

**Index**

|  |  |  |
| --- | --- | --- |
| **No** | **Title** | **Page No.** |
| 1 | Study and implementation of Infrastructure as a Service | 3 |
| 2 | Study and implementation of Platform as a Service | 29 |
| 3 | Study and implementation of Software as a Service | 35 |
| 4 | Study and implementation of Storage as a Service | 53 |
| 5 | User Management in Cloud | 59 |
| 6 | Study and implementation of Identity and Access Management | 65 |
| 7 | Study and implementation of MFA in the environment of Popular Cloud service provider | 79 |
| 8 | Write a Program for Web Feed | 86 |
| 9 | Study and implementation of Single-sign-on (SSO) | 95 |
| 10 | Case Study on Google Cloud | Secondpdf |
|  |  |  |

**Practical No. 1**

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

**Theory:** 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 provider provides the following services -**

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

There are the following advantages of IaaS computing layer -

**1. Shared infrastructure**

IaaS allows multiple users to share the same physical infrastructure.

**2. Web access to the resources**

Iaas allows IT users to access resources over the internet.

**3. Pay-as-per-use model**

IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

**4. Focus on the core business**

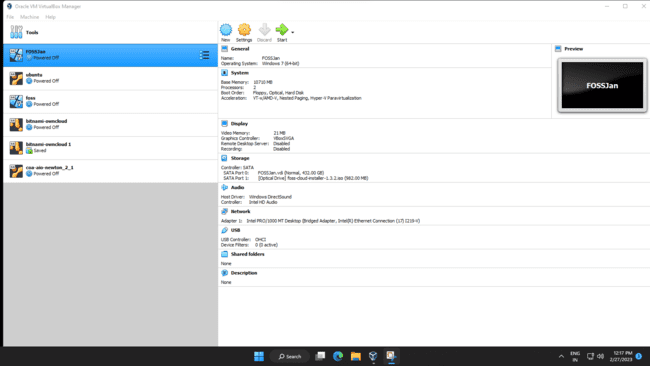
IaaS providers focus on the organization's core business rather than on IT infrastructure.

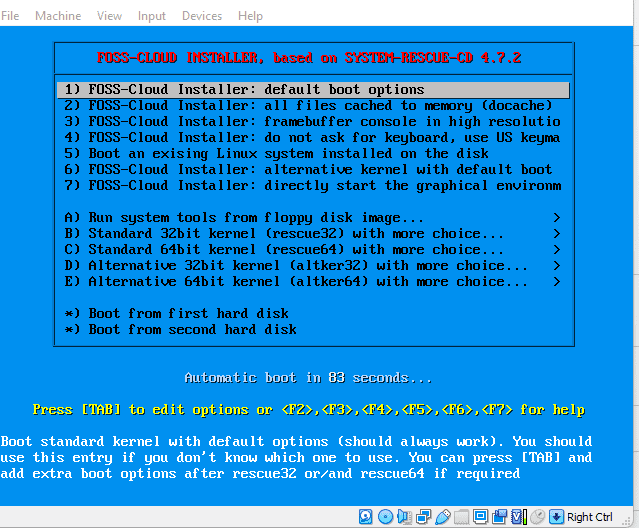
**5. On-demand scalability**

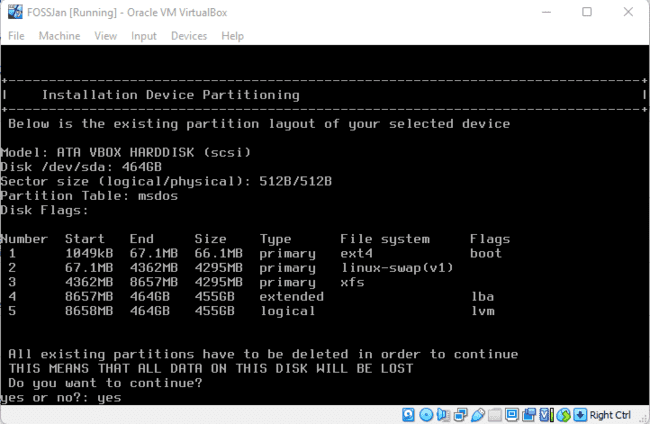
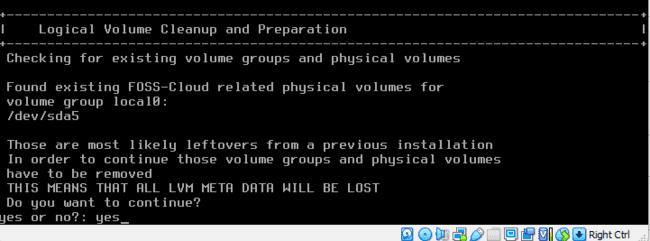
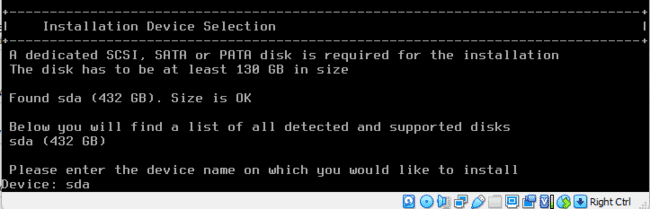
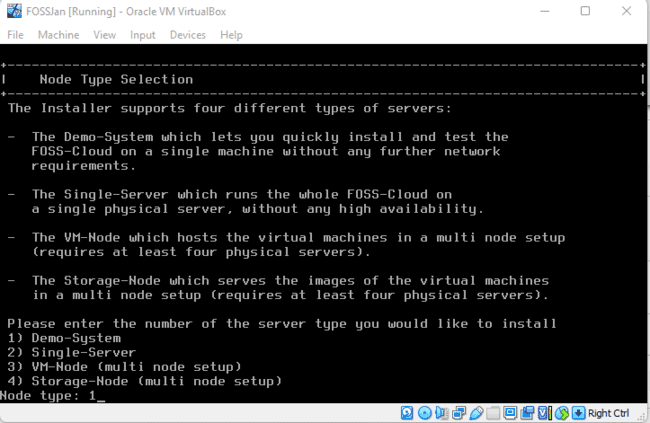
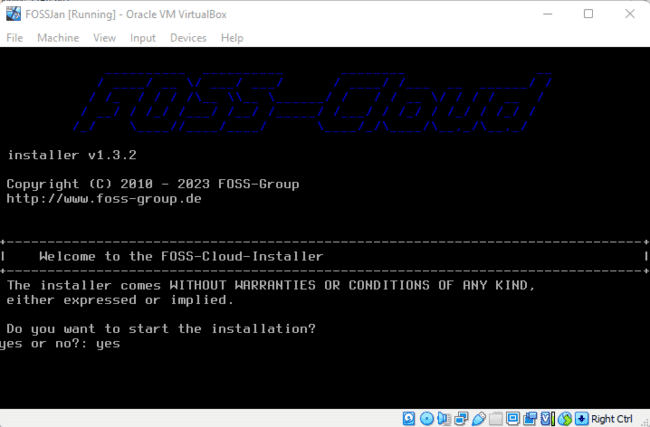
On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

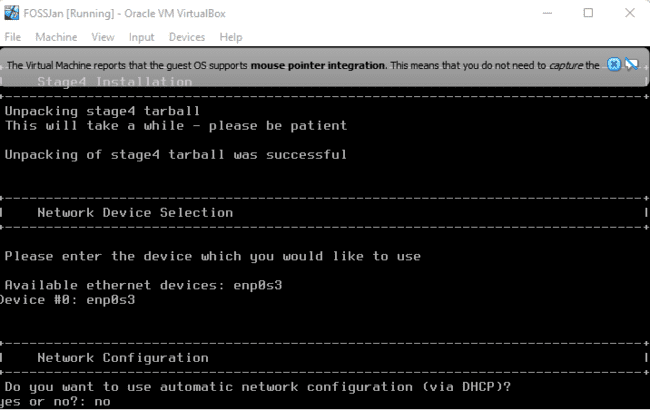
**Methods and Steps:**

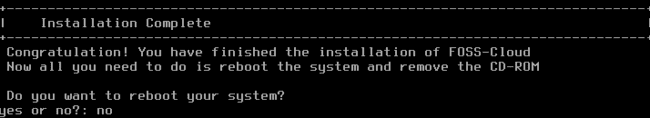
1. Using FOSS Demo / FOSS Server.

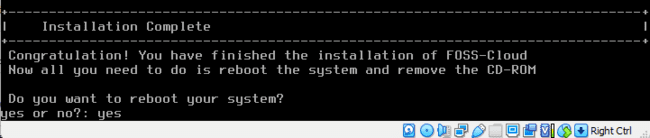
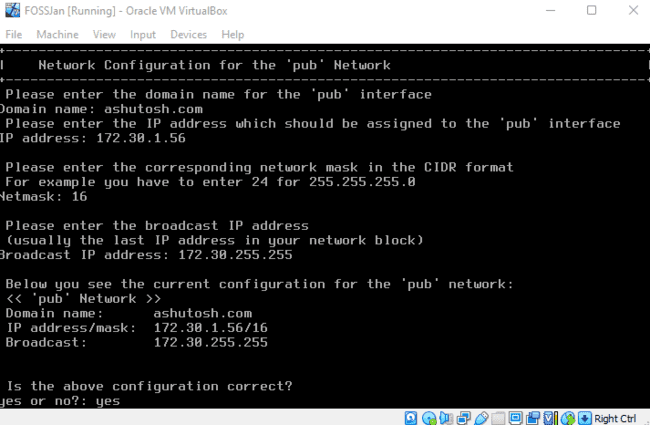
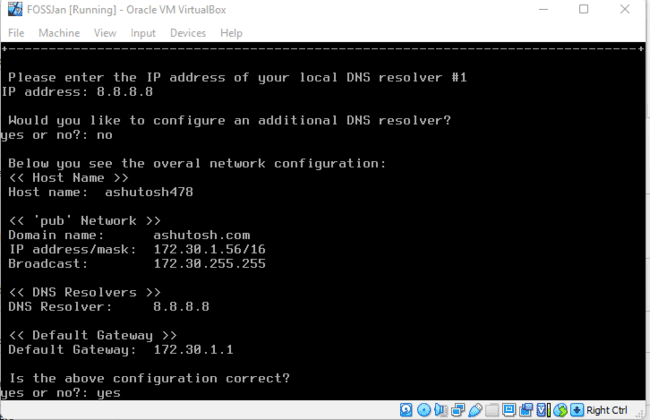
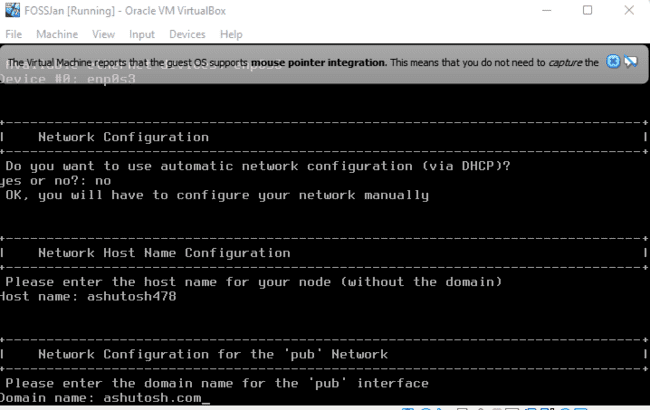
INSTALLATION:  




