Bansilal Ramnath Agarwal Charitable Trust's

Vishwakarma Institute of Technology, Pune-37

(An autonomous Institute of Savitribai Phule Pune University)

Department of Artificial Intelligence and Data Science

Manual

Course Code	Course Name	Teaching Scheme (Hrs. /Week)	Credits
	Cloud Computing	2 Theory, 2 Lab,1 Tut	2

Course Outcomes:

The student will be able to –

1. Illustrate the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud.
2. Investigate the resource virtualization technique for a given business case.
3. Choose the appropriate file system and database for a given business case.
4. Develop an application for a given business case using various cloud platforms.
5. Understand service management of cloud services.
6. Identify the challenges in Cloud Management and Cloud Security.

Class: -TY	Branch :-Artificial Intelligence and Data Science
Year:-2023-24	Prepared By :-Prof. S. B. Adsul

Required H/W and S/W: Cloud Platforms (Own Cloud, AWS, Windows Azure, Google App Engine

INDEX

EXPERIMENT NO.: 01

Title: Installation and configuration of own Cloud

Solution:

Own Cloud is a suite of client–server software for creating and using file hosting services. Own Cloud functionally has similarities to the widely used Dropbox. The primary functional difference between own Cloud and Dropbox is that own Cloud is primarily server software. (The company's own Cloud. Online is a hosted service.) The Server Edition of own Cloud is free and open-source, thereby allowing anyone to install and operate it without charge on their own private server.

ownCloud supports extensions that allow it to work like Google Drive, with online office suite document editing, calendar and contact synchronization, and more. Its openness avoids enforced quotas on storage space or the number of connected clients, instead of having hard limits (for example on storage space or number of users) limits are determined by the physical capabilities of the server.

ownCloud Features

Main features of ownCloud are:

- Open API, open source
- Clients for PC, Mac, Linux
- Native Apps for iOS, Android
- Password protected public links
- Notifications
- Collaboration
- Online document editing
- Comments, tagging
- Calendars and contacts
- External storage handling
- Activity feed & notifications
- Versioning and undelete
- Galleries
- Music and video playback
- Password storage
- Anti-virus scanning
- Integrated logging
- Quota management
- ownBrander

own Cloud Benefit:

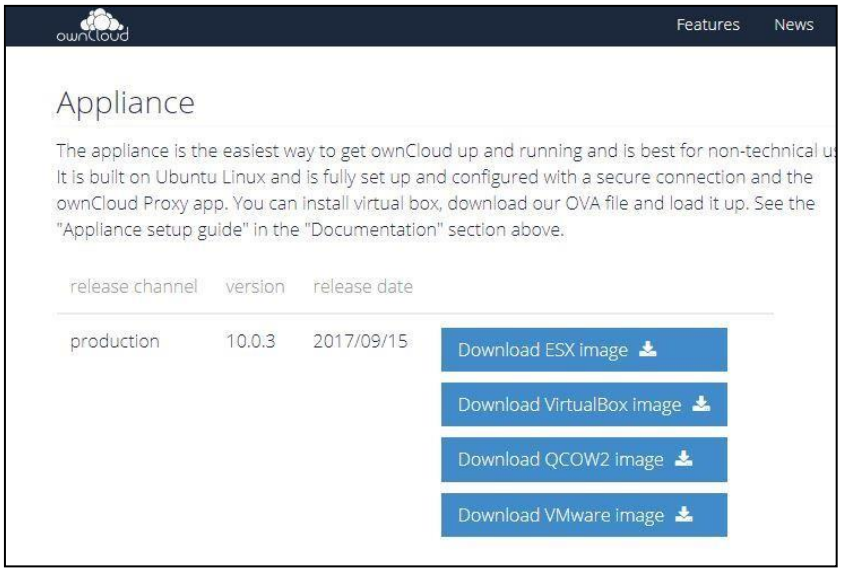
The main benefits of ownCloud are seamless file sharing and syncing, secure data viewing, and multiple device file access. Clients can effortlessly get to their information anytime and anywhere by utilizing the local Android and iOS applications, which can transfer pictures after they are taken automatically.

How To Install OwnCloud server on VirtualBox Virtual Machine

For the ownCloud Installation follows following Step:

Step 1:

Go to Owncloud.org websites download page.



Step 2:

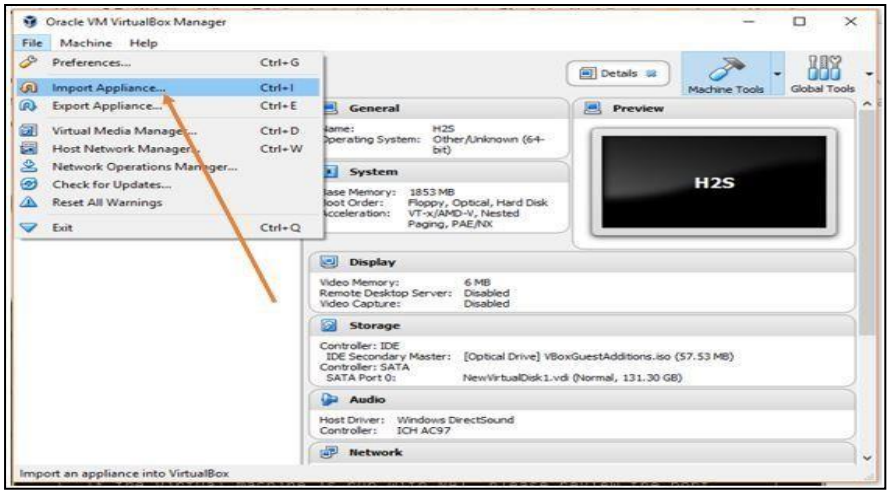
Download the OwnCloud Virtual appliance image according to your Virtual Machine software. Like here, in this tutorial we are using the Virtualbox, so we download the Virtualbox image.

Step 3:

After downloading the image(iso file), go to file menu on VirtualBox.

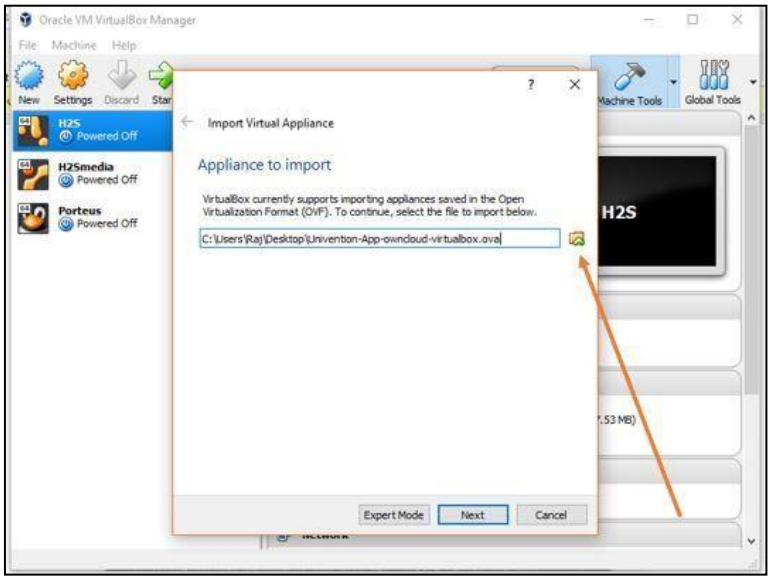
Step 4:

Click on the Import Appliance option.



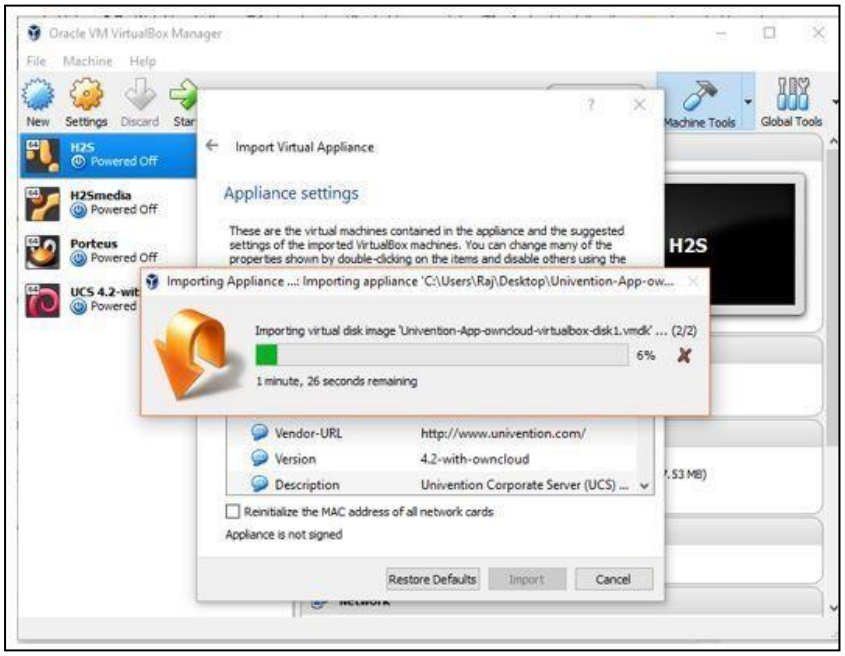
Step 5:

Now click on the file browser button and select the downloaded Virtualbox OVA image. Click on the Next button.



Step 6:

After importing, if you want to change any appliance settings such network and storage. Then click on the Import button.

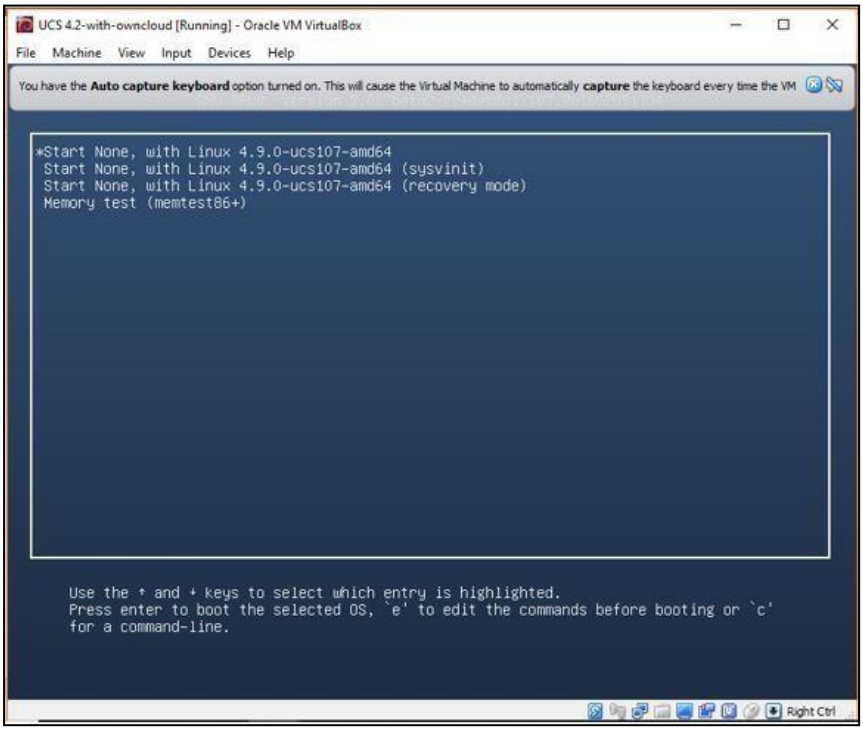


Step 7:

Once the importing is complete, the Owncloud virtual will be shown on the left side panel in the powered off mode. To start it just double click on it.

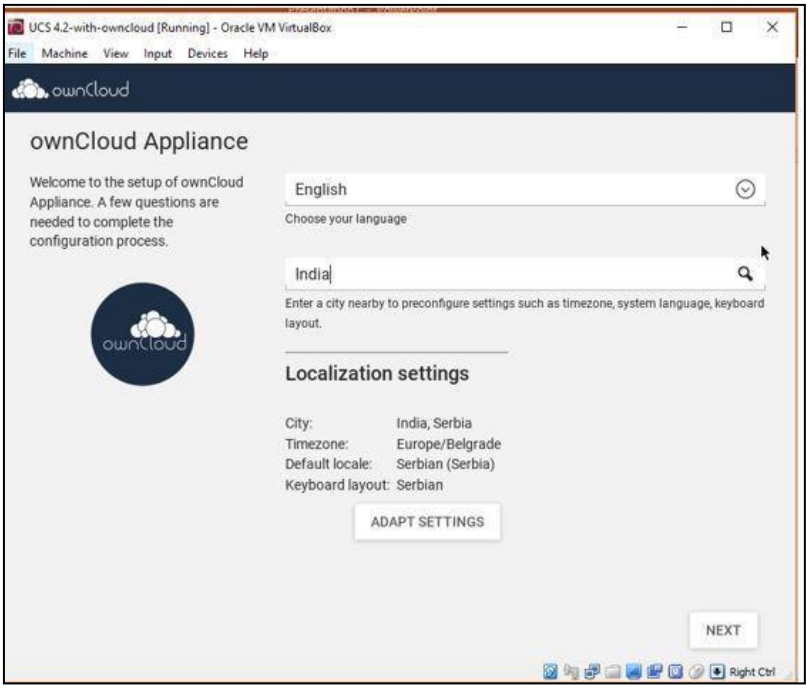
Step 8:

After starting the Owncloud Virtual machine you get three options, leave the default option and just hit the enter button.



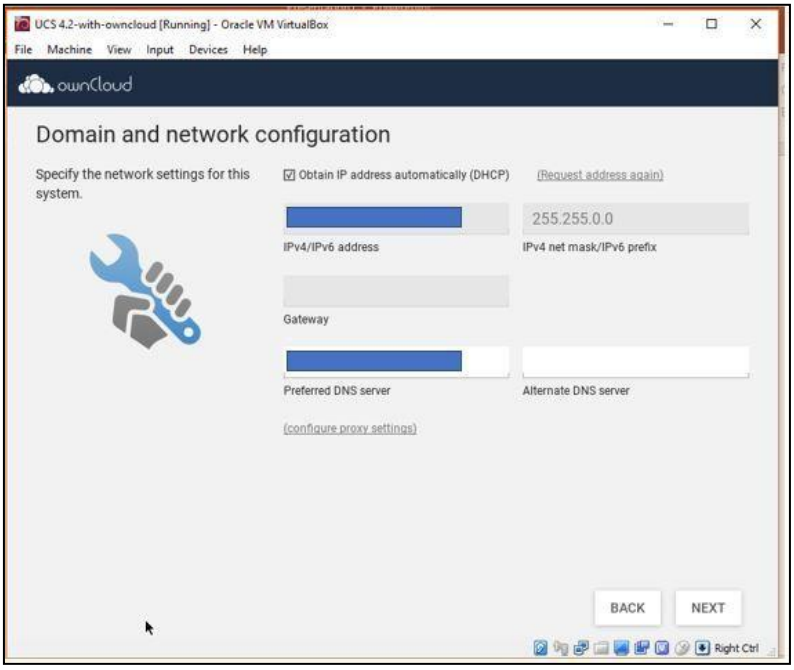
Step 9:

Finally, you will see the OwnCloud configuration screen. Choose your language and country after that click on the ADAPT settings to set the keyboard preference and other location settings.



Step 10:

In this step configure the IP address to access the Owncloud locally. If you have router or DHCP, the machine will automatically assign the IP address. In case it not or you do not have the DHCP setup then uncheck the box given in the front of "Obtain the IP address automatically (DHCP)" and add the IP address manually.

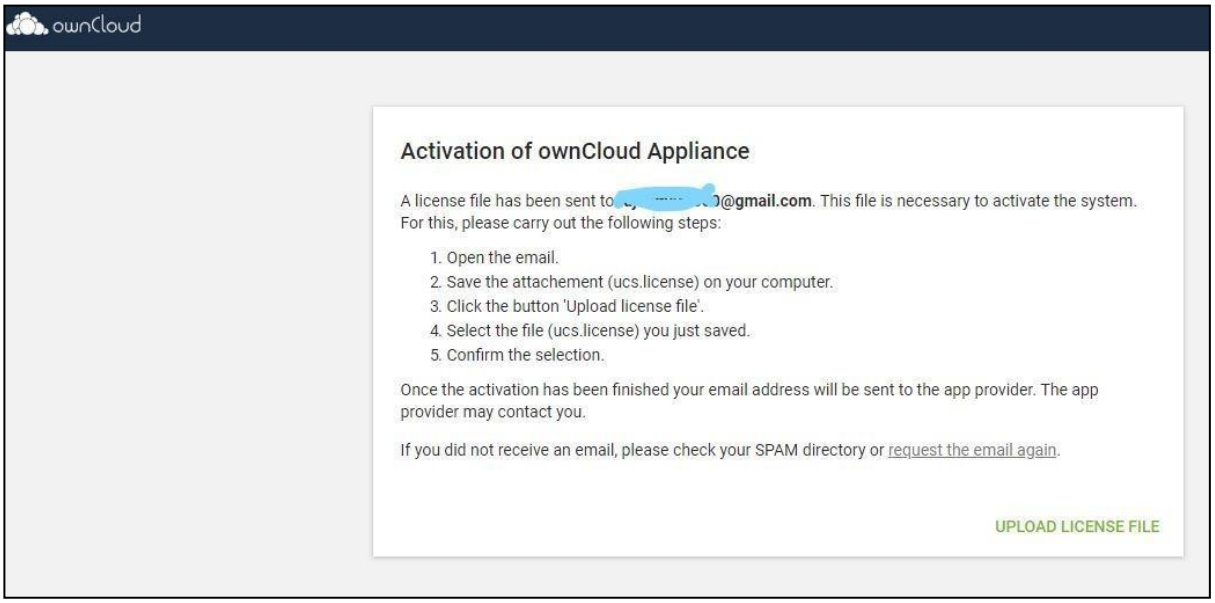


Step 11:

After setting up the Owncloud virtual machine, it will restart automatically and show you the IP address which you can use to access the OwnCloud locally on any system using the browser.

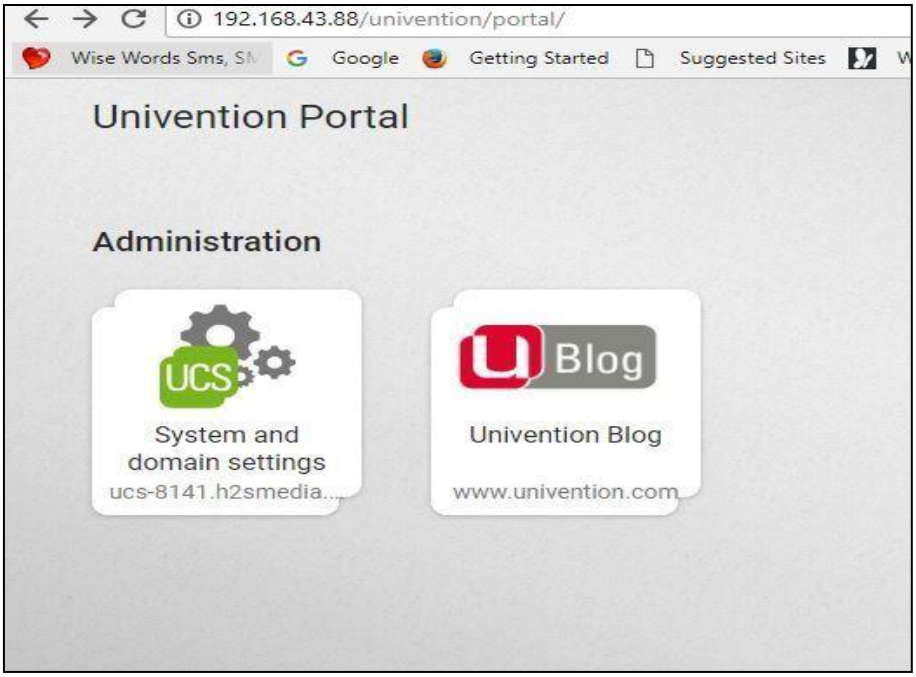
Step 12:

So, go to your browser and type that given IP address. The OwnCloud will open and ask you for the email address to send you the license to activate the Univention software that powered the Owncloud virtual machine. Once you get the license file just upload it and this software will get activated.



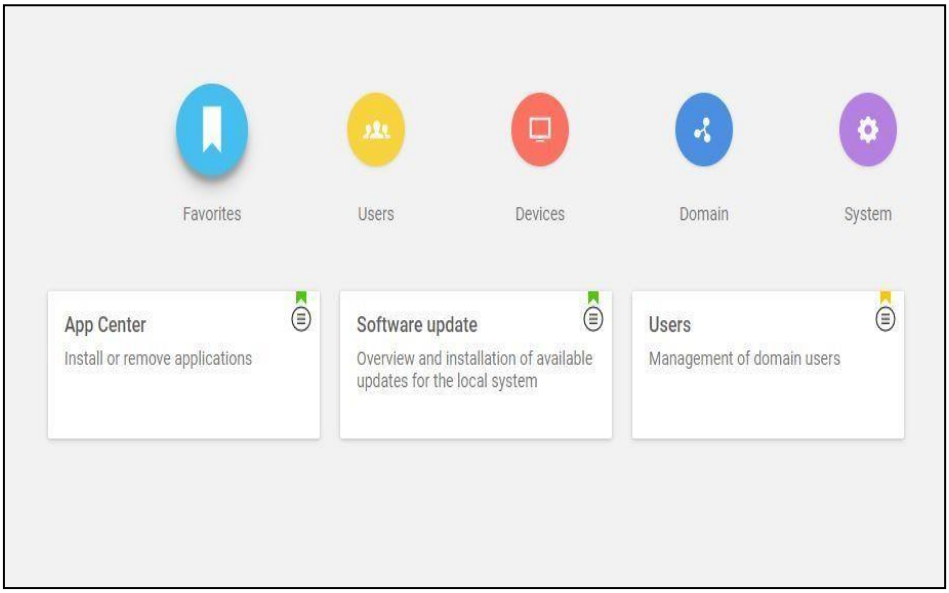
Step 13:

After uploading, you will get a portal screen from where you need to select the administrative account that you have created while installing the OwnCloud. The username willbe **Administrator** but the password you have to enter is that you have been created for root account while installing the OwnCloud.

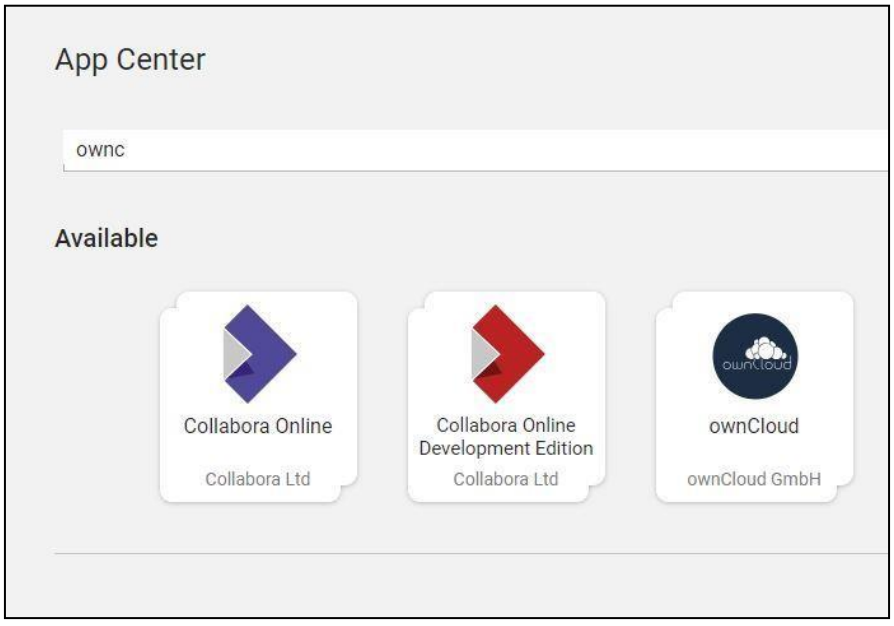


Step 14:

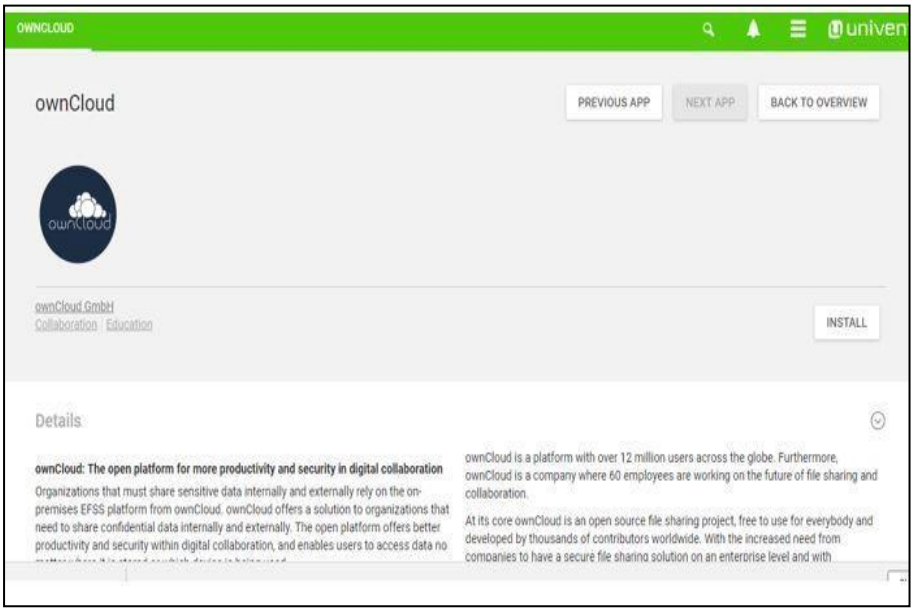
Once you get login then select the option APP Center.



Step 15:
Now search for the OwnCloud and click on it, when appears.



Step 16:
After Clicking the OwnCloud app, it will open. Now, click on the **INSTALL** button to install the OwnCloud successfully.



OR

Another Ways install and configure the ownCloud.

Step 1:

The ownCloud server package does not exist within the default repositories for Ubuntu. However, ownCloud maintains a dedicated repository for the distribution that we can add to our server.

To begin, download their release key using the curl command and import it with the apt-key utility with the add command:

curl https://download.owncloud.org/download/repositories/10.0/Ubuntu_18.04/Release.key | sudo apt-key add -

Step 2:

The 'Release.key' file contains a PGP (Pretty Good Privacy) public key which apt will use to verify that the ownCloud package is authentic.

In addition to importing the key, create a file called owncloud.list in the sources.list.d directory for apt. The file will contain the address to the ownCloud repository.

echo 'deb http://download.owncloud.org/download/repositories/10.0/Ubuntu_18.04/ /' | sudo tee /etc/apt/sources.list.d/owncloud.list

Step 3:
Now, we can use the package manager to find and install ownCloud. Along with the main package, we will also install a few additional PHP libraries that ownCloud uses to add extra functionality. Update your local package index and install everything by typing:

sudo apt update
sudo apt install php-bz2 php-curl php-gd php-imagick php-intl php-mbstring php-xml php-zip owncloud-files

Step 4:
Adjusting the Document Root

The ownCloud package we installed copies the web files to /var/www/owncloud on the server. Currently, the Apache virtual host configuration is set up to serve files out of a different directory. We need to change the DocumentRoot setting in our configuration to pointto the new directory.

You find which virtual host files reference your domain name or IP address using the apache2ctl utility with the DUMP_VHOSTS option. Filter the output by your server's domain name or IP address to find which files you need to edit in the next few commands:

sudo apache2ctl -t -D DUMP_VHOSTS | grep server_domain_or_IP

The output will probably look something like this:

```
Output
*:443                  server_domain_or_IP (/etc/apache2/sites-enabled/server_domain_or_IP-le-ssl.conf:2)
        port 80 namevhost server_domain_or_IP (/etc/apache2/sites-enabled/server_domain_or_IP
```

Step 5:
In the parentheses, you can see each of the files that reference the domain name or IP address we'll use to access ownCloud. These are the files you'll need to edit.

For each match, open the file in a text editor with sudo privileges:

$sudo nano /etc/apache2/sites-enabled/server_domain_or_IP.conf

Inside, search for the DocumentRoot directive. Change the line so that it points to the /var/www/owncloud directory:

```
<VirtualHost *:80>
   . . .
   DocumentRoot /var/www/owncloud
   . . .
</VirtualHost>
```

Step 6:

Save and close the file when you are finished. Complete this process for each of the files that referenced your domain name (or IP address if you did not configure a domain for your server).

When you are finished, check the syntax of your Apache files to make sure there were no detectable typos in your configuration:

$sudo apache2ctl configtest

```
Output
Syntax OK
```

Depending on your configuration, you may see a warning about setting ServerName globally. As long as the output ends with Syntax OK, you can ignore that warning. If you see additional errors, go back and check the files you just edited for mistakes.

If your syntax check passed, reload the Apache service to activate the new changes:

sudo systemctl reload apache2

Step 7:

Configuring the MySQL Database

Before we move on to the web configuration, we need to set up the database. During the web-based configuration process, we will need to provide an database name, a database username, and a database password so that ownCloud can connect and manage its information within

MySQL.

Begin by logging into your database with the MySQL administrative account:

sudo mysql

Step 8:
If you set up password authentication for MySQL root account, you may have to use this syntax instead:

mysql -u root -p

Step 9:

Create a dedicated database for ownCloud to use. We will name the database owncloud for clarity:

Mysql> CREATE DATABASE owncloud;

Step 10:

create a separate MySQL user account to manage the newly created database. Creating one-function databases and accounts is a good idea from a management and security standpoint. As with the naming of the database, choose a username that you prefer. We elected to go with the name owncloud in this guide.

GRANT ALL ON owncloud.* to 'owncloud'@'localhost' IDENTIFIED BY 'owncloud_database_password';

Step 11:
With the user assigned access to the database, perform the flush privileges operation to ensure that the running instance of MySQL knows about the recent privilege assignment:

Mysql> FLUSH PRIVILEGES;

You can now exit the MySQL session by typing:

Mysql> exit

With the ownCloud server installed and the database set up, we are ready to turn our attention

to configuring the ownCloud application.

