

Practical No: 1

Date:

Aim: To study cloud architecture and cloud computing model.

Hardware/software Required: Ubuntu operating system, Internet

Theory:

Cloud computing enables companies to consume, compute resources as a utility - just like electricity - rather than having to build and maintain computing infrastructure - in-house. Cloud computing promises several attractive benefits for businesses and end users.

Three benefits of cloud computing include:

- ① Self-service provisioning: End users can spin up computing resources for almost any type of workload on demand.
- ② Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- ③ Pay per use: Computing resources are measured at a granular level, allowing users to pay only for resources and workloads they use.

Cloud computing services can be Private, Public or Hybrid. Private cloud services are delivered from a business data center to internal users.

Public cloud, a third party provider delivers cloud service over the Internet. These are sold on demand.

Hybrid cloud is combination of public cloud and on-premises private cloud - with orchestration and automation between two.

## Types of cloud computing:

- Infrastructure as Service (IaaS):

IaaS means you're buying access to raw computing hardware over the Net, such as servers or storage since you buy what you need and pay-as-you-go, this is often referred to as utility computing. Ordinary Web hosting is a simple example of IaaS.

- Software as a Service (SaaS): It means you use a complete application running on someone else's system. Web based email and Google Documents are perhaps the examples. Zoho is another well-known SaaS provider.

- Platform as Service (PaaS): It means, you develop applications using web based tools, so they run on systems software and hardware provided by another company. Google App Engine are examples of PaaS.

## Advantages of cloud computing:

The pros of cloud computing are obvious and compelling. If your business is selling books, or repairing shoes, cloud computing allows you to buy in only services you want, when you use them, cutting them in front capital costs of computers and peripherals. You can add extra services at a moment's notice as your business needs change. It is really quick and easy to add new application or services to your business without waiting for weeks/months.

### Disadvantages:

Instant convenience comes at a price. Instead of purchasing computer and software, cloud computing means you buy services so one-off, upfront capital costs become ongoing operating costs instead. That might work out much more expensive in long term.

### Conclusion:

Cloud computing enables a convenient and on demand network access to a wide range of resources. The different services and also the deployment models allow flexible service provider interaction with minimal human intervention. It saves costs but also can lead to risk issues and suspension of resources when in huge quantity.

Date:

Practical No: 2

Aim: Installation and configuration of Virtualization using KVM

Objectives:

Understand concepts of virtualization

Understand KVM architecture and its configuration

Hardware / software required: Ubuntu operating system, Open source software

Theory:

Virtualization is software that separates physical infrastructures to create various dedicated resources. It is a fundamental technology that powers cloud computing. The technology behind virtualization is known as a virtual machine monitor (VMM) or Virtual Manager, which separates compute environments from the actual physical infrastructure.

Virtualization makes servers, workstations, storage and other systems independent of physical hardware layer. This is done by installing a Hypervisor on top of the hardware layer, where the systems are then installed. There are three areas of IT where virtualization is making headways, network virtualization, storage virtualization and server virtualization.

Network virtualization is a method of combining available resources in network by splitting up the available bandwidth into channels. Storage virtualization is pooling of physical storage from multiple network SD into what appears to be single storage device. Server virtualization is masking of server resources, no; and identity of individual physical servers, processors, and operating from server users. It is to centralize administrative tasks while improving scalability and work loads.

## 1. Procedure:

Installation Steps :

1. sudo grep -c "svm\|vmx" /proc/cpuinfo
2. sudo apt-get install qemu-kvm libvirt-bin bridge-utils virt-manager
3. sudo adduser rait
4. sudo adduser rait  
libvird
5. virsh -c qemu:///system list

(Run following command after logging back in as rait and you should see an empty list of virtual machines. This indicates that everything is working correctly.)

6. virt-manager

(Open Virtual Machine Manager application and Create Virtual Machine )

## 7. Result:

### SNAPSHOTS

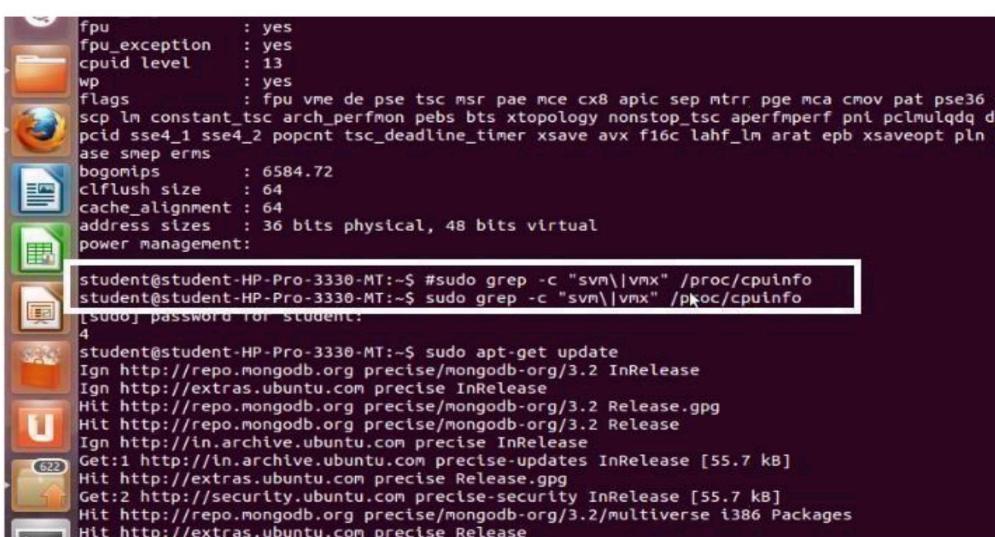
Step 1 : #sudo grep -c "svm\|vmx" /proc/cpuinfo



```
student@student-HP-Pro-3330-MT: ~
student@student-HP-Pro-3330-MT:~$ sudo grep -c "svm\|vmx" /proc/cpuinfo
student@student-HP-Pro-3330-MT:~$ clear

student@student-HP-Pro-3330-MT:~$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 38
stepping        : 9
microcode      : 0x19
cpu MHz        : 1600.000
cache size     : 3072 KB
physical id    : 0
siblings        : 4
core id        : 0
cpu cores      : 2
```

Step 2 : #sudo apt-get install qemu-kvm libvirt-bin bridge-utils virt-manager.

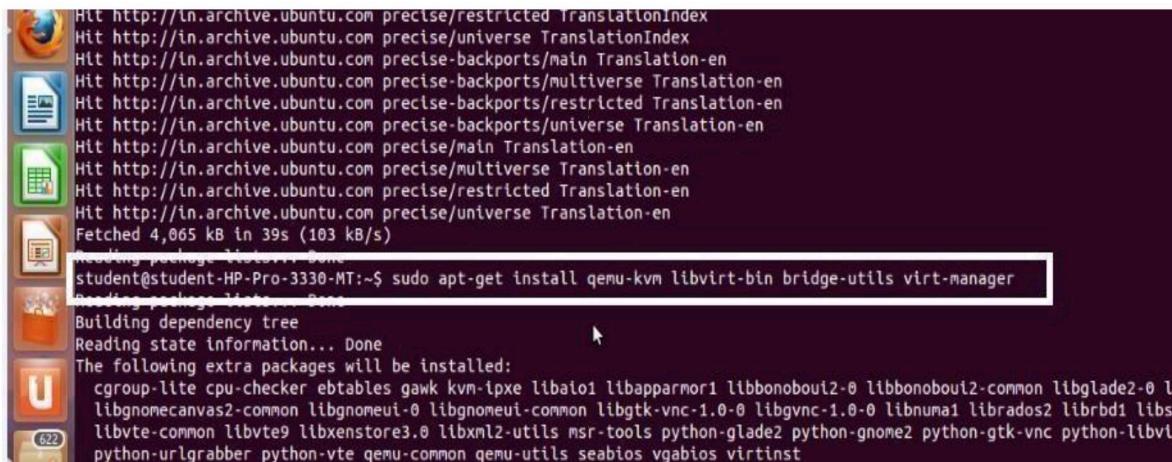


```
fpu           : yes
fpu_exception : yes
cpuid level   : 13
wp            : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
                cpb lm constant_tsc arch_perfmon pebs bts xtopology nonstop_tsc aperfmpf perf pni pclmulqdq d
                pcid sse4_1 sse4_2 popcnt tsc_deadline_timer xsave avx f16c lahf_lm arat epb xsaveopt pln
                ase smep erms
bogomips      : 6584.72
clflush size  : 64
cache_alignment : 64
address sizes  : 36 bits physical, 48 bits virtual
power management:

student@student-HP-Pro-3330-MT:~$ sudo grep -c "svm\|vmx" /proc/cpuinfo
student@student-HP-Pro-3330-MT:~$ sudo grep -c "svm\|vmx" /proc/cpuinfo
[sudo] password for student:
4
student@student-HP-Pro-3330-MT:~$ sudo apt-get update
Ign http://repo.mongodb.org precise/mongodb-org/3.2 InRelease
Ign http://extras.ubuntu.com precise InRelease
Hit http://repo.mongodb.org precise/mongodb-org/3.2 Release.gpg
Hit http://repo.mongodb.org precise/mongodb-org/3.2 Release
Ign http://in.archive.ubuntu.com precise InRelease
Get:1 http://in.archive.ubuntu.com precise-updates InRelease [55.7 kB]
Hit http://extras.ubuntu.com precise Release.gpg
Get:2 http://security.ubuntu.com precise-security InRelease [55.7 kB]
Hit http://repo.mongodb.org precise/mongodb-org/3.2/multiverse i386 Packages
Hit http://extras.ubuntu.com precise Release
```

Step 3 : #sudo adduser rait

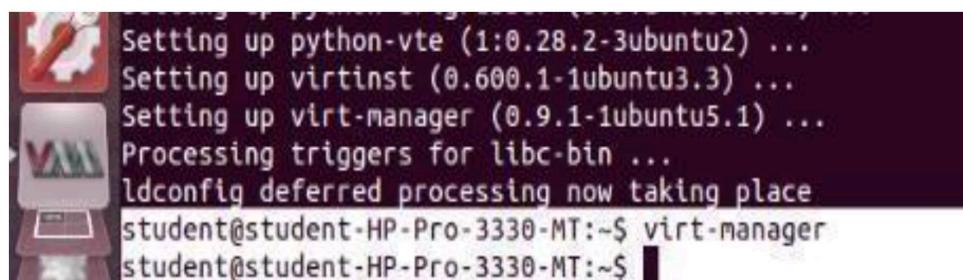
After running this command, log out and log back in as rait



```
Hit http://in.archive.ubuntu.com precise/restricted TranslationIndex
Hit http://in.archive.ubuntu.com precise/universe TranslationIndex
Hit http://in.archive.ubuntu.com precise-backports/main Translation-en
Hit http://in.archive.ubuntu.com precise-backports/multiverse Translation-en
Hit http://in.archive.ubuntu.com precise-backports/restricted Translation-en
Hit http://in.archive.ubuntu.com precise-backports/universe Translation-en
Hit http://in.archive.ubuntu.com precise/main Translation-en
Hit http://in.archive.ubuntu.com precise/multiverse Translation-en
Hit http://in.archive.ubuntu.com precise/restricted Translation-en
Hit http://in.archive.ubuntu.com precise/universe Translation-en
Fetched 4,065 kB in 39s (103 kB/s)
Reading package lists... Done
student@student-HP-Pro-3330-MT:~$ sudo apt-get install qemu-kvm libvirt-bin bridge-utils virt-manager
[sudo] password for student:
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
cgroup-lite cpu-checker ebttables gawk kvm-ipxe libata1 libapparmor1 libbonoboui2-0 libbonoboui2-common libglade2-0 libgnomecanvas2-common libgnomeui-0 libgnomeui-common libgtk-vnc-1.0-0 libgvnc-1.0-0 libnuma1 librados2 librbd1 libs
libvte-common libvte9 libxenstore3.0 libxml2-utils msr-tools python-glade2 python-gnome2 python-gtk-vnc python-libv
python-urlgrabber python-vte qemu-common qemu-utils seabios vgabios virtinst
[sudo] password for student:
```

Step 4 : #sudo adduser rait libvirtd

After running this command, log out and log back in as rait

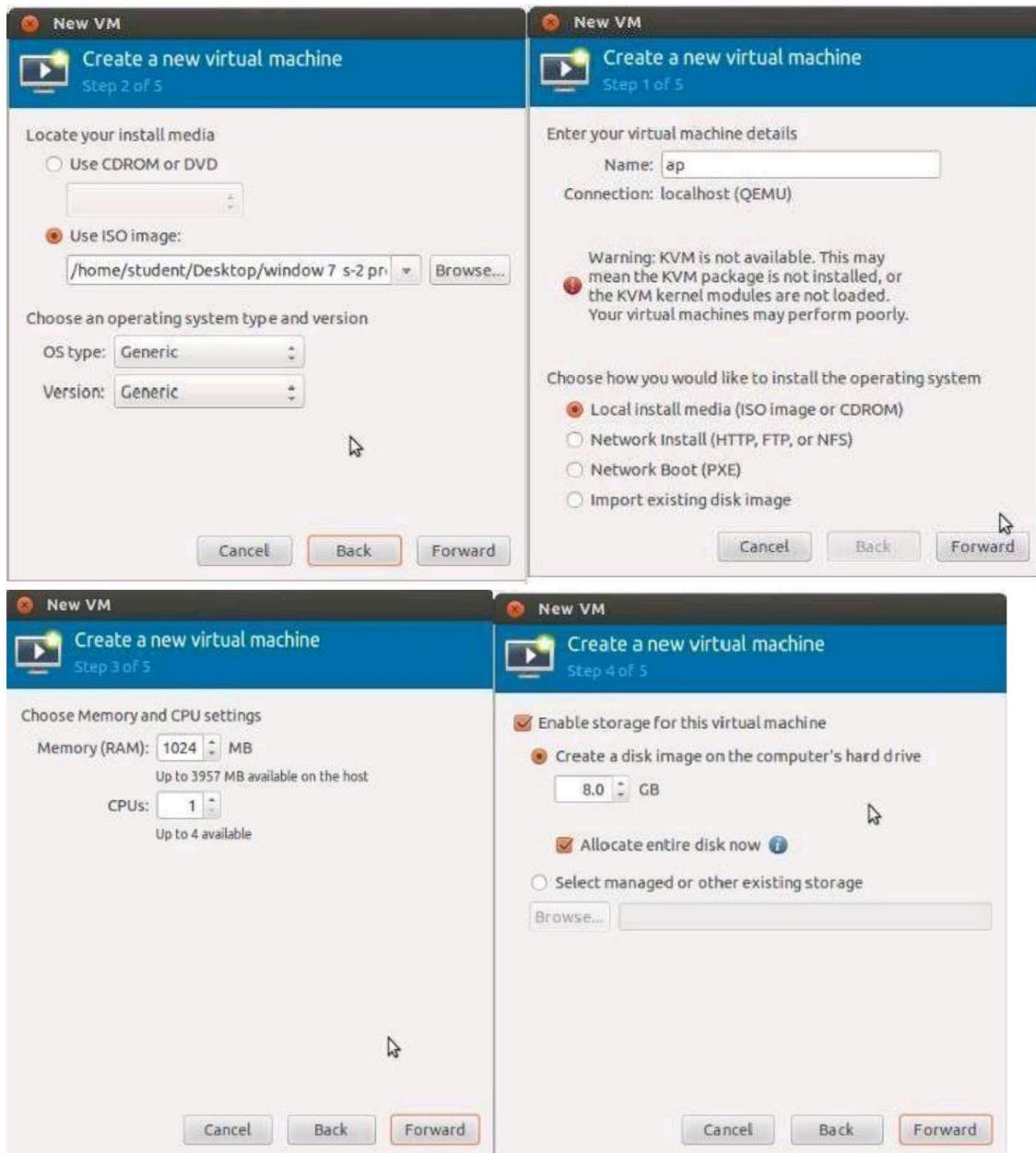


```
Setting up python-vte (1:0.28.2-3ubuntu2) ...
Setting up virtinst (0.600.1-1ubuntu3.3) ...
Setting up virt-manager (0.9.1-1ubuntu5.1) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
student@student-HP-Pro-3330-MT:~$ virt-manager
student@student-HP-Pro-3330-MT:~$
```