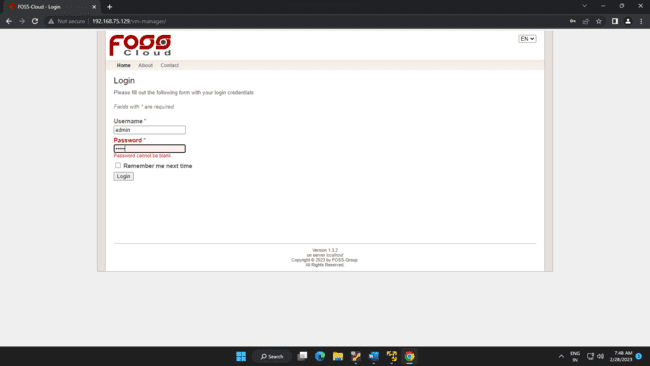




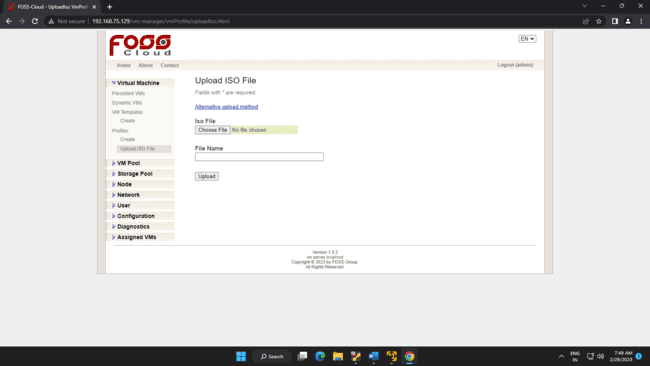




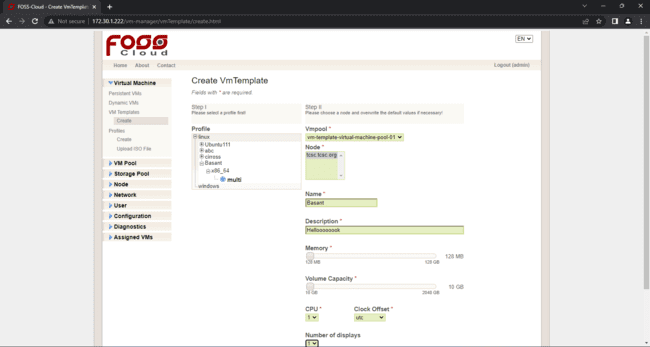
**Step 1:**After installation, it will show you  an IP Address. Put it in your browser to access your administrator page. The default user credentials are user: admin and password: admin. For root login – username- root and password – password.

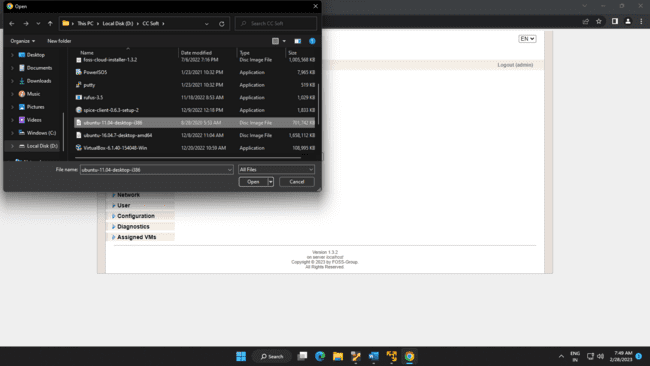
\

**Step 2:**The first screen after login shows many options to install and deploy any virtual machine. To install a virtual machine click on Virtual Machine-> Upload ISO File option and upload the bootable ISO file. Here, we are going to upload Linux Elementary OS ISO.

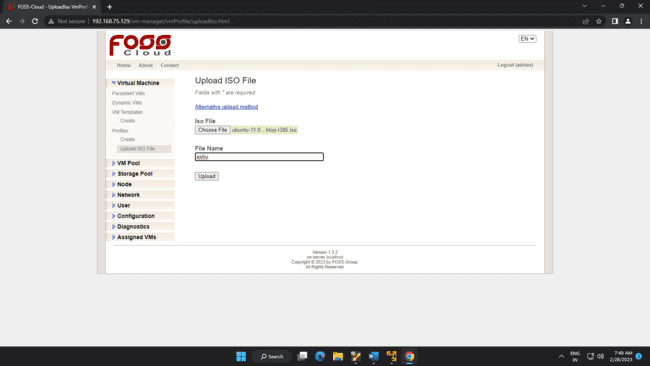


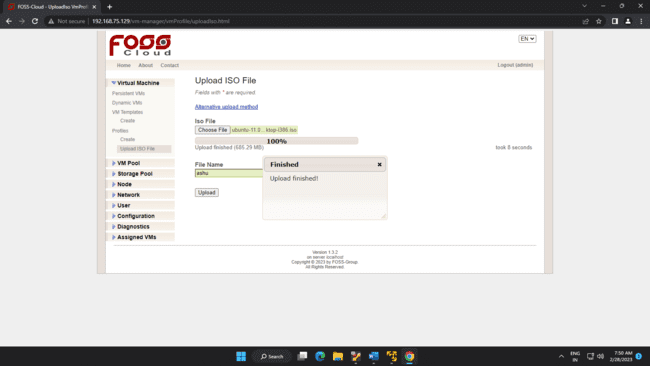
**Step 3:**Once you uploaded the file, create VmTemplate. In this option you are basically configuring your virtual machine’s storage location, CPU, Memory, Node etc. Here, you will find single nodes and VM pool in respective options because everything  was installed at the single server.

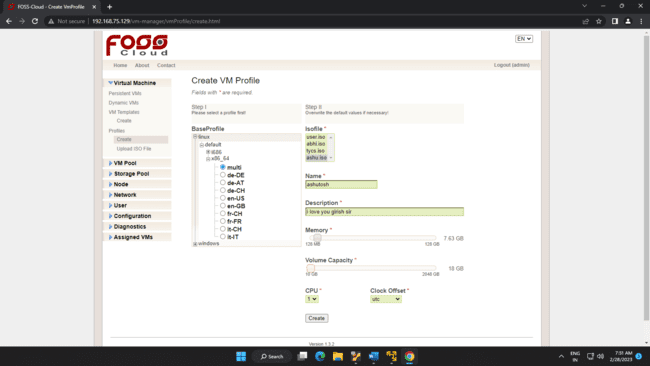


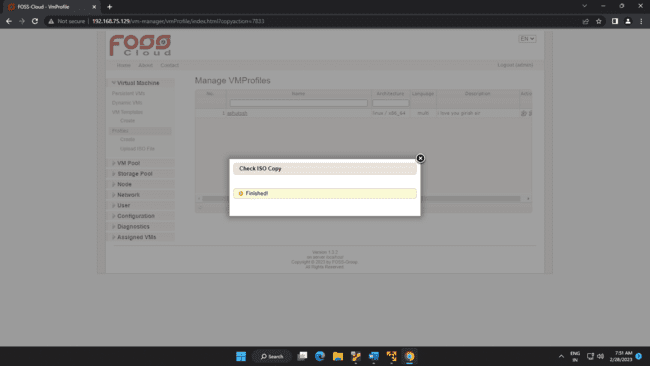


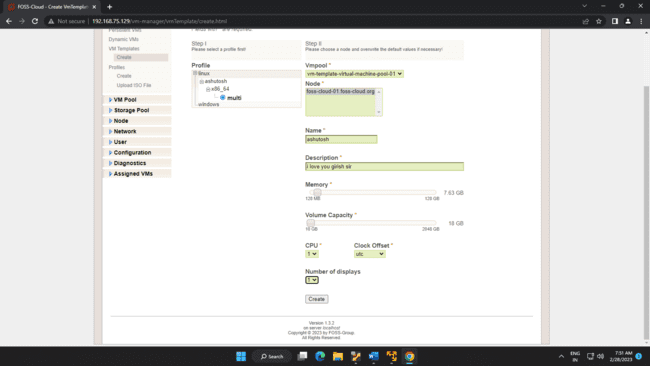
**Step 4:**Now, click on VMTemplates  and you will see a template which you have created in step 4. To start your machine go to Run action Tab and click on the green arrow. Under status tab, it shows the running text with the green circle which shows that your machine is running without any errors. To view your virtual machine click on a blue square box under Action Tab.

