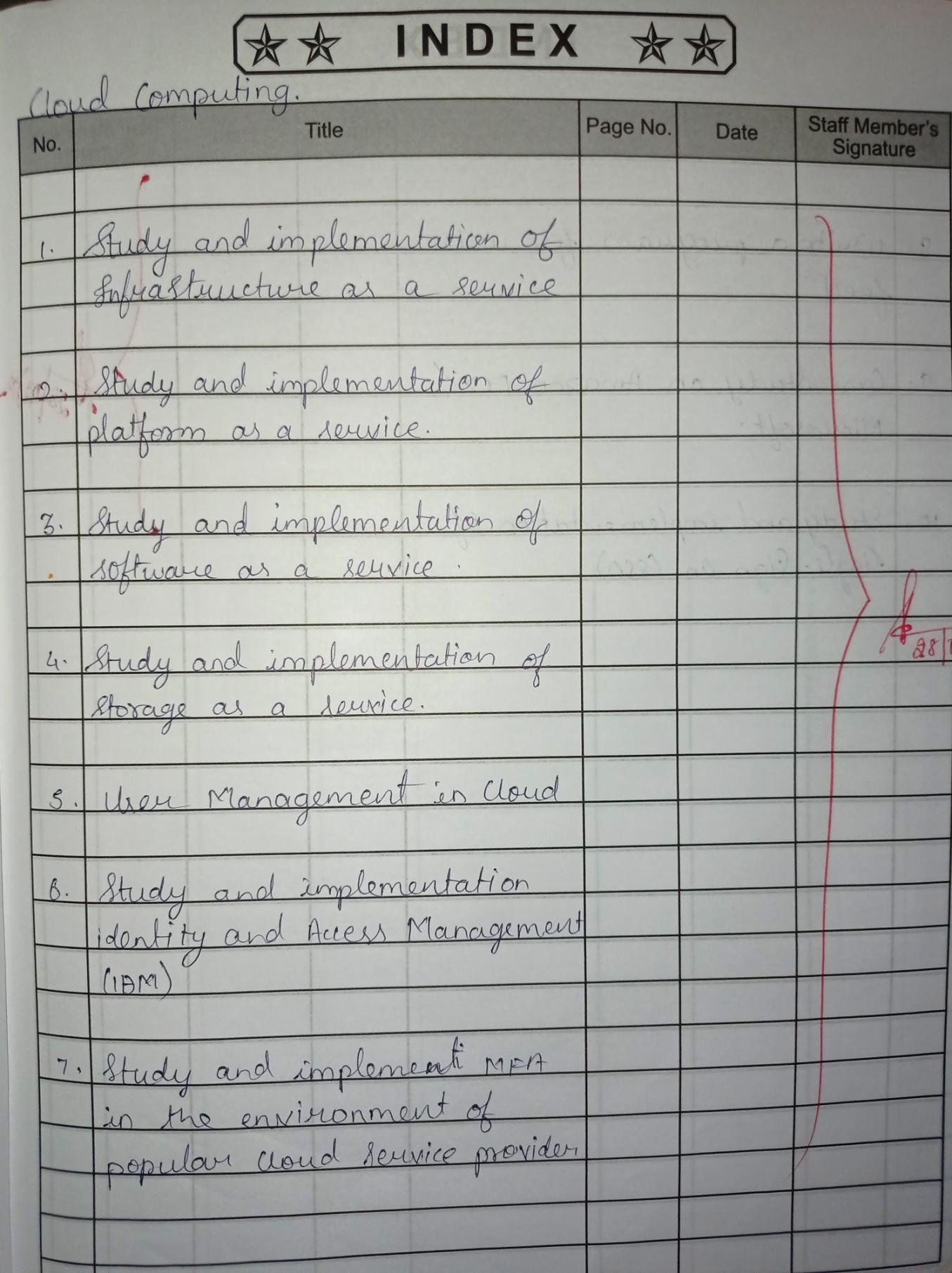
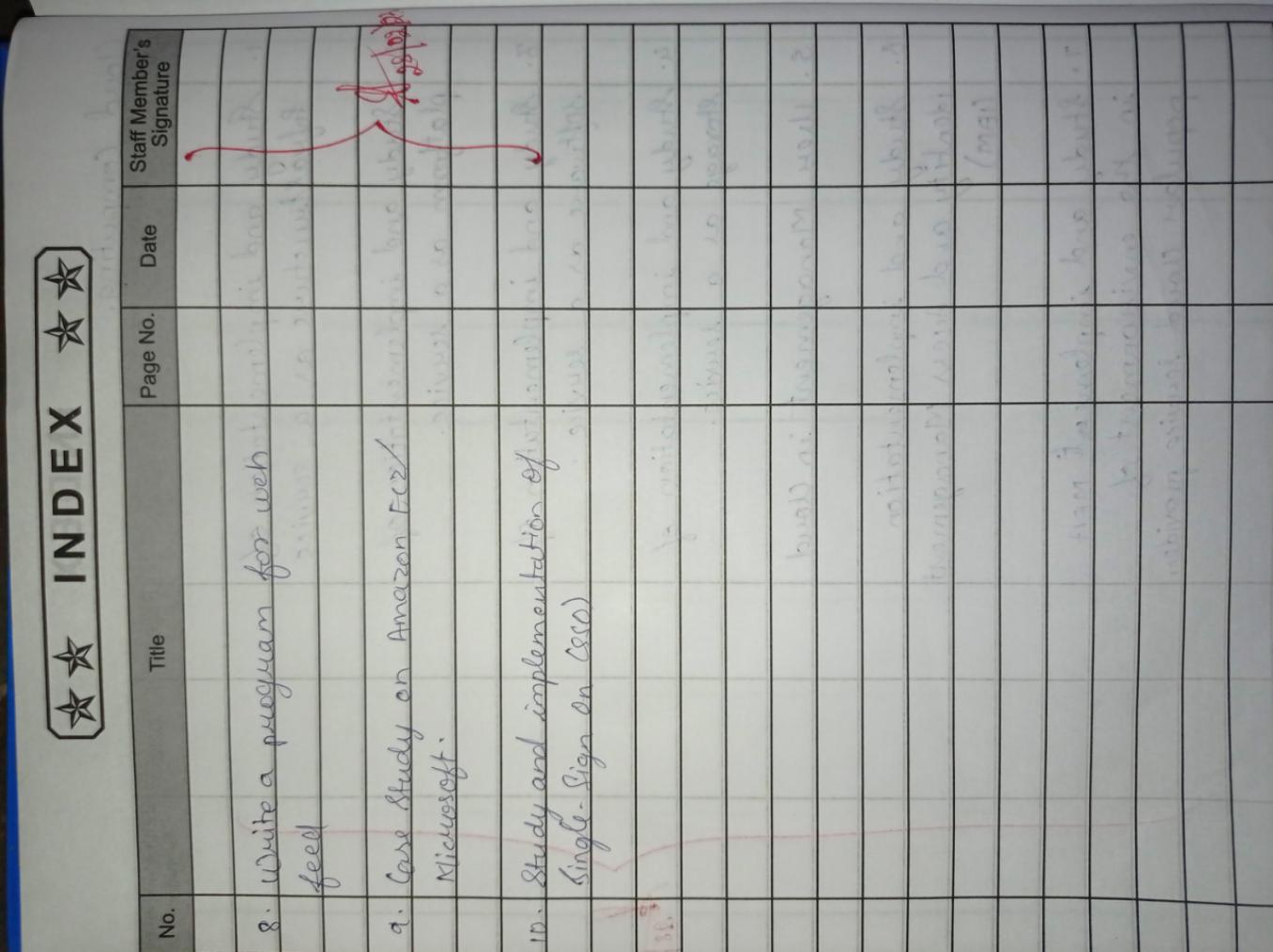


# Index Page

****

****

**Practical No:01**

# Aim: Study and implementation of infrastructure as a service.

**Theory:**

**Definition:** Infrastructure as a service (IaaS) is a cloud computing offering in which a vendor provides users access to computing resources such as storage, networking, and servers. Organizations use their own platforms and applications within a service provider’s infrastructure.

Iaas is also known as Hardware as a Service (HaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources.

Customers access these resources on the Internet using a pay-as-per use model. ---In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration.

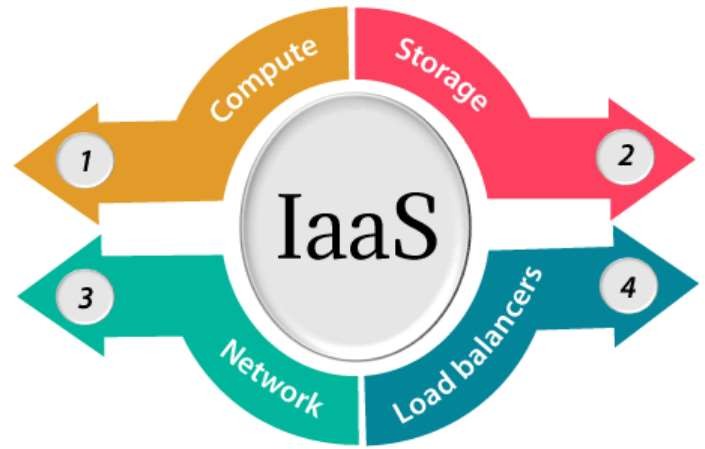
The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

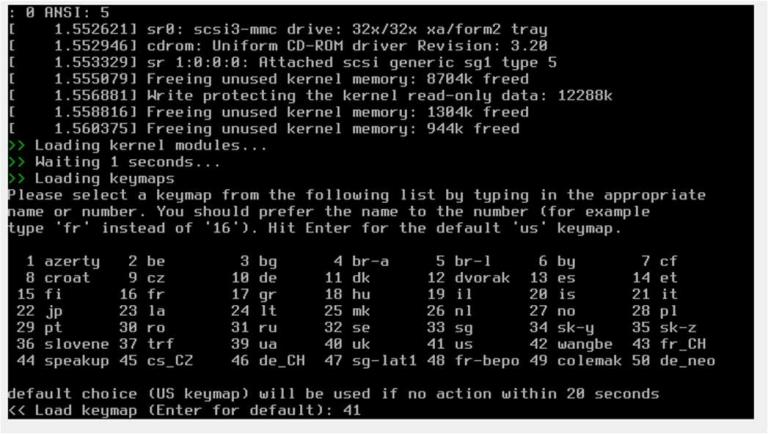
IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud. IaaS provider provides the following services –

Compute: Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.

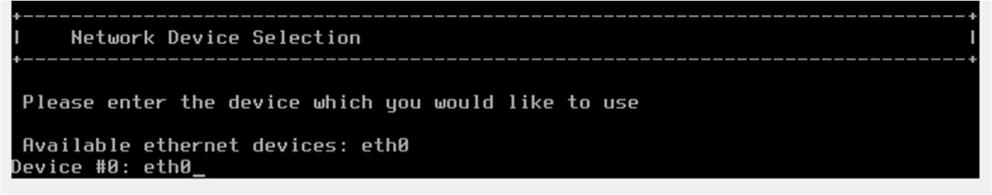
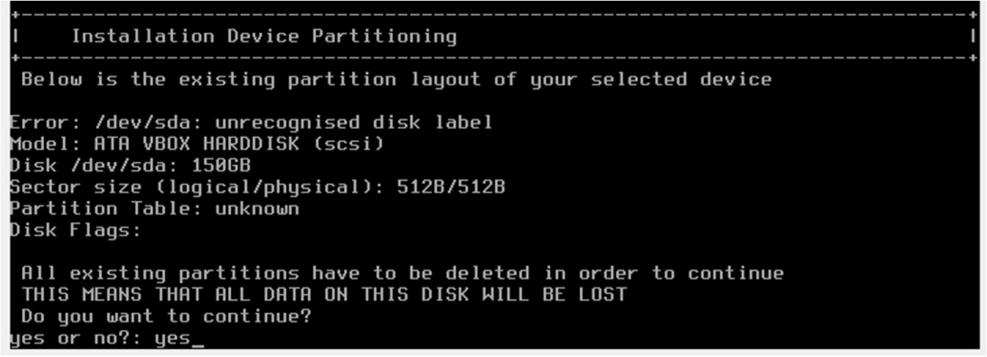
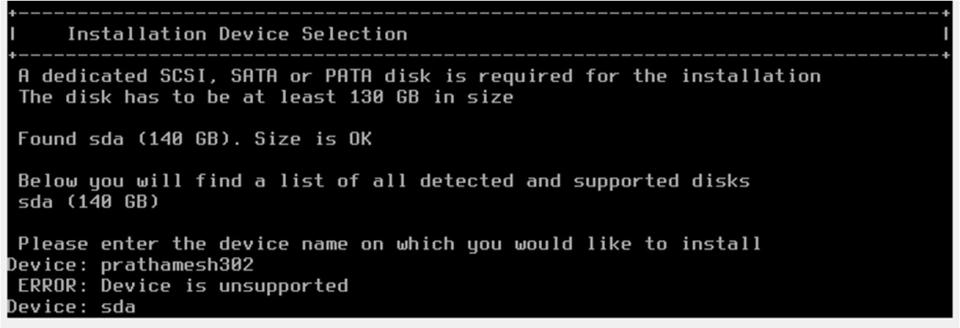
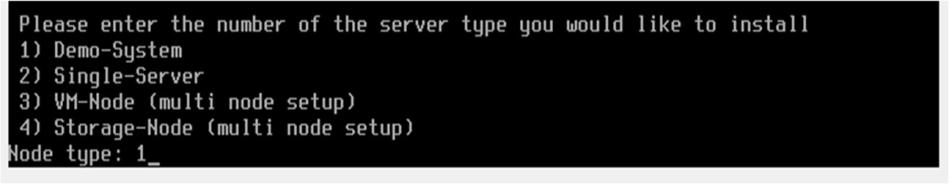
* Storage: IaaS provider provides back-end storage for storing files.
* Network: Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
* Load balancers: It provides load balancing capability at the infrastructure layer.