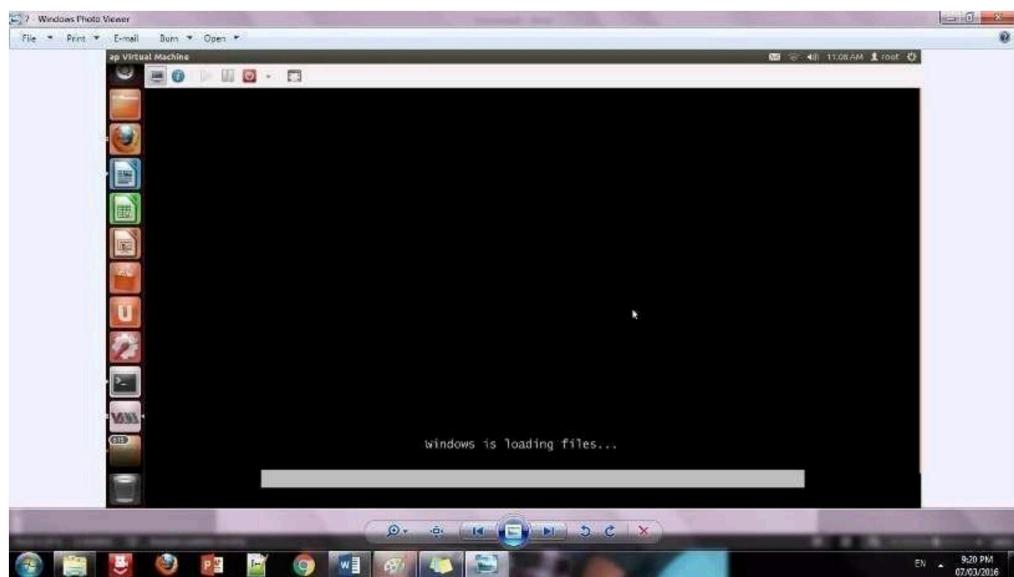
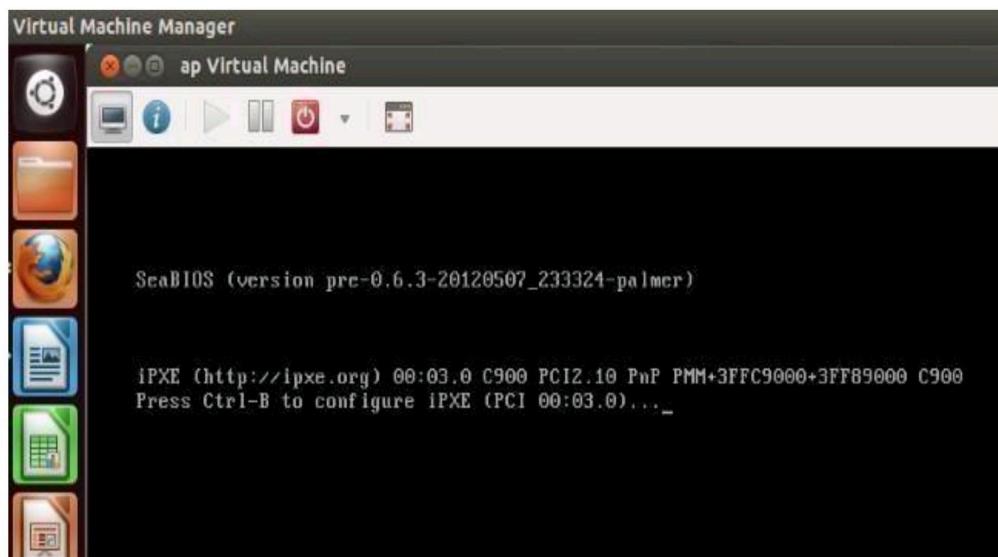
Step 5 : Open Virtual Machine Manager application and Create Virtual Machine  
#virt-manager as shown below



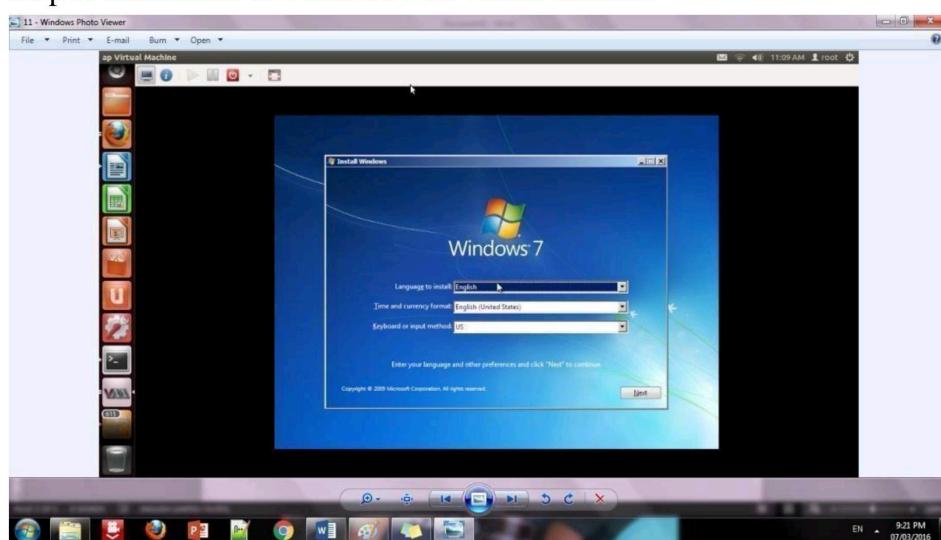
Step 6 : Create a new virtual machine as shown below



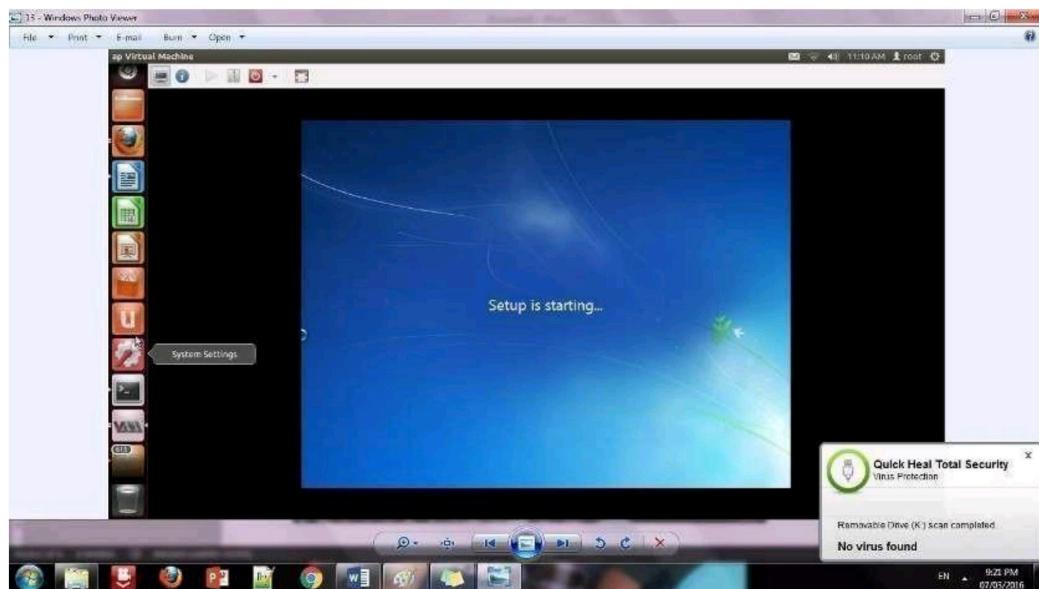
Step 7 : Install windows operating system on virtual machine



### Step 9: Installation of windows 7 on virtual machine



## Step 10: Initialization of windows on virtual machine



## Conclusion:

Installation and configuration of KVM have been done successfully onto Ubuntu and users added. Like this we can create as many virtual machines as possible on OS and can install any windows onto it.

Practical No: 3

Date:

Aim: Study and implementation of storage as a Service.

#### Description

Storage as a service is a business model in which a large company rents space in their storage infrastructure to smaller company or individual.

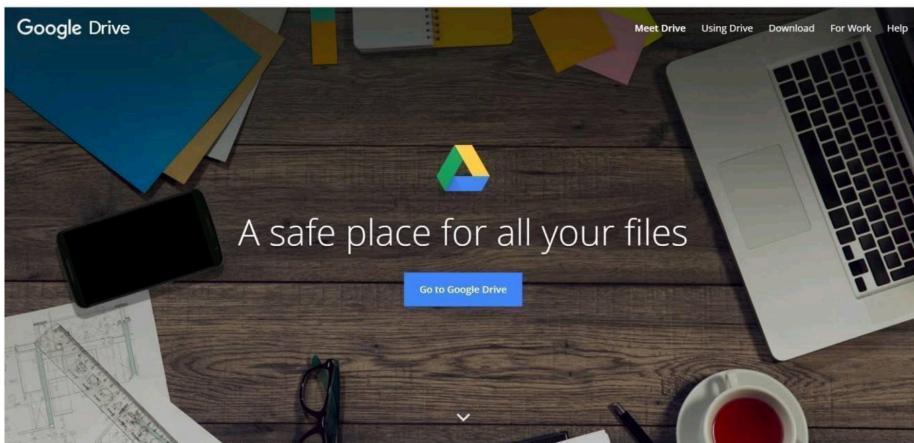
In the enterprise, SaaS vendors are targeting secondary storage applications by promoting SaaS as convenient way to manage backups. The key advantage to SaaS is enterprise is in cost savings - in personnel, in hardware, and in physical storage space. For instance, instead of maintaining a large tape library and arranging to vault (store) tapes offsite, a network administrator that used SaaS for backups could specify what data on network should be backed up and how often it should be backed up.

This company would sign a service level agreement (SLA) whereby SaaS provider agreed to rent storage space on a cost per gigabyte stored and cost per data transfer basis and basis company's data would be automatically transferred at specified time over storage provider's proprietary WAN or Internet.

Storage as a Service is generally seen as a good alternative for a small and mid-sized business that lacks the capital budget and / or technical personnel to implement and maintain their own storage infrastructure. SaaS is also being promoted as a way for all businesses to mitigate risk in disaster recovery, provide long-term retention for records.

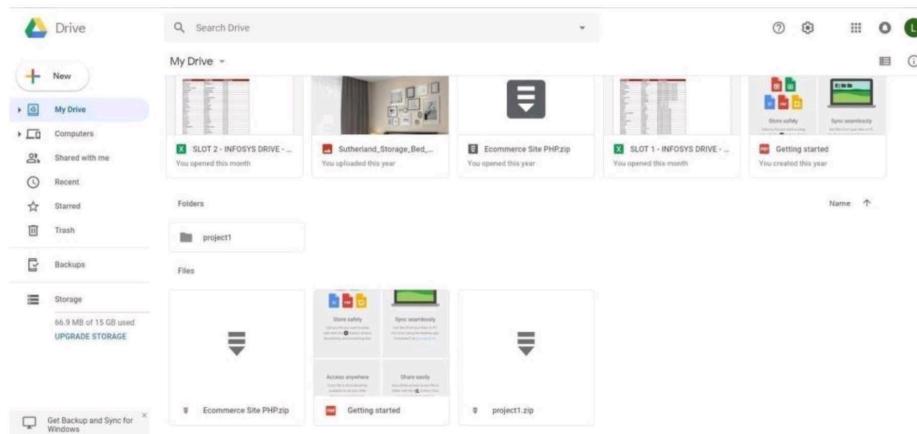
## Procedure:

### Step 1: open chrome->search for google drive

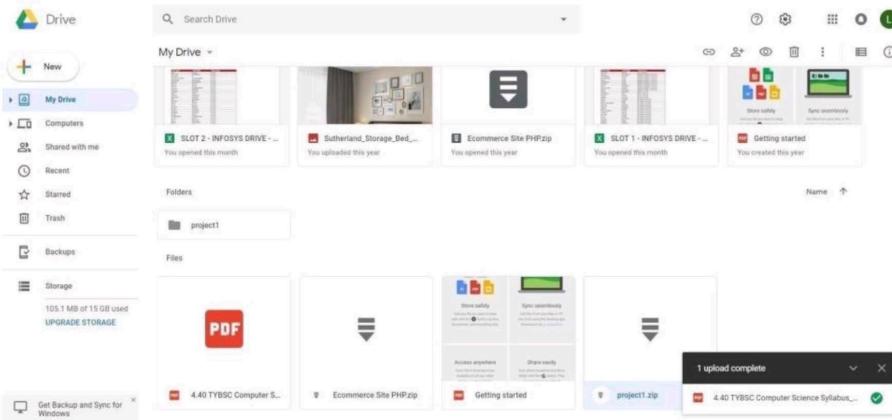


Step 2: now click on **GO TO DRVIE**

now sign in with google account and this interface will appear.

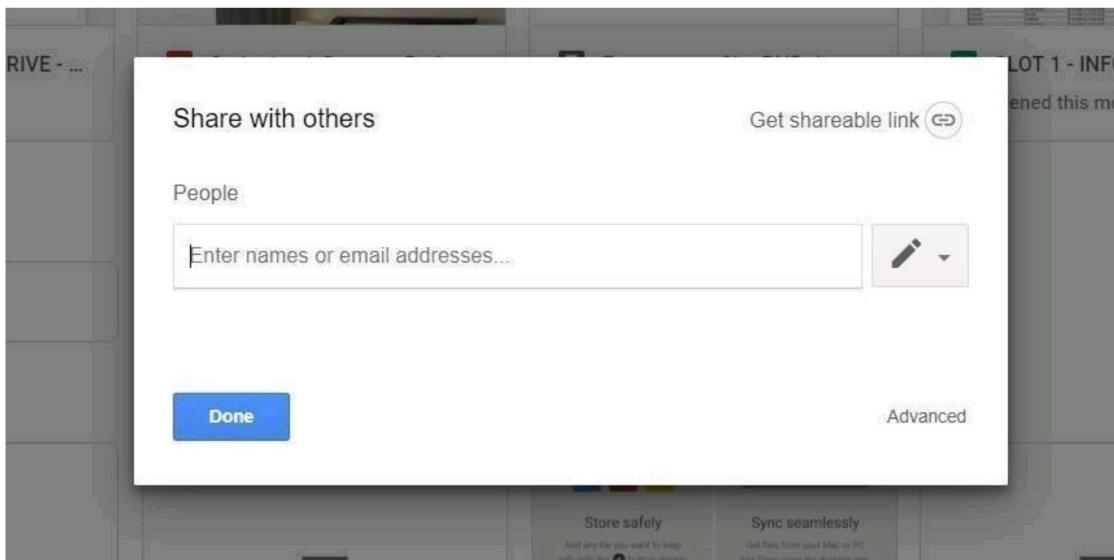


Step 3: Now click **New** to upload file on drive->select the file that you have to upload from your Computer.And click on open. If the file is uploaded then it will show successfully uploaded as shown in image.



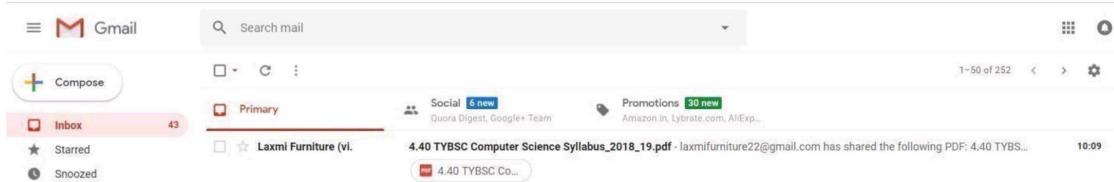
#### 4. Now sharing that file with your friends.

Select that doc which you have uploaded right click on that and click on share

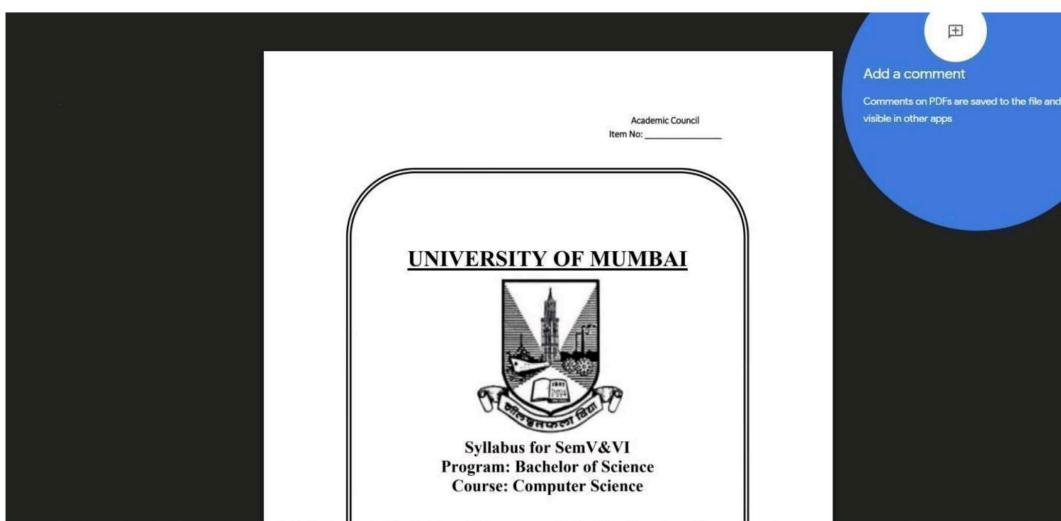


5. Now enter the email of your friend and provide subject name and click done.

Your friend will receive the mail as shown in image.