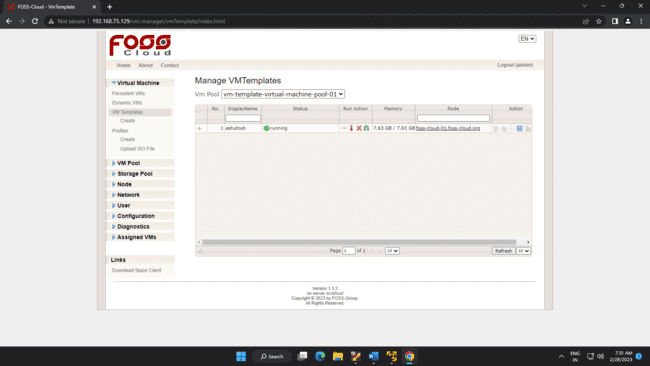


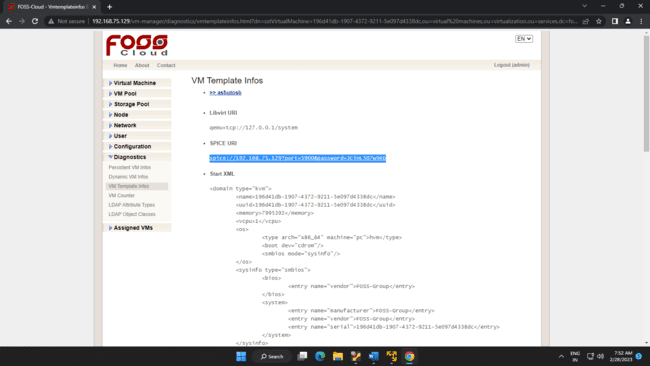




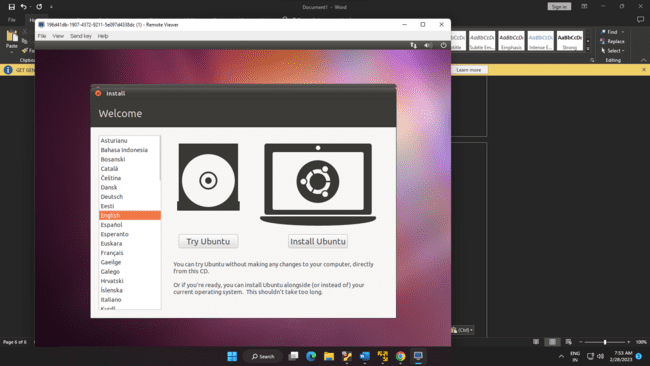




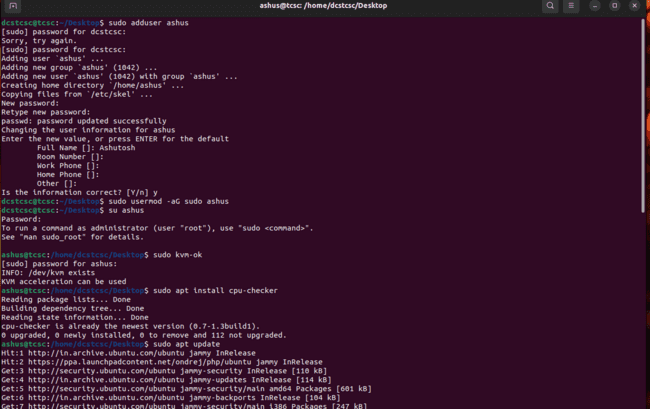


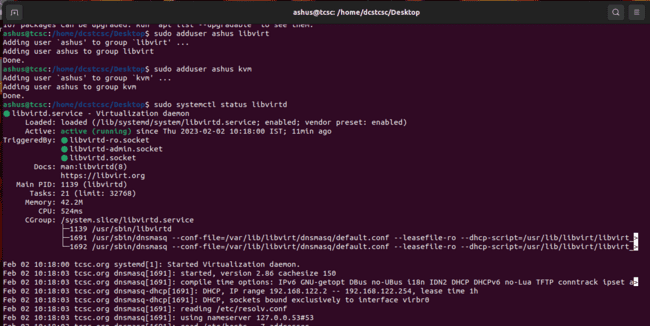


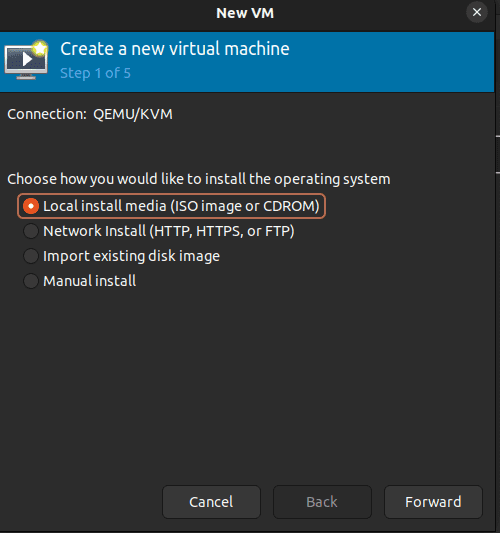


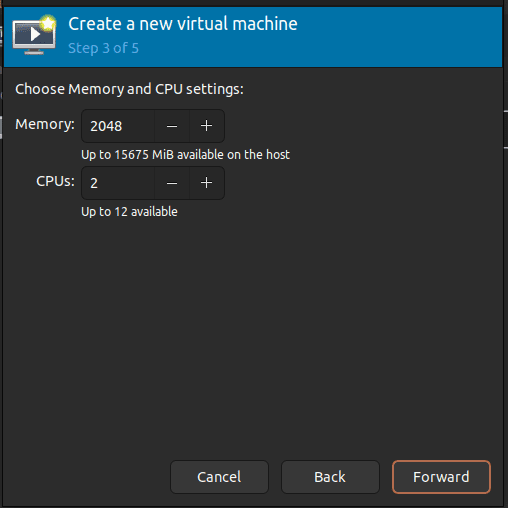
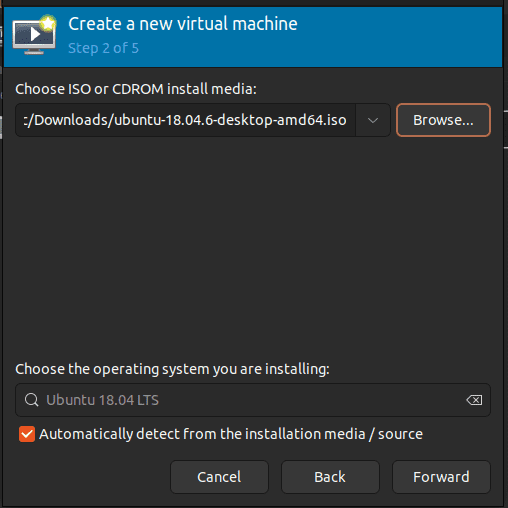


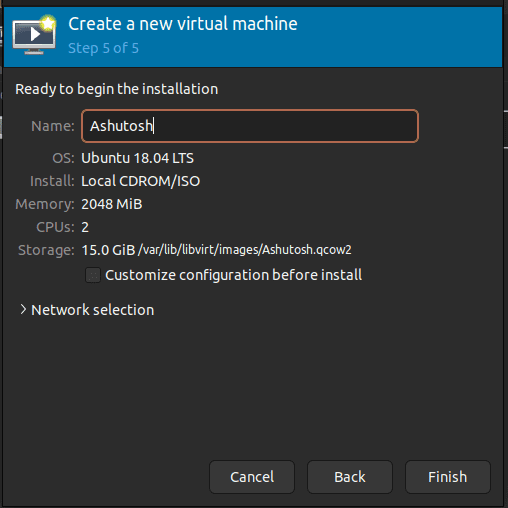
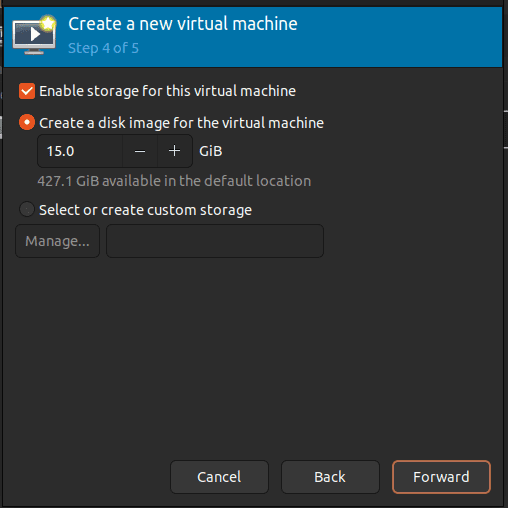
B. USING Ubuntu and KVM

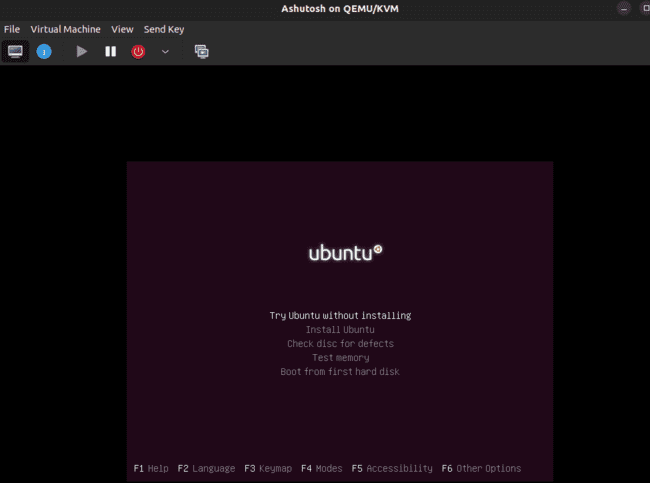
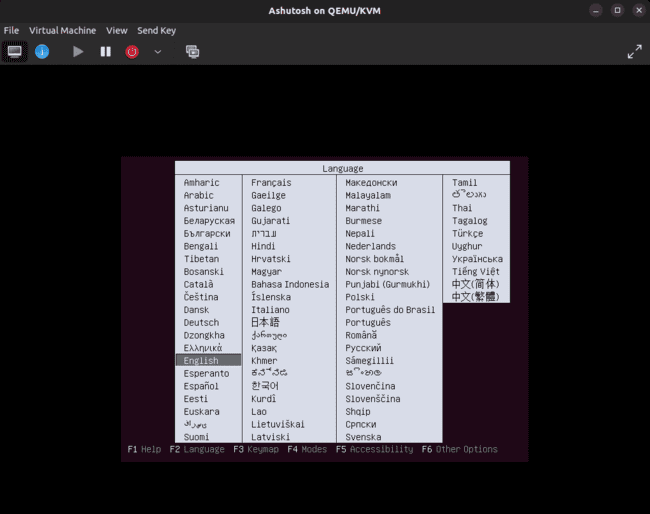