Step 12:

Configuring ownCloud

To access the ownCloud web interface, open a web browser and navigate to the following address:

https://server_domain_or_IP

Step 13:

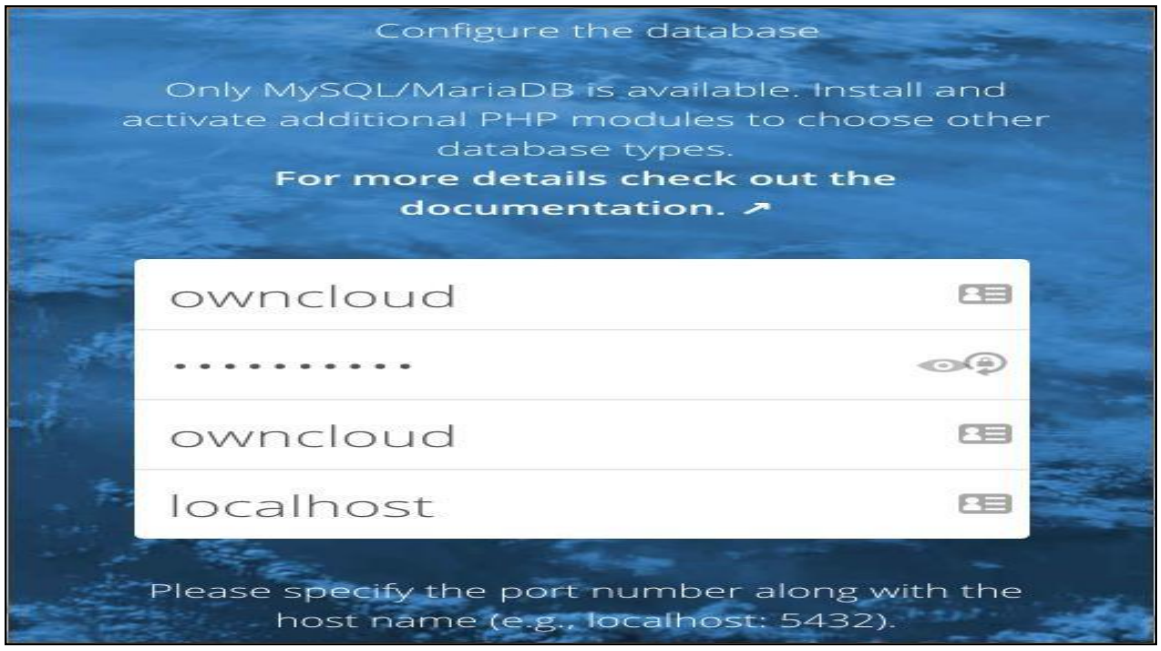
Create an admin account by choosing a username and a password. For security purposes it is not recommended to use something like “admin” for the username:

Step 14:

Next, leave the **Data folder** setting as-is and scroll down to the database configuration section.

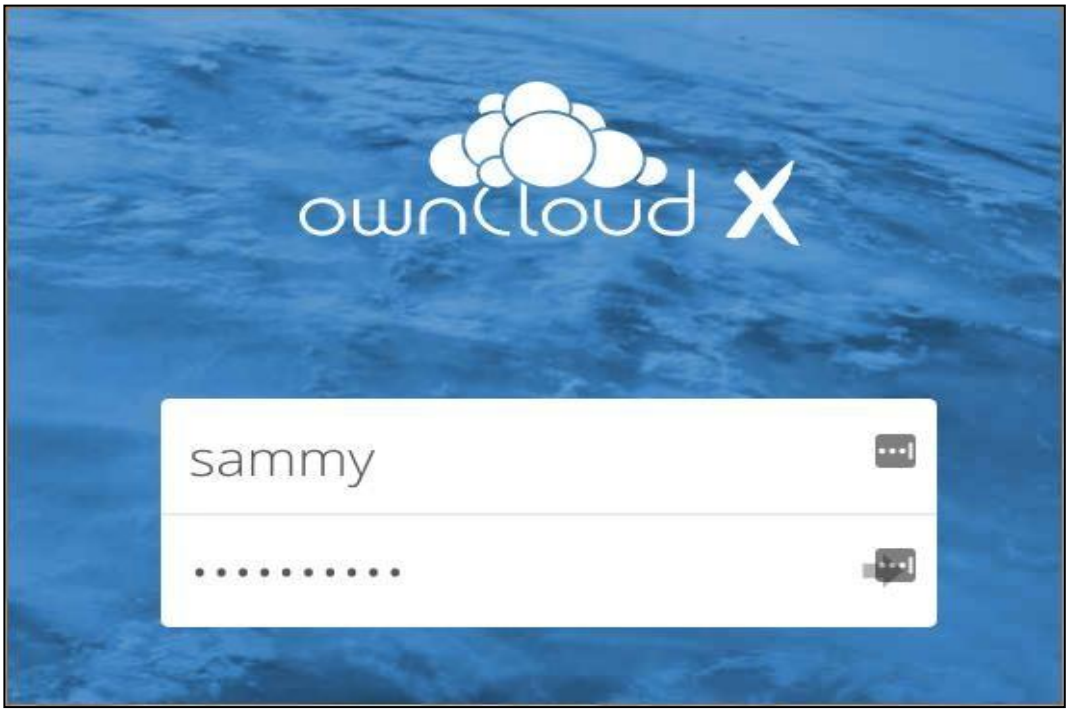
Fill out the details of the database name, database username, and database password you

created in the previous section. If you used the settings from this guide, both the database name and username will be owncloud. Leave the database host as localhost:



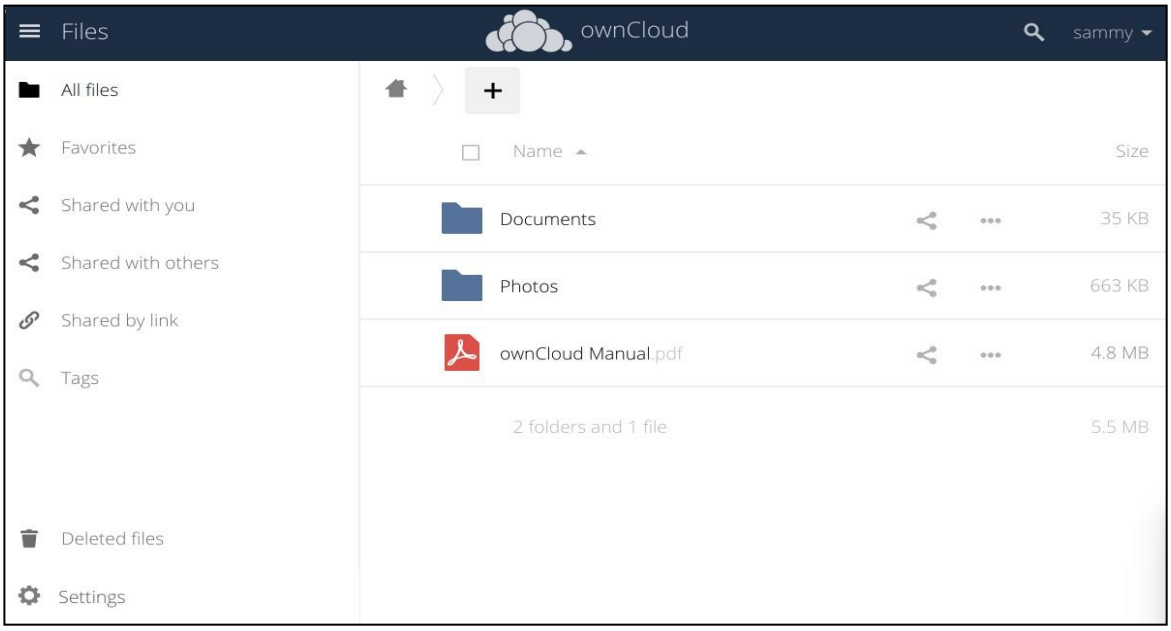
Step 15:

Click the **Finish setup** button to finish configuring ownCloud using the information you've provided. You will be taken to a login screen where you can sign in using your new account:



Step 16:

On your first login, a screen will appear where you can download applications to sync your files on various devices. You can download and configure these now or do it at a later time. When you are finished, click the **x** in the top-right corner of the splash screen to access the main interface:



Companies use OwnCloud:

We have data on 981 companies that use ownCloud. The companies using ownCloud are most often found in United States and in the Computer Software industry. ownCloud is most often used by companies with 10-50 employees and 1M-10M dollars in revenue. Our data for ownCloud usage goes back as far as 4 years and 4 months.

Conclusion:

ownCloud can replicate the capabilities of popular third-party cloud storage services. Content can be shared between users or externally with public URLs. The advantage of ownCloud is that the information is stored in a place that you control and manage without a third party.

EXPERIMENT NO.:02

Title: Study and implementation of infrastructure as Service using OpenStack

Solution:

Infrastructure as-a-service (IaaS)

IaaS includes the delivery of computing infrastructure such as a virtual machine, disk image library, raw block storage, object storage, firewalls, load balancers, IP addresses, virtual local area networks and other features on-demand from a large pool of resources installed in data centres. Cloud providers bill for the IaaS services on a utility computing basis; the cost is based on the amount of resources allocated and consumed.

OpenStack: a free and open-source cloud computing platform

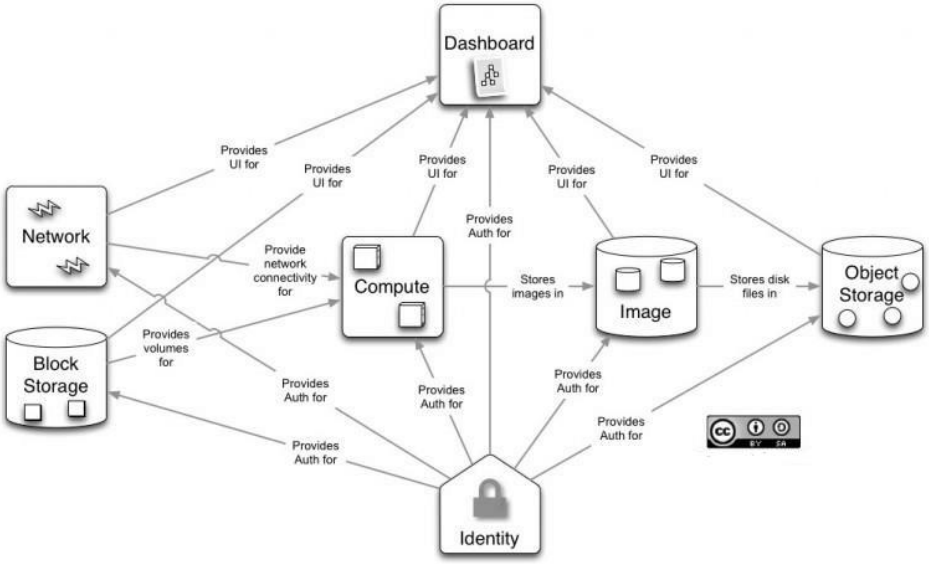
OpenStack is a free and open source, cloud computing software platform that is widely used in the deployment of infrastructure-as-a-Service (IaaS) solutions. The core technology with OpenStack comprises a set of interrelated projects that control the overall layers of processing, storage and networking resources through a data centre that is managed by the users using a Web-based dashboard, command-line tools, or by using the RESTful API. Currently, OpenStack is maintained by the OpenStack Foundation, which is a non-profit corporate organisation established in September 2012 to promote OpenStack software as well as its community.

Companies are Works with Open Stack Community:

Many corporate giants have joined the project, including GoDaddy, Hewlett Packard, IBM, Intel, Mellanox, Mirantis, NEC, NetApp, Nexenta, Oracle, Red Hat, SUSE Linux, VMware, Arista Networks, AT&T, AMD, Avaya, Canonical, Cisco, Dell, EMC, Ericsson, Yahoo!, etc.

OpenStack computing components:

OpenStack has a modular architecture that controls large pools of compute, storage and networking resources.



1. Compute (Nova):
OpenStack Compute (Nova) is the fabric controller, a major component of Infrastructure as a Service (IaaS), and has been developed to manage and automate pools of computer resources. It works in association with a range of virtualization technologies. It is written in Python and uses many external libraries such as Event let, Kombu and SQLAlchemy.

2. Object storage (Swift): It is a scalable redundant storage system, using which objects and files are placed on multiple disks throughout servers in the data center, with the OpenStack software responsible for ensuring data replication and integrity across the cluster. OpenStack Swift replicates the content from other active nodes to new locations in the cluster in case of server or disk failure.

3. Block storage (Cinder): OpenStack block storage (Cinder) is used to incorporate continual block-level storage devices for usage with OpenStack compute instances. The block storage system of OpenStack is used to manage the creation, mounting and unmounting of the block devices to servers. Block storage is integrated for performance-aware scenarios including database storage, expandable file systems or providing a server with access to raw block level storage.

4. Networking (Neutron): Formerly known as Quantum, Neutron is a specialized component of OpenStack for managing networks as well as network IP addresses. OpenStack networking makes sure that the network does not face bottlenecks or any complexity issues in cloud deployment. It provides the users continuous self-service capabilities in the networks infrastructure.

4. Dashboard (Horizon): The OpenStack dashboard (Horizon) provides the GUI (Graphical User Interface) for the access, provision and automation of cloud-based resources. It embeds

various third-party products and services including advance monitoring, billing and various management tools.

5. Identity services (Keystone): Keystone provides a central directory of the users, which is mapped to the OpenStack services they are allowed to access. It refers and acts as the centralized authentication system across the cloud operating system and can be integrated with directory services like LDAP. Keystone supports various authentication types including classical username and password credentials, token-based systems and other log-inmanagement systems.

6. Image services (Glance): OpenStack Image Service (Glance) integrates the registration, discovery and delivery services for disk and server images. These stored images can be used as templates. It can also be used to store and catalogue an unlimited number of backups. Glance can store disk and server images in different types and varieties of back-ends, including Object Storage.

7. Telemetry (Ceilometer): OpenStack telemetry services (Ceilometer) include a single point of contact for the billing systems. These provide all the counters needed to integrate customer billing across all current and future OpenStack components.

8. Orchestration (Heat): Heat organizes a number of cloud applications using templates with the help of the OpenStack-native REST API and a CloudFormation-compatible Query API.

9. Database (Trove): Trove is used as database-as-a-service (DaaS), which integrates and provisions relational and non-relational database engines.

10. Elastic Map Reduce (Sahara): Sahara is the specialized service that enables data processing on OpenStack-managed resources, including the processing with Apache Hadoop.

Benefits of OpenStack:

1. **Enables rapid innovation**

OpenStack's orchestration and self-service capabilities offers developers and IT staff with faster and better access to IT resources. Because developers can provision machines rapidly and on-demand, they can significantly reduce development and testing periods and have more freedom to experiment with new ideas.

2. **Cuts down time-to-market**

Faster deployment of IT resources also means end users and business units no longer have to wait days or weeks to start using the network services and applications they need. In turn, they would be more capable of rolling out and completing projects earlier than before.

3. **Boosts scalability and resource utilization**

Although not as scalable as public clouds, OpenStack private clouds still offer a significant degree of scalability. You can still spin up and spin down servers on-demand. So, for example, if one department encounters a surge in demand for computing resources, IT resources may be temporarily redirected from other departments to the one that currently needs it the most.

4. Eases regulatory compliance

Because OpenStack enables the construction of private, on-premise clouds, it can help in regulatory compliance endeavors. If your cloud is in your own data center, you'll have more control of access privileges, security measures, and security policies. You can personally take charge of ensuring that policies for securing personal data, financial data, and other confidential and regulated information are actually enforced and not just printed on a piece of paper.

5. Devoid of vendor lock-in

One major problem with using a proprietary solution is vendor lock-in. If you're not happy with the vendor's services or the vendor closes shop, you cannot easily hop on to the next. OpenStack supports a variety of proprietary technologies and can operate in a smorgasbord of hypervisor and bare metal environments. Its ability to work with commodity hardware gives you more flexibility in choosing solutions based on a wider range of costs and competencies.

Hardware Requirement for installation of OpenStack are Follows:

- Processor - at least two cores
- Memory - at least 8GB
- Hard Drive - at least 60GB
- NIC - at least 2 NICs

DevStack can be installed on the following kind of operating systems:

- Ubuntu 16.04/17.04/18.04
- Fedora 24/25
- Debian
- CentOS/RHEL 7
- OpenSUSE

Ubuntu operating system is the most tested and most reliable option for DevStack.

Step installation Of IaaS OpenStack are Follows:

Step 1:

Installation of OpenStack

In order to install the DevStack in a system, first, you have to create a Linux VM on your computer (such as using VirtualBox or VMware).The VM must have at least 6GB of memory, and the proper internet connection is also important. Here, we are going to use one version of the ubuntu, i.e., 18.04.

Step 2:

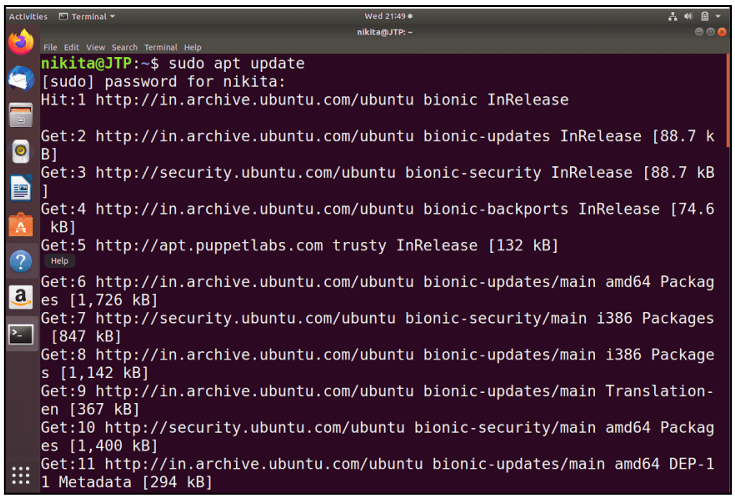
Update Ubuntu System

Open the terminal and run the following command to ensure that the system is up to date:

$ sudo apt update

$ sudo apt -y upgrade

$ sudo apt -y dist-upgrade



Step 3:

Reboot the system after running the above command. To reboot the system, run the following command :

$ sudo reboot OR $ init 6

Step 4:

Create Stack User

It is important that the devstack must run as a regular user (non-root user) with the sudo enabled.

To keep this note in mind, let's create a new user with the name "stack" and assign the sudo permissions or privileges. To create a stack user, run the following command in your terminal:

$ sudo useradd -s /bin/bash -d /opt/stack -m stack

```
nikita@JTP:~$ sudo useradd -s /bin/bash -d /opt/stack -m stack
nikita@JTP:~$
```

Now, to assign the sudo privileges to the stack user, run the following command:

$ echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack

```
nikita@JTP:~$ echo "stack ALL=(ALL) NOPASSWD:ALL" | sudo tee /etc/sudoers.d/stack
stack ALL=(ALL) NOPASSWD:ALL
nikita@JTP:~$
```

Step 5:

Switch to the 'stack' user by running the following command:

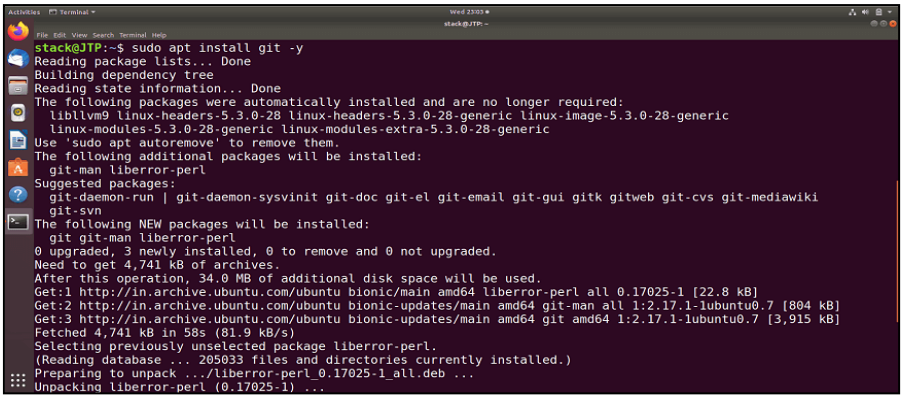
$ sudo su - stack

```
nikita@JTP:~$ sudo su - stack
stack@JTP:~$
```

Step 6:
Install the Git

In ubuntu systems, git comes by default. But if git is missing on your system, then install it by running the following command:

$ sudo apt install git -y

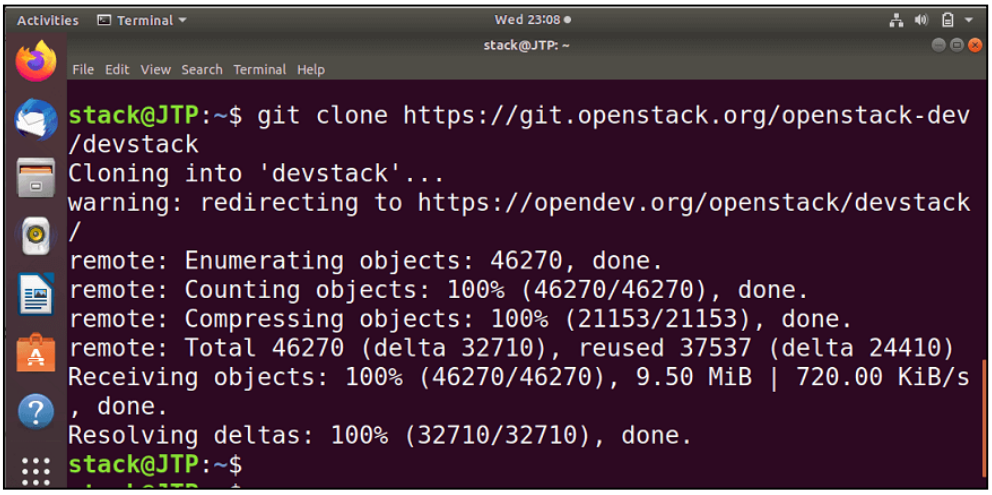


Step 7:

Download the Open Stack

Once you install the git, use the git command to download the DevStack from Github.

$ git clone https://git.openstack.org/openstack-dev/devstack

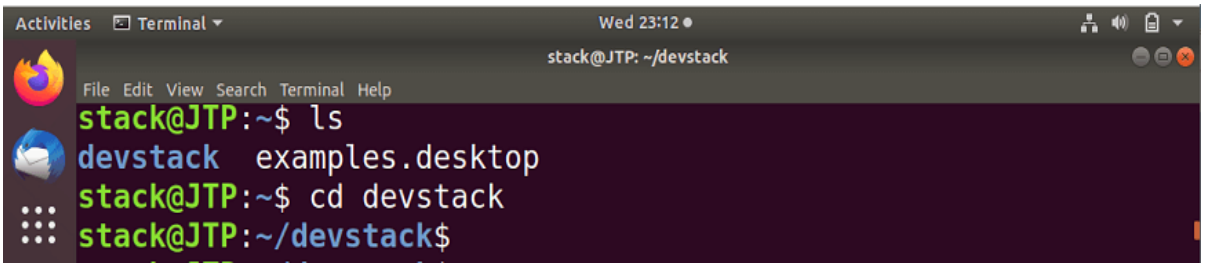


Step 8:

Create the DevStack configuration file

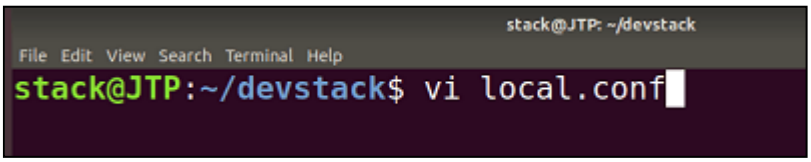
First of all, go to the devstack directory by running the following command :

$ cd devstack



Now, create a local.conf file in which you have to enter the four passwords and the host IP address:

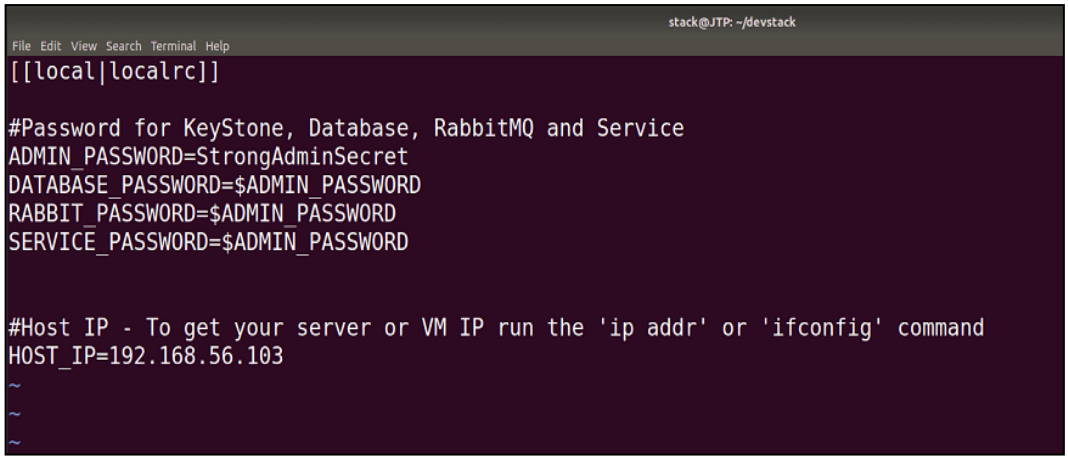
$ ifconfig (check IP address)



Copy the following line of content in the file:

[[local|localrc]]
 # Password for KeyStone, Database, RabbitMQ and Service
ADMIN_PASSWORD=StrongAdminSecret
DATABASE_PASSWORD=$ADMIN_PASSWORD
RABBIT_PASSWORD=$ADMIN_PASSWORD
SERVICE_PASSWORD=$ADMIN_PASSWORD

 # Host IP -
To get your Server or VM IP, run the 'ip addr' or 'ifconfig' command
HOST_IP=192.168.56.103



Step 9:

Press the **ESC**, then wq to save and then exit from the local.conf file.

Here, ADMIN_PASSWORD is the password that we will use to log into the OpenStack login page. The default username for an OpenStack is 'admin'. And HOST_IP is the IP address of your system. To get your Server or VM IP, run the 'ifconfig' or 'ip addr' command.

Step 10:
Install OpenStack using DevStack

To install and run the openstack, execute the following command:

$ ./stack.sh

DevStack will install the following components:

- Compute Service (Nova)
- Image Service- Glance
- Identity Service-Keystone,
- Block Storage Service - Cinder
- OpenStack Dashboard - Horizon

- Network Service - Neutron
- Placement API - Placement
- Object Storage - Swift

The installation will take about 10-20 minutes, mostly depends on your internet speed.

At the very end of the installation, you will get the host's IP address, URL for managing it and the username and password to handle the administrative task.

Step 11:

Copy the horizon URL given in the installation output and paste it into your browser :

http://<IP Address>/dashboard

Step 12:

To login to OpenStack with the default username - admin or demo and configured password - secret.

Once you login into the OpenStack, you will be redirected to the Dashboard of OpenStack. This dashboard screen is called the OpenStack management web console.

Step 13:

On the main dashboard screen, you will see the instance's overview.

You can also create your own instance in the OpenStack. Instances are nothing but a virtual machine. To create a new virtual machine, click on the **instances** from the left side of the page.

And then click on Launch Instances. Fill in all the required fields. Once you fill all the required fields, an instance will create.

Conclusion

OpenStack is one of the best environments in organizations for cloud computing. OpenStack's ease of linear scalability and open-source architecture have attracted many clients and enthusiasts of technology to come forward and contribute to development. This has only made OpenStack stronger over the years. OpenStack can be called for cloud computing, with all the benefits and endless modular functionality, as it proves to be an affordable option for the longer term.

EXPERIMENT NO.:03

Title: Installing two Virtual Machines on VirtualBox and let them communicate with each other

Solution:

1. **Virtualization:**

Virtualization is technology that lets you create useful IT services using resources that are traditionally bound to hardware. It allows you to use a physical machine's full capacity by distributing its capabilities among many users or environments.

Type of Virtualizations:

- Data Virtualization
- Desktop Virtualization
- Server Virtualization
- Operating System Virtualization
- Networks Functions Virtualization

2. **Virtual Machine:**

A virtual machine (VM) is a virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises). Software called a hypervisor separates the machine's resources from the hardware and provisions them appropriately so they can be used by the VM.

How do virtual machines work?

The virtual machine runs as a process in an application window, similar to any other application, on the operating system of the physical machine. Key files that make up a virtual machine include a log file, NVRAM setting file, virtual disk file and configuration file.

Advantages of virtual machines

Virtual machines are easy to manage and maintain, and they offer several advantages over physical machines:

- VMs can run multiple operating system environments on a single physical computer, saving physical space, time and management costs.
- Virtual machines support legacy applications, reducing the cost of migrating to a new operating system. For example, a Linux virtual machine running a distribution of Linux as the guest operating system can exist on a host server that is running a non-Linux operating system, such as Windows.
- VMs can also provide integrated disaster recovery and application provisioning options.

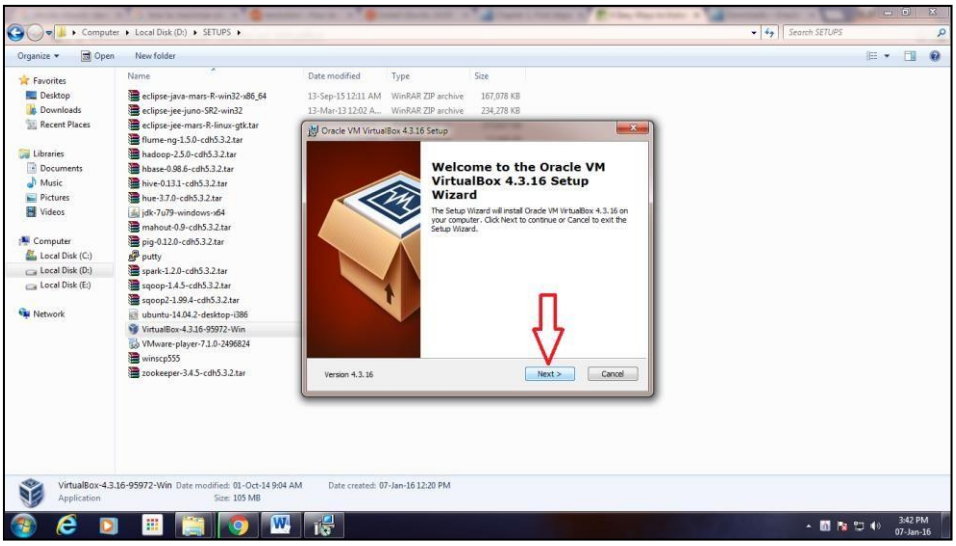
The two types of virtual machines

Users can choose from two different types of virtual machines—process VMs and system VMs:

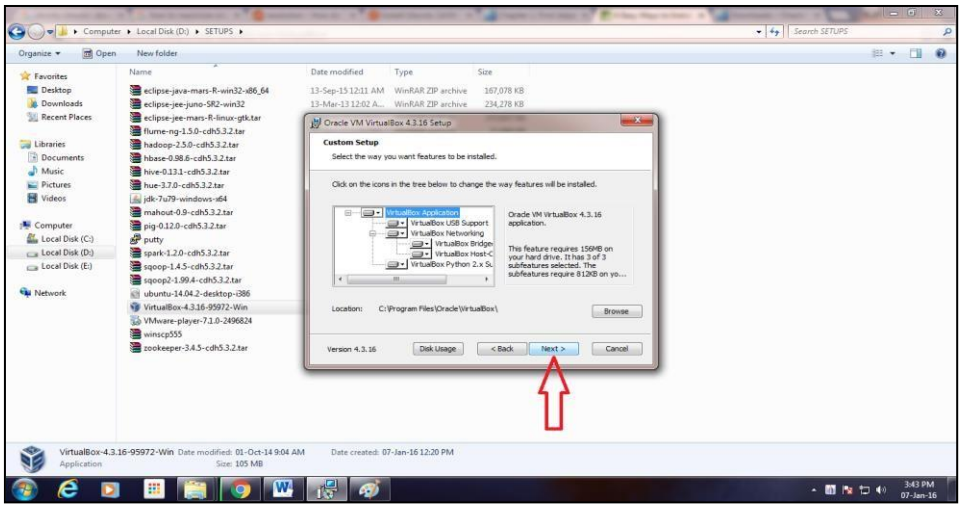
- **A process virtual machine** allows a single process to run as an application on a host machine, providing a platform-independent programming environment by masking the information of the underlying hardware or operating system. An example of a process VM is the Java Virtual Machine, which enables any operating system to run Java applications as if they were native to that system.
- **A system virtual machine** is fully virtualized to substitute for a physical machine. A system platform supports the sharing of a host computer's physical resources between multiple virtual machines, each running its own copy of the operating system. This virtualization process relies on a hypervisor, which can runon bare hardware, such as VMware ESXi, or on top of an operating system.