6. Now click on open that document will open which you have share to your friend.



Practical No: 4

Date:

Aim: study and implementation of Identity Management

Description :

Identity Management's primary goal in cloud computing is managing personal identity information so that access to computer resources, applications, data, and services is controlled properly. Identity Management is one area of IT security that offers genuine benefits beyond reducing risk of security breaches. Identity Management helps prevent security breaches and plays a significant role in helping your company meet IT security compliance regulations. The benefits of keeping your consumer or company financial data safe from unauthorized access can be huge.

In addition, you reap many benefits from Identity Management that occurs everyday, not just during a major threat.

- Improved user productivity: Productivity improvement comes from simplifying sign on interface and ability to quickly change access rights. Productivity is likely to improve further where you provide user self service.
- Improved customer and partner service: customers and partners also benefit from a more streamlined, secure process when accessing applications and data.
- Reduced help desk costs: IT help desks typically experience few calls about forgotten passwords when an identity management process is implemented.
- Reduced IT costs: Identity Management enables automatic provisioning, providing or revoking user access rights to systems and applications.

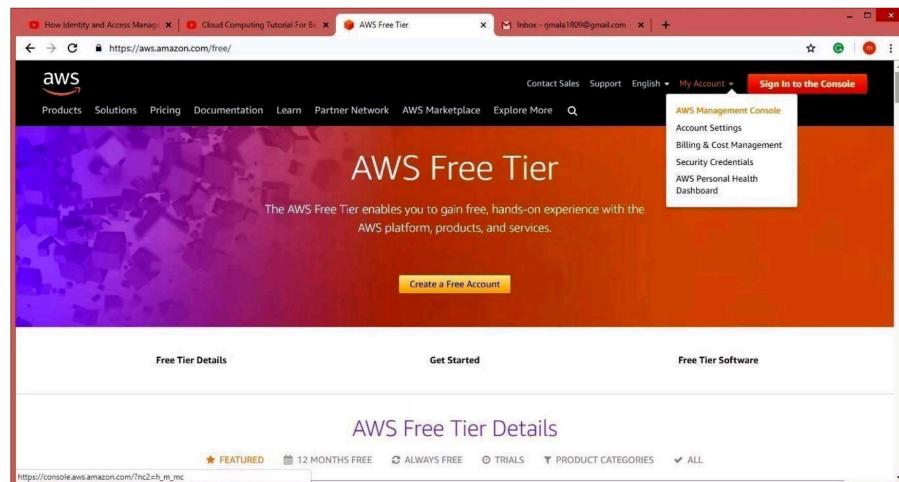
## Procedure:

1.Click on link below.

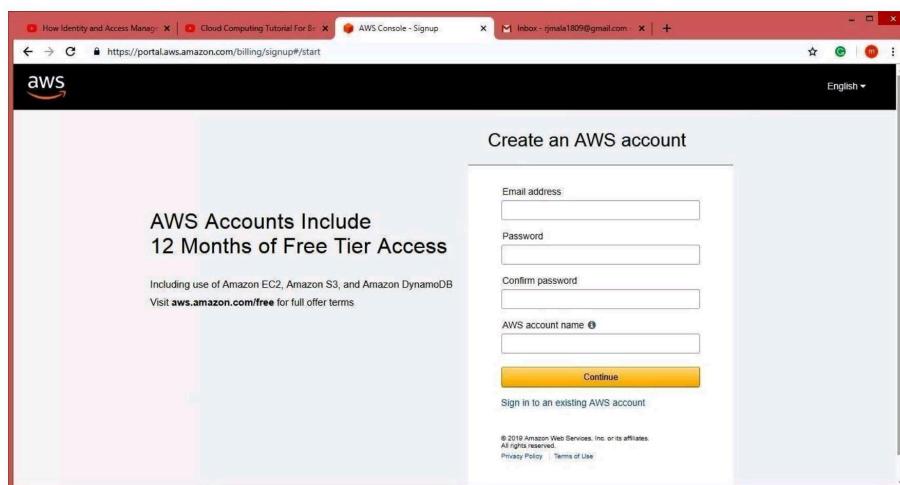
<https://aws.amazon.com/console/>



2.Go to "My Account" > "AWS Management Console".



3.Create AWS account(fill the required details)



The screenshot shows the 'Create an AWS account' page. On the left, there's a promotional message: 'AWS Accounts Include 12 Months of Free Tier Access' with a note about EC2, S3, and DynamoDB. Below that is a link to 'aws.amazon.com/free'. The main form on the right requires the following information:

- Email address: rjma1809@gmail.com
- Password: (redacted)
- Confirm password: (redacted)
- AWS account name: USER

At the bottom, there's a 'Continue' button, a 'Sign in to an existing AWS account' link, and a small note about copyright and terms.

The screenshot shows the 'Contact Information' page. It asks users to select an account type (Professional or Personal) and provides fields for full name, phone number, country/region, address, city, and state/province. A note at the top says 'All fields are required.'

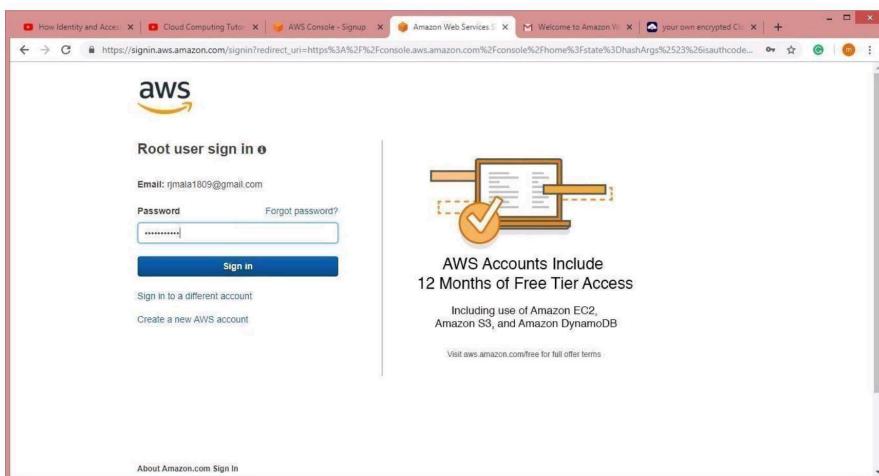
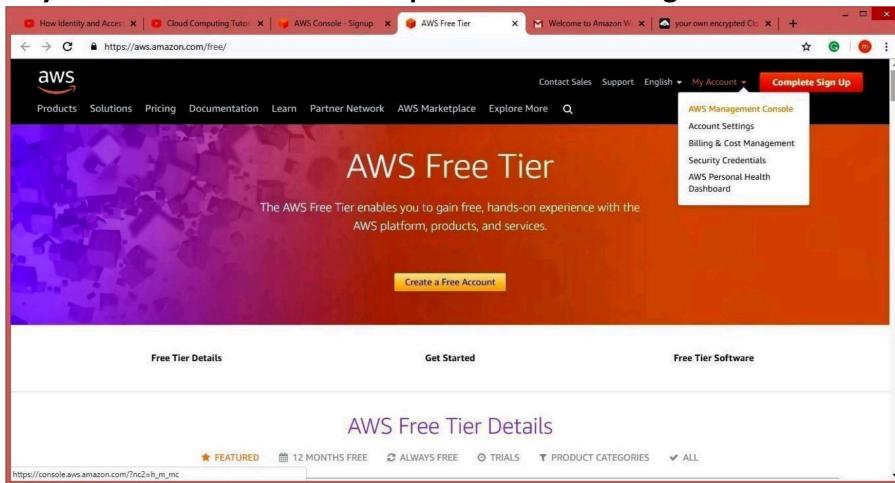
The screenshot shows the 'Address' details page. It requires input for address, city, state/province, and postal code. The city field is filled with 'mumbai' and the state/province field with 'maharashtra'. The postal code field is highlighted in yellow and contains '421306'. At the bottom, there's a checkbox for accepting the Customer Agreement and a 'Create Account and Continue' button.

**NOTE:- Do not provide any kind of credit/debit card details or bank details.)**

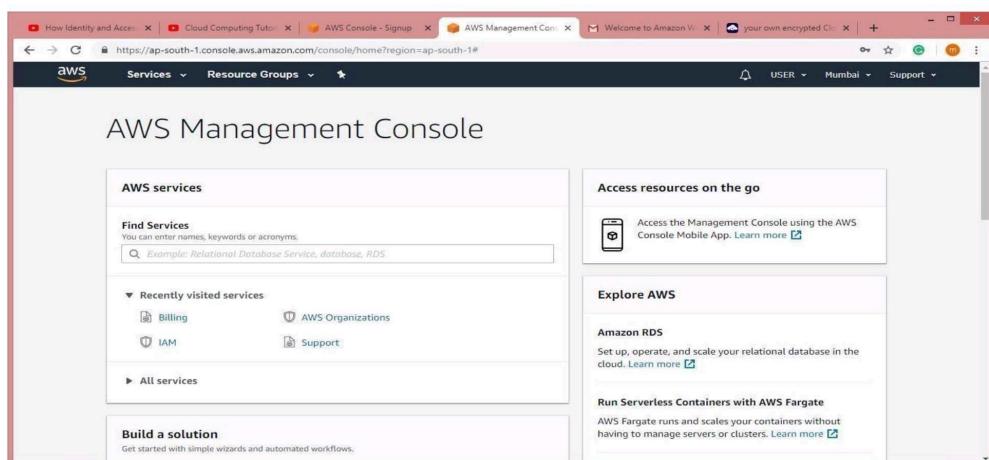
**Click on next**

#### 4.Click on My Account, Select AWS Management Console.

Enter your aws account userid and password click on sign in button

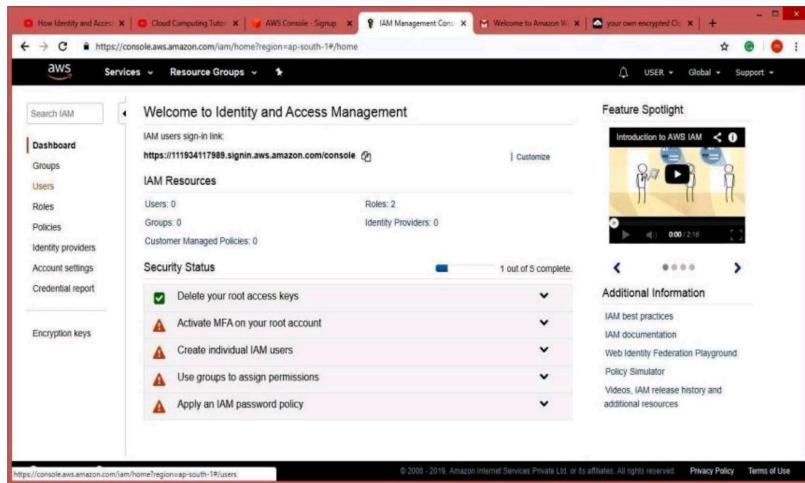


#### 5.Now it will redirect you to home page without asking any other details. Now to we have to add user and group and assign them privilages.



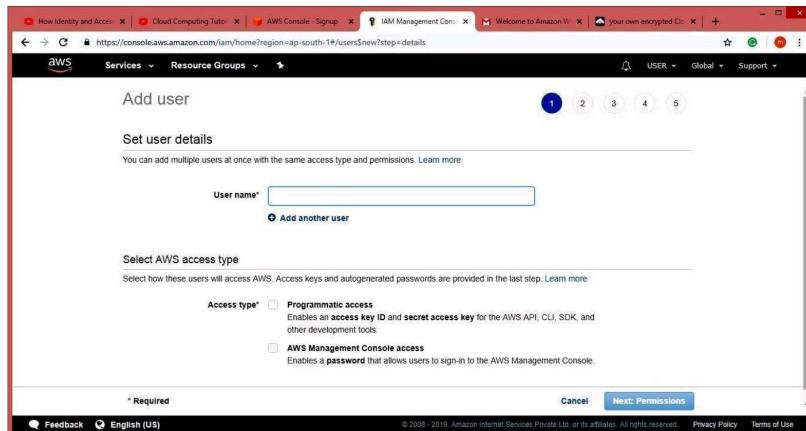
## 6.Go to “My Security”

Credentials”.Click on “Users”.

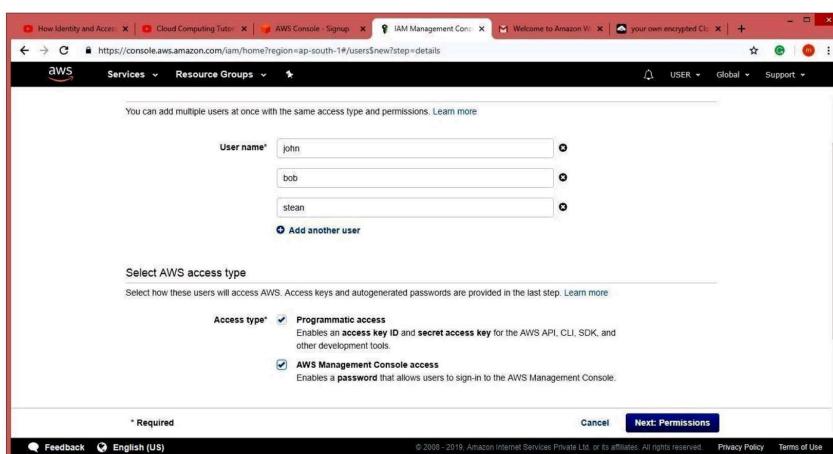


## 7.Click on “Add user”.

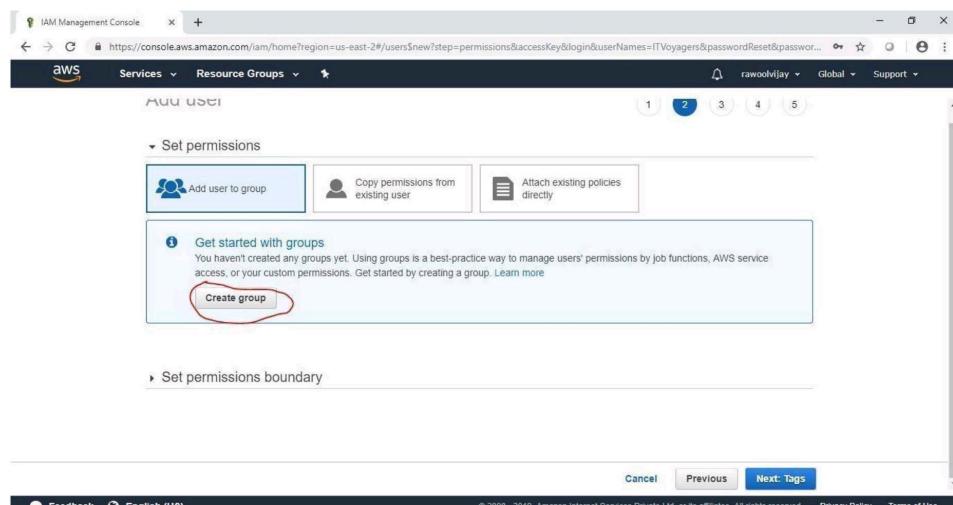
Enter the name for the user. Check the check box in front of “Programmatic access” and “AWS Management Console access”.