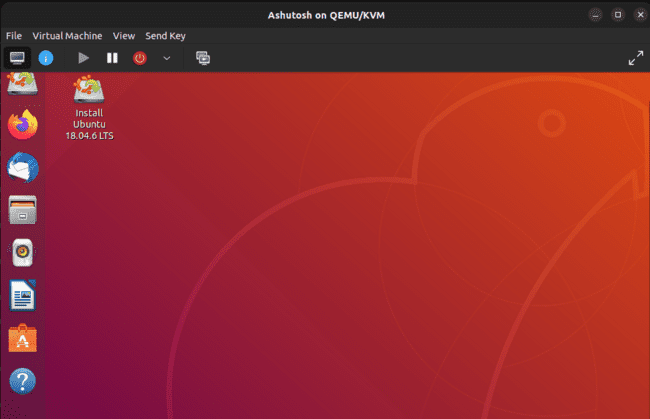






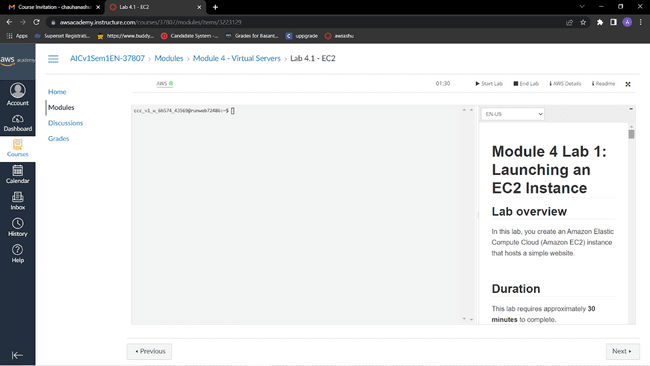






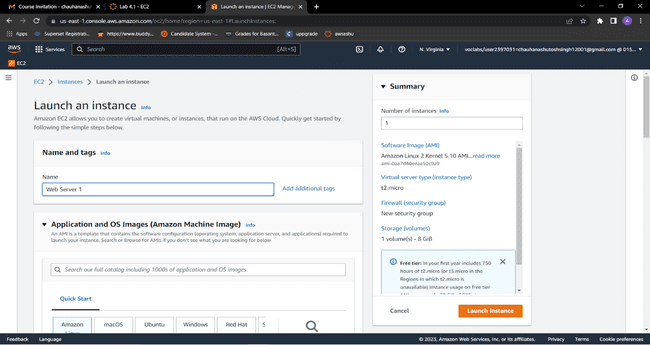
D. GCP/AWS/IBM/Azure/…

1. Choose the **Services** menu, locate the **Compute** services, and select **EC2**.

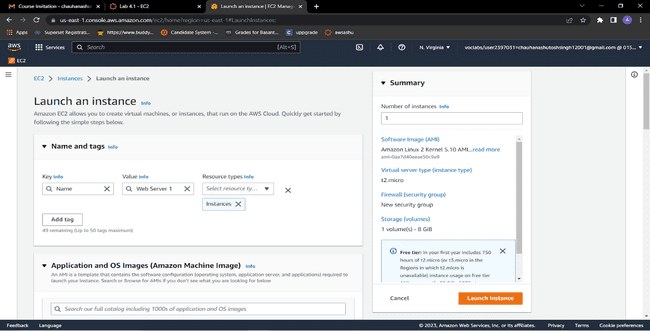


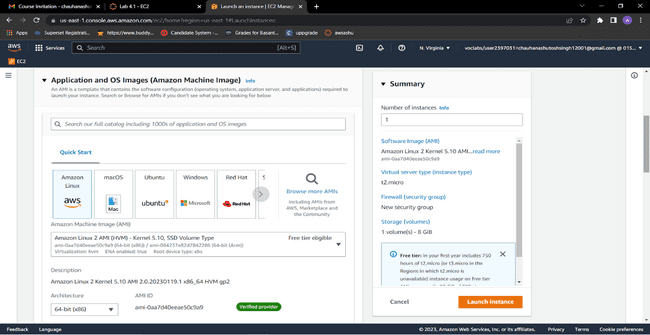
2.Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.

3.Give it the name Web Server 1



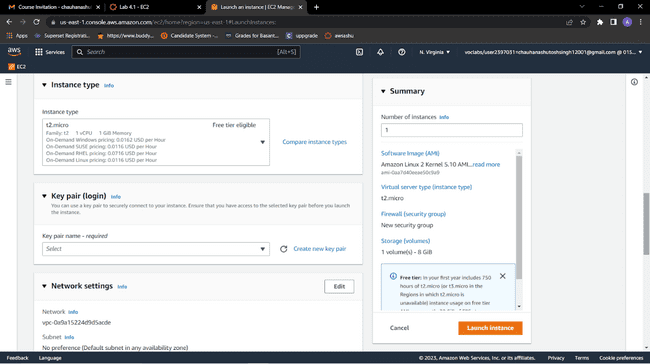
4.Choose an AMI from which to create the instance:

* In the list of available *Quick Start* AMIs, keep the default **Amazon Linux** AMI selected.
* Also keep the default **Amazon Linux 2 AMI (HVM)** selected.  
  The type of *Amazon Machine Image (AMI)* you choose determines the Operating System (OS) that will run on the EC2 instance that you launch. In this case, you have chosen Amazon Linux 2 as the guest OS.



5.In the *Instance type* panel, keep the default t2.micro selected.

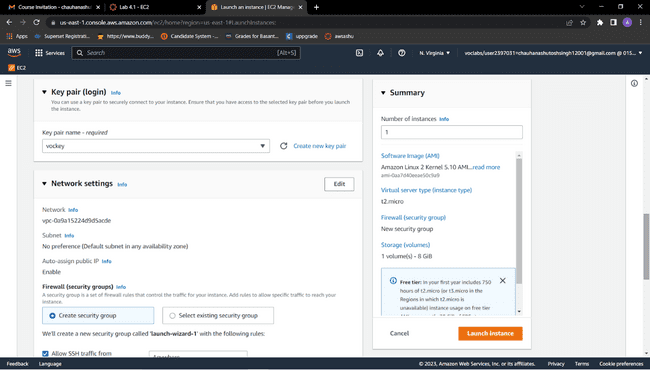
6.Select the key pair to associate with the instance From the Key pair name menu, select vockey.

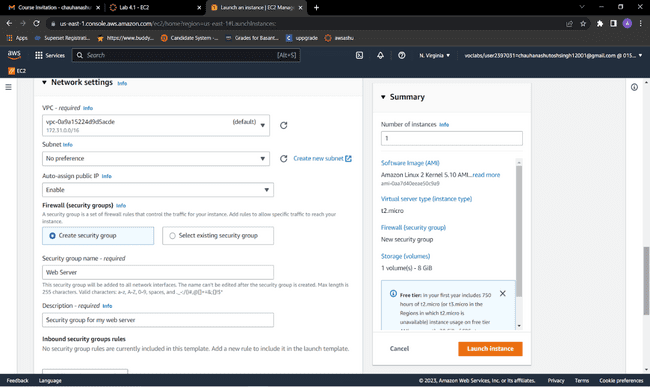


7.Next to Network settings, choose **Edit**.

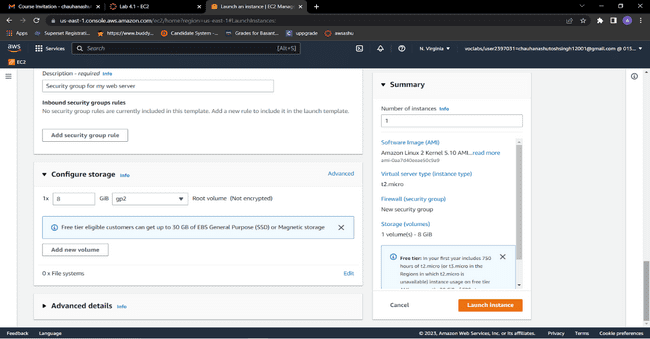
8.Keep the default *VPC* and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.

9.Under *Firewall (security groups)*, keep the default **Create security group** option chosen.



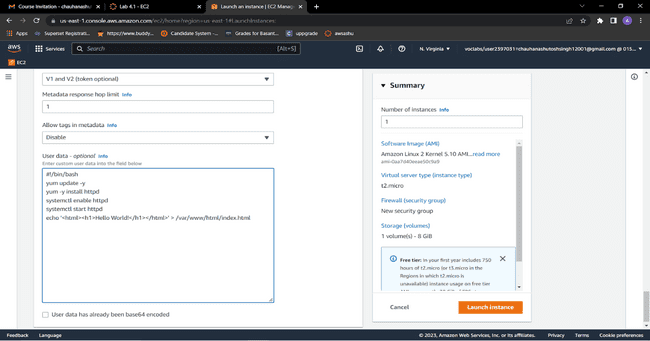


1. Configure a new security group:
   * Keep the default selection **Create a new security group**.
   * **Security group name:** Clear the text and enter Web Server
   * **Description:** Clear the text and enter Security group for my web server
   * Choose **Remove** to remove the default SSH inbound rule.