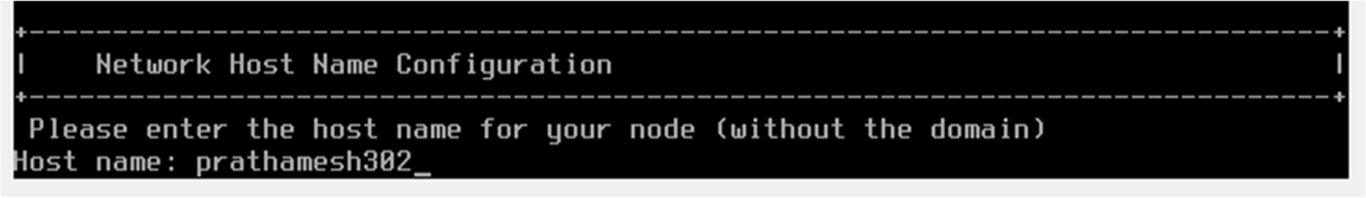


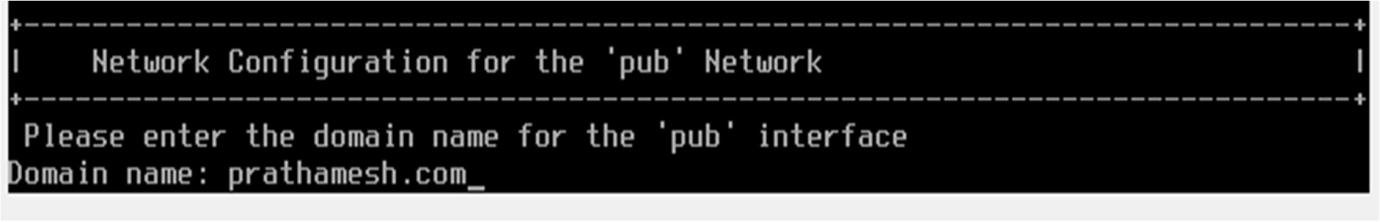
**Procedure:**

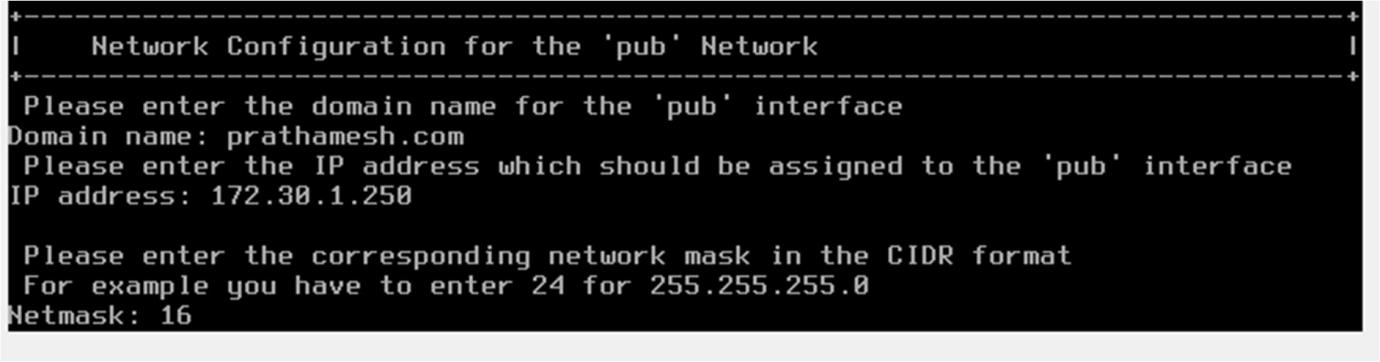


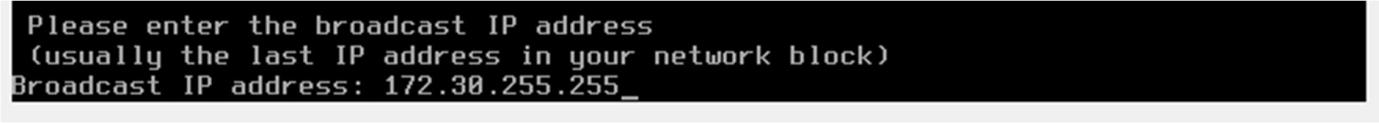


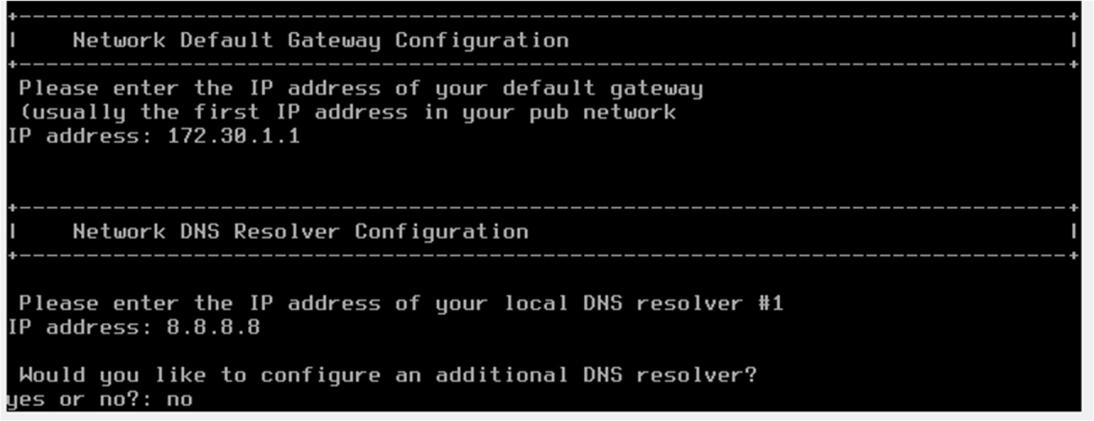


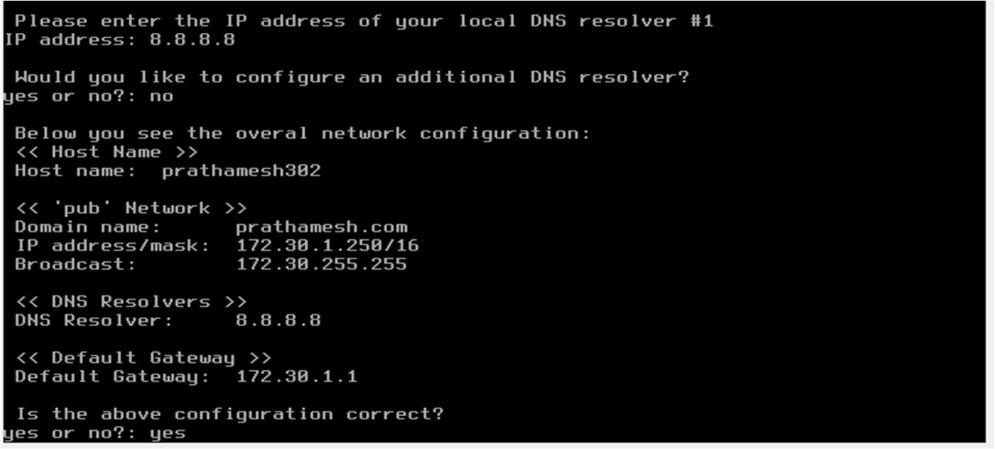


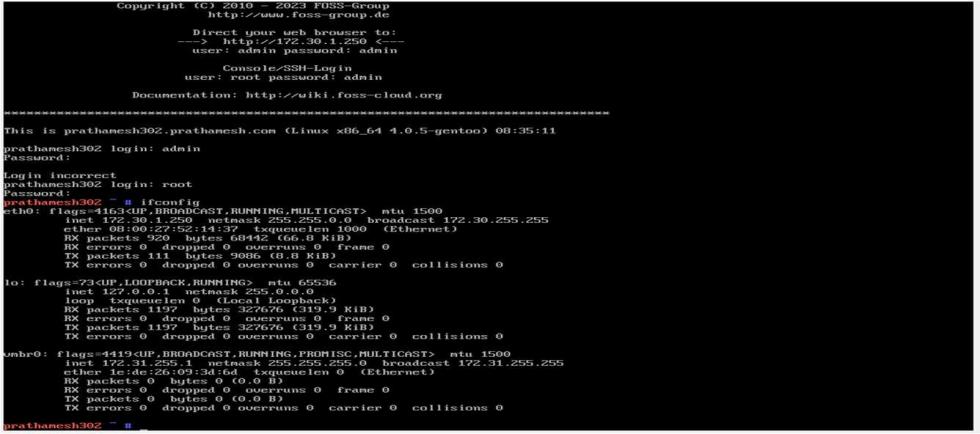


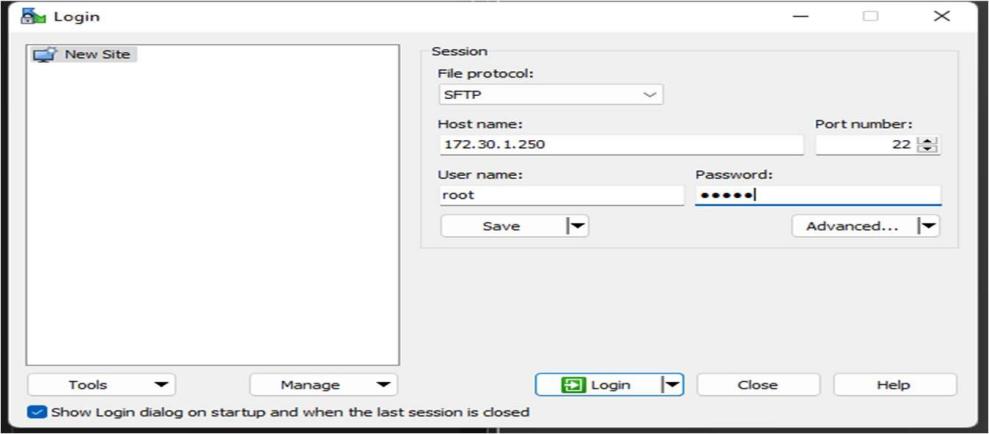


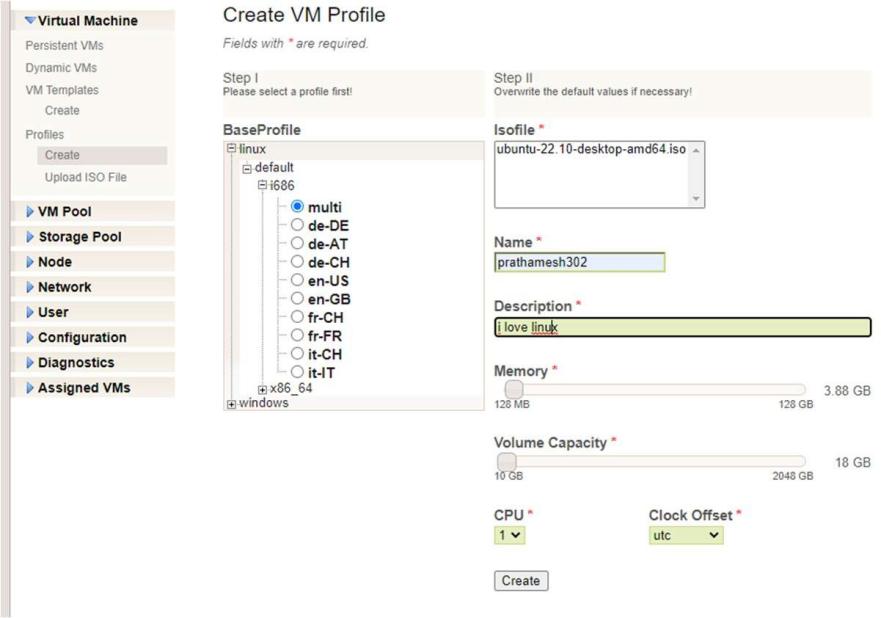
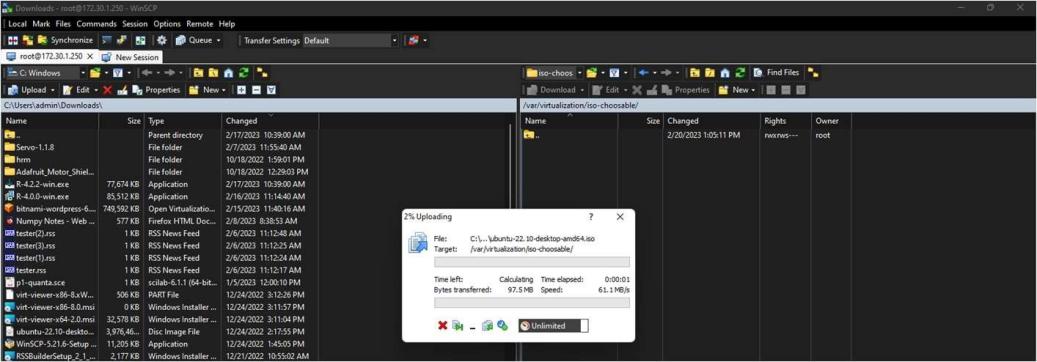


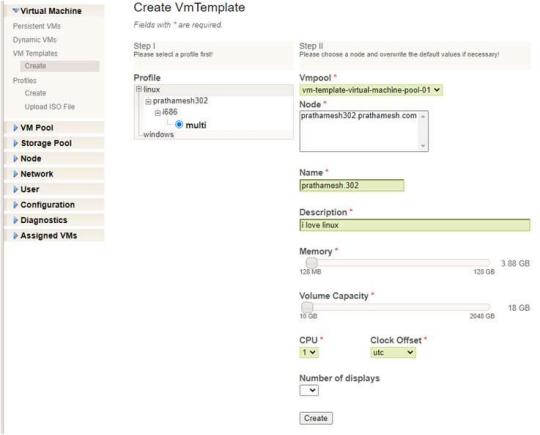








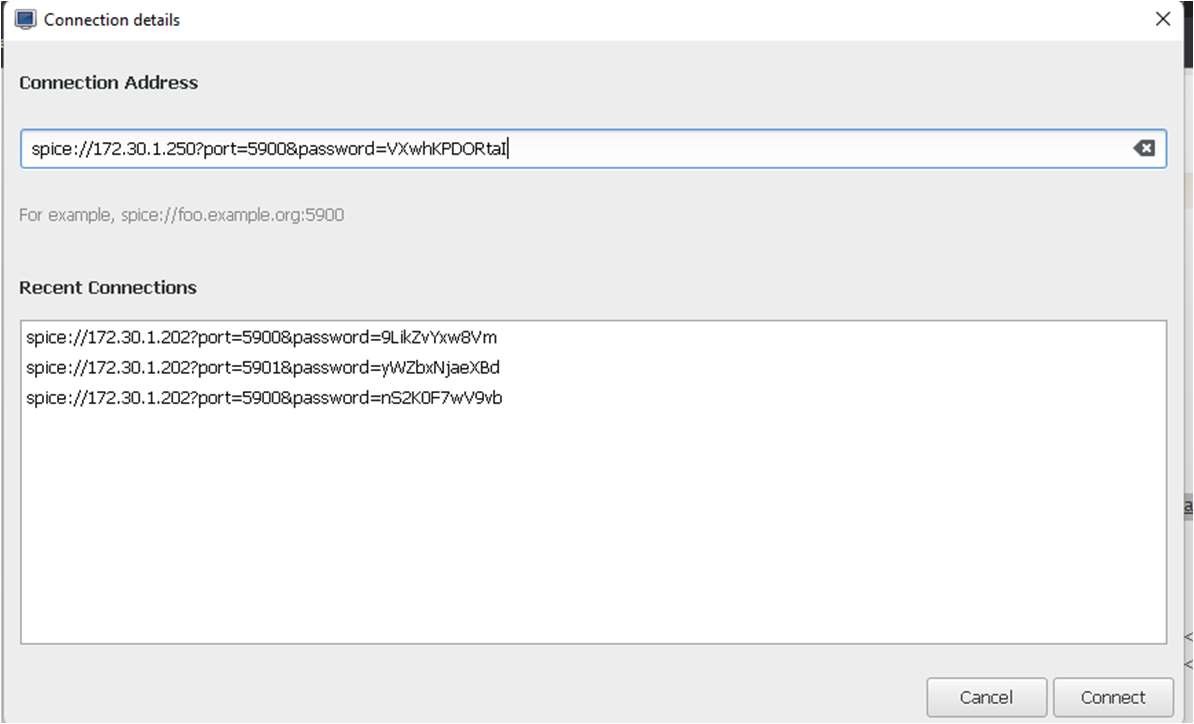








Remote viewer



**Conclusion:** Hence Successfully Studied and implementation of infrastructure as a service.

# Practical No:02

**Aim: Study and implementation of Platform as a Service**

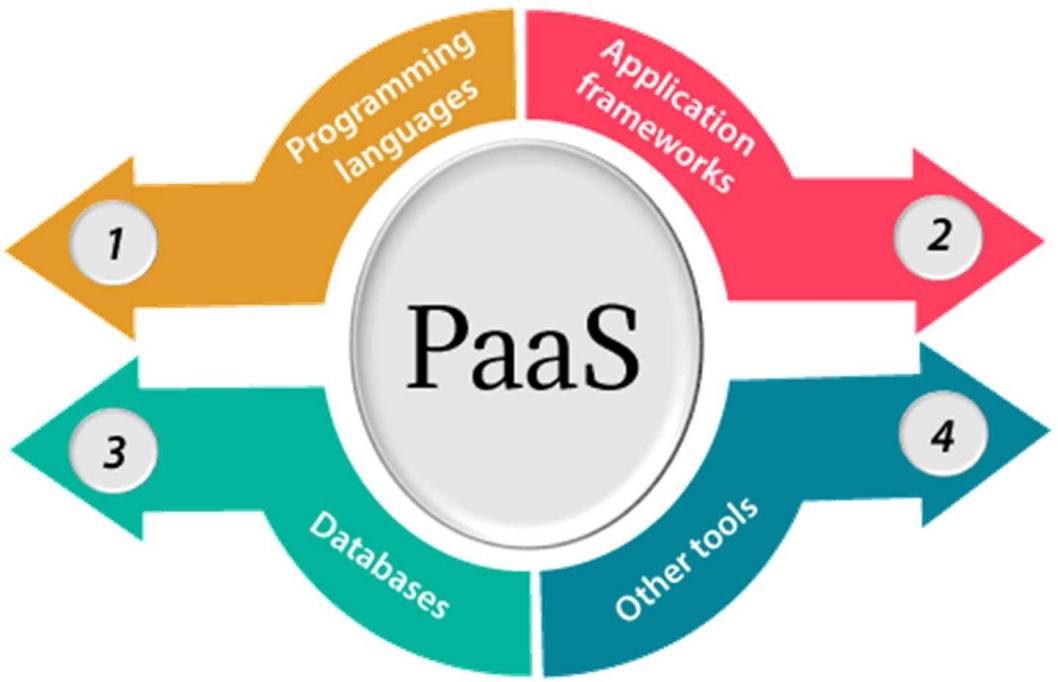
**Theory:**

Platform as a Service (PaaS) provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. You can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back-end scalability is managed by the cloud service provider, so end- users do not need to worry about managing the infrastructure.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.

**Example:** Google App Engine, Force.com, Joyent, Azure.

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:



1. Programming languages

PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

1. Application framework:

PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

1. Databases

PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

1. Other tools

PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

**Advantages of PaaS**

There are the following advantages of PaaS -

1. Simplified Development

PaaS allows developers to focus on development and innovation without worrying about infrastructure management.

1. Lowerrisk Learn more

No need for up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.

1. Prebuilt business functionality

Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.

1. Instant community

PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.