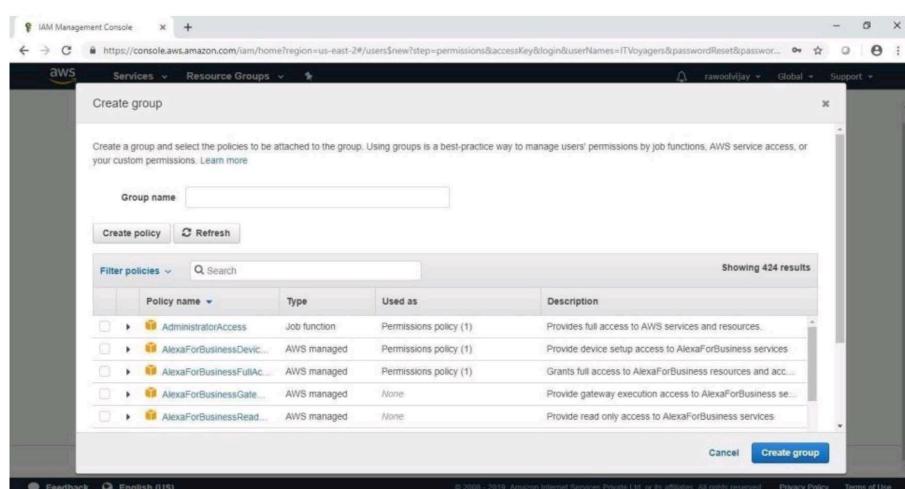
8.Scroll down and select “Custom password” and enter the password for the new user and click on “Next: Permissions”.Next



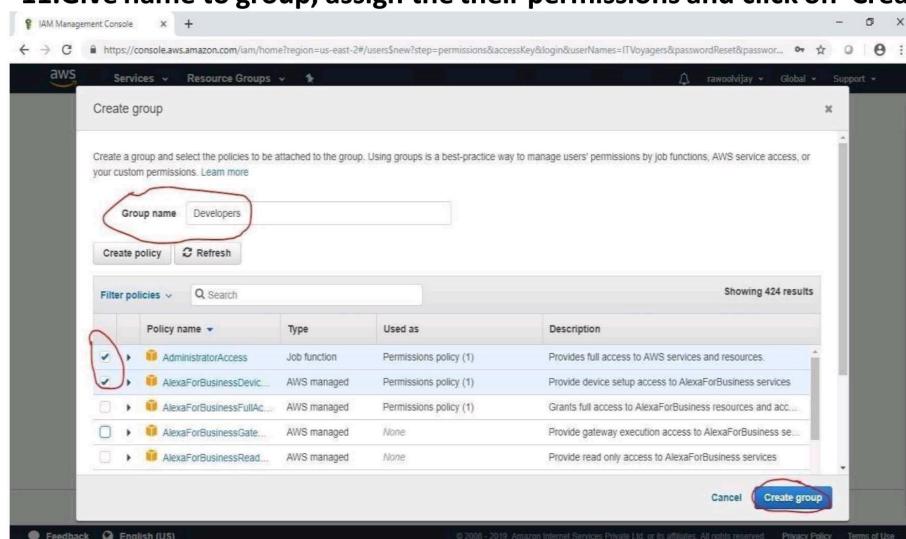
**9. Next it allow you to create group or you can just pass it. We are going to create group click on “Create group”.**



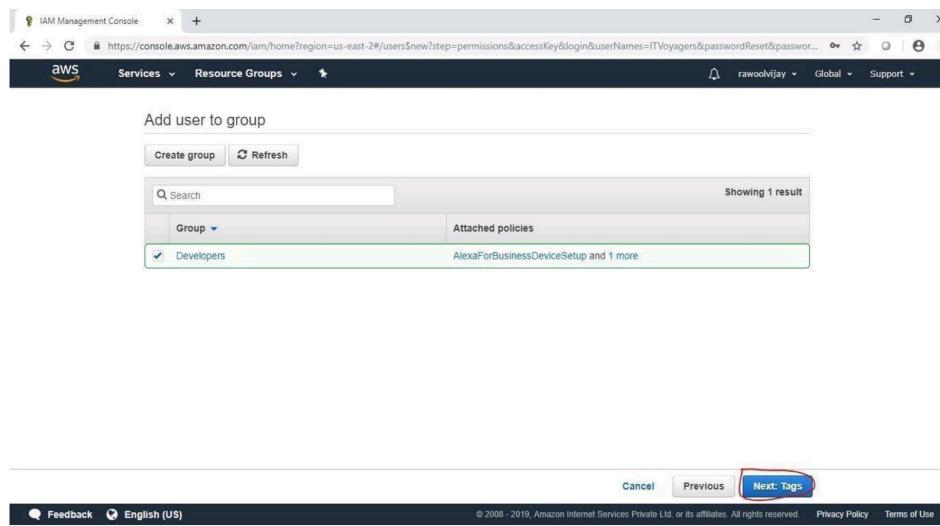
**10. Following window will appear.**



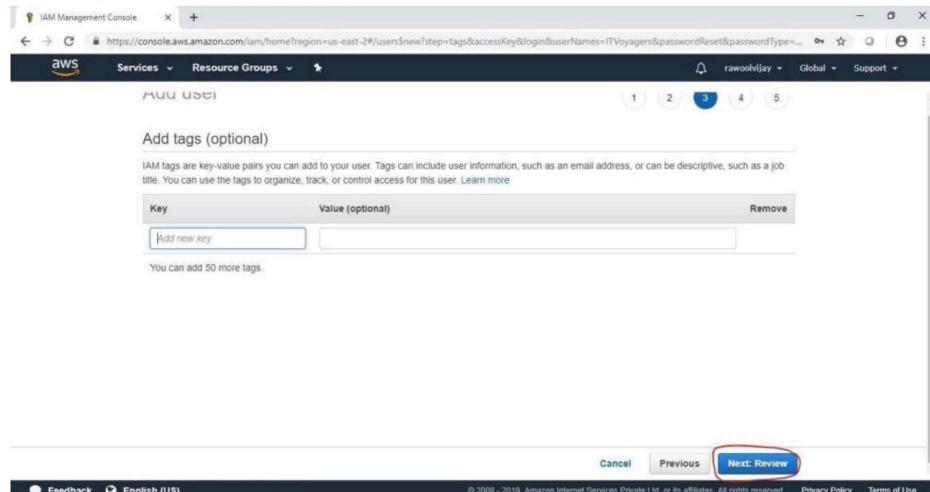
**11. Give name to group, assign the their permissions and click on “Create group”.**



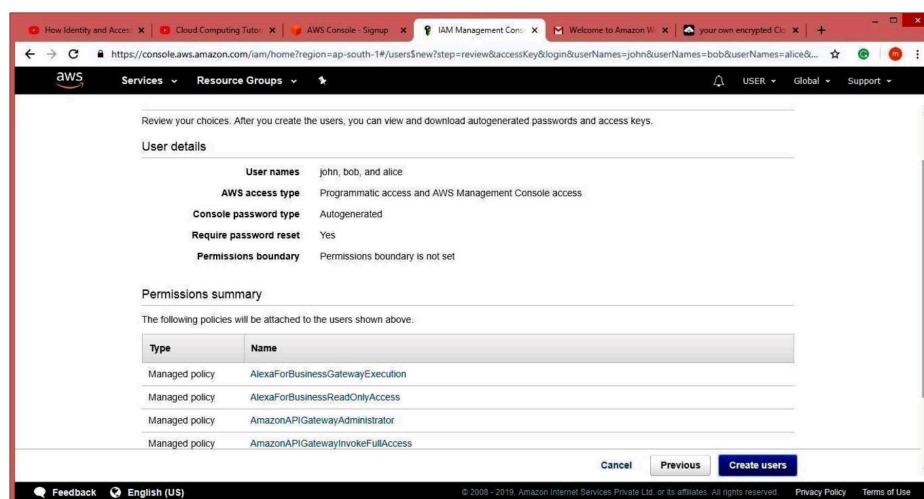
**12.Your group is created now click on “Next: Tags”.**



**13.Click on “Next: Review”.**



**14.Check the Review for the user and click on “Create user”.  
Click on**



**15.Click on “Close”.**

**Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also generate temporary security credentials for your users. These credentials will be available for 1 hour. You can sign in to the AWS Management Console using these credentials.

User	Access key ID	Secret access key	Password	Email login instructions
john	AKIAJY4PKRBM3TPPS27A	***** Show	***** Show	Send email
bob	AKIAIBBDBAY2B67AJGA	***** Show	***** Show	Send email
alice	AKIACN7NVCOIPJL6A	***** Show	***** Show	Send email

**16.Click on “Group”. You will see the group you just created.**

**Welcome to Identity and Access Management**

IAM users sign-in link: <https://111934117988.signin.aws.amazon.com/console>

**IAM Resources**

Users: 0      Roles: 2  
Groups: 0      Identity Providers: 0  
Customer Managed Policies: 0

**Security Status**

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

**17.Now log out of admin account and try to login as user (newly created).**

**Navigate to link below.**

**<https://aws.amazon.com/console/>**

**Go to “My Account” > “AWS Management Console”.**

**AWS Free Tier**

The AWS Free Tier enables you to gain free, hands-on experience with the AWS platform, products, and services.

**Create a Free Account**

**My Account**

- AWS Management Console
- Account Settings
- Billing & Cost Management
- Security Credentials
- AWS Personal Health Dashboard

Practical No: 8

Date:

Aim: case study on Google cloud platform

Description:

Google cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end user products, such as Google search and YouTube. Alongside a set of management tools, it provides a series of modular cloud services, including computing, data storage, data analytics, and machine learning. Registration requires a credit card or bank account details.

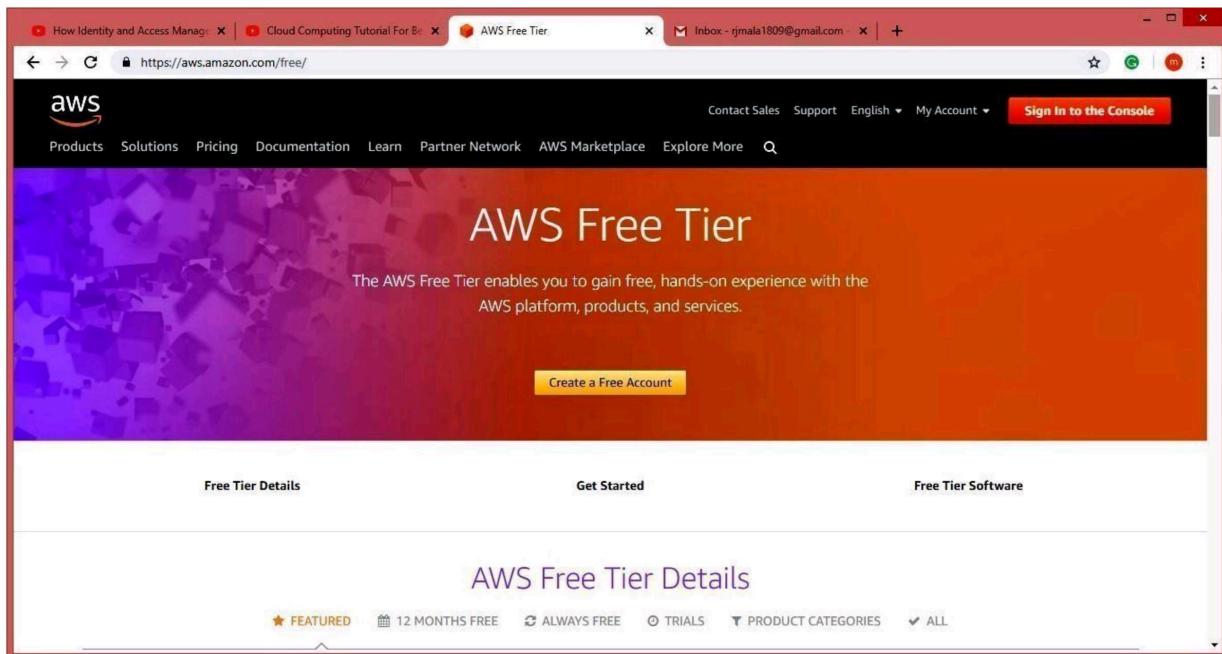
Google cloud Platform provides Infrastructure as a service, Platform as a service and serverless computing environments.

In April 2008, Google announced App Engine, a platform for developing and hosting web applications in Google-managed data centres, which was the first cloud computing service from company. This service became generally available in Nov 2011. Since the announcement of App Engine, Google added multiple cloud services to the platform.

Google cloud Platform is a part of Google cloud, which includes Google cloud Platform public cloud infrastructure, as well as G Suite, enterprise versions of Android and Chrome OS, and application programming interfaces (APIs) for machine learning and enterprise mapping services.

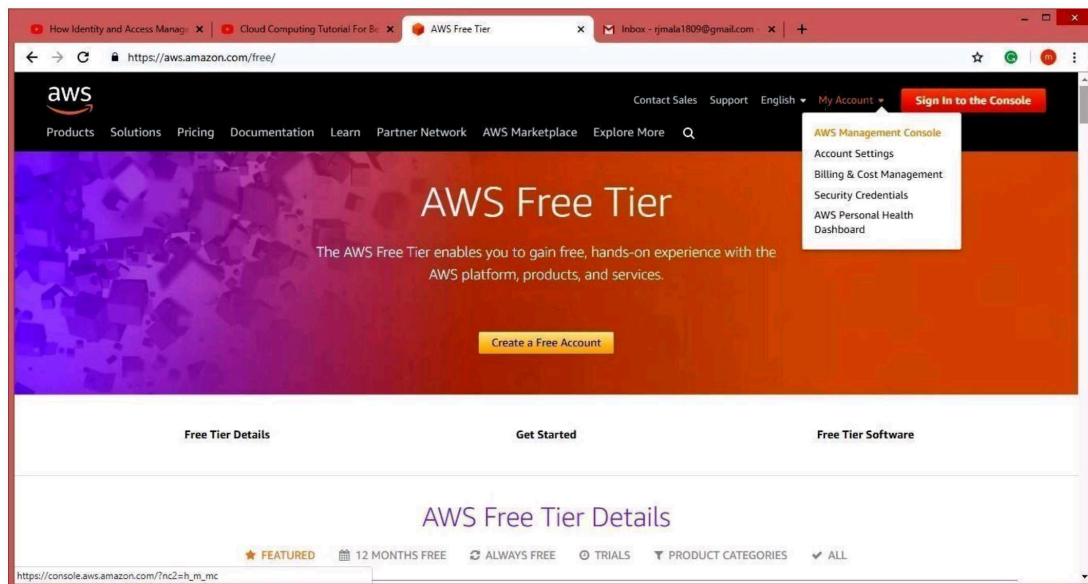
## Procedure:

1: Go to aws.amazon.com



2: Click On My Account.

3: Select aws management console and click on it.



#### 4: Create AWS account(fill the required details)

The screenshot shows the 'Create an AWS account' form on the AWS Console. The page includes a promotional message about free tier access and links to privacy policy and terms of use. The form fields are empty.

AWS Accounts Include  
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB  
Visit [aws.amazon.com/free](https://aws.amazon.com/free) for full offer terms

Email address:

Password:

Confirm password:

AWS account name:

**Continue**

Sign in to an existing AWS account

© 2019 Amazon Web Services, Inc. or its affiliates.  
All rights reserved.  
[Privacy Policy](#) | [Terms of Use](#)

The screenshot shows the same 'Create an AWS account' form, but with the email address and AWS account name fields populated. The other fields remain empty.

AWS Accounts Include  
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB  
Visit [aws.amazon.com/free](https://aws.amazon.com/free) for full offer terms

Email address:

Password:

Confirm password:

AWS account name:

**Continue**

Sign in to an existing AWS account

© 2019 Amazon Web Services, Inc. or its affiliates.  
All rights reserved.  
[Privacy Policy](#) | [Terms of Use](#)

Contact Information

Please select the account type and complete the fields below with your contact details.

Account type ⓘ

Professional  Personal

Full name

USER

Phone number

Country/Region

United States

Address

Street, P.O. Box, Company Name, c/o  
Apartment, suite, unit, building, floor, etc.

City

State / Province or region

AB Complex

City

mumbai

State / Province or region

maharashtra

Postal code

421306

Amazon Internet Services Pvt. Ltd. Customer Agreement

Customers with an India contact address are now required to contract with Amazon Internet Service Private Ltd. (AISPL). AISPL is the local seller for AWS infrastructure services in India.

Check here to indicate that you have read and agree to the terms of the AISPL Customer Agreement

Create Account and Continue

**NOTE:- Do not provide any kind of credit/debit card details or bank details.)**

**5: Click on next**

(open your gmail check you will get message from amazon).

**6: Click on My Account, Select AWS Management Console.**

**7: Enter your aws account userid and password click on sign in button**

The screenshot shows the AWS Free Tier landing page. At the top right, there is a 'My Account' dropdown menu with options: 'AWS Management Console', 'Account Settings', 'Billing & Cost Management', 'Security Credentials', 'AWS Personal Health', and 'Dashboard'. Below the menu, there is a 'Create a Free Account' button. At the bottom of the page, there are three buttons: 'Free Tier Details', 'Get Started', and 'Free Tier Software'.

The screenshot shows the AWS sign-in page for a root user. It features a form with fields for 'Email' (rjmalai1809@gmail.com) and 'Password'. There are links for 'Forgot password?' and 'Sign in'. Below the form, there are links for 'Sign in to a different account' and 'Create a new AWS account'. To the right, there is an illustration of a key being inserted into a lock. Text below the illustration states: 'AWS Accounts Include 12 Months of Free Tier Access' and 'Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB'. A small note at the bottom says 'Visit [aws.amazon.com/free](#) for full offer terms'.