Step Of Installation of Virtual Machine:

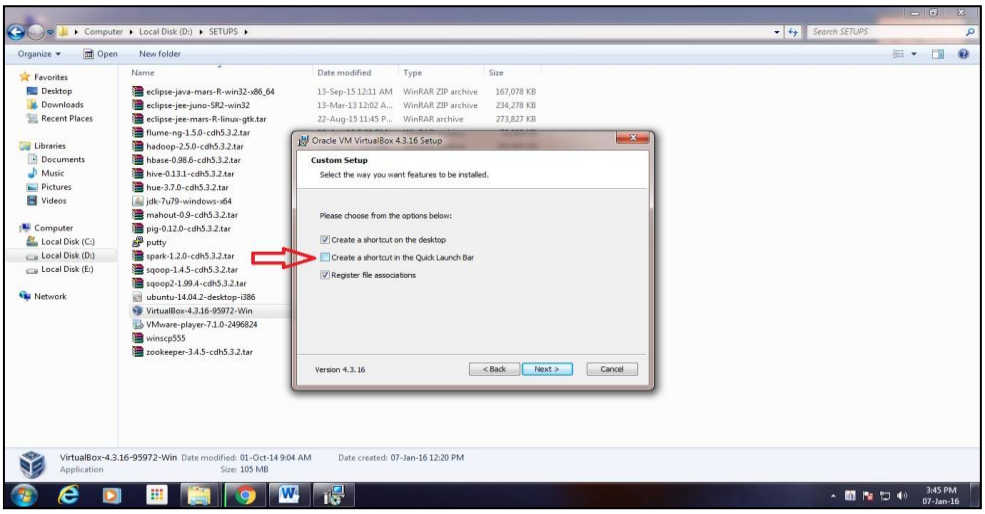
Step 1.



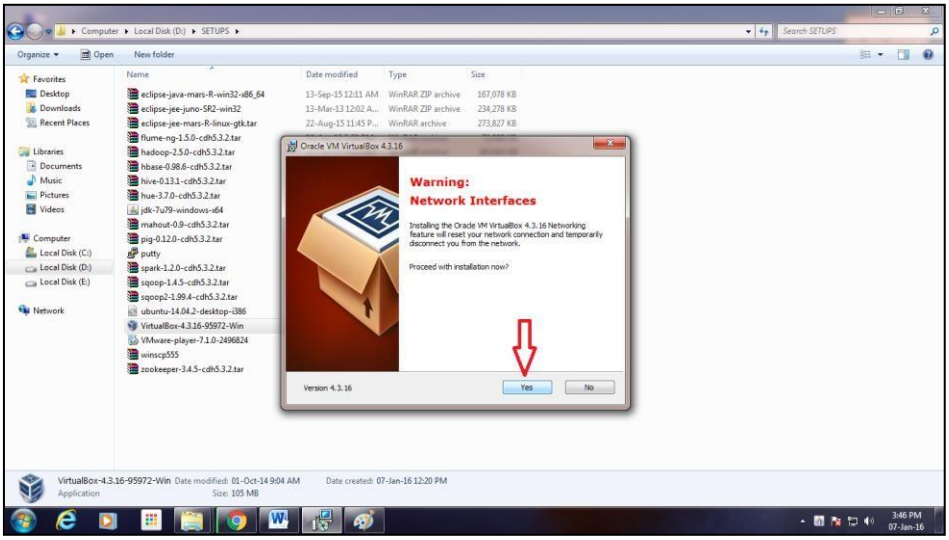
Step 2.



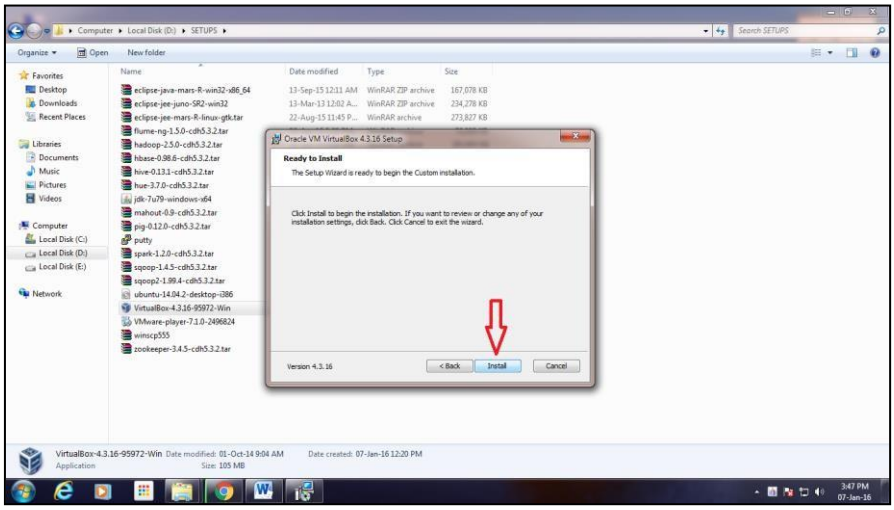
Step 3.


Oracle VM VirtualBox 4.3.16 Setup
Custom Setup
Select the way you want features to be installed.
Please choose from the options below:
Create a shortcut on the desktop
Create a shortcut in the Quick Launch Bar
Register file associations
Version 4.3.16
< Back
Next >
Cancel

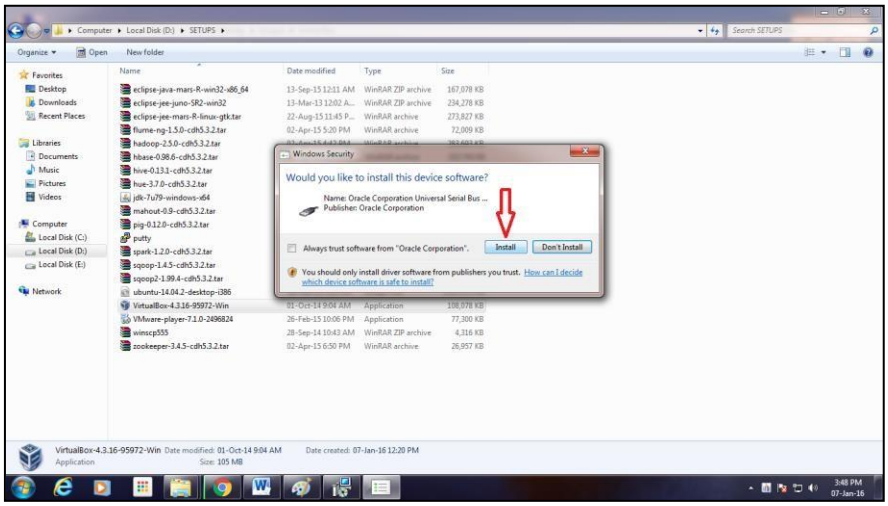
Step 4.


Oracle VM VirtualBox 4.3.16
Warning:
Network Interfaces
Installing the Oracle VM VirtualBox 4.3.16 Networking feature will reset your network connection and temporarily disconnect you from the network.
Proceed with installation now?
Version 4.3.16
Yes
No

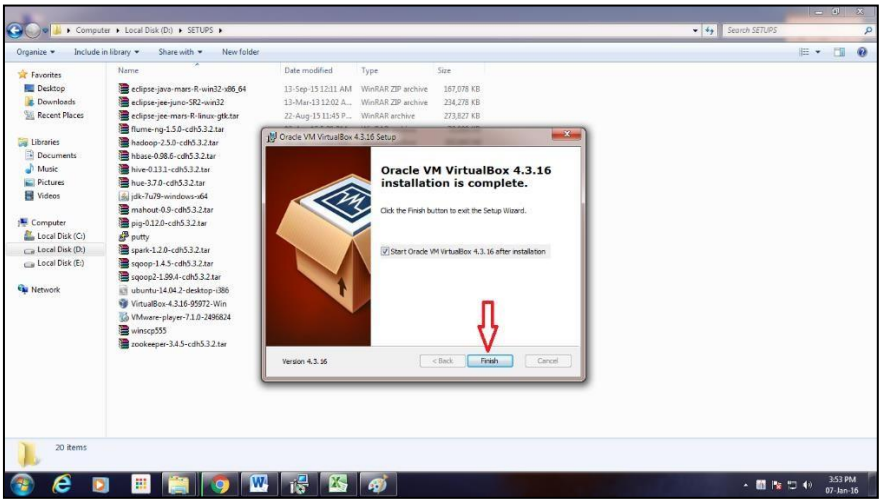
Step 5.


Oracle VM VirtualBox 4.3.16 Setup
Ready to Install
The Setup Wizard is ready to begin the Custom installation.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Version 4.3.16
< Back
Install
Cancel

Step 6.

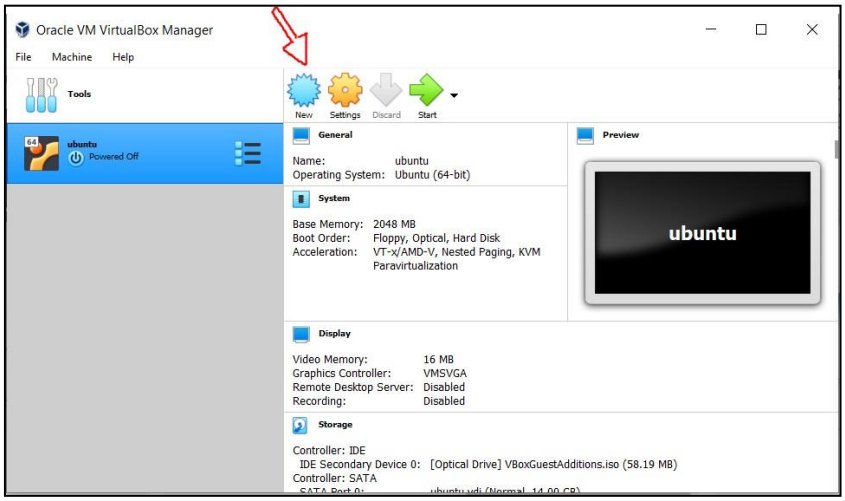

Windows Security
Would you like to install this device software?
Name: Oracle Corporation Universal Serial Bus ...
Publisher: Oracle Corporation
Always trust software from "Oracle Corporation".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Step 7.

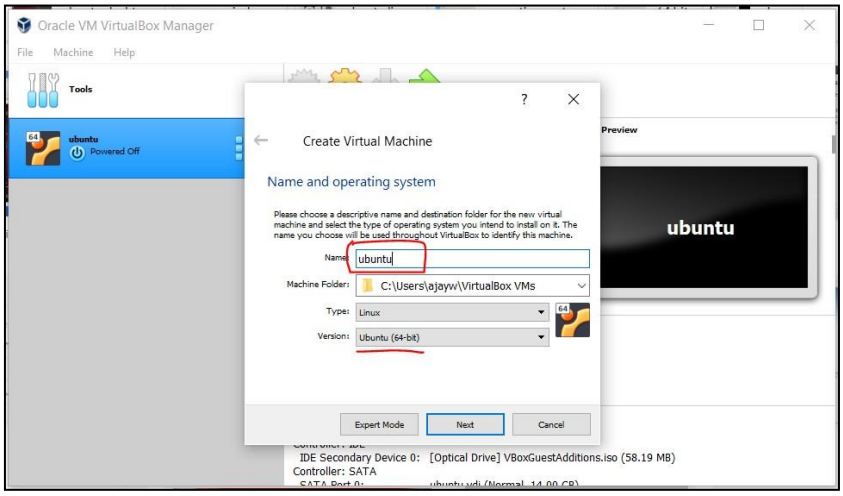


An ISO file is **an image file of a CD/DVD or other disc**. It contains all the files from the disc, neatly packed into a single. iso file. This allows users to burn new copies of the disc, or they can open the ISO file to browse and copy its contents to their system.

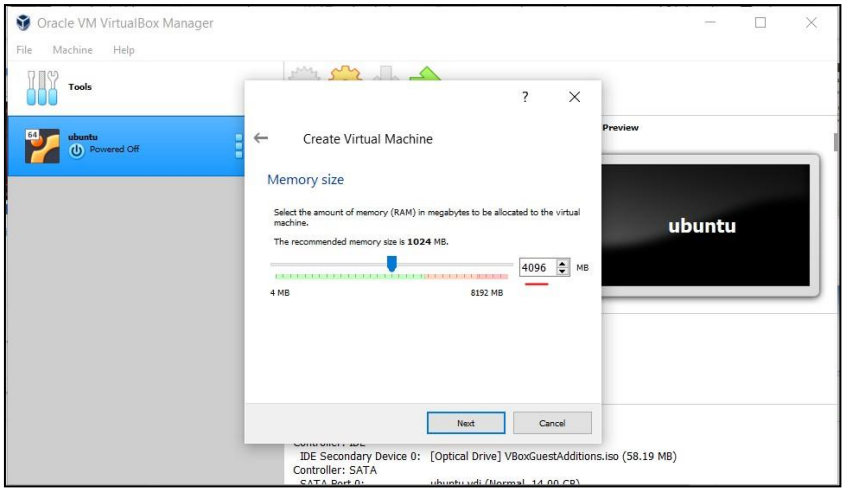
Step 8.



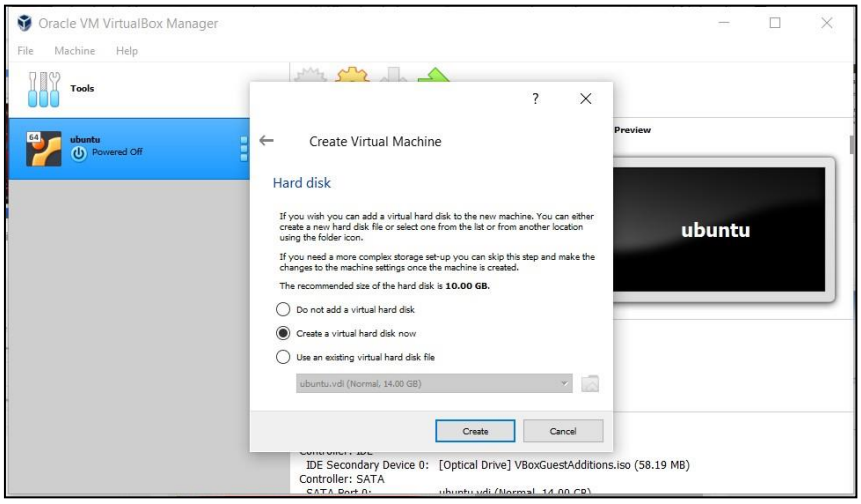
Step 9.



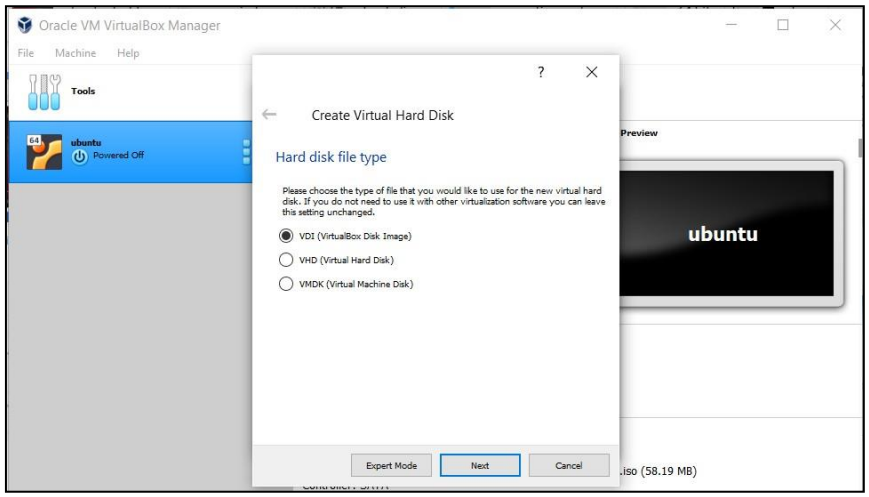
Step 10.



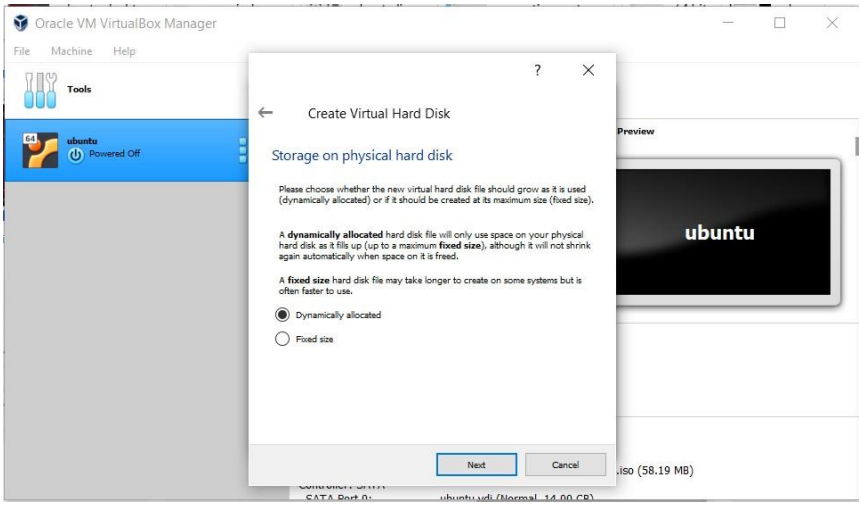
Step 11.



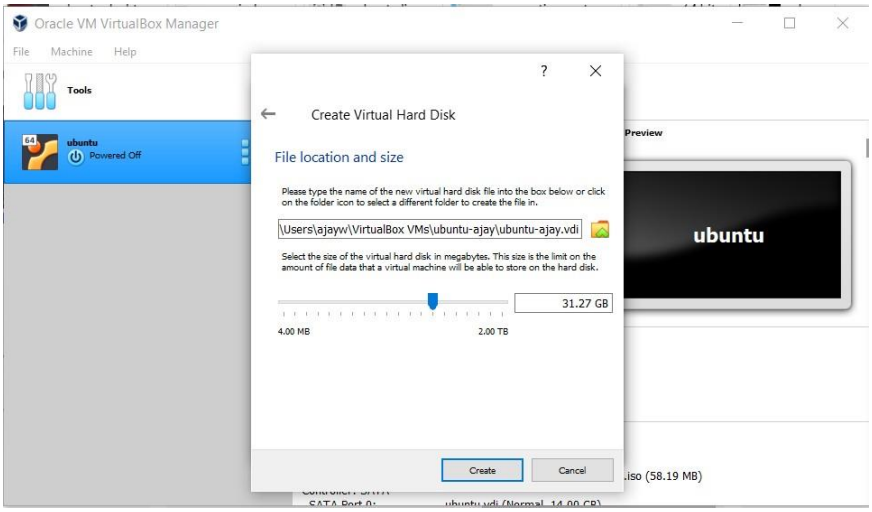
Step 12.



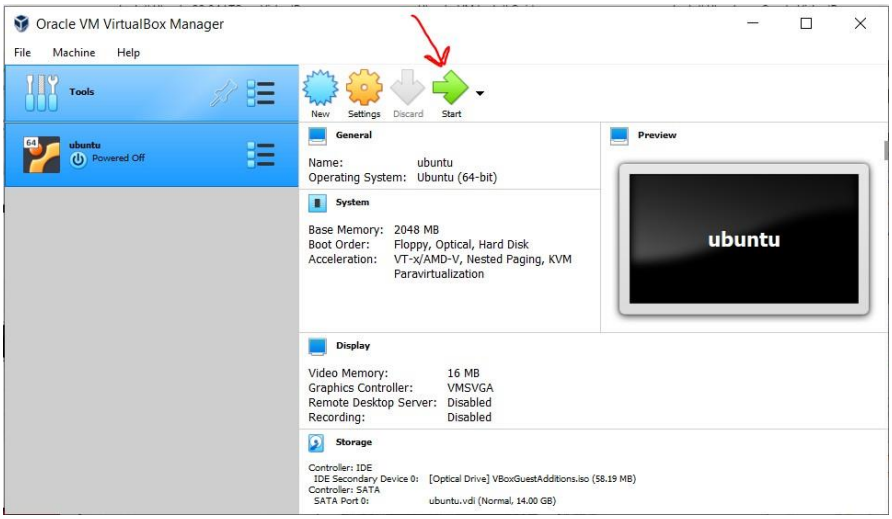
Step 13.



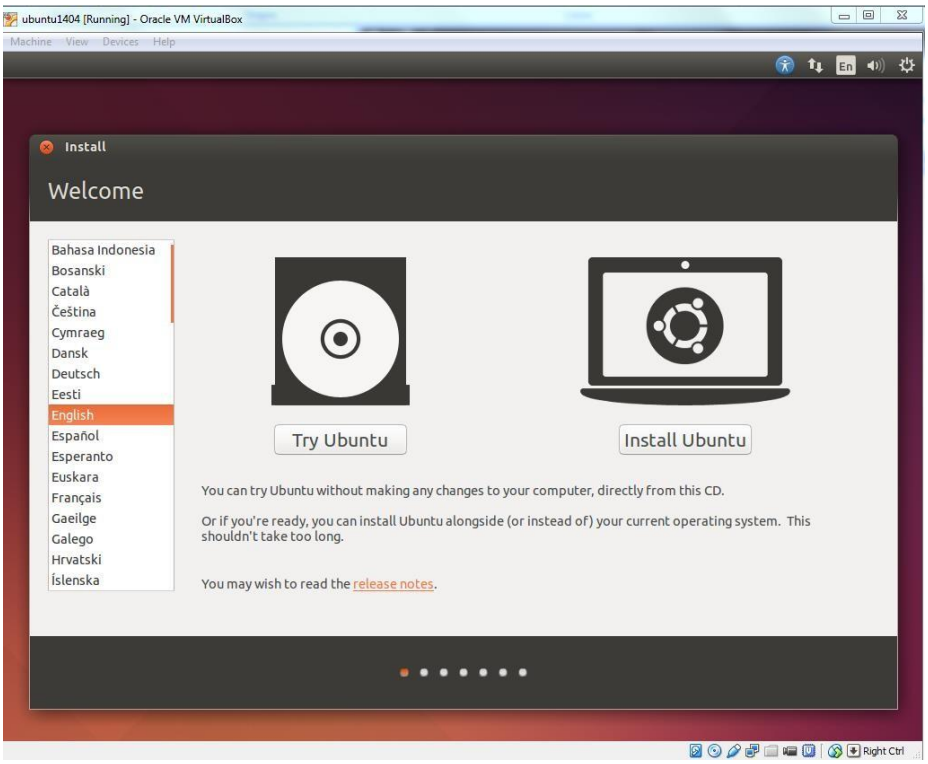
Step 14.



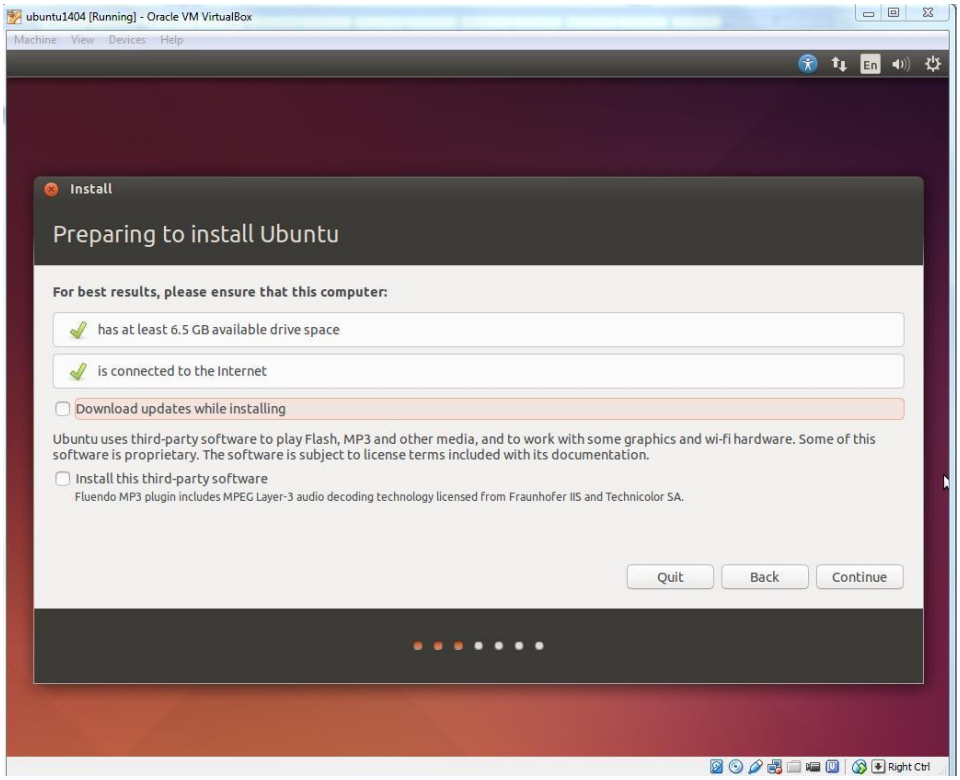
Step 15.



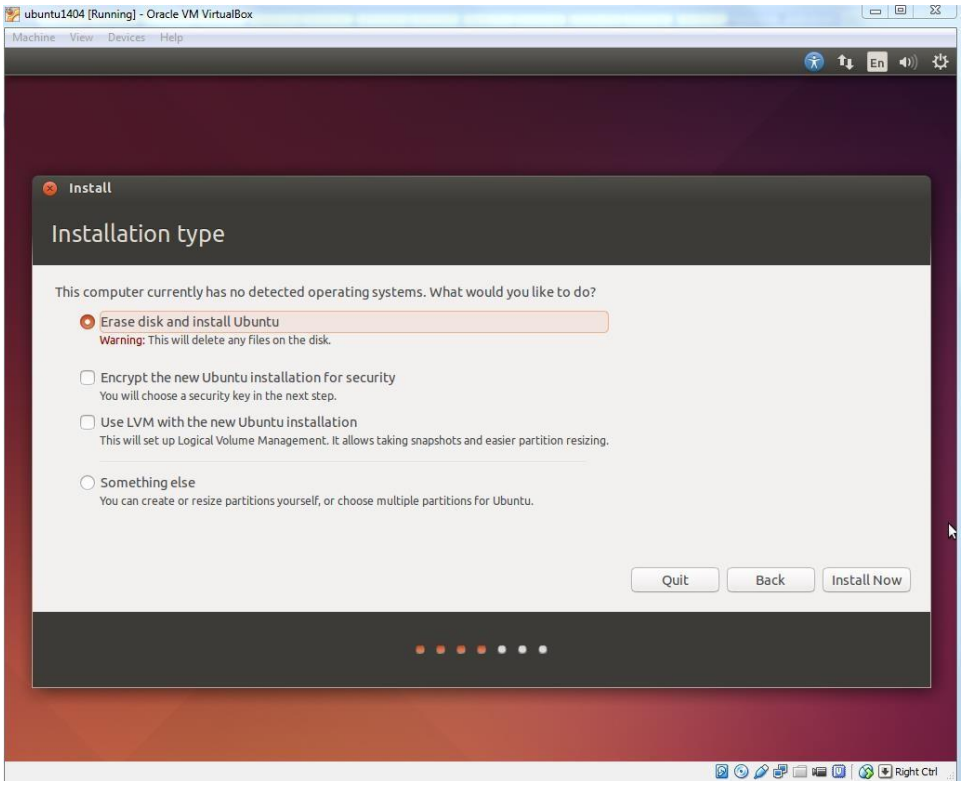
Step 16.



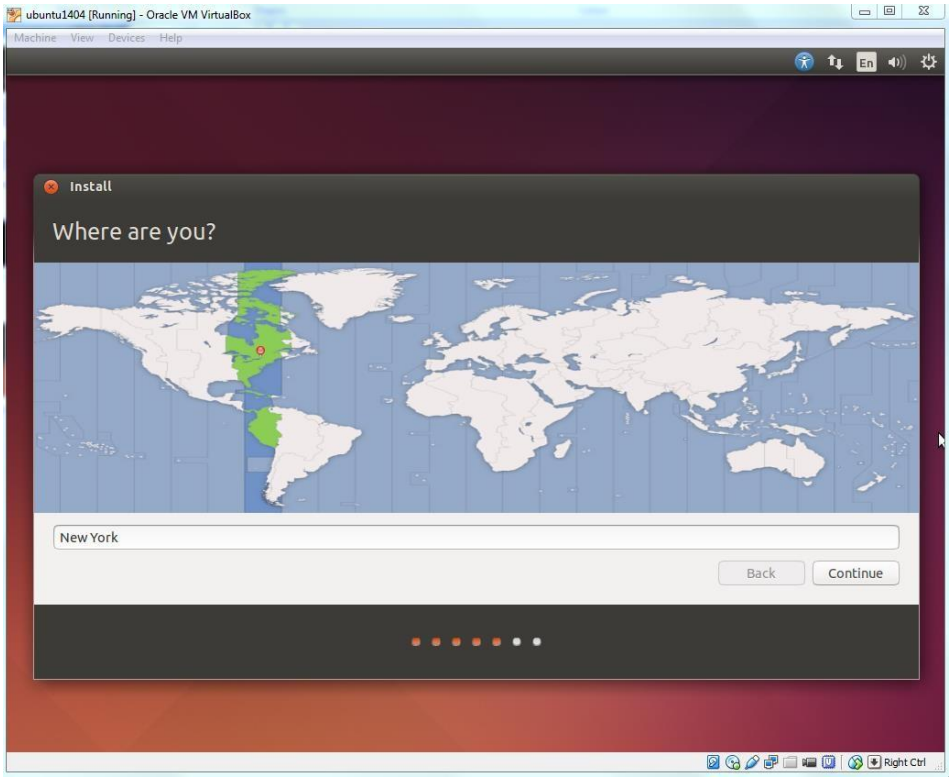
Step 17.