**Conclusion:** Hence Successfully Studied and implementation of Platform as a Service

**Practical No:03**

**Aim:** Implement Software as a Service

**Theory:**

Software as a Service | SaaS

SaaS is also known as "On-Demand Software". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

There are the following services provided by SaaS providers -

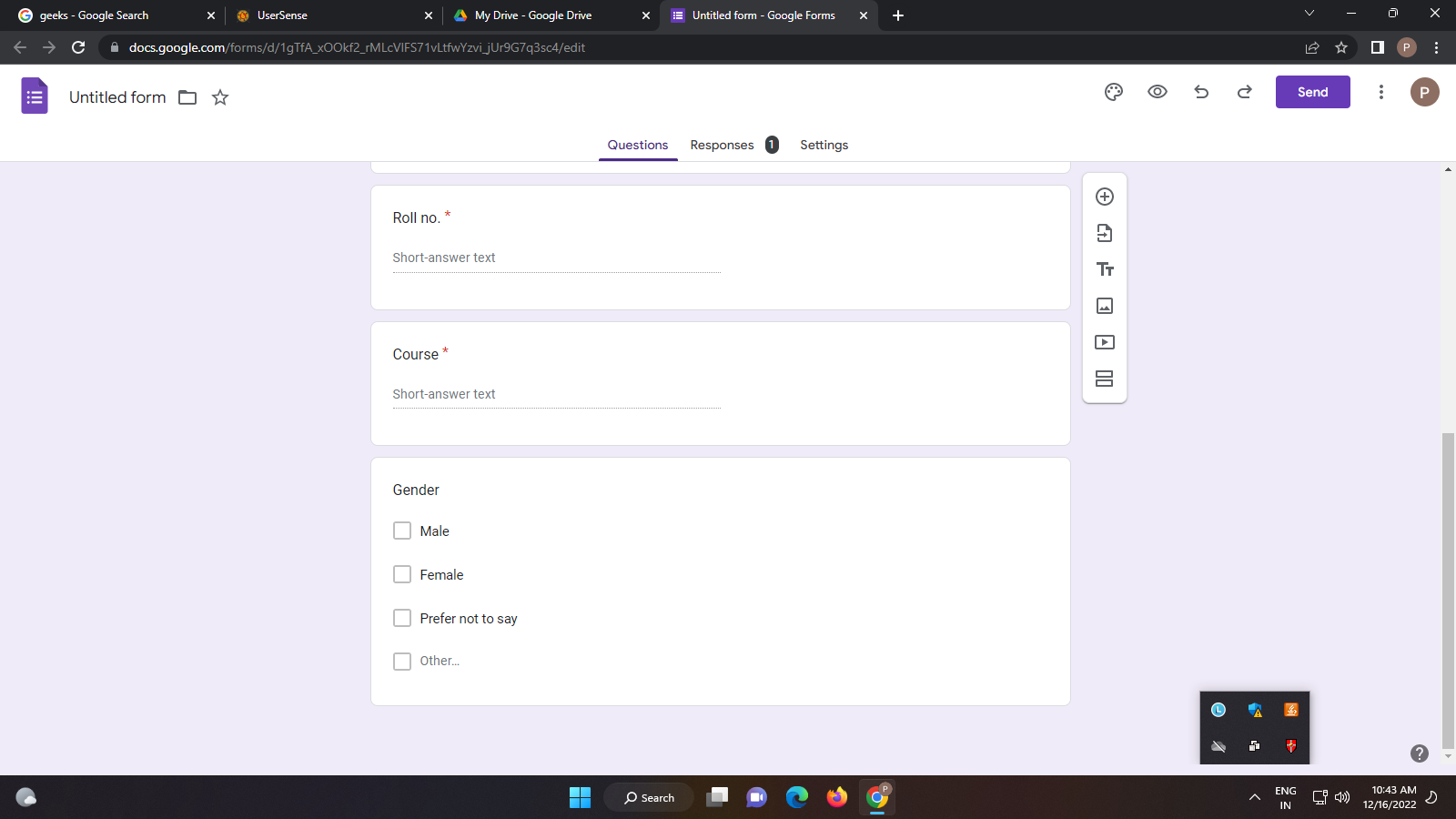
Business Services - SaaS Provider provides various business services to start-up the business. The SaaS business services include ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), billing, and sales.

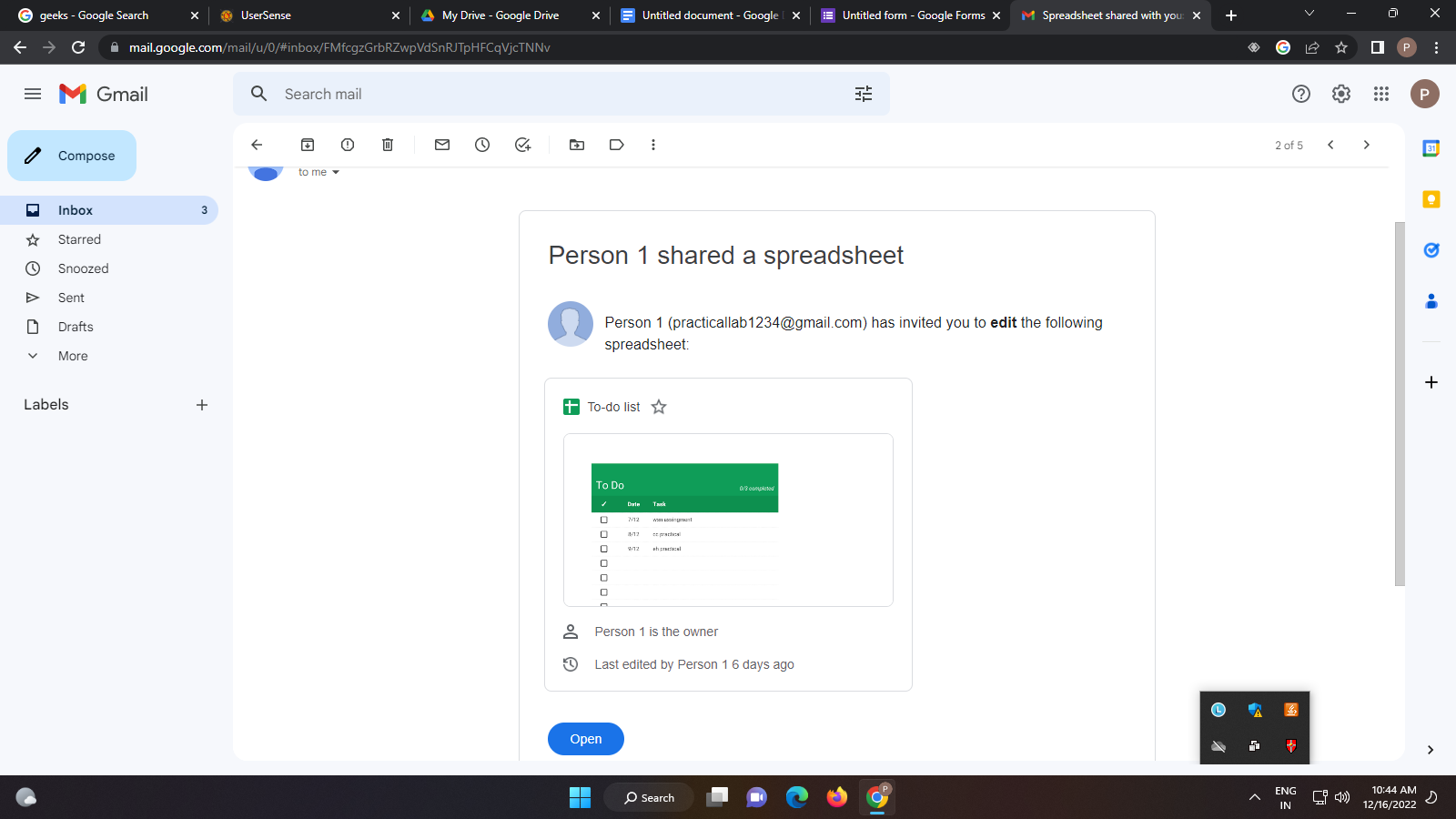
Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.

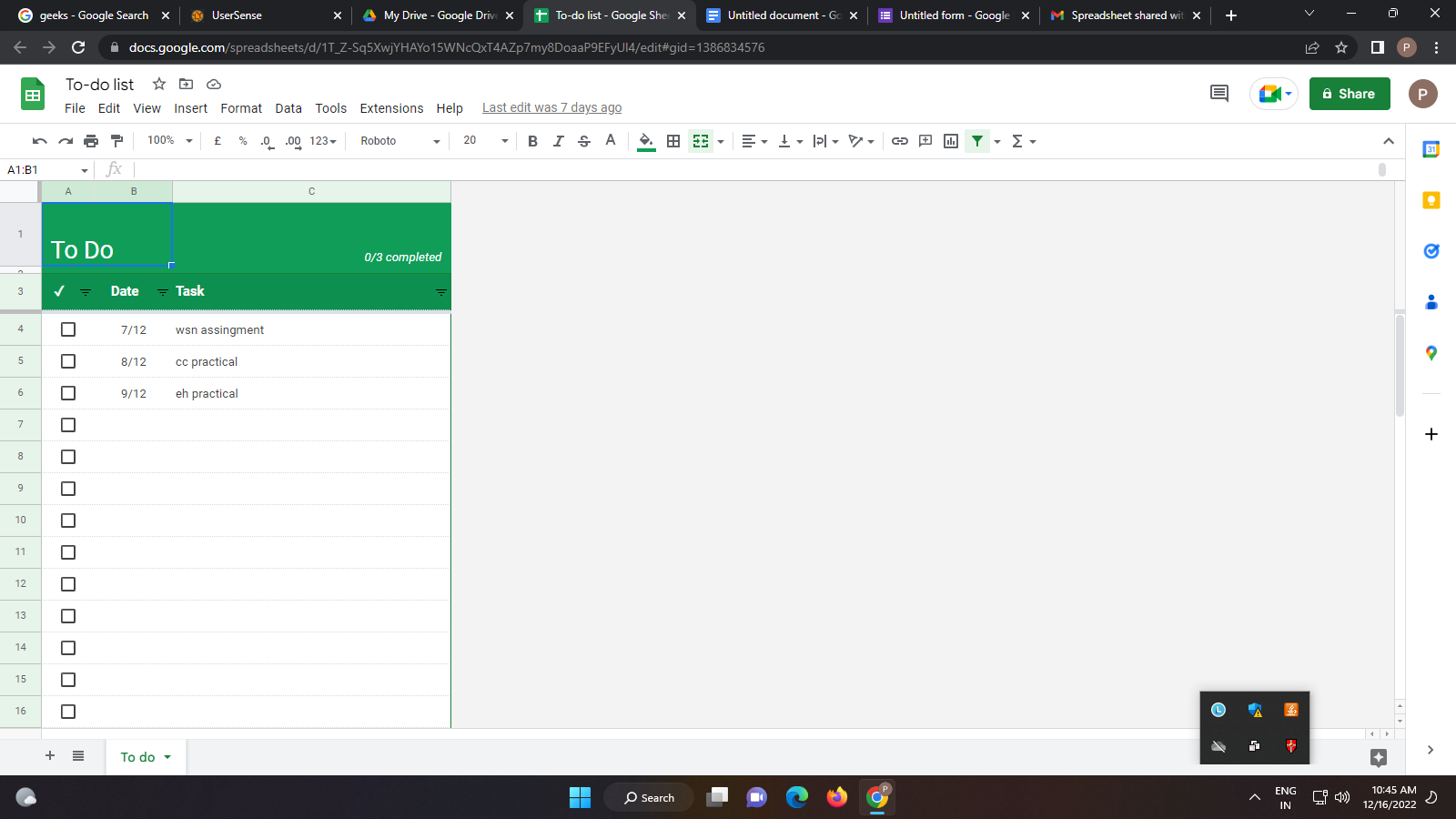
Example: Slack, Samepage, Box, and Zoho Forms.

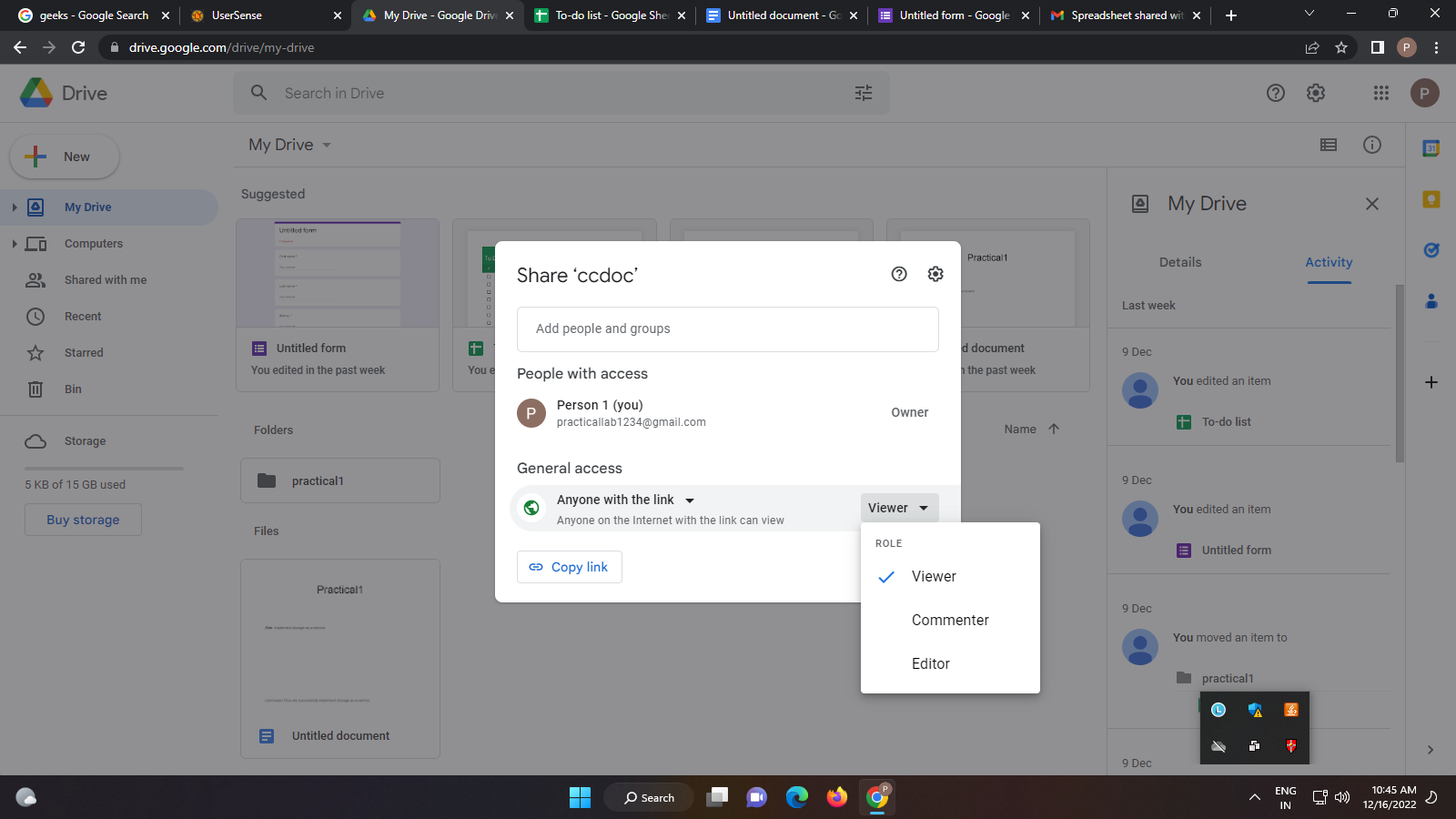
Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

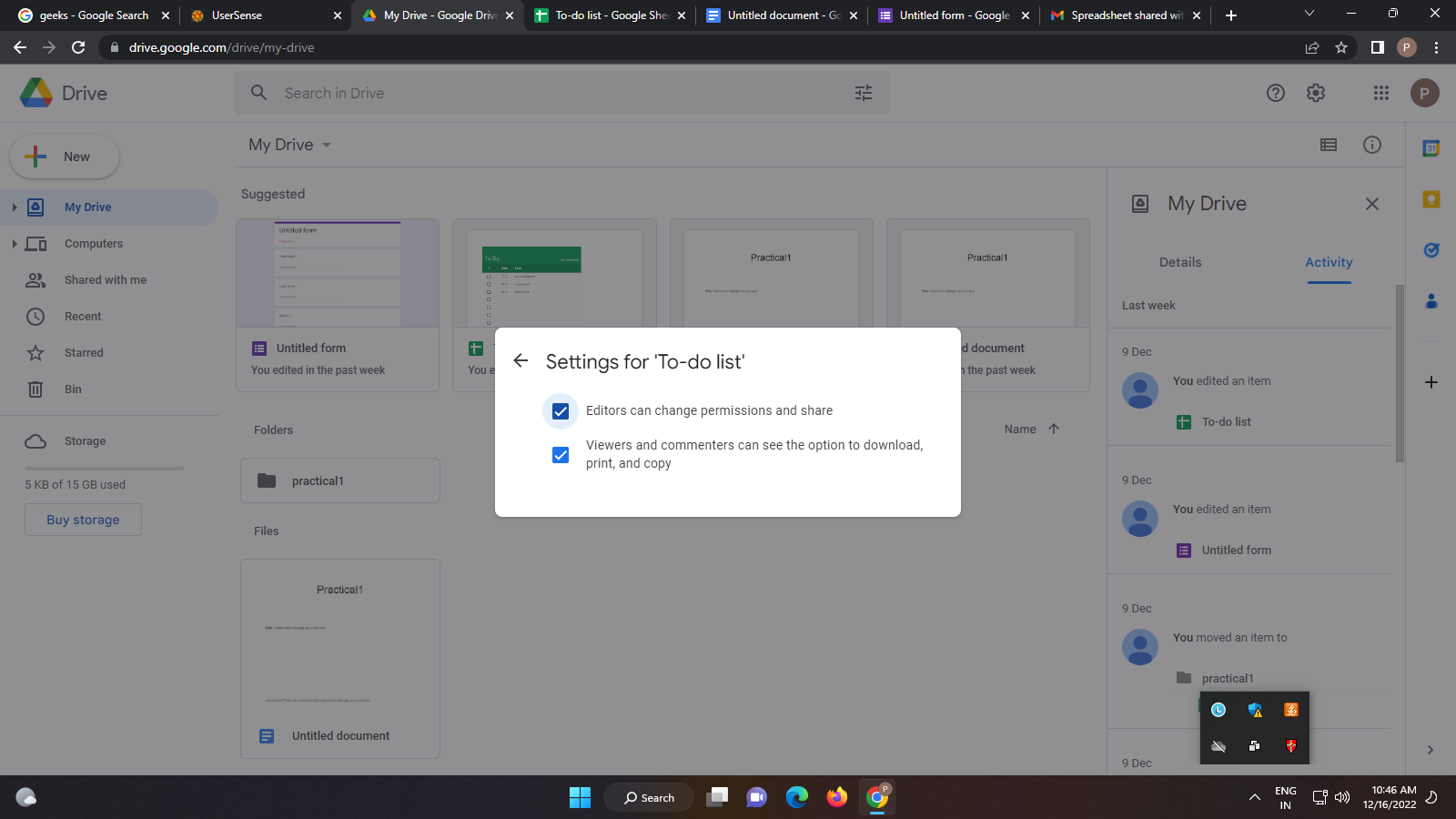
Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.











