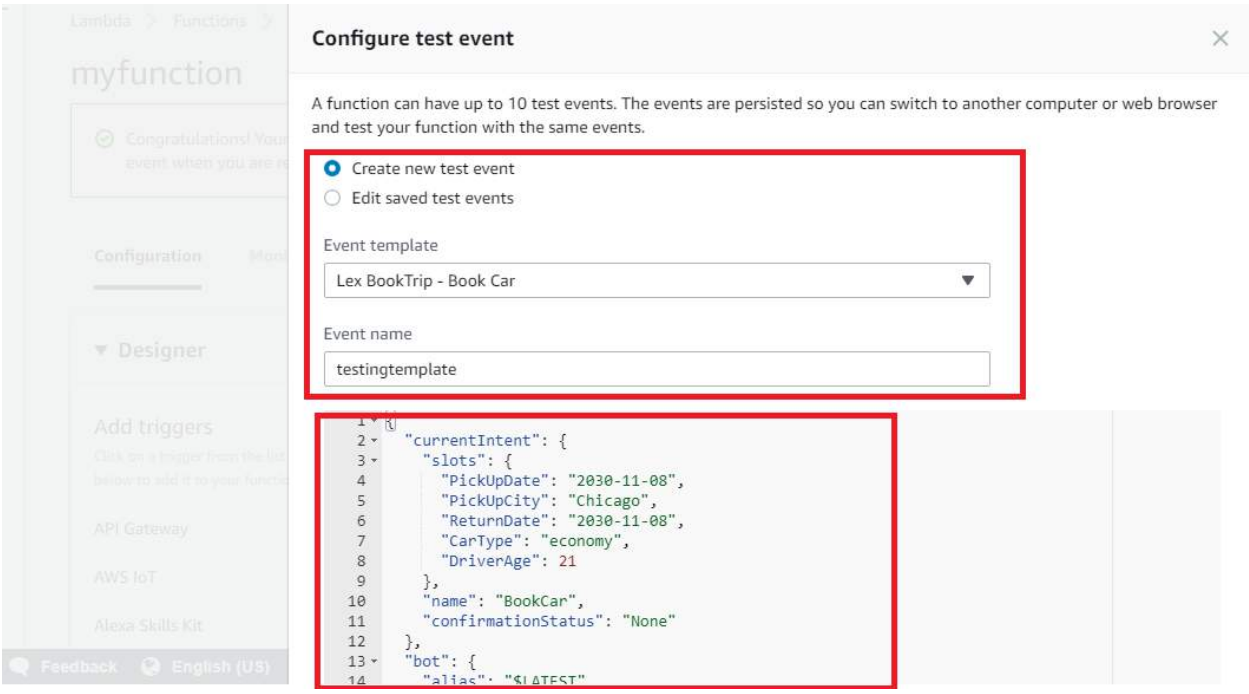
- Provide the function name, choose the runtime and click on create.



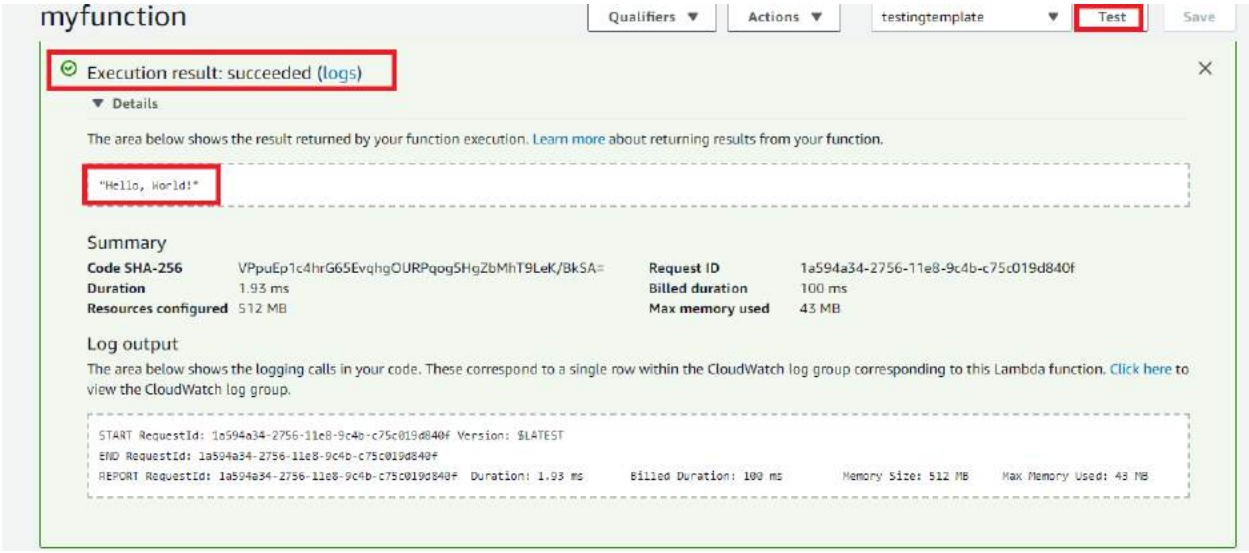
- Select the drop down to write your own coding.



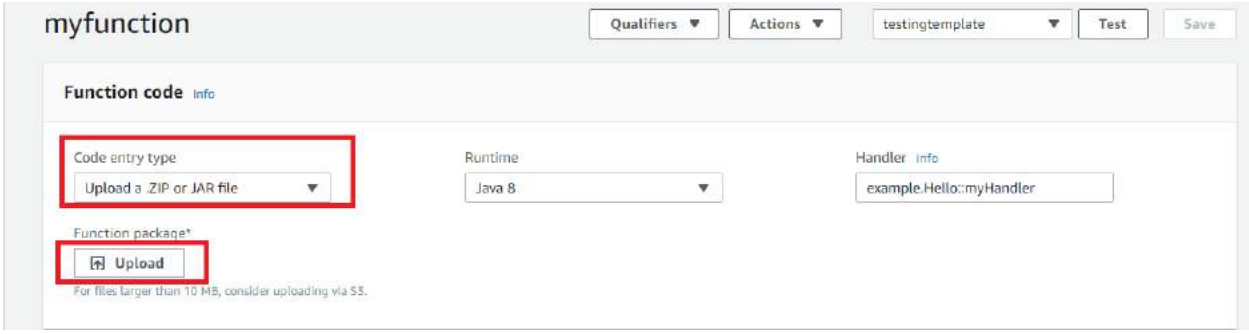
- Create a new test event and choose an existing template and provide the Event Name.



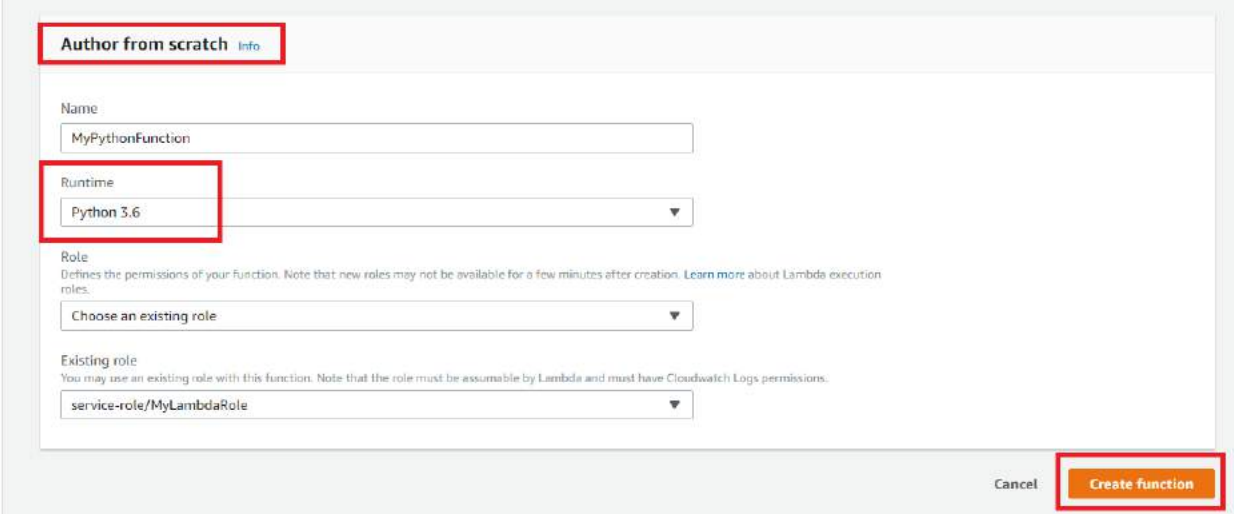
- Click on Test to execute the same.



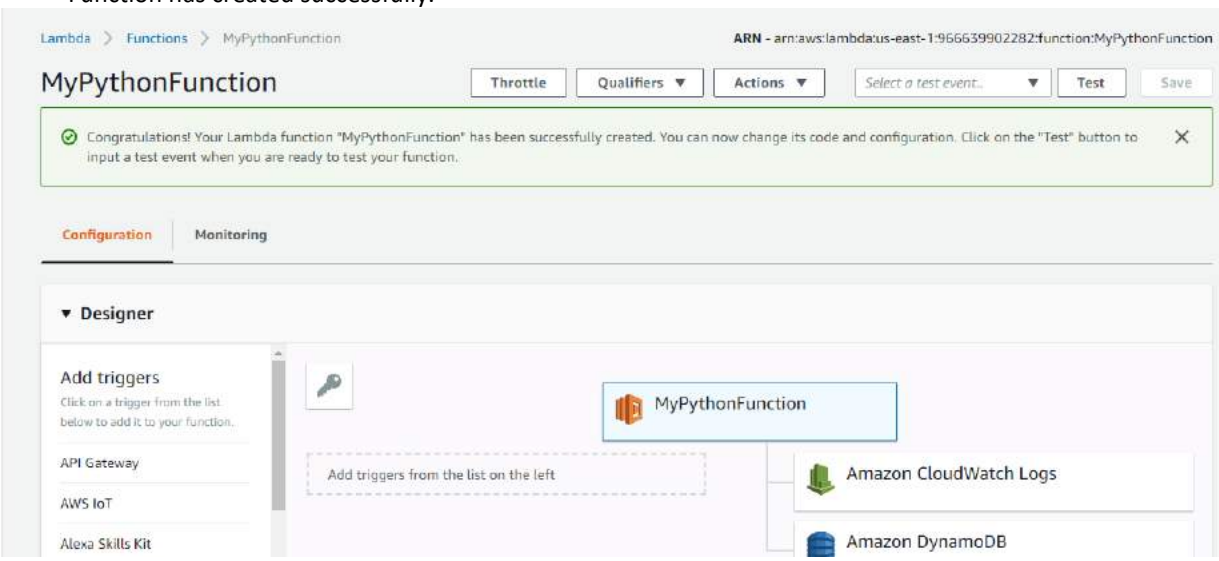
- If any jar or zip files needs to be uploaded from your local, same can be done as we shown below.



- Please find the below screenshot for creating a new function for python.

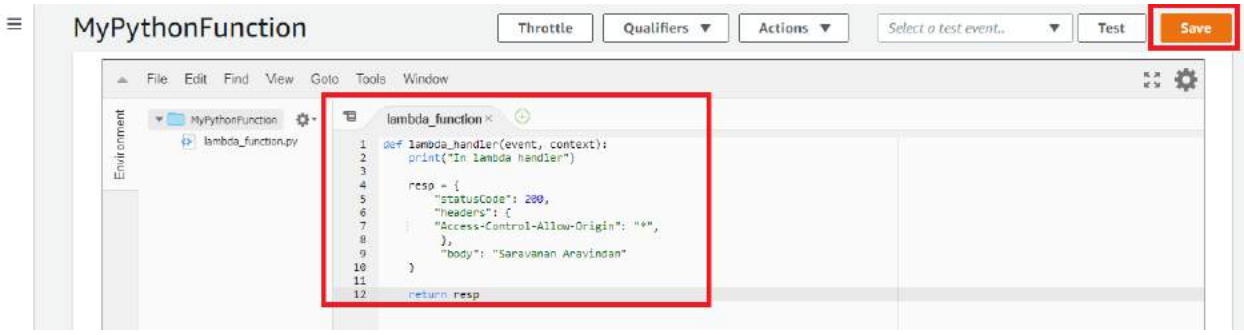


- Function has created successfully.

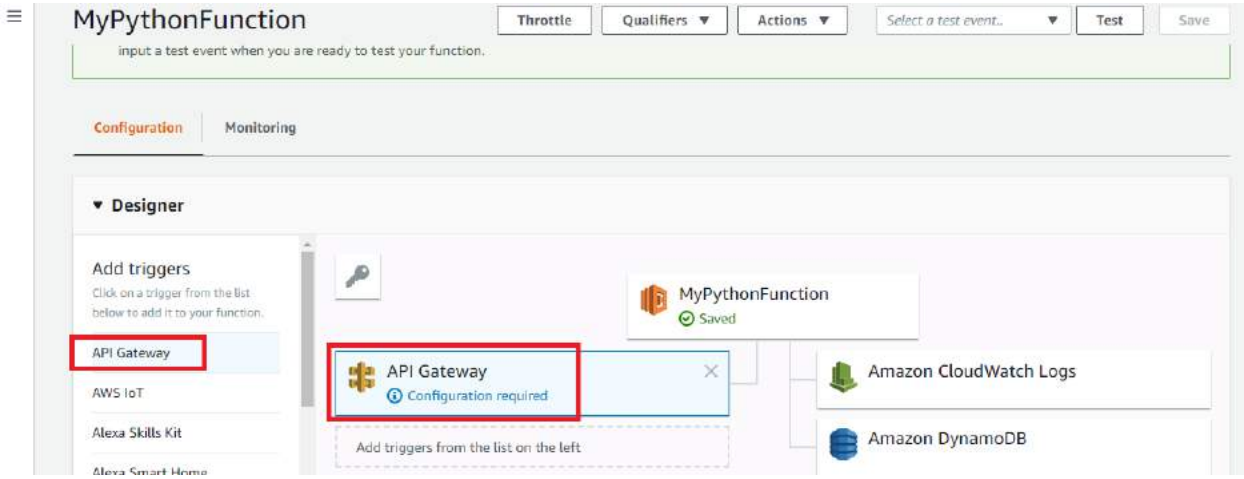


- By Scrolling down, type the sample python code. Here, I have written a code which displays my name through an API. Refer the below code and screenshot.

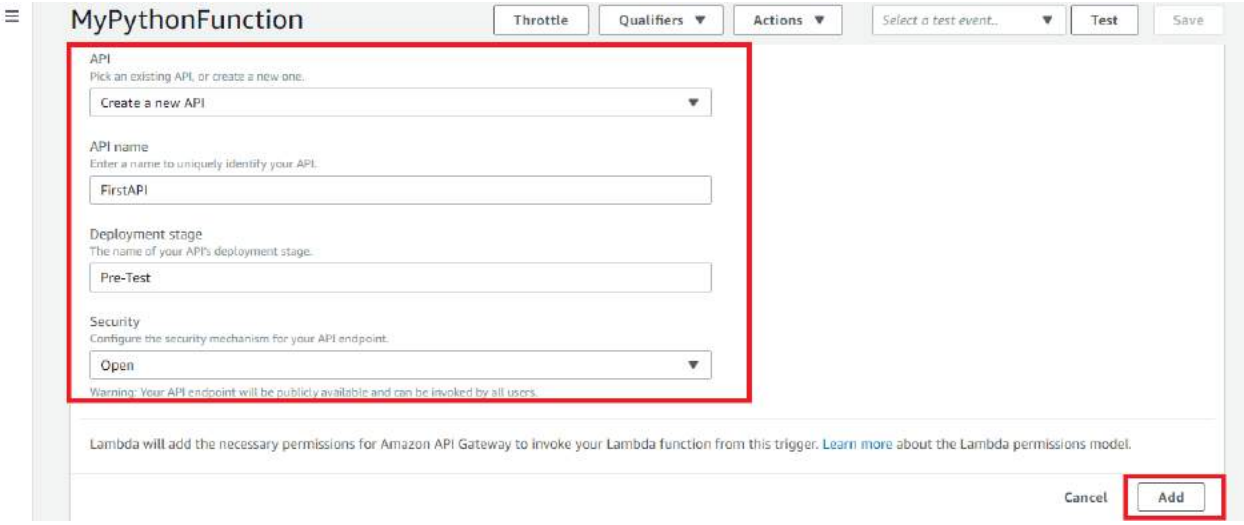
```
def lambda_handler(event, context):
print("In lambda handler")

resp = {
"statusCode": 200,
"headers": {
"Access-Control-Allow-Origin": "*",
},
"body": "Saravanan Aravindan"
}

return resp
```



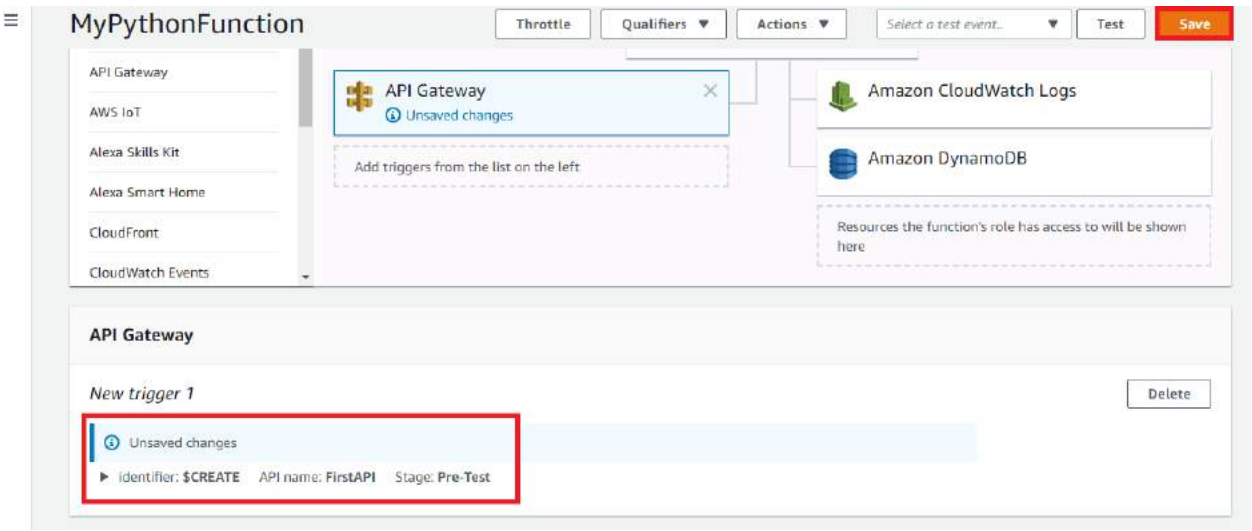
- After saving the code, click on API Gateway which would execute the code.



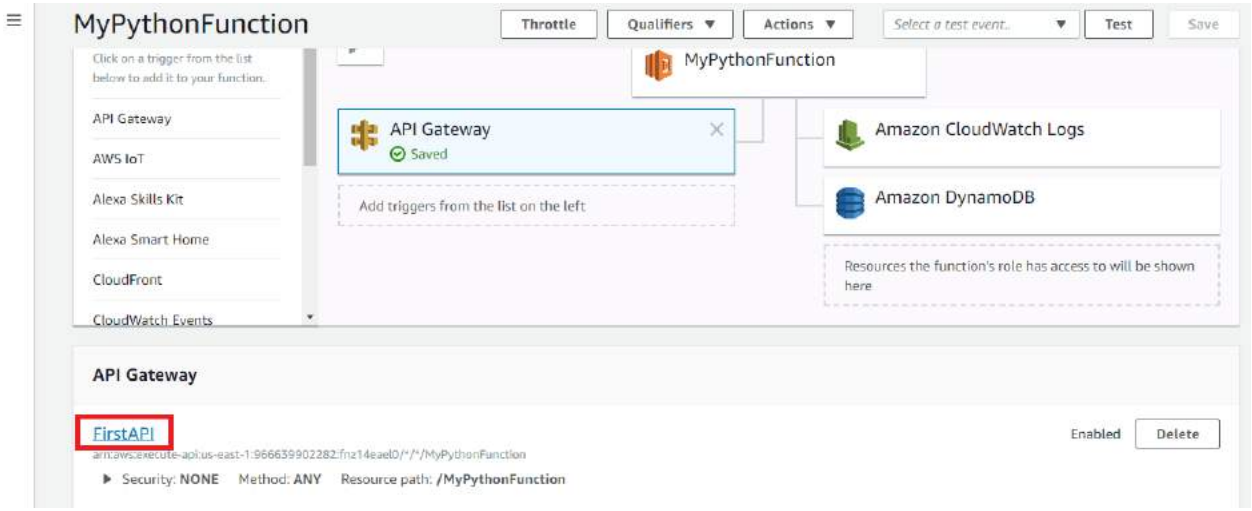
- Create a new API, choose Open to access this API globally.



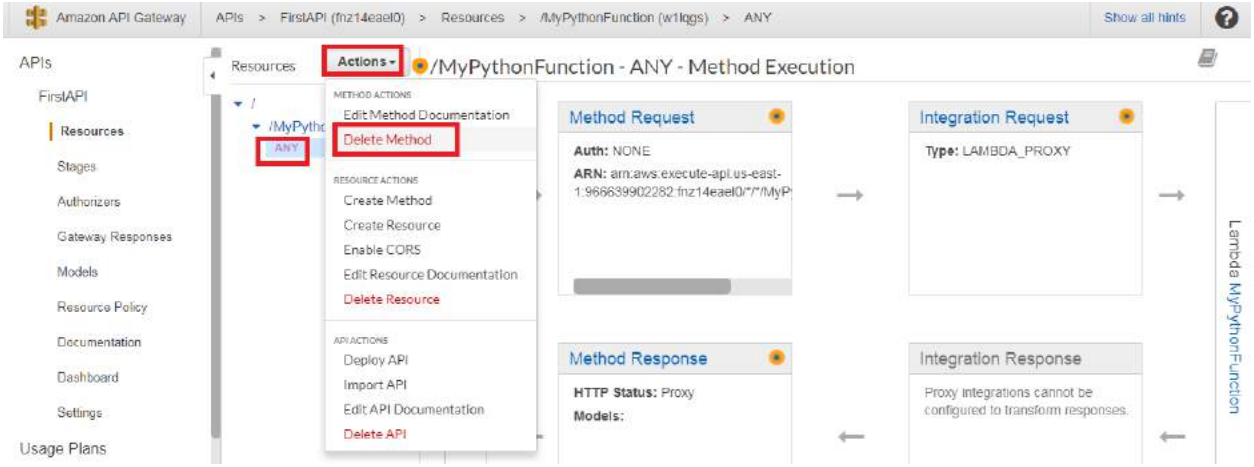
- API has been created and click on save for next steps.



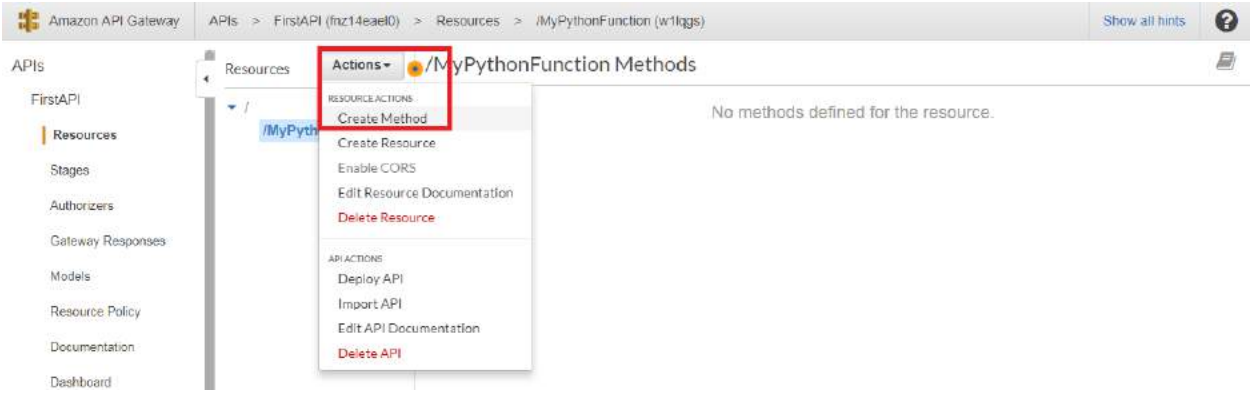
- API has been saved successfully and click on the API name which you have been provided.



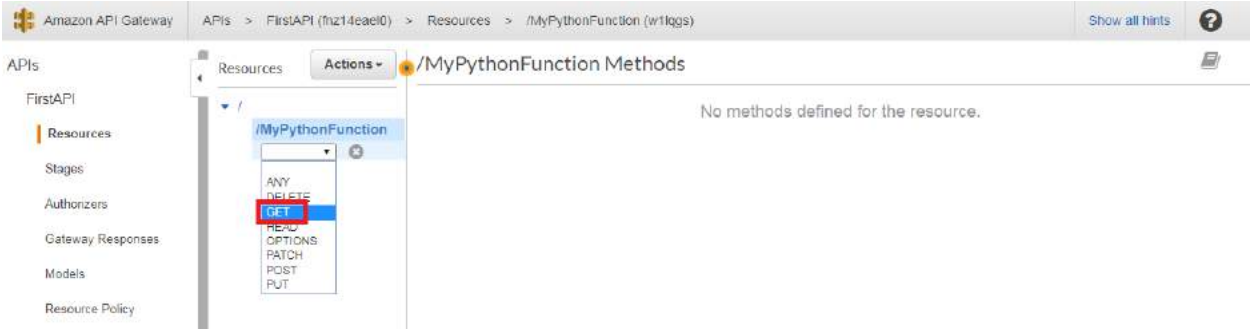
- We need to use Get Method instead of ANY. So am deleting the ANY method.



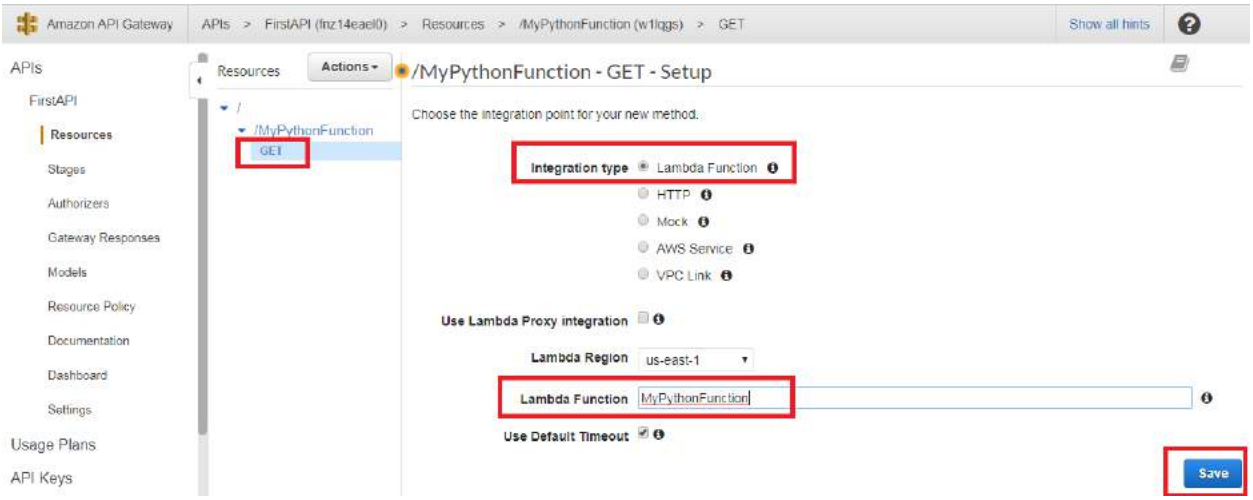
- Creating a new GET method.