11. In the *Configure storage* section, keep the default settings.

12. Configure a script to run on the instance when it launches:

* Expand the **Advanced details** panel.
* Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:

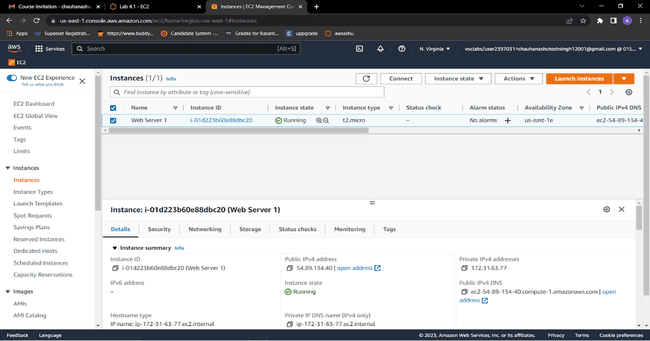
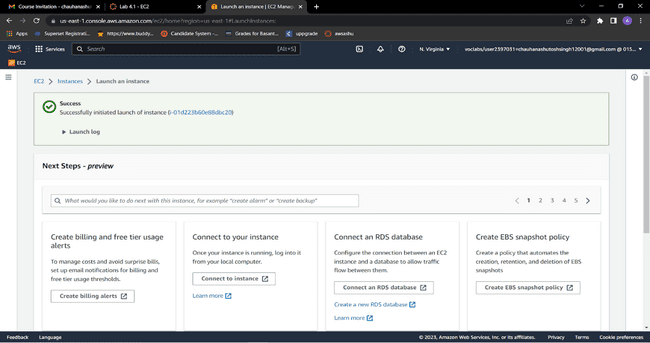


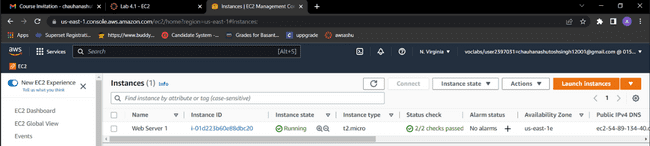
13. At the bottom of the **Summary** panel on the right side of the screen choose **Launch instance** You will see a Success message.

14. Go to  **View all instances**

15. Before you continue, wait for your instance to display the following:

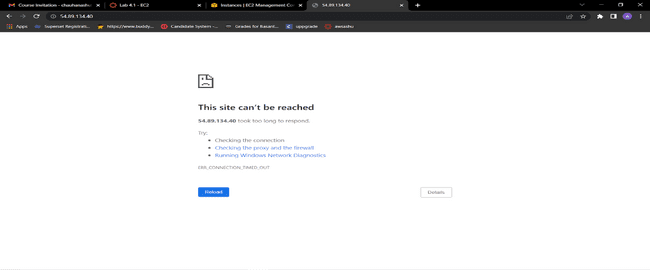
* **Instance state:** *Running*
* **Status check:** *2/2 checks passed*

**

**

14.From the **Details** tab, copy the **Public IPv4 address** value of your instance to your clipboard.

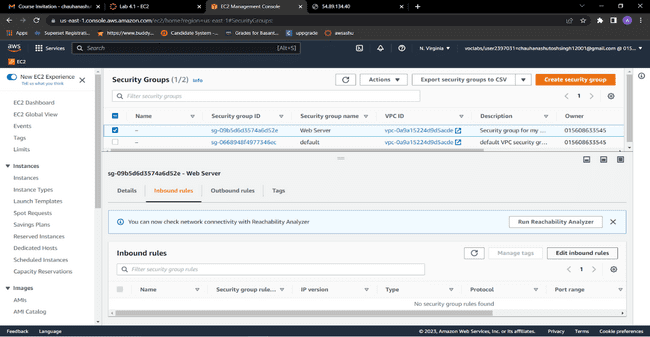
Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**.The webpage does not load. You must update the security group to be able to access the page.



15.Return to the **EC2 Management Console** browser tab.

16.In the left navigation pane, under **Network & Security**, choose **Security Groups**.

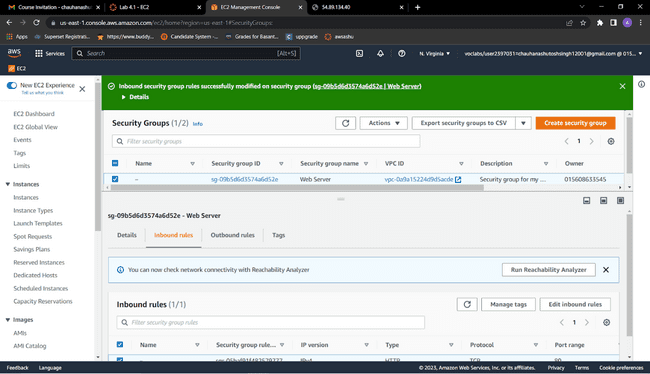
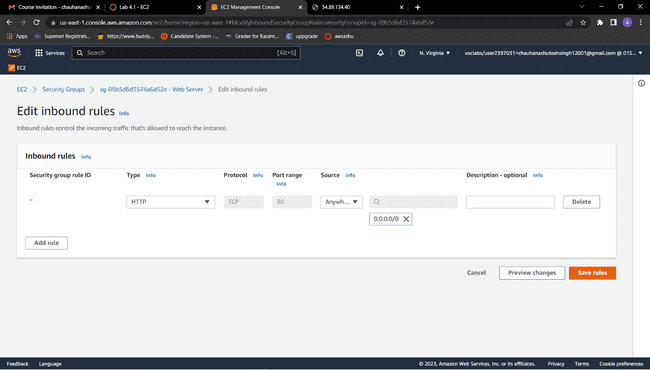
17.Select the **Web Server** security group, which you created when launching your EC2 instance.

18.In the lower pane, choose the **Inbound rules** tab.

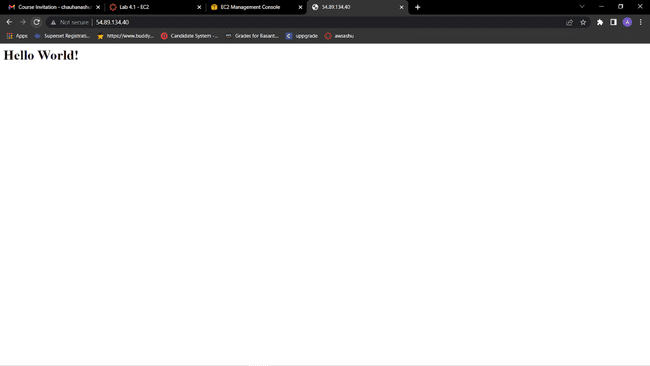
19.Choose **Edit inbound rules**, and then choose **Add rule**.Configure the following:

* **Type:** HTTP,**Source:** Anywhere-IPv4,Choose **Save rules**

The new inbound HTTP rule creates an entry for IPv4 IP (0.0.0.0/0) and IPv6 IP addresses (::/0).



20.Return to the tab that you used to try to connect to the web server.Refresh the page.The page should display the message *Hello World!*

**

**Conclusion**: Successfully performed Iaas ,The IaaS cloud computing platform vendor can get access to your sensitive data.

**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.

2. Application frameworks

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.

3. Databases

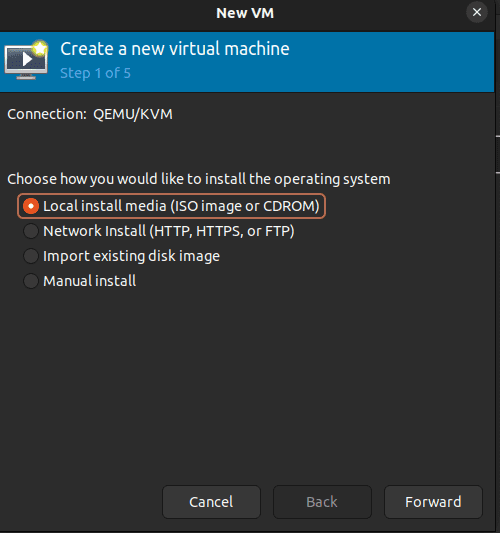
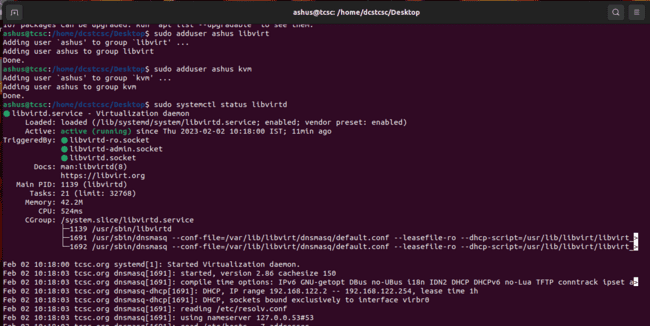
PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

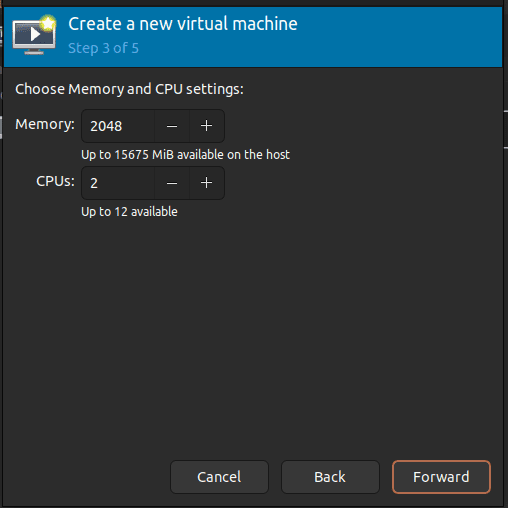
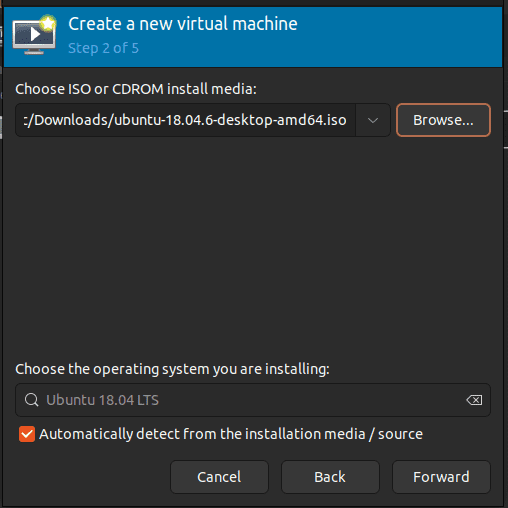
4. Other tools