**Conclusion:** Thus we successfully implement Software as a service

**Practical No:04**

**Aim**: Study and implementation of Storage as a Service

**Theory:**

Storage as a Service or SaaS is cloud storage that you rent from a Cloud Service Provider (CSP) and that provides basic ways to access that storage. Enterprises, small and medium businesses, home offices, and individuals can use the cloud for multimedia storage, data repositories, data backup and recovery, and disaster recovery. There are also higher-tier managed services that build on top of STaaS, such as Database as a Service, in which you can write data into tables that are hosted through CSP resources.

The key benefit to STaaS is that you are offloading the cost and effort to manage data storage infrastructure and technology to a third-party CSP. This makes it much more effective to scale up storage resources without investing in new hardware or taking on configuration costs. You can also respond to changing market conditions faster. With just a few clicks you can rent terabytes or more of storage, and you don’t have to spin up new storage appliances on your own.

How Does Storage as a Service Work?

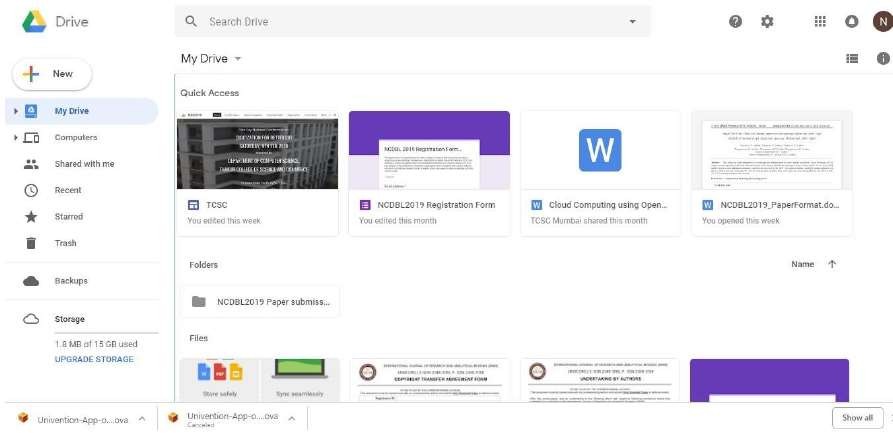
Some STaaS offerings can be rented based on quantity, others are rented based on a service level agreement (SLA). SLAs help establish and reinforce conditions for using data storage, such as uptime and read/write access speed. The storage you choose will typically depend on how often you intend to access the data. Cold data storage is data that you leave alone or access infrequently, whereas warm or hot data is accessed regularly and repeatedly. Pricing by quantity tends to be more cost efficient but isn’t intended to support fast and frequent access for day-to-day business productivity. For hot or warm data, an SLA will be crucial to leveraging data storage in support of current projects or ongoing processes.

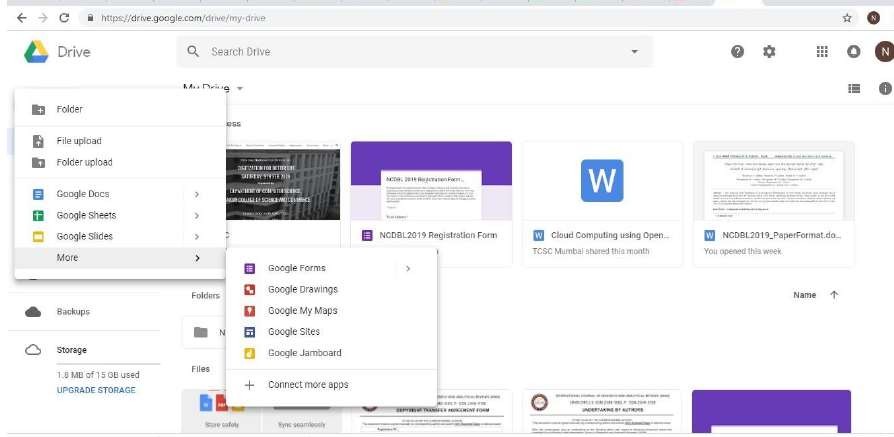
Many CSPs make it easy to onboard and upload data into their STaaS infrastructure for little to no cost at all. However, there may be hidden fees and it can be extremely costly to migrate or transfer your data to a different cloud platform.

# Understanding Data Types

Another factor that influences cost is the type of data storage used. There are three main types of cloud storage: block storage, file storage, and object-based storage.

* **Block storage** breaks data into segmented pieces and distributes them to the storage environment wherever it is most efficient for the platform to do so. This simulates the same functionality as writing data to a standard hard disk drive or solid-state drive. Data remains available for quick access, but it is also costly to maintain and works best for warm or hot data storage.
* **File storage** lists data in a navigable hierarchy, usually a file directory. This is most like the file storage system that you would find on a PC or in cloud storage apps like Microsoft OneDrive. Because it is designed for humans to navigate, file storage is ideal anytime you need to collaborate on a project with other people or businesses. Whether the data is hot or cold doesn’t matter as much. However, file storage does not scale well. The more files you add, the more complex the system becomes and the more difficult it is to navigate.
* **Object-based storage** organizes data by adding meta information to it, making it easy to recognize and retrieve at any time. This type of cloud storage scales up in the most cost-efficient manner, because you can keep adding to it. It is typically the least expensive type of STaaS and best suited for massive amounts of cold media or data files.





**Conclusion:**

Google Docs provide an efficient way for storage of data. It fits well in Storage as a service (SaaS). It has varied options to create documents, presentations and also spreadsheets. It saves documents automatically after a few seconds and can be shared anywhere on the Internet at the click of a button.

**Practical No:05**

**Aim:** User Management in cloud

**Theory:**

User management describes the ability for administrators to manage devices, systems, applications, storage systems, networks, SaaS services, and user access to other various IT resources. User management is a core part to any identity and access management (IAM) solution, in particular directory services tools. Controlling and managing user access to IT resources is a fundamental security essential for any organization. A user management system 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 the IT admin had dictated.

user management solves the problem of managing user access to various resources. For example, the marketing team generally requires access to different resources than the accounting team. Further, an employee on the marketing team likely doesn’t need access to internal financial systems and vice versa, a finance employee isn’t requiring access to Salesforce or Marketo. User management enables IT administrators to manage resources and provision users based on need and role while keeping their digital assets secure. For end users, the tasks of user management are often invisible to them, but the results are not. End users want secure, frictionless access to their IT resources so that they can get their jobs done.

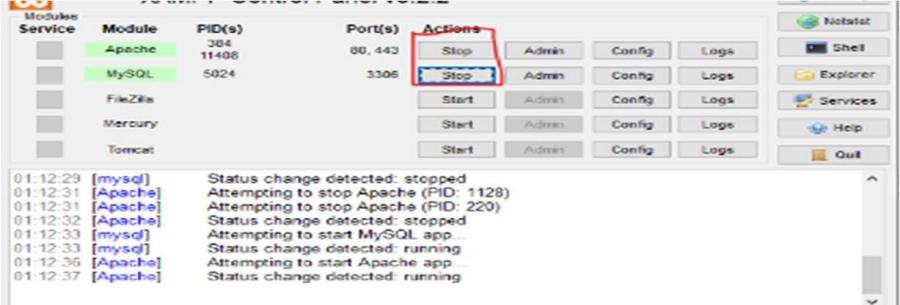
Active Directory made this straightforward and simple for an on-prem Windows network. But, recent innovations in cloud technology have sparked a revolution in cloud Infrastructure-as-a-Service (IaaS) such as AWS, Azure, and Google Cloud Platform among others. Coupled with web applications, users have more IT resources available at their fingertips than ever before, which is why user management has never been more essential – and complicated.

While there are various approaches to user management, one thing is certain – managing user identities is the foundation of identity access management. And, with identities being the number one path to a security breach, IT admins are

more invested than ever in making sure that only the right people utilize their IT resources.

**Procedure:**

First open XAMPP Control Panel and Start “Apache” and “MySQL” Services

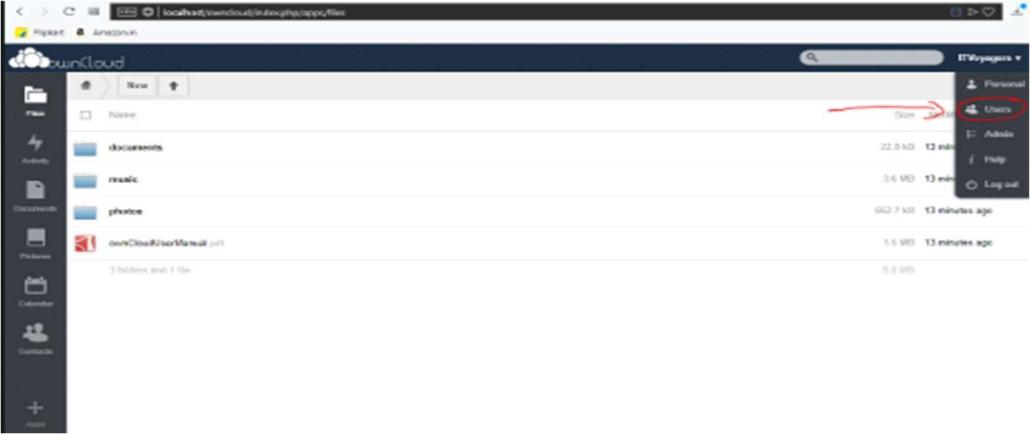


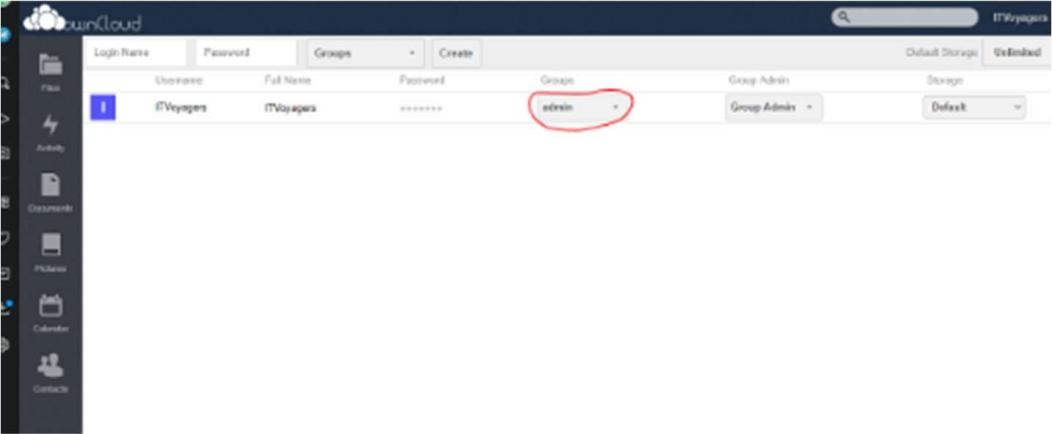
Open browser and type “localhost/owncloud/” in url bar and press “enter”



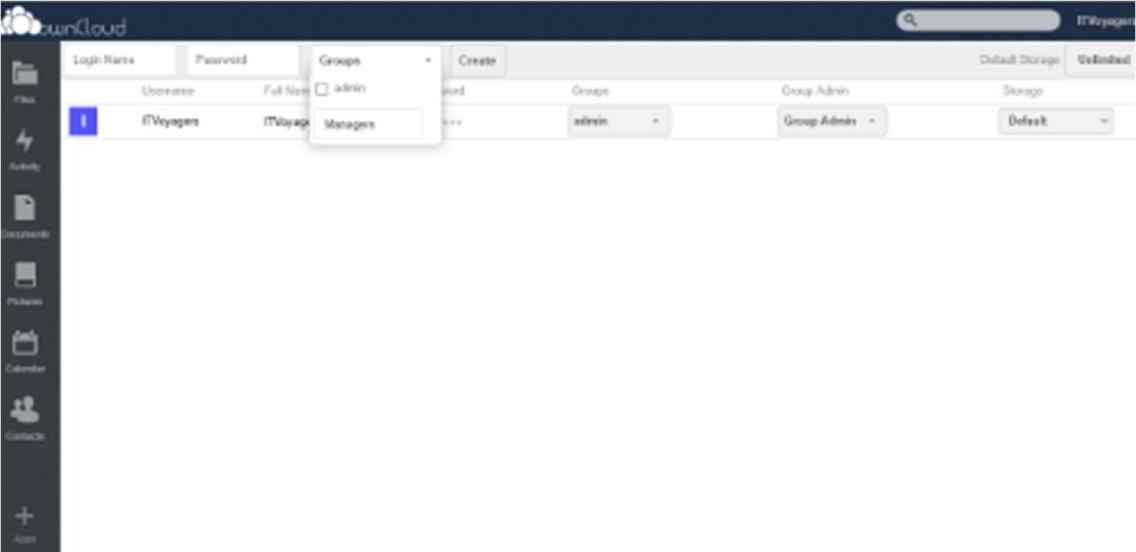


Now goto user



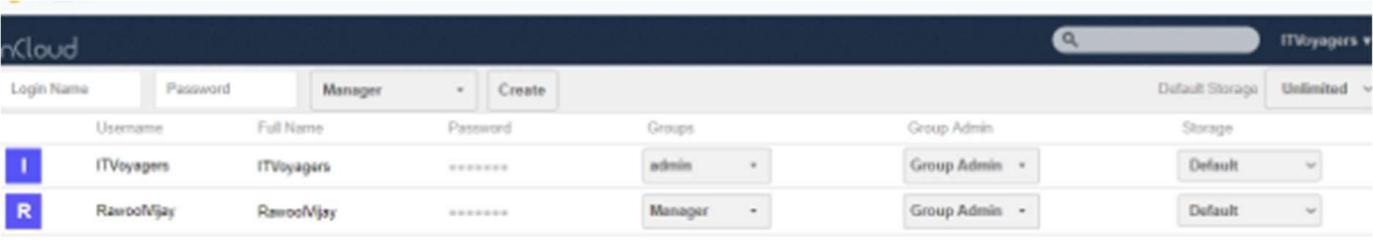


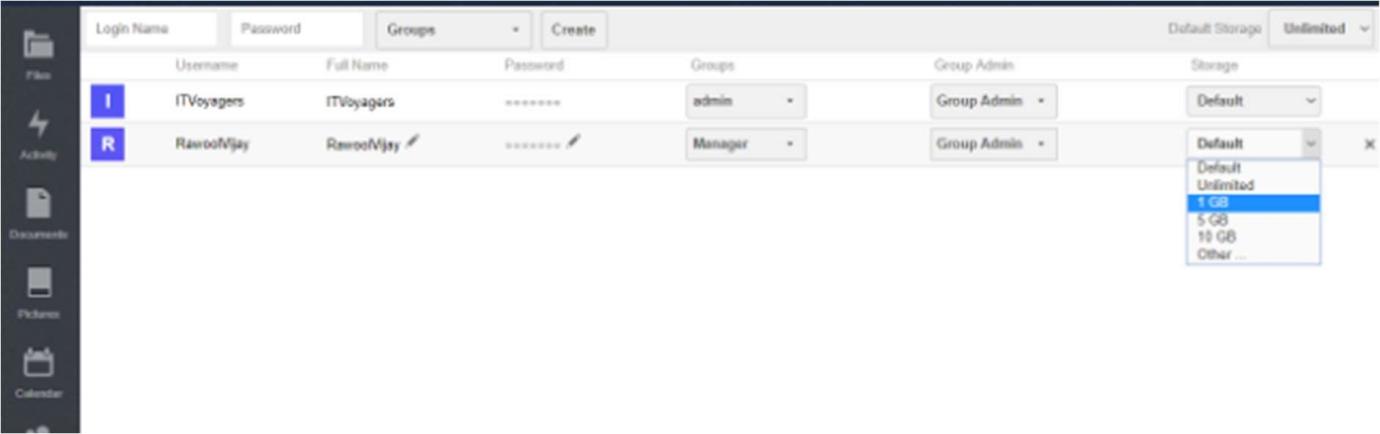
Add a group -> and enter the group name Our group is been added as below



Now enter “Login Name” and “Password” for the user and click on create

As show below our user has been added and we can change the storage limit for new user

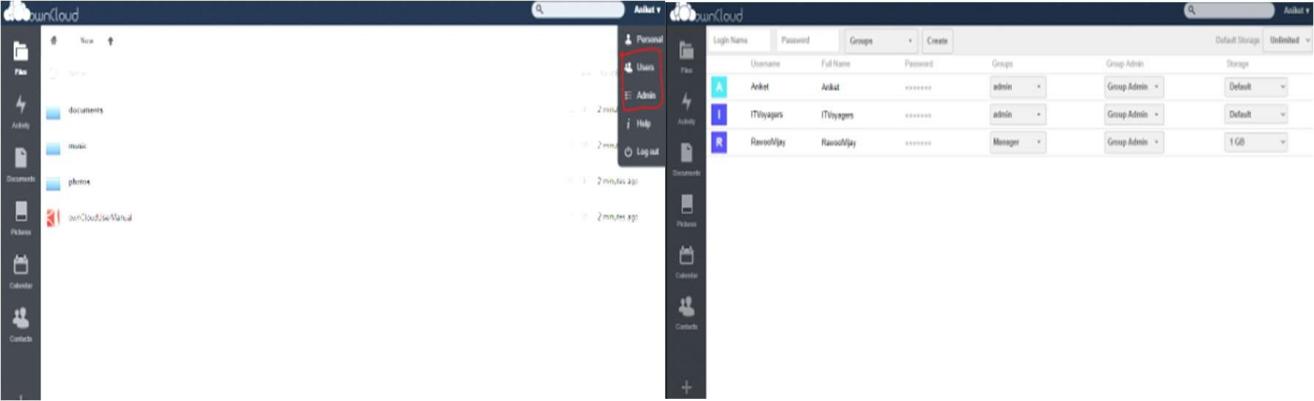




Now lets try to log in from the user account who is admin group

As we can see below this user has privilages of admin because he is in admin group . This user will have all rights that admin posses like adding or deleting user.