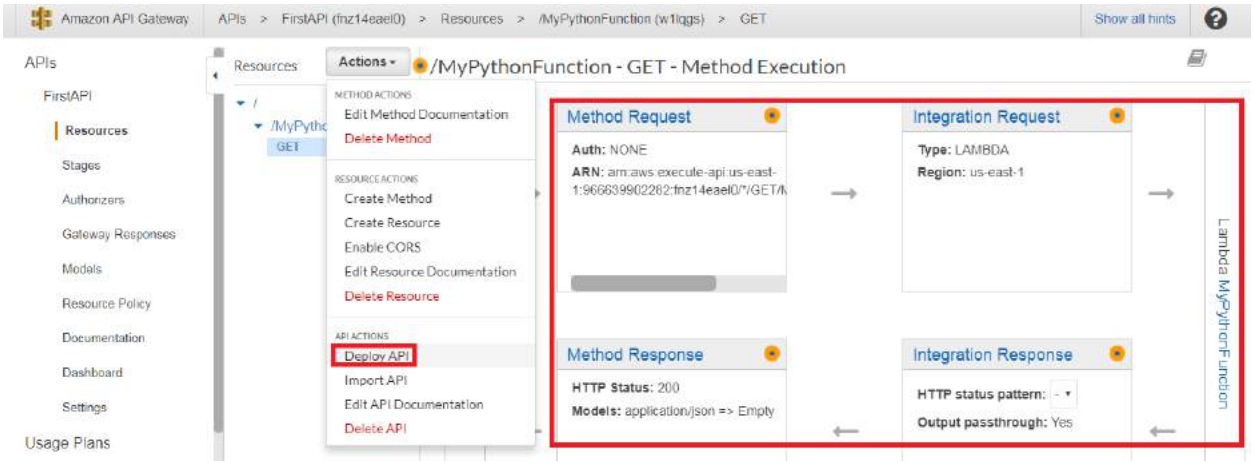
- Choose GET Method and click on Right Tick Mark.



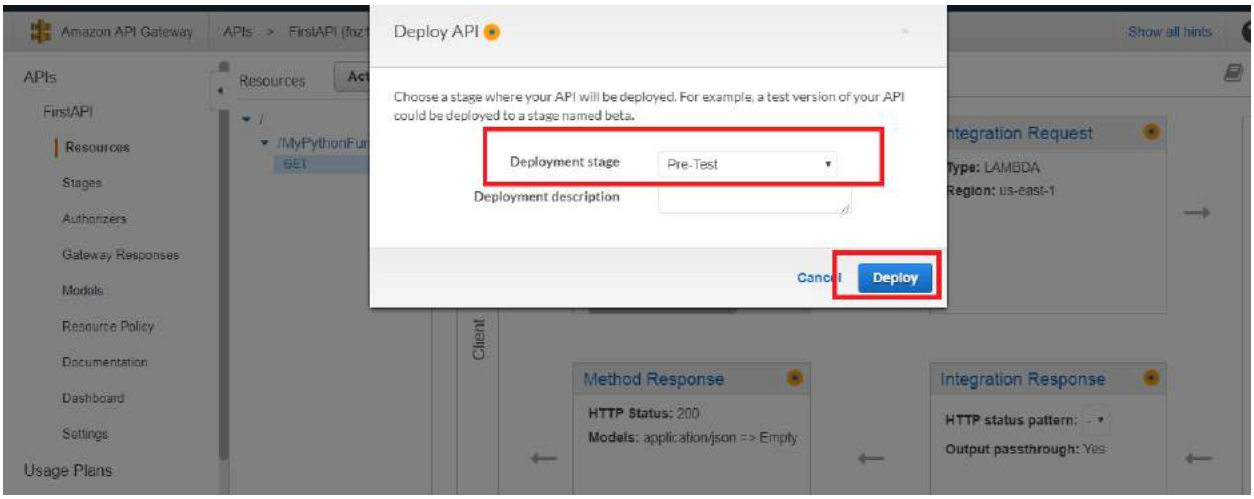
- Choose the Type as Lambda Function and select the function name which has been created earlier.



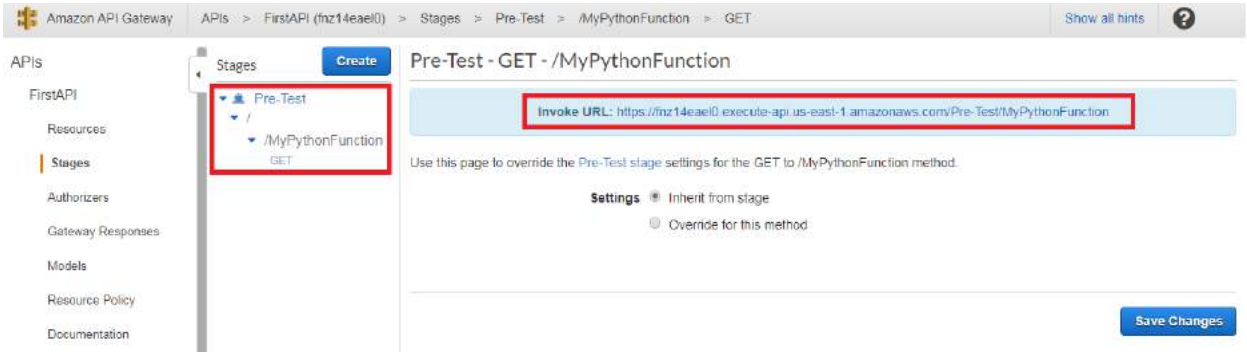
- Followed by, deploy an API.



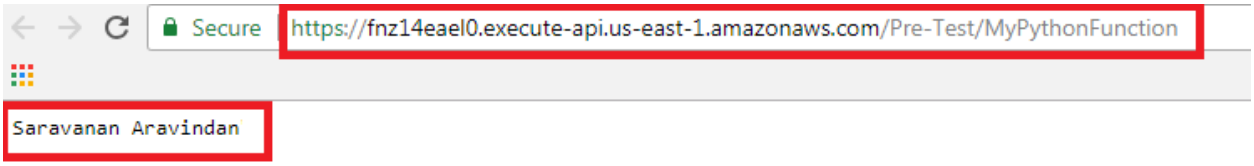
- Choose the Stage which has been created during API creation.



- Invoke URL has been generated and this URL would be used to test the Python code which has been created.



- Open any browser and paste the Invoke URL which gives you an Output of the Python code.



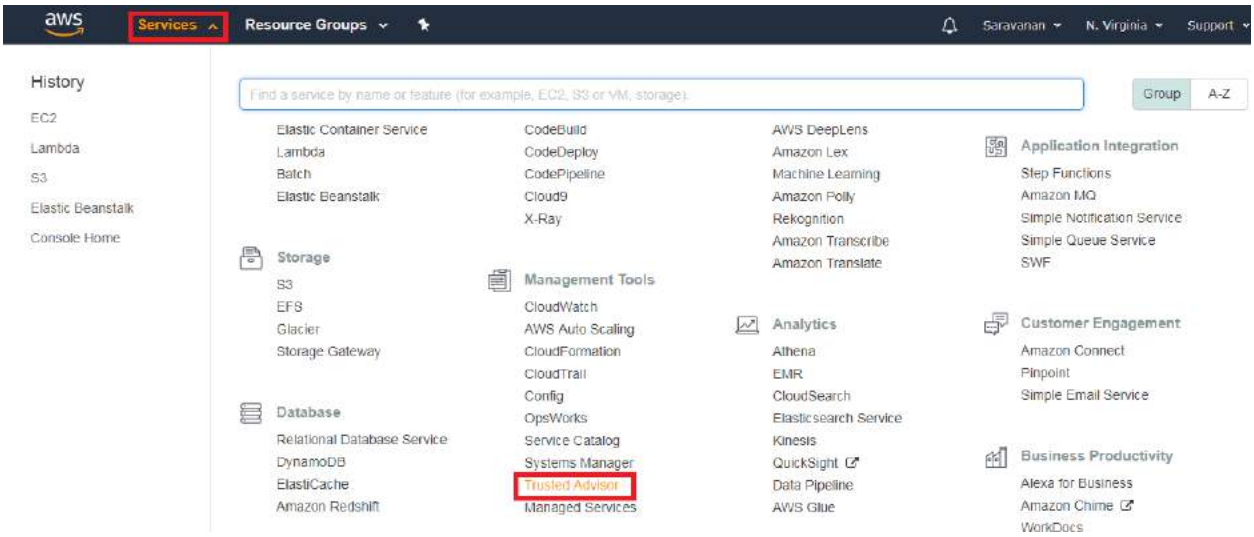
- Delete the API and function after validating this execution steps.

Advantages of Lambda:

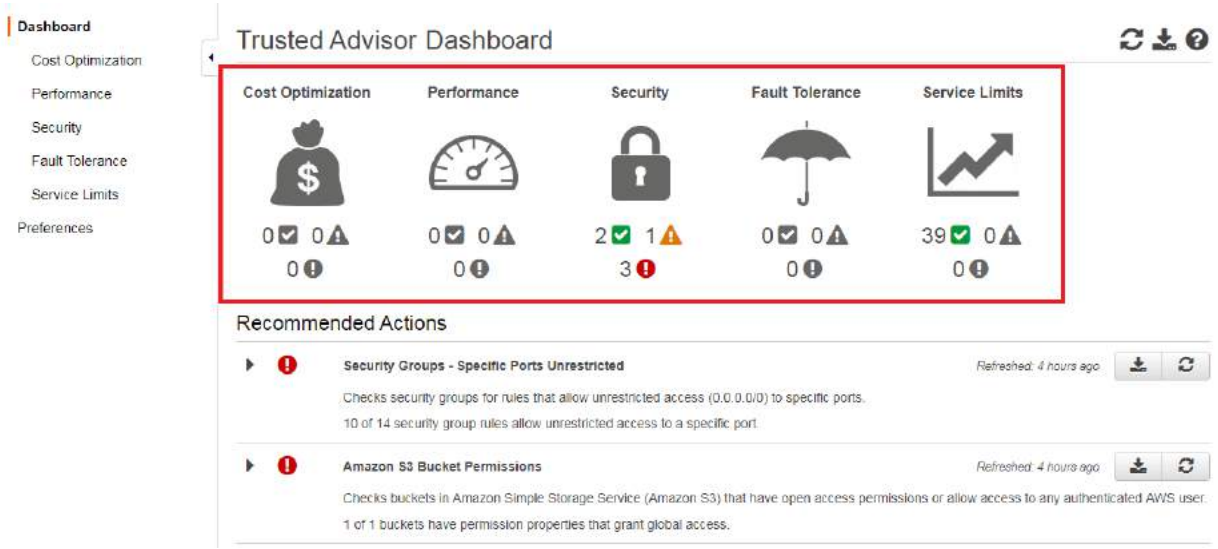
- Reduced cost: We can do computing without any server as an outsourced infrastructure, sometimes we are paying for managing our servers.
- Using AWS LAMBDA Technology, we cut the cost because we are using services not to pay extra attention to maintain machines.
- Reduced scaling cost: we only must pay for the resources we are using, without using any server can bring a big cost cut for you.
- Easier operational management: As the automatic scaling logic of our infrastructure is handled by the vendor.

Security Management - Trusted Advisor:

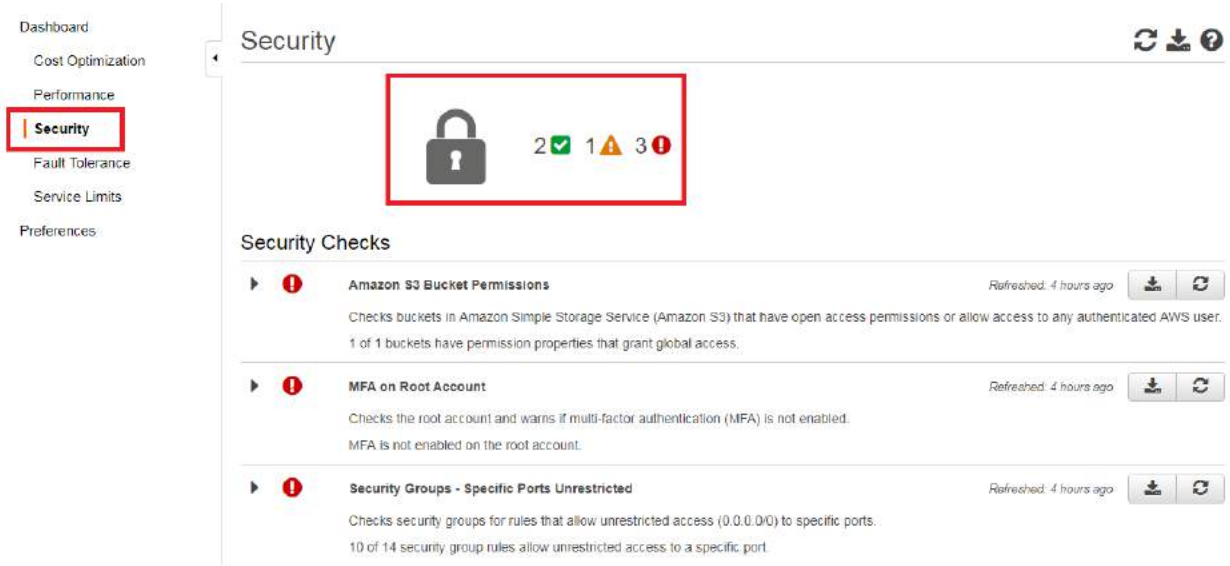
- AWS Trusted Advisor is your customized cloud expert! It helps you to observe best practices for the use of AWS by inspecting your AWS environment with an eye toward saving money, improving system performance and reliability, and closing security gaps. Since we launched Trusted Advisor in 2013, our customers have viewed over 1.7 million best-practice recommendations for cost optimization, performance improvement, security, and fault tolerance and have reduced their costs by about 300 million dollars.
- Click on Services and choose Trusted Advisor.

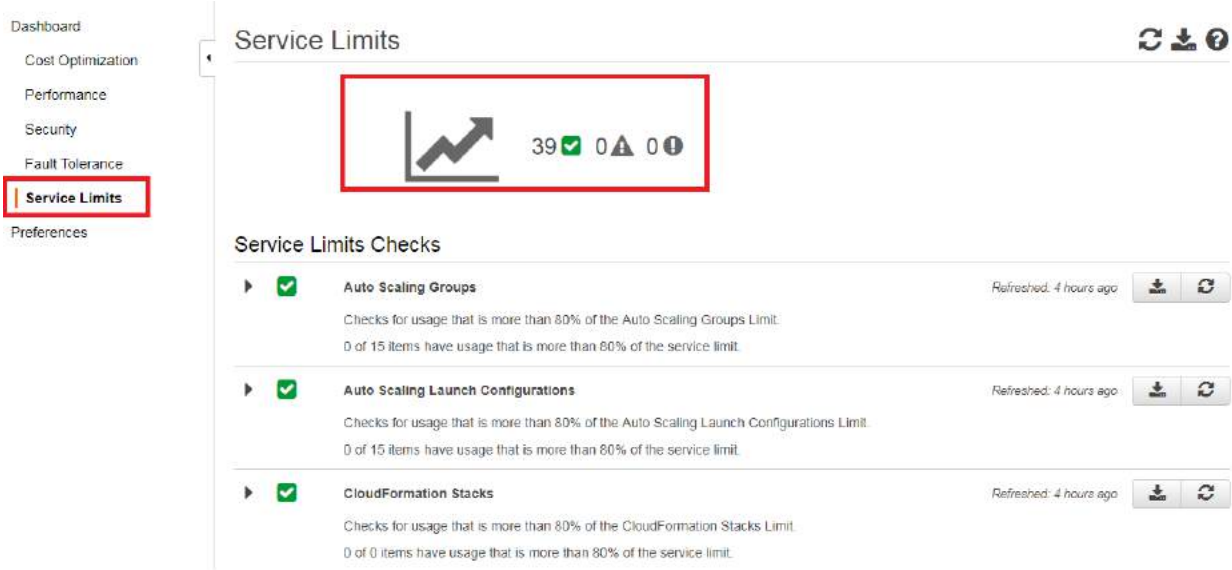


- By default, you would be able to view 5 Advisor options in which are there are two free services which is being offered by AWS.

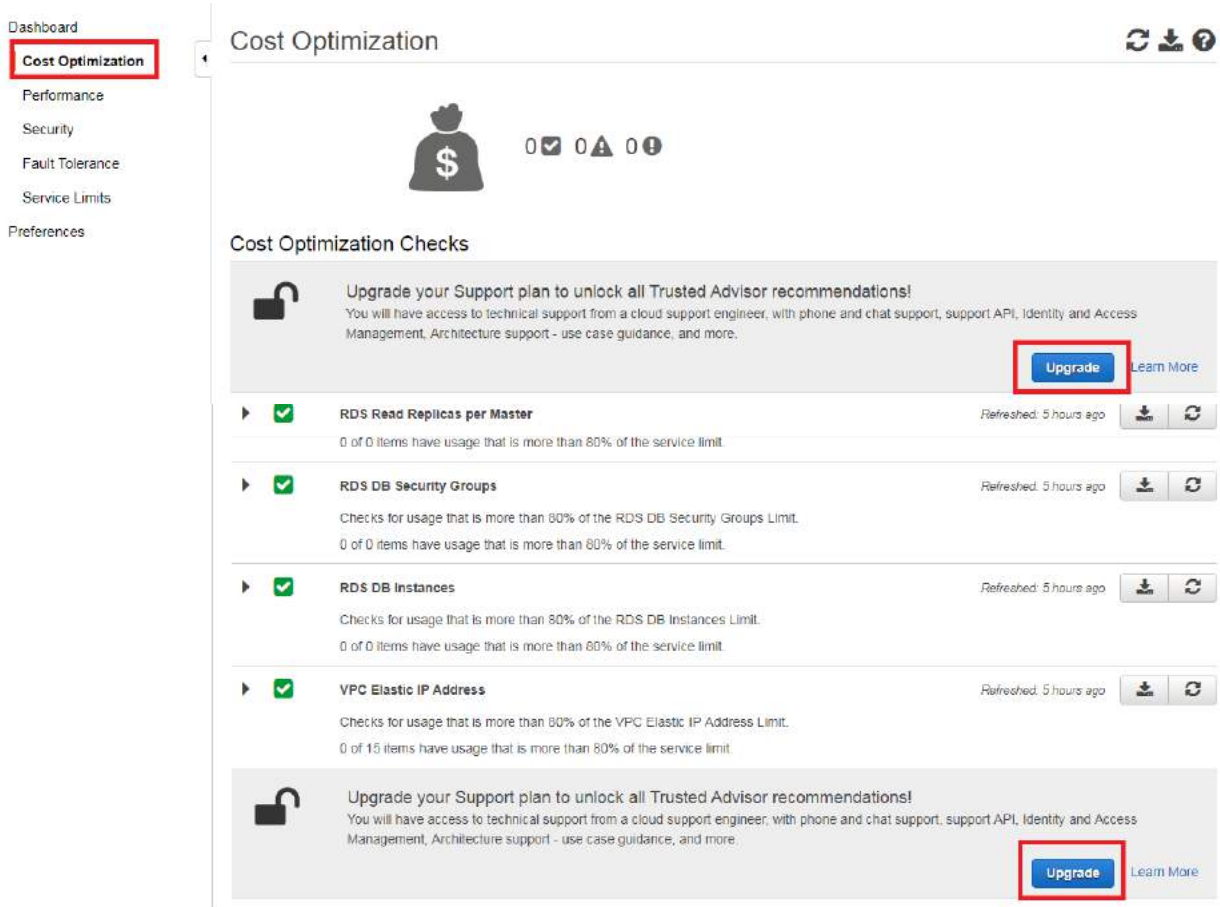


- The two free services are Security and Service Limits. AWS providing an input to use these two effectively as we shown below.





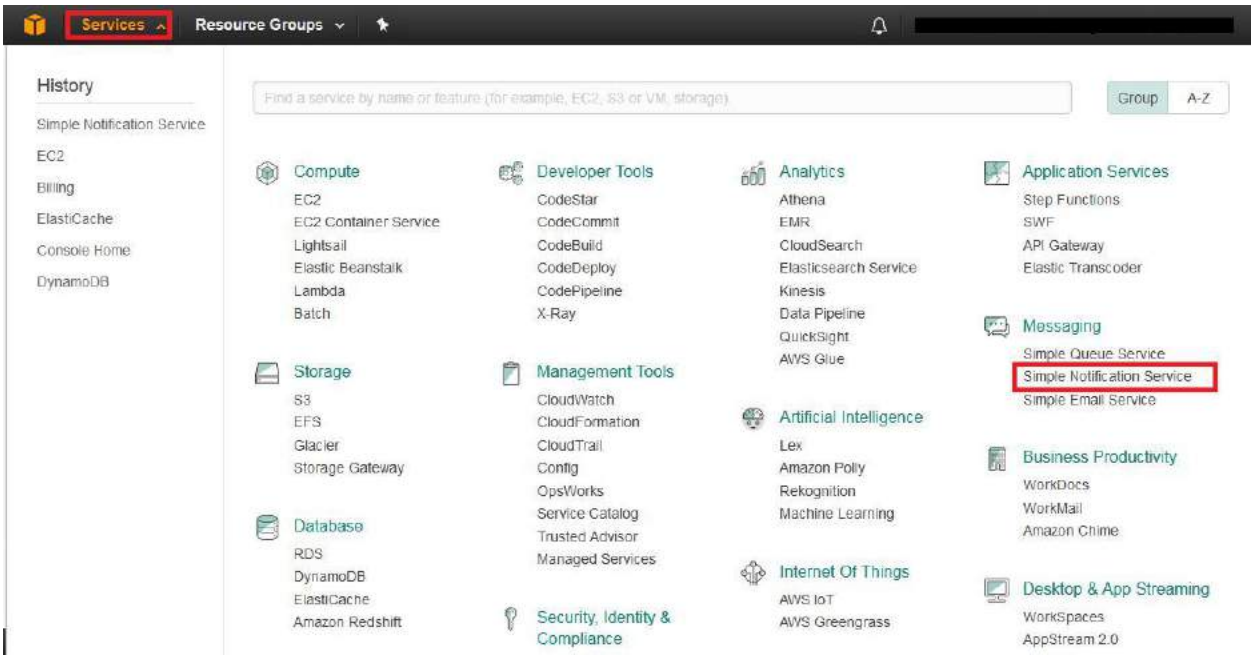
- In case, if you are choosing for payable one, you need to upgrade your plan to premium.



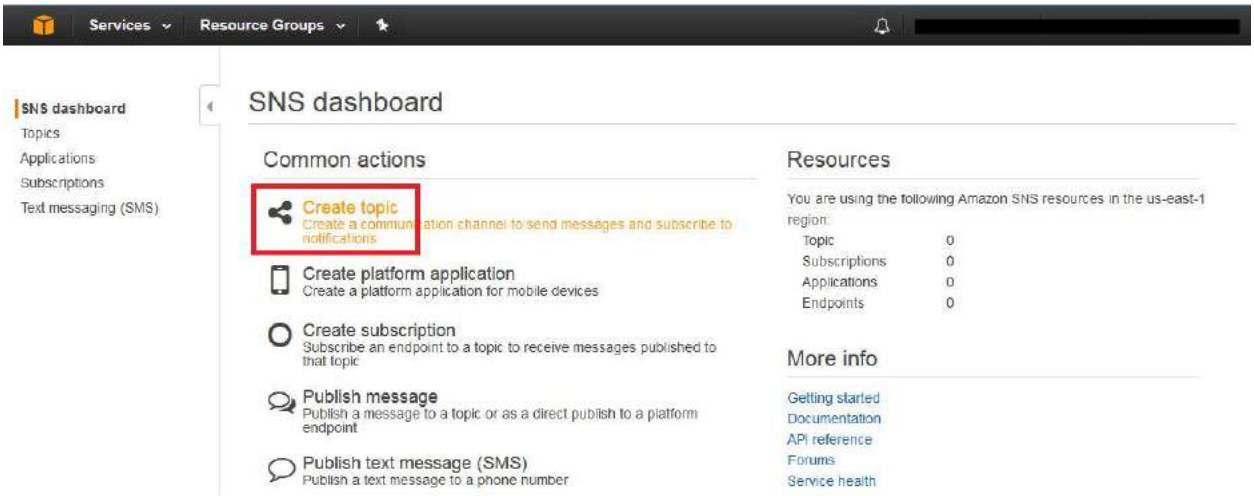
Simple Notification Service (SNS):

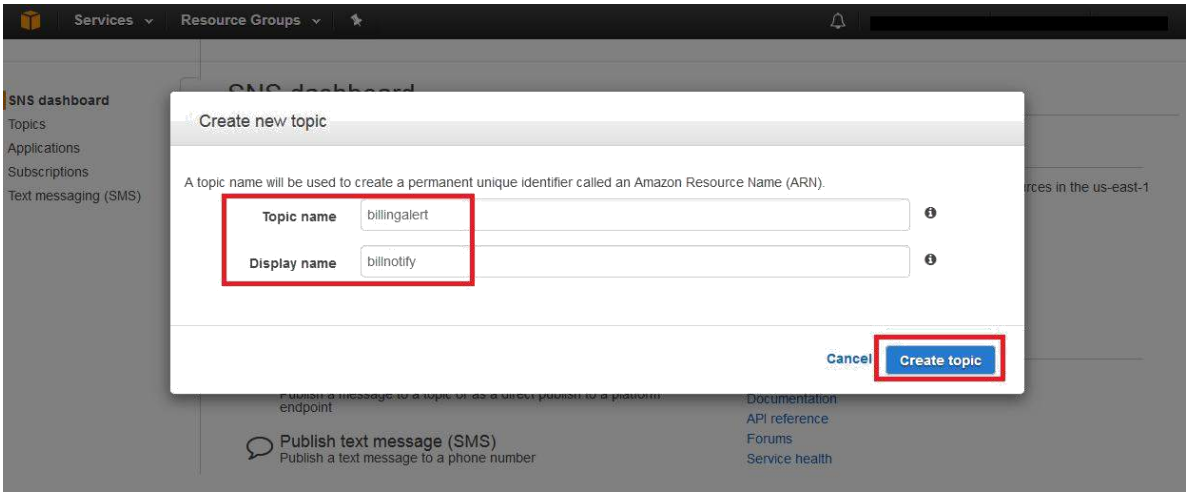
- Amazon Simple Notification Service (Amazon SNS) is a web service that enables applications, end-users, and devices to instantly send and receive notifications from the cloud.

- Go to Services and Select SNS under Messaging as like shown below.
- This SNS would help to create an alarm in CloudWatch to monitor all the resources in AWS.