## 8: Click on Services tab

The screenshot shows the AWS Management Console home page. At the top, there is a navigation bar with tabs for 'Services' and 'Resource Groups'. Below the navigation bar, the title 'AWS Management Console' is displayed. On the left side, there is a sidebar titled 'AWS services' which includes sections for 'Find Services', 'Recently visited services' (listing Billing, IAM, AWS Organizations, Support), and 'Build a solution'. On the right side, there are two main sections: 'Access resources on the go' (with a link to the AWS Console Mobile App) and 'Explore AWS' (listing Amazon RDS and Run Serverless Containers with AWS Fargate). The 'Services' tab is highlighted in the navigation bar.

## 9: Click on Security, identity & Appliances Select IAM

The screenshot shows the AWS Management Console home page with the 'Services' tab selected. In the sidebar, under the 'History' section, the 'IAM' link is highlighted. The main content area displays a grid of AWS services categorized by color-coded icons. The 'Security, Identity, & Compliance' category, which includes the IAM service, is highlighted with a blue border. Other services listed in this category include Resource Access Manager, Cognito, Secrets Manager, GuardDuty, Inspector, Amazon Macie, AWS Organizations, and AWS Single Sign-On. The URL at the bottom of the browser window is <https://console.aws.amazon.com/iam/home?region=ap-south-1>.

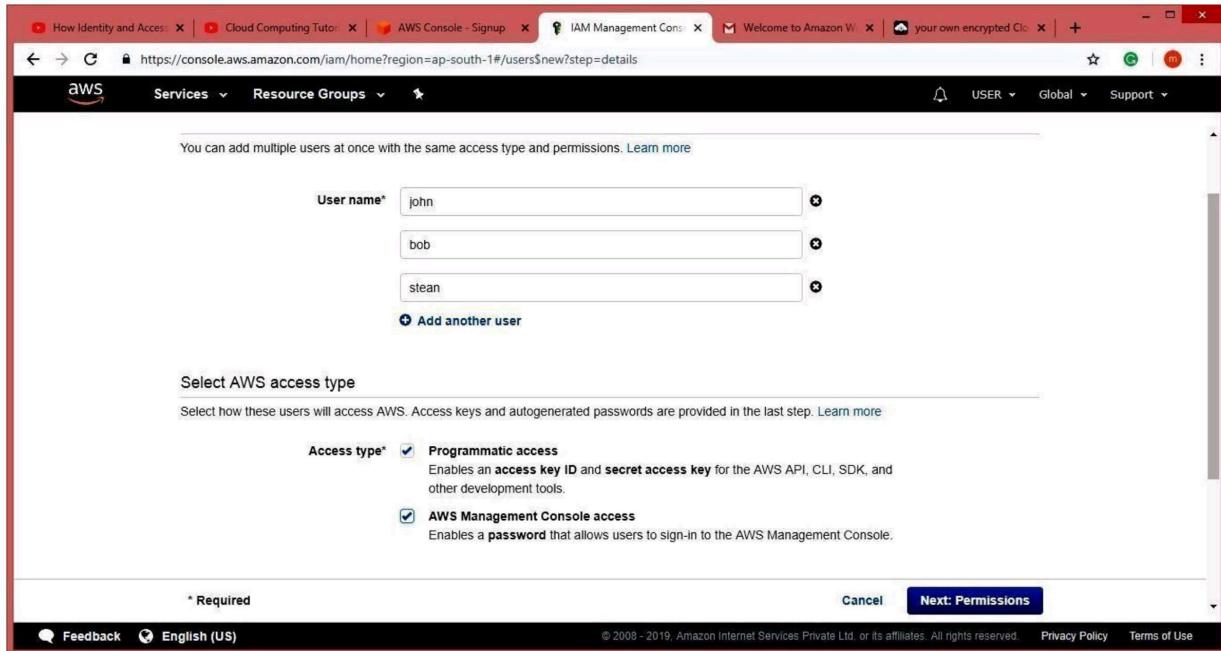
## 10: Click on Users From Dashboard

The screenshot shows the AWS IAM Management Console dashboard. On the left, there's a sidebar with a 'Dashboard' button highlighted, along with other options like Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area has a title 'Welcome to Identity and Access Management'. It displays statistics: Users: 0, Groups: 0, Roles: 2, and Identity Providers: 0. Below this is a 'Security Status' section with five items: 'Delete your root access keys' (checked), 'Activate MFA on your root account', 'Create individual IAM users', 'Use groups to assign permissions', and 'Apply an IAM password policy'. To the right, there's a 'Feature Spotlight' section with a video thumbnail titled 'Introduction to AWS IAM' and an 'Additional Information' section with links to IAM best practices, documentation, and videos.

## 11: Click on Add User and Add the users.

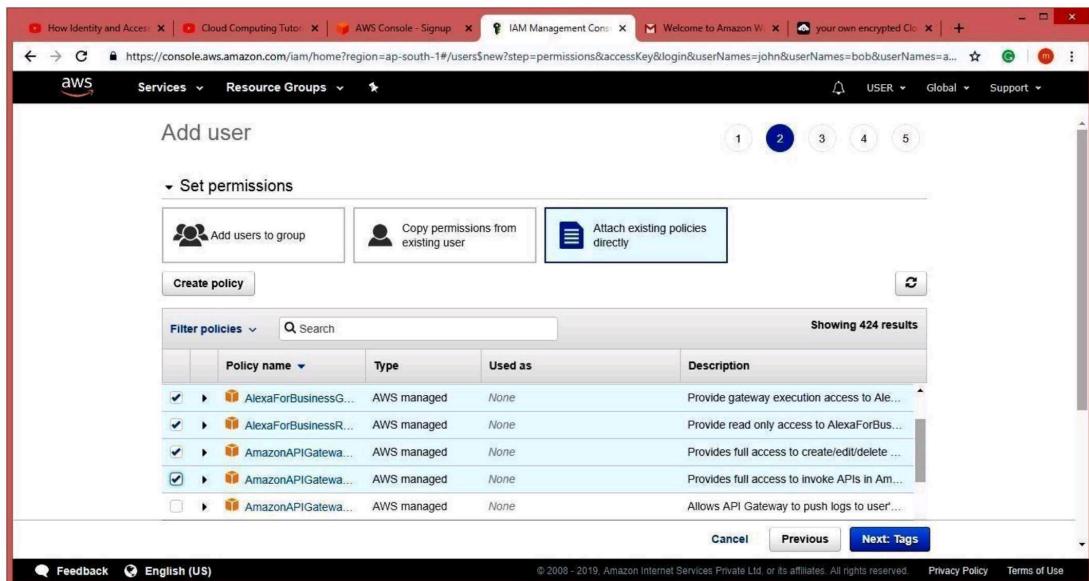
The screenshot shows the 'Add user' wizard, step 1: Set user details. At the top, it says 'Add user' and shows a progress bar with step 1 highlighted. Below that is a 'Set user details' section with a note: 'You can add multiple users at once with the same access type and permissions. Learn more'. There's a 'User name\*' input field containing 'testuser' and a link to 'Add another user'. The next section, 'Select AWS access type', asks 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more'. It lists two options: 'Programmatic access' (selected) and 'AWS Management Console access'. Both descriptions mention the creation of access keys and secret access keys. At the bottom, there are buttons for 'Required' (marked with an asterisk), 'Cancel', and 'Next: Permissions'.

**12:** Goto Select AWS access type check both the radiobutton. And click on next permission



**13:** Click on Attach Existing Policy Directly.

Attach Policy to the users. And press Next Tab.



The screenshot shows the AWS IAM Management Console interface. At the top, there are three main buttons: 'Add users to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. Below these buttons is a 'Create policy' button. A search bar labeled 'Search' is positioned above a table titled 'Showing 424 results'. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. The first few rows of the table list various AWS managed policies, such as 'AmazonChimeFullAccess', 'AmazonChimeReadOnly', etc. At the bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

#### 14: Click On Create User(Here Users are created.)

The screenshot shows the 'Create users' step in the AWS IAM Management Console. It displays a summary of user details and attached policies. The 'User details' section includes fields for 'User names' (set to 'john, bob, and alice'), 'AWS access type' (set to 'Programmatic access and AWS Management Console access'), 'Console password type' (set to 'Autogenerated'), 'Require password reset' (set to 'Yes'), and 'Permissions boundary' (set to 'Permissions boundary is not set'). The 'Permissions summary' section shows a table of attached policies:

Type	Name
Managed policy	AlexaForBusinessGatewayExecution
Managed policy	AlexaForBusinessReadOnlyAccess
Managed policy	AmazonAPIGatewayAdministrator
Managed policy	AmazonAPIGatewayInvokeFullAccess

At the bottom of the screen, there are buttons for 'Cancel', 'Previous', and 'Create users'.

**15:** Now download the csvfile . and click on close.

The screenshot shows the AWS IAM Management Console interface. A success message box is displayed, stating: "Success: You successfully created the users shown below. You can view and download user security credentials. You can instructions for signing in to the AWS Management Console. This is the last time these credentials will be available; you can create new credentials at any time." Below the message, there is a "Download .csv" button. To the right, a sidebar menu is open under the "USER" tab, showing options like "My Account", "My Organization", "My Billing Dashboard", "My Security Credentials" (which is highlighted in yellow), and "Sign Out". At the bottom of the page, there is a "Close" button and a URL bar with the address https://console.aws.amazon.com/iam/home?region=ap-south-1#security\_credentials.

**16:** Now Goto Account and select My Security Credential tab > Click on Continew to security credentials .

The screenshot shows the AWS IAM Management Console with a modal dialog box in the foreground. The dialog contains the following text: "You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources. To help secure your account, follow an AWS best practice by creating and using AWS Identity and Access Management (IAM) users with limited permissions." Below the text are two buttons: "Continue to Security Credentials" and "Get Started with IAM Users". There is also a checkbox labeled "Don't show me this message again". In the background, the main IAM dashboard is visible, showing sections for Multi-factor authentication (MFA), Access keys (access key ID and secret access key), CloudFront key pairs, X.509 certificate, and Account identifiers. The URL in the address bar is https://console.aws.amazon.com/iam/home?region=ap-south-1#security\_credentials.

## 17: Click on Multi-factor authentication(MFA)

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=ap-south-1#/security\\_credentials](https://console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials). The left sidebar includes links for Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Your Security Credentials' and contains a section for 'Multi-factor authentication (MFA)'. A sub-section for 'Activate MFA' is visible.

## 18: Click On Active MFA

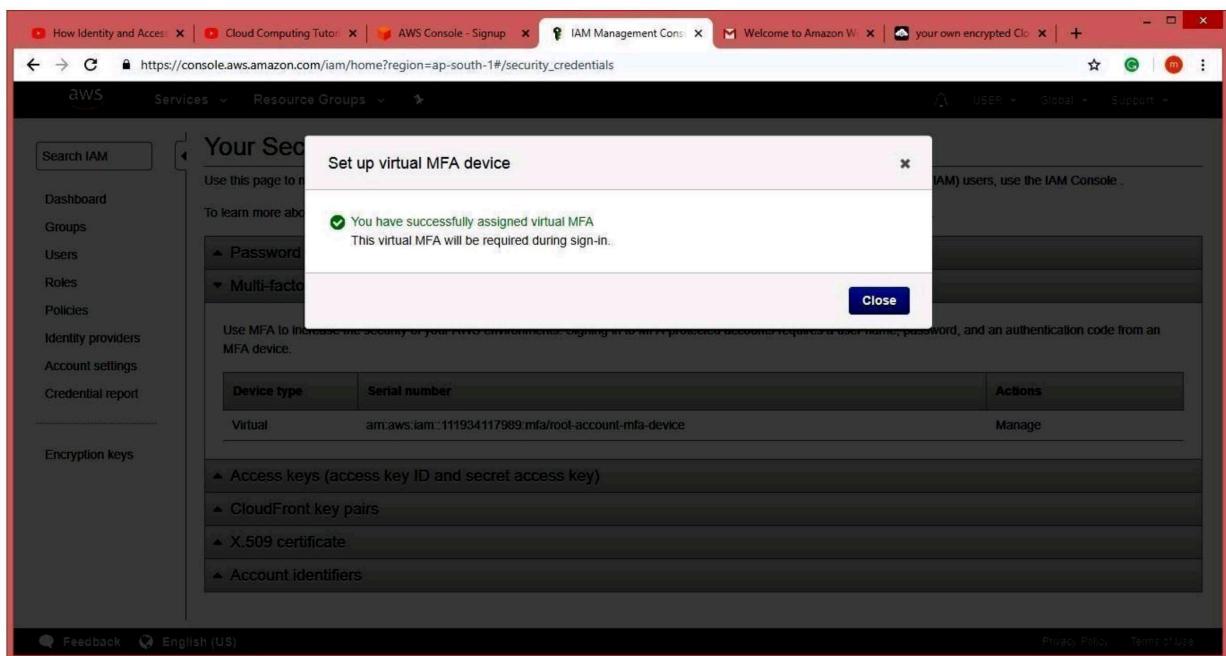
The screenshot shows the same AWS IAM Management Console interface as the previous step. The 'Multi-factor authentication (MFA)' section is expanded, and the 'Activate MFA' button is highlighted with a blue border.

## 19: Select Virtual MFA device and Click on Continue tab

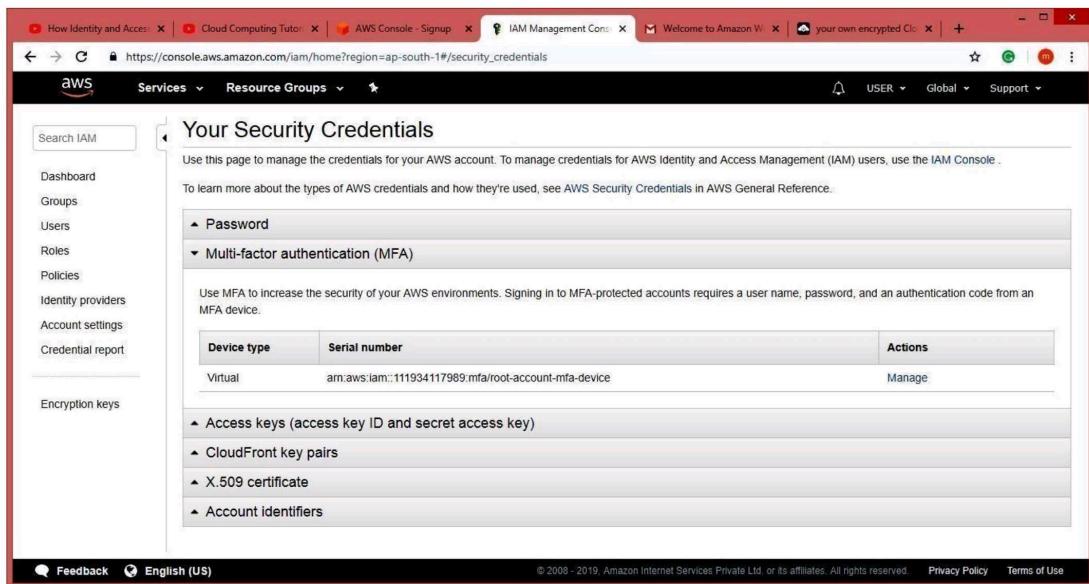
**Note: Download Barcode Scanner and Google Authentication App in your Mobile Phone.**

The image consists of two screenshots of the AWS IAM Management Console. The top screenshot shows the 'Manage MFA device' dialog, which asks to choose the type of MFA device. The 'Virtual MFA device' option is selected, with a sub-note about an authenticator app installed on a mobile device or computer. Other options like 'U2F security key' and 'Other hardware MFA device' are also listed. The bottom screenshot shows the 'Set up virtual MFA device' dialog, which displays a QR code for scanning and two input fields for entering consecutive MFA codes. One field contains 'MFA code 1: 765229' and the other is empty. At the bottom are 'Cancel', 'Previous', and 'Assign MFA' buttons.

**20:** Scan the QR code and enter the MFA code from ur mobile phone and then click on assign Assign MFA tab



21: Now the page look like this.



## 22: Click On Dashboard Go to Additional Information Select Policy Simulator

The screenshot shows the AWS IAM Management console. The left sidebar has 'Dashboard' selected. The main area displays 'Welcome to Identity and Access Management' with a sign-in link. Below it, 'Now Resources' shows 3 Users, 2 Roles, 0 Groups, and 0 Identity Providers. A 'Security Status' section lists five items: 'Delete your root access keys' (checked), 'Activate MFA on your root account' (checked), 'Create individual IAM users' (checked), 'Use groups to assign permissions' (warning icon), and 'Apply an IAM password policy' (warning icon). To the right, a 'Feature Spotlight' video player is shown, followed by the 'Additional Information' section which includes links to IAM best practices, documentation, and the 'Policy Simulator' (which is underlined).