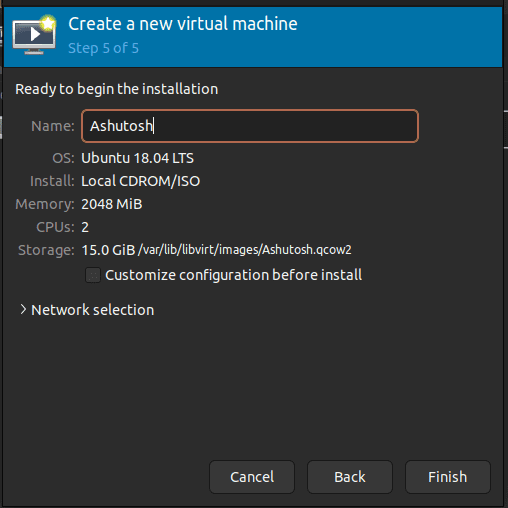
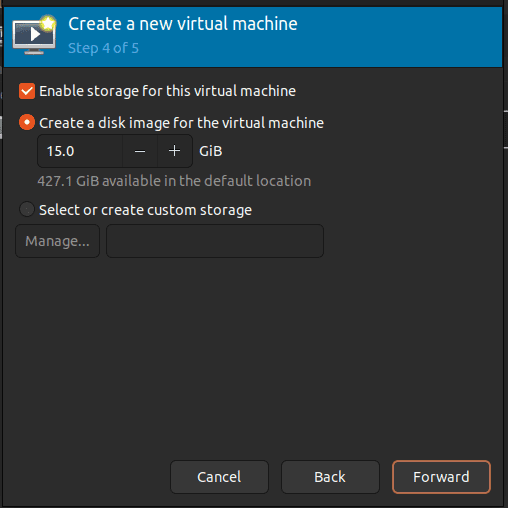
PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

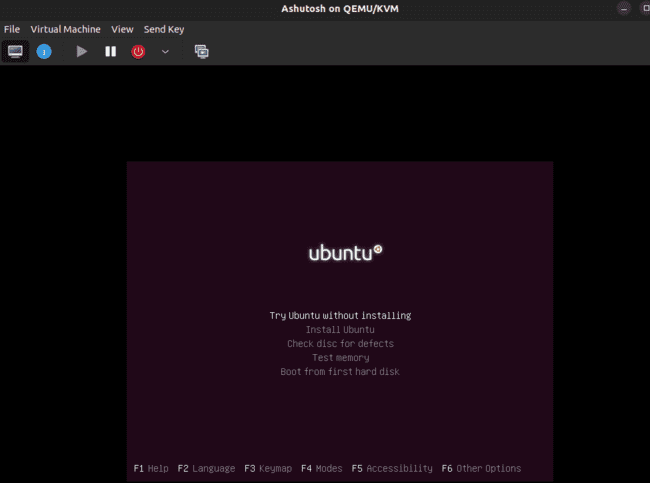
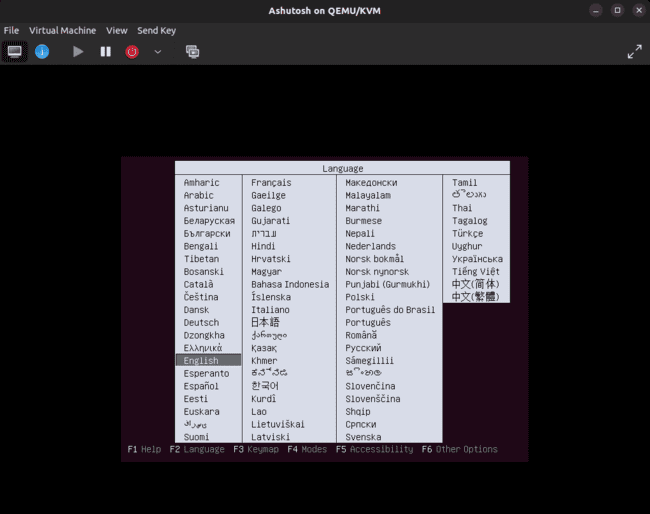
**Method and Steps:**

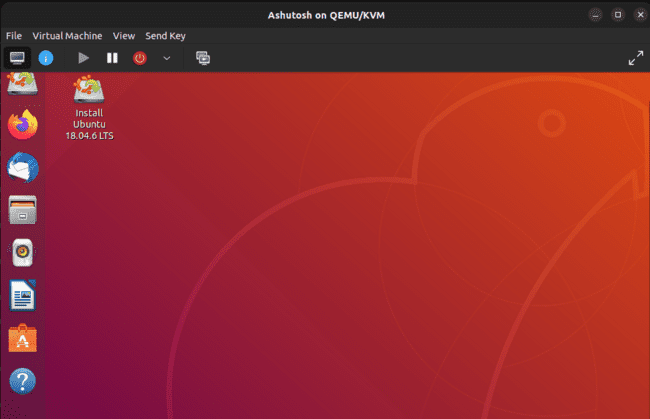
1. Using KVM.

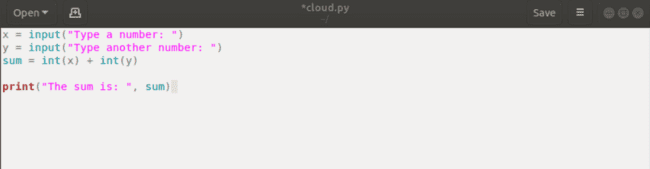












**CONCLUSION :**

**There are the following advantages of PaaS -Simplified Development , Lower risk, Prebuilt business functionality, Instant community, Scalability**

**Disadvantages of PaaS cloud computing layer - Vendor lock-in , Data Privacy, Integration with the rest of the systems applications.**

**Practical No. 03**

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

**Theory:** 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.

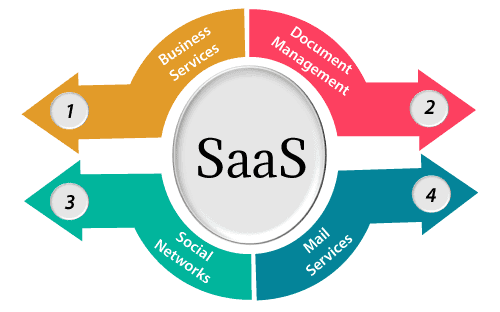
There are the following services provided by SaaS providers -

**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.

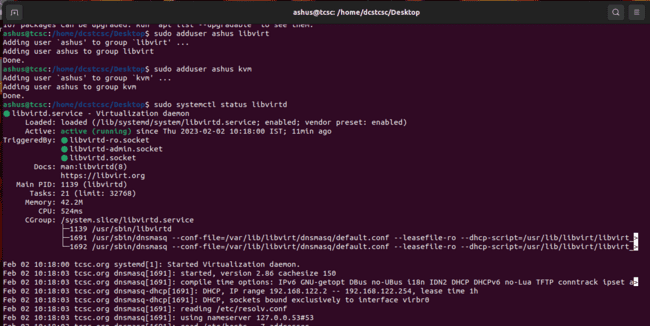
**Social Networks** - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

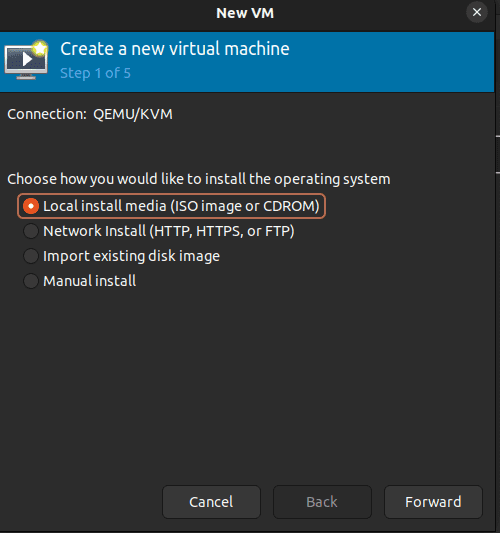
**Mail Services** - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

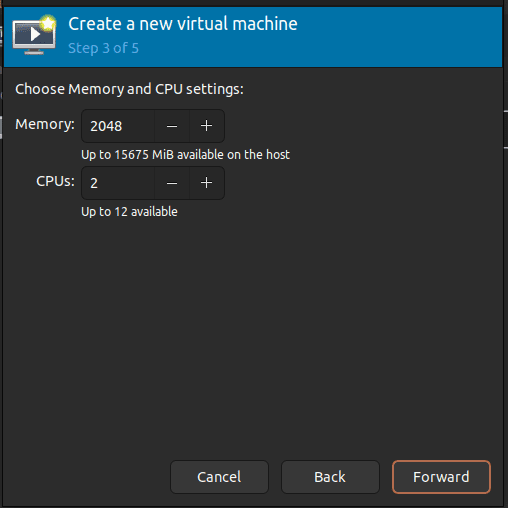
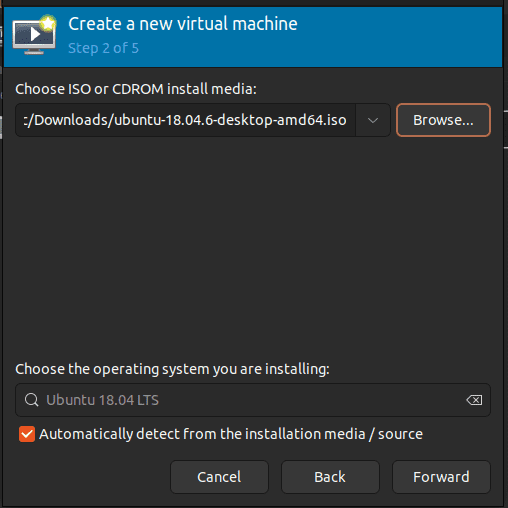


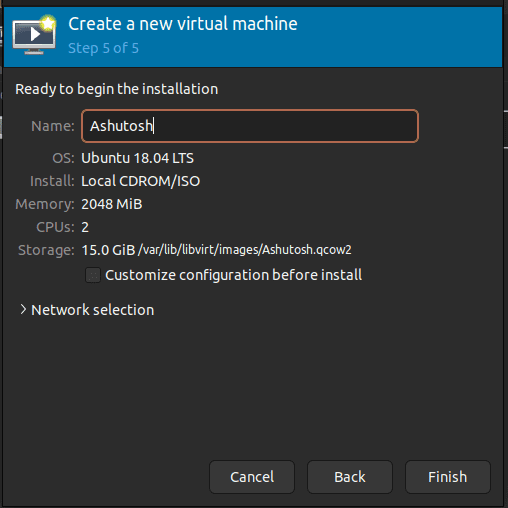
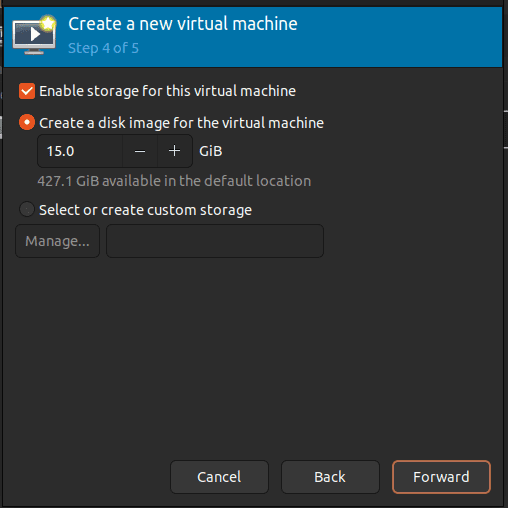
**Methods and Steps:**