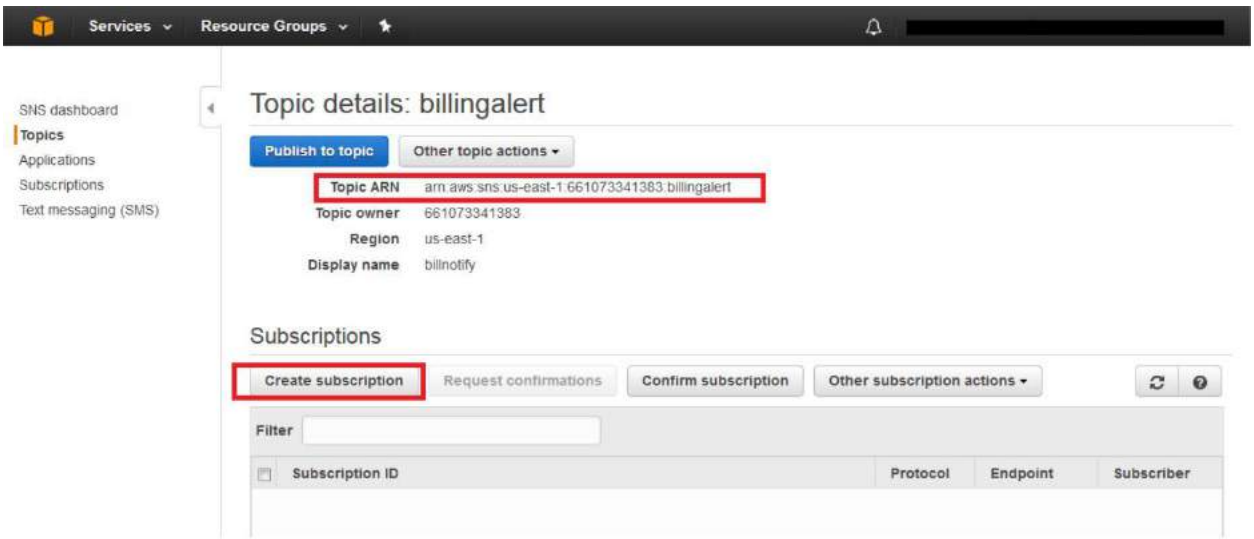


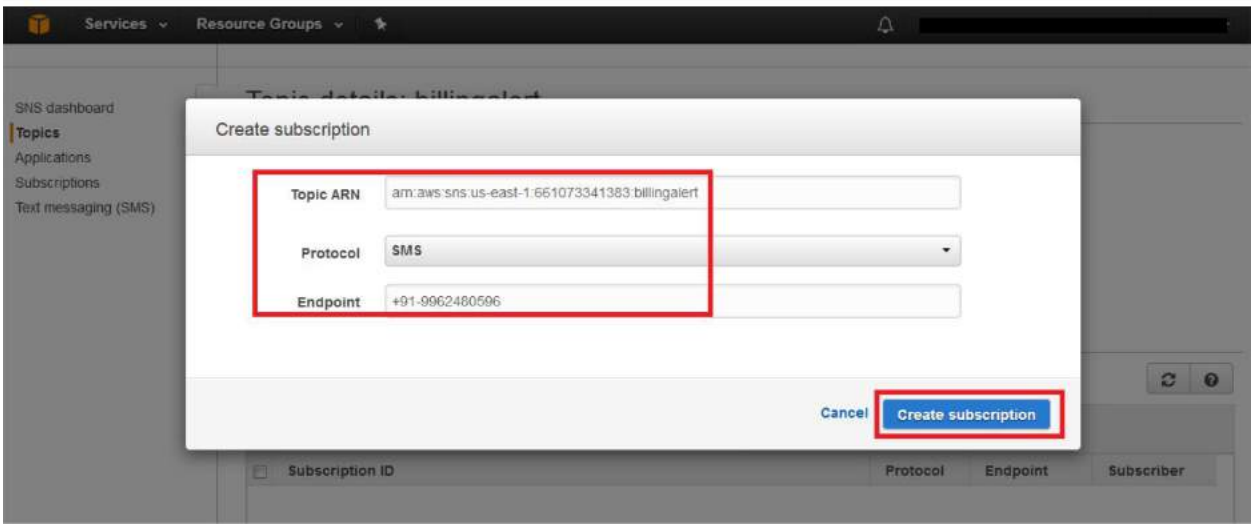
- Create a new topic by providing topic and Display name of the resource you are going to monitor. This topic would help to create a new subscription.

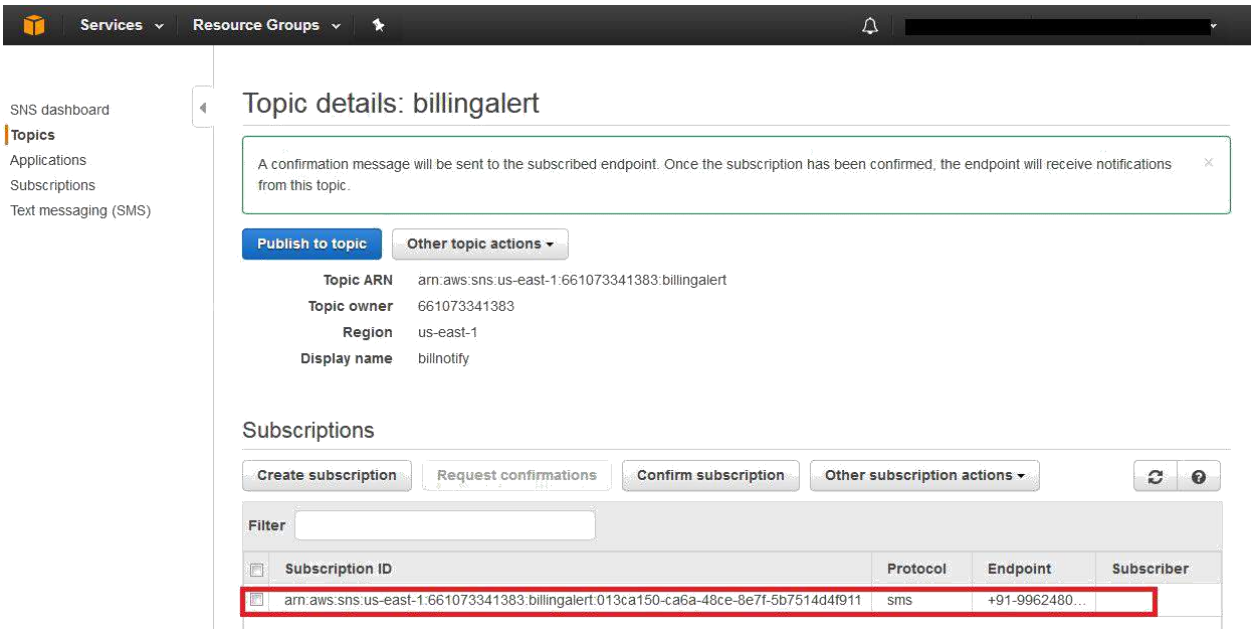




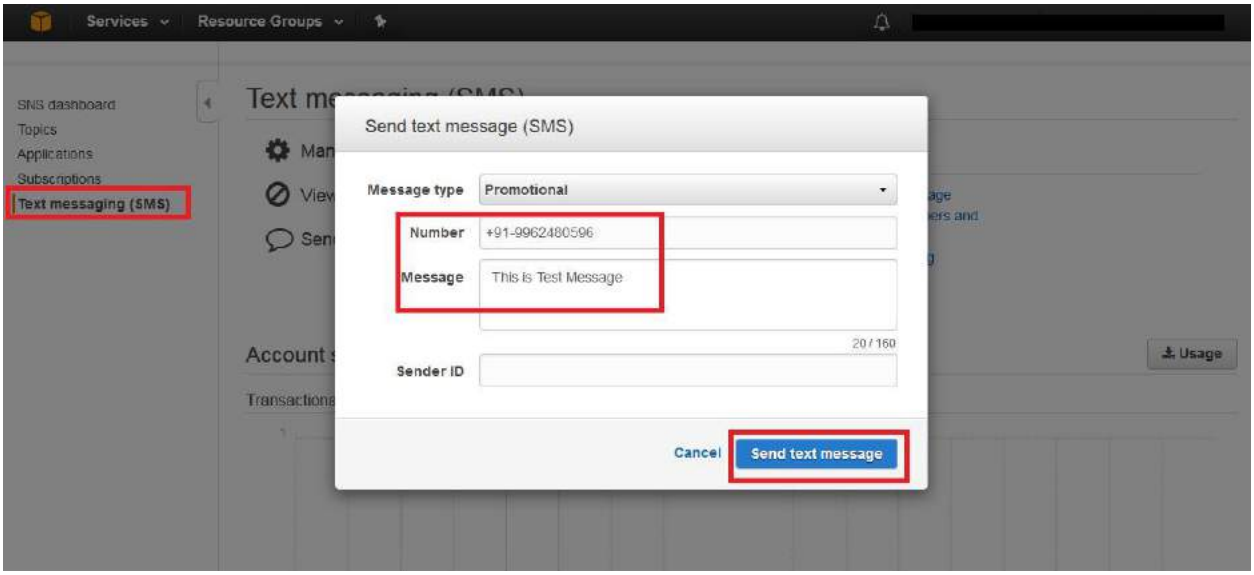
- After creation of new topic, proceed to create a new subscription under the topic as like shown below. Choose the protocol from which source you need to get an alert / notification.







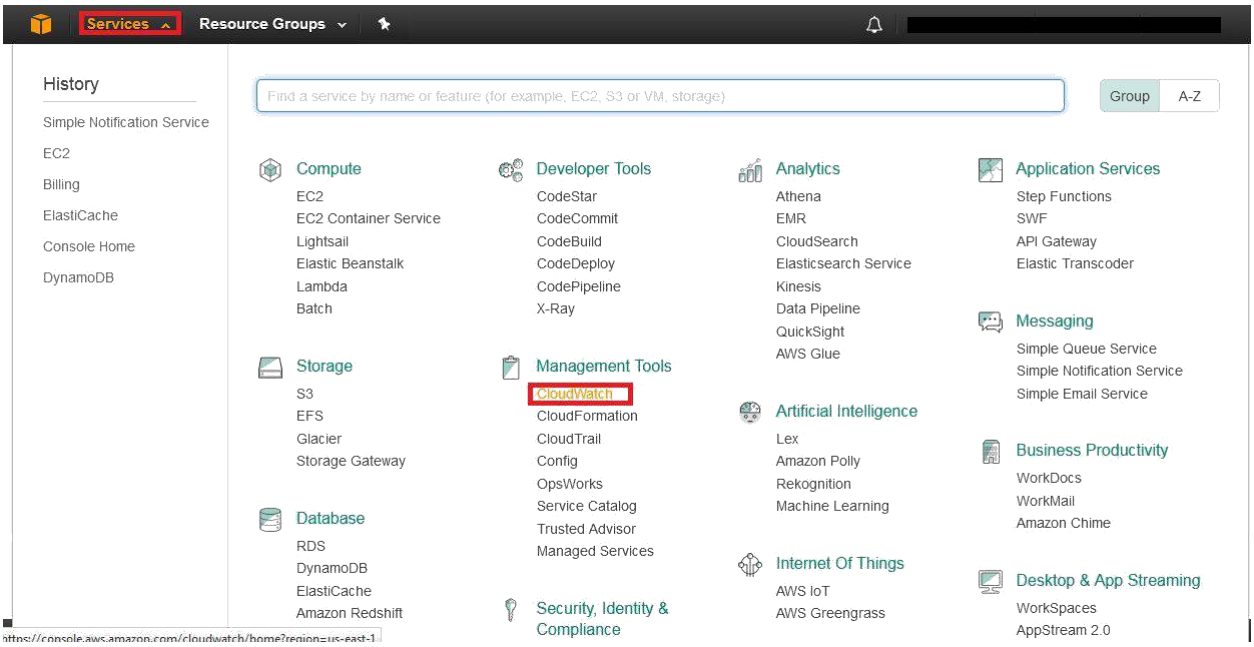
- Also, we would be able to send a Text message from AWS SNS by providing a phone number of recipient as like shown below.



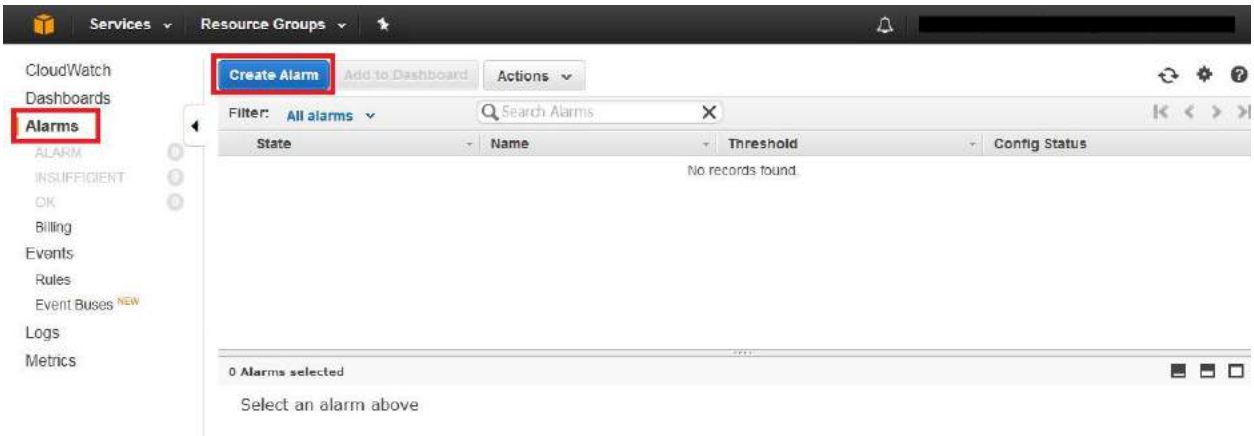
Management Tools:

CloudWatch:

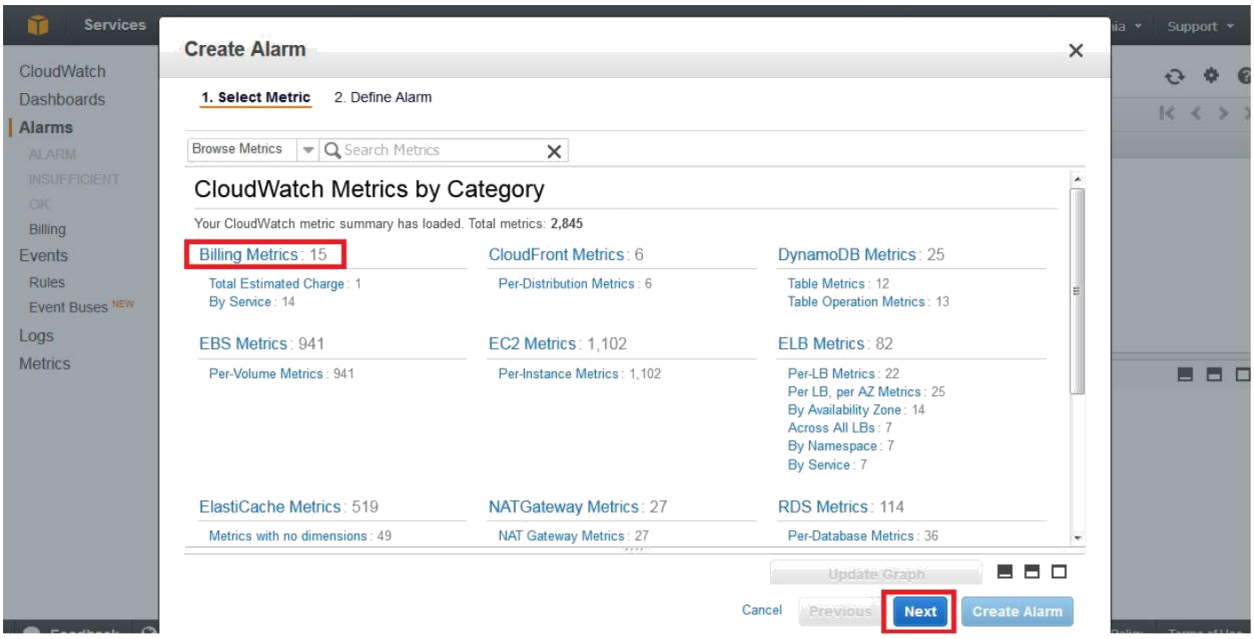
- Amazon CloudWatch provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.
- Use CloudWatch to monitor your AWS resources and the applications you run on AWS in real time.
- Go to Services and Click on CloudWatch under Management as like shown below.

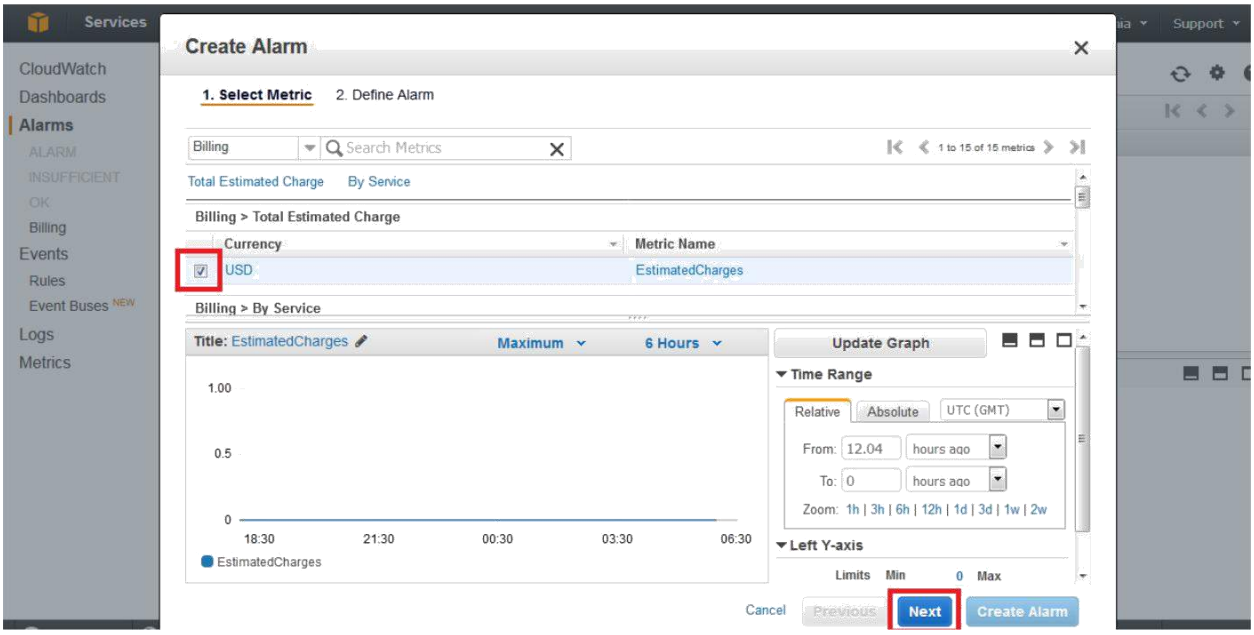


- Choose Alarm option, Click on Create Alarm.

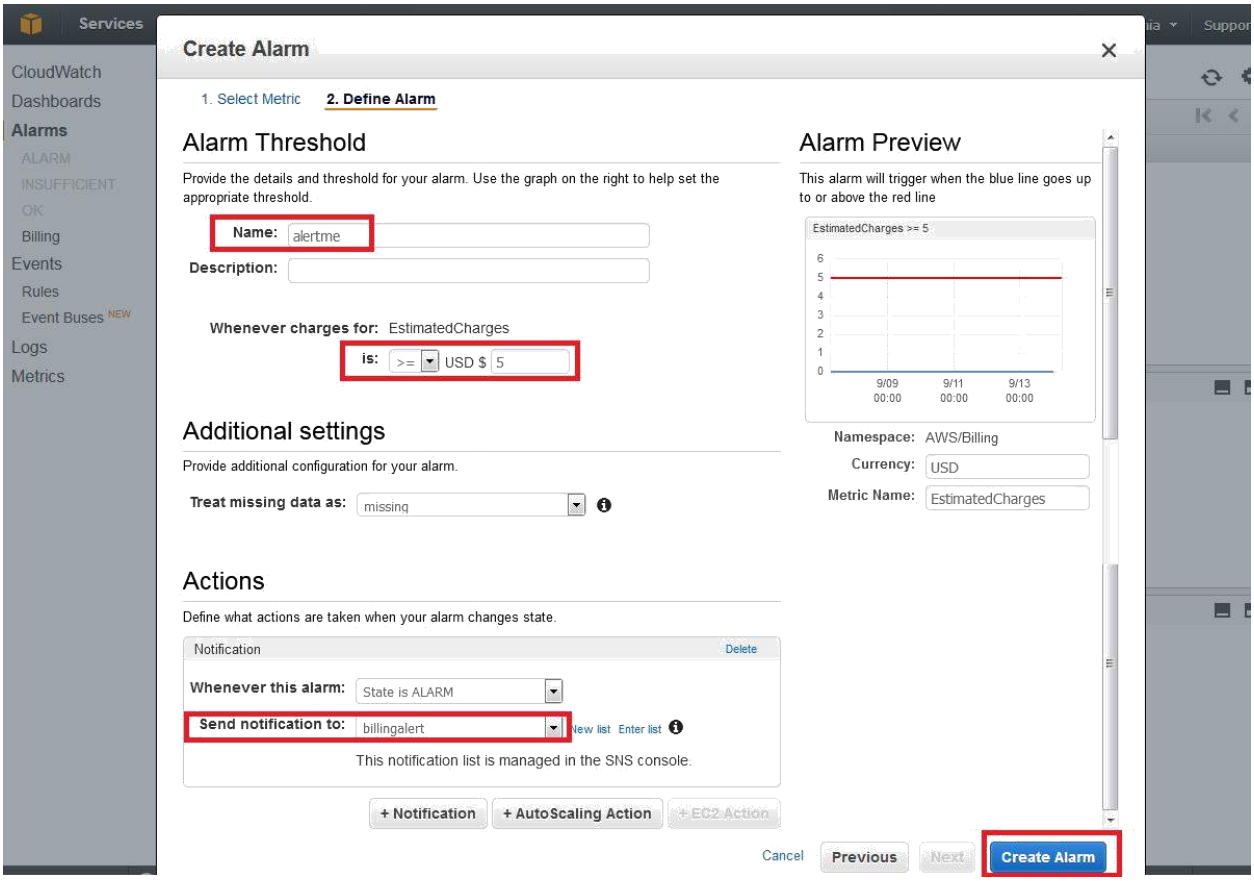


- AWS providing an option to monitor all your resources which are available and to do the same, we need to choose the metrics which we need to monitor.
- These metrics can be anything like Billing, S3 usage, EC2, RDS, DynamoDB, ELB, EBS, etc.
- Also, we can able to create an Alarm for monitoring Servers which are running under EC2. For example, if we need to monitor CPU / Disk Read & Write Operations, create an alarm for the same by choosing the respective server.
- Now, am choosing the Billing Metrics in an alarm which are creating now and the same can be seen below.





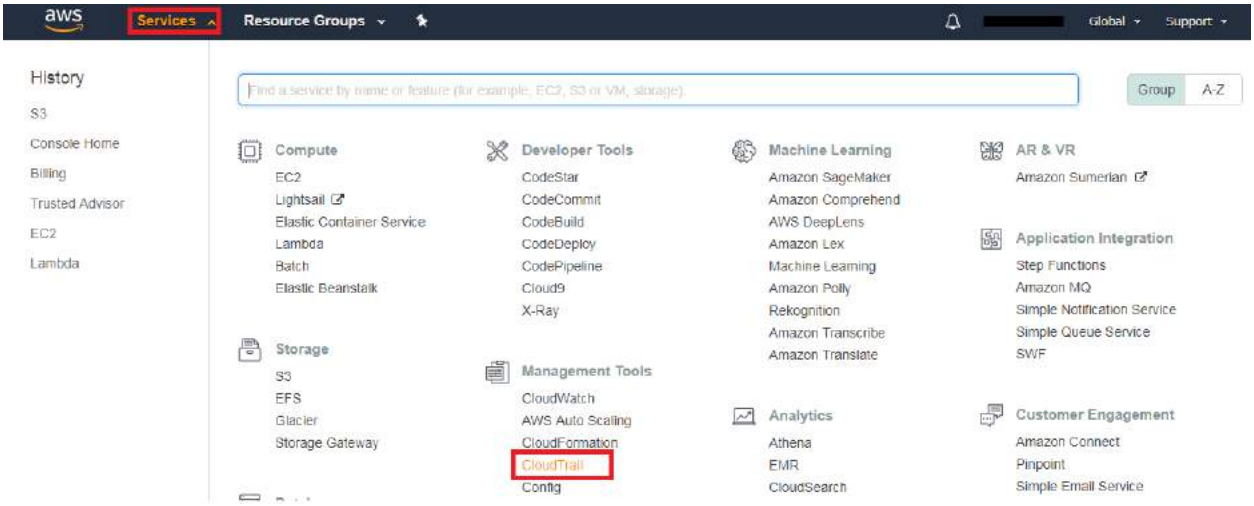
- Provide the name for Alarm, provide the condition that > or = certain bill amount and choose a notification to which protocol which has been created in SNS.



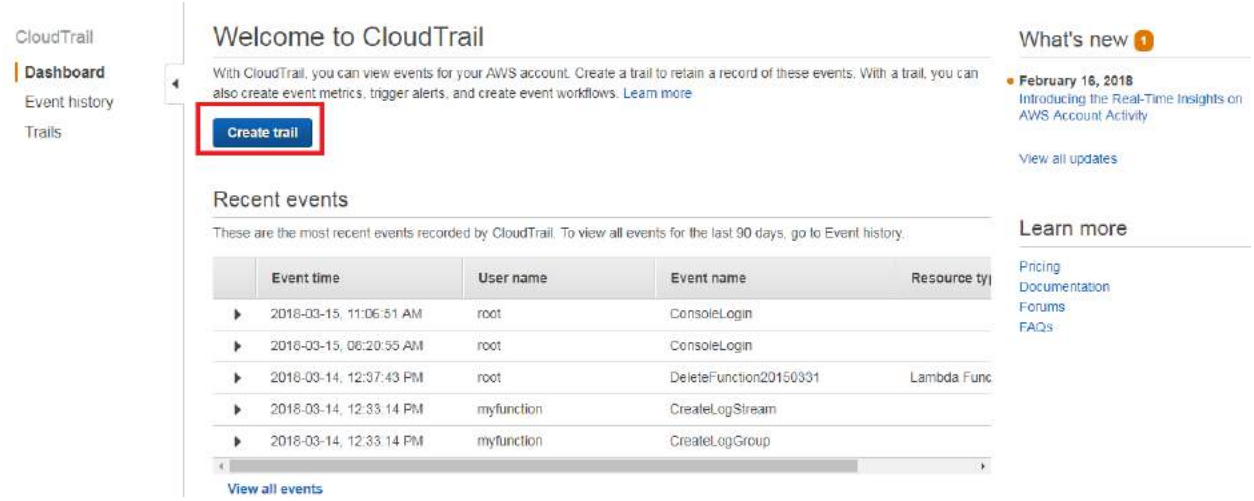
- New alarm has been created and if billing amount reaching $5 or above, we would be getting a notification to mobile since we have been chosen SMS protocol during SNS creation on previous topic.

Cloud Trail:

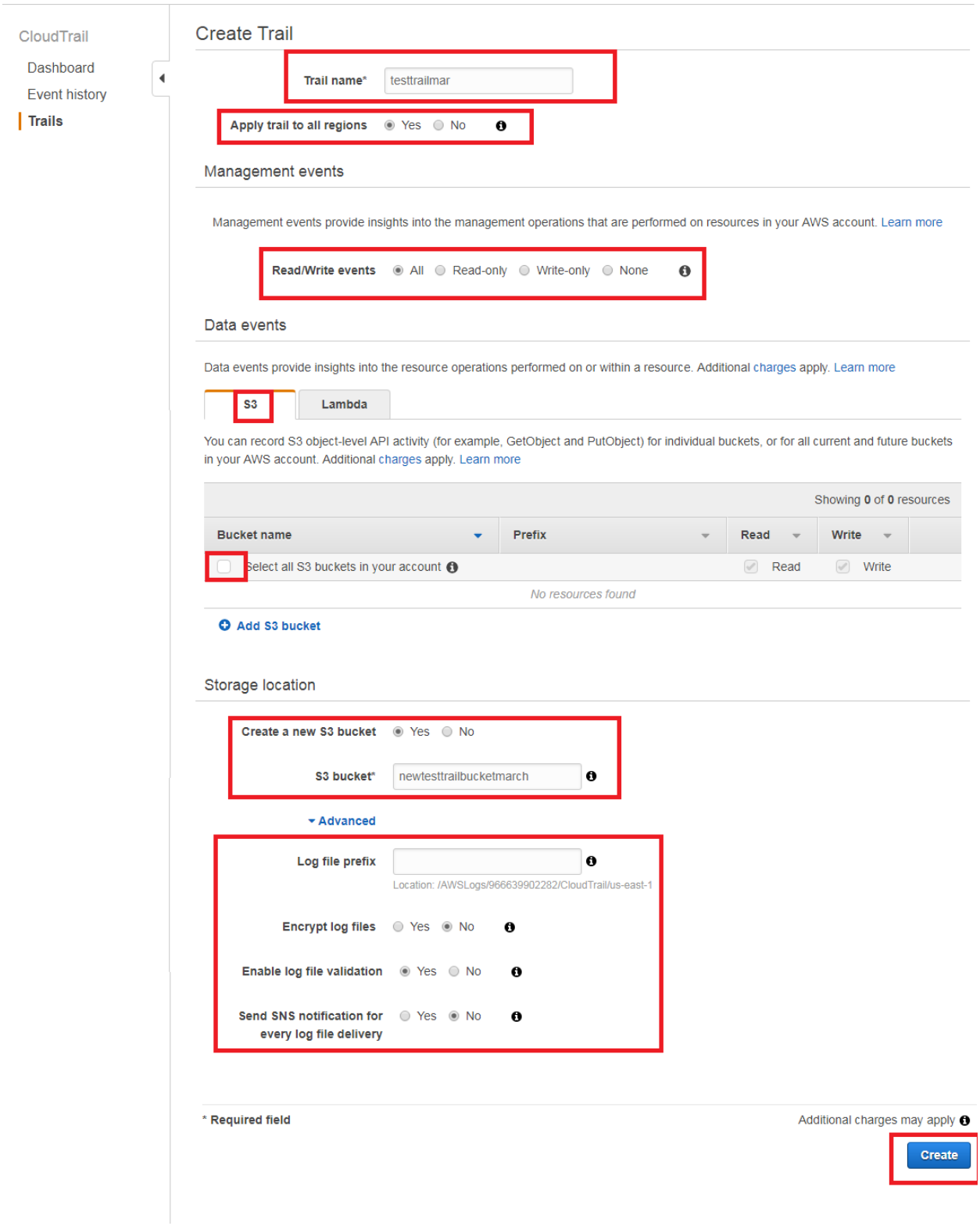
- AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.
- CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
- When you are having more IAM users, you could use this feature to track all the users' actions across all regions.
- Click on Services and Select Cloud Trail Option.