**Output:**



**Conclusion:** Hence Successfully implemented user management using own cloud.

**Practical No:06**

**Aim:** Study and implementation of identity management

**Theory:**

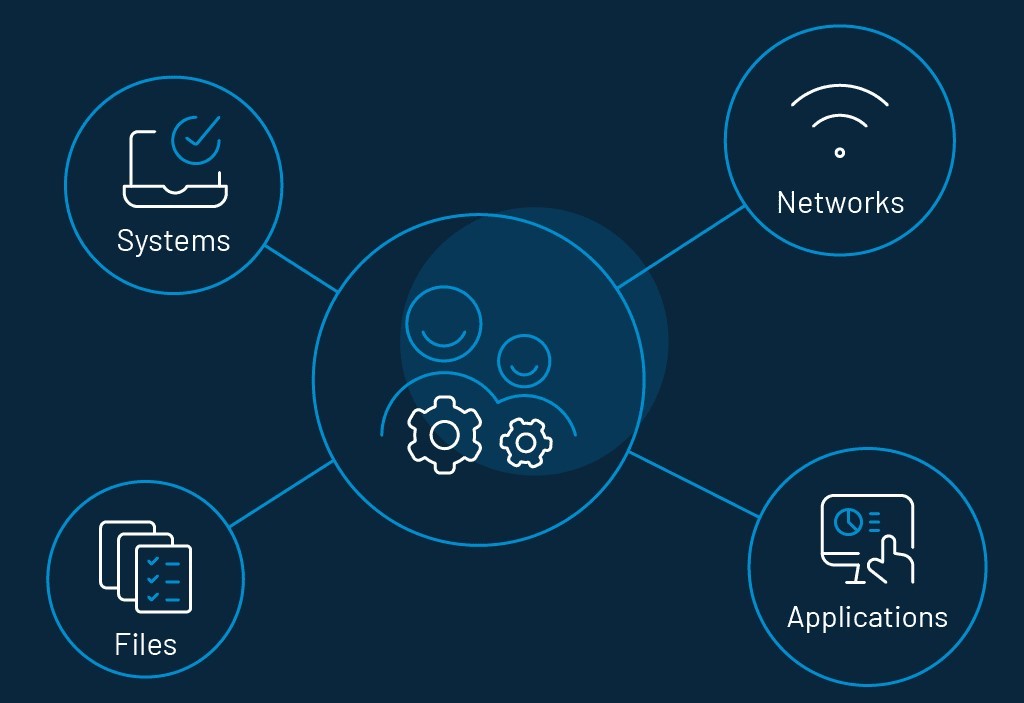
Identity management (IM) is a term that refers to the information system being used within the enterprise. This represents the systematic management of any single identity and provides authentication, privileges, authorization, and roles of the enterprise boundaries. The primary purpose is to upgrade security and productivity by decreasing the total cost, repetitive tasks, and system downtime. Identity management in cloud computing covers all types of users who can work with defined devices under different circumstances. Various identity management (IM) services imply that wired and wireless user can support the directory integration. The availability of BYOD makes it a time- saving service for the individual user. Further, there are some additional security services, which are mentioned below:

* Access Control
* Password Manager
* Digital Identity Management
* Single Sign-On

**Few Benefits of Identity Management in Cloud Security**

Cloud services offer several advantages over all other traditional products. Go through the following actions to understand the few benefits of identity management in cloud computing:

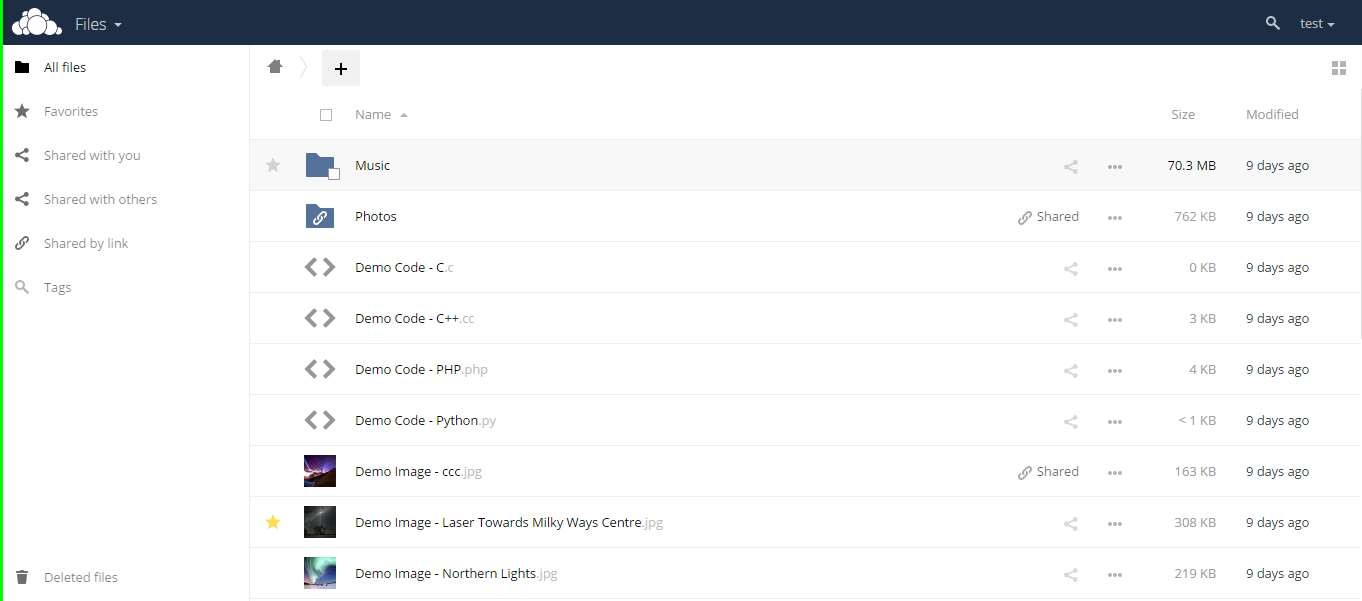
* **Enhanced Network Abilities:** Identity management (IM) makes it simple in sharing the network capabilities with a complete grid of users who were connected with it.
* **Provides a secure collaboration:** SaaS protocol is designed and utilized as a hub for connecting with all virtual networks of suppliers, distributors, and trading partners.
* **Support On-demand improvement:** The problem that affects from churn protects organizations with a cloud-based solution. All experts can be able to provide 24\*7 hours support and monitoring, whenever needed.
* **Increase Overall Productivity:** It is completely known that cloud-based services are configured and hosted by service providers. This may also get a little or zero hassle either for users or any other clients. As a result, many organizations can improve their overall productivity.
* **Centralized Management System:** Business users can be able to manage all services and programs at one place with the cloud-based services. Identity management can be done with one click on a single dashboard.



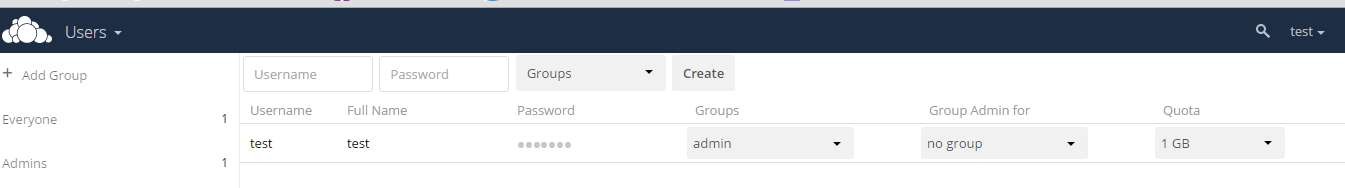
**Procedure:**

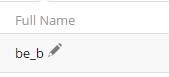
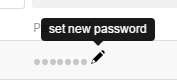
1: Open own cloud-> login user ID and password

2: By default, the ownCloud Web interface opens to your Files page. You can add, remove, and share files, and make changes based on the access privileges set by you (if you are administering the server) or by your server administrator. You can access your ownCloud files with the ownCloud web interface and create, preview, edit, delete, share, and re-share files. Your ownCloud administrator has the option to disable these features, so if any of them are missing on your system ask your server administrator.

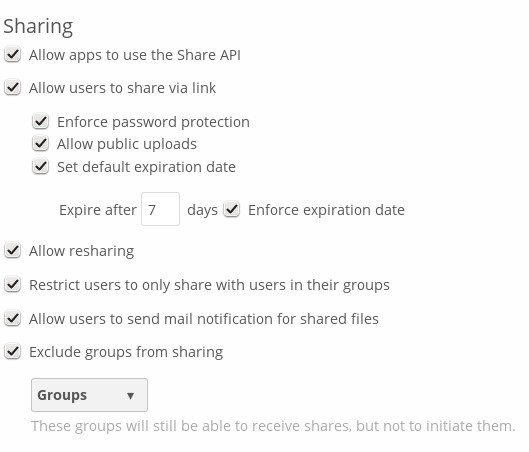


3: Apps Selection Menu: Located in the upper left corner, click the arrow to open a dropdown menu to navigate to your various available apps. Apps Information field: Located in the left sidebar, this provides filters and tasks associated with your selected app. Application View: The main central field in the ownCloud user interface. This field displays the contents or user features of your selected app.





4: Share the file or folder with a group or other users, and create public shares with hyperlinks. You can also see who you have shared with already, and revoke shares by clicking the trash can icon. If username auto-completion is enabled, when you start typing the user or group name ownCloud will automatically complete it for you. If your administrator has enabled email notifications, you can send an email notification of the new share from the sharing screen.



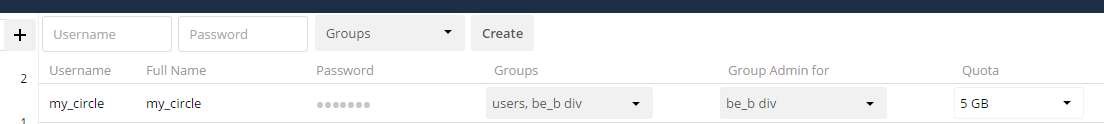
5: Five Share permissions are :

Can share; allows the users you share with to re-share.

Can edit; allows the users you share with to edit your shared files, and to collaborate using the Documents app.

Create; allows the users you share with to create new files and add them to the share. Change; allows uploading a new version of a shared file and replacing it.

Delete; allows the users you share with to delete shared files.



**Conclusion:**

We have studied how to use ownCloud for ensuring identity management of the users. We can create multiple groups and provide privileges to view or modify data as per defined permissions. It also enables simplified look and feel to be used by anyone.

**Practical No:07**

**Aim:** Study and implement MFA in the environment of popular Cloud Service Provider

**Theory**:

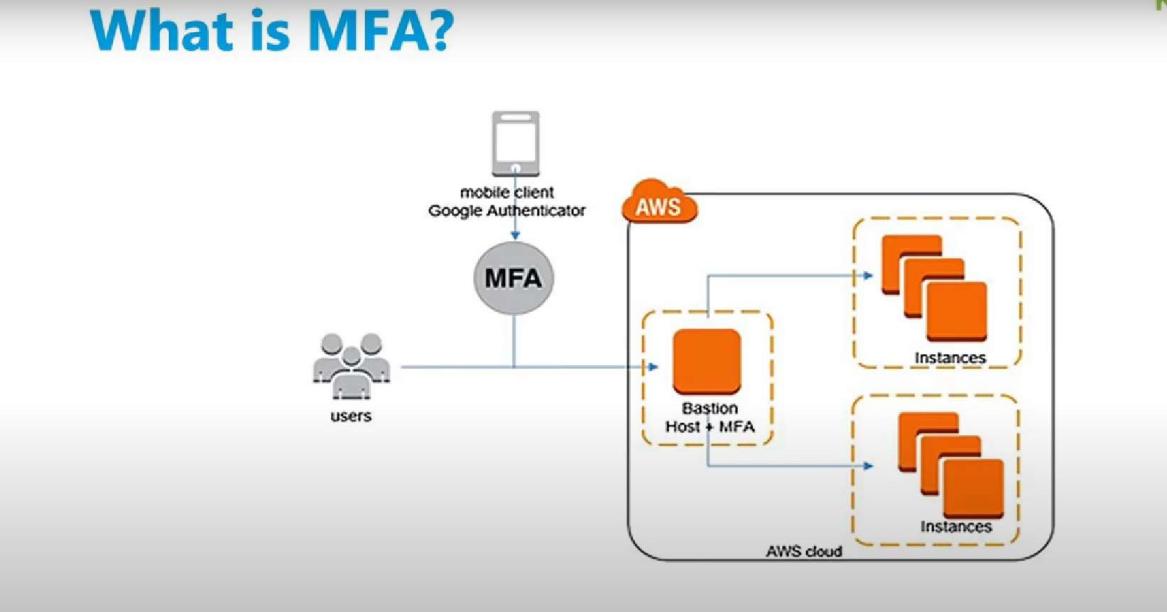
AWS multi-factor authentication (MFA) is an AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

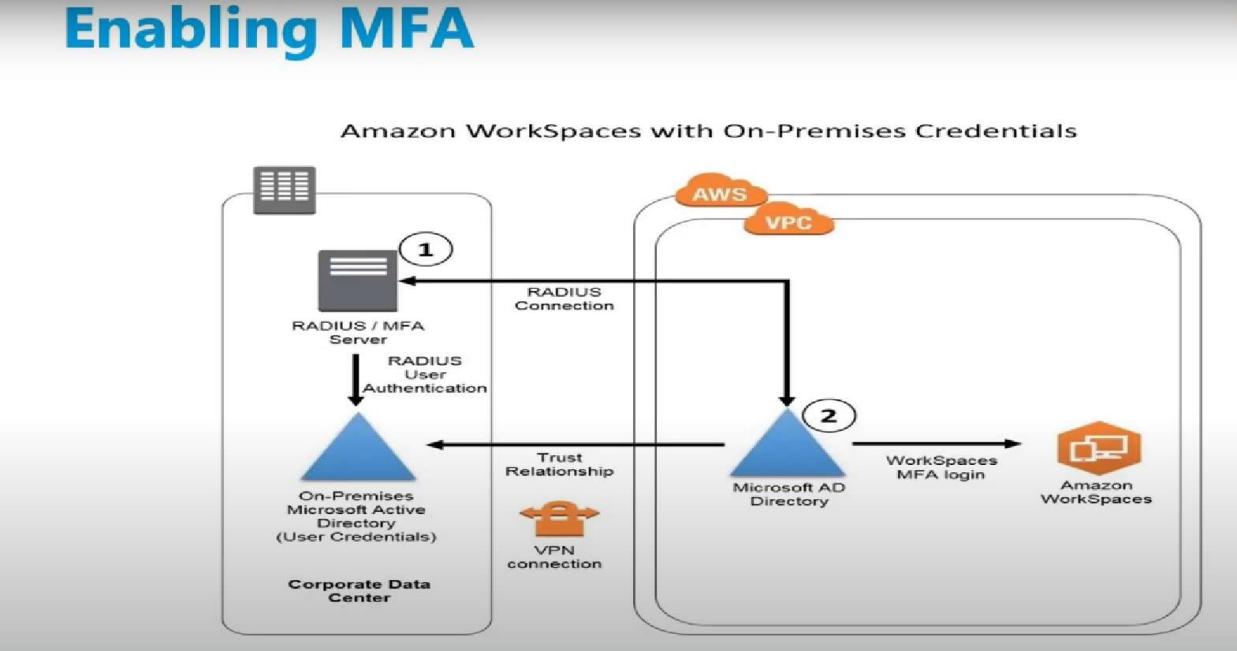
*AWS is expanding eligibility for its free MFA security key program. Verify your eligibility and order your free MFA key.*

With MFA enabled, when a user signs in to the AWS Management Console, they are prompted for their user name and password— *something they know*—and an authentication code from their MFA device— *something they have* (or if they use a biometrics-enabled authenticator, *something they are*). Taken together, these factors improve security for your AWS accounts and resources.