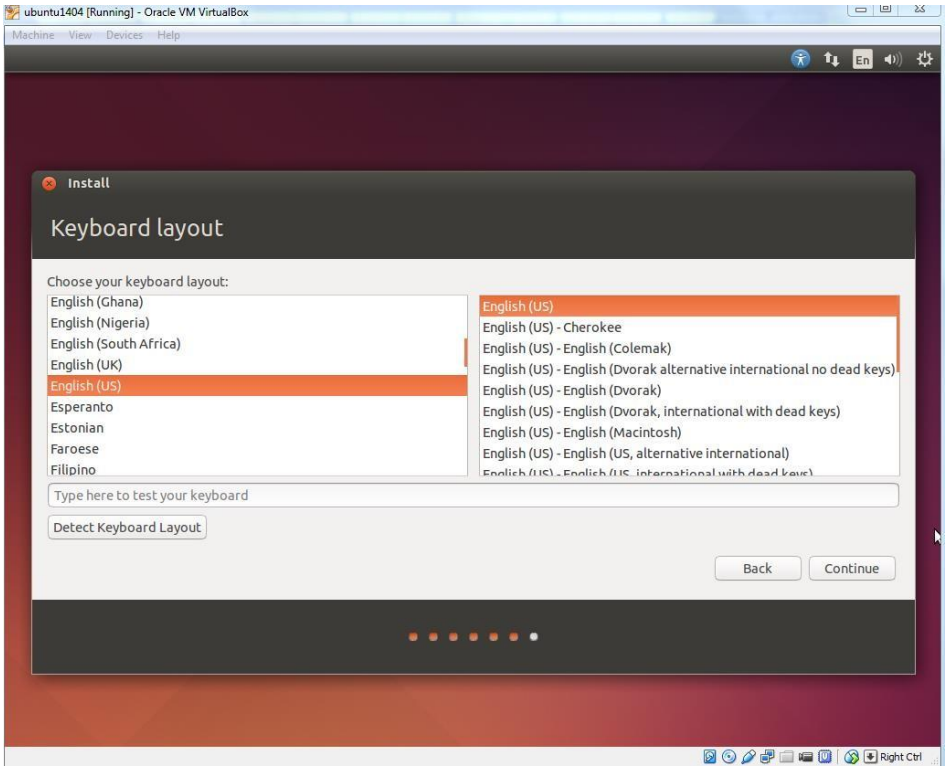
Step 18.



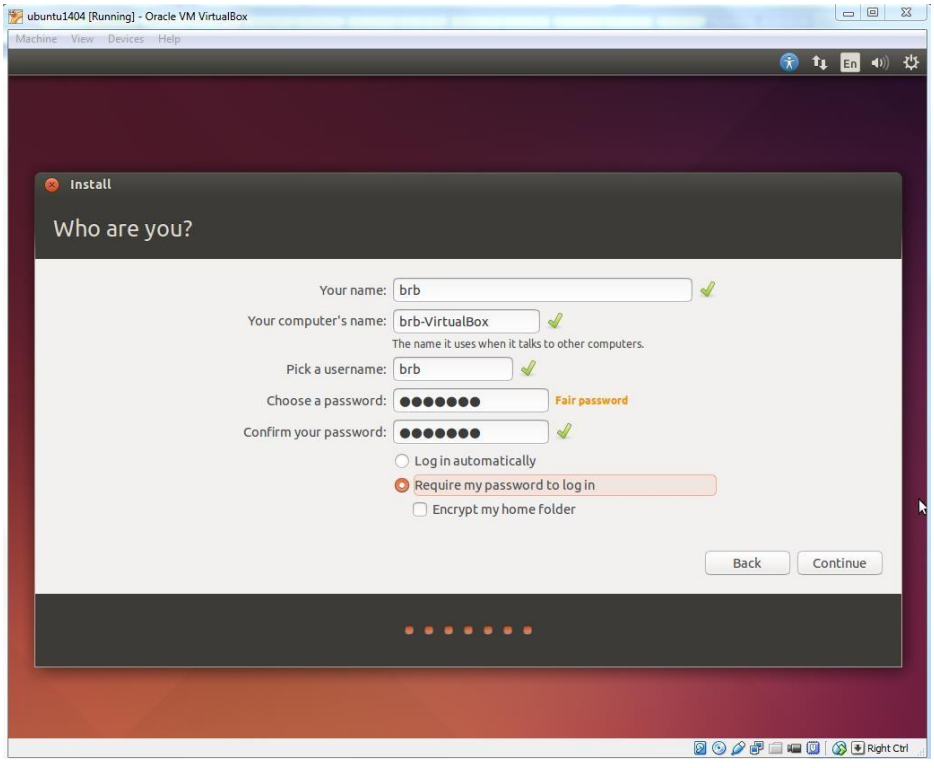
Step 19.



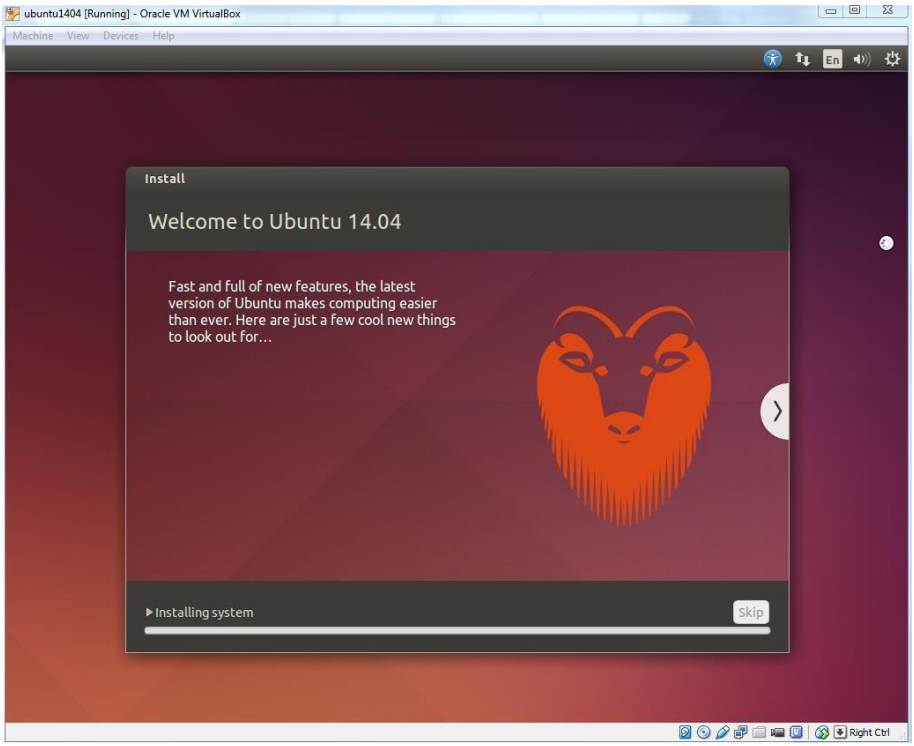
Step 20.



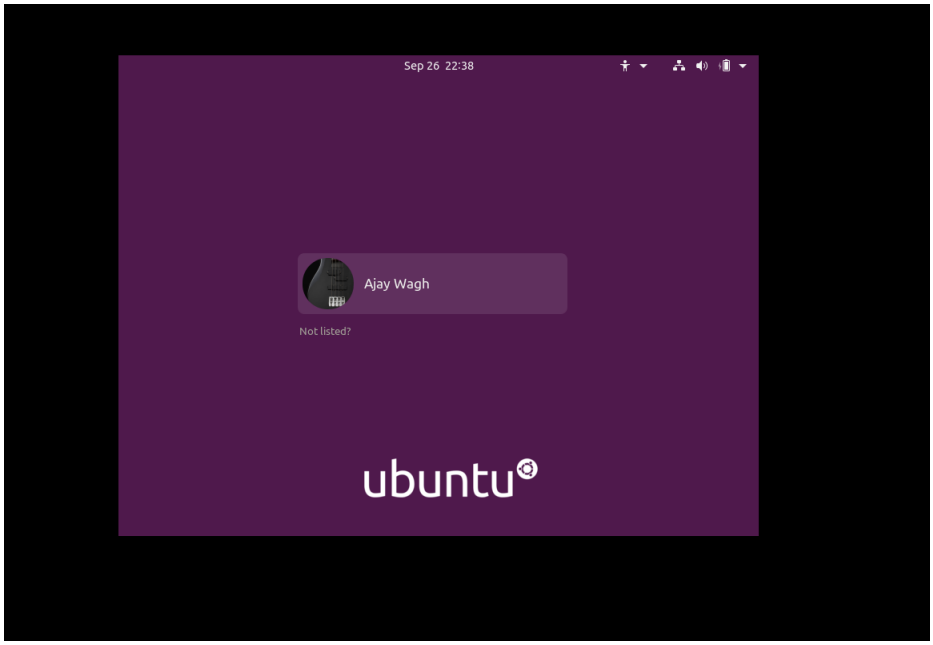
Step 21.



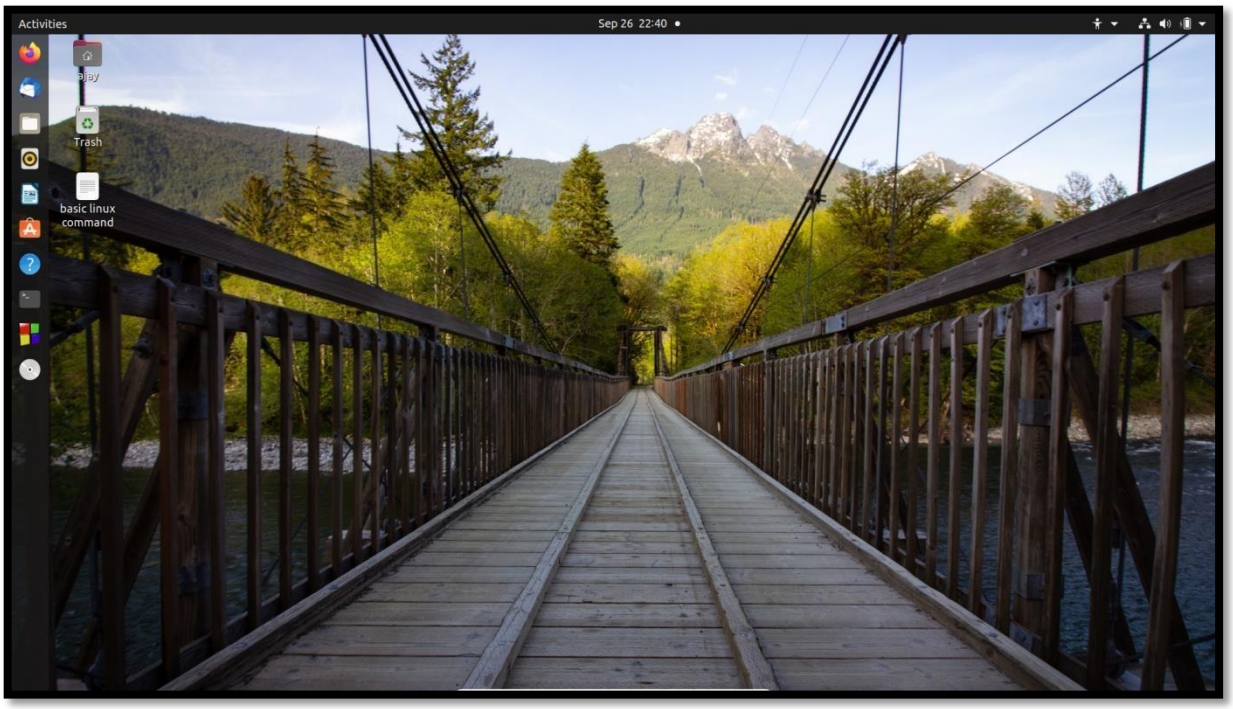
Step 22.



Step 23.



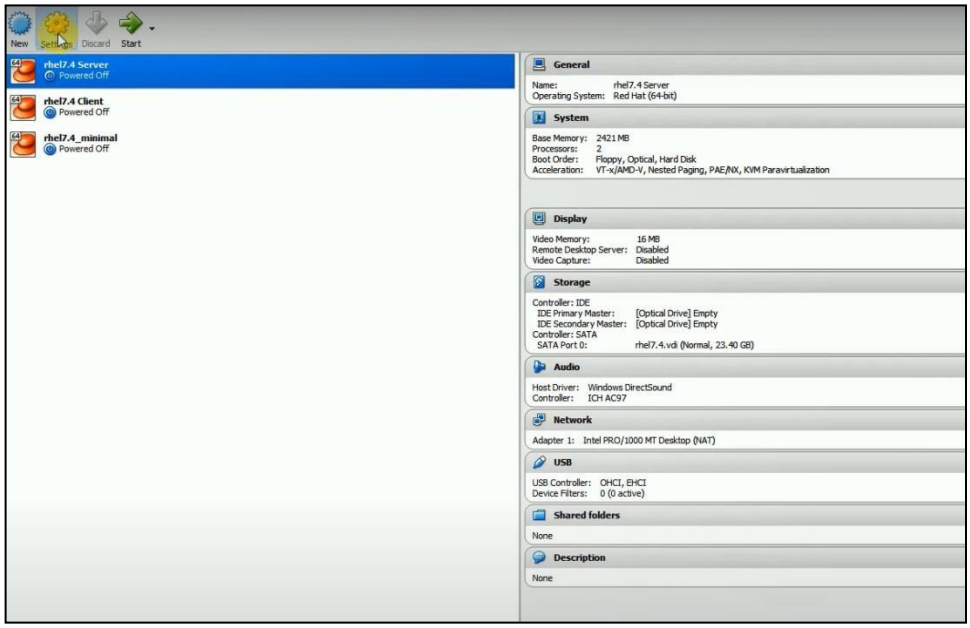
Ubuntu Run successfully in Virtual Machine.



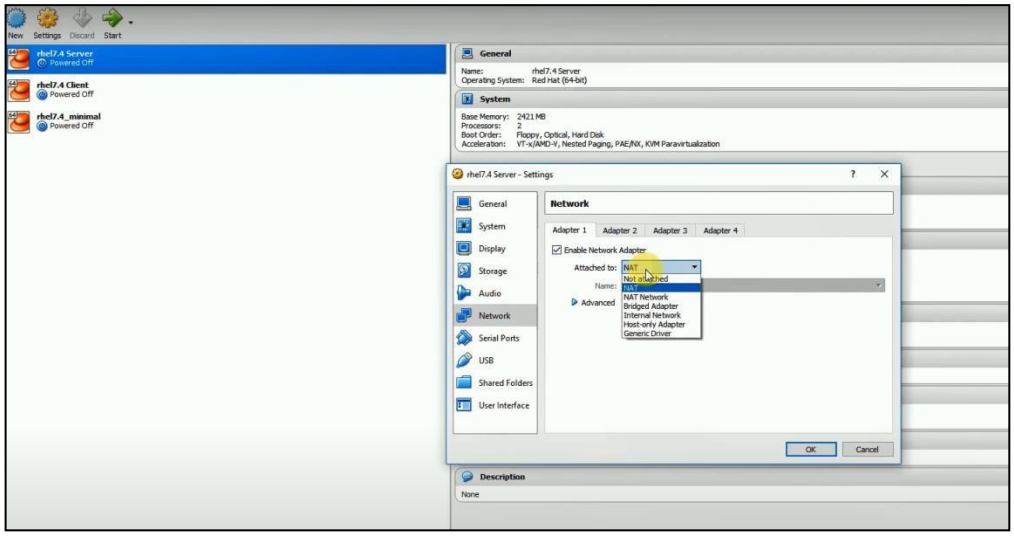
3. Communicate the Two Virtual Machine:

The VirtualBox graphical user interface supports only four network adapters for each VM. This limits the complexity of network scenarios you can create. Fortunately, VirtualBox really supports up to thirty-six network adapters per VM. These additional network adapters may be configured using the VirtualBox command-line interface.

Step 1: Go to VM Setting**.**



Step 2: Open Network tap and check the network adaptor with NAT Network are Available or Not.

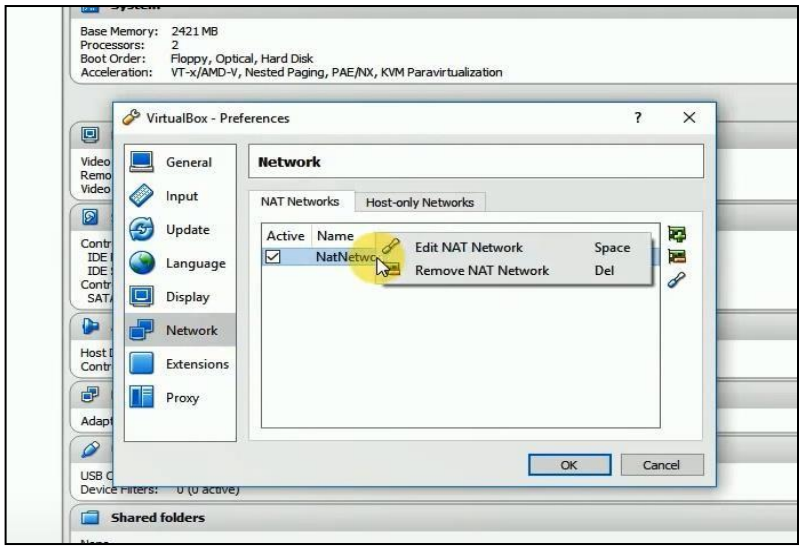


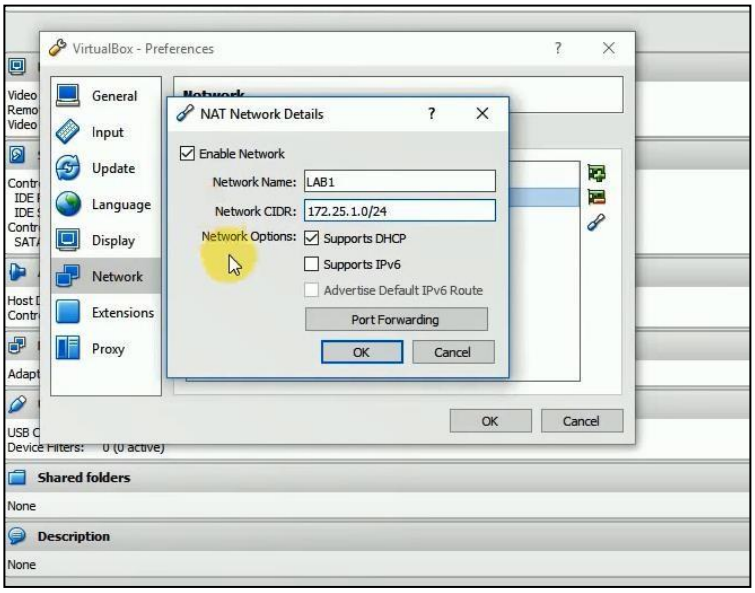
If Not Available Follow Step.

Step 3: click on File menu in VM select the **Preferences** or use Shortcut key (Ctrl + G). A new Windows are open. Select

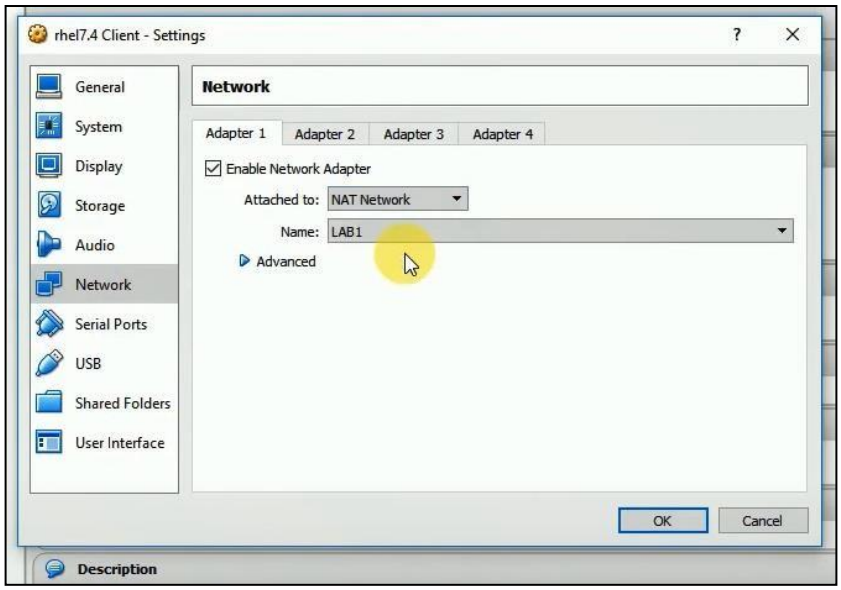
Network -> NAT Networks -> Add NAT Networks

One network is created. Click On given network and edit NAT network Details**.**





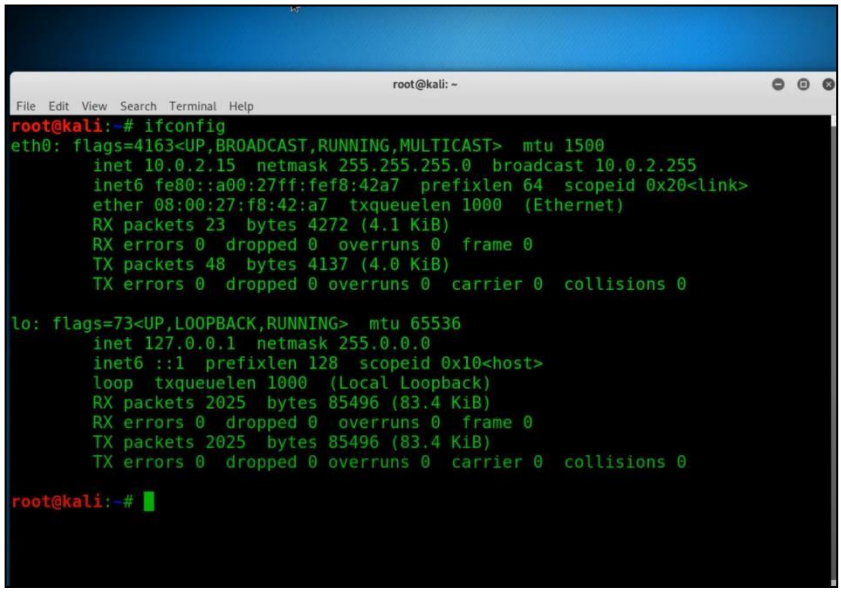
Step 4: Go to Both Virtual Machine Setting and Change the Network Adaptor with Created NAT Neworks.



Step 5: Start the Both Virtual Machine**.**

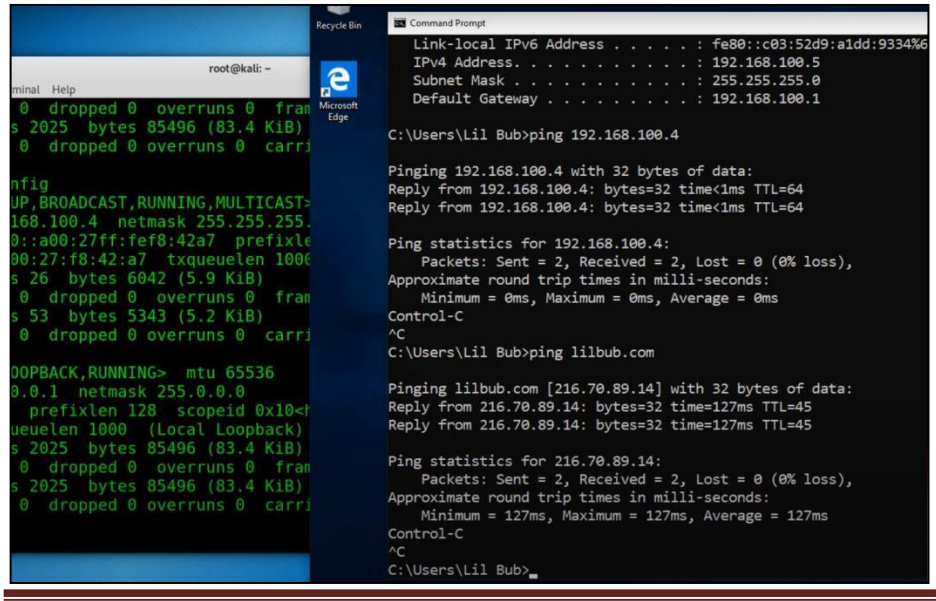
Step 6: Open Terminal and check IP address of both Virtual Machine using

~ifconfig Command



Step 7: Create the Communications between Two Virtual Machine using

$ ping <IP Address Other VM>



Step 8: Repeat the Step 7 for Other Virtual Machine.

Conclusion: Here we have installed two Virtual Machines on VirtualBox and they can communicate with each other over VM.

EXPERIMENT NO:04

Title: Implementation and case study of Google App Engine

Solution:

Google App Engine (often referred to as GAE or simply App Engine) is a cloud computing platform as a service for developing and hosting web applications in Google- managed data centers. Applications are sandboxed and run across multiple servers. App Engine offers automatic scaling for web applications—as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

Google App Engine primarily supports Go, PHP, Java, Python, Node.js, .NET, and Ruby applications, although it can also support other languages via "custom runtimes". The service is free up to a certain level of consumed resources and only in standard environment but not in flexible environment.

Fees are charged for additional storage, bandwidth, or instance hours required by the application. It was first released as a preview version in April 2008 and came out of preview in September 2011.

Why Google App Engine is used?

Google allows you to add your web application code to the platform while managing the infrastructure for you. The engine ensures that your web apps are secure and running and saves them from malware and threats by enabling the firewall.

Feature of Google Cloud App Engine

1	**Popular Language**	Build your application in Node.js,Java,Ruby,C#,Python or PHP-or bring your own language runtime
2	**Open and flexible**	Custom runtimes allow you to bring any library and framework to App Engine by supplying a Docker container.
3	**Fully Managed**	A fully managed environment lets you focus on code while App Engine manages infrastructure concerns.
4	**Powerful application diagnostics**	Use Cloud Monitoring and Cloud Logging to monitor the health and performance of your app and Cloud Debugger and Error Reporting to diagnose and fix bugs quickly.

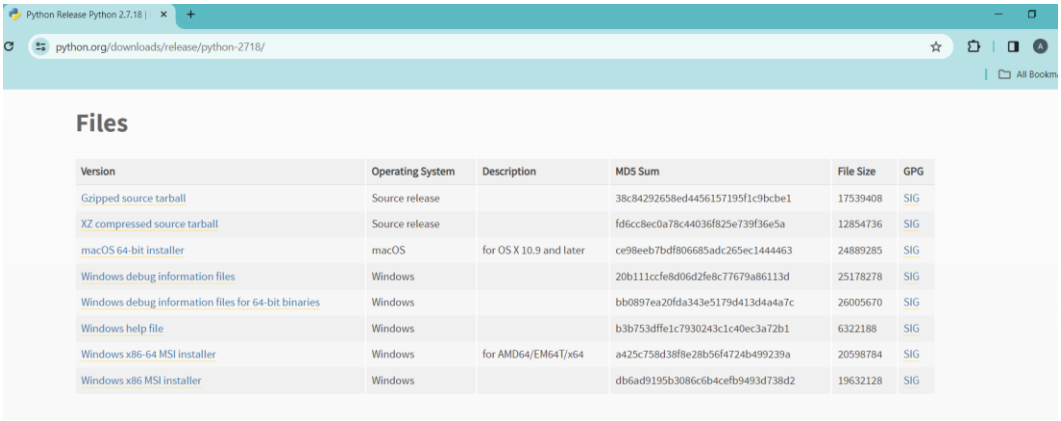
5	**Application Versioning**	Easily host different versions of your app, and easily create development, test, staging, and production environments.
6	**Traffic Splitting**	Route incoming requests to different app versions, A/B test, and do incremental feature rollouts.
7	**Application Security**	Help safeguard your application by defining access rules with App Engine firewall and leverage managed SSL/TLS certificates by default on your custom domain at no additional cost.
8	**Services Ecosystem**	Tap a growing ecosystem of Google Cloud services from your app including an excellent suite of cloud developer tools.

1. Installing Python and Google Cloud Sdk

i. Installing Python 2.7.18:

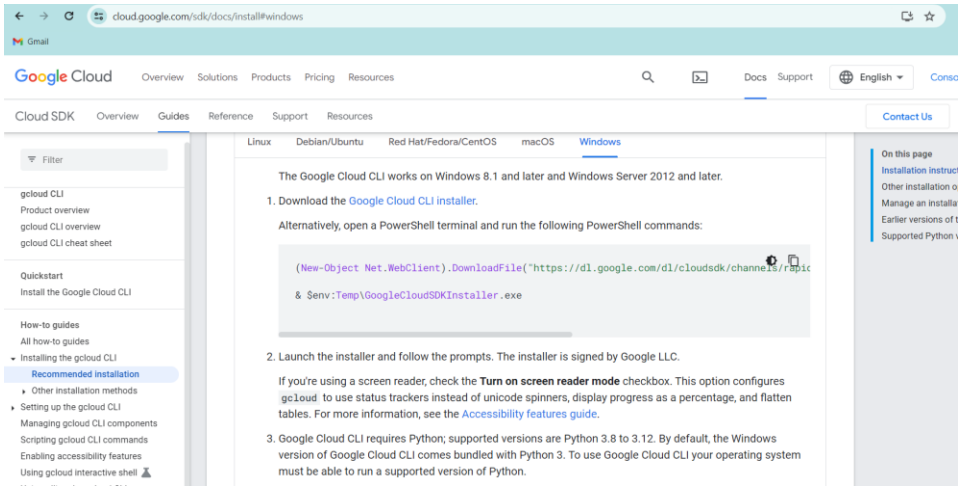
Go to link: https://www.python.org/downloads/release/python-2718/ and install the appropriate version.