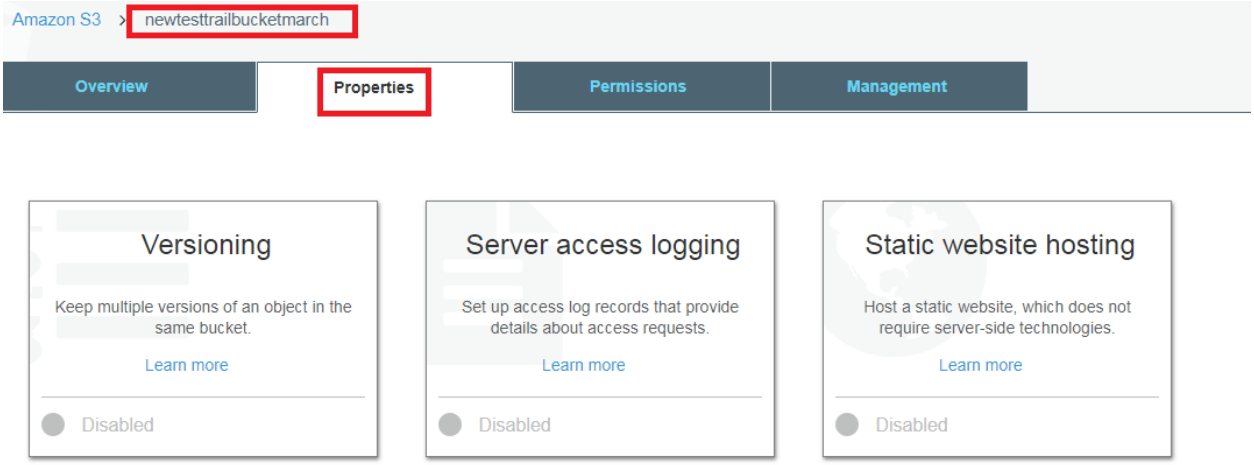
- Click on create trail.



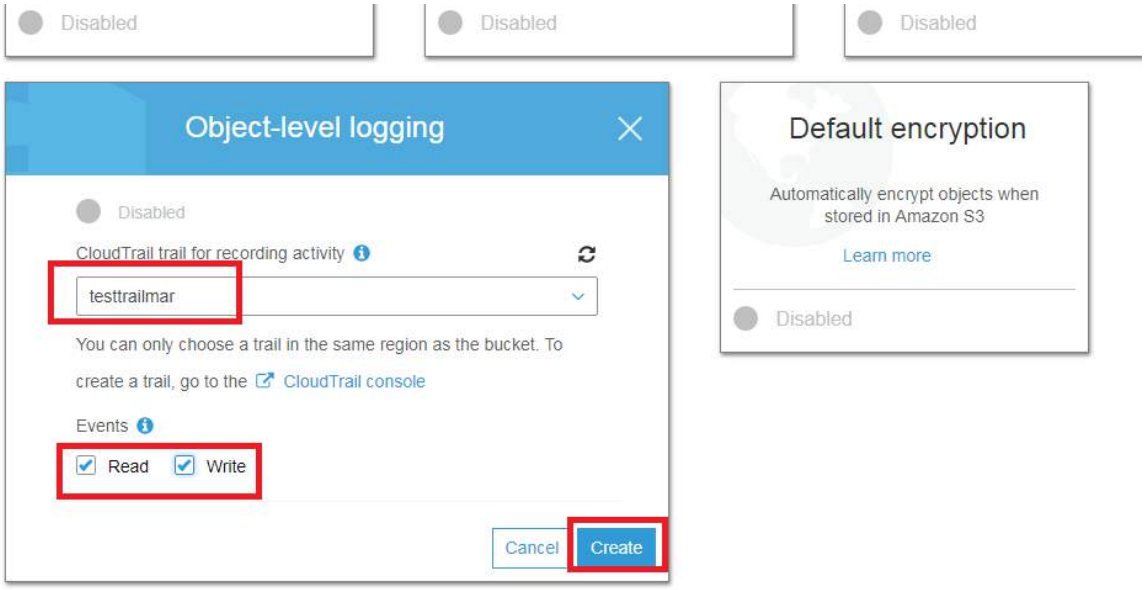
- Provide the Cloud trail name, select all regions if you want to monitor and if you require specific regions, same could be selected. If you want to monitor / track S3 and Lambda enable the same in Data Events.
- Create a new S3 bucket to save the log files or if you have an existing one, map the same.



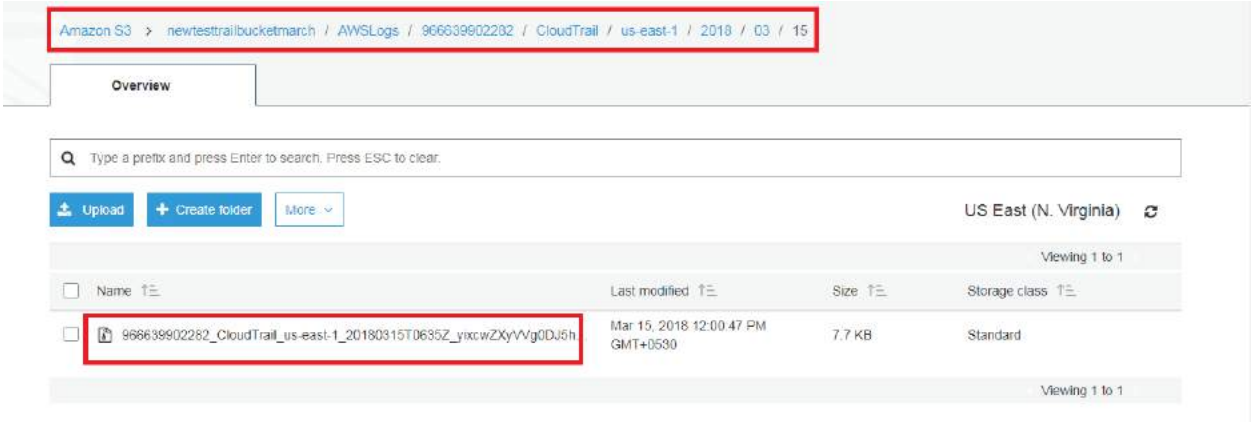
- After creating this Cloud Trail, navigate to S3 bucket which has been created automatically to change the permissions as well as to enable Object Logging under the properties.



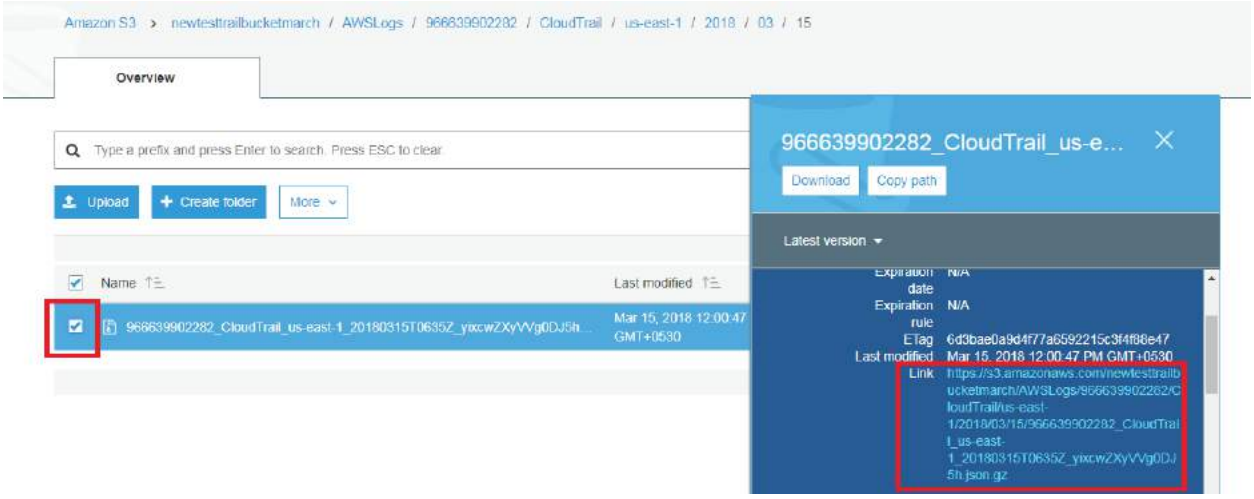
- Select an Events as Read & Write.



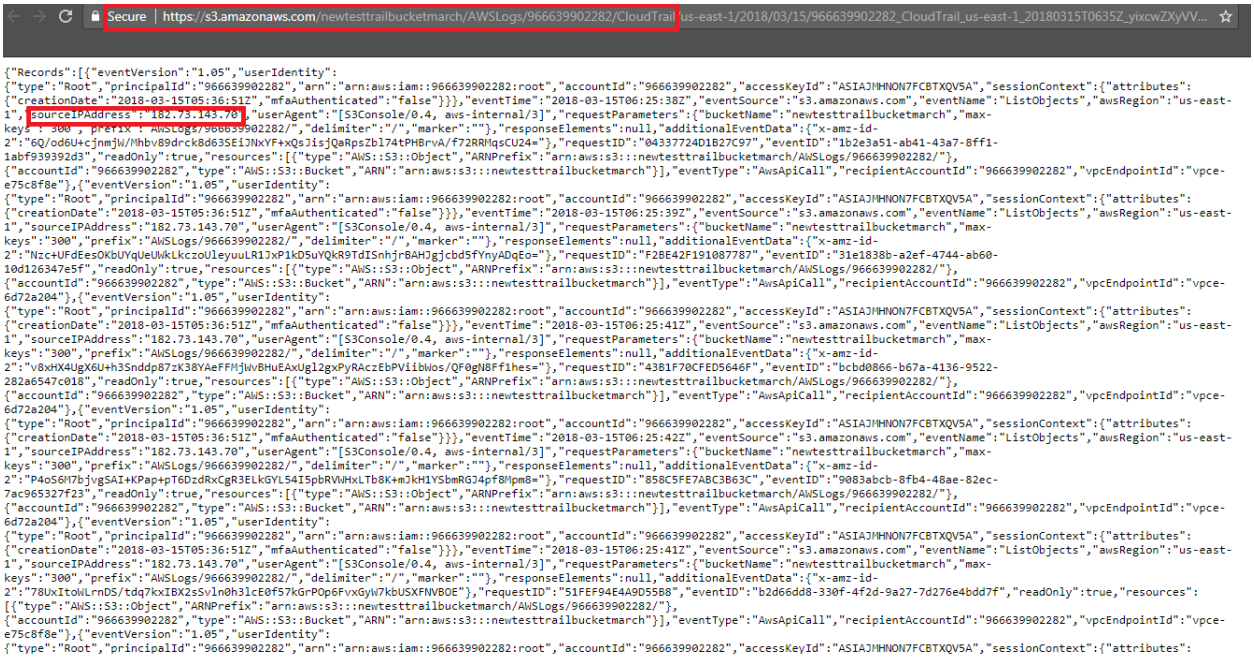
- Once this has been enabled, log files would be generated under this bucket and the same be like given below.



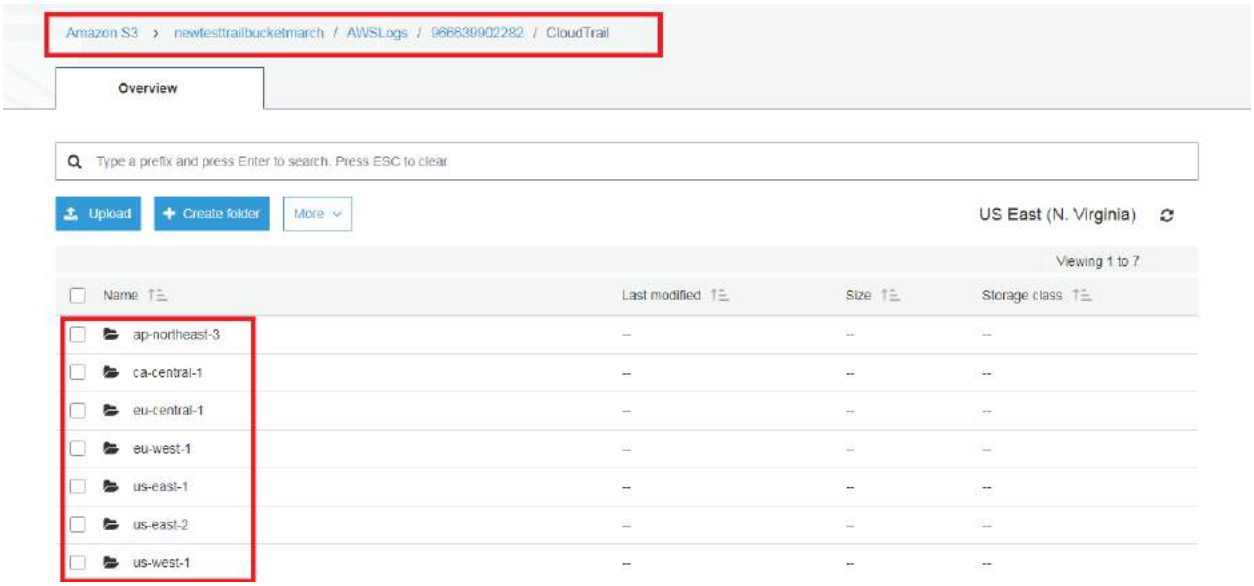
- Provide the permission / make public to access this respective log file.



- You could be able to track all user's actions by region wise along with Source IP address, date and time.

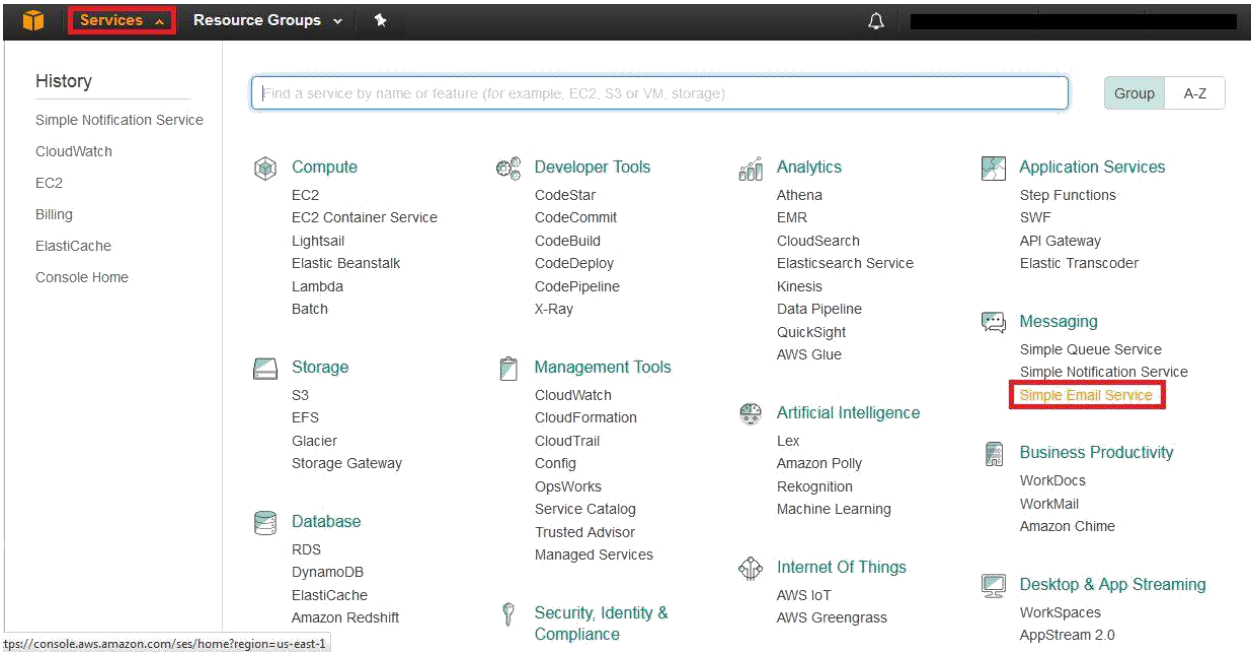


- All regions log files has been generated.

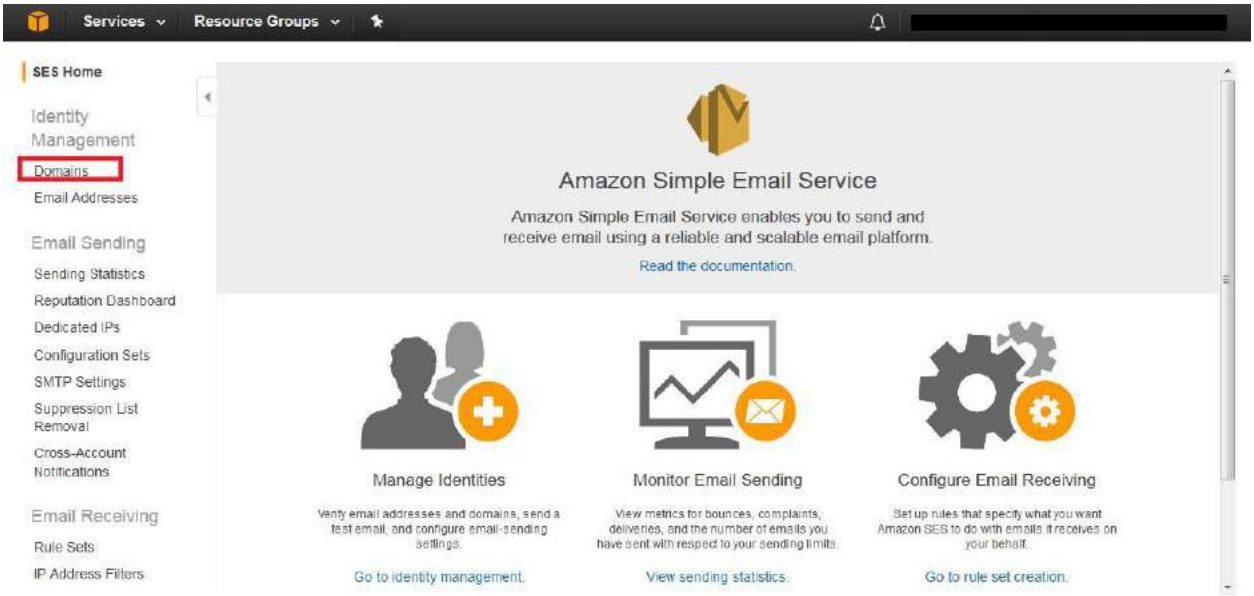


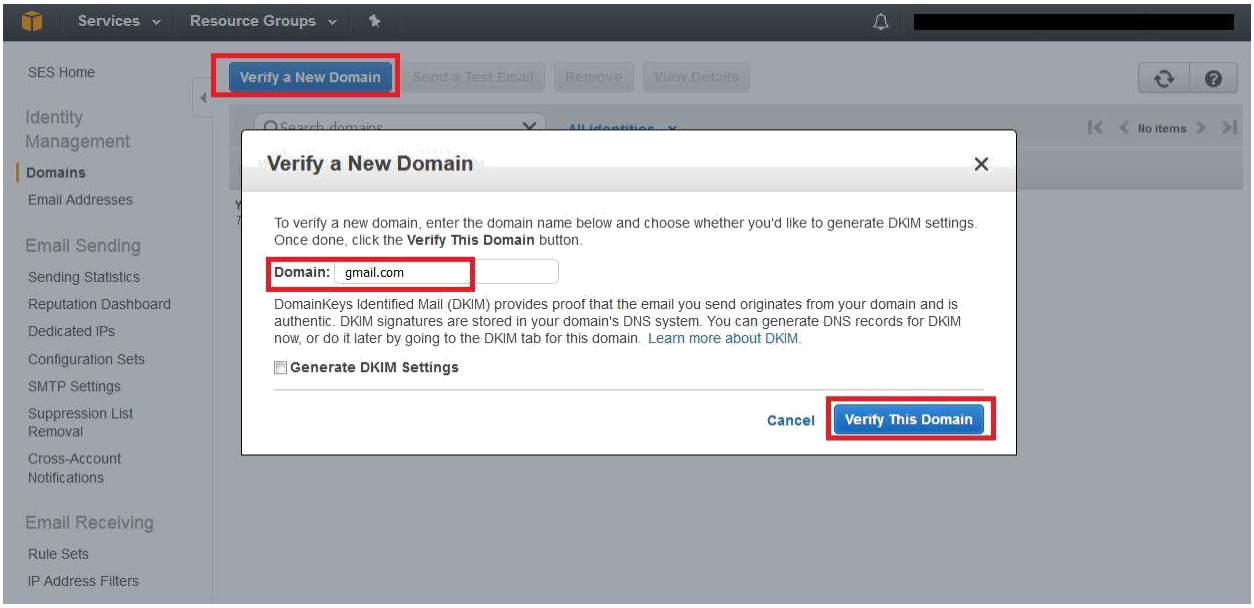
Simple E-Mail Service (SES):

- Amazon SES is an email sending and receiving service that provides an easy, cost-effective way for you to send email.
- Navigate to Services and choose SES under Messaging module as like shown below.

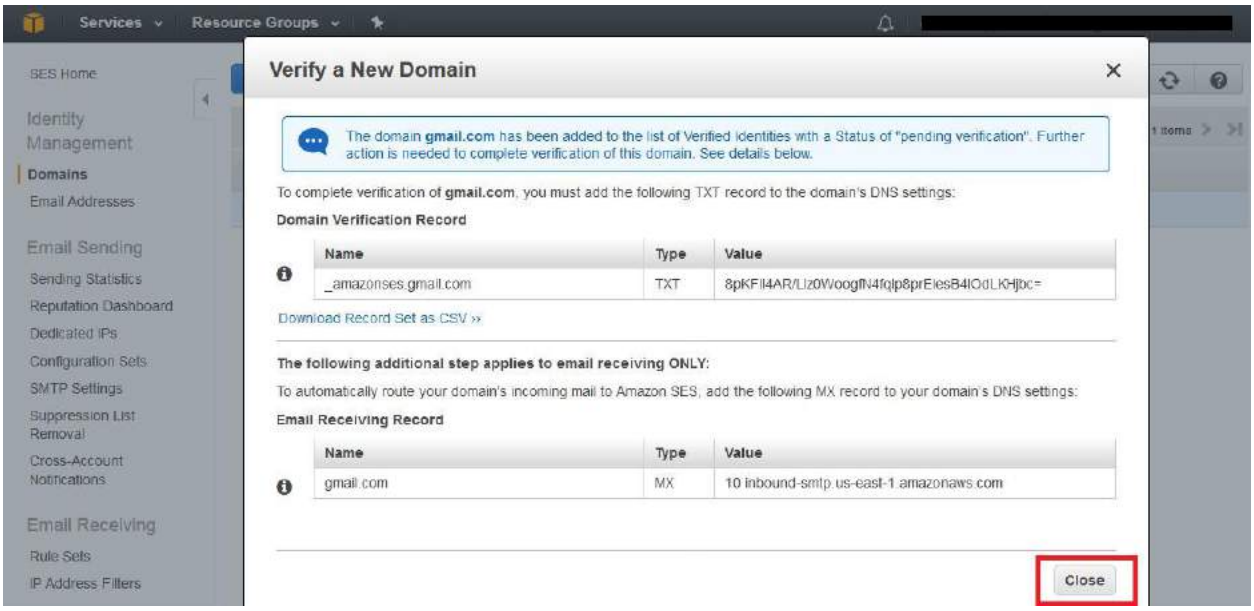


- Click on Domain for registering a new domain and it would take 24 hours of time to register a new domain by verifying AWS.

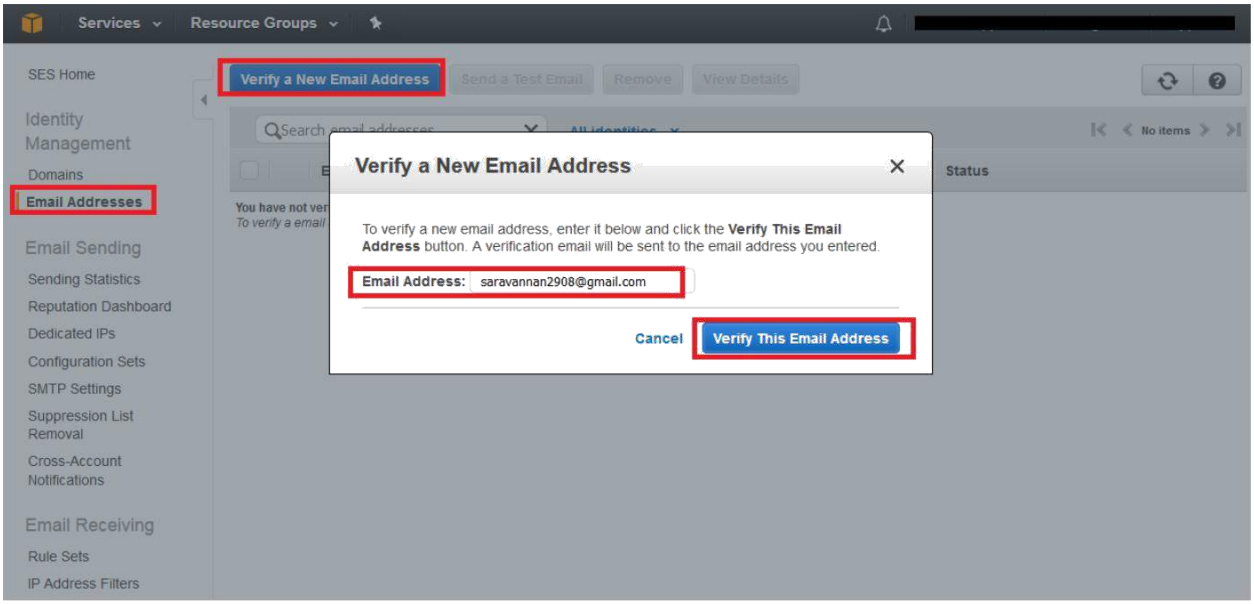


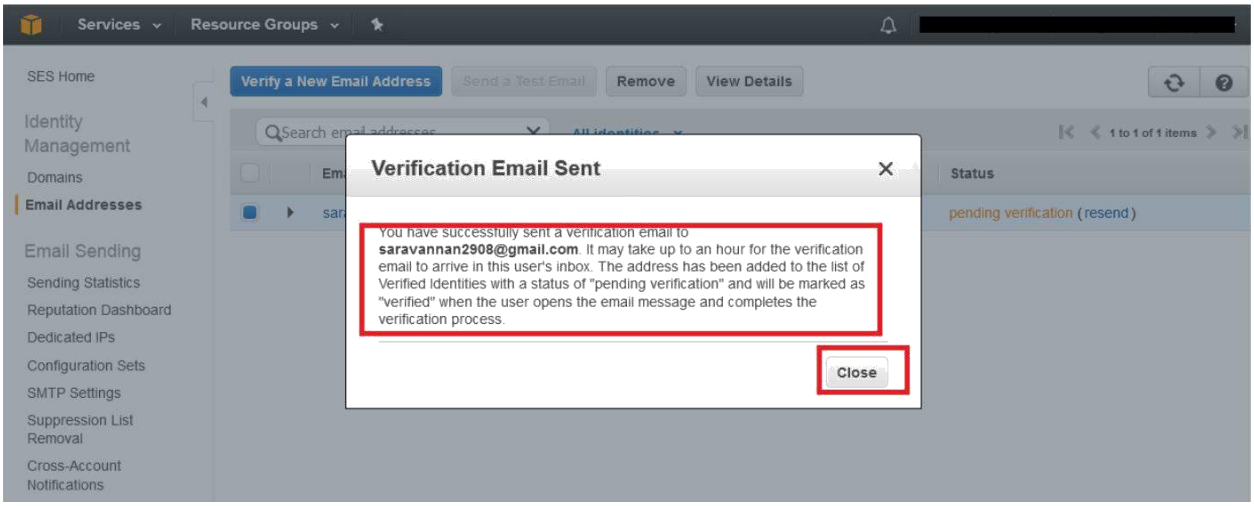


- After mapping a domain, we need to add this record values in Domain's DND settings.