## 23: Select The User select services and service action and click on Run Simulator Tab

The screenshot shows the 'IAM Policy Simulator' interface. On the left, a sidebar lists 'Users, Groups, and Roles' with 'Users' selected, showing entries for 'alice', 'bob', and 'john'. The main area is titled 'Policy Simulator' and contains a table with the following columns: Service, Action, Resource Type, Simulation Resource, and Permission. The table is currently empty. At the top of the main area, there are buttons for 'Mode : Existing Policies', 'USER', and 'Run Simulation'.

Practical No: 6

Date:

Aim : Study and Implementation of Single-Sign-On

Description :

Single-sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications. The service authenticates the end user for all applications the user has been given rights to and eliminates further prompts when user switches applications during same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.

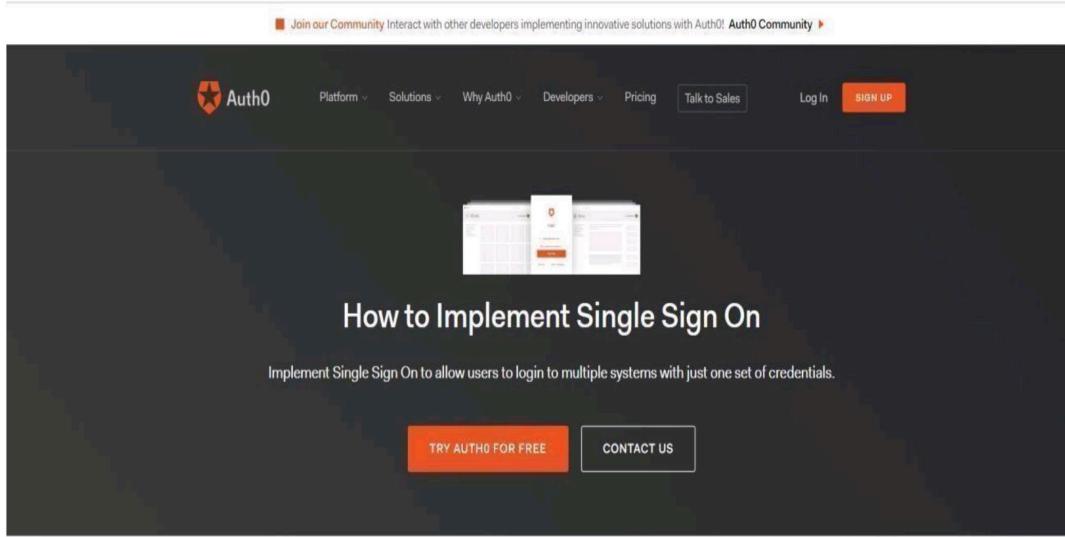
In a basic Web SSO service, an agent module on the application server retrieves the specific authentication credential for an individual user from a dedicated SSO policy server, while authenticating the user against a user switches applications such as lightweight directory access protocol (LDAP) directory.

Some SSO services use protocols such as Kerberos and the security assertion markup language (SAML). SAML is an XML standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML based SSO services involve communications between the user, an identity provider that maintains a user directory and a service provider.

## Procedure:

1: Open chrome->go to the URL-> <https://auth0.com/learn/how-to-implement-single-sign-on/>

And this page will appear



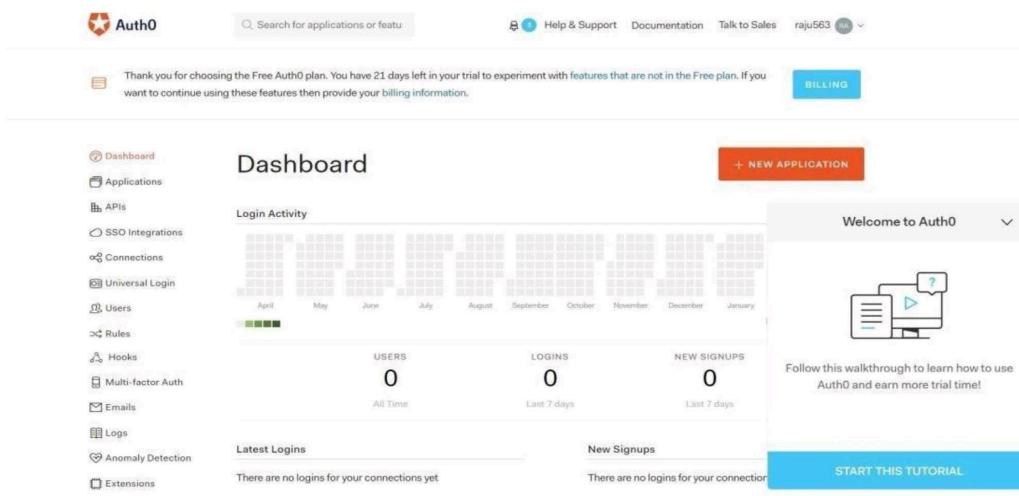
2: Click on **TRY AUTH FOR FREE** -> now sign up -> provide user name(Click on next)->select

1-account type(personal)

2-Role(Non developer)

3-Project(just playing around)

3: Click on CREATE ACCOUNT->Dashboard will appear



4: Click on Connection-> select (**Social**)-> click on google try as shown in Image

The screenshot shows the Auth0 dashboard. On the left, there's a sidebar with various navigation items like Dashboard, Applications, APIs, SSO Integrations, Connections (with sub-options for Database, Social, Enterprise, and Passwordless), Universal Login, Users, Rules, Hooks, Multi-factor Auth, Emails, Logs, Anomaly Detection, Extensions, and a '...' button. The main area is titled 'Configure social connections like Facebook, Twitter, Github and others so that you can let your users login with them.' It features a grid of social connection icons: Google (highlighted with a yellow arrow), LinkedIn, Bitbucket, Twitter, Vendav, Facebook, GitHub, PayPal, Amazon, YAHOO!, Microsoft, Dropbox, and 37signals. Each icon has a toggle switch next to it. A 'TRY' button is located above the Google icon. To the right, there's a 'Welcome to Auth0' message with a 'START THIS TUTORIAL' button.

## 5.Sign in with same account n you will get this output.

The screenshot shows a browser window with the URL [https://manage.auth0.com/tester/callback?connection=google-oauth2&code=o3L0O65kvM\\_E7cX#](https://manage.auth0.com/tester/callback?connection=google-oauth2&code=o3L0O65kvM_E7cX#). The page displays a JSON object representing a user profile:

```
{
  "sub": "google-saunth|10877120705469514498",
  "given_name": "Raju",
  "family_name": "Gupta",
  "nickname": "raju89_rg",
  "name": "Raju Gupta",
  "picture": "https://lh3.googleusercontent.com/-lwEuvhns/MAAMAMAM/ACewiQH-20GmHE2bAtexiPh6gXidN",
  "locale": "en-US",
  "updated_at": "2019-02-26T05:19:17.29Z"
}
```

Below the JSON, there's a message: 'If you can see this page, it means that your connection works.' and 'This is the user profile the application will receive:' followed by a 'TAKE ME TO THE DASHBOARD' button. The browser taskbar at the bottom shows the Windows logo, a search bar with 'Search the web and Windows', and several pinned icons.

## Practical No: 2

Date:

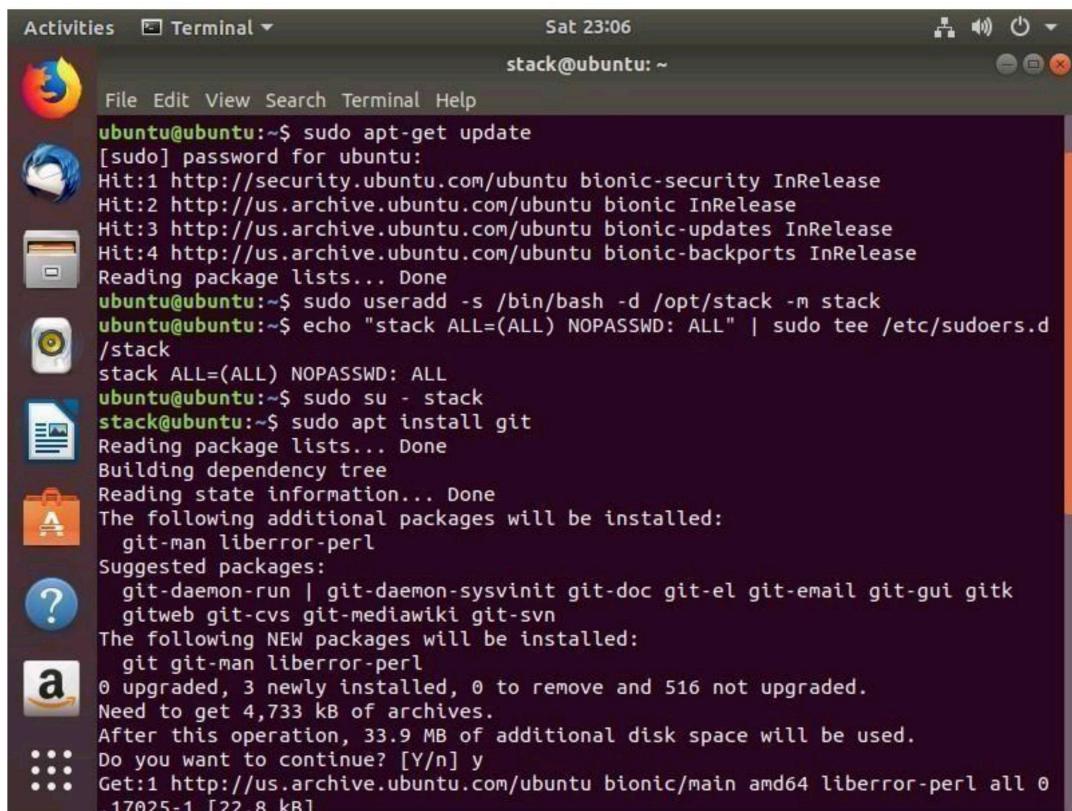
Aim: User Management in cloud

Description:

User Management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks, SaaS services and more. User management is a core part to any directory service and is a basic security essential for any organization. User management enables admins to control user access and on board and off-board users to and from IT resources. Subsequently a directory service will then authenticate, authorize, and audit user access to IT resources based on what IT admin had dictated.

Traditionally, User Management has been grounded with on-prem servers, databases, and closed private networks (VPN). However, recent trends are seeing a shift towards cloud-based identity and access management (IAM), granting administrators even greater control over digital assets.

## Procedure:

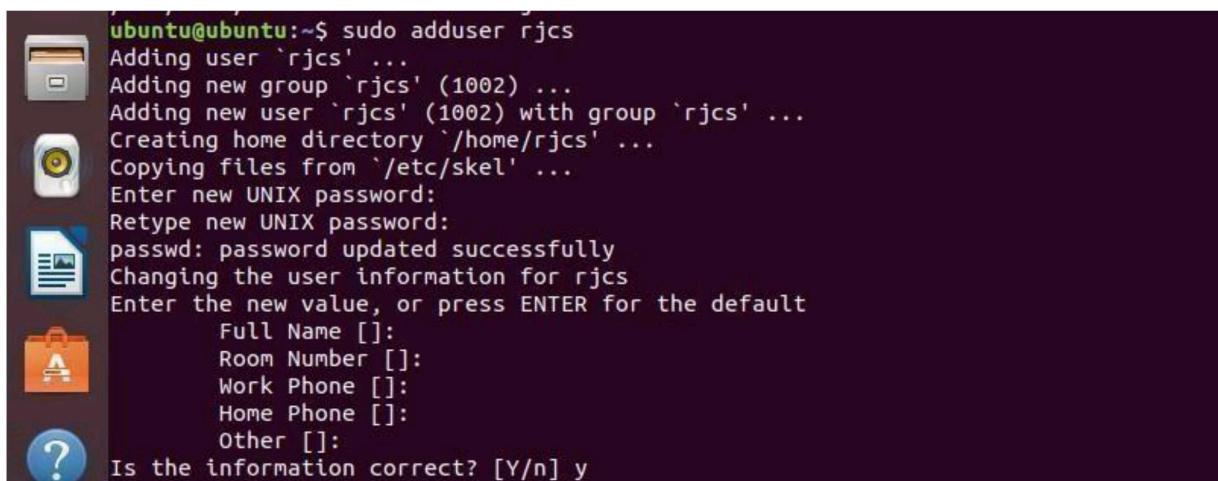


A screenshot of a Ubuntu desktop environment. A terminal window is open in the top panel, titled 'Terminal'. The terminal shows the following command-line session:

```
Activities Terminal ▾ Sat 23:06
stack@ubuntu: ~
File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo apt-get update
[sudo] password for ubuntu:
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
ubuntu@ubuntu:~$ sudo useradd -s /bin/bash -d /opt/stack -m stack
ubuntu@ubuntu:~$ echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
stack ALL=(ALL) NOPASSWD: ALL
ubuntu@ubuntu:~$ sudo su - stack
stack@ubuntu:~$ sudo apt install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 516 not upgraded.
Need to get 4,733 kB of archives.
After this operation, 33.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 liberror-perl all 0.17.0-25.1 [22.8 kB]
```

### 1: Adding a user on ubuntu

```
sudo adduser rjcs
```



A screenshot of a Ubuntu desktop environment. A terminal window is open in the top panel, titled 'Terminal'. The terminal shows the following command-line session:

```
ubuntu@ubuntu:~$ sudo adduser rjcs
Adding user `rjcs' ...
Adding new group `rjcs' (1002) ...
Adding new user `rjcs' (1002) with group `rjcs' ...
Creating home directory `/home/rjcs' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for rjcs
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n] y
```

To Add a system user rjcs run the ollowing command

```
ubuntu@ubuntu:~$ sudo adduser --system rjcs
Adding system user `rjcs' (UID 130) ...
Adding new user `rjcs' (UID 130) with group `nogroup' ...
```

Login as rjcs user by using following command

```
ubuntu@ubuntu:~$ su - rjcs
Password:
rjcs@ubuntu:~$
```

```
rjcs@ubuntu:~$ whoami
rjcs
rjcs@ubuntu:~$
```

## 2: Adding a group on ubuntu

```
ubuntu@ubuntu:~$ sudo addgroup student
Adding group `student' (GID 1003) ...
Done.
ubuntu@ubuntu:~$
```

## 3: Adding a User to a group on ubuntu

```
ubuntu@ubuntu:~$ sudo usermod -aG student rjcs
ubuntu@ubuntu:~$
```

You can login as a rjcs and run the following command.

```
ubuntu@ubuntu:~$ su - rjcs
Password:
rjcs@ubuntu:~$
```

```
rjcs@ubuntu:~$ groups
rjcs student
rjcs@ubuntu:~$
```

#### 4: Removing the user from a group on ubuntu

```
ubuntu@ubuntu:~$ sudo deluser rjcs student
Removing user `rjcs' from group `student' ...
Done.
ubuntu@ubuntu:~$
```

```
a ubuntu@ubuntu:~$ su - rjcs
Password:
rjcs@ubuntu:~$ groups
rjcs
rjcs@ubuntu:~$
```

#### 5: Removing a user on ubuntu

```
a ubuntu@ubuntu:~$ sudo deluser rjcs
Removing user `rjcs' ...
Warning: group `rjcs' has no more members.
Done.
ubuntu@ubuntu:~$
```

#### 6: Deleting a group on ubuntu

```
ubuntu@ubuntu:~$ sudo delgroup student
Removing group `student' ...
Done.
ubuntu@ubuntu:~$
```

#### 7: Listing all the users on ubuntu

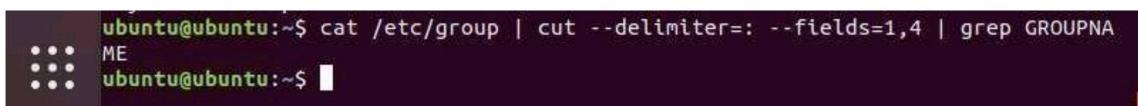
```
ubuntu@ubuntu:~$ cut --delimiter=: --field=1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-network
systemd-resolve
syslog
messagebus
aot
```

**8: Listing all the groups on ubuntu**



```
ubuntu@ubuntu:~$ cut --delimiter=: --fields=1 /etc/group
root
daemon
bin
sys
adm
tty
disk
lp
mail
news
uucp
man
proxy
kmem
dialout
fax
voice
cdrom
floppy
tape
sudo
audio
dip
www-data
backup
operator
```

**9: Listing all the user in a group on ubuntu**



```
ubuntu@ubuntu:~$ cat /etc/group | cut --delimiter=: --fields=1,4 | grep GROUPNAME
ME
ubuntu@ubuntu:~$
```

Practical No: 5

AIM: Study cloud security Management.