After installation, go to environment variables>user variables>path><Enter your python file path>, according to the folder location.



ii. Installing Google Cloud Sdk:

a. Go to link: https://cloud.google.com/sdk/docs/install and install the Google Cloud CLI installer.



2. Writing the Program

Create a folder and create 2 files.

1. Main.py

Write the following program in main.py file. Make sure webapp2 is installed.

```
Welcome | app.yaml | main.py
Cloud > main.py
1  import webapp2
2
3  class MainPage(webapp2.RequestHandler):
4      def get(self):
5          self.response.write("Hello World!")
6
7  app = webapp2.WSGIApplication([('/', MainPage)], debug=True)
8
```

2. App.yaml

Write the following instructions in the app.yaml file.

```
Welcome | app.yaml | main.py
Cloud > app.yaml
1  runtime: python27
2  api_version: 1
3  threadsafe: true
4
5  handlers:
6  - url: /
7    script: main.app
```

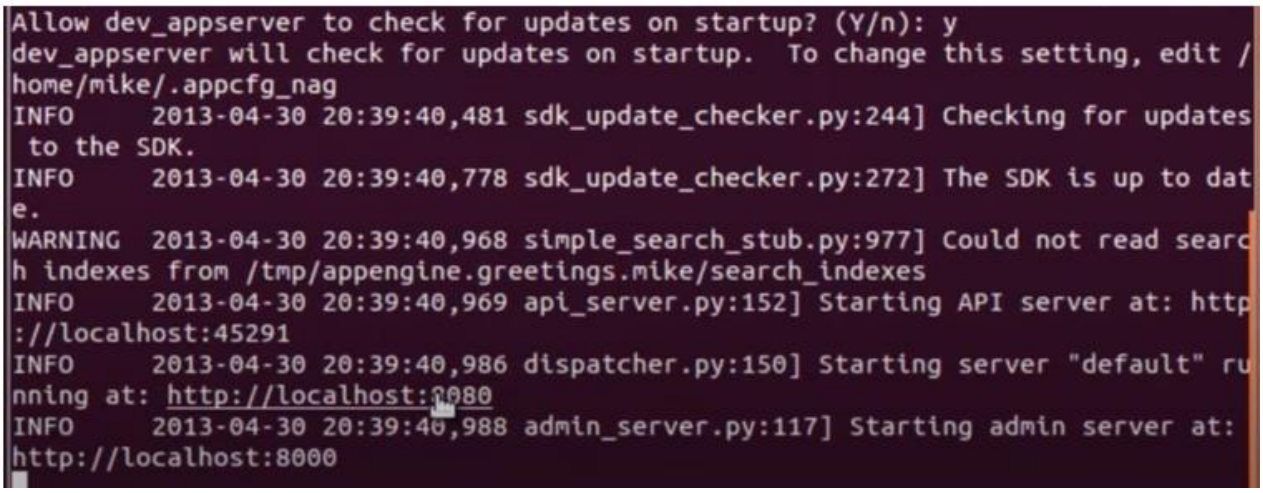
3. Running the Program

i. Check if the CLI recognizes the python version by entering: *python -V*

ii. To run the program, open Google Cloud SDK Shell and type the following command:
py google-cloud-sdk\bin\dev_appserver.py <Folder location where both programs are located>

4. Output

This is the generated output window where link to the localhost is listed.



Go to browser and paste the localhost address to see the output.

Conclusion: Thus, we have studies Google App Engine and implemented simple app on Google App Engine.

EXPERIMENT NO.:05

Title: Implementation and case study of Saleforce.com cloud

Solution:

Salesforce Service Cloud is a customer relationship management (CRM) platform for customer service and support. Salesforce based Service Cloud on its Sales Cloud product, a popular CRM software for sales professionals.

Service Cloud enables users to automate service processes, streamline workflows and find key articles, topics and experts to support customer service agents. The purpose is to foster one-to-one marketing relationships with every customer across multiple channels and devices.

Salesforce.com applied cloud computing in several ways. One of these ways included the use of contemporary Saleforce.com web site that focused on cloud computing and grading of commodities into three basic forms of clouds, namely; custom clouds, sevice cloud and sales cloud.

The firm applied both Sales and Service clouds in enhancing client related services. The firm also utilized the Force.com to enable its clients comes up with personal applications for utilization within the wider firm's network. That is the Force.com offered both IT services and tools that gave clients the capability to tailor their customer relationship management applications.

Main feature and benefits:

1. **Agent workspace.** This is a comprehensive and customizable user interface (UI) for customer service agents that offers various productivity tools, analytics and customer views.
2. **Case management.** Agents can use Service Console to juggle multiple cases at once across multiple channels. Case management is accessible via both desktop and mobile apps.
3. **Knowledge management.** Agents can create and access resources within the company's knowledge base.
4. **Service process automation.** Support functions can be automated with artificialintelligence (AI).
5. **Omnichannel routing.** Cases and leads can be automatically directed to specific employees based on factors such as employee skill set and availability. Supervisors can access a complete view of routing and agent activity.
6. **Service analytics.** Dashboards give employees easy access to reporting and key CRM data, such as backlog analysis, chatbot performance, case history and volume, and agent productivity and activity.

7. **Computer telephony integration (CTI).** Service calls to and from customers can be managed with customer information on hand.
8. **Automation with macros.** Repetitive customer service tasks can be automated.
9. **Asset and order management.** This tracks customer data, such as assets, order history and support history.

Salesforce Sales Cloud vs. Service Cloud

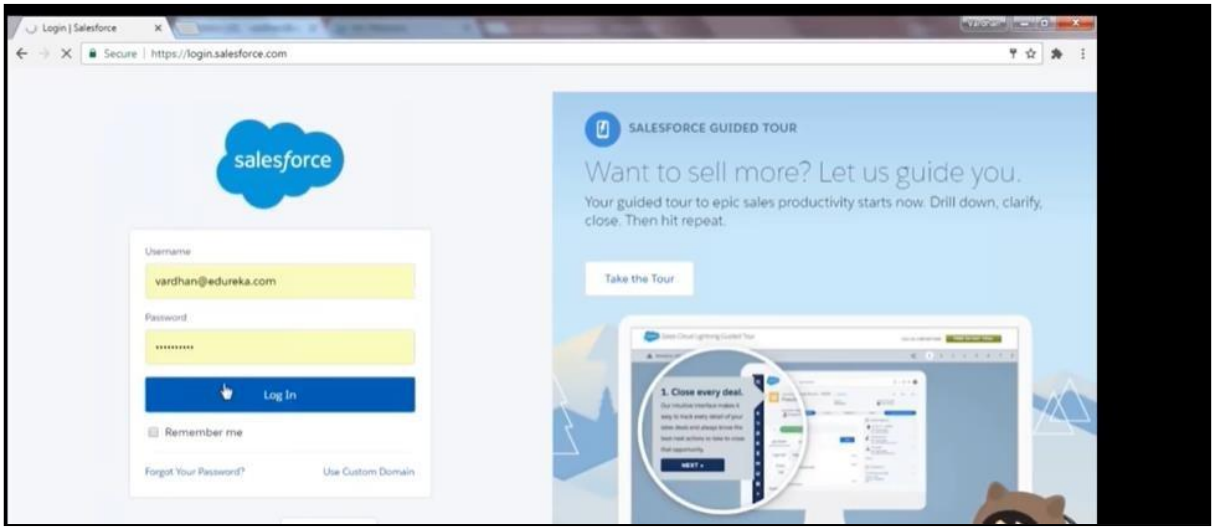
When customers enroll with Salesforce products, they have the option to choose between the Sales Cloud and the Service Cloud modules. There is considerable overlap between the two modules. The Sales Cloud product is used by businesses that are focused on generating leads, opportunities and sales. Salesforce Service Cloud, however, contains all of the features that Sales Cloud includes, plus additional features for service-oriented businesses with higher support process demands.

Follows Step for implementation of salesforce Cloud

Step 1:

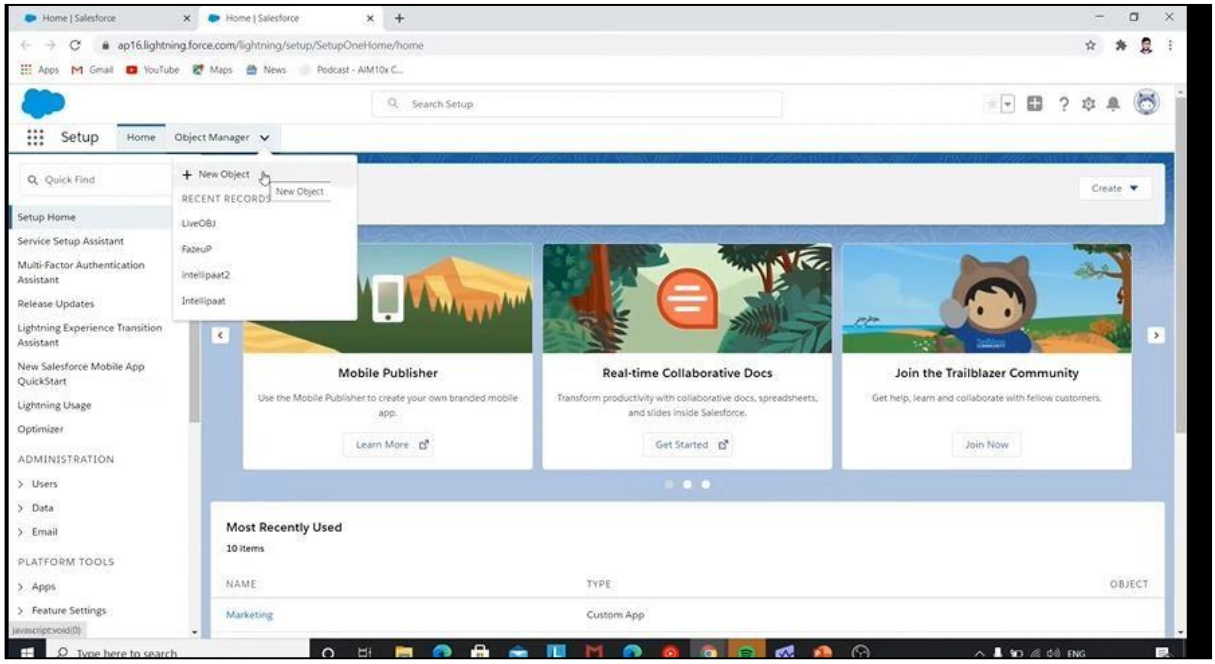
Open the Salesforce website URL
https://www.salesforce.org/

and login with Username and Password or create new cloud service account.



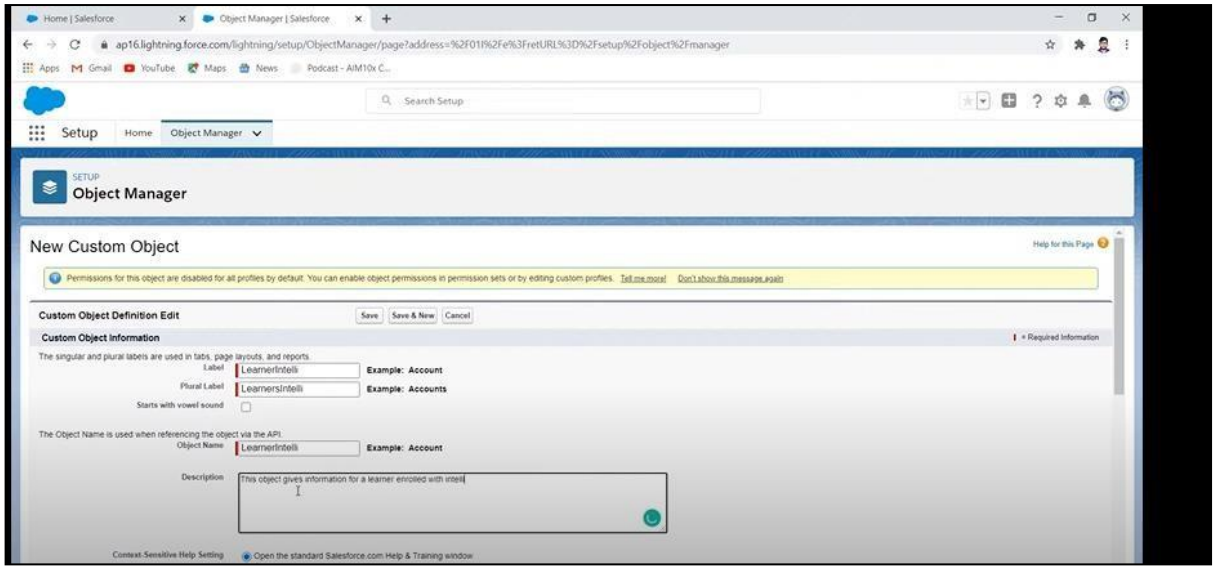
Step 2:

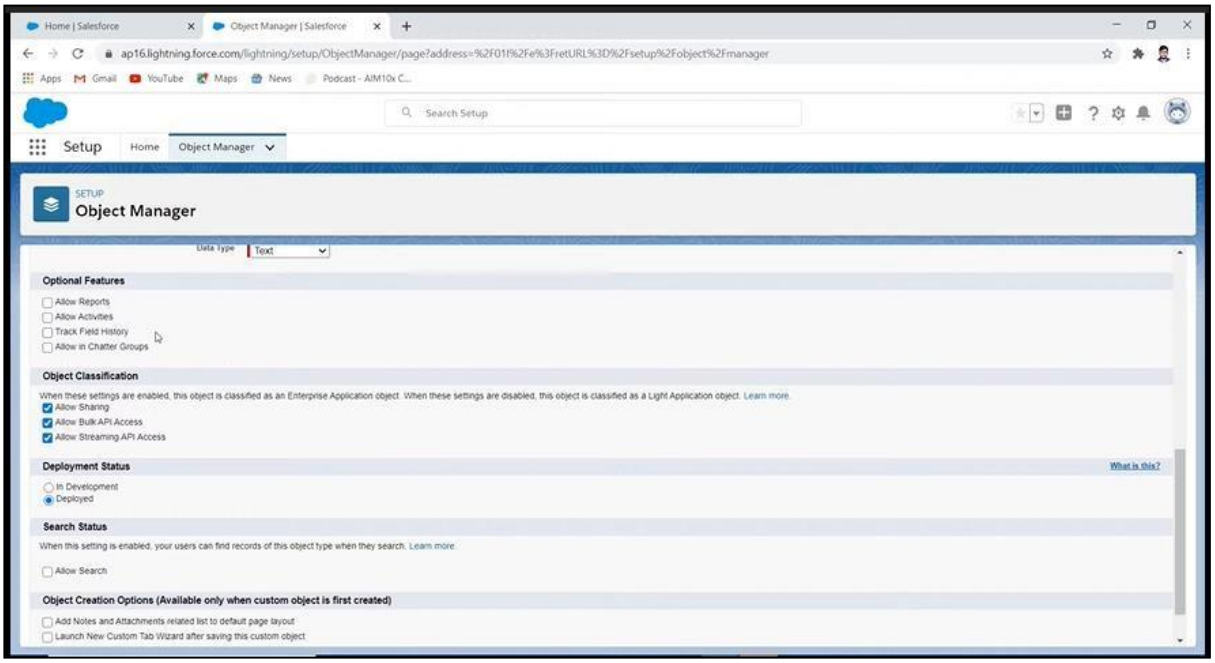
For the create new app in cloud first create the new object instances.



Step 3:

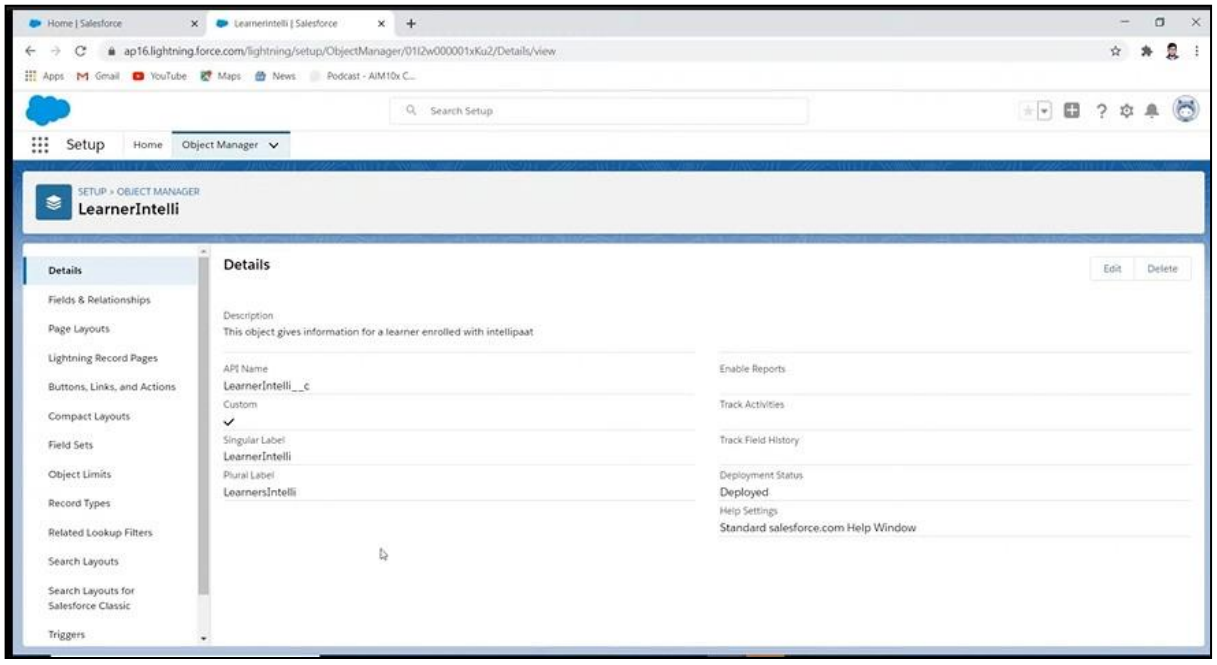
The new windows will be open fill the information related to the object creation.





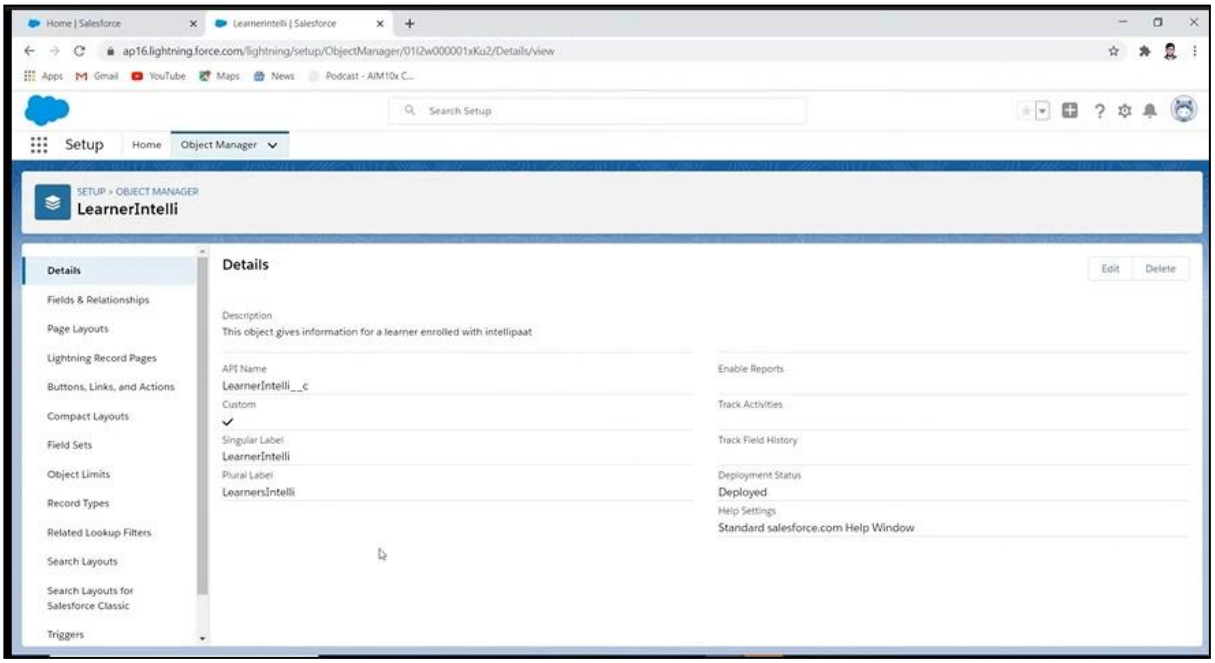
Step 4:

The new Object will be ready.



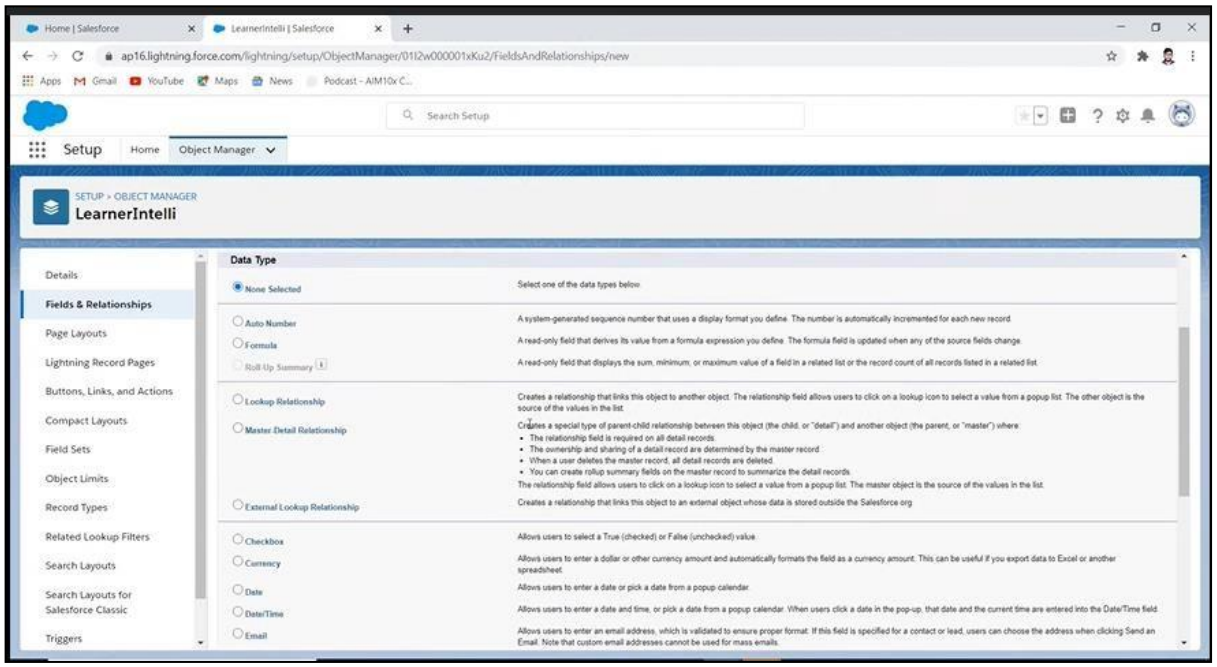
Step 5:

For accessing service and set implementation we add some properties,



Step 6:

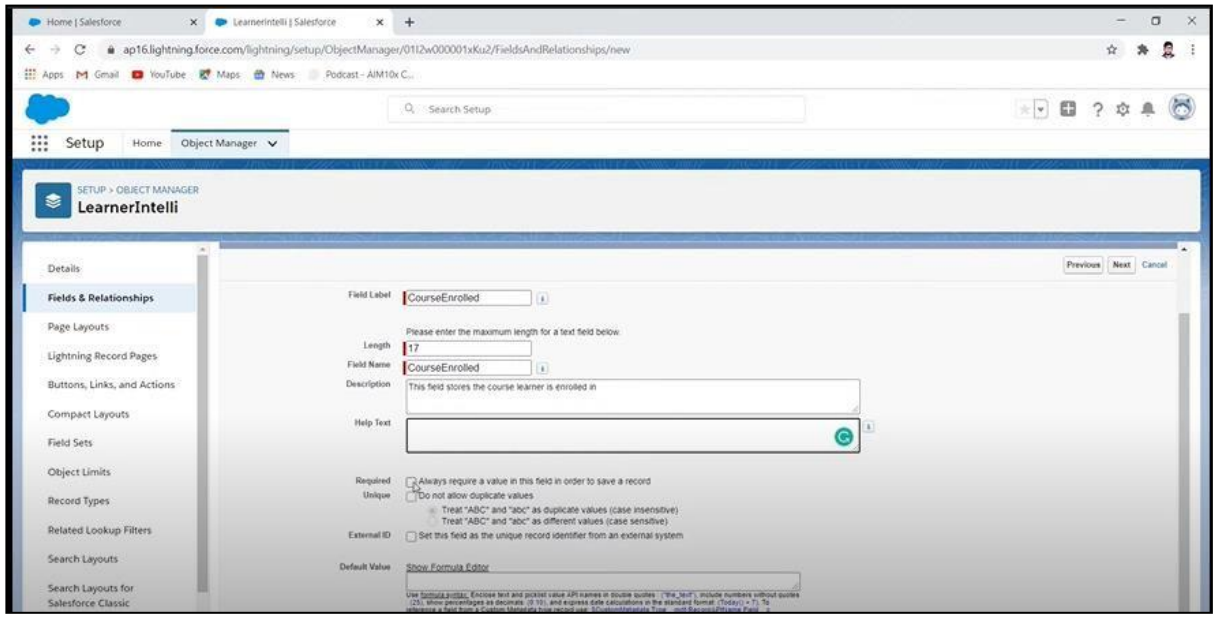
Go to the Fields and Relationship options and create new Fields,

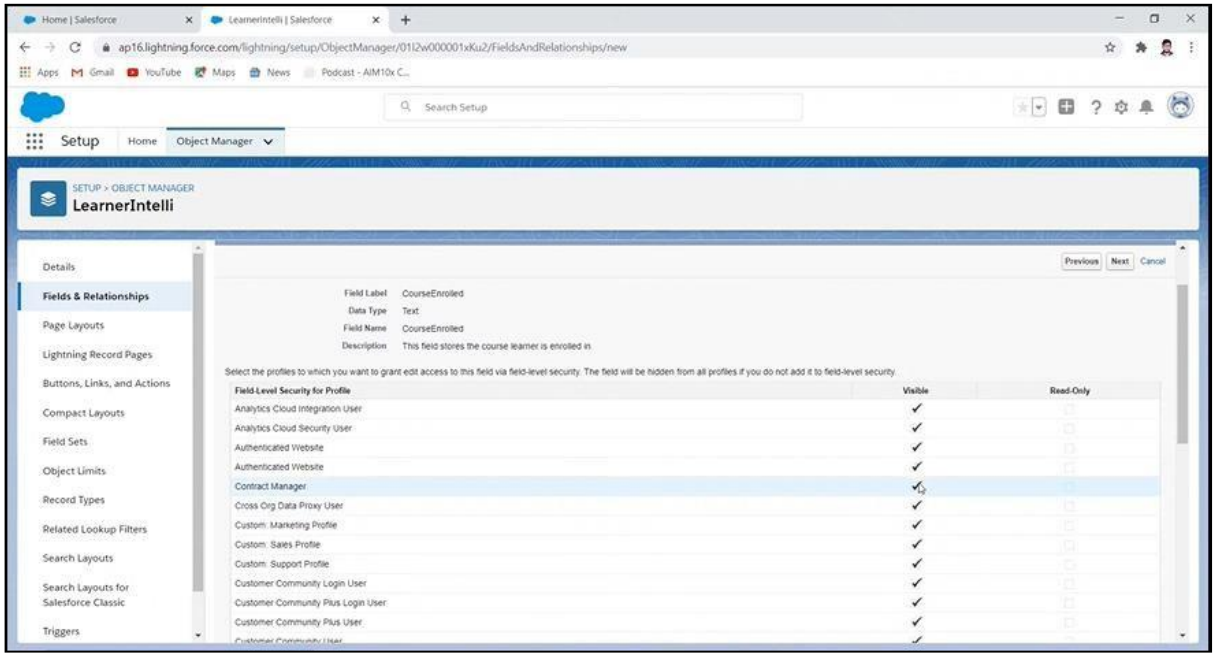


Step 7:

For example, create the text field in the properties list we select the text option.

Open new fields create windows will be open.

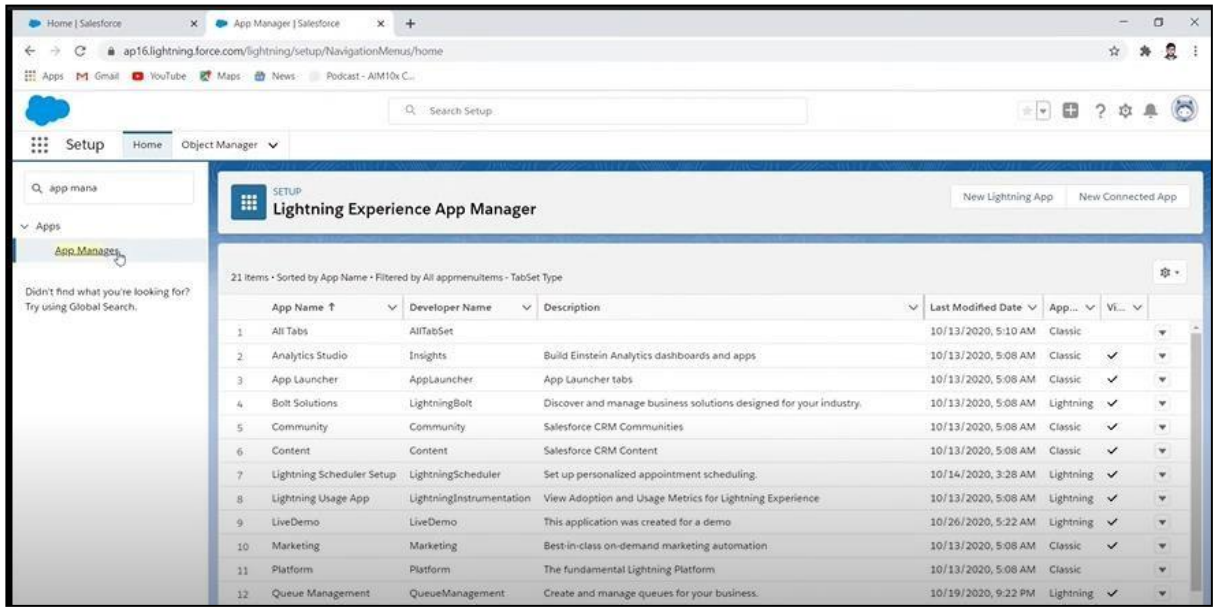




We create the app object.