- Navigate to E-Mail addresses, provide a send email address from which you need to send an email to all participants as like shown below.





- Verification email would be sent, and we need to click on confirming an email address for activating this email ID which we have been mapped as like shown below.
- Click on the link which has been received for activating this email address.
- After that, message would be displayed by stating Email address has been verified successfully.
- Navigate back to AWS and refresh the screen by clicking on refresh symbol as like shown below to display email has been verified.

Amazon Web Services – Email Address Verification Request in region US East (N. Virginia)

Inbox x

Amazon Web Services <no-reply-aws@amazon.com>

to me

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US East (N. Virginia). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

https://email-verification.us-east-1.amazonaws.com/?AWSAccessKeyId=AKIAJRRY6IQWNCSWXCTA&Context=661073341383&Identity.IdentityName=saravannan2908%40gmail.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=3QTKFkZ4MtWDmVLoYXEomSsWtLAfX7sR3JLte1R2ylc%3D&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-09-14T06%3A46%3A30.905Z

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Menu | aws | Products | Solutions | Pricing | More | English | My Account | Create an AWS Account

PRODUCTS & SERVICES

- Verification Successful
- Product Details
- Pricing
- Getting Started
- Resources
- FAQs

RELATED LINKS

- Documentation
- Management Console
- Release Notes

Congratulations!

You have successfully verified an email address. You can now start sending email from this address.

For new Amazon SES users—If you have not yet applied for a sending limit increase, then you are still in the sandbox environment, and you can only send email to addresses that have been verified. To verify a new email address or domain, see the **Identity Management** section of the Amazon SES console.

For new Amazon Pinpoint users—If you have not yet applied for a sending limit increase, then you are still in the sandbox environment, and you can only send email to addresses that have been verified. To verify a new email address or domain, see the **Settings** > **Channels** page on the Amazon Pinpoint console.

If you have already been approved for a sending limit increase, then you can start sending email to non-verified addresses.

Thank you for using Amazon Web Services!

Services | Resource Groups | [redacted]

SES Home

Identity Management

- Domains
- Email Addresses

Email Sending

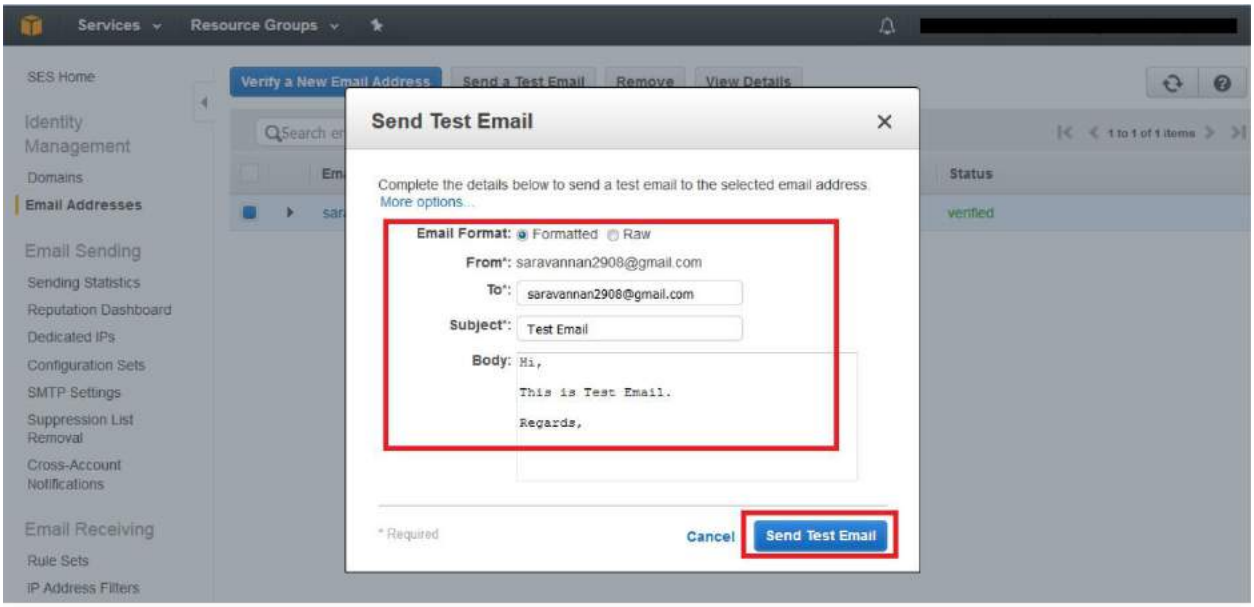
- Sending Statistics
- Reputation Dashboard
- Dedicated IPs
- Configuration Sets
- SMTP Settings
- Suppression List Removal
- Cross-Account Notifications

Verify a New Email Address | Send a Test Email | Remove | View Details

Search email addresses | All identities | 1 to 1 of 1 items

Email Address Identities	Status
saravannan2908@gmail.com	verified

- Once an email address has been verified, Click on Send Test email for verifying the same and also ensure you have been received an email through AWS SES as like shown below.



Simple Queue Service:

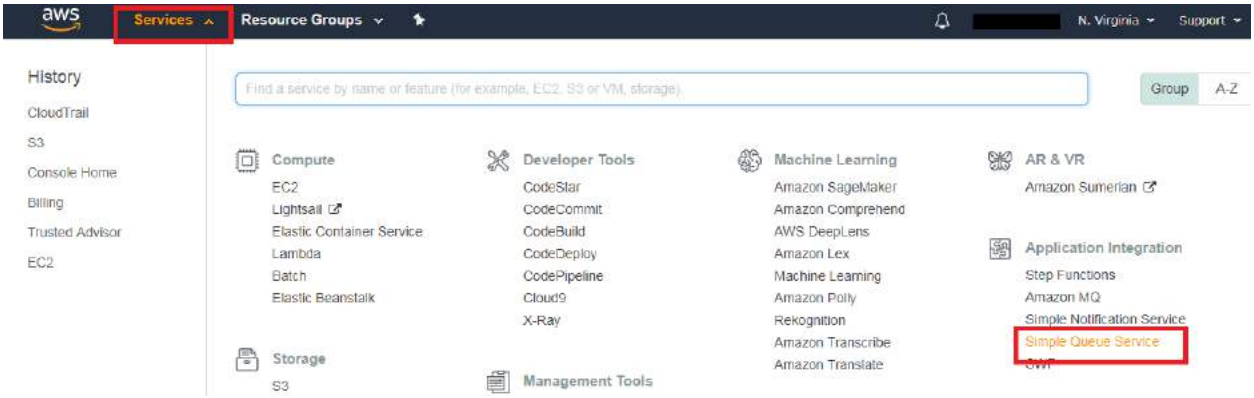
- Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.

- Building applications from individual components that each perform a discrete function improves scalability and reliability and is best practice design for modern applications.

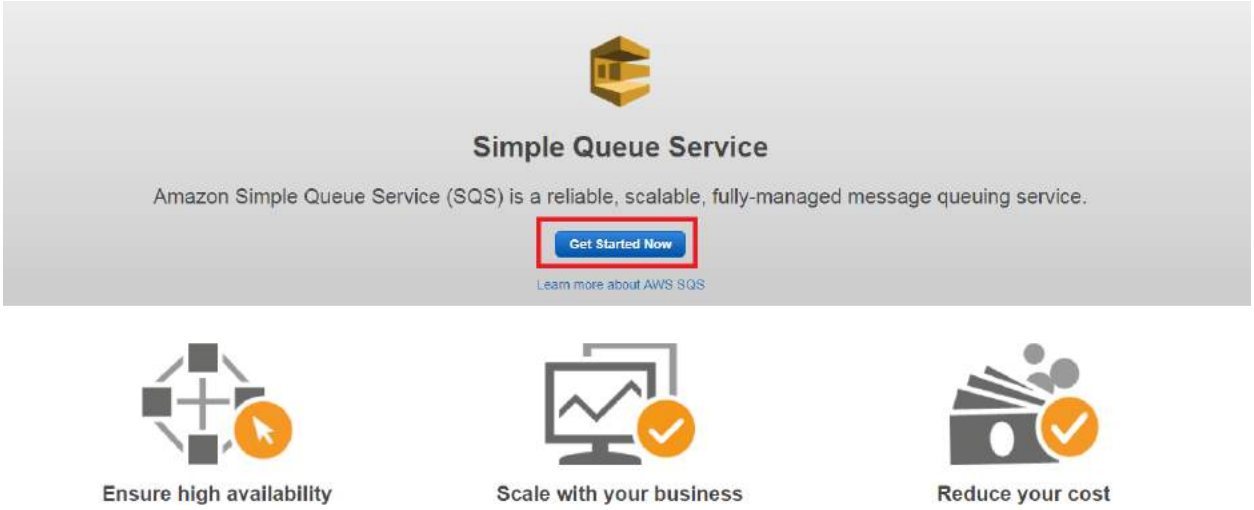
- SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available.

- SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent, with limited throughput.

- Click on Services and Select SQS.

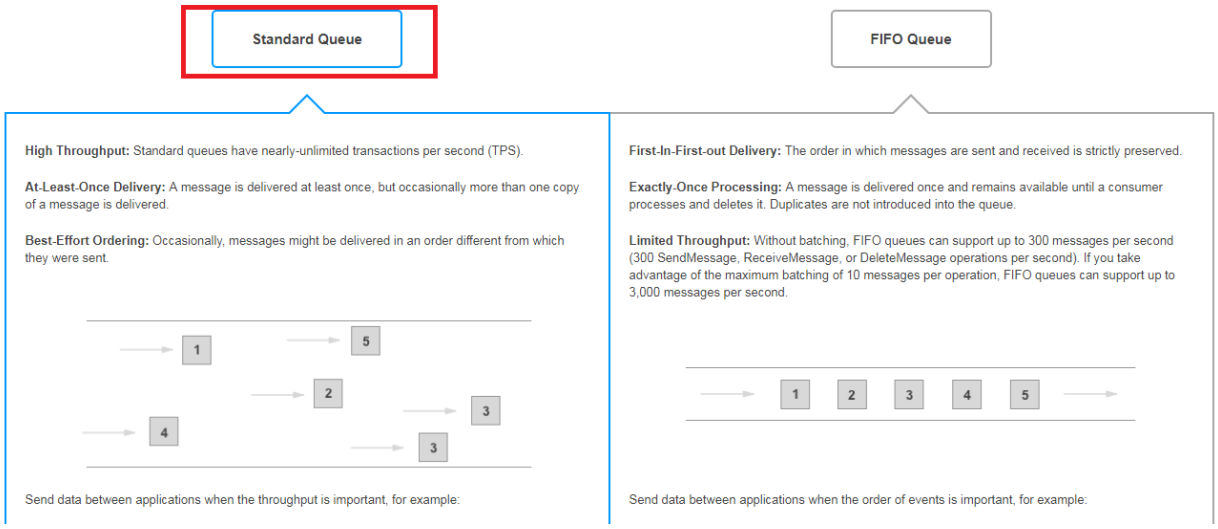


- Click on Get Started Now.

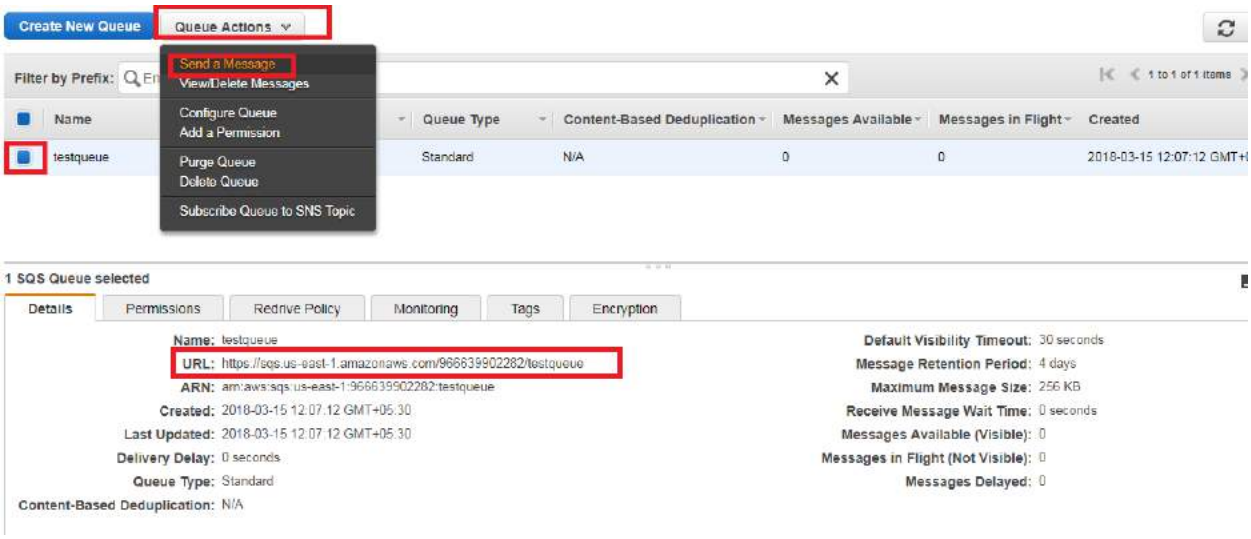


- Provide the Queue name.

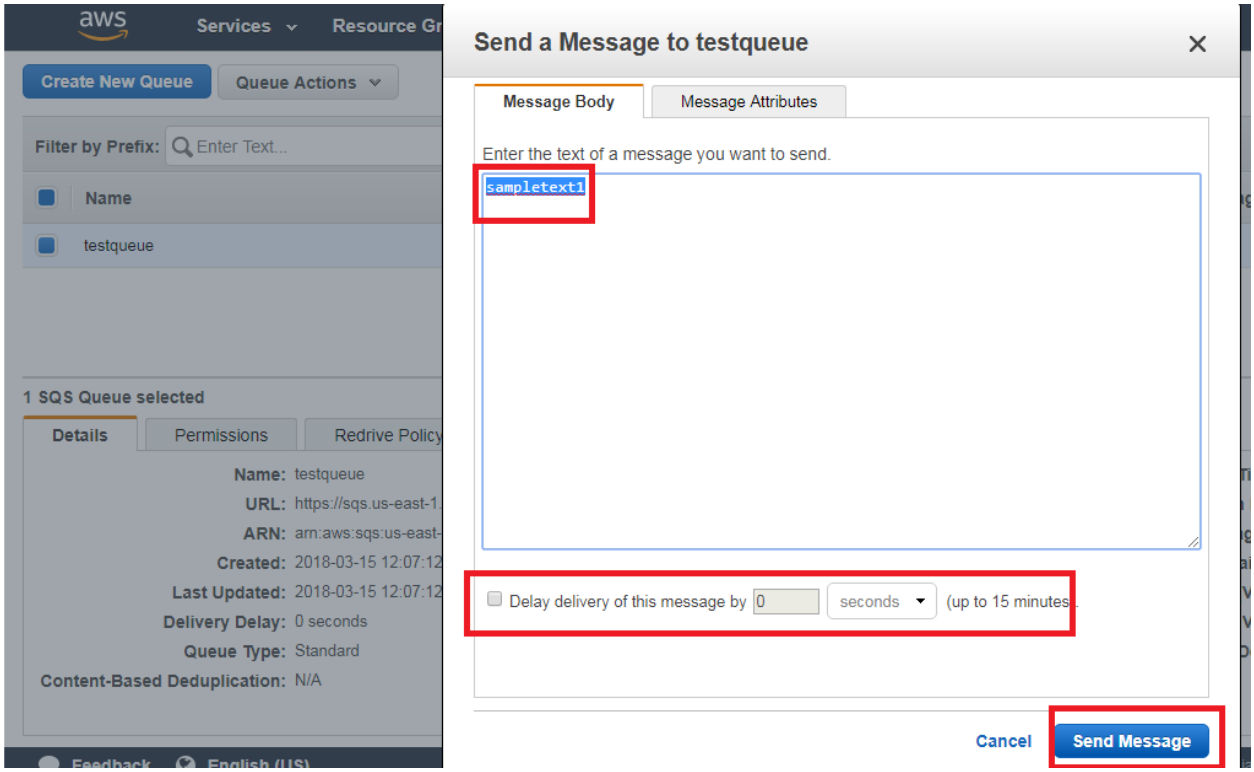
- Choose the type based upon application functionality.



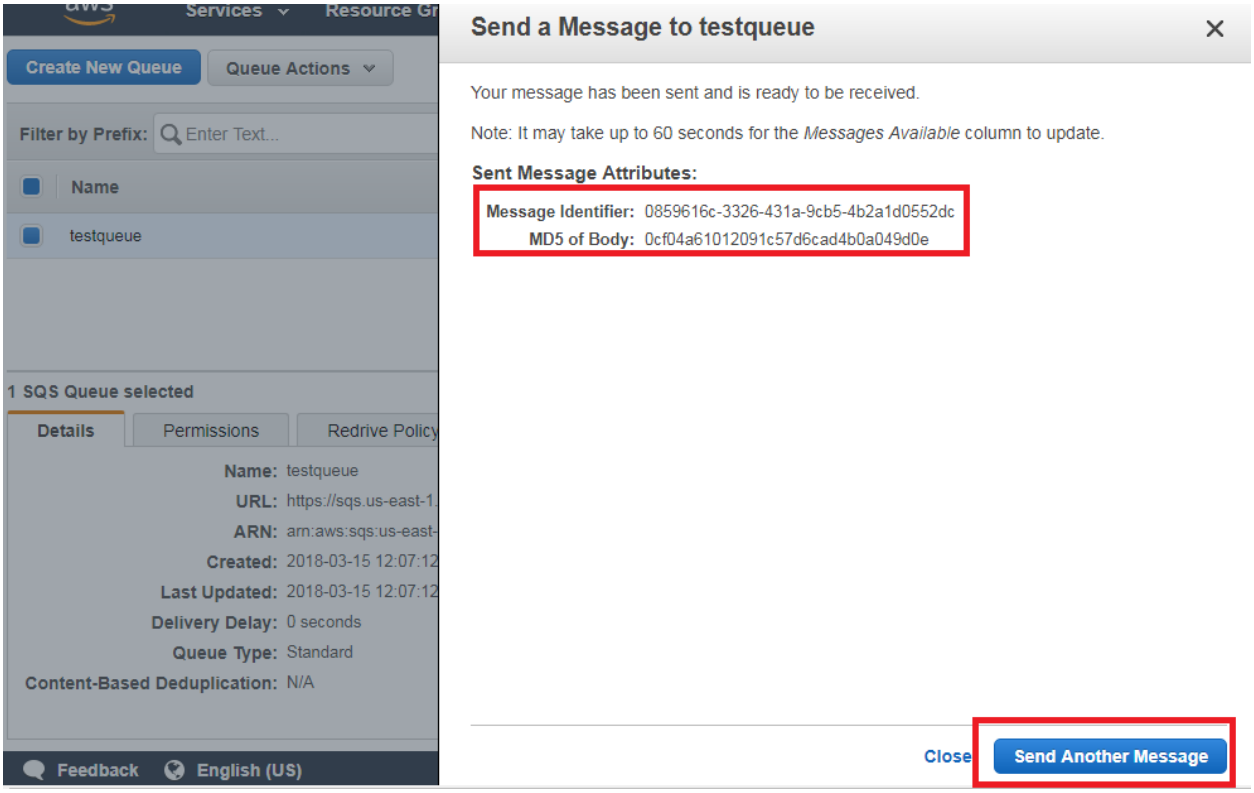
- After the Queue creation, you could be able to see an URL which could be configured in your application. So that, end users will be accessing your application to send any messages which will be saved in this SQS.



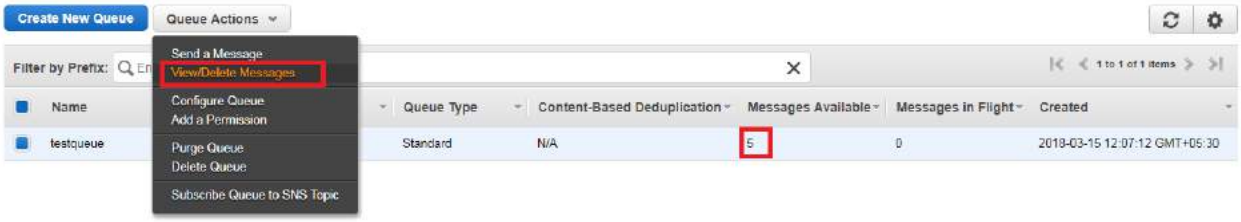
- Since we do not have an application, we are sending these messages manually to check the functionality of the same.



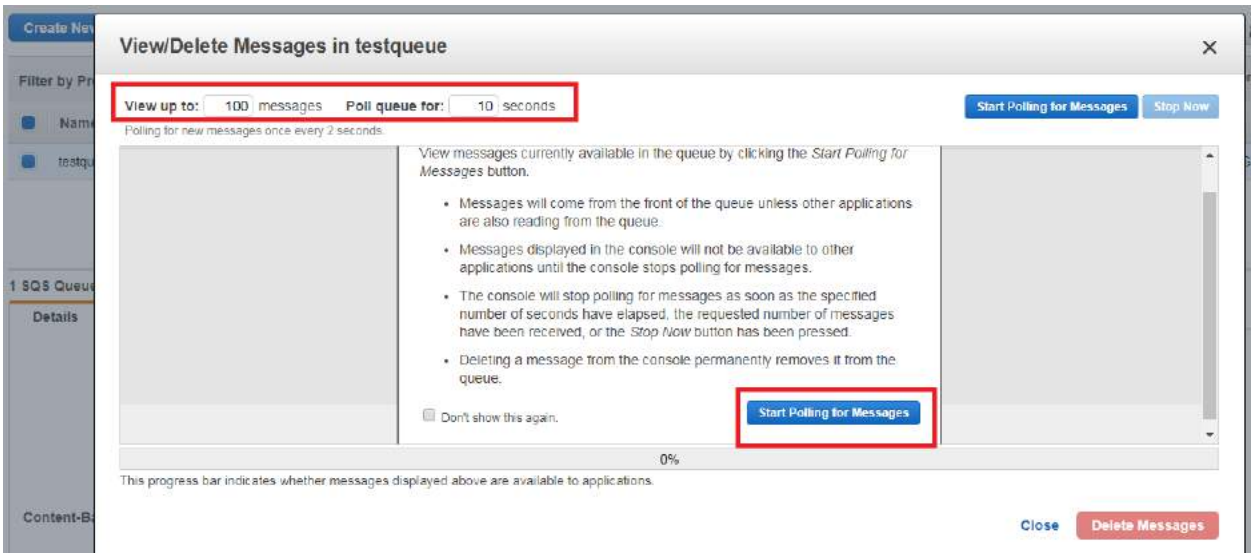
- You could send number of messages and after sending each messages, you will be receiving message identifier.



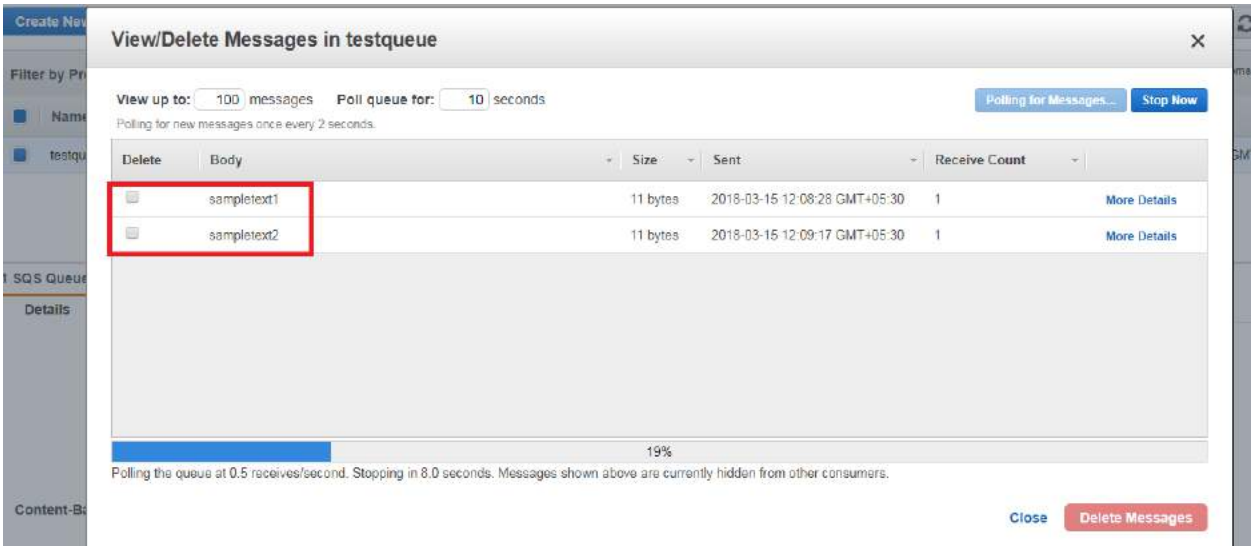
- 5 Messages are available in Queue and the same can be loaded into SQS by choosing View / Delete messages.



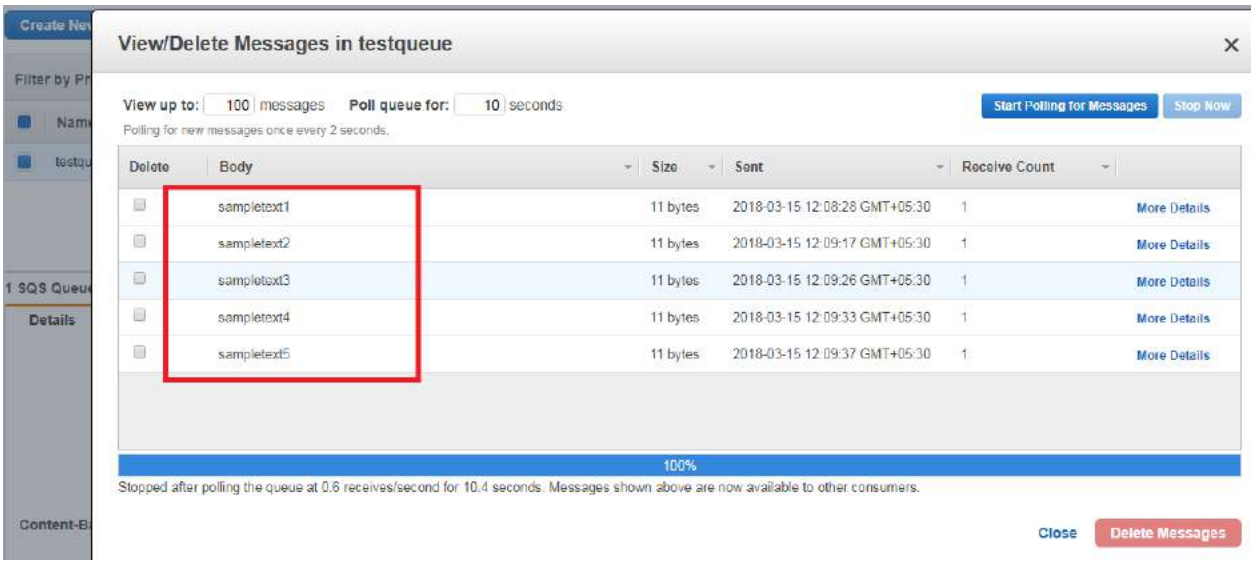
- Click on Start Polling messages to generate the same.