Description:

1. Ensure effective governance and compliance  
 Most organizations have security, privacy and compliance policies and procedures to protect their IP and assets. In addition to this, organizations should establish a formal governance framework that outlines chains of responsibility, authority and communication. This describes the roles and responsibilities of those involved.

2. Audit operation and business processes.

It is important to audit the compliance of IT system vendors that host the applications and data in the cloud. There are three important areas that need to be audited by cloud service customers internal control environment of a cloud service provider, access to corporate audit trail, and cloud service facilities security.

3. Manage people, roles and identities  
 Using the cloud means there will be employees from cloud service that can access the data and applications, as well as employees of the organization that perform operations on the providers system. Organizations must ensure that provider has processes that govern who has access to consumer data and applications. The provider must allow the customer to assign and manage roles and authorization for each of their users. The provider must have secure system.

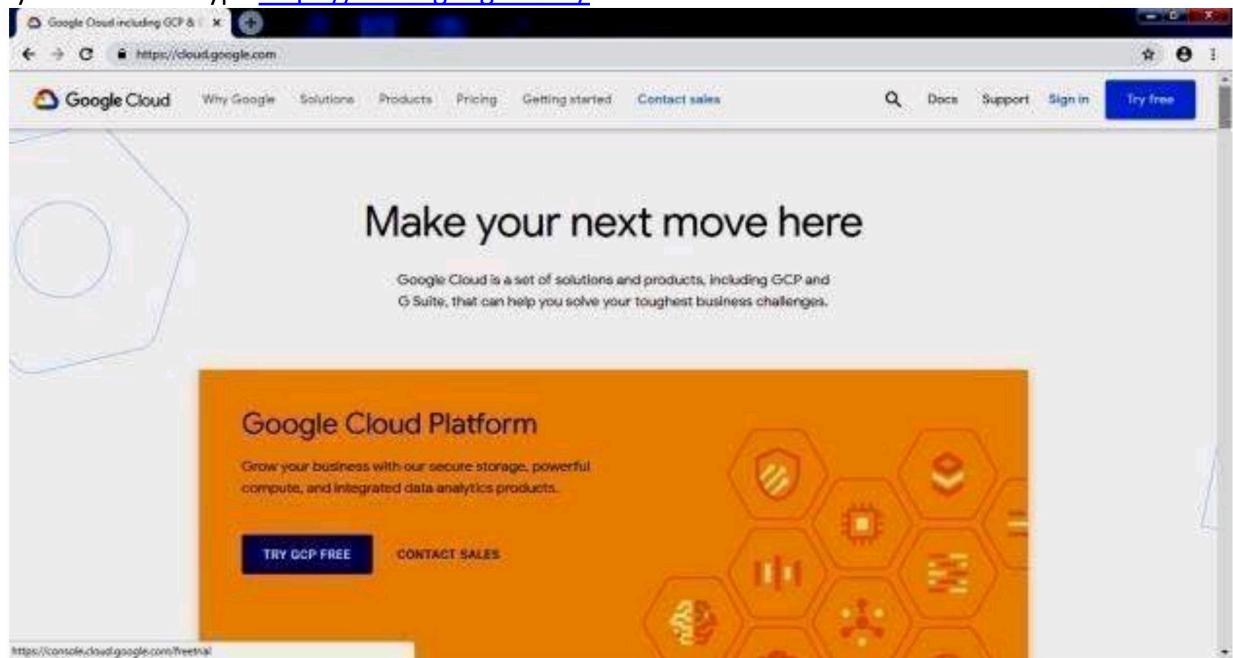
4. Proper protection of data

Data is the core of all IT security concerns for any organization. Cloud computing does not change this concern but brings new challenges because of nature of cloud computing.

## **Procedure:**

### **STEPS:**

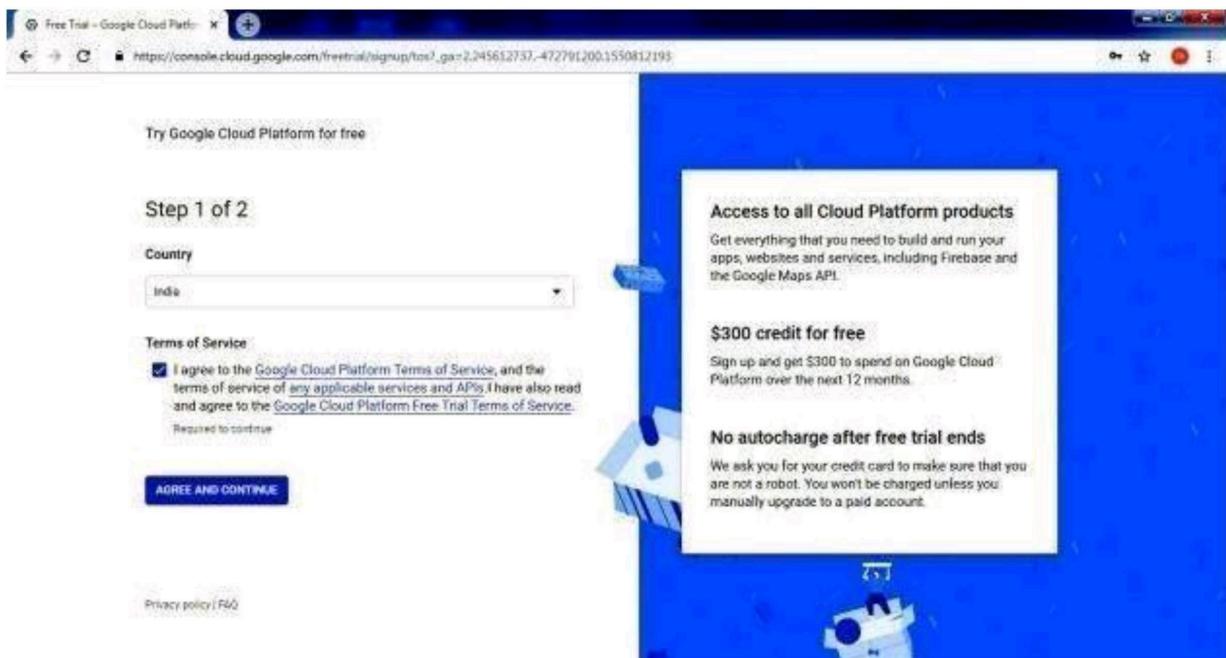
Open any browser and type <https://cloud.google.com/> and then click on TRY GCP FREE



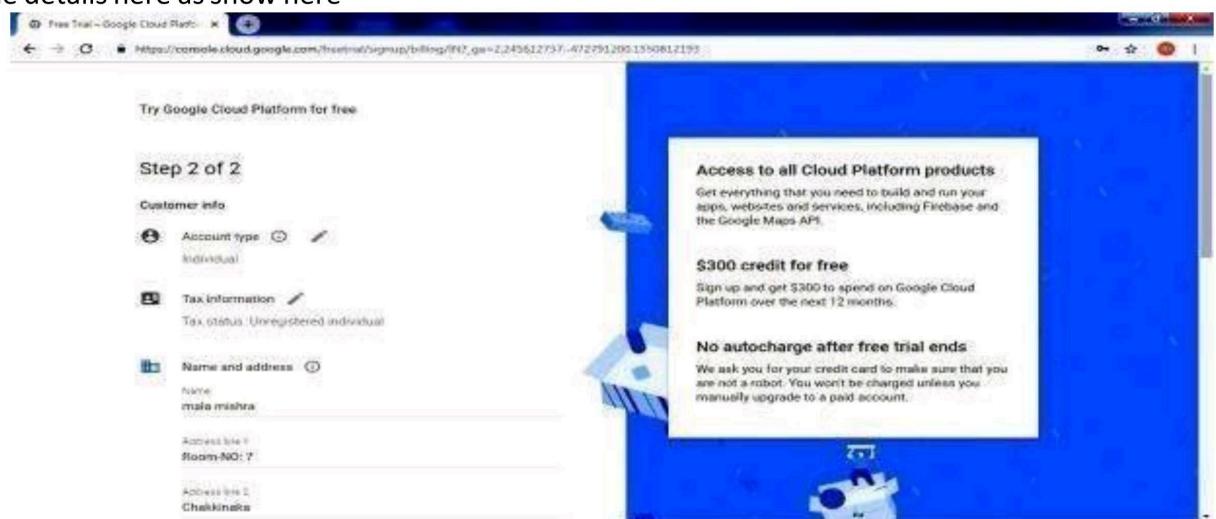
After click on TRY GCP FREE your email page is open for sign in , enter your email-id and password.



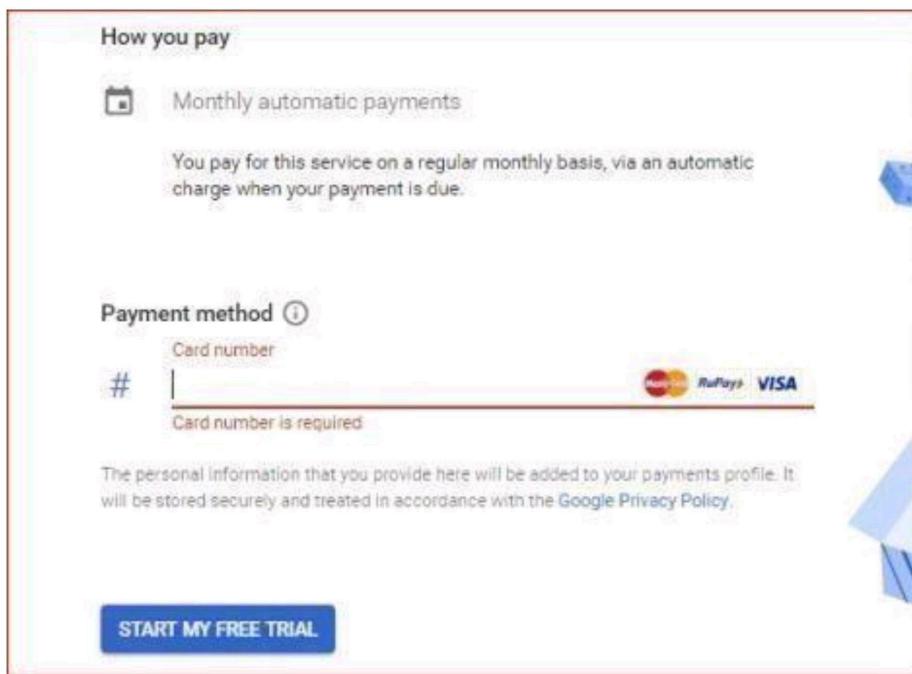
After Login your account it will ask to accept the service, then click on AGREE AND CONTINUE



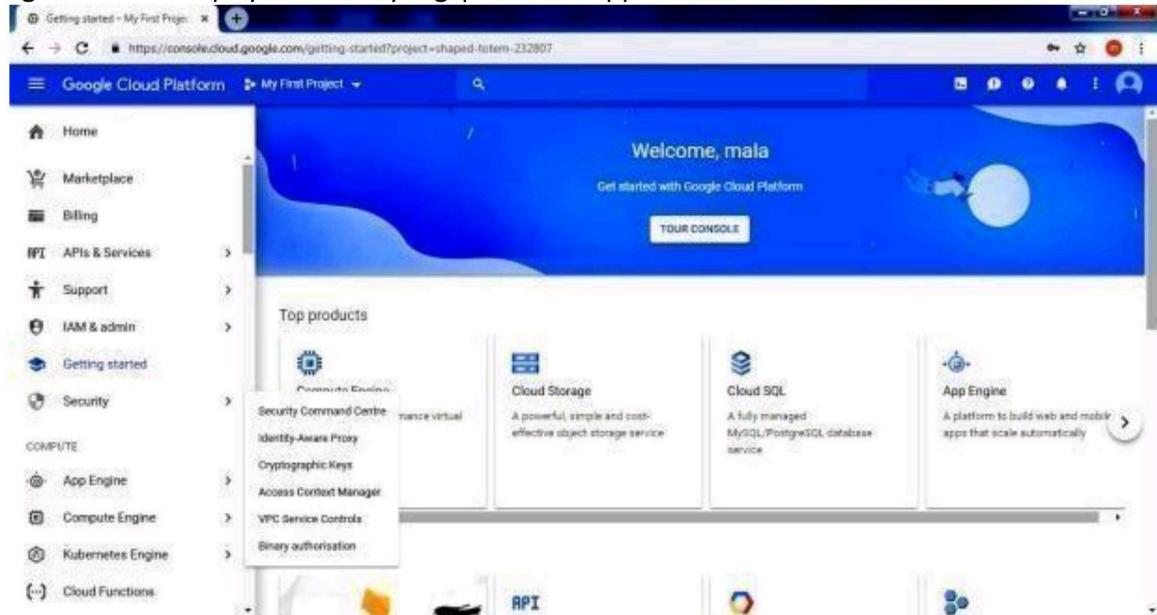
Enter the details here as show here



Enter the card detail here to make payment and then click on START MY FREE TRIAL.



After doing the above steps your free tryer gcp window appear.



To check **Payment Overview**, go to **Billing**

The top screenshot shows the Google Cloud Platform dashboard for 'My First Project'. It includes sections for Project Info (Project name: My First Project, Project ID: 186724114731, Project number: 218724114731), APIs & Services (with a note about no data available for the selected time range), Resources (no resources listed), and Compute Engine (with a note about trace data for the last 7 days). The bottom screenshot shows the 'Billing' section of the dashboard, specifically the 'Overview' tab. It displays payment information (Your payment information could not be processed. Visit the payment overview page to make sure that your payment information is up to date and to pay any outstanding charges), credits (₹21,312.75, Credits remaining: Out of ₹21,312.75), and projects linked to the billing account (My First Project, Project ID: shaped-totem-232807).

Now Click on **Payment Overview**.

Billing Overview My Billing Account RENAME BILLING ACCOUNT CHANGE BILLING ACCOUNT HIDE INFO PANEL

Billing account overview Payment overview

Your payment information could not be processed. Visit the payment overview page to make sure that your payment information is up to date and to pay any outstanding charges.

Billing account ID: 01FF7E-9CCF4F-3BD5F7

Credits

₹21,312.75 Credits remaining Out of ₹21,312.75

364 Days remaining Ends 24 Feb 2020

Projects linked to this billing account

Project name Project ID

My First Project shaped-totem-232807

My Billing Account

PERMISSIONS

Add members Select a role Add

Search members Filter by name or role

Billing Account Administrator (1 member)  
Authorized to view and manage all aspects of billing accounts

Click on verify Now.

Google Cloud Platform

Billing Overview My Billing Account

Overview Budgets & alerts Transactions Billing export Payment settings Payment method Reports

Billing account overview Payment overview

You haven't completed the verification process for RuPay --- 0291. VERIFY NOW

Your balance ₹0.00 PAY EARLY

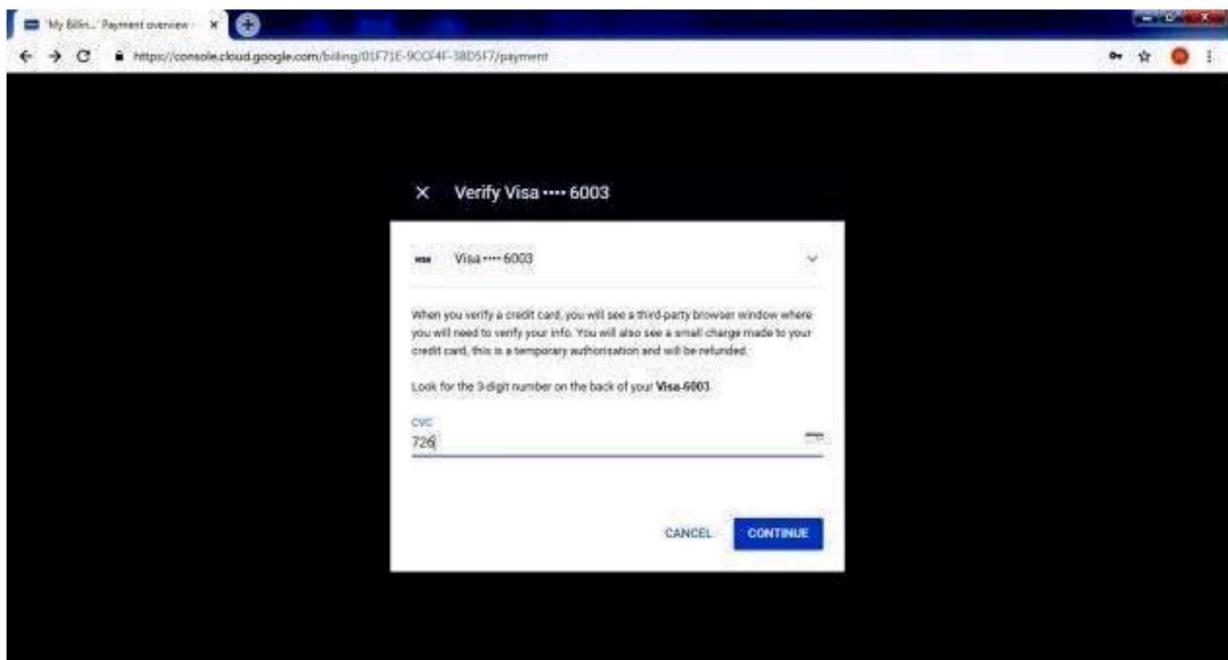
Automatic payments

Transactions You don't have any transactions yet.