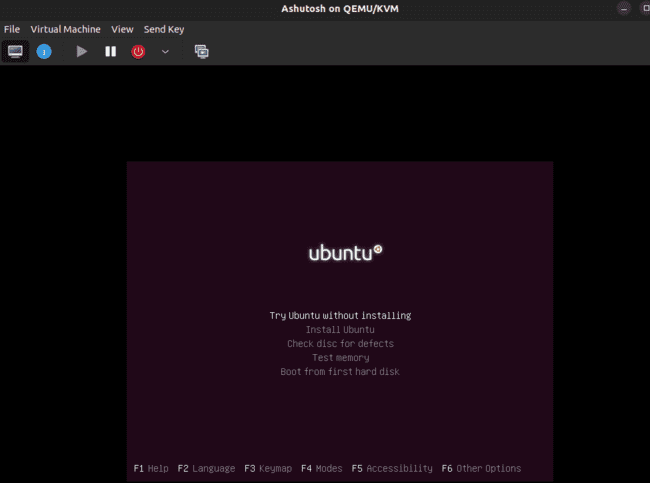
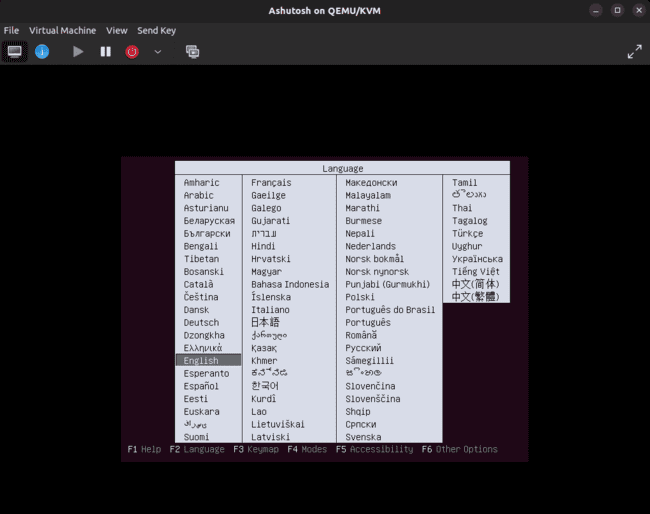
1. Using FOSS Server

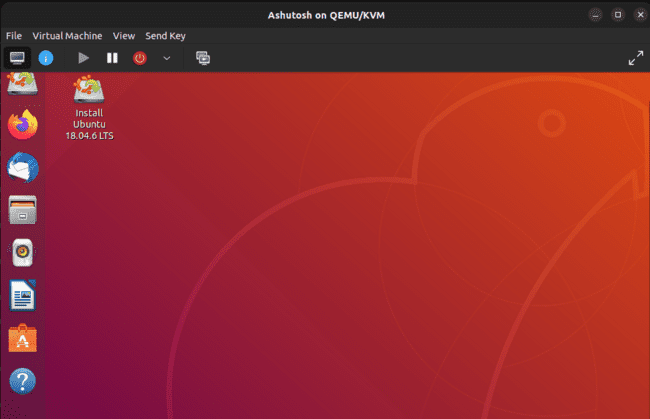


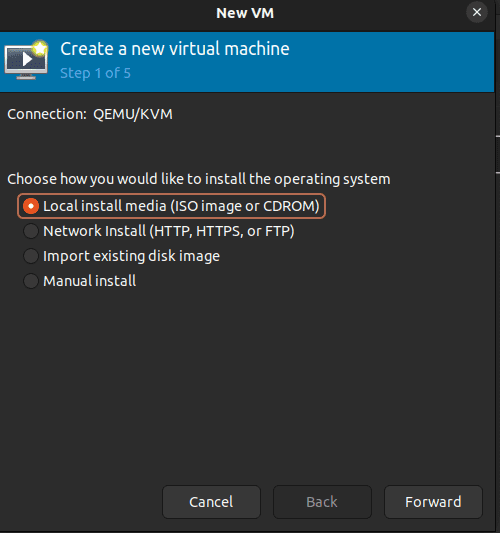
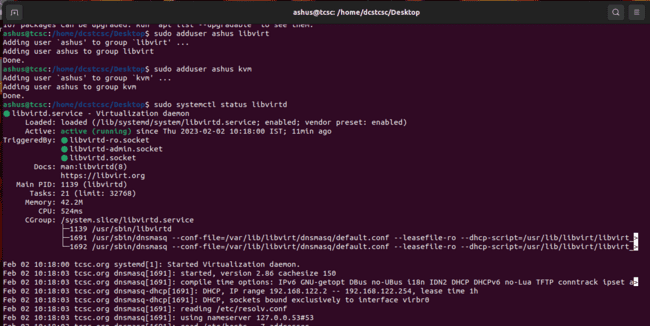


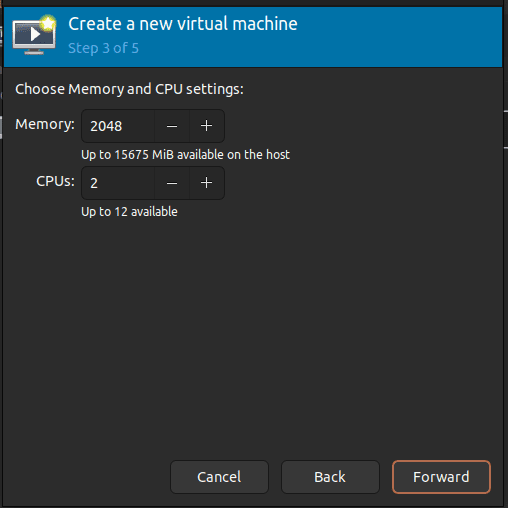
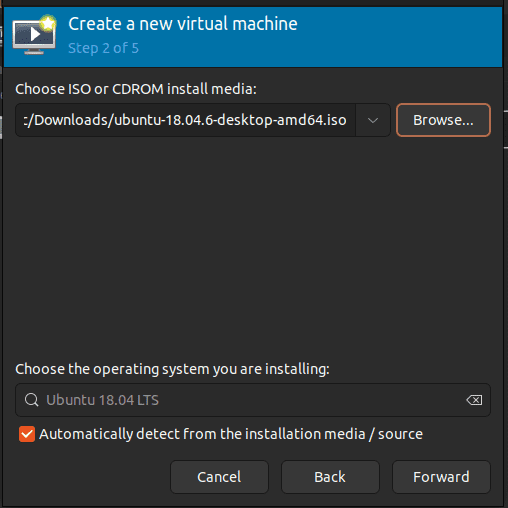


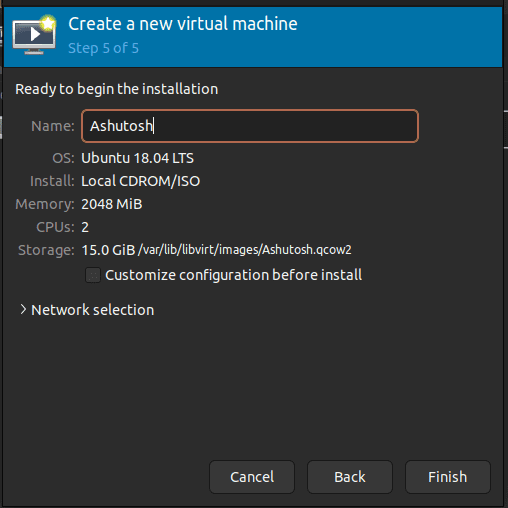
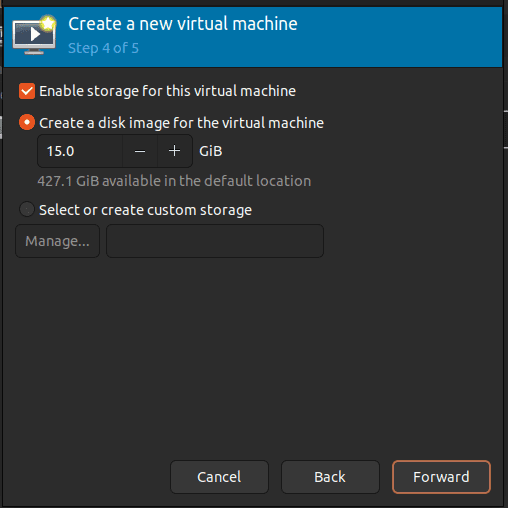