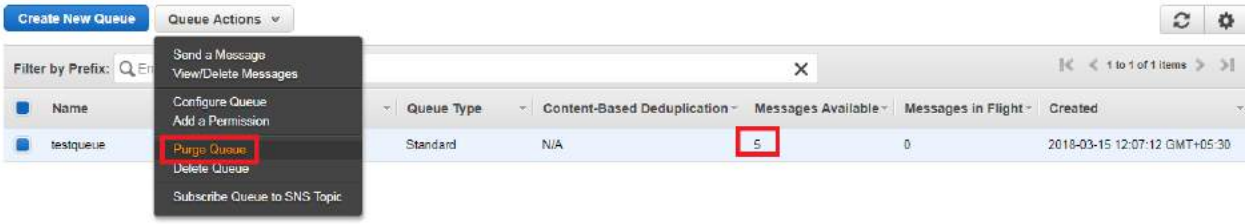
- Messages are started to receive in SQS.



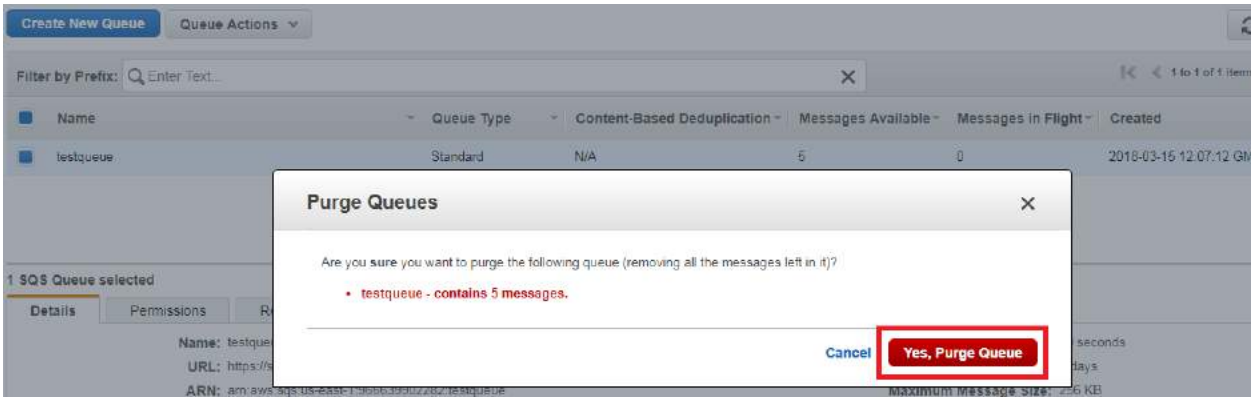
- We have been received all the messages which has been sent in a 10 seconds of time.



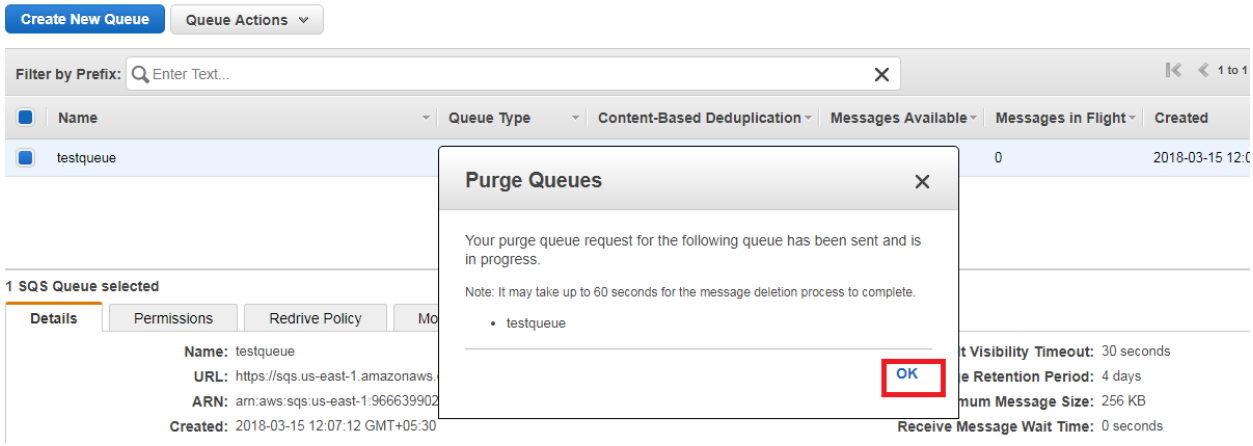
- Purge Queue is to delete the messages without deleting the SQS.



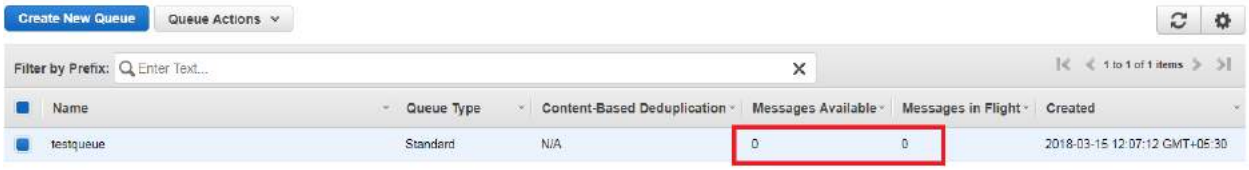
- Confirm to delete the messages.



- Messages are started to delete once you click on ok.

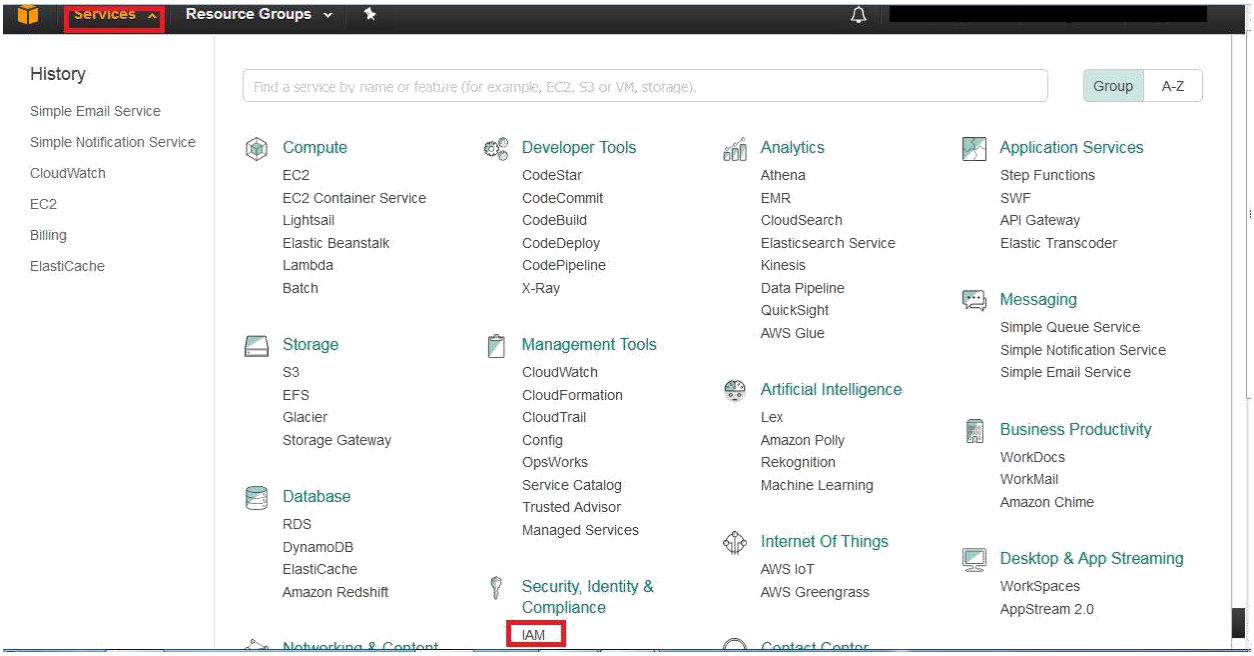


- All the messages have been deleted successfully.

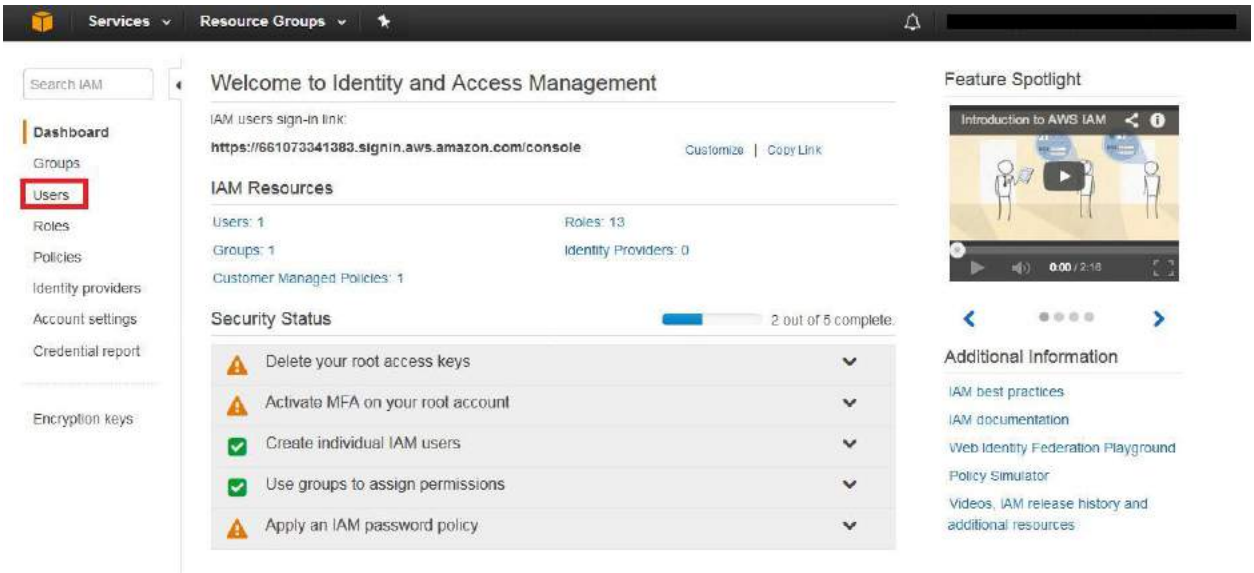


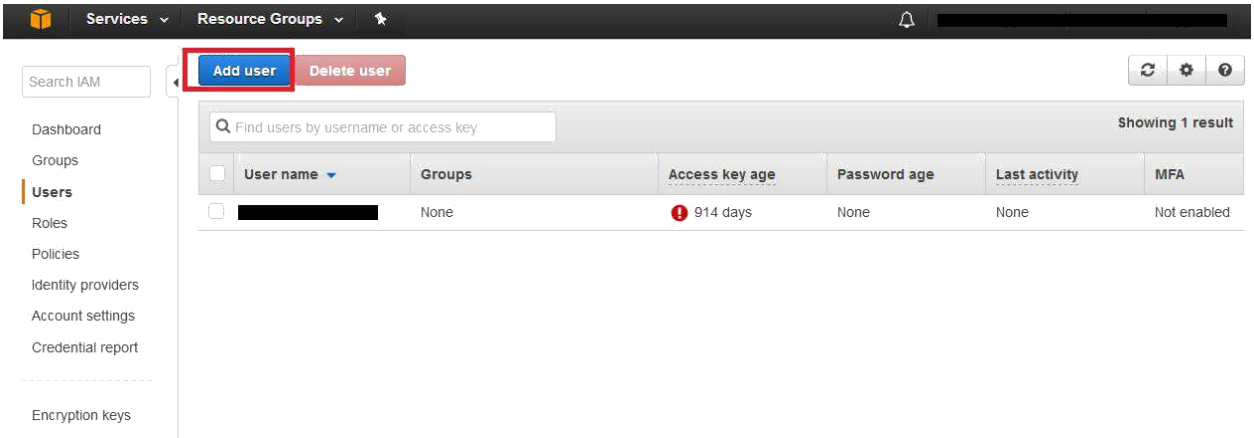
Identity and Access Management (IAM):

- AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.
- To be simple, you would be able to create several sub users under your primary account and also able to allocate specific privileges to those sub users which are being created.
- Navigate to service; select IAM under Security, Identity & Compliance as like shown below.

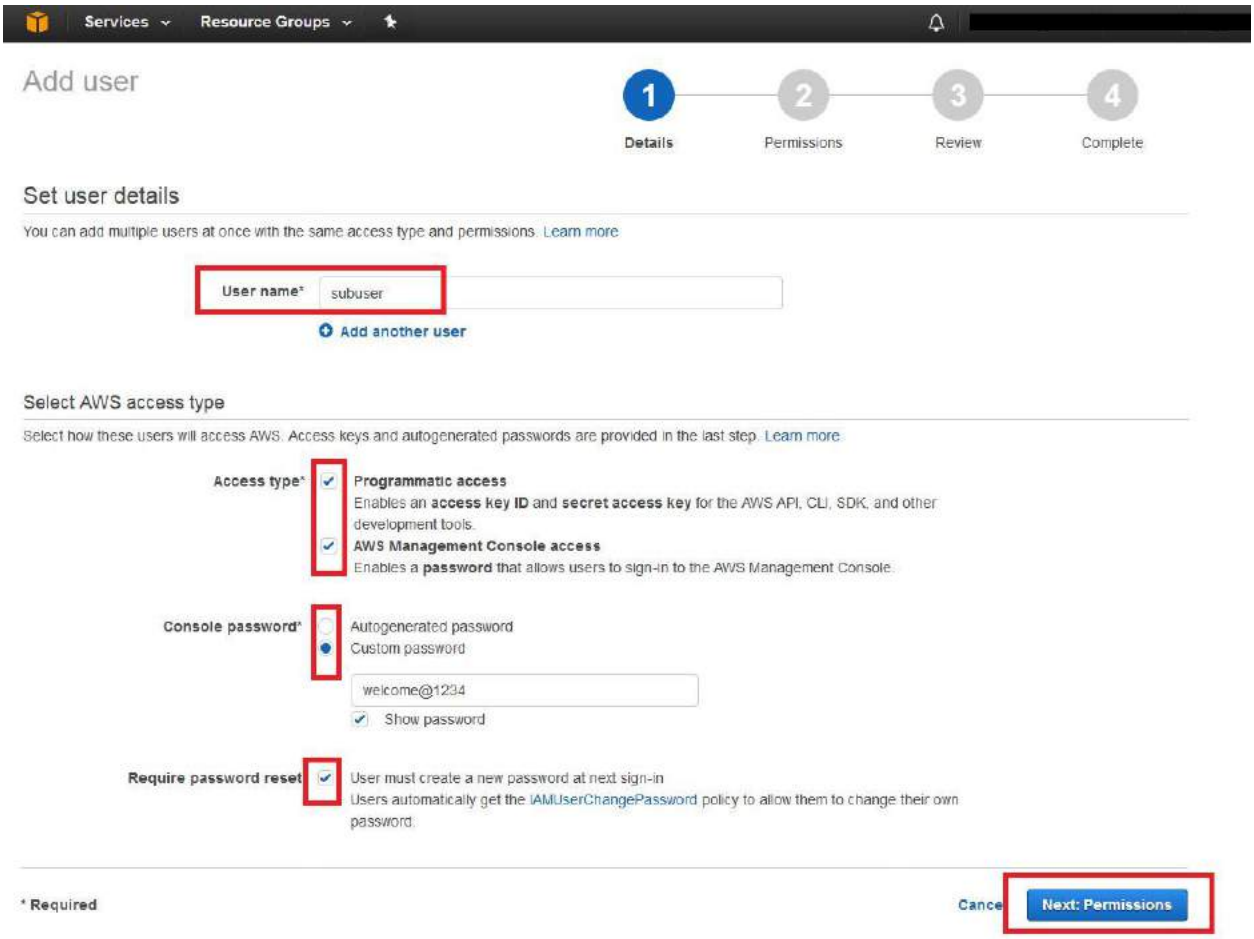


- Click on Users >> Add User for creating a new user under primary account.

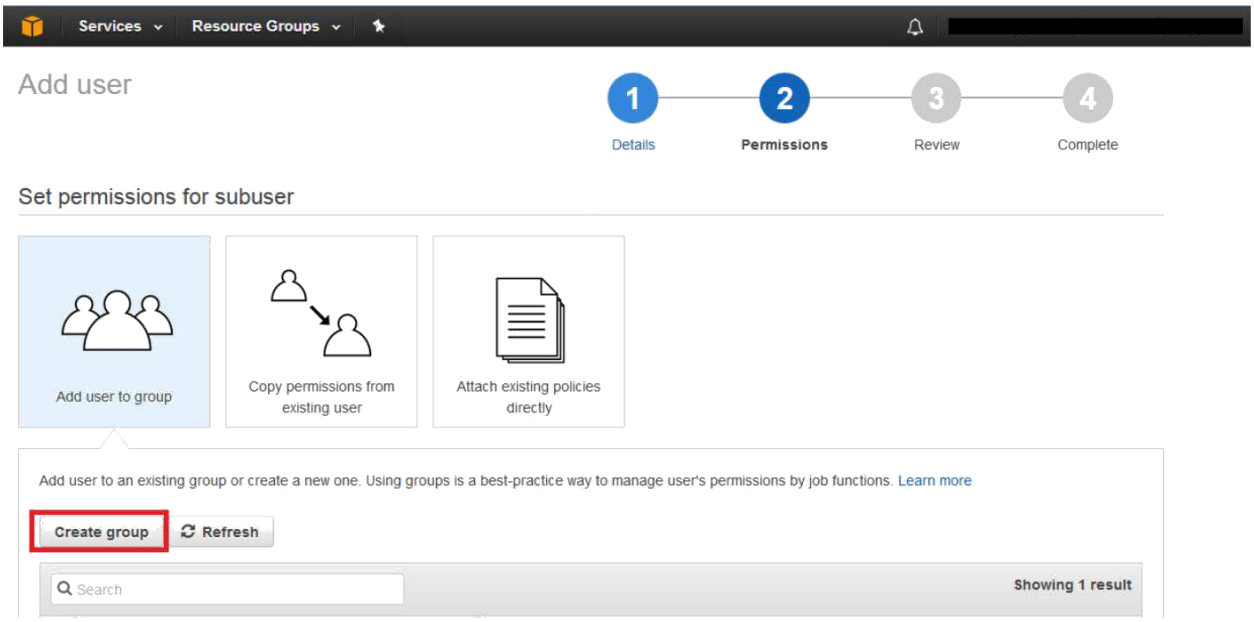


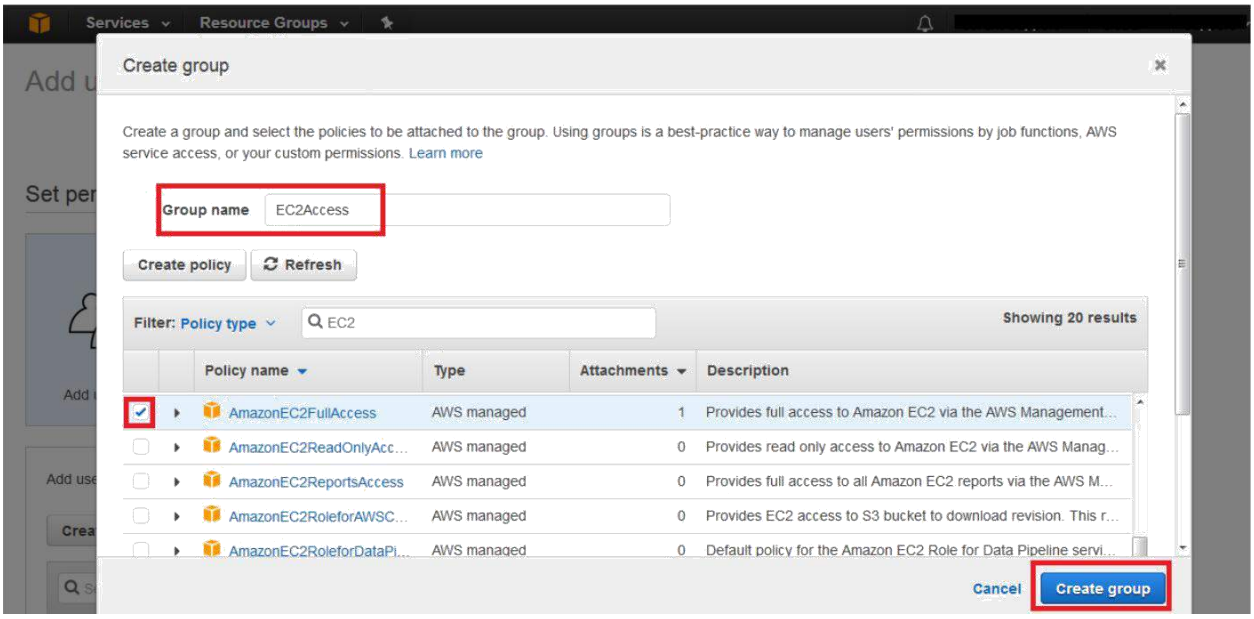


- Provide a username, Access type whether to access AWS in browser or using CLI and type the password for sub user account & proceed with Next steps as like shown below.

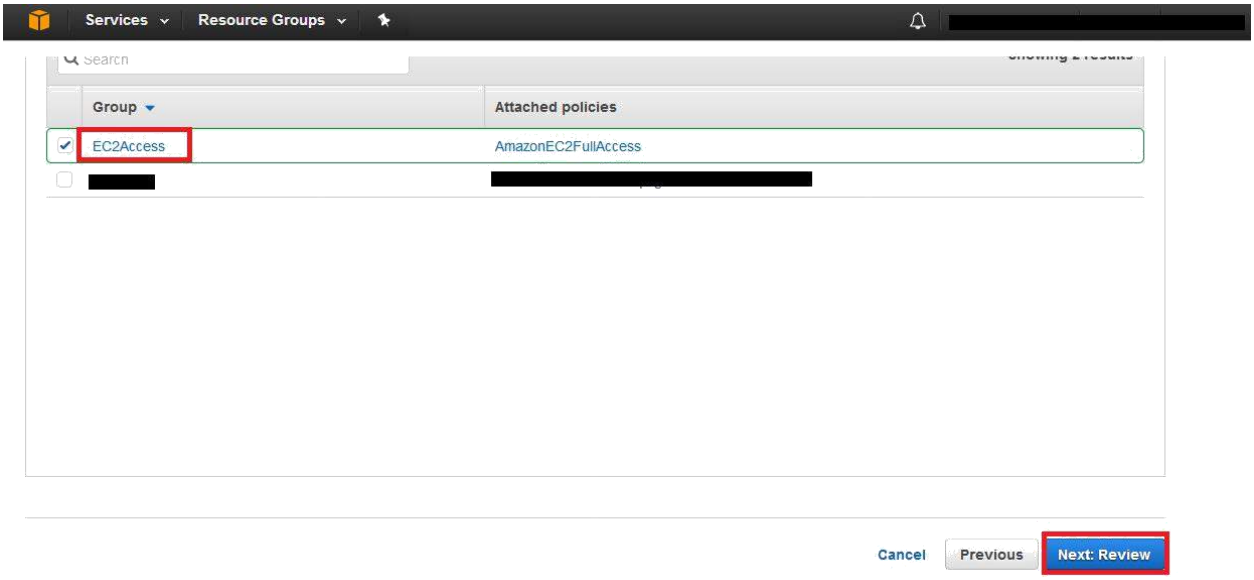


- Create a new Group to determine a certain privilege for this user which are being created.

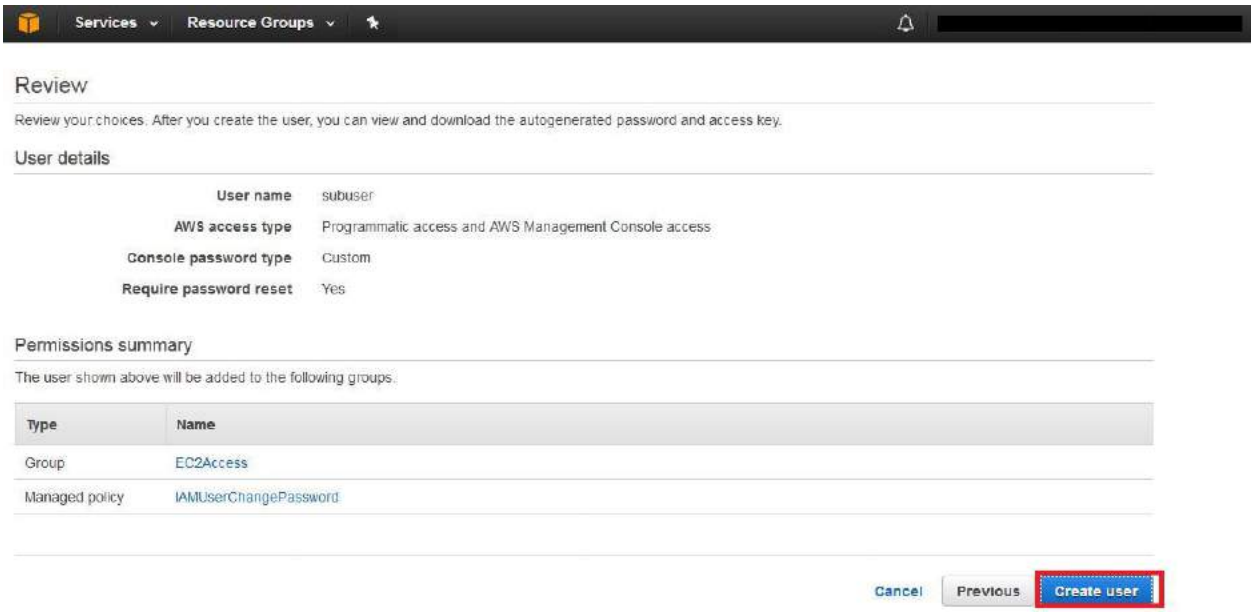




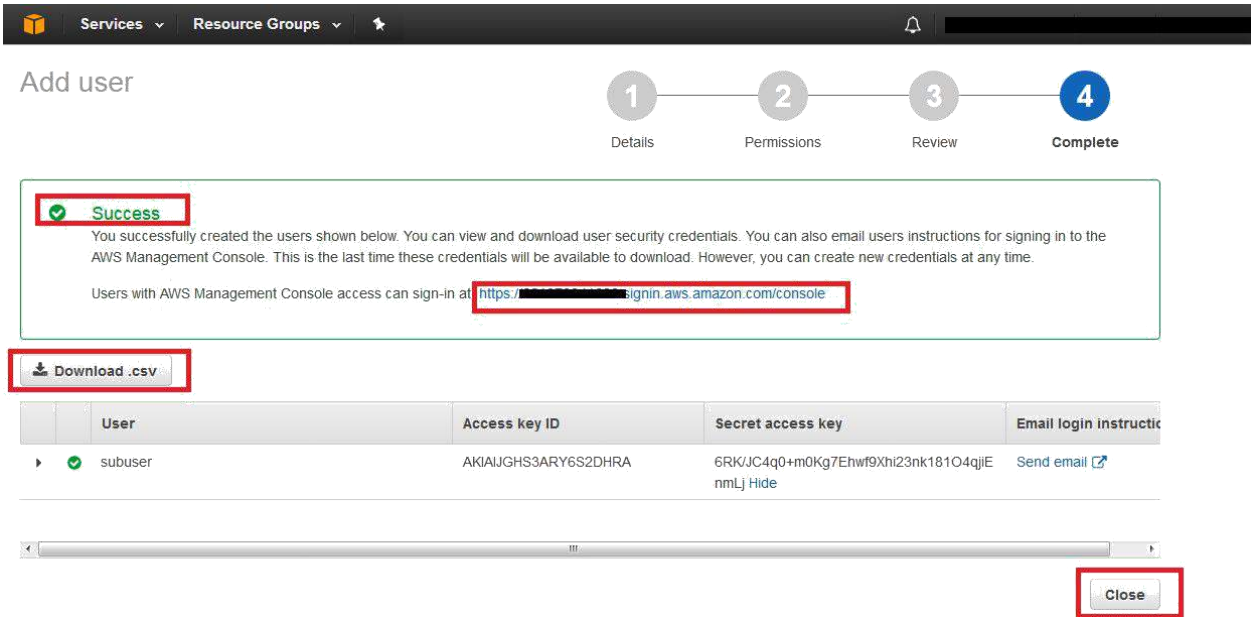
- After allocating the privileges to this user, click on create Group and proceed with the next steps for creating a new user.
- We have been provided all privileges to access EC2 console for this sub account.
- This user wouldn't be able to access any other modules except EC2, since we have provided only EC2 permission while creating a group as seen above.