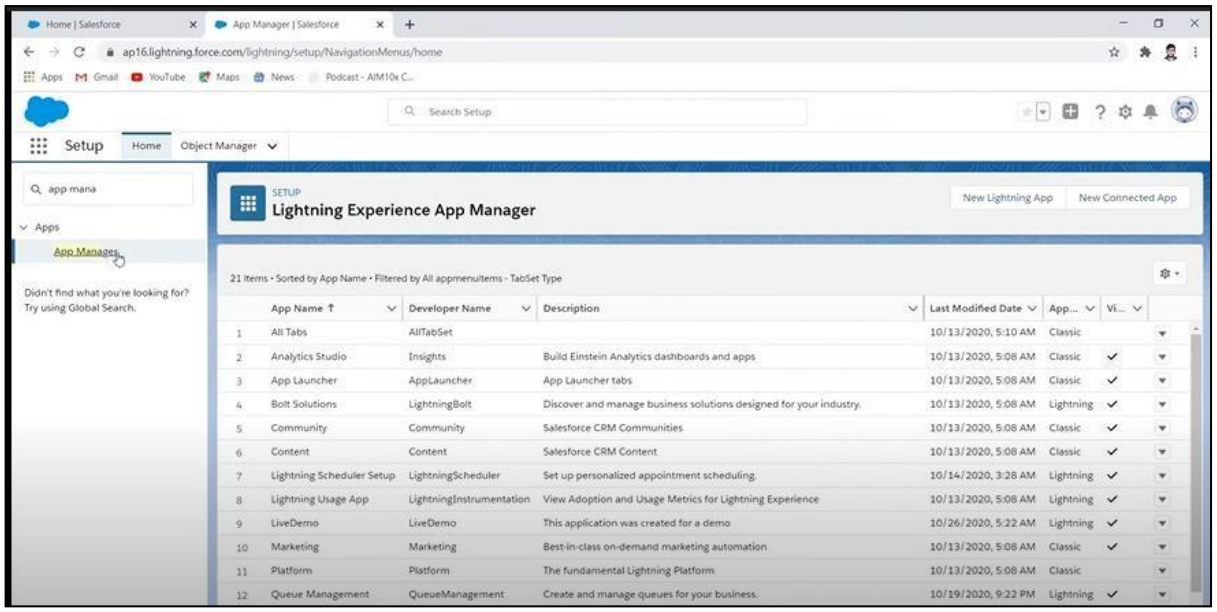
Step 8:

For app creation go to search bar and find app manager.

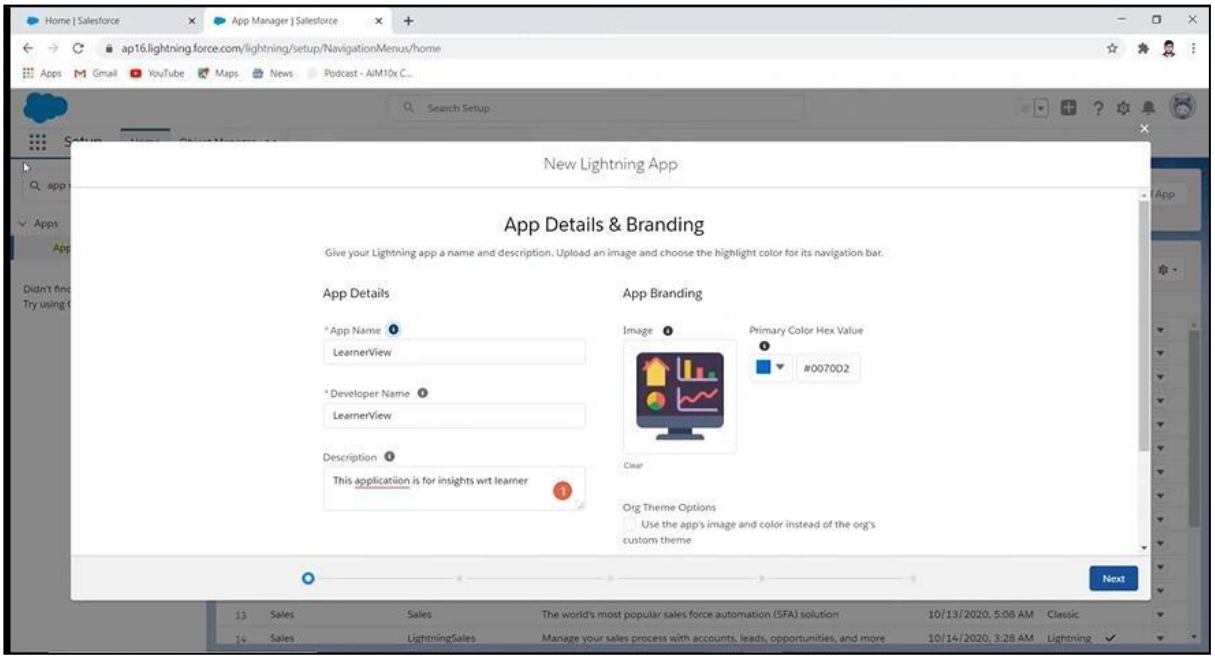


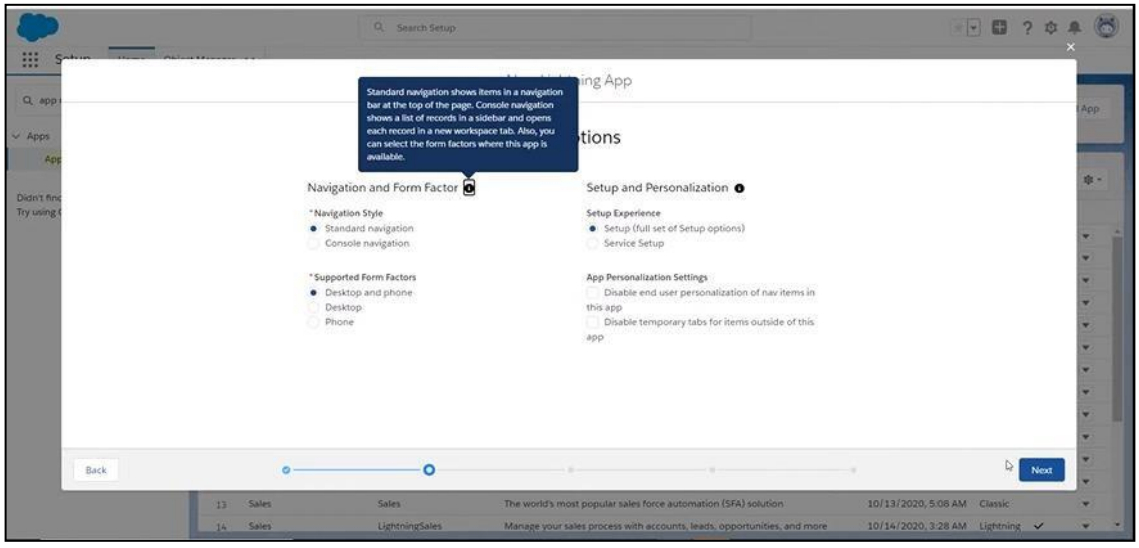
Step 9:

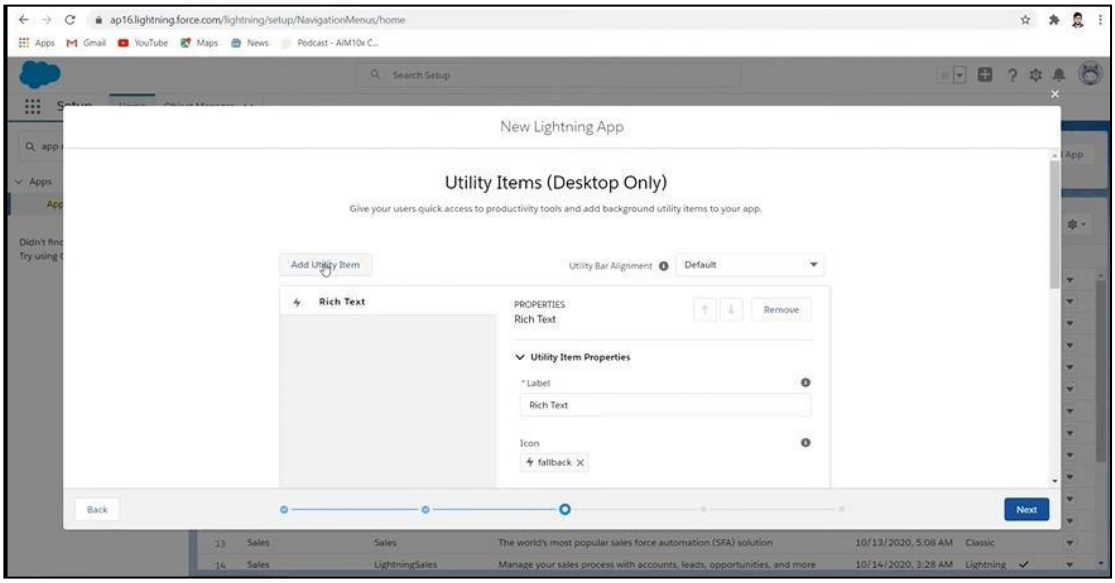
There are many ready app is available with two type (classic and Lighting).
But we create new app click the new app (classic and Lighting).

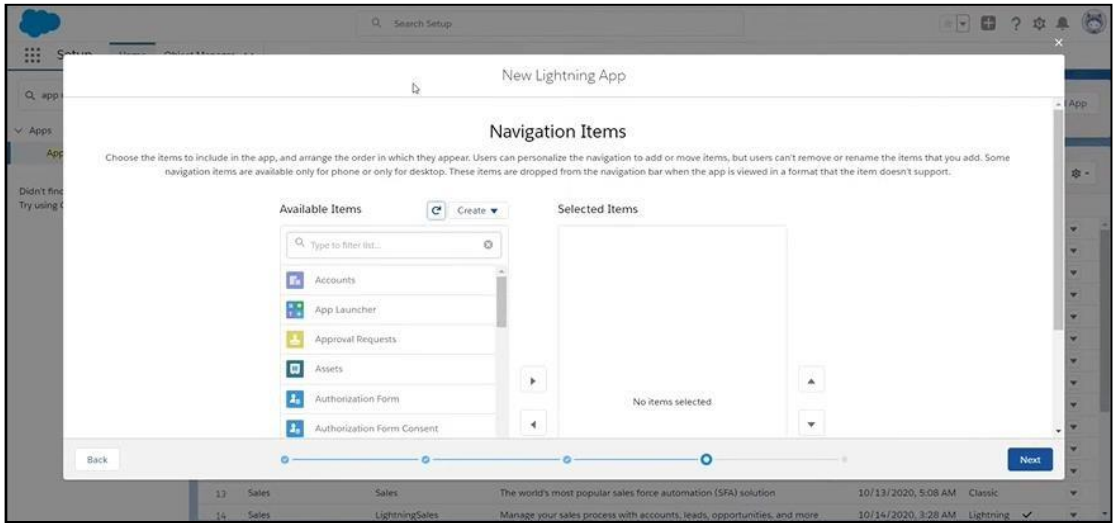


And fill all app properties and require data.


Home | Salesforce
App Manager | Salesforce
ap16.lightning.force.com/lightning/setup/NavigationMenus/home
Search Setup
New Lightning App
App Details & Branding
Give your Lightning app a name and description. Upload an image and choose the highlight color for its navigation bar.
App Details
* App Name
LearnerView
* Developer Name
LearnerView
Description
This applicatiion is for insights wrt learner
App Branding
Image
Primary Color Hex Value
#0070D2
Clear
Org Theme Options
Use the app's image and color instead of the org's custom theme
Next
13 Sales Sales The world's most popular sales force automation (SFA) solution 10/13/2020, 5:08 AM Classic
14 Sales LightningSales Manage your sales process with accounts, leads, opportunities, and more 10/14/2020, 3:28 AM Lightning


Search Setup
Standard navigation shows items in a navigation bar at the top of the page. Console navigation shows a list of records in a sidebar and opens each record in a new workspace tab. Also, you can select the form factors where this app is available.
Navigation and Form Factor
* Navigation Style
Standard navigation
Console navigation
* Supported Form Factors
Desktop and phone
Desktop
Phone
Setup and Personalization
Setup Experience
Setup (full set of Setup options)
Service Setup
App Personalization Settings
Disable end user personalization of nav items in this app
Disable temporary tabs for items outside of this app
Back
Next
13 Sales Sales The world's most popular sales force automation (SFA) solution 10/13/2020, 5:08 AM Classic
14 Sales LightningSales Manage your sales process with accounts, leads, opportunities, and more 10/14/2020, 3:28 AM Lightning



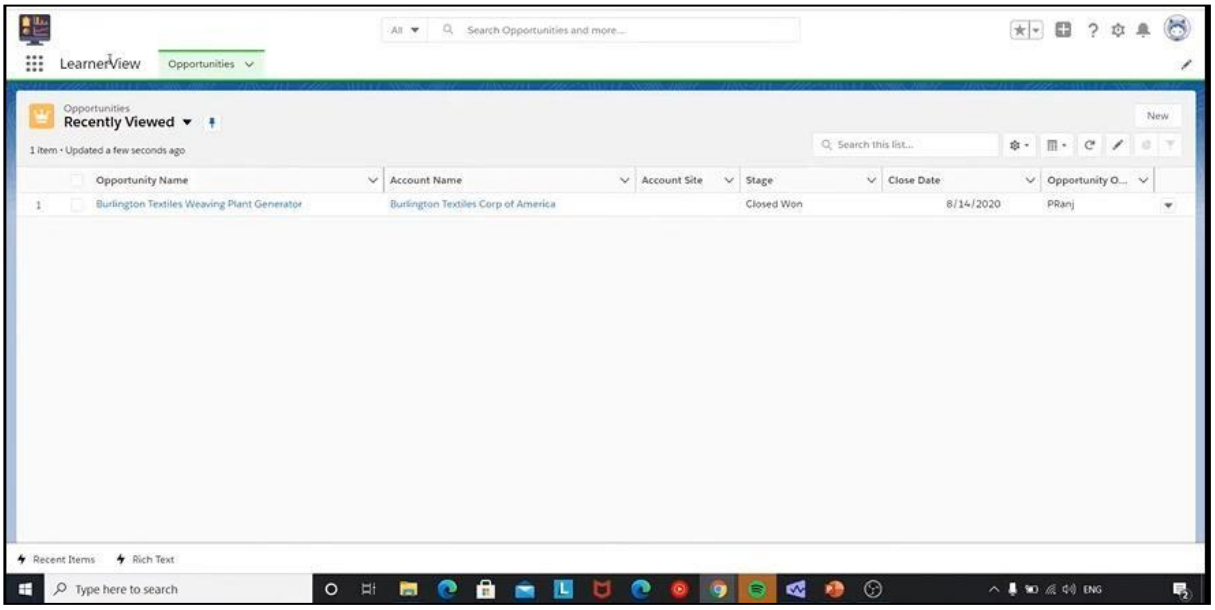


Step 10:

All the properties set; the app will be creating.

Go to app manager search the app name.

App will be created with properties and fields.



Step 11:

Set your all properties and develop your own app using custom feature.

Conclusion: We have studied and implemented own app on Salesforce.com

EXPERIMENT NO.:06

Title: Study and Implementation of any one cloud file system

Solution:

A file system in the cloud is a hierarchical storage system that provides shared access to file data. Users can create, delete, modify, read, and write files and can organize them logically in directory trees for intuitive access.

Amazon EFS:

Amazon Elastic File System (Amazon EFS) is a simple, serverless, set-and-forget, elastic file system. There is no minimum fee or setup charge. You pay only for the storage you use, for read and write access to data stored in Infrequent Access storage classes, and for any provisioned throughput.

Amazon EFS supports the Network File System version 4 (NFSv4.1 and NFSv4.0) protocol, so the applications and tools that you use today work seamlessly with Amazon EFS. Multiple compute instances, including Amazon EC2, Amazon ECS, and AWS Lambda, can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one compute instance or server.

With Amazon EFS, you pay only for the storage used by your file system and there is no minimum fee or setup cost. Amazon EFS offers a range of storage classes designed for different use cases. These include:

- **Standard storage classes** – EFS Standard and EFS Standard–Infrequent Access (Standard–IA), which offer multi-AZ resilience and the highest levels of durability and availability.

- **One Zone storage classes** – EFS One Zone and EFS One Zone–Infrequent Access (EFS One Zone–IA), which offer customers the choice of additional savings by choosing to save their data in a single AZ'.

The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS file systems using Standard storage classes store data and metadata across multiple Availability Zones in an AWS Region. EFS file systems can grow to petabyte scale, drive high levels of throughput, and allow massively parallel access from compute instances to yourdata.

Amazon EFS is designed to provide the throughput, IOPS, and low latency needed for a broad range of workloads. With Amazon EFS, you can choose from two performance modes and two throughput modes:

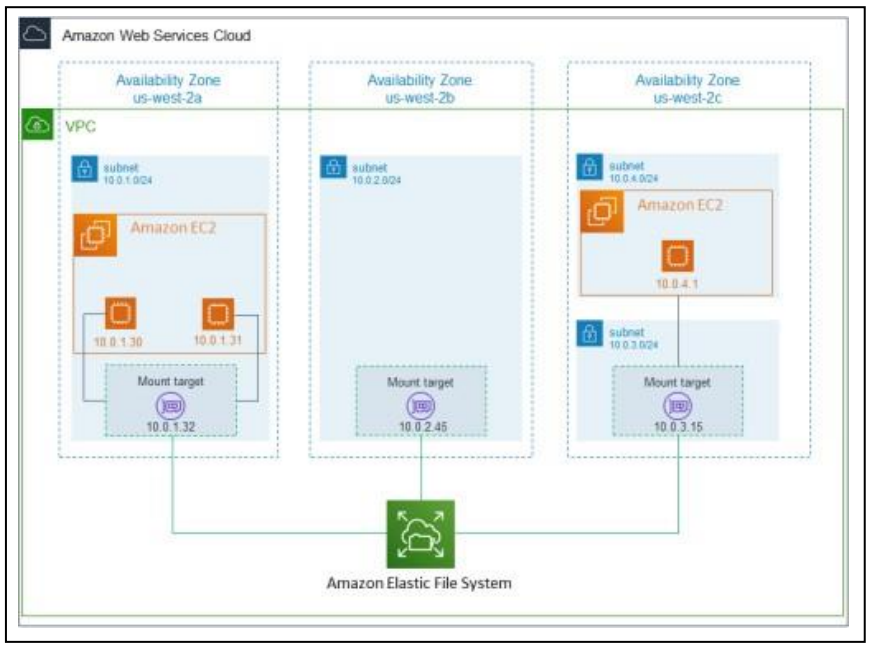
• The default General Purpose performance mode is ideal for latency-sensitive use cases, like web serving environments, content management systems, home directories, and general file serving. File systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations persecond with a tradeoff of slightly higher latencies for file metadata operations. For more information, see Performance.

• Using the default Bursting Throughput mode, throughput scales as your file system grows. Using Provisioned Throughput mode, you can specify the throughput of your file system independent of the amount of data stored. For more information, see Amazon EFS performance.

How Amazon EFS works with Amazon EC2 and other supported compute instances.

1. **Amazon EFS with Standard storage classes**

The following illustration shows multiple EC2 instances accessing an Amazon EFS file system that is configured with Standard storage classes from multiple Availability Zones in an AWS Region. In this illustration, the Amazon VirtualPrivate Cloud (VPC) has three Availability Zones. Because the file system uses Standard storage classes, a mount target was created in each Availability Zone. We recommend that you access the file system from a mount target within the same Availability Zone for performance and cost reasons.



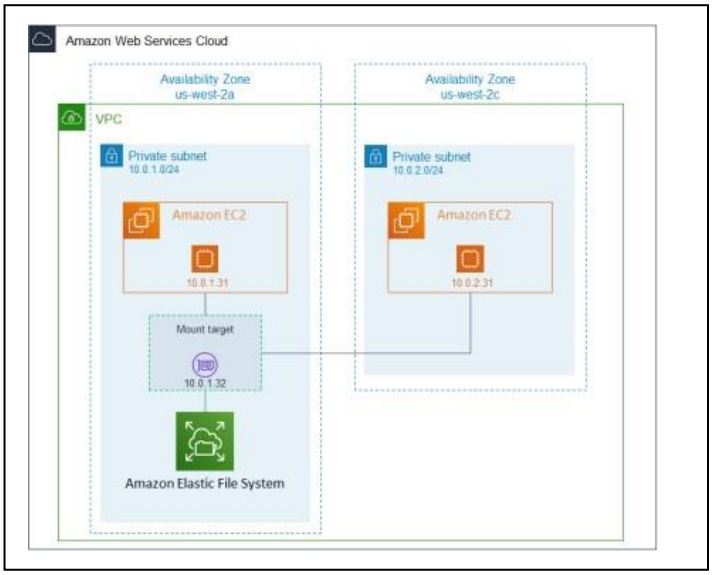
Creating this setup works as follows:

1. Create your Amazon EC2 resources and launch your Amazon EC2 instance. For more information on Amazon EC2, see Amazon EC2 - Virtual Server Hosting.
2. Choose Regional durability and availability when creating your Amazon EFS file system.
3. Connect to each of your Amazon EC2 instances, and mount the Amazon EFS file system.

2. Amazon EFS with One Zone storage classes

The following illustration shows multiple EC2 instances that are accessing an Amazon EFS file system. This file system is configured with One Zone storage from multiple Availability Zones in an AWS Region.

In this illustration, the VPC has two Availability Zones, each with one subnet. The file system uses One Zone storage classes, so it can only have a single mount target. For better performance and cost, we recommend that you access the file system froma mount target in the same Availability Zone as the EC2 instance that you're mounting it on.



In this example, the EC2 instance in the us-west-2c Availability Zone will pay EC2 data access charges for accessing a mount target in a different Availability Zone. Creating this setup works as follows:

1. Create your Amazon EC2 resources and launch your Amazon EC2 instance. For more information about Amazon EC2, see Amazon EC2.
2. Create your Amazon EFS file system with One Zone storage.
3. Connect to each of your Amazon EC2 instances, and mount the Amazon EFS file system using the same mount target for each instance.

How Amazon EFS works with AWS Direct Connect and AWS Managed VPN

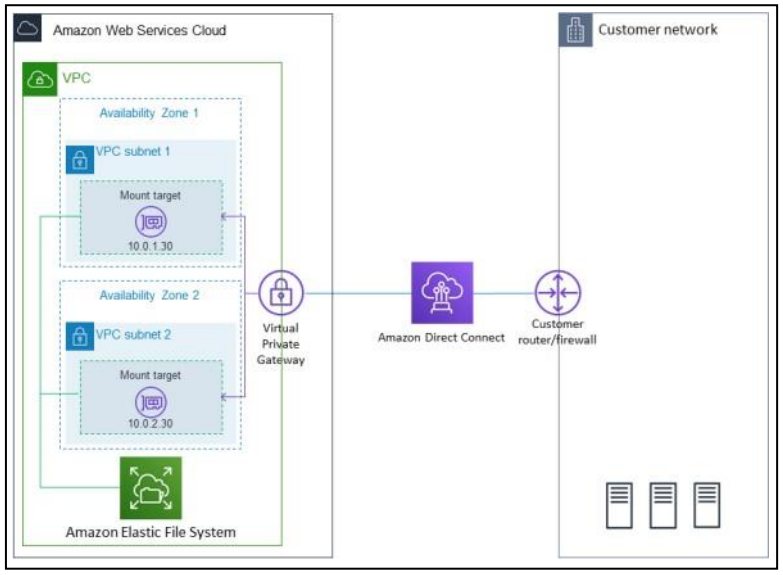
By using an Amazon EFS file system mounted on an on-premises server, you can migrate on-premises data into the AWS Cloud hosted in an Amazon EFS file system. You can also take advantage of bursting. In other words, you can move data from your on-premises servers into Amazon EFS and analyze it on a fleet of Amazon EC2 instances in your Amazon VPC. You can then store the results permanently in your file system or move the results back to your on-premises server.

Keep the following considerations in mind when using Amazon EFS with an on-premises server:

- Your on-premises server must have a Linux-based operating system. We recommend Linux kernel version 4.0 or later.
- For the sake of simplicity, we recommend mounting an Amazon EFS file system on an on-premises server using a mount target IP address instead of a DNS name.

There is no additional cost for on-premises access to your Amazon EFS file systems. You are charged for the AWS Direct Connect connection to your Amazon VPC. For more information, see AWS Direct Connect pricing.

The following illustration shows an example of how to access an Amazon EFS file system from on-premises (the on-premises servers have the file systems mounted).



You can use any mount target in your VPC if you can reach that mount target's subnet by using an AWS Direct Connect connection between your on-premises server and VPC. To access Amazon EFS from an on-premises server, add a rule to your mount target security

group to allow inbound traffic to the NFS port (2049) from your on-premises server.

To create a setup like this, you do the following:

1. Establish an AWS Direct Connect connection between your on-premises data center and your Amazon VPC. For more information on AWS Direct Connect, see AWS Direct Connect.
2. Create your Amazon EFS file system.
3. Mount the Amazon EFS file system on your on-premises server.

How Amazon EFS works with AWS Backup

For a comprehensive backup implementation for your file systems, you can use Amazon EFS with AWS Backup. AWS Backup is a fully managed backup service that makes it easy to centralize and automate data backup across AWS services in the cloud and on-premises. Using AWS Backup, you can centrally configure backup policies and monitor backup activityfor your AWS resources. AmazonEFS always prioritizes file system operations over backup operations. To learn more about backing up EFS file systems using AWS Backup, see Using AWS Backup to back up and restore Amazon EFS file systems.

Authentication and access control for EFS

You must have valid credentials to make Amazon EFS API requests, such as create a file system. In addition, you must also have permissions to create or access resources. By default, when you use the root account credentials of your AWS account you can create and access resources owned by that account.

However, we don't recommend using root account credentials. In addition, any AWS Identity and Access Management (IAM) users and roles that you create in your account must be granted permissions to create or access resources. For more information about permissions, see Identity and access management for Amazon EFS.

EFS lifecycle management

Amazon EFS lifecycle management automatically manages cost-effective file storage for your file systems. When enabled, lifecycle management migrates files that haven't been accessed for a set period of time to an infrequent access storage class, Standard-IA or One Zone-IA. You define that period of time by using a lifecycle policy. For more information, see Amazon EFS lifecycle management.

For Create Your Amazon EFS file system follows Steps

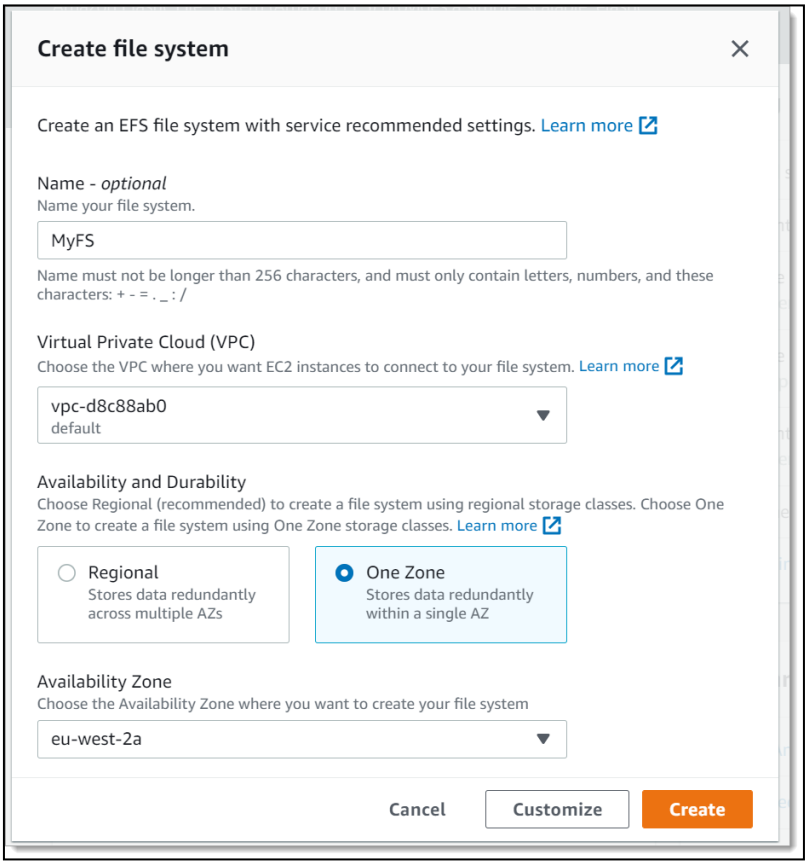
Step 1:

Open the Amazon EFS Management Console at

https://console.aws.amazon.com/efs/

Step 2:

Choose Create file system to open the Create file system dialog box



Step 3:

(Optional) Enter a **Name** for your file system.

Step 4:

For **Virtual Private Cloud (VPC)**, choose your VPC, or keep it set to your default VPC.

Step 5:

For **Availability and Durability**, choose one of the following:

- **Regional** to create a file system that uses Standard storage classes. Standard storage classes store file system data and metadata redundantly across all Availability Zones within an AWS Region. **Regional** offers the highest levels of availability and durability.
- **One Zone** to create a file system that uses One Zone storage classes. One Zone storage classes store file sytem data and metadata redundantly within a single Availability Zone which makes it less expensive than Standard storage classes.

Because EFS One Zone storage classes store data in a single AWS Availability Zone, data stored in these storage classes may be lost in the event of a disaster or other fault that affects all copies of the data within the Availability Zone, or in the event of Availability Zone destruction resulting from disasters, such as earthquakes and floods.

Step 6:

Choose **Create** to create a file system that uses the following service recommended settings:

- Automatic backups turned on, for more information, see Using AWS Backup to back up and restore Amazon EFS file systems.
- Mount targets – Amazon EFS creates mount targets with the following settings:
    1. For file systems that use Standard storage classes, a mount target is created in each Availability Zone in the AWS Region in which the file system is created. For file systems that use One Zone storage classes, a single mount target is created in the Availability Zone you specified.
    2. Located in the default subnets of the VPC you selected.
    3. Using the VPC's default security group – You can manage security groups after the file system is the created.