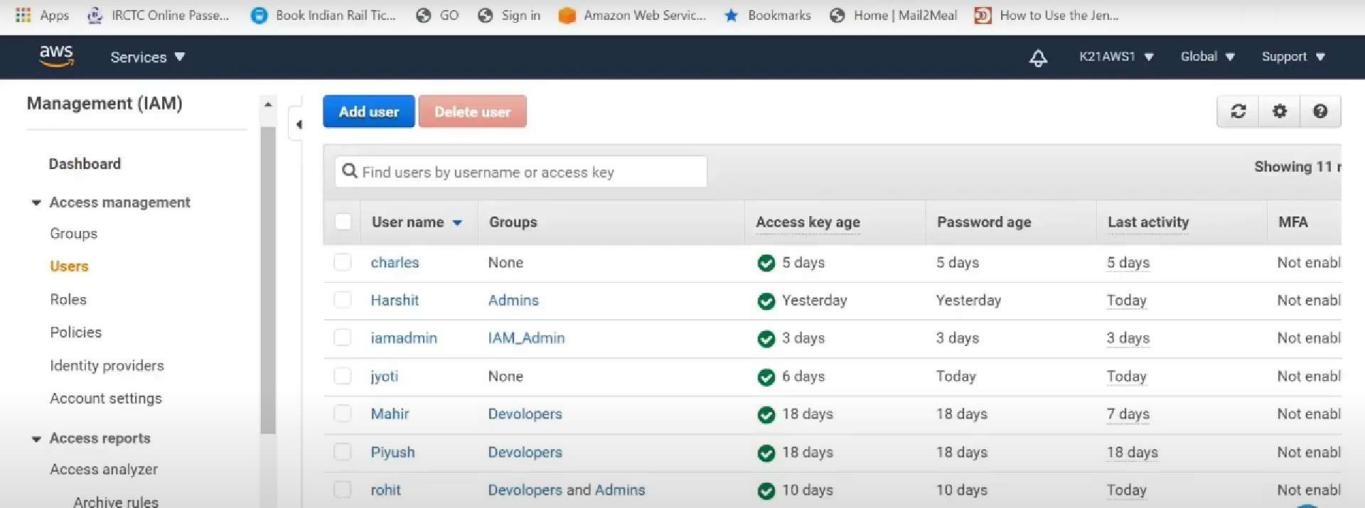
We recommend that you require your human users to use temporary credentials when accessing AWS. Your users can use an identity provider to federate into AWS, where they can authenticate with their corporate credentials and MFA configurations. To manage access to AWS and business applications, we recommend that you use AWS IAM Identity Center. For more information, see the IAM Identity Center User Guide.

See the following available MFA options that you can use with your IAM MFA implementation. You can download virtual authenticator apps through the links provided, or you can acquire a hardware MFA device from the respective manufacturer. After you've acquired a supported virtual or hardware MFA device, AWS does not charge additional fees for using MFA

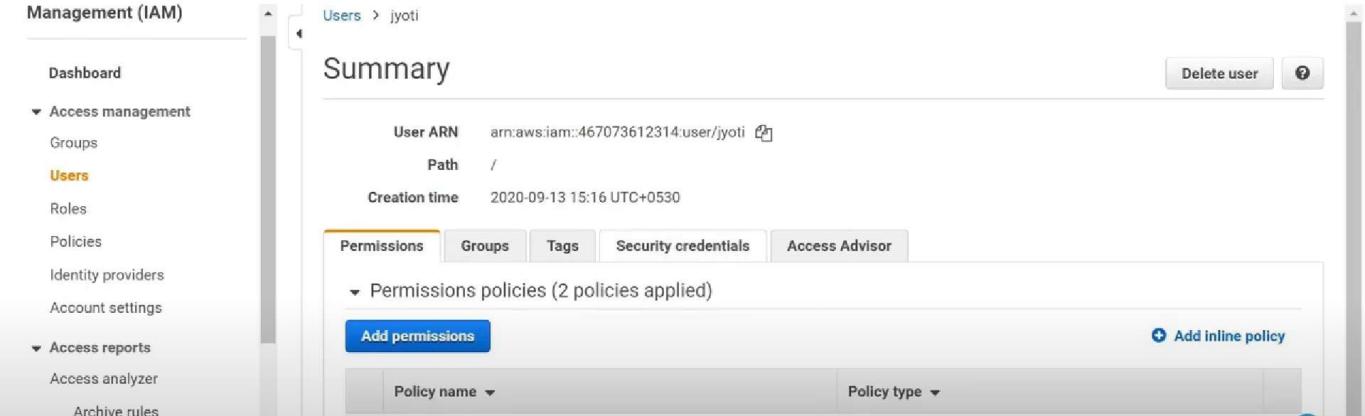


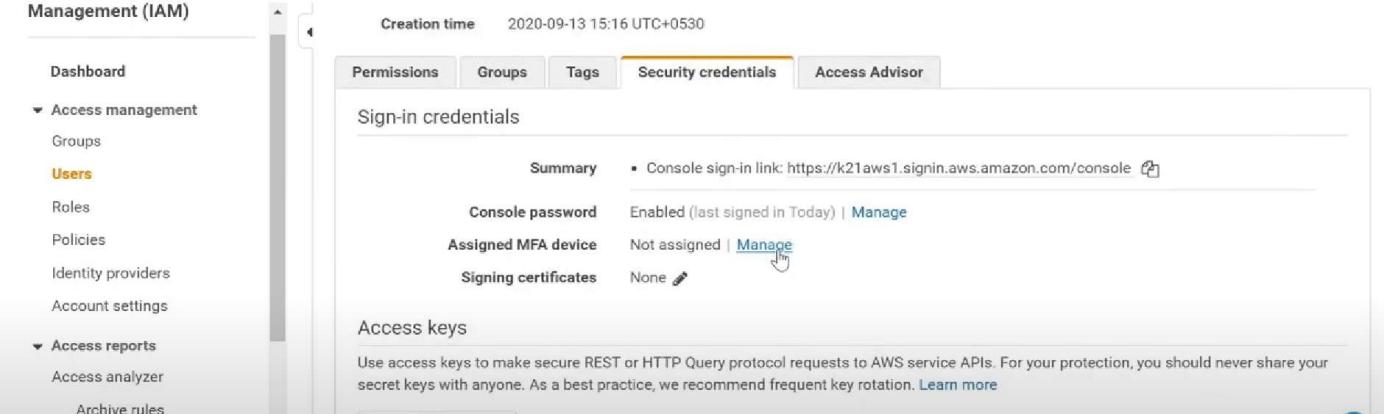


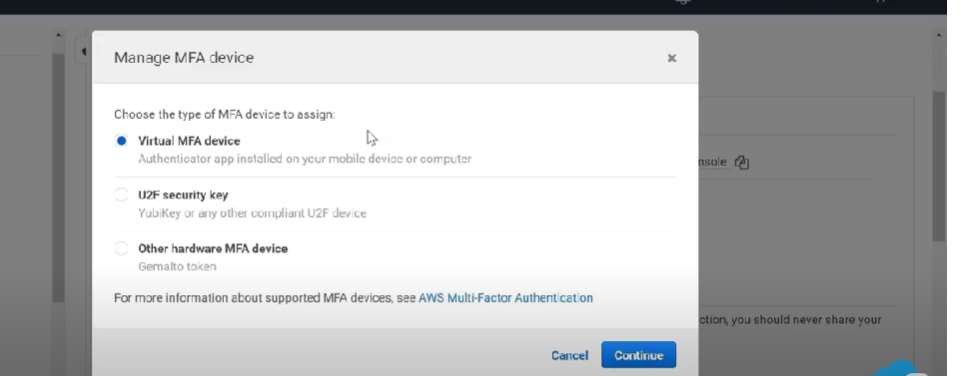
**Procedure:**

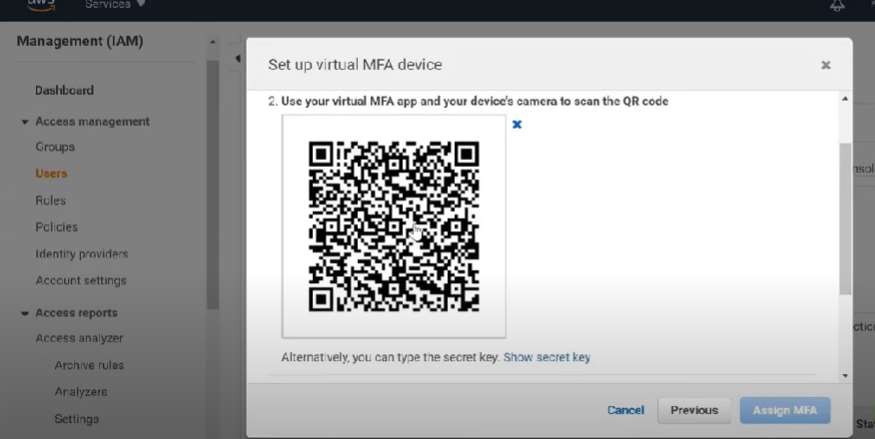


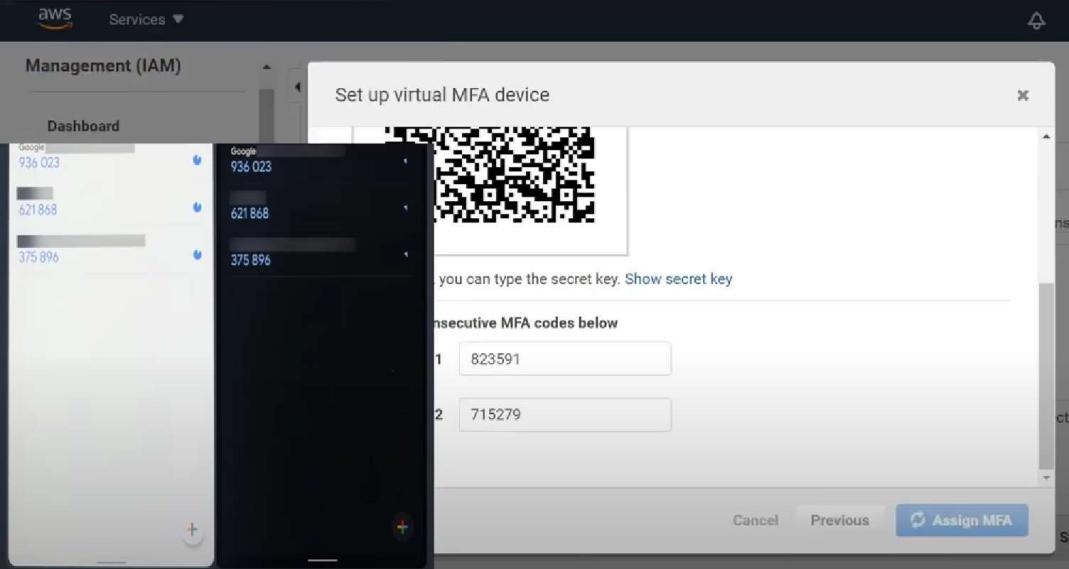
Click on any of user ->select security credentials -> Below you will find Assign MFA device

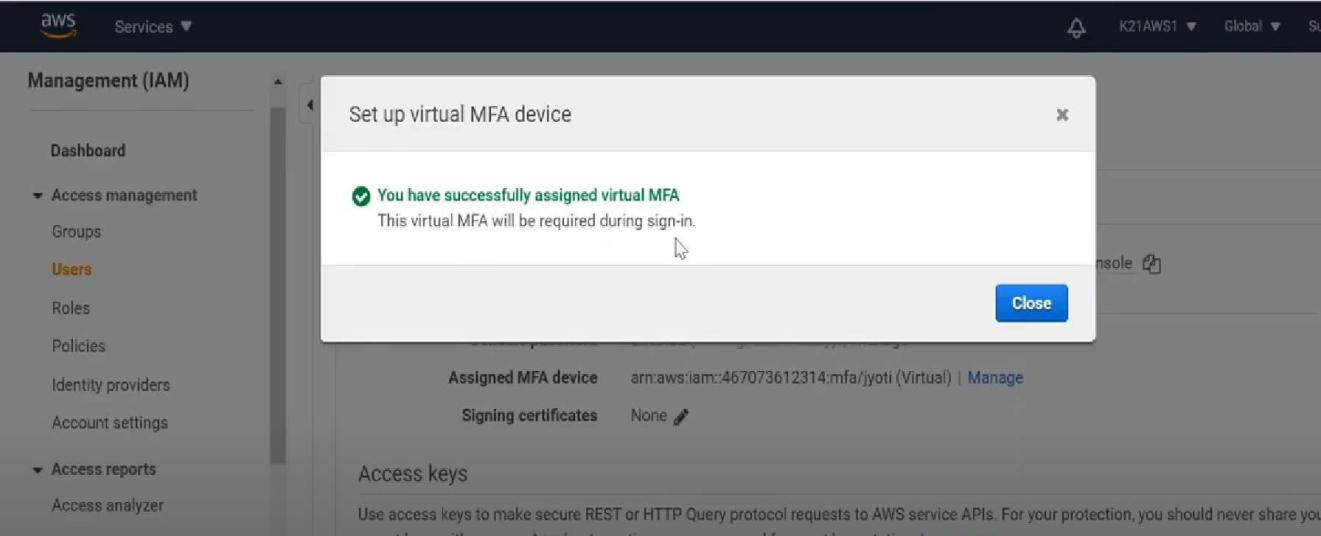












**Conclusion:** Hence, Successfully implemented in MFA in AWS.

**Practical No:08**

**Aim:** Write a program for web feed

**Theory:**

With RSS it is possible to distribute up-to-date web content from one web site to thousands of other web sites around the world.

RSS allows fast browsing for news and updates. RSS was designed to show selected data.

Without RSS, users will have to check your site daily for new updates. This may be too time-consuming for many users. With an RSS feed (RSS is often called a News feed or RSS feed) they can check your site faster using an RSS aggregator (a site or program that gathers and sorts out RSS feeds).

Since RSS data is small and fast-loading, it can easily be used with services like cell phones or PDA's.

Web-rings with similar information can easily share data on their web sites to make them better and more useful.

Here are some benefits of using RSS:

Choose your news

With RSS you can choose to view the news you want, the news that interest you and are relevant to your work.

Remove unwanted information

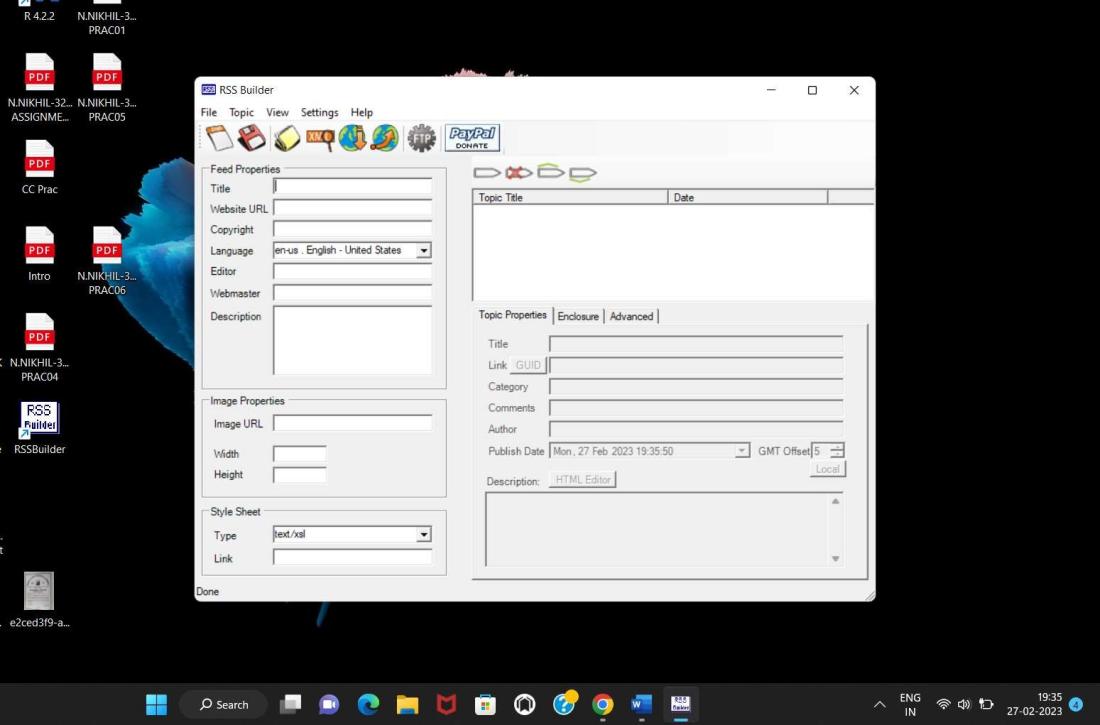
With RSS you can (finally) separate wanted information from unwanted information (spam)!