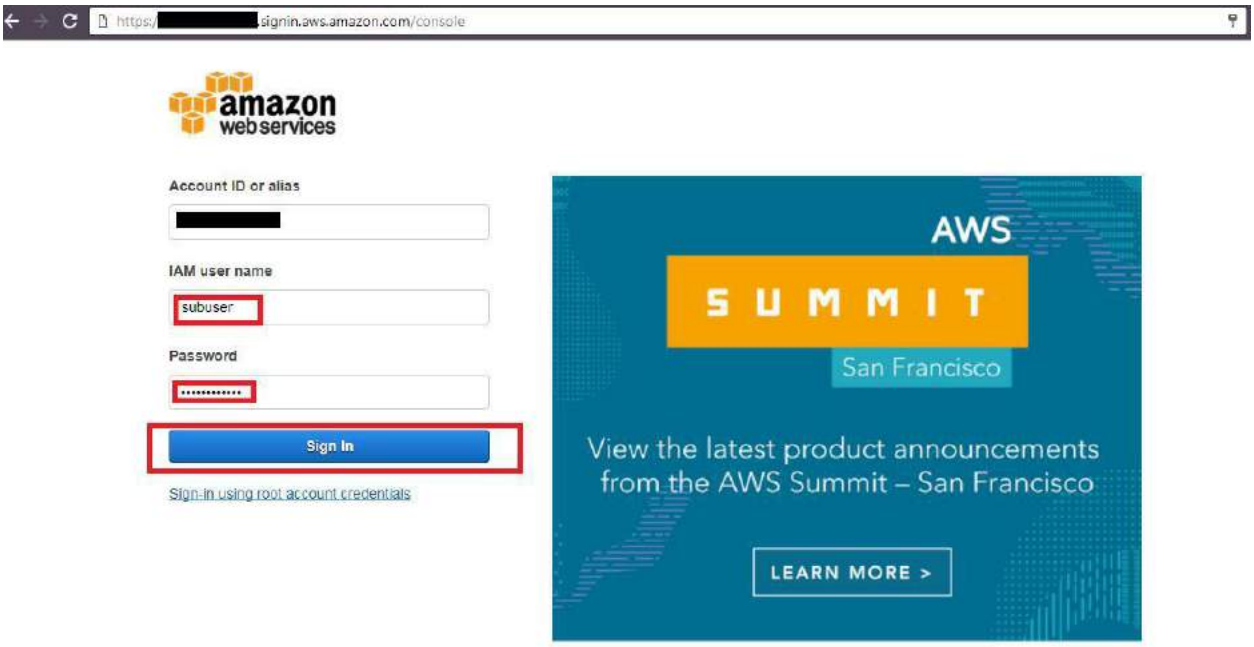
- Click on Create user for creating a new user.



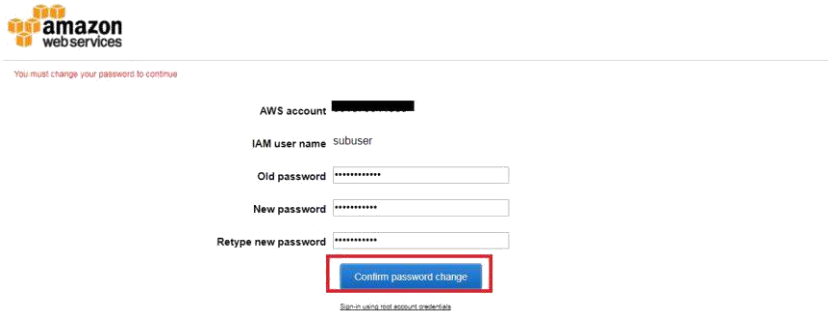
- Copy this URL for logging into sub account, download this csv files which contains Access Key and Secret key for future use.



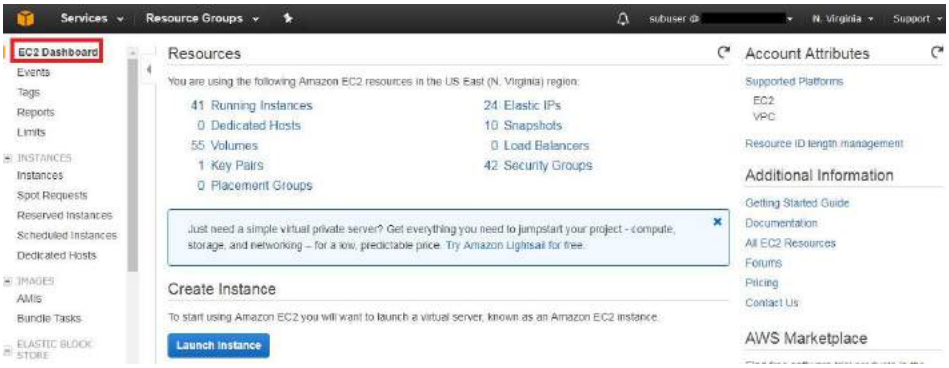
- Open a new browser paste the copied URL for logging into Sub Account / User by providing an authentication which has been created now as like shown below.



- After Sign in, it would prompt to change the password. Provide the new password for this sub account and proceed with next steps.

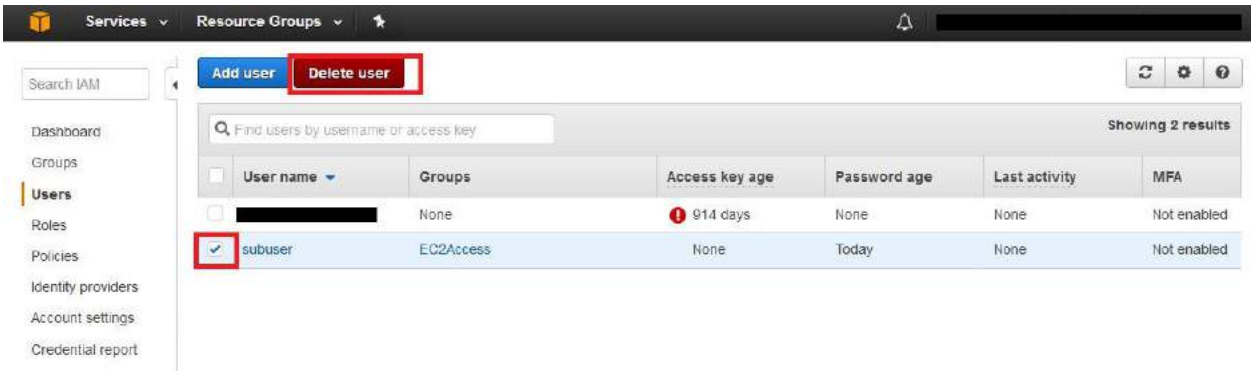


- Logged into Sub Account, navigated to EC2 section as like shown below. This Sub account has privileges to do any changes in an EC2.



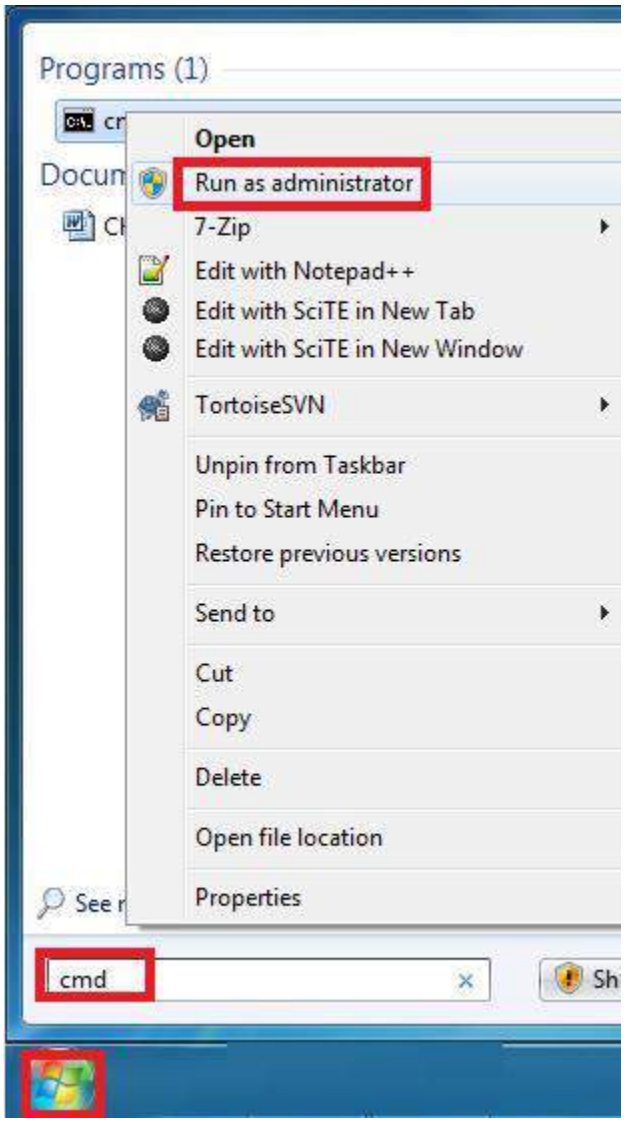
- Now, when that user trying to access any other modules apart from EC2, it will throw up an error message as like shown below.

- Click on created sub user for deleting the same and once user has been deleted, it cannot be retrieved back.



Command Line Interface (CLI):

- The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.
- Download this CLI using below URL.
- https://s3.amazonaws.com/aws-cli/AWSCLI32.msi
- Proceed with an installation once this file has been downloaded as like normal exe file installation.
- Once this installation completed, open a command prompt with Administrator Privileges as like shown below.



- Execute the following commands in command prompt to map your AWS account in CLI using Access Key and Secret key which can be found in IAM.
- aws configure
- Provide Access Key

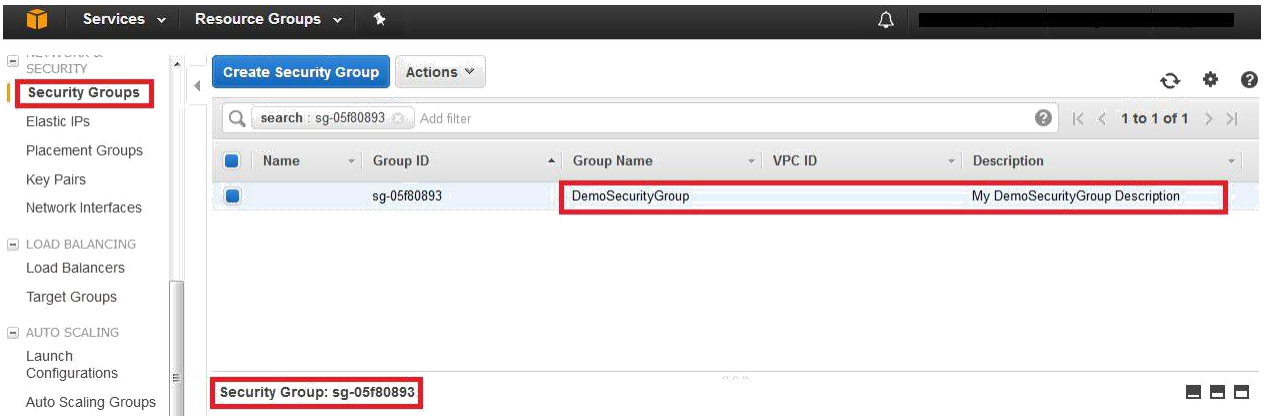
- Provide Secret Key
- Provide Default Region as us-east-1
- Provide output as text

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>aws configure
AWS Access Key ID [**********75JQ]: [redacted]
AWS Secret Access Key [**********hIUT]: [redacted]
Default region name [us-east-1]: us-east-1
Default output format [text]: text

C:\Windows\system32>
```

- After executing these commands, you would be able to do any actions in your AWS account without logging into browser. There are millions of commands to do any actions in AWS account and the same can be found in below given URL for your reference.
- http://docs.aws.amazon.com/cli/latest/reference/
- I am going to create a new security group on EC2 using the CLI. Command to create it is given below. After execution of this command, a new Security Group will be created and Security Group ID would be displayed in Command Prompt itself.
- aws ec2 create-security-group --group-name DemoSecurityGroup --description "My DemoSecurityGroup Description"

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>aws configure
AWS Access Key ID [**********75JQ]: [redacted]
AWS Secret Access Key [**********hIUT]: [redacted]
Default region name [us-east-1]: us-east-1
Default output format [text]: text

C:\Windows\system32>aws ec2 create-security-group --group-name DemoSecurityGroup
 --description "My DemoSecurityGroup Description"
sg-05f80893

C:\Windows\system32>_
```

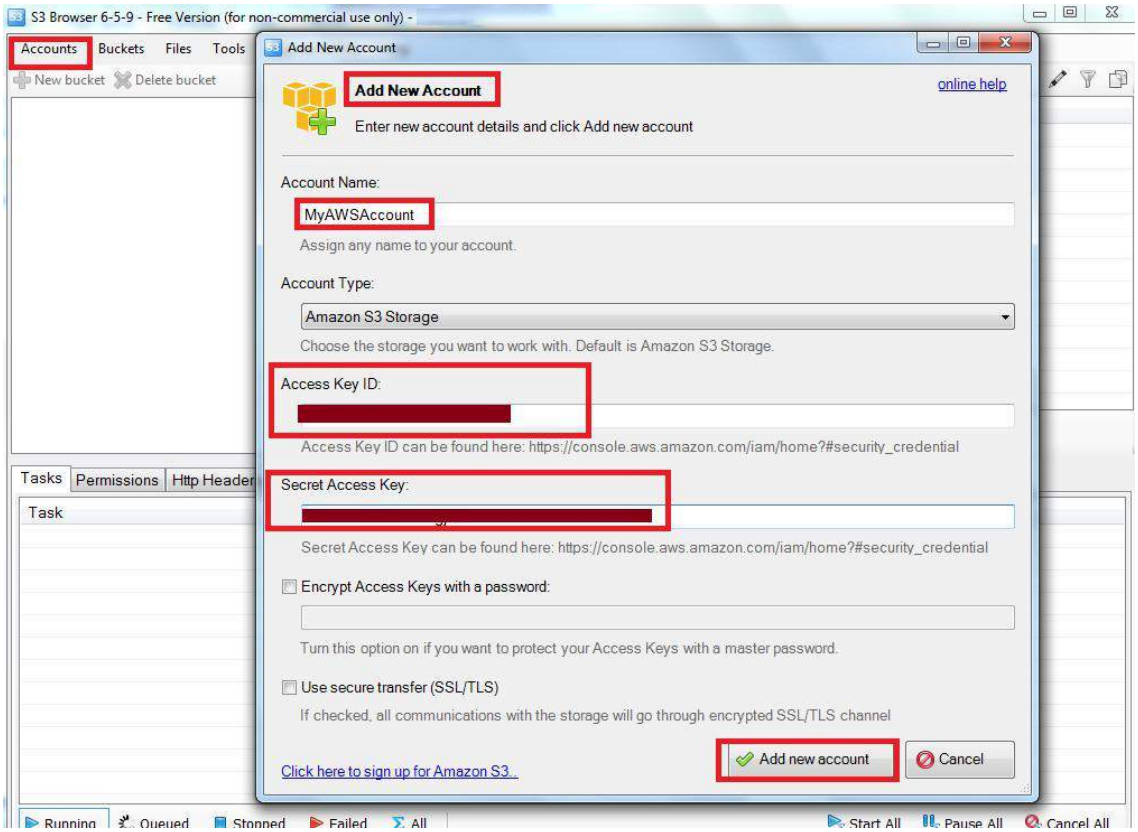
- Now, ensure the same by navigating to AWS console >> EC2 >> Security Groups as like given below. Security Group which has been created in CLI has been displayed in AWS console.



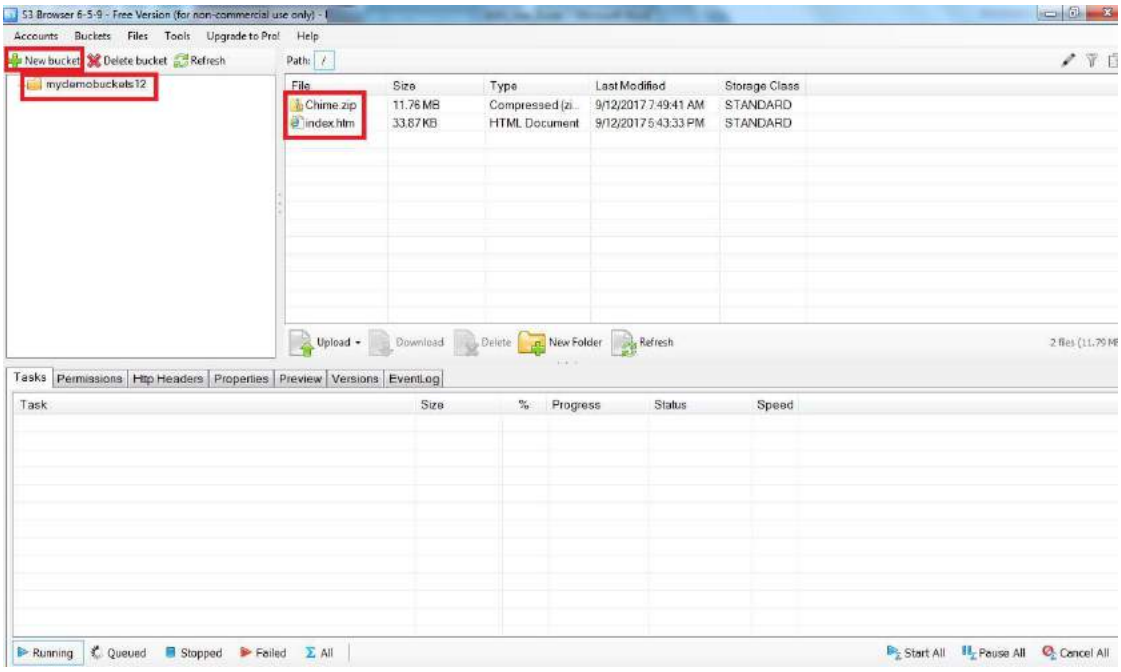
- Similarly, you would be able to do everything using the commands in CLI and you can refer the URL given above for finding more commands.

Simple Storage Service Browser (S3 Browser):

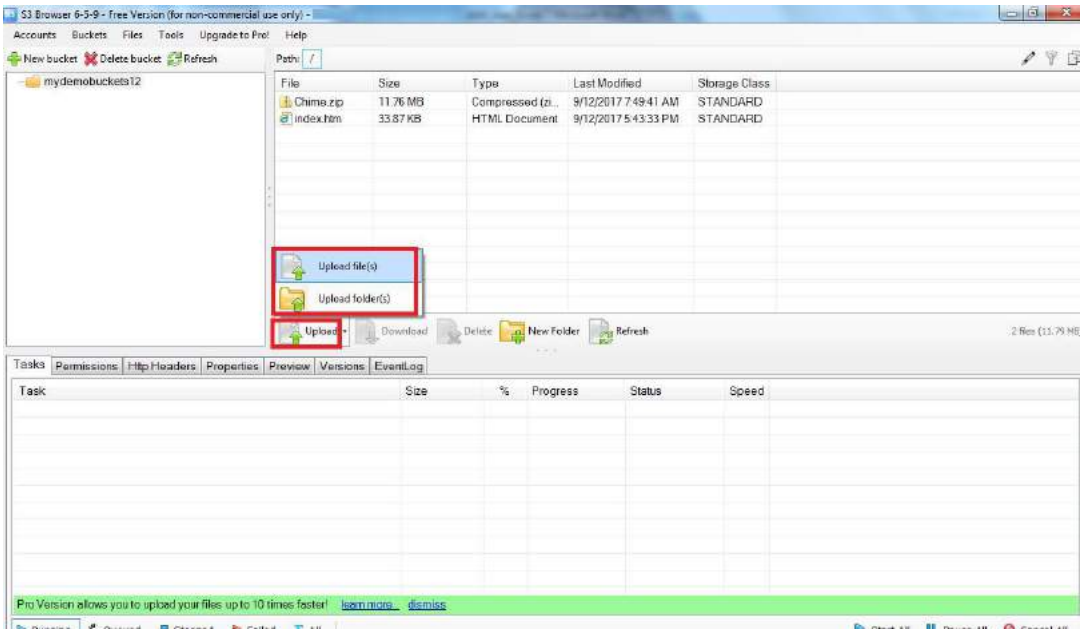
- S3 Browser is a freeware Windows client for Amazon S3. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.
- Download the file using the below link and proceed with an installation activity. http://netsdk.s3.amazonaws.com/s3browser/6.5.9/s3browser-6-5-9.exe
- After installation, open a S3 browser to add your AWS account using Access key and Secret Key.

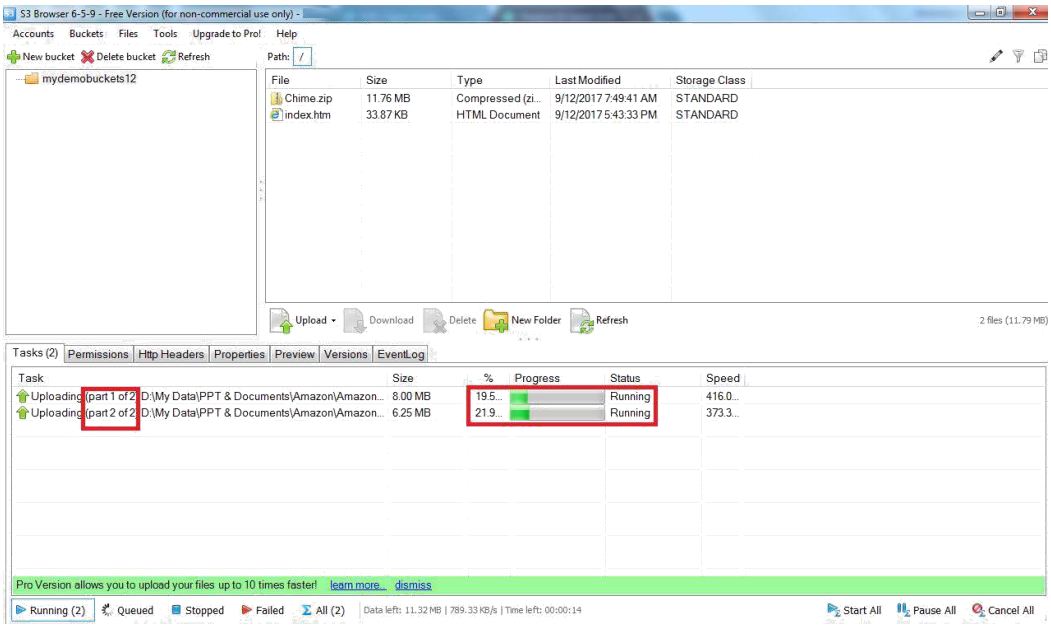


- After adding AWS account, you would be able to view the list of buckets which are available in your account. Also, you would be able to all actions whichever you are doing in AWS console.

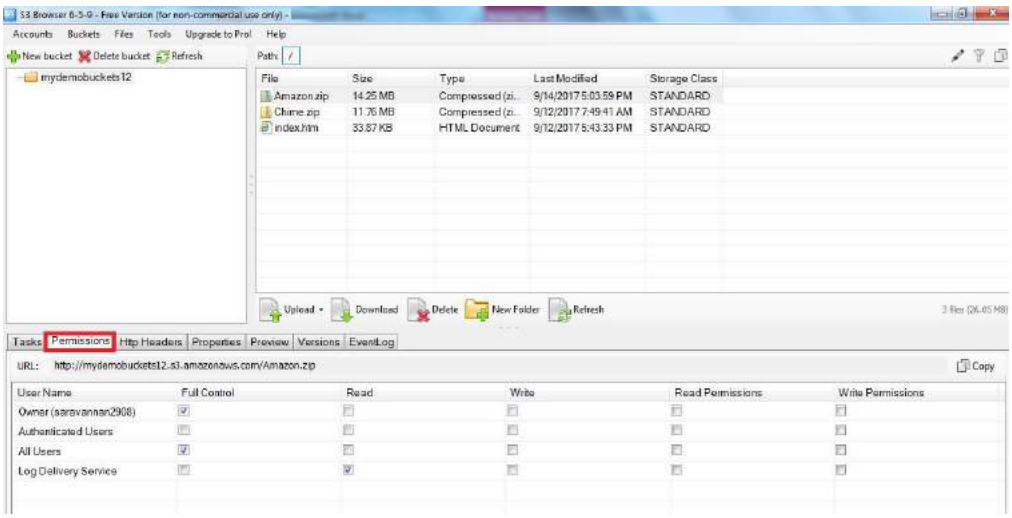


- Main advantage of using this S3 Browser is, during uploading of any huge volume of data to S3 Bucket and if network has been failed, it would be resuming an upload activity from where it has been failed since the data file would be uploaded part wise.
- Example of uploading the data files into the bucket is given below.



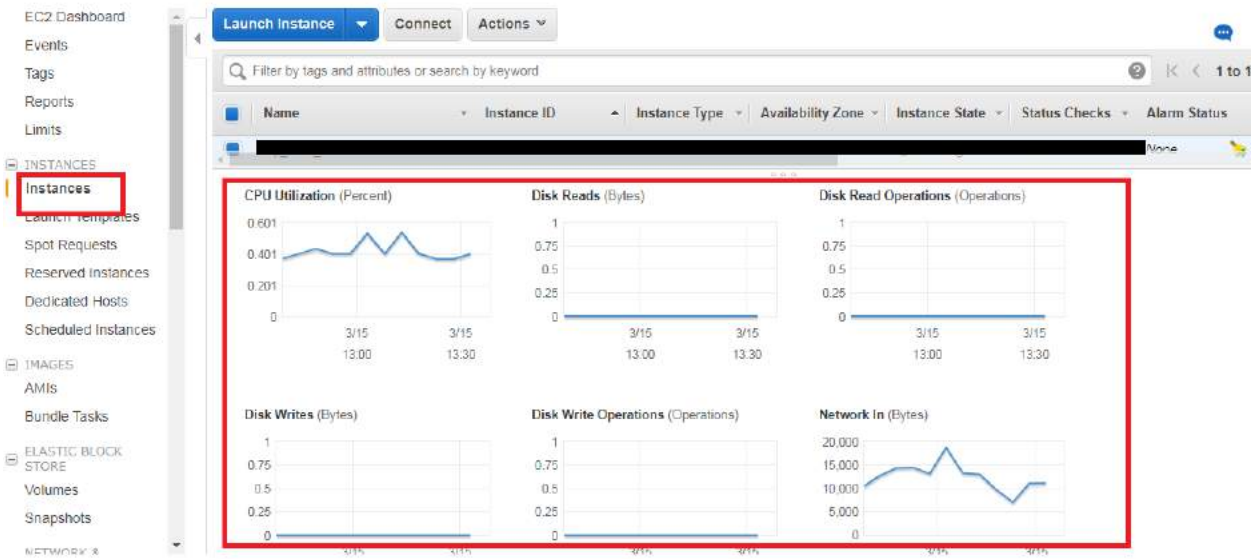


- We can able to provide permissions for uploaded file as like shown below.