  For more information, see Managing file system network accessibility.
- General Purpose performance mode – For more information, see Performance modes.
- Bursting throughput mode – For more information, see Throughput modes.
- Encryption of data at rest enabled using your default key for Amazon EFS (aws/elasticfilesystem) – For more information, see Encrypting data at rest.
- Lifecycle Management – Amazon EFS creates the file system with the following lifecycle policies:
    I. **Transition into IA** set to **30 days since last access**
    II. **Transition out of IA** set to **On first access**

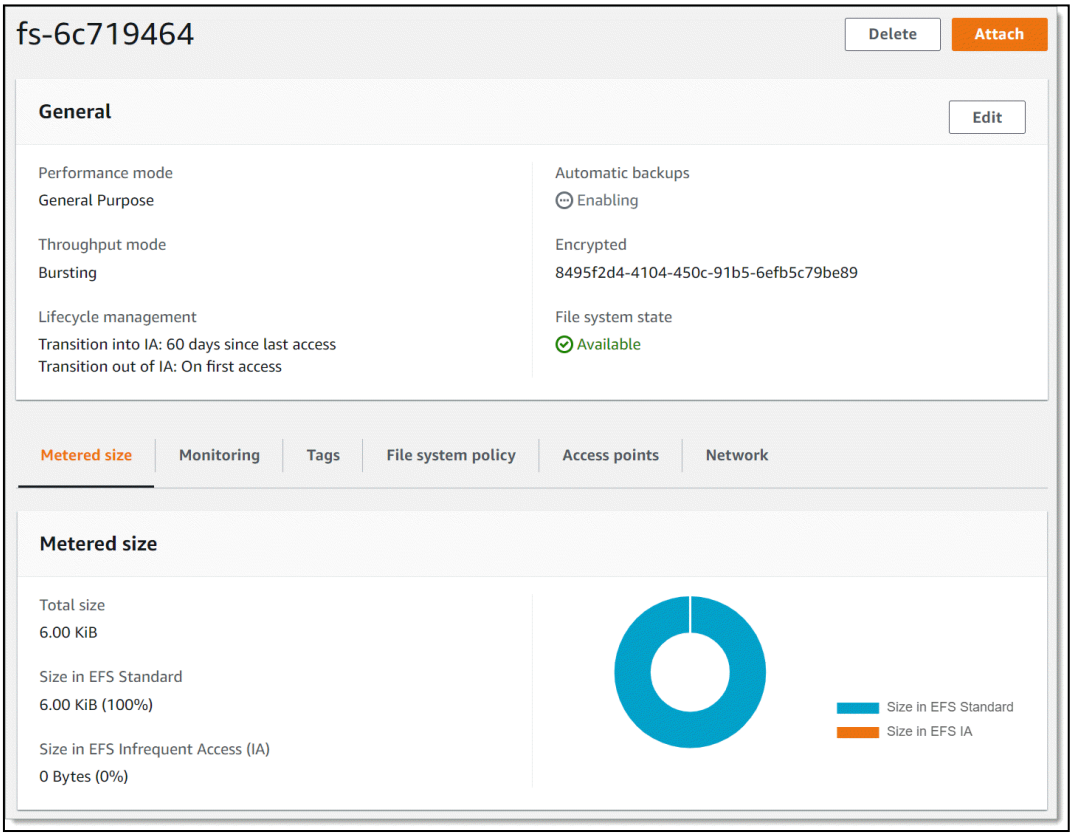
  For more information, see Amazon EFS lifecycle management.

After you create the file system, you can customize the file system's settings with the exception of availability and durability, encryption, and performance mode.

If you want to create a file system with a customized configuration, choose **Customize**. For more information about creating a file system with customizedsettings, see Creating a file system with custom settings using the Amazon EFS console.

Step 7:

The **File systems** page appears with a banner across the top showing the status of the file system you created. A link to access the file system details page appears in the banner when the file system becomes available.



For Create your EC2 resources and launch your EC2 instance follows Steps.

Before you can launch and connect to an Amazon EC2 instance, you need to create a key pair, unless you already have one. You can create a key pair using the Amazon EC2 console, and then you can launch your EC2 instance.

Step 1:

Open the Amazon EC2 console at
https://console.aws.amazon.com/ec2/

Step 2: Choose Launch Instance

Step 3:

Choose an Amazon Machine Image (AMI), find an Amazon Linux 2 AMI at the top of the list and choose **Select**.

Step 4:

Choose an Instance Type, choose **Next: Configure Instance Details**.

Step 5:

Configure Instance Details, provide the following information:

- Leave **Number of instances** at one.
- Leave **Purchasing option** at the default setting.
- For **Network**, choose the entry for the same VPC that you noted when you created your EFS file system in Step 1: Create your Amazon EFS file system.
- For **Subnet**, choose a default subnet in any Availability Zone.
- For **File systems**, make sure that the EFS file system that you created in Step 1: Create your Amazon EFS file system is selected. The path shown next to the file system ID is the mount point that the EC2 instance will use, which you can change.
- The **User data** automatically includes the commands for mounting your Amazon EFS file system.

Step 6:

Choose **Next: Add Storage**.

Step 7:

Choose **Next: Add Tags**.

Step 8:

Name your instance and choose **Next: Configure Security Group**.

Step 9:

In **Step 6: Configure Security Group**, set **Assign a security group** to **Select an existing security group**. Choose the default security group to make sure that it can access your EFS file system.

You can't access your EC2 instance by Secure Shell (SSH) using this security group. SSH access isn't required for this exercise. To add access by SSH later, you can edit the default security and add a rule to allow SSH. Or you can create a new security group that allows SSH. You can use the following settings to add SSH access:

- **Type:** SSH
- **Protocol:** TCP
- **Port Range:** 22
- **Source:** Anywhere 0.0.0.0/0

Step 10:

Choose **Review and Launch**.

Step 11:

Choose **Launch**.

Step 12:

Select the check box for the key pair that you created, and then choose **Launch Instances**.

Conclusion: Here we have studied and implemented Cloud File System- Amazon Elastic File System.

EXPERIMENT NO.:07

Title: Study and implementation of MongoDB cloud database

Solution:

MongoDB is an open-source database management system (DBMS) that uses a document-oriented database model. MongoDB is written in C++. MongoDB supports various forms of data. MongoDB stores data in flat files using their own binary storage objects. This meansthat data storage is very compact and efficient, perfect for high data volumes. MongoDB stores data in JSON-like documents, which makes the database very flexible and scalable.

MongoDB is a document-oriented database model. Each MongoDB database contains collections and which in turn contains documents. Each document can be different and depends on the varying number of fields. The model of each document will be different in size and content from each other. The data model features allow you to store arrays and complex structured in a hierarchical relationship.

Characteristics of MongoDB

- MongoDB is Schema-Less: MongoDB is a schema-less database which flexible than traditional database tables. It is written in language C++. It has no schema to have many fields, content, and size different from another document in the same collection.
- High Performance: MongoDB is an open-source database with high performance. MongoDB is a high availability and scalability database. It supports faster query response because of features like indexing and replication.
- MongoDB Indexing: Indexing is very important for improving the performances of search queries. MongoDB uses indexing of dataset to enhance query performances and searches. MongoDB indexing enhances the performance for the faster search query. Document in a MongoDB can be used for indexing using primary and secondary indices.
- File storage: MongoDB can be used as a file system with load balancing and data replication features over multiple machines for storing files.
- Replication: The feature of replication is to distribute data to multiple nodes. It can have primary nodes and secondary nodes to replicate data. Replication of data is done using master-slave architecture. MongoDB provides a replication feature by distributing data across multiple machines.
- Sharding: This process distributes data across multiple physical partitions called shards, due to sharding MongoDB automatic process load balancing. We use sharding in cases where we need to work on very larger datasets.

Advantage of MongoDB

- Flexible Document Schemas

MongoDB's document model allows virtually any kind of data structure to be modeled and manipulated easily. MongoDB's BSON data format, inspired by JSON, allows you to have objects in one collection have different sets of fields (say, a middle name on a user only when applicable, or region-specific information that only applies to some records).
MongoDB supports creating explicit schemas and validating data so it doesn't get out of control, but this flexibility is an incredible asset when handling real-world data, and handling changes in requirements or environment.

- Code-native data access

Most databases force you to use heavy wrappers, like ORMs (Object Relational Mappers), to get data into Object form for use in programs. MongoDB's decision to store and represent data in a document format means that you can access it from any language, in data structures that are native to that language (e.g. dictionaries in Python, associative arrays in JavaScript, Maps in Java, etc.).

- Change-friendly design

If you're used to having to bring down your site or application in order to change the structure of your data, you're in luck: MongoDB is designed for change.
We spend a lot of time and effort designing efficient processes, and learning from our mistakes, but typically the database is slowing the whole thing down. There's no downtime required to change schemas, and you can start writing new data to MongoDB at any time, without disrupting its operations.

- Powerful querying and analytics

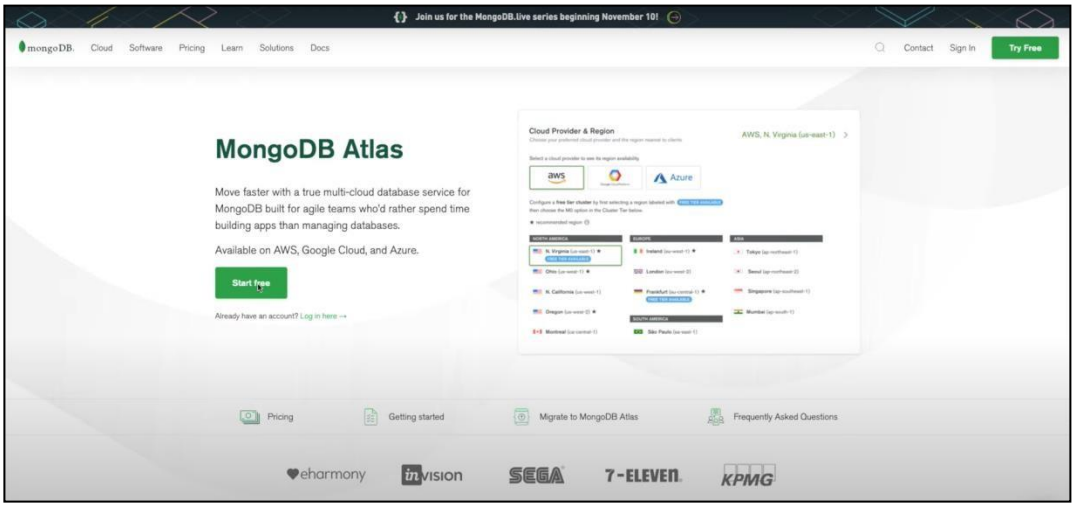
What good is a database if you can't find things inside it? MongoDB is designed to make data easy to access, and rarely to require joins or transactions, but when you need to do complex querying, it's more than up to the task.
The MongoDB Query Language (MQL) is a full-featured, powerful language that allows you to query deep into documents, and even perform complex analytics pipelines with just a few lines of JSON-like MQL.

- Easy horizontal scale-out

MongoDB is designed from the ground up to be a distributed database. Create clusters with real-time replication, and shard large or high-throughput collections across multiple clusters to sustain performance and scaler horizontally.
For implementation of MongoDB Database Cloud follows steps:

Step 1:
Open the Follows URL in Web browser:
https://www.mongodb.com/cloud/atlas

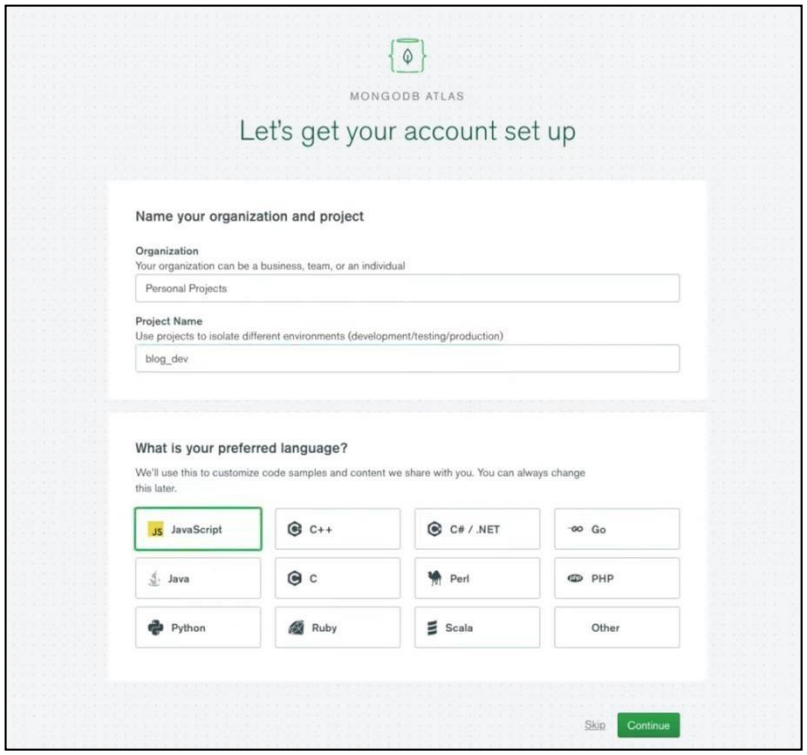
web page will be open click into the "Start Free" or "Try Free" Button.



Step 2:
Create your MongoDB Atlas Account.

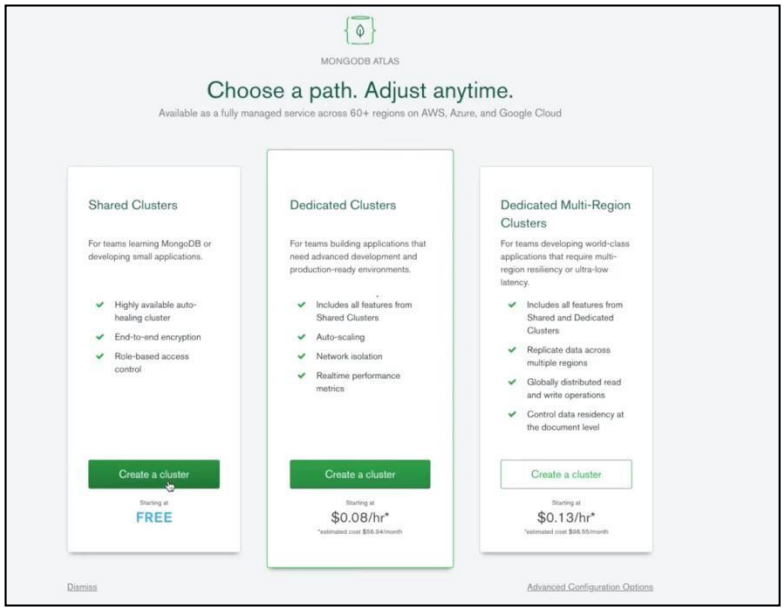
Step 3:
Enter Your

1. **Organization name.**
2. **Project name (for Create Project).**
3. **Select the Programming language you referred.**



Step 4:

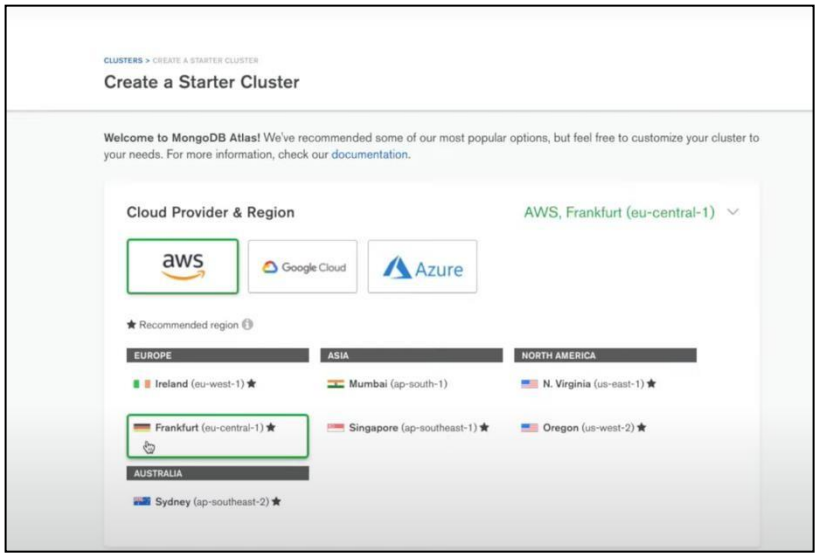
Choose your Database Cluster Plan , for Practices Purpose select Free Plan



Step 5:

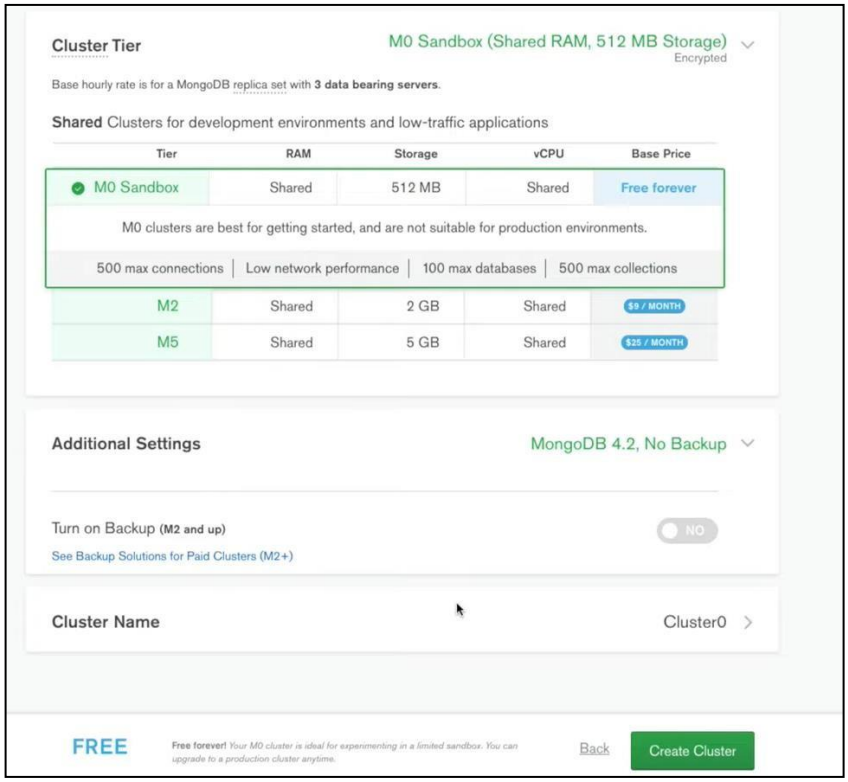
Create Starter Cluster

Select the Cloud Provider Company and Region

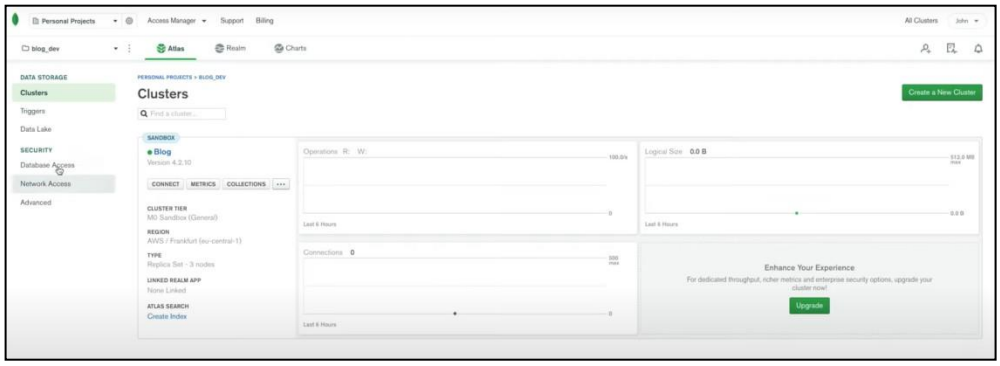


Step 6:

Click on Cluster Tier and Select the M0 Sandbox (Free Version)
And Change the Cluster Name Which name you need.



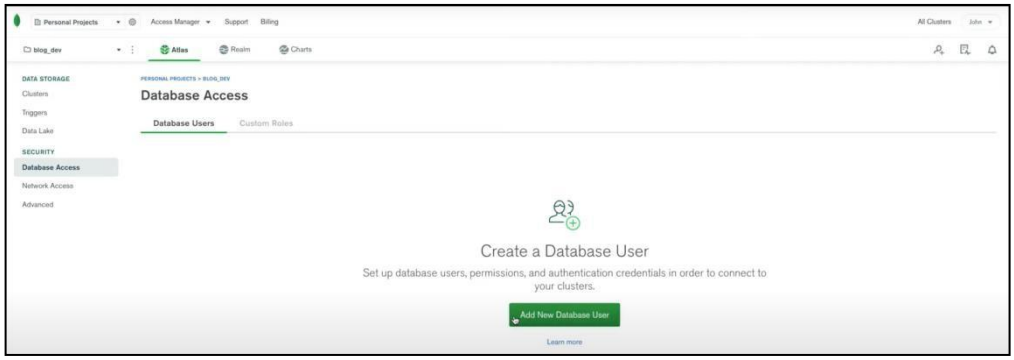
Step 7:



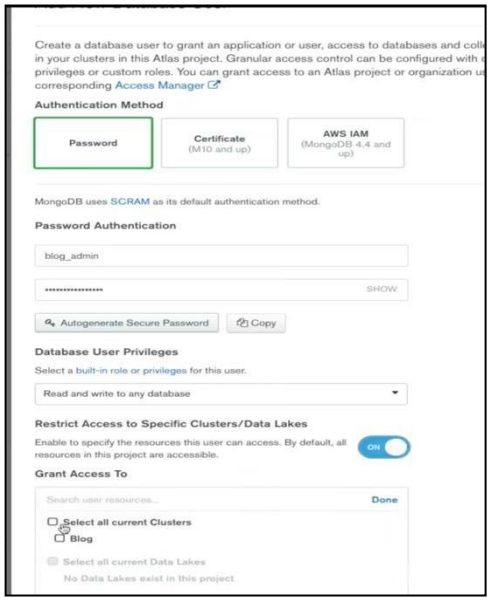
Go to the Left Side Panel And click the 'Database Access' Option.

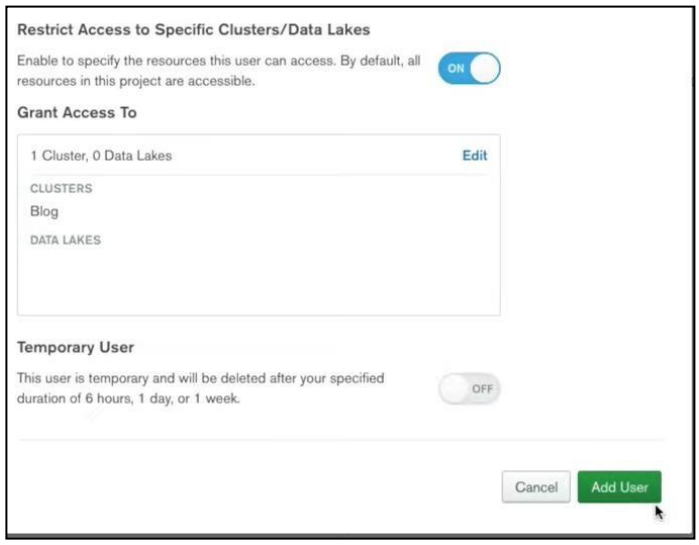
Step 8:

For Create the New Database User Click Add New Database User Button.



Fill the Follows Forms



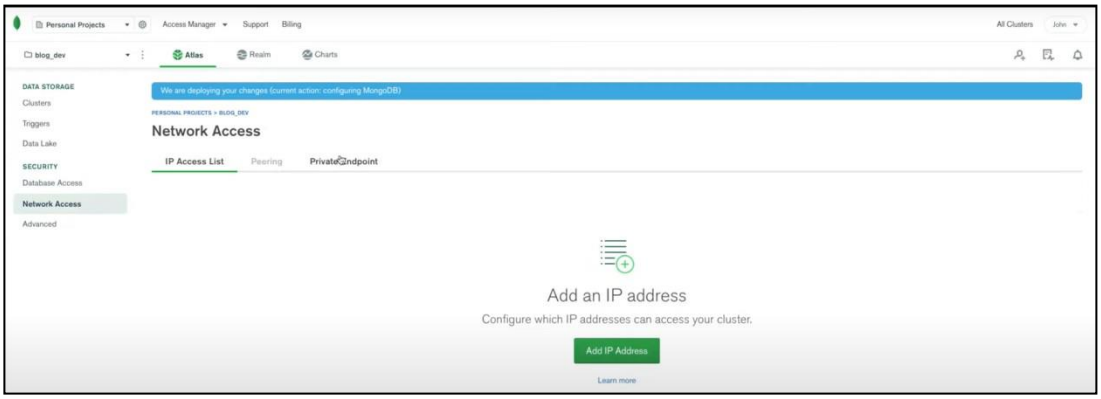


Step 9:
User Will be created

Your can Also Edit and Delete User Using Right Side Options.

Step 10:
Create Networks Access for Database

Go to left side panel click Networks Access options. And then Click the Add IP Address Button.



Step 10:

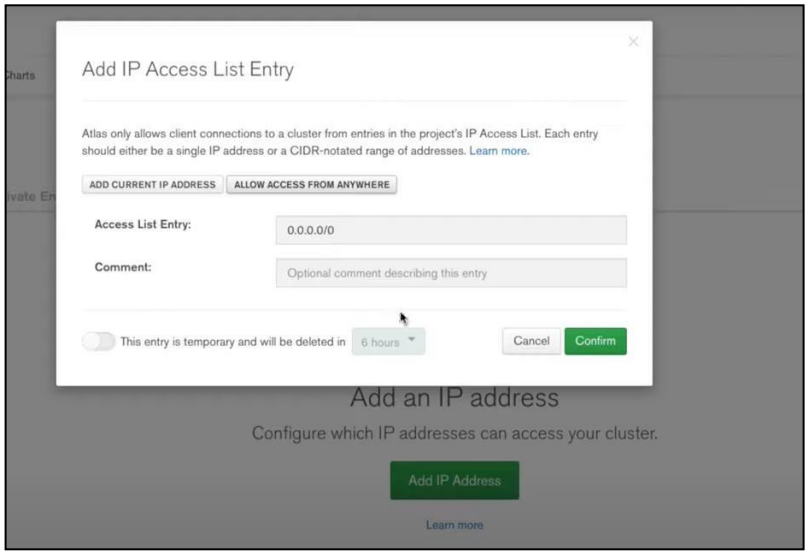
A new popup windows will be open. There are two options are available for IP address

1. Add Current IP Address

These options are more secure and database cluster share with authorize userusing generated IP address.

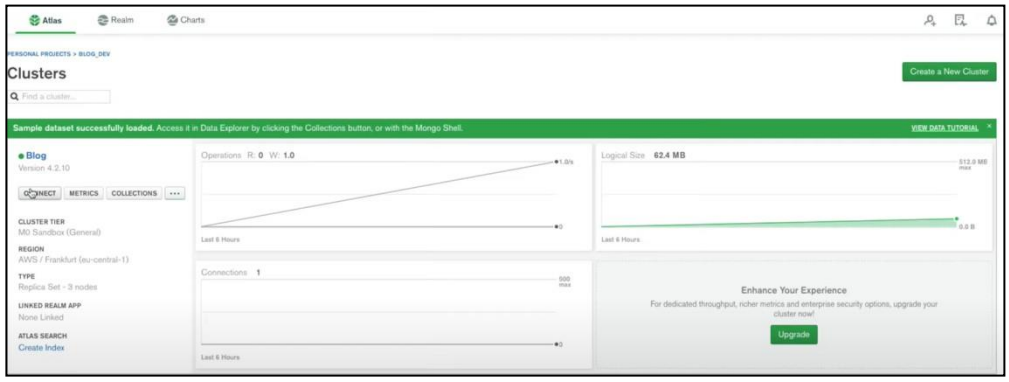
2. Allow Access from Anywhere

These options are not secure and any one can access and use the cluster using generated IP address.



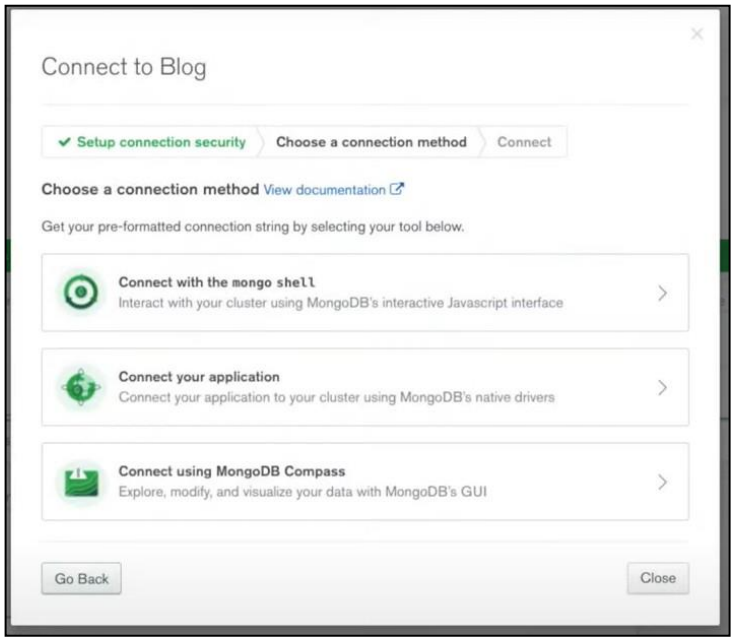
Step 11:

Connection the cluster with local device choose the connect button.



Step 12:

There are three options Will be Display.

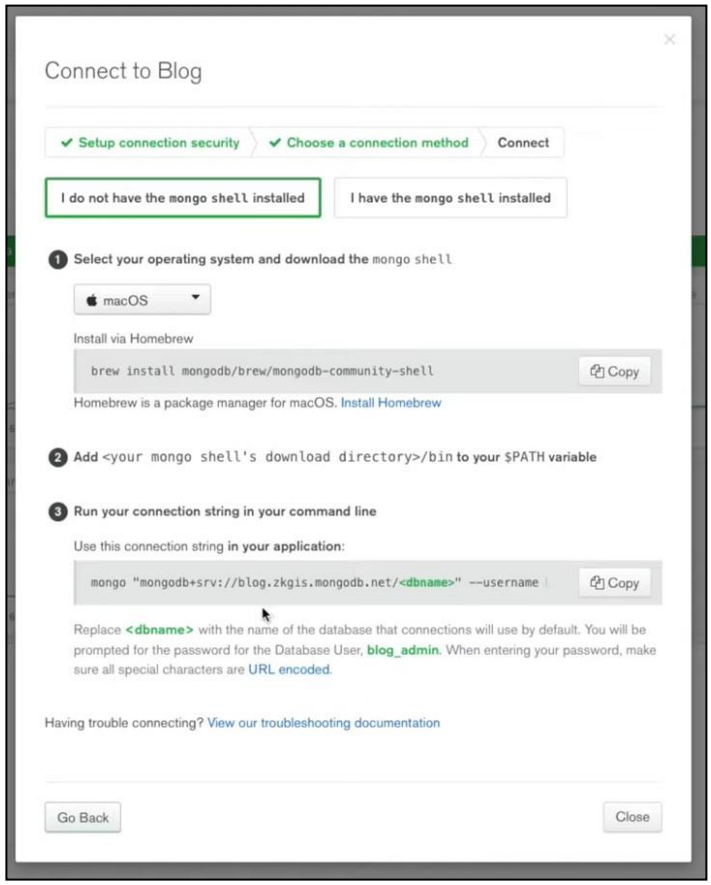


Step 13:

Select the options that help to easily.