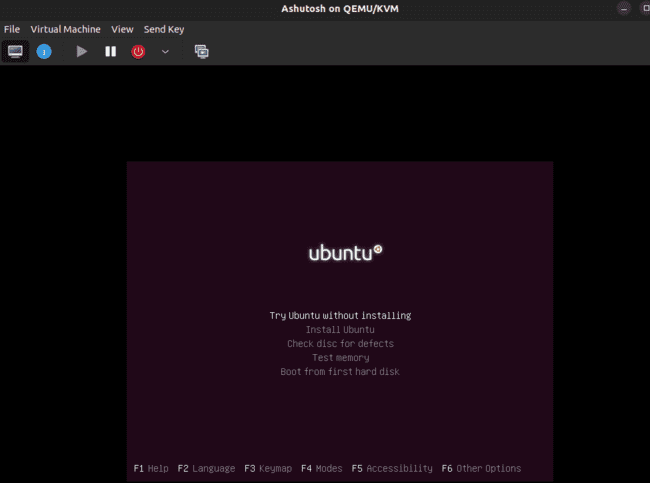
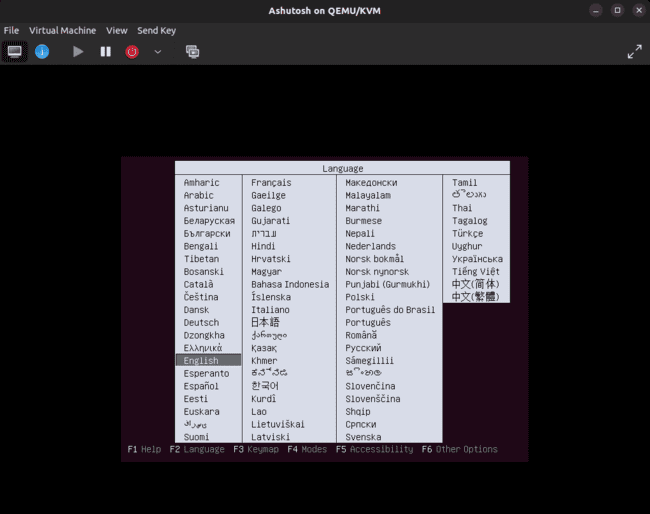


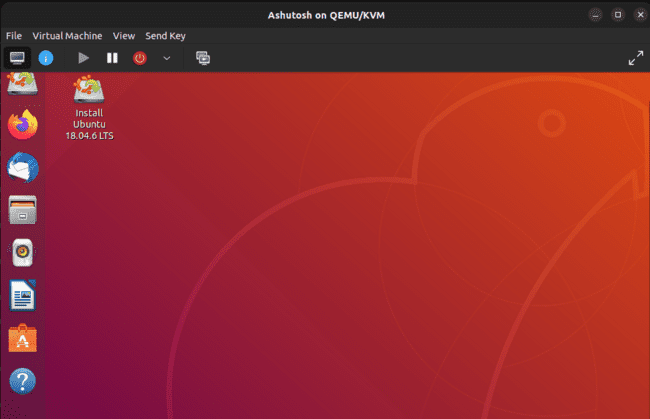


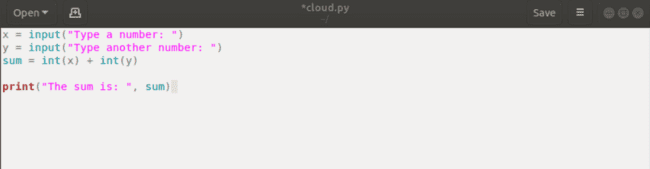


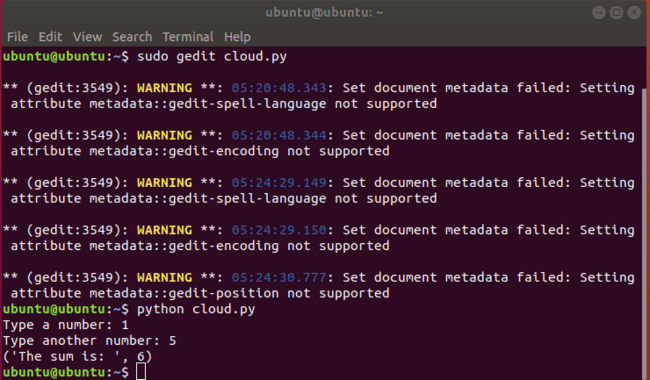




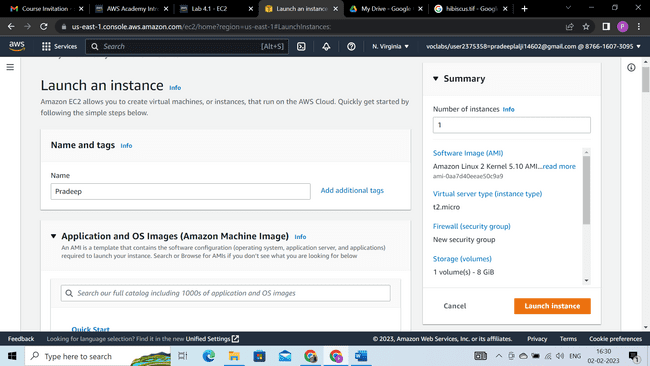


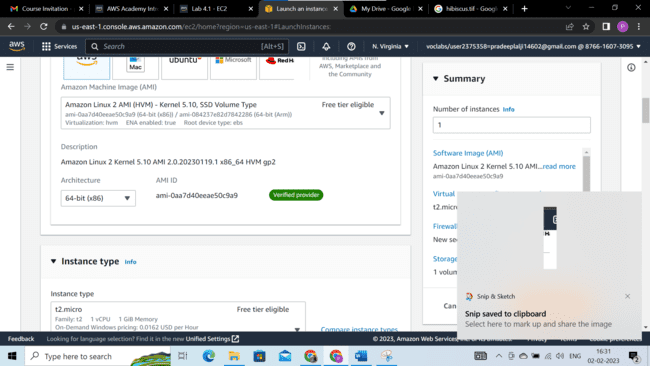


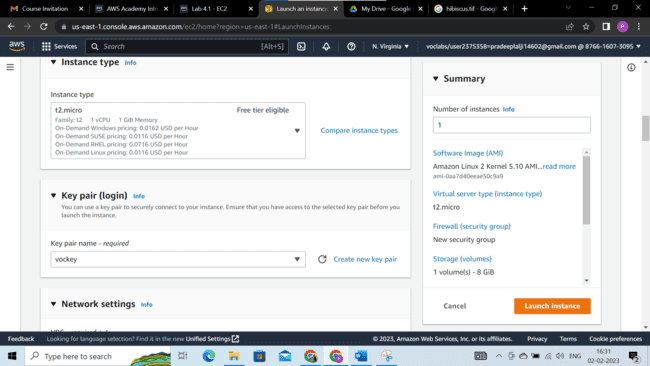


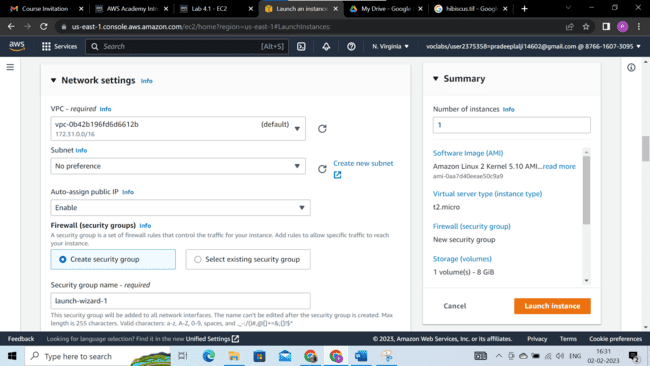


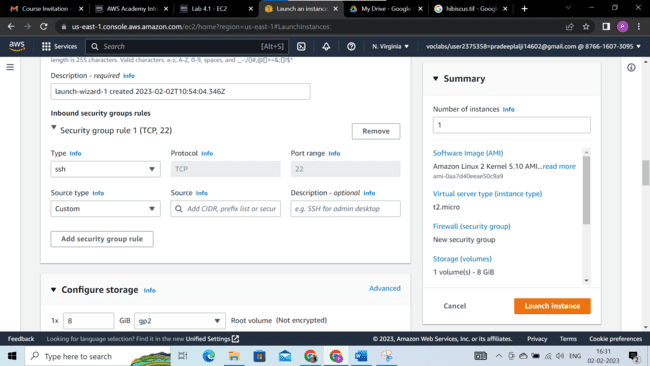
. B.GCP/AWS/IBM/AZure/...

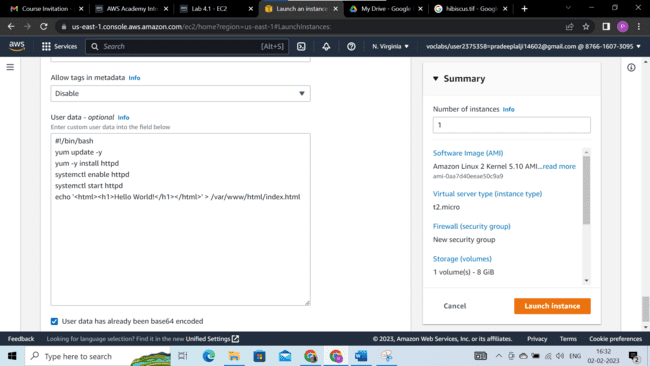


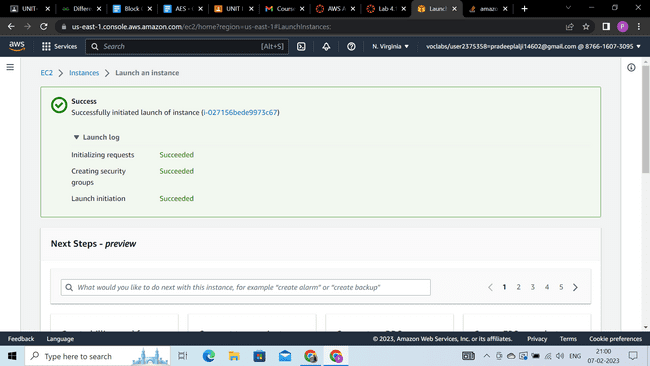


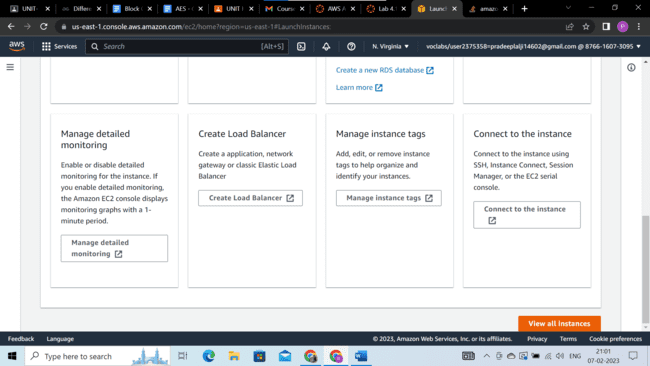