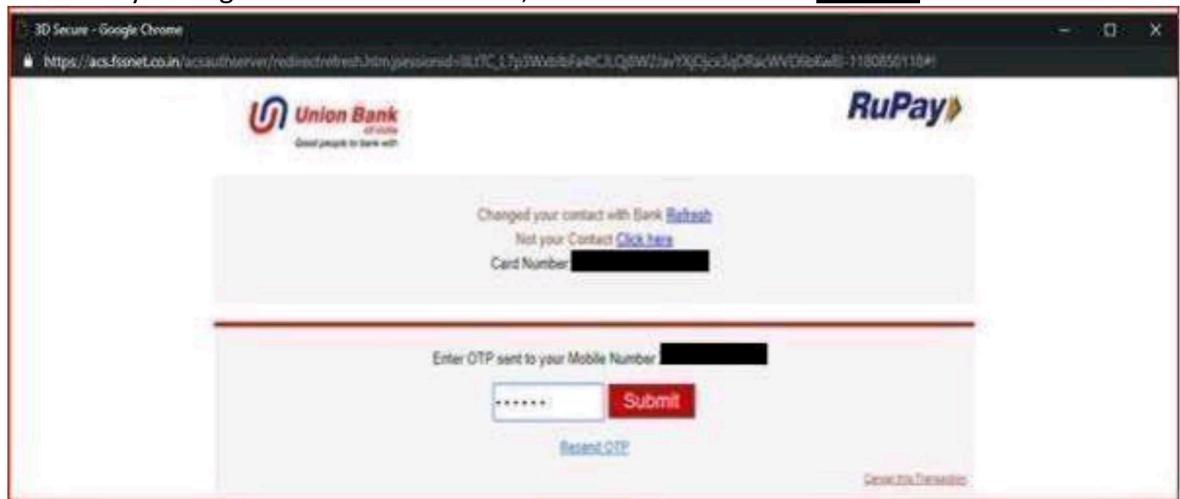
How you pay

RuPay --- 0291 Expires 08/24

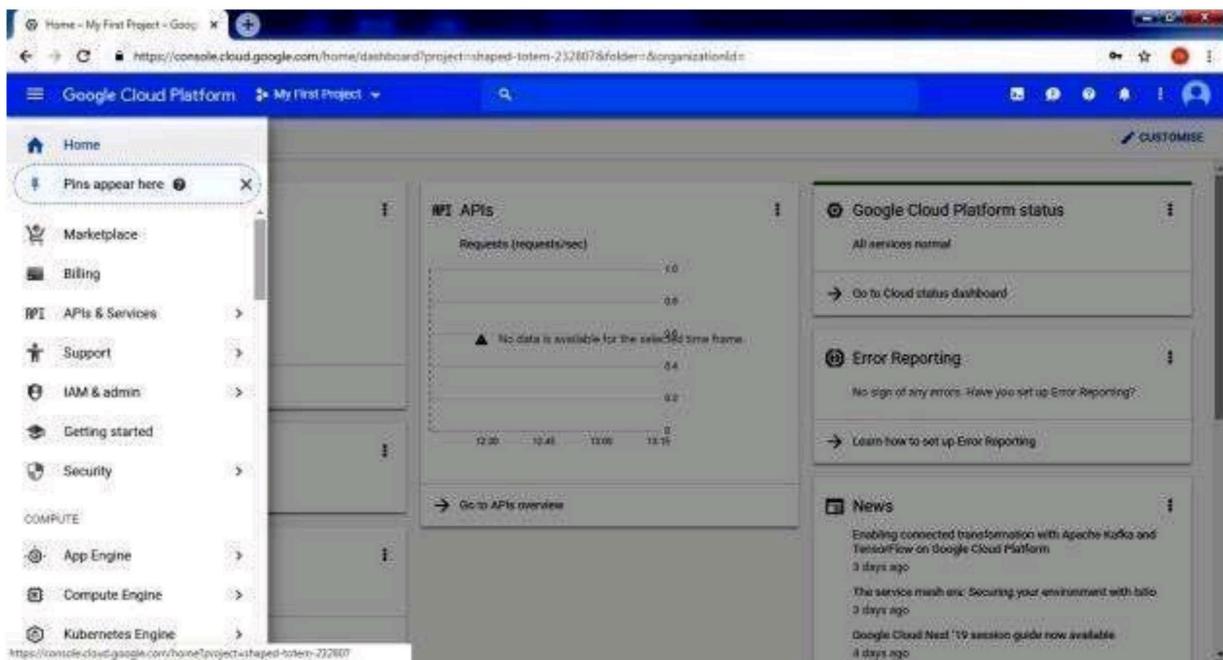
After it will ask for CVV number. Enter cvc number, click on CONTINUE.



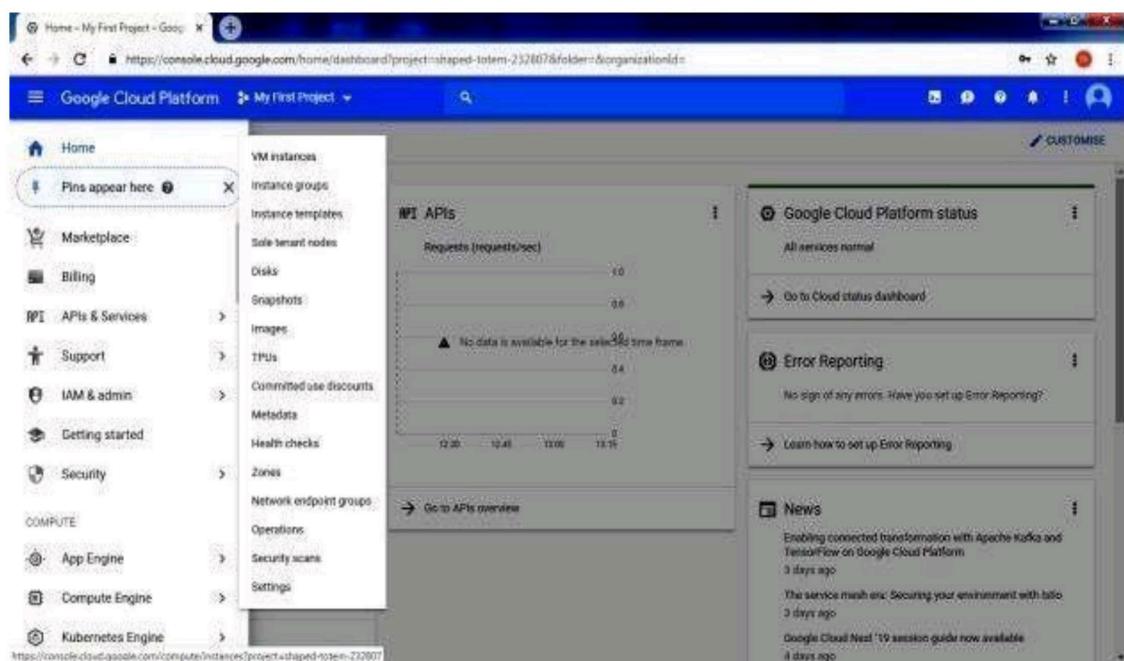
It send the OTP on your registered mobile number, enter number click on **SUBMIT**.



Now come back to **HOME**→**Compute Engine**→click on **VM Instances**.

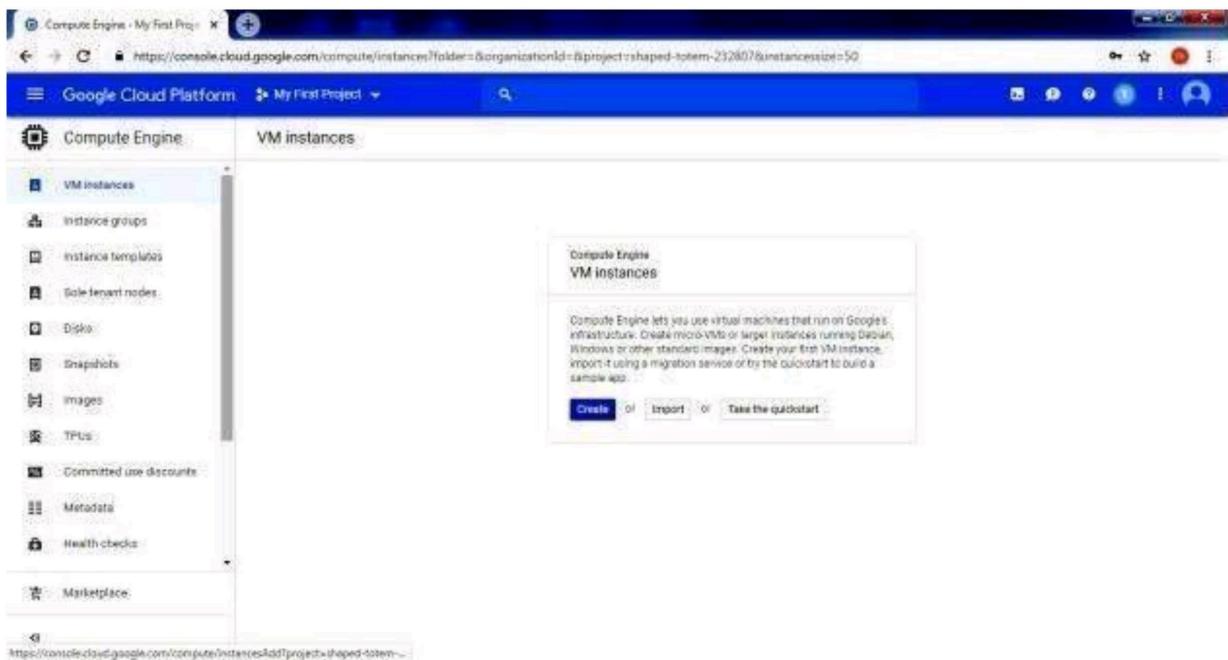


The screenshot shows the Google Cloud Platform Home dashboard for a project named "My First Project". The left sidebar includes links for Marketplace, Billing, APIs & Services, Support, IAM & admin, Getting started, Security, App Engine, Compute Engine, and Kubernetes Engine. The main content area displays the "APIs" section with a chart showing requests per second over time, stating "No data is available for the selected time frame". It also includes links to "Go to APIs overview" and "Go to Cloud status dashboard". The right sidebar features "Google Cloud Platform status" (All services normal), "Error Reporting" (No sign of any errors), and "News" (articles about Apache Kafka and TensorFlow, service mesh, and Google Cloud Next '19 sessions).

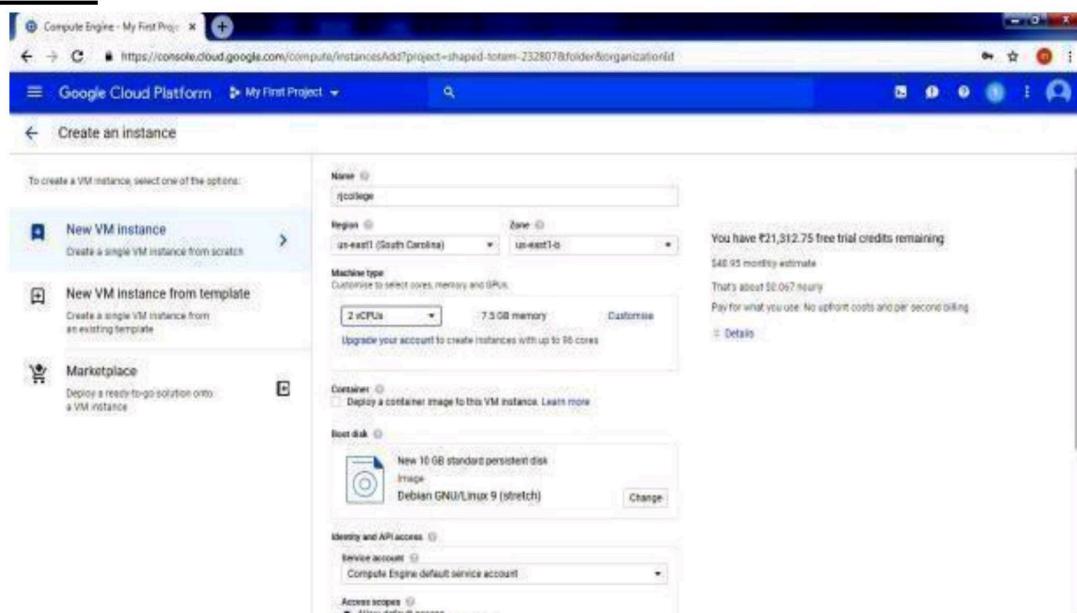


The screenshot shows the Google Cloud Platform Compute Instances dashboard for the same project. The left sidebar lists VM instances, instance groups, instance templates, sole-tenant nodes, Disks, Snapshots, Images, TPLs, Committed use discounts, Metadata, Health checks, Zones, Network endpoint groups, Operations, Security scans, and Settings. The main content area displays the "APIs" section with the same request chart and links. The right sidebar remains identical to the Home dashboard.

Now click on **CREATE**.



Give your instance name and you can give your Machine CPU to 2vCPUs to running better ,then click on CREATE.



**Identity and API access**

**Service account**  
Compute Engine default service account

**Access scopes**

- Allow default access
- Allow full access to all Cloud APIs
- Set access for each API

**Firewall**  
Add tags and firewall rules to allow specific network traffic from the Internet.

- Allow HTTP traffic
- Allow HTTPS traffic

**Management, security, disks, networking, sole tenancy**

Your free trial credit will be used for this VM instance. GCP Free Tier

**Create** **Cancel**

Now here your instance is created, select the instance and from SSH select Open in new Window.

The screenshot shows the Google Cloud Platform Compute Engine interface. The left sidebar has options like VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots, Images, and TPUs. The main area is titled 'VM instances' and shows a table with one row:

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect	PERMISSIONS	MONITORING	LABELS
rjcollege	us-east1-b			10.142.0.2	34.73.137.6 (nyc3)	SSH			

A message at the bottom right says 'Please select at least one resource.'

The screenshot shows the Google Cloud Platform Compute Engine interface. On the left, a sidebar lists various resources: VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots, Images, TPUs, Committed use discounts, Metadata, Health checks, and Marketplace. The main area displays a table of VM instances with columns for Name, Zone, Recommendation, In use by, Internal IP, External IP, and Connect. The 'rjcollege' instance is selected, and a context menu is open over it, listing options such as 'Open in browser window', 'Open in browser window on custom port', 'View gcloud command', and 'Use another SSH client'. The 'PERMISSIONS' tab is currently active in the top navigation bar.

Now new Command line window will appear. Here I had done some simple command of linux you can try more command here.

```
rjmalai809@rjcollege: ~ - Google Chrome
https://ssh.cloud.google.com/projects/shaped-totem-232807/zones/us-east1-b/instances/rjcollege?authuser=0&hl=en_GB&projectNu...
Connected, host fingerprint: ssh-rsa 0 36:82:1F:3:c6:93:50:37:3E:6C:20:7C:45:B6:CE
:00:0B:C1:73:65:12:CA:89:51:27:E2:92:9E:70:FC:57:1E:CE
Linux rjcollege 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Feb 25 07:58:12 2019 from 173.194.93.96
rjmalai809@rjcollege:~$ mkdir tybsc
rjmalai809@rjcollege:~$ ls
gcp rjsty tybsc tyos
rjmalai809@rjcollege:~$
```

For stoping the instance click square symbol.

The screenshot shows the Google Cloud Platform Compute Engine interface again. The 'rjcollege' instance is now listed as 'STOPPED' in the status column. The 'STOP' button for this instance is highlighted in red, while the 'START' button is greyed out. The rest of the interface remains the same, with the sidebar and other instances visible.