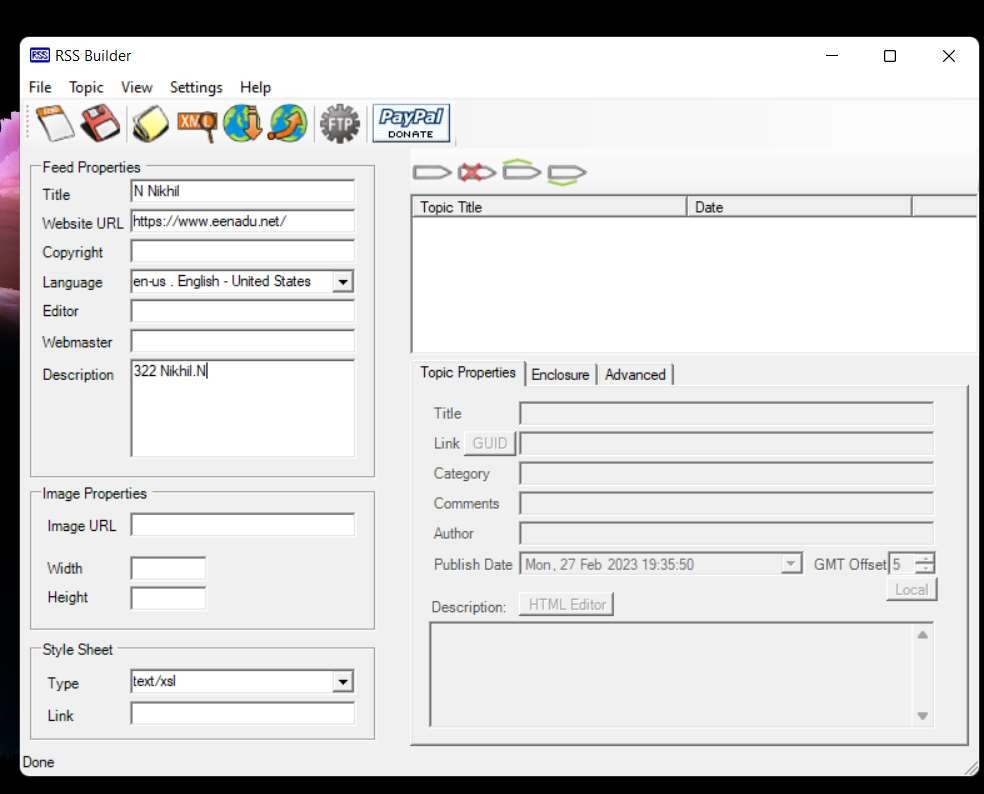
Increase your site traffic

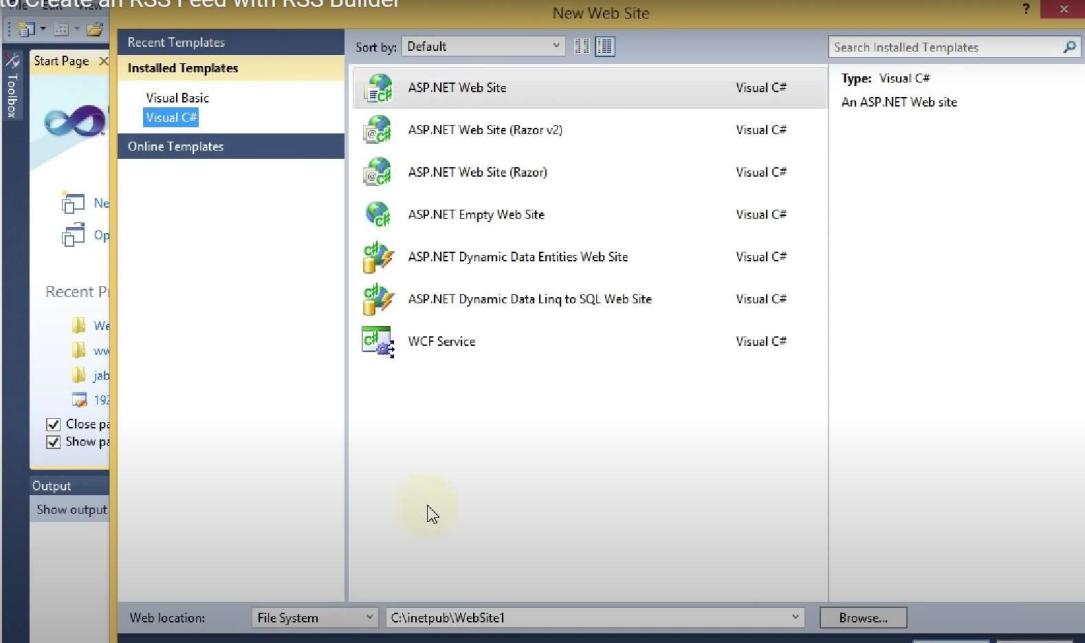
With RSS you can create your own news channel, and publish it to the Internet!

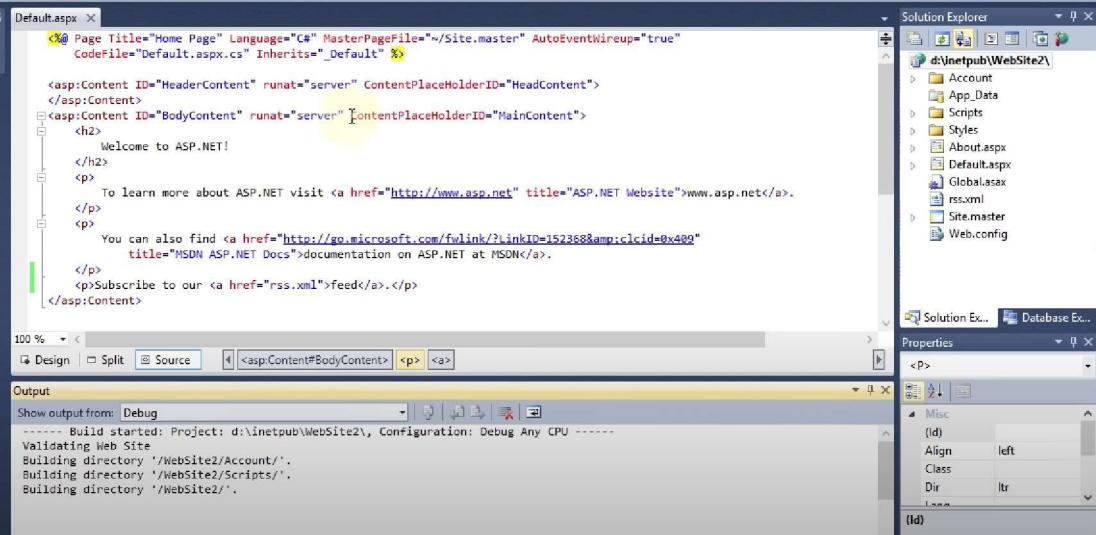
**Procedure:**

Install RSS Builder











**Conclusion**: Hence, Successfully implemented program for web feed.

**Practical No:09**

**Aim**: Study and implementation of Single-Sign-On (SSO).

**Theory**: SSO is a system that merges several application login windows into a single screen. To access all of their SaaS services, a user just has to input their login credentials once on a single page using SSO.

SSO is widely used in a corporate context where user applications are allocated and managed by an internal IT team. Remote employees that use SaaS services benefit from SSO as well.

Consider what would happen if customers who had previously been admitted to a bar were required to present their identity card each time they sought to purchase further alcoholic beverages. Some consumers would become upset with the constant inspections and would even try to get around them by bringing their own beverages in.

Most businesses, on the other hand, will simply verify a customer's identity once and then offer the person multiple beverages throughout the evening. This is identical to an SSO system in that instead of establishing their identity many times, a user creates their identity once and then has access to multiple services.

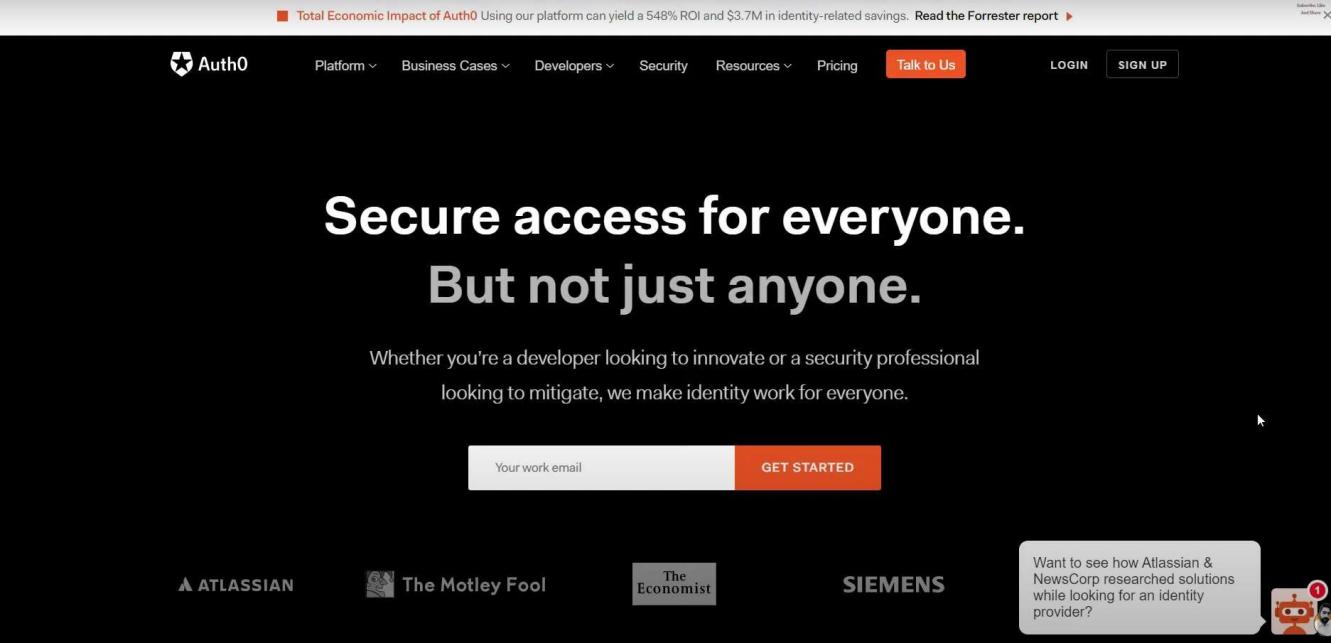
Many identities and access management (IAM) or access control solutions include single sign-on (SSO). Verifying a user's identity is essential for determining which rights each user should have. One example of an access control system that works with SSO solutions for controlling users' identities is Cloudflare Zero Trust.

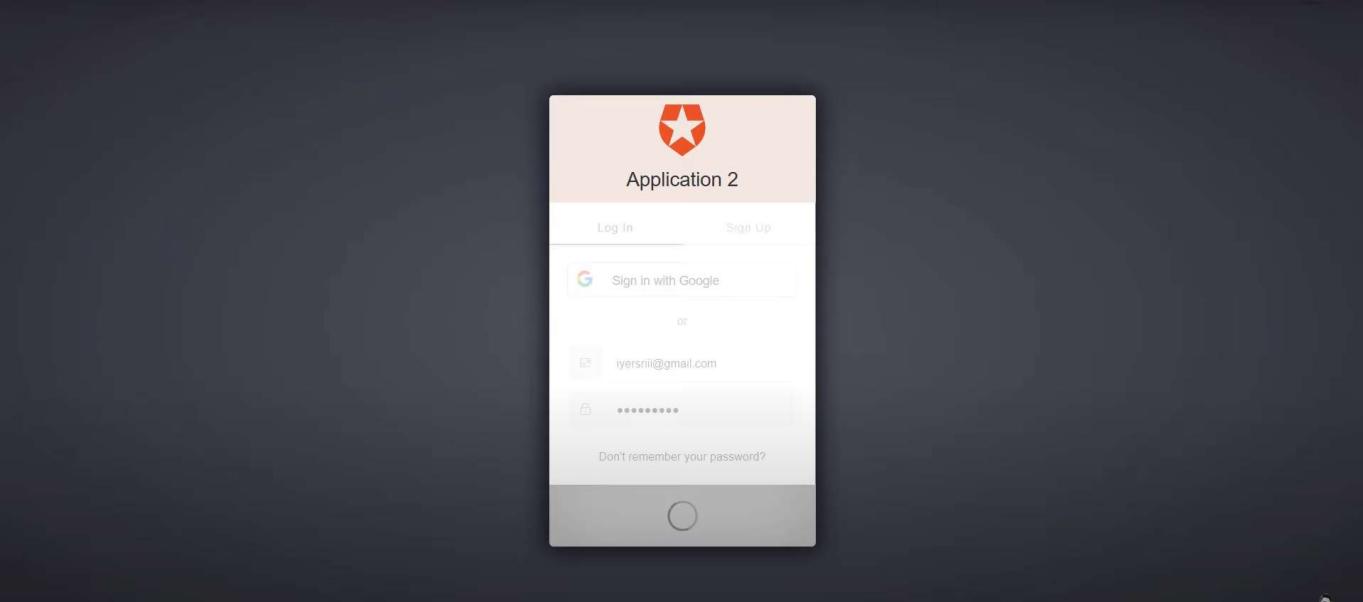
How Does Single Sign-On Work?

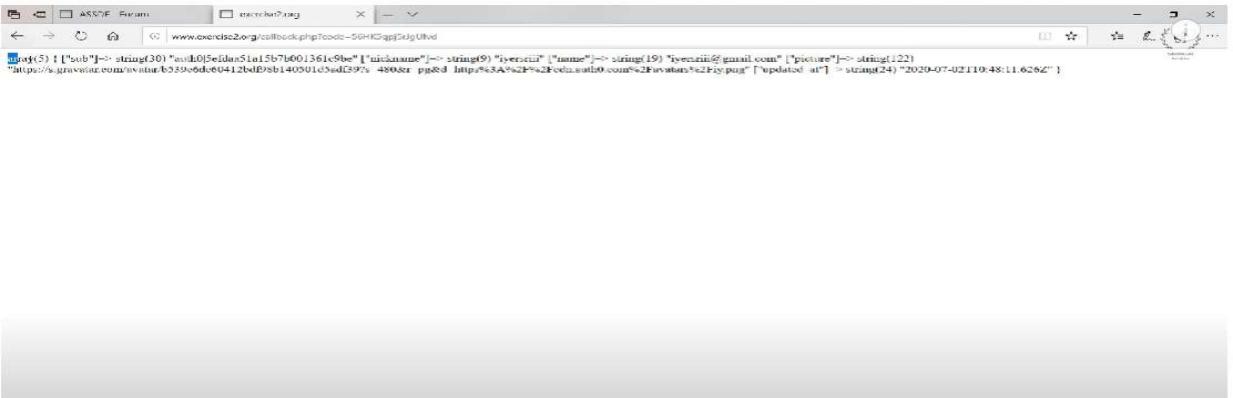
SSO is predicated on the establishment of a trust relationship between a service provider and an identity provider, such as OneLogin. This trust relationship is frequently established by the exchange of a certificate between the identity supplier and the service provider. This certificate can be used to check identity information transmitted from the identity provider to the service provider, ensuring that the service provider is receiving it from a reliable source. This identification data is stored in the form of tokens in SSO, which contain identifying info about the user, such as an email address or a username.