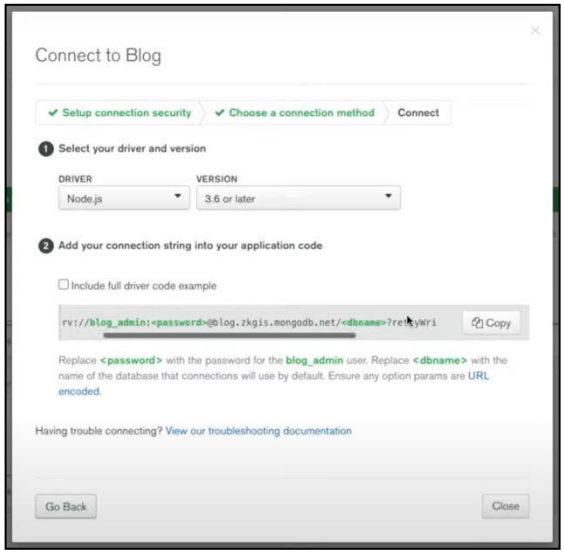
1. **Connect with the mongo shell**

Follows the Following Steps



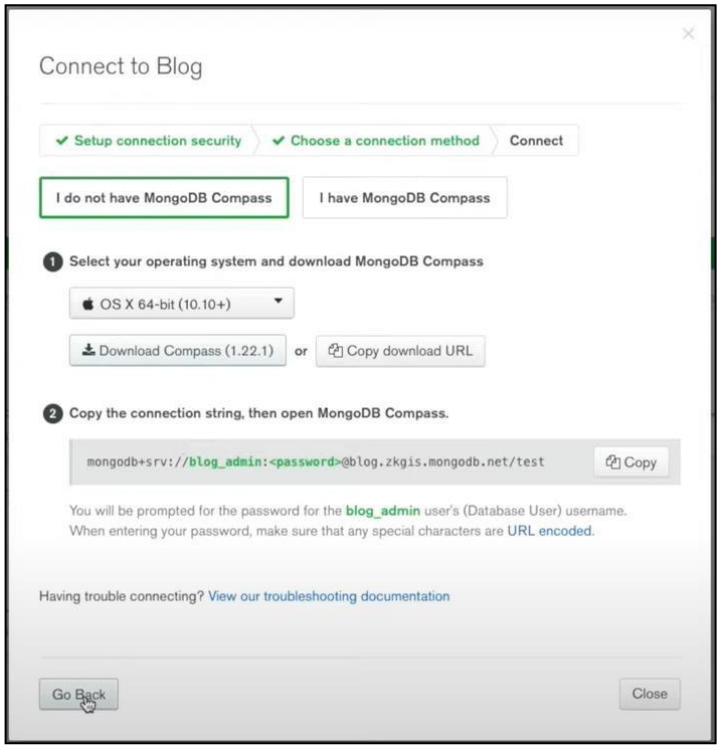
2. Connect your application

Follows the Following Steps



3. Connect using MongoDB Compass

Follows the Following Steps



Step 14:
Select the Code line into connect windows are in local project.

Conclusion: Hence, we have studied MangoDB Cloud Database and implemented local project on it.

EXPERIMENT NO.:08

Title: Implementation of Map-Reduce model

Solution:

MapReduce is a programming model and implementation for processing and producing large data sets on a cluster using a distributed, parallel method. A MapReduce programmer consists of a map technique for filtering and sorting (for example, sorting students by first name into queues, one queue for each name) and a reduction method for summarizing (such as counting the number of students in each queue, yielding name frequencies). The "MapReduce System" (also known as "infrastructure" or "framework") orchestrates the processing by marshalling distributed servers, running multiple tasks in parallel, managing all communications and data transfers between the various parts of the system, and ensuring redundancy and fault tolerance.

The model is a variation on the split-apply-combine data analysis technique. Although its purpose in the MapReduce framework is not the same as in their original versions, it is influenced by the map and reduce functions often employed in functional programming. The MapReduce framework's main contributions are not the map and reduce functions themselves (which, for example, are similar to the reduce and scatter operations in the 1995 Message Passing Interface standard), but the scalability and fault-tolerance achieved for a variety of applications by optimizing the execution engine. [As a result, a single-threaded MapReduce implementation is rarely quicker than a classical (non-MapReduce) version; any speedups are usually only found with multi-threaded MapReduce implementations on multi-processor hardware. Only when this model is used is it advantageous.

I. Key Feature of Map-Reduce:

1. Scalability

Apache Hadoop is a scalability-focused framework. This is due to its ability to store and distribute large amounts of data over a large number of servers. All of these servers are low-cost and can run in parallel. By adding servers to the cluster, we can simply grow the storage and compute power.

Hadoop MapReduce programming allows businesses to run programmes over a huge number of nodes, potentially involving thousands of gigabytes of data. Business enterprises can use Hadoop MapReduce programming to run applications across a large number of nodes. Thousands of gigabytes of data can be used in this process.

2. Flexibility

MapReduce programming allows businesses to access new data sources. It helps businesses to work with many forms of data. It enables businesses to access both structured and unstructured data, and to draw significant value from the many data sources.

Additionally, the MapReduce framework supports different languages and data from a variety of sources, including email, social media, and clickstream.

MapReduce works with data in simple key-value pairs, which means it can handle meta-data, pictures, and big files. As a result, MapReduce is more versatile than standard DBMS when it comes to dealing with data.

3. Security and Authentication

The MapReduce programming model makes use of the HBase and HDFS security platforms, which restrict access to the data to only authenticated users. As a result, it prevents unwanted access to system data and improves security.

4. Cost-effective solution

Hadoop's scalable architecture, together with the MapReduce programming framework, enables for the cost-effective storing and processing of massive data volumes.

5. Fast

Hadoop employs a distributed storage system known as the Hadoop Distributed File System, which is essentially a mapping system for locating data in a cluster.

Data processing techniques, such as MapReduce programming, are typically housed on the same servers as the data, allowing for speedier data processing. So, even if we're dealing with a lot of data,

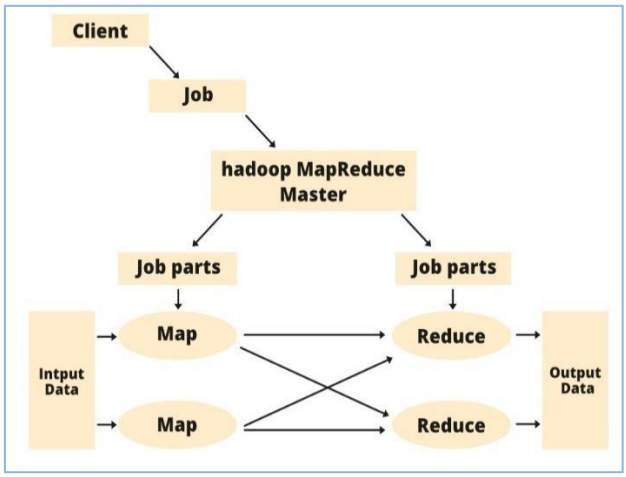
6. Simple model of programming

Among Hadoop MapReduce's many benefits, one of the most essential is that it is based on a simple programming model. Essentially, this enables programmers to create MapReduce systems that can easily and efficiently handle workloads.

MapReduce programmes can be developed in Java, which is a simple to learn language that is extensively used. As a result, anyone can learn how to develop MapReduce algorithms and use them to suit their data processing needs.

II. MapReduce Architecture:

MapReduce is a programming model for simultaneous processing of big data sets in a distributed environment. To obtain the final output, the data is separated first and then combined. MapReduce libraries are created in a variety of programming languages, each with its own set of optimizations. The goal of Hadoop's MapReduce is to map each job and then reduce it to equivalent tasks in order to eliminate overhead on the cluster network and reduce processing power. The MapReduce work is split into two parts: the Map Phase andthe Reduce Phase.



MapReduce Architecture Components:

1. Client: The MapReduce client is the one who submits the Job for processing to MapReduce. There may be several clients accessible that send jobs to the Hadoop MapReduce Manager on a regular basis.

2. Job: The MapReduce Job is the client's actual work, which is made up of many smaller tasks that the client wants to process or execute.

3. Hadoop MapReduce Master: This component distributes a single job into many segments.

4. Job-Parts: The tasks or sub-jobs that are created when the primary job is divided. The final product is the outcome of combining all of the job-parts.

5. Input Data: The data set that will be processed by MapReduce.

6. Data for Output:After the processing, the final output is acquired.

III. Example of Map-Reduce:

Amazon Elastic MapReduce (EMR)

Amazon Elastic MapReduce is a web service that provides a managed framework for easily, cost-effectively, and securely running data processing frameworks including Apache Hadoop, Apache Spark, and Presto. It's utilised for a variety of things, including data analysis, web indexing, data warehousing, financial analysis, scientific simulation, and more.

Amazon Elastic MapReduce is used by 1,929 businesses. The majority of organisations that use Amazon Elastic MapReduce are in the Computer Software industry and are based in the United States. Companies with 50-200 people and a revenue of more than $1 billion are the most likely to adopt Amazon Elastic MapReduce. Our Amazon Elastic MapReduce utilisation statistics spans five years and seven months.

IV. Which company use the Amazon Elastic MapReduce

Company	Website	Country
UnitedHealth Group Inc	unitedhealthgroup.com	United States
Lorven Technologies	lorventech.com	United States
Judo Bank	judo.com	Australia
Hotstar	hotstar.com	India
Policy Bazaar	policybazaar.com	India

V. Implementation of the Amazon Map-Reduce:

Step I:

Sign in to AWS account and select Amazon EMR on management console.

Step II:

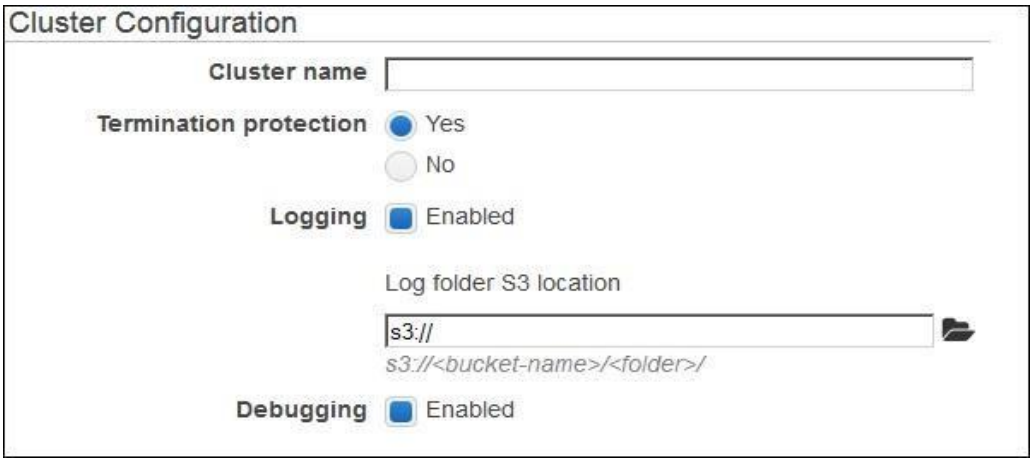
Create Amazon S3 bucket for cluster logs & output data. (Procedure is explained in detail in Amazon S3 section).

Step III: Launch Amazon EMR cluster.

Following are the steps to create cluster and launch it to EMR.

- Use this link to open Amazon EMR console https://console.aws.amazon.com/elasticmapreduce/home

– Select create cluster and provide the required details on Cluster Configuration page.



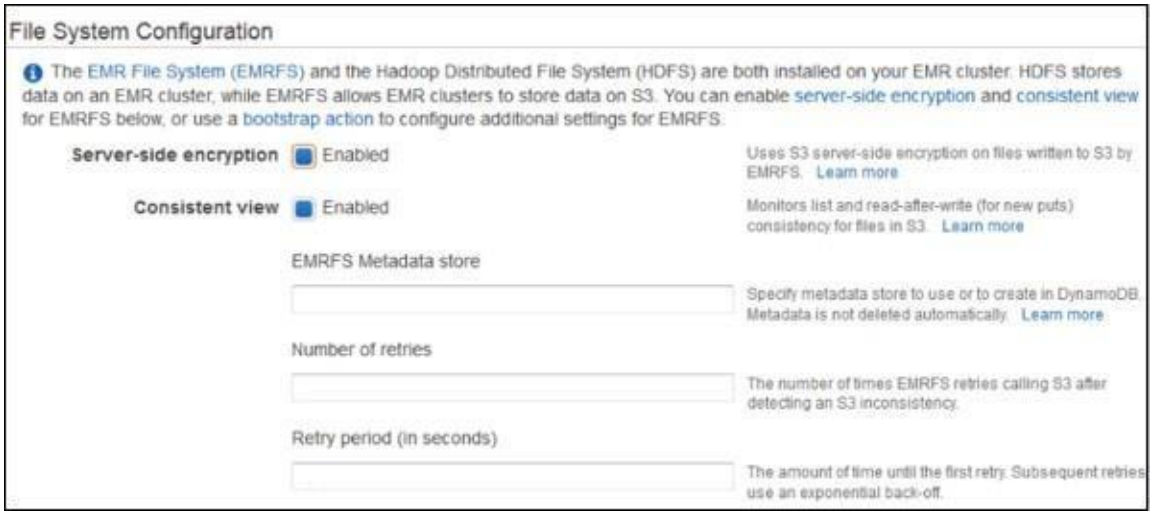
Step IV:

– Leave the Tags section options as default and proceed.

– On the Software configuration section, level the options as default.

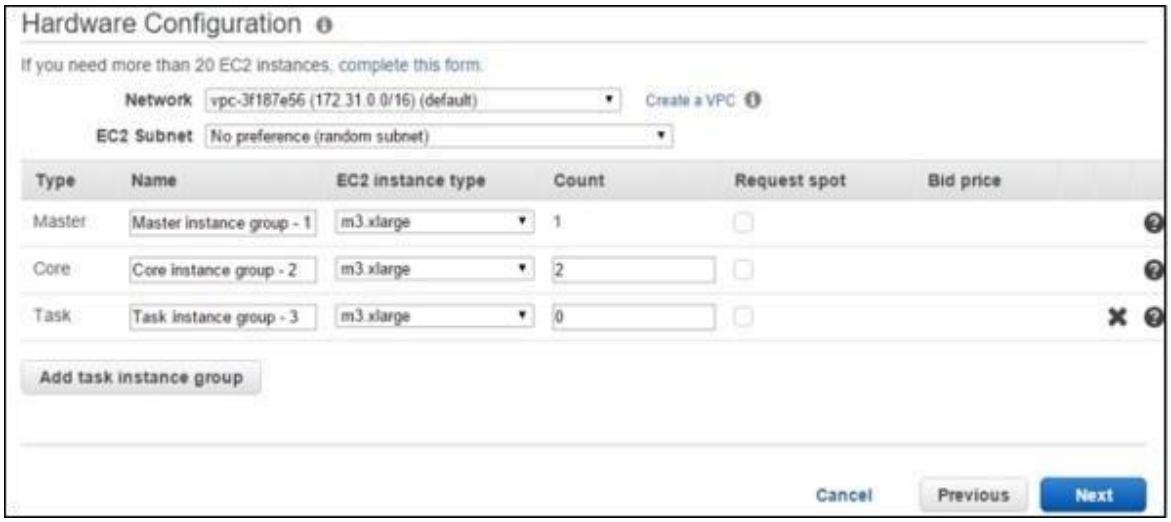
Step V:

On the File System Configuration section, leave the options for EMRFS as set by default. EMRFS is an implementation of HDFS, it allows Amazon EMR clusters to store data on Amazon S3.



Step VI:

On the Hardware Configuration section, select m3.xlarge in EC2 instance type field and leave other settings as default. Click the Next button.



Step VII:

- On the Security and Access section, for EC2 key pair, select the pair from the list in EC2 key pair field and leave the other settings as default.
- On Bootstrap Actions section, leave the fields as set by default and click the Add button. Bootstrap actions are scripts that are executed during the setup before Hadoop starts on every cluster node.

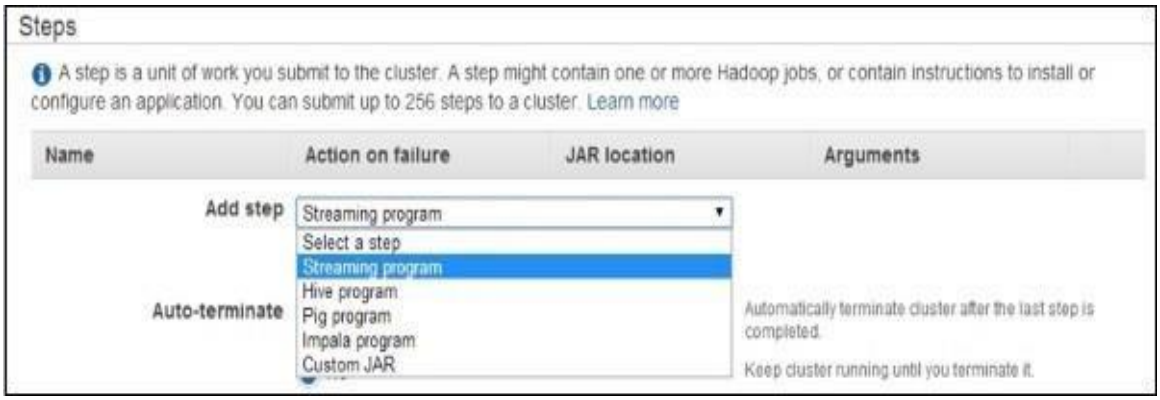
Step VIII:

- On the Steps section, leave the settings as default and proceed.
- Click the Create Cluster button and the Cluster Details page opens. This is where we should run the Hive script as a cluster step and use the Hue web interface to query the data.

Step IX:

Run the Hive script using the following steps.

- Open the Amazon EMR console and select the desired cluster.
- Move to the Steps section and expand it. Then click the Add step button.
- The Add Step dialog box opens. Fill the required fields, then click the Add button.



Step X:

To view the output of Hive script, use the following steps −

- Open the Amazon S3 console and select S3 bucket used for the output data.
- Select the output folder.
- The query writes the results into a separate folder. Select os_requests.
- The output is stored in a text file. This file can be downloaded.

Conclusion: Thus, we have implemented Map-Reduce model.

EXPERIMENT NO.:09

Title: Case study on any one Cloud Monitoring tool

Theory:

Amazon Cloud Watch monitors your AWS cloud environment, allowing you to collect metrics about all of the resources and apps that your organization uses in the cloud. You can monitor apps that run on AWS with Amazon EC2, in containers or server less.This service gives you system-wide visibility into your cloud environment's performance, usage and operational health. Your customized Cloud Watch homepage delivers detailed metrics about each of the AWS services you use. For more granular monitoring, you can create specific dashboards that go into more detail about custom apps, your usage and more.

Top use cases for monitoring with Amazon Cloud-Watch include:

- Infrastructure monitoring and troubleshooting
- Proactive resource monitoring
- Application monitoring
- Mean-time-to-resolution improvement
- Log analytics

You can access Amazon Cloud Watch through the Cloud Watch API, a command-line interface, AWS SDKs, and the AWS Management Console.

Working Of Amazon Cloud Watch

Monitoring with Amazon Cloud Watch allows you to drill down into your cloud resources and apps to identify anomalies and the root-cause of these performance issues.

This service surfaces insights into how to keep your AWS cloud environment running smoothly. It collects and delivers a unified view of logs, events and related metrics to give you a full view of your AWS cloud performance. By visualizing this side-by-side information, you can determine what is working and what isn't within your environment.

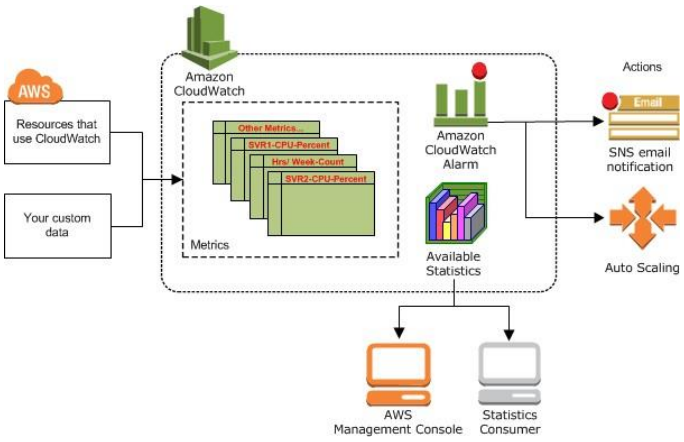


Fig 1.Working of Amazon Cloud Watch

Need of Cloud Watch

There are distinct benefits to keeping track of your AWS cloud performance by monitoring with Amazon Cloud Watch. First, you are able to observe your AWS cloud environment's apps and infrastructure across a single, easy-to-use platform. This breaks down data silos to give you essential, system-wide visibility. Second, Cloud Watch provides the easiest way to collect both your AWS and on-premise metrics because it natively integrates with more than 70 AWS sources, including Amazon S3, AWS Lambda, Amazon EC2 and more. It also works with hybrid-cloud architecture to deliver an entire snapshot of your environment. Third, monitoring with Amazon Cloud Watch means you get operational visibility and insight at your fingertips thanks to a unified, granular, real-time view of all of your services, resources and apps. Having all of this easily accessible, visible information means you can use your logs to derive actionable insights that will help you optimize your resources and improve operational performance across your cloud. As AWS puts it, Amazon Cloud Watch lets you Collect, Monitor, Analyze and Act by giving you all of the key data you need to make sure your AWS cloud environment is running as intended and remains within your usage parameters.

Benefits

Use a single platform for observability

Modern applications, such as those running on microservices architectures, generate large volumes of data in the form of metrics, logs, and events. Amazon Cloud Watch allows you to collect, access, and correlate this data on a single platform from across all your AWS resources, applications, and services running on AWS and on-premises, helping you break down data silos to gain system-wide visibility and quickly resolve issues.

Collect metrics on AWS and on premises

Monitoring your AWS resources and applications is easy with Cloud Watch. It natively integrates

with more than 70 AWS services, such as Amazon EC2, Amazon Dynamo DB, Amazon S3, Amazon ECS, Amazon EKS, and AWS Lambda. It automatically publishes detailed one-minute metrics and custom metrics with up to one-second granularity so you can dive deep into your logs for additional context. You can also use CloudWatch in hybrid environments by using the CloudWatch Agent or API to monitor your on-premises resources.

Improve operational performance and resource optimization

Set alarms and automate actions based on predefined thresholds or on machine learning (ML) algorithms that identify anomalous behavior in your metrics. For example, you can start Amazon EC2 Auto Scaling automatically or stop an instance to reduce billing overages. You can also use CloudWatch Events for server less to trigger workflows with services like AWS Lambda, Amazon SNS, and AWS Cloud Formation.

Get operational visibility and insight

To optimize performance and resource utilization, you need a unified operational view, real-time granular data, and historical reference. CloudWatch provides automatic dashboards, data with one-second granularity, and up to 15 months of metrics storage and retention. You can also perform metric math on your data to derive operational and utilization insights; for example, you can aggregate usage across an entire fleet of EC2 instances.

Derive actionable insights from logs

Explore, analyze, and visualize your logs so you can troubleshoot operational problems with ease. With CloudWatch Logs Insights, you pay only for the queries you run. It scales with your log volumeand query complexity, giving you answers in seconds. In addition, you can publish log-based metrics,create alarms, and correlate logs and metrics together in CloudWatch Dashboards for complete operational visibility.

Application

CloudWatch Logs:

This service enables users to collect and store logs for vended services for customers, logs for specific AWS services such as AWS Cloud Trail, AWS Lambda, Amazon API Gateway, Amazon Simple Notification Service, or for proprietary applications and on-premises resources. CloudWatch Logs Insights can provide quick queries and visualization of log data.

Metrics collection:

Users can collect default metrics from more than 70 distributed AWS applications and view them in one place. They also can collect metrics and customize logs from their own applicationsor on-premises resources.

Container Insights:

This feature collects, aggregates and monitors metrics and logs for containerized applications and microservices. It can also troubleshoot Amazon Elastic Kubernetes Service and Amazon Container Orchestration Service.

CloudWatch Lambda Insights:

This service collects, aggregates and monitors AWS Lambda logs and performance metrics from each container, including CPU, memory and disk information.

Contributor Insights.:

This feature provides a view of the top contributors influencing system performance, such as API calls, applications or customer accounts.

Unified view. This feature enables users to create dashboard views for selected applications, graphs and other visualized cloud data.

Composite alarms:

This function unifies alarms for different issues affected by the same application into a single notification. This can help root-cause diagnosis.

High resolution alarms. Users can set thresholds for specific metrics that trigger alarm actions, such as shutting down unused instances.

Correlation:

CloudWatch can correlate specific patterns in logs with metrics to diagnose a root cause.

Application Insights for .NET and SQL Server.

This feature provides easy monitoring for .NET and SQL Server applications, with automated dashboards and smart metrics.

Anomaly Detection:

Machine learning algorithms can detect abnormal activity in AWS systems.

ServiceLens:

This service monitors the performance, health and availability of applications and dependencies to reduce bottlenecks, recognize affected users and diagnose root causes.

Synthetics.

This facility monitors application endpoints and alerts the user to errors and abnormal infrastructure issues.

Metric Streams.:

This feature enables users to create near real-time metric streams to other applications, such as Amazon S3, or share them with third-party service providers.

Auto Scaling.

This feature automates capacity and resource planning.

CloudWatch Events. This service provides a near real-time stream of system events and automates responses to operational changes.

Log analytics.

Advanced analytics are available for the information in CloudWatch Logs, without provisioning additional servers or the need for extra software. Queries can be exported to dashboards.

Integration with AWS Identity and Access Management.

This facility provides a management console to control which users and applications have access to CloudWatch data and resources.

Cloud Watch VS Cloud Trail

CloudWatch and CloudTrail are both monitoring services for AWS resources and applications.

AWS CloudWatch is a service that monitors system performance for AWS applications and resources, and AWS CloudTrail is a web service that monitors the activity within the AWS environment through tracking API calls.CloudTrail provides a detailed log of all actions in the AWS system, and helps users track user activity and changes, monitoring the trail of activity, hence the name. AWS CloudTrail provides information on the who, what, where and when of activity in the AWS account and environment.

Challenges of Cloud Watch

- costs more than most third-party monitoring and log tools;
- many standard AWS metrics cannot be seen in units smaller than one-minute intervals;
- advanced integration is mostly limited to AWS resources; and
- more advanced use of CloudWatch can have a high learning curve.

Conclusion:

CloudWatch enables you to monitor your complete stack (applications, infrastructure, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.

EXPERIMENT NO.:10

Title: Case study on any one Cloud Security tool

Your on-campus or cloud-hosted security solutions are encapsulated by Cloud Access Security Broker (CASB) products. CASBs are stop-gap and gateway solutions that connect consumers to cloud service providers. They can be physical or digital. This includes IaaS, PaaS, and certain (but not all) SaaS setups.

What are Cloud Access Security Broker (CASB) Tools and How Do They Work?

Your on-campus or cloud-hosted security solutions are encapsulated by Cloud Access Security Broker (CASB) products. CASBs are stop-gap and gateway solutions that connect consumers to cloud service providers. They can be physical or digital.

This includes IaaS, PaaS, and certain (but not all) SaaS setups. In a nutshell, CASB closes security gaps by allowing enterprises to extend their security policies outside the campus to the cloud, as well as develop cloud-only security controls.

Amazon Security Tool:

With the most versatile and secure cloud computing environment available today, AWS gives you the power and trust you need to operate your business safely. As an AWS client, you'll have access to AWS data centers and a network that's designed to keep your data, identities, apps, and devices safe. With AWS' broad services and features, you can increase your capacity to satisfy fundamental security and compliance needs such as data location, protection, and confidentiality.
You may use AWS to automate manual security processes so you can focus on growing and improving your company. Furthermore, you only pay for the services that you utilize. AWS is the only commercial cloud whose service offerings and accompanying supply chain have been verified and accepted as secure enough for top-secret workloads, which benefits all customers.

Benefits of Amazon Security:

- Scale Securely with Superior Visibility and Control.
- Automate and Reduce Risk with Deeply Integrated Services.
- Build with the Highest Standards for Privacy and Data Security.
- Largest Ecosystem of Security Partners and Solutions.
- Inherit the Most Comprehensive Security and Compliance Controls.

Strategic Defense :

AWS is built to assist you in constructing secure, high-performing, robust, and efficient infrastructure for your applications. Our infrastructure is monitored by world-class security professionals who also design and manage our comprehensive range of innovative security services, which may help you satisfy your own security and regulatory needs more easily. Our security services and solutions are designed to provide the following important strategic benefits that are crucial to assisting you in achieving your organization's ideal security posture:

1. **Prevent :**For a seamless and planned AWS adoption strategy, define user rights and identities, infrastructure protection, and data protection procedures.
2. **Detect :**With logging and monitoring services, you may get a better understanding of your company's security posture. Incorporate this data into a scalable event management, testing, and auditing platform.
3. **Respond :**Automated incident response and recovery to enable security teams move their primary focus from reaction to root cause analysis.
4. **Repair :**Make use of event. driven automation to swiftly remediate and protect your AWS environment.

Partners of Amazon Security Tool :

Hundreds of industry-leading security solutions are available from APN Partners to help businesses enhance their security and compliance. Our partners can develop world-class products for clients because to the cloud's scalability, visibility, and affordability. Learn about AWS Partner Competency Program-prequalified products and solutions that may help you with infrastructure security, policy management, identity management, security monitoring, vulnerability management, data protection, and consulting services.

These solutions work in tandem with other AWS services to help you build a more complete security architecture and provide a more consistent experience across cloud and on-premises settings. Also, check out our Security Solutions in AWS Marketplace for a wide range of security solutions from hundreds of independent software suppliers.

Conclusion: Hence we have studied Cloud Security Tool- Amazon Security Tool