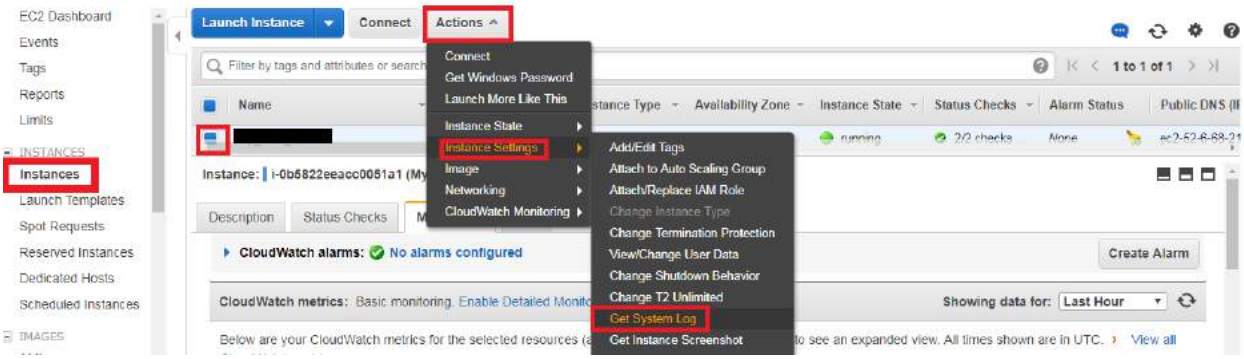


Troubleshooting:

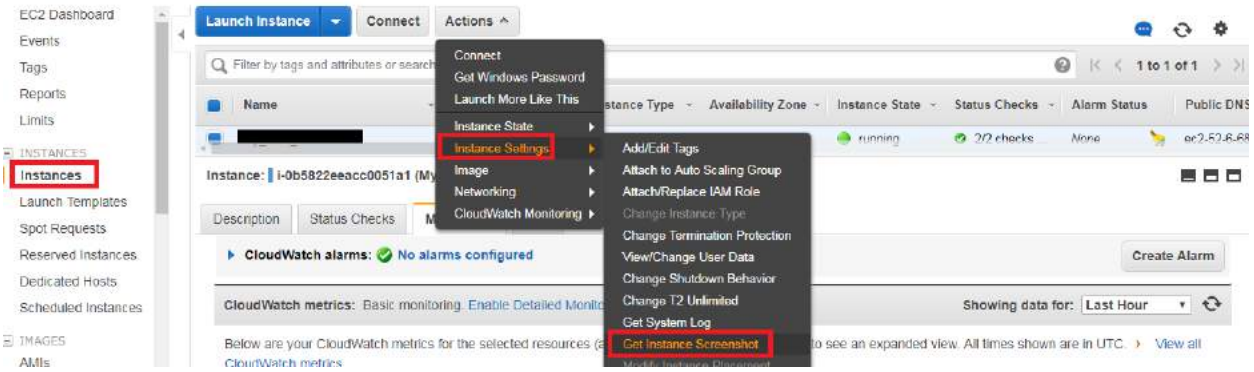
- If you couldn't able to take RDP or SSH of your EC2 instances, ensure RDP or SSH port has been opened in Security Group.
- If new volume has been attached and if it is not visible in EC2 instances, ensure that it is manually mounted.
- If you couldn't able to take SSH or RDP of the server check with instance health status like CPU & RAM by choosing monitoring option.



- To ensure the instance has been booted up properly, navigate to Actions >> Instance Settings >> Get System logs.



- Get an instance screenshot by navigating to Actions >> Instance Settings >> Get Instance Screenshot.



- If 2/2 status check doesn't come in display screen, restart or stop and start the server.

Error connecting to your instance: Connection timed out:

- Route table, for the subnet, does not have a route that sends all traffic destined outside the VPC to the Internet gateway for the VPC.
- Security group does not allow inbound traffic from the public ip address on the proper port
- ACL does not allow inbound traffic from and outbound traffic to the public ip address on the proper port
- Private key used to connect does not match with key that corresponds to the key pair selected for the instance during the launch
- Appropriate user name for the AMI is not used for e.g. user name for Amazon Linux AMI is ec2-user, Ubuntu AMI is ubuntu, RHEL5 AMI & SUSE Linux can be either root or ec2-user, Fedora AMI can be fedora or ec2-user
- If connecting from a corporate network, the internal firewall does not
- allow inbound and outbound traffic on port 22 (for Linux instances) or port 3389 (for Windows instances).
- Instance does not the same public IP address, which change during restarts. Associate an Elastic IP address with the instance
- CPU load on the instance is high; the server may be overloaded.

User key not recognized by server

- private key file used to connect has not been converted to the format as required by the server.

Host key not found, Permission denied (publickey), or Authentication failed, permission denied

- appropriate user name for the AMI is not used for connecting
- proper private key file for the instance is not used

Unprotected Private Key File

- private key file is not protected from read and write operations from any other users.

Server refused our key or No supported authentication methods available

- appropriate user name for the AMI is not used for connecting

EC2 Troubleshooting Instances with Failed Status Checks

- System Status Check – Checks Physical Hosts
- Loss of Network connectivity
- Loss of System power
- Software issues on physical host
- Hardware issues on physical host

Resolution

- Amazon EBS-backed AMI instance – stop and restart the instance
- Instance-store backed AMI – terminate the instance and launch a replacement.
- Instance Status Check – Checks Instance or VM

Possible reasons

- Misconfigured networking or startup configuration
- Exhausted memory
- Corrupted file system

- Failed Amazon EBS volume or Physical drive
- Incompatible kernel

Resolution

- Rebooting of the Instance or making modifications in your Operating system, volumes

EC2 Troubleshooting Instance Capacity

Insufficient Instance Capacity

- AWS does not currently have enough available capacity to service your request. There is a limit for number of instances of instance type that can be launched within a region.

Instance Limit Exceeded

- Concurrent running instance limit, default is 20, has been reached.

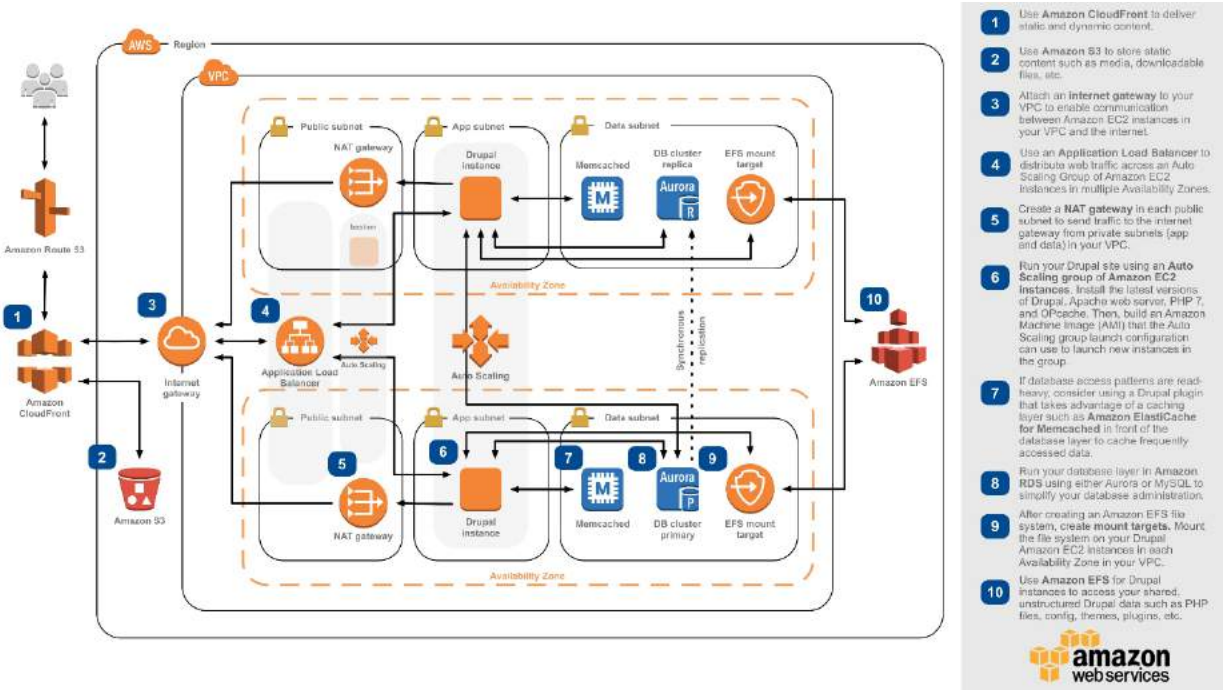
- Refer the below given URL for troubleshooting EC2 Instances and RDS.
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-troubleshoot.html
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html

Pricing:

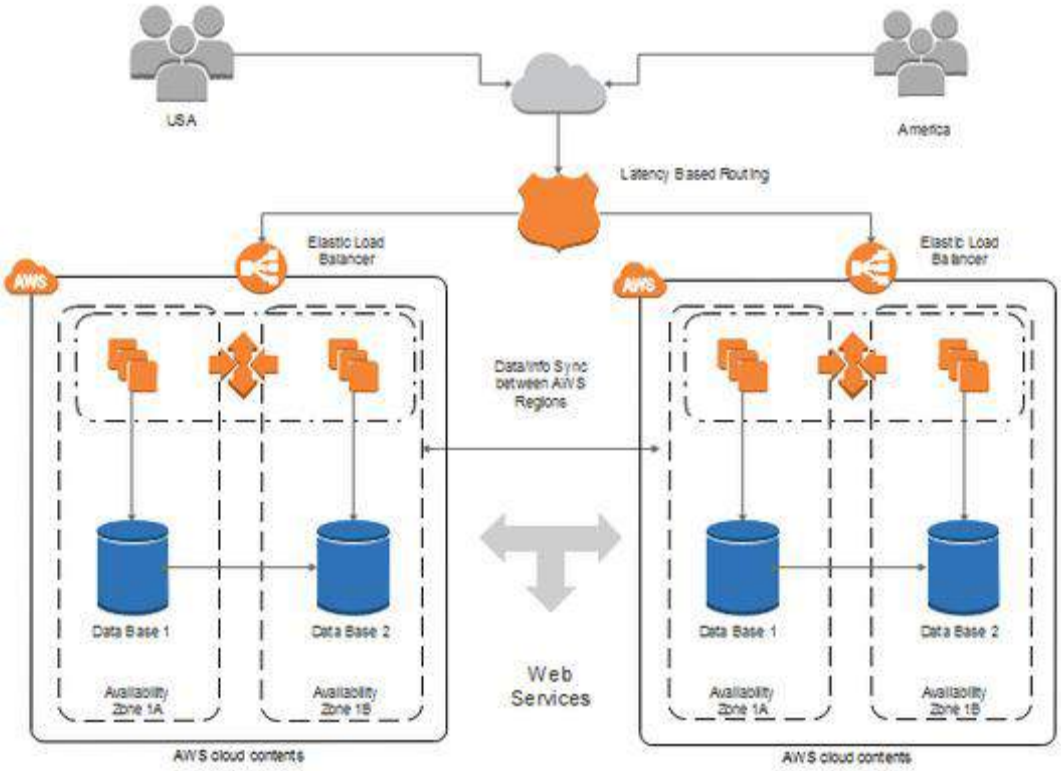
- Amazon EC2 is free to try. There are four ways to pay for Amazon EC2 instances: On-Demand, Reserved Instances, and Spot Instances. You can also pay for Dedicated Hosts which provide you with EC2 instance capacity on physical servers dedicated for your use.
- With **On-Demand instances**, you pay for compute capacity by per hour or per second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.
- Amazon EC2 **Spot instances** are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. EC2 Spot enables you to optimize your costs on the AWS cloud and scale your application's throughput up to 10X for the same budget. By simply selecting Spot when launching EC2 instances, you can save up-to 90% on On-Demand prices.
- **Reserved Instances** provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.
- **A Dedicated Host** is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements.
- Refer the below given URL for more information about EC2 pricing
- https://aws.amazon.com/ec2/pricing/

Architecture Design:

- Before we are provisioning any AWS services, at first, we need to design an Architecture which is based on customer requirements and with application behavior.
- Include necessary services in AWS to make your application to be always in available state. For example, see the below architecture diagram with 0% downtime.



- If you want to manage your application in different regions, same can be possible with Route53 by mapping two regions ELB as a record set.



DevOps Fundamentals:

Chef:

- Chef is a configuration management technology developed by Opscode to manage infrastructure on physical or virtual machines. It is an open source developed using Ruby, which helps in managing complex infrastructure on the fly. This tutorial provides a basic understanding of the infrastructure and fundamental concepts of managing an infrastructure using Chef.
- Chef server is available in AWS and refer the below URL for more information.
- http://docs.aws.amazon.com/quickstart/latest/chef-server/welcome.html?shortFooter=true
- We need to install the starter Kit and the same can be performed by referring below given URL.
- http://docs.aws.amazon.com/opsworks/latest/userguide/opscm-starterkit.html
- Refer the below YouTube Video URL.
- https://www.youtube.com/watch?v=MSeiFsvLGoc
- Download URL for ChefDK of Window Server 2012 R2 can be found below.
- https://packages.chef.io/files/stable/chefdk/2.4.17/windows/2012r2/chefdk-2.4.17-1-x64.msi
- https://drive.google.com/file/d/1_PzGr3tYPIGIv_EsHwmFET8bLuK2VKi_/view?usp=sharing
- Chef Configuration to get SSL and merging StarterKit & ChefDK
- CD c:\
- chef generate repo chef-repo (Creates chef-repo foler)
- $source = 'c:\Chef\myfirstchefserver-c0jzeynbyxwhi4b8\.chef' (Starter-Kit Location)
- Copy-Item -Path $source -Destination.\chef-repo -Recurse (Copying. chef file from Starter-Kit to created folder)
- CD .\chef-repo
- knife ssl fetch https://myfirstchefserver-c0jzeynbyxwhi4b8.us-west-2.opsworks-cm.io (Getting SSL certificates from Chef Server)
- cd .\cookbooks
- Download the sample script from below given url.
- https://drive.google.com/file/d/1gR0_zmZBzGX377EYZ4CdxuJ12sfA_uIV/view?usp=sharing
- Download the Chef Complete User Guide from below given URL.
- https://drive.google.com/file/d/15tKDUCWcw7UGzjTLIFZEVMWrsfOycpKj/view?usp=sharing

Puppet:

- In computing, Puppet is an open-source software configuration management tool.
- It runs on many Unix-like systems as well as on Microsoft Windows and includes its own declarative language to describe system configuration.
- Puppet is designed to manage the configuration of Unix-like and Microsoft Windows systems declaratively.
- The user describes system resources and their state, either using Puppet's declarative language or a Ruby DSL (domain-specific language).
- This information is stored in files called "Puppet manifests". Puppet discovers the system information via a utility called Facter and compiles the Puppet manifests into a system-specific catalog containing resources and resource dependency, which are applied against the target systems. Any actions taken by Puppet are then reported.
- Puppet consists of a custom declarative language to describe system configuration, which can be either applied directly on the system, or compiled into a catalog and distributed to the target system via client–server paradigm (using a REST API), and the agent uses system specific providers to enforce the resource specified in the manifests.
- The resource abstraction layer enables administrators to describe the configuration in high-level terms, such as users, services and packages without the need to specify OS specific commands (such as rpm, yum, apt).
- Puppet server is also available in AWS and please refer the below given URL for provisioning the same.
- https://docs.aws.amazon.com/quickstart/latest/puppet/welcome.html
- Download the Complete Guide of Puppet in below given URL.

- https://drive.google.com/file/d/1LY5aVUzismfzaJvVhBV7O19aYUMsANvE/view?usp=sharing
- Download the sample puppet script from below URL to install software.
- https://drive.google.com/file/d/12-G_BoKSI9K2JU9XSzQoFSWLbIPV9fwc/view?usp=sharing

Ansible:

- Ansible is powerful IT automation that you can learn quickly. It's simple enough for everyone in your IT team to use, yet powerful enough to automate even the most complex deployments.
- Ansible handles repetitive tasks, giving your team more time to focus on innovation.
- With Ansible you can start to do real work in just minutes due to its simple, human-readable language. Altogether its powerful capabilities allow orchestration of your entire application lifecycle regardless of where it's deployed.
- And Ansible's agentless architecture means it is one less thing to keep secure.
- Refer the below given URL to know more information about Ansible.
- https://www.ansible.com/resources/videos/quick-start-video
- http://docs.ansible.com/ansible/latest/index.html
- Download a User Guide from below given URL.
- https://drive.google.com/file/d/1Ni__ZaYPvCXUiOH4Ivzh_3tHX757btOx/view?usp=sharing
- To install Ansible in Admin VM or any Controller VM, please follow the below given commands.
- sudo -s
- yum update -y
- rpm -ivh http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
- yum install ansible -y
- ansible --version
- ssh-keygen
- ssh-copy-id <Username>@<Client-IP>
- cd /etc/ansible
- chmod -R 777 *.*
- chmod -R 777 hosts
- vi hosts
    - [Client-Hostname]
    - <Client-IP> ansible_user=<Username>
- To test Controller VM is reaching the Client VM, use the below command.
- ansible -m ping <Client-IP>
- Ensure Client VM Disk size by using below command.
- ansible -m shell -a 'df -h' [Client-Hostname]
- Ensure Client VM RAM size by using below command.
- ansible -m shell -a 'free -m' [Client-Hostname]
- Copy the data to Client VM from Controller VM by using below command.
- ansible [Client-Hostname] -m copy -a "src=/etc/hosts dest=/tmp/hosts"
- Install any software on Client VM by using below command.
- ansible [Client-Hostname] -m git -a "repo=https://foo.example.org/repo.git dest=/srv/myapp version=HEAD"
- Ensure Client VM Service is started by using below command.
- ansible [Client-Hostname] -m service -a "name=httpd state=started"
- Please find the below command and playbook for installing nginx.
- vi nginx.yml

```
---
- name: Install nginx
  hosts: [Client-Hostname]
  become: true
  tasks:
  - name: Add epel-release repo
   yum:
    name: epel-release
```

```
  state: present
 - name: Install nginx
  yum:
   name: nginx
   state: present
 - name: Insert Index Page
   template:
    src: index.html
    dest: /usr/share/nginx/html/index.html
 - name: Start NGiNX
   service:
   name: nginx
   state: started
```

- To execute this play book, use the below command.
- ansible-playbook nginx.yml -f 10

Ant:

- Apache Ant is a software tool for automating software build processes, which originated from the Apache Tomcat project in early 2000. It was a replacement for the Make build tool of Unix and was created due to several problems with Unix's make.
  It is like Make but is implemented using the Java language, requires the Java platform, and is best suited to building Java projects.
- The most immediately noticeable difference between Ant and Make is that Ant uses XML to describe the code build process and its dependencies, whereas Make uses the Make file format.
- By default, the XML file is named build.xml.
- Below is listed a sample build.xml file for a simple Java "Hello, world" application. It defines four targets - clean, clobber, compile and jar, each of which has an associated description. The jar target lists the compile target as a dependency. This tells Ant that before it can start the jar target it must first complete the compile target.

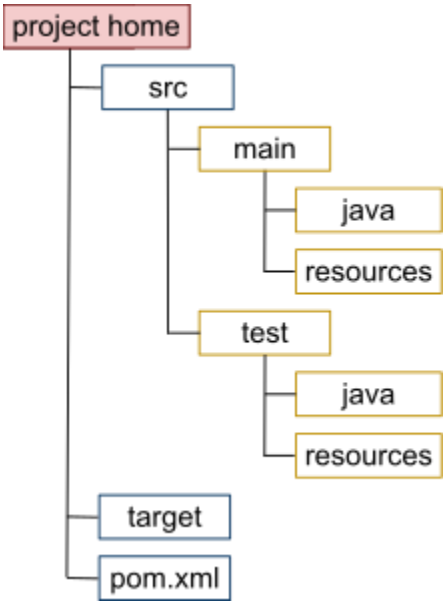
```
<?xml version="1.0"?>
<project name="Hello" default="compile">
<target name="clean" description="remove intermediate files">
<delete dir="classes"/>
</target>
<target name="clobber" depends="clean" description="remove all artifact files">
<delete file="hello.jar"/>
</target>
<target name="compile" description="compile the Java source code to class files">
<mkdir dir="classes"/>
<javac srcdir="." destdir="classes"/>
</target>
<target name="jar" depends="compile" description="create a Jar file for the application">
<jar destfile="hello.jar">
<fileset dir="classes" includes="**/*.class"/>
<manifest>
<attribute name="Main-Class" value="HelloProgram"/>
</manifest>
</jar>
</target>
</project>
```

- Within each target are the actions that Ant must take to build that target; these are performed using built-in tasks. For example, to build the compile target Ant must first create a directory called classes (which Ant will do only if it does not already exist) and then invoke the Java compiler. Therefore, the tasks used are mkdir and javac. These perform a similar task to the command-line utilities of the same name.

- Download the User Guide from below given URL for more information.
- https://drive.google.com/file/d/1AYWn9avcGmkd3TkW9eed6ICvNcNy6qTb/view?usp=sharing

Maven:

- Maven is a build automation tool used primarily for Java projects.
- Maven addresses two aspects of building software: first, it describes how software is built,[clarification needed] and second, it describes its dependencies. Unlike earlier tools like Apache Ant, it uses conventions for the build procedure, and only exceptions need to be written down. An XML file describes the software project being built, its dependencies on other external modules and components, the build order, directories, and required plug-ins. It comes with pre-defined targets for performing certain well-defined tasks such as compilation of code and its packaging.
- Maven dynamically downloads Java libraries and Maven plug-ins from one or more repositories such as the Maven 2 Central Repository and stores them in a local cache. This local cache of downloaded artifacts can also be updated with artifacts created by local projects. Public repositories can also be updated.
- Maven can also be used to build and manage projects written in C#, Ruby, Scala, and other languages. The Maven project is hosted by the Apache Software Foundation, where it was formerly part of the Jakarta Project.
- Maven is built using a plugin-based architecture that allows it to make use of any application controllable through standard input. Theoretically, this would allow anyone to write plugins to interface with build tools (compilers, unit test tools, etc.) for any other language. Support and use for languages other than Java has been minimal. Currently a plugin for the .NET framework exists and is maintained, and a C/C++ native plugin is maintained for Maven 2.
- Alternative technologies like Gradle and sbt as build tools do not rely on XML but keep the key concepts Maven introduced. With Apache Ivy, a dedicated dependency manager was developed as well that also supports Maven repositories.



- Maven projects are configured using a Project Object Model, which is stored in a pom.xml-file. Here's a minimal example:

```
<project>
<!-- model version is always 4.0.0 for Maven 2.x POMs -->
<modelVersion>4.0.0</modelVersion>
<!-- project coordinates, i.e. a group of values which
uniquely identify this project -->
<groupId>com.mycompany.app</groupId>
<artifactId>my-app</artifactId>
<version>1.0</version>
<!-- library dependencies -->
```

```
<dependencies>
<dependency>
<!-- coordinates of the required library -->
<groupId>junit</groupId>
<artifactId>junit</artifactId>
<version>3.8.1</version>
<!-- this dependency is only used for running and compiling tests -->
<scope>test</scope>
</dependency>
</dependencies>
</project>
```

- This POM only defines a unique identifier for the project (coordinates) and its dependency on the JUnit framework. However, that is already enough for building the project and running the unit tests associated with the project. Maven accomplishes this by embracing the idea of Convention over Configuration, that is, Maven provides default values for the project's configuration.
- The directory structure of a normal idiomatic Maven project has the following directory entries:
- The Maven software tool auto-generated this directory structure for a Java project.
- Directory name Purpose
- **project home** - Contains the pom.xml and all subdirectories.
- **src/main/java** - Contains the deliverable Java sourcecode for the project.
- **src/main/resources** - Contains the deliverable resources for the project, such as property files.
- **src/test/java** - Contains the testing Java sourcecode (JUnit or TestNG test cases, for example) for the project.
- **src/test/resources** - Contains resources necessary for testing.

Git:

- The first step is to install the GIT in the machine where the repository is to be cloned.
- **Steps to install Git in Linux machines:**
- **# yum update**
- Next, install Git by typing the following command:
- **# yum install git**
- After git successfully installed, you can issue the following command to display the version of Git installed:
- **# git –version**
- **Command to clone the Gitlab repository:**
- One the git is installed, then clone the repository contain the structure into the local machine using the git clone command.
- **# git clone PASTE HTTPS OR SSH HERE**
- The entire the repo is clone onto your local machine which contains all the files based on the repository structure.
- **Locating an existing ssh key pair:**
- **Git Bash on Windows / GNU/Linux / macOS / PowerShell:**
- **cat ~/.ssh/id_rsa.pub**
- **Generating a new SSH key pair:**
- To generate a new SSH key pair, use the following command:
- **Git Bash on Windows / GNU/Linux / macOS:**
- **ssh-keygen -t rsa -C "your.email@example.com" -b 4096**
- **cat ~/.ssh/id_rsa.pub**
- The final step is to add your public SSH key to GitLab.
- Navigate to the **'SSH Keys'** tab in your **'Profile Settings'**. **Paste** your key in the **'Key'** section and give it a relevant 'Title'.
- If you manually copied your public SSH key make sure you copied the entire key starting with ssh-rsa and ending with your email.

- **Optional**: You can test your setup by running ssh -T git@example.com (replacing example.com with your GitLab domain) and verifying that you receive a Welcome to GitLab message
- **On the command line to clone your project:**
- Go to your computer's shell and type the following command:
- git clone PASTE HTTPS OR SSH HERE
- A clone of the project will be created in your computer.
- **Note**: If you clone your project via an URL that contains special characters, make sure that they are URL-encoded
- Go into a project, directory or file to work in it
- cd NAME-OF-PROJECT-OR-FILE
- Go back one directory or file
- cd ../
- View what’s in the directory that you are in
- ls
- Create a directory
- mkdir NAME-OF-YOUR-DIRECTORY
- Create a file in directory
- touch filename
- nano filename
- #### ADD YOUR INFORMATION
- #### Press: control + X
- #### Type: Y
- #### Press: enter
- Remove a file
- rm NAME-OF-FILE
- Remove a directory and all of its contents
- rm -rf NAME-OF-DIRECTORY
- View history in the command line
- history
- Carry out commands for which the account you are using lacks authority
- Tell where you are
- pwd
- **Go to the master branch to pull the latest changes from there**
- git checkout master
- **Download the latest changes in the project**
- This is for you to work on an up-to-date copy (it is important to do every time you work on a project), while you setup tracking branches.
- git pull REMOTE NAME-OF-BRANCH -u
- (REMOTE: origin) (NAME-OF-BRANCH: could be "master" or an existing branch)
- **Create a branch:**
- Spaces won't be recognized, so you will need to use a hyphen or underscore.
- git checkout -b NAME-OF-BRANCH
- **Work on a branch that has already been created**
- git checkout NAME-OF-BRANCH
- **View the changes:**
- Getting status of your changes is.
- git status
- **Add changes to commit**
- **Note**: You'll see your changes in red when you type "git status".
- git add CHANGES IN RED
- git commit -m "DESCRIBE THE INTENTION OF THE COMMIT"

- **Send changes to gitlab.com**
- git push REMOTE NAME-OF-BRANCH
- **Delete all changes in the Git repository, but leave un-staged things**
- git checkout .
- **Delete all changes in the Git repository, including untracked files**
- git clean -f
- **Merge created branch with master branch**
- **Note**: You need to be in the created branch.
- git checkout NAME-OF-BRANCH
- git merge master
- **Merge master branch with created branch**
- **Note**: You need to be in the master branch.
- git checkout master
- git merge NAME-OF-BRANCH
- **Fork a project:**
- A fork is a copy of an original repository that you can put in another namespace where you can experiment and apply changes that you can later decide if publishing or not, without affecting your original project.
- It takes just a few steps to fork a project in GitLab.
- Go to a project's dashboard under the Project tab and click on the Fork button.
- Click on Fork button
- You will be asked where to fork the repository. Click on the user or group to where you would like to add the forked project.
- Choose namespace
- After a few moments, depending on the repository's size, the forking will complete.
- **Create a merge request:**
- Merge requests are useful to integrate separate changes that you have made to a project, on different branches. This is a brief guide on how to create a merge request. For more information, check the merge requests documentation.
- Before you start, you should have already created a branch and pushed your changes to GitLab.
- Go to the project where you would like to merge your changes and click on the Merge requests tab.
- Click on New merge request on the right side of the screen.
- From there on, you have the option to select the source branch and the target branch you would like to compare to. The default target project is the upstream repository, but you can choose to compare across any of its forks.
- Select a branch
- When ready, click on the Compare branches and continue button.
- At a minimum, add a title and a description to your merge request. Optionally, select a user to review your merge request and to accept or close it. You may also select a milestone and labels.
- New merge request page
- When ready, click on the Submit merge request button. Your merge request will be ready to be approved and merged.

Download the Dump Questions from below given URL.

- ***https://drive.google.com/file/d/16uDe-SbacF9G6ioZ6FzSqsnifn-qPgdG/view?usp=sharing***

User Guide By,

Saravanan Aravindan

+91-9962480596