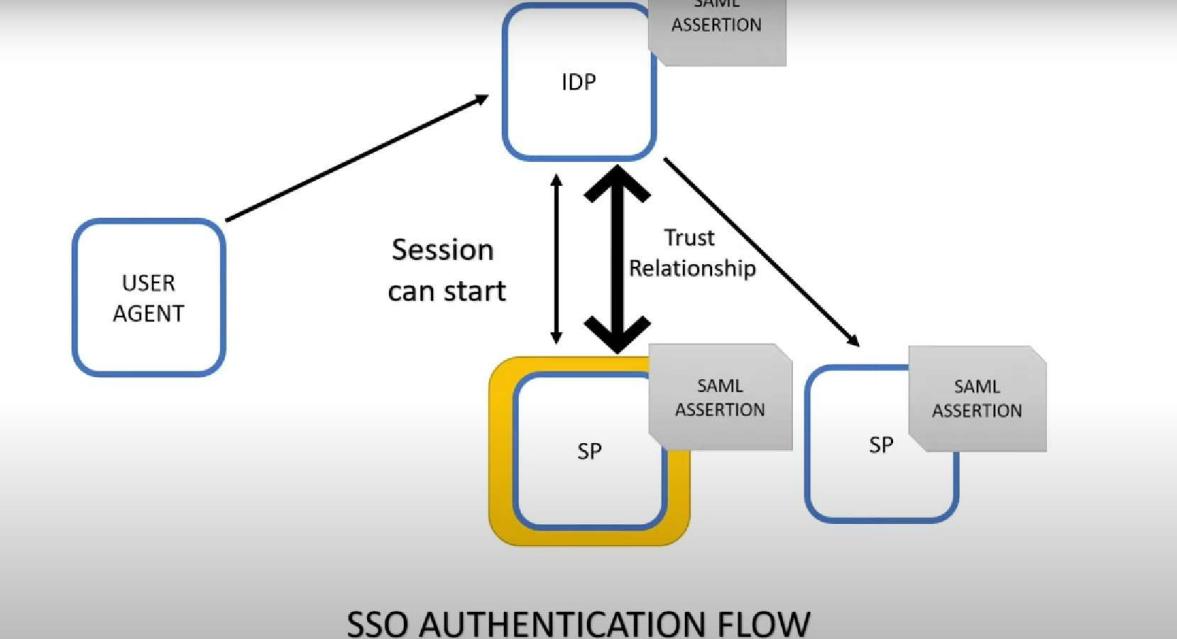
The following is a typical **login flow** −

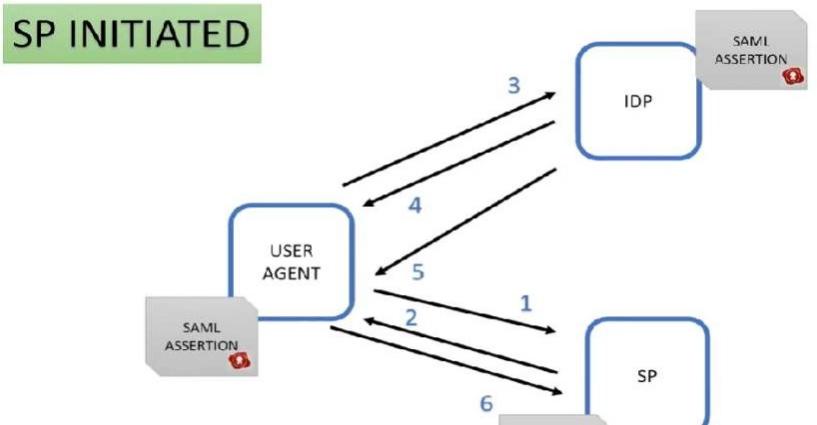
* A user reaches the Service Provider, which is the program or website to which they seek to access.
* The Service Provider transmits a token to the SSO system, or the Identity Provider, as part of a request to authenticate the user. The token contains some information about the user, such as their email address.
* The Identity Provider initially checks to determine if the user has already been authenticated; if so, the user will be granted access to the Service Provider application, and step 5 will be skipped.
* If the user hasn't logged in yet, they will be requested to do so by entering the Identity Provider's credentials.
* This might be as straightforward as a username and password, or it could consist of another type of authentication, such as a One-Time Password.
* When the Identity Provider checks the provided credentials, it returns a token to the Service Provider, indicating that the authentication was successful.
* The user's browser sends this token to the Service Provider.
* The trust connection that the Service Provider and the Identity Provider established during the initial configuration is used to validate the token that the Service Provider gets.
* Access to the Service Provider is provided to the user.
* When the user attempts to visit a different website, the new website must be established with a similar trust relationship with the SSO solution, and authentication follows similar steps

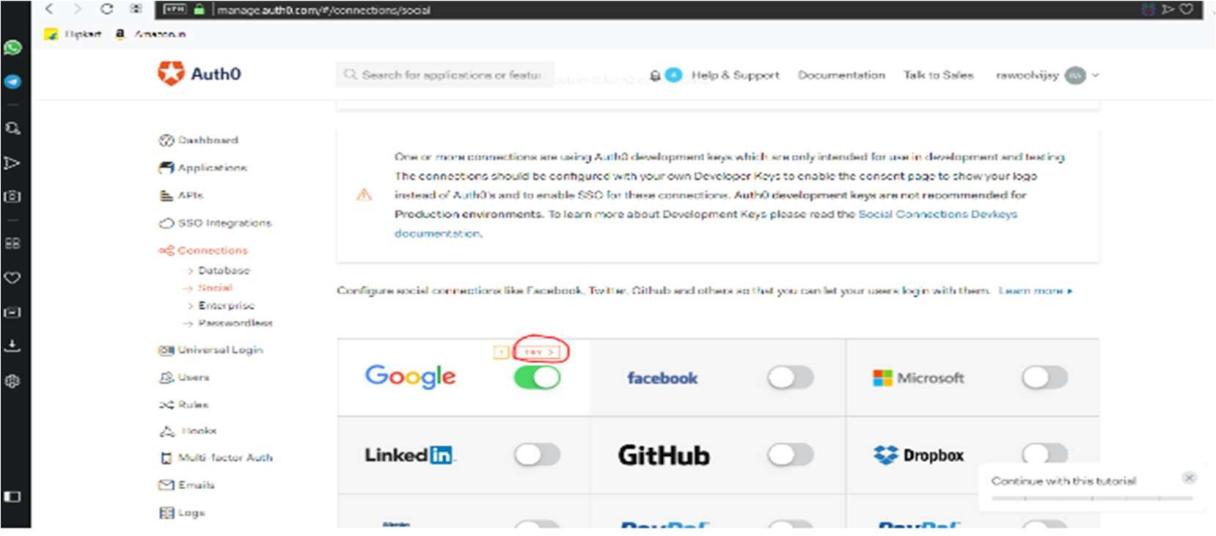


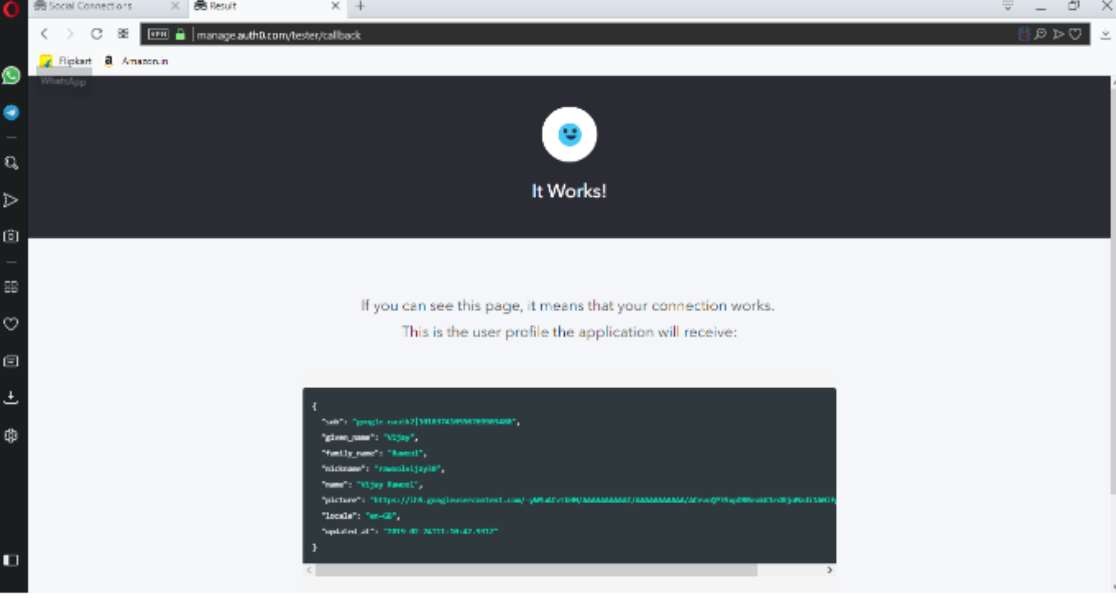












**Conclusion:** Hence, successfully implemented Single-Sign-On (SSO).

**Practical No:10**

**Aim:** Case study on Amazon EC2

Elastic IP addresses allow you to allocate a static IP address and programmatically assign it to an instance. You can enable monitoring on an Amazon EC2 instance using Amazon CloudWatch2 in order to gain visibility into resource utilization, operational performance, and overall demand patterns (including metrics such as CPU utilization, disk reads and writes, and network traffic). You can create Auto-scaling Group using the Auto-scaling feature3 to automatically scale your capacity on certain conditions based on metric that Amazon CloudWatch collects. You can also distribute incoming traffic by creating an elastic load balancer using the Elastic Load Balancing4 service. Amazon Elastic Block Storage (EBS)5 volumes provide network-attached persistent storage to Amazon EC2 instances. Point-in-time consistent snapshots of EBS volumes can be created and stored on Amazon Simple Storage Service (Amazon S3)6.

Amazon S3 is highly durable and distributed data store. With a simple web services interface, you can store and retrieve large amounts of data as objects in buckets (containers) at any time, from anywhere on the web using standard HTTP verbs. Copies of objects can be distributed and cached at 14 edge locations around the world by creating a distribution using Amazon CloudFront7 service – a web service for content delivery (static or streaming content). Amazon SimpleDB8 is a web service that provides the core functionality of a database- real-time lookup and simple querying of structured data – without the operational complexity. You can organize the dataset into domains and can run queries across all of the data stored in a particular domain. Domains are collections of items that are described by attribute-value pairs.

Amazon Relational Database Service9 (Amazon RDS) provides an easy way to setup, operate and scale a relational database in the cloud. You can launch a DB Instance and get access to a full-featured MySQL database and not worry about common database administration tasks like backups, patch management etc.

Amazon Simple Queue Service (Amazon SQS)10 is a reliable, highly scalable, hosted distributed queue for storing messages as they travel between computers and application components.

Amazon Simple Notifications Service (Amazon SNS) provides a simple way to notify applications or people from the cloud by creating Topics and using a publish-subscribe protocol.

Amazon Elastic MapReduce provides a hosted Hadoop framework running on the web-scale infrastructure of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3) and allows you to create customized JobFlows. JobFlow is a sequence of MapReduce steps.

Amazon Virtual Private Cloud (Amazon VPC) allows you to extend your corporate network into a private cloud contained within AWS. Amazon VPC uses IPSec tunnel mode that enables you to create a secure connection between a gateway in your data center and a gateway in AWS.

Amazon Route53 is a highly scalable DNS service that allows you manage your DNS records by creating a HostedZone for every domain you would like to manage.

AWS Identity and Access Management (IAM) enable you to create multiple Users with unique security credentials and manage the permissions for each of these Users within your AWS Account. IAM is natively integrated into AWS Services. No service APIs have changed to support IAM, and exiting applications and tools built on top of the AWS service APIs will continue to work when using IAM.

AWS also offers various payment and billing services that leverages Amazon’s payment infrastructure.

All AWS infrastructure services offer utility-style pricing that require no long- term commitments or contracts. For example, you pay by the hour for Amazon EC2 instance usage and pay by the gigabyte for storage and data transfer in the case of Amazon S3. More information about each of these services and their pay-as-you-go pricing is available on the AWS Website.

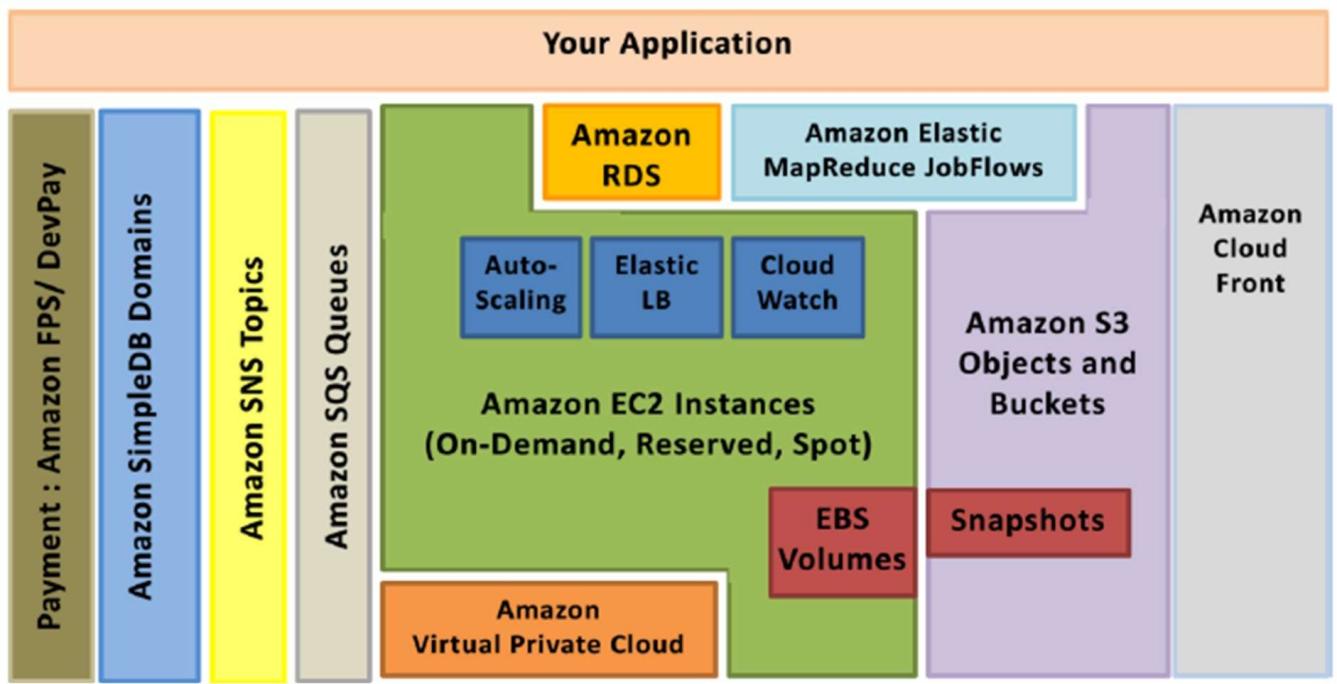
Note that using the AWS cloud doesn’t require sacrificing the flexibility and control you’ve grown accustomed to:

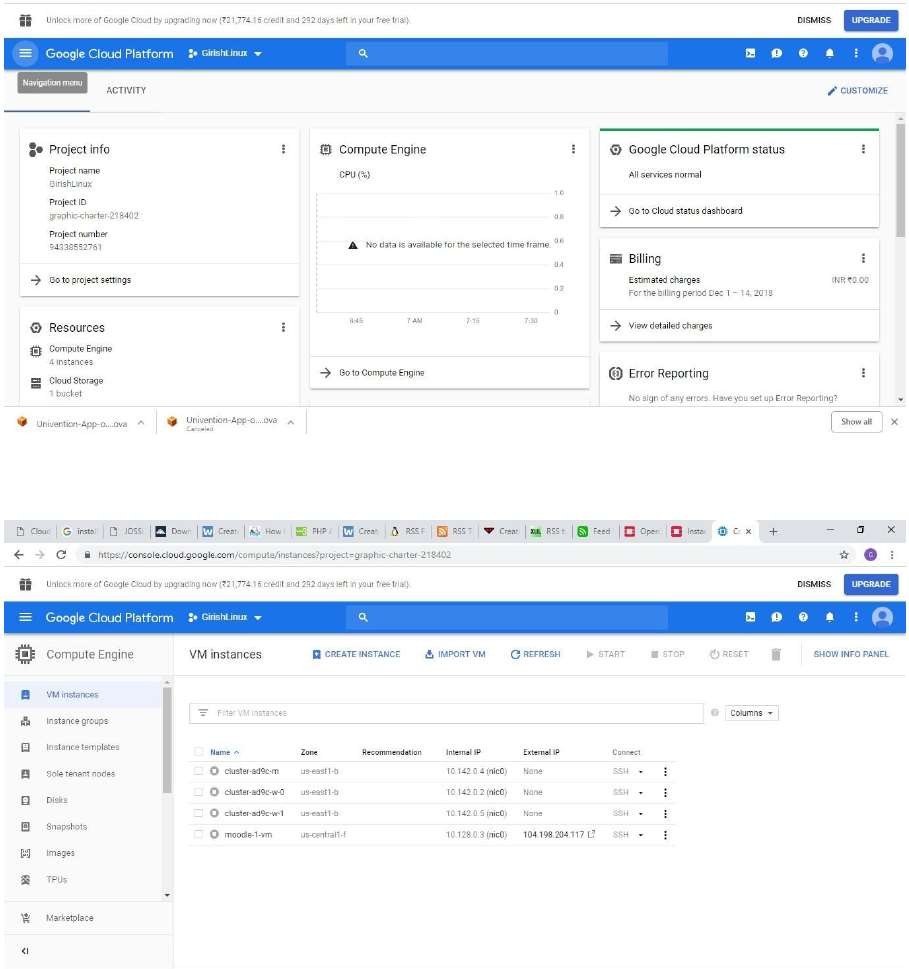
You are free to use the programming model, language, or operating system (Windows, OpenSolaris or any flavor of Linux) of your choice.

You are free to pick and choose the AWS products that best satisfy your requirements—you can use any of the services individually or in any combination.

Because AWS provides resizable (storage, bandwidth and computing) resources, you are free to consume as much or as little and only pay for what you consume.

You are free to use the system management tools you’ve used in the past and extend your datacenter into the cloud.





**Conclusion:** Successfully studied AWS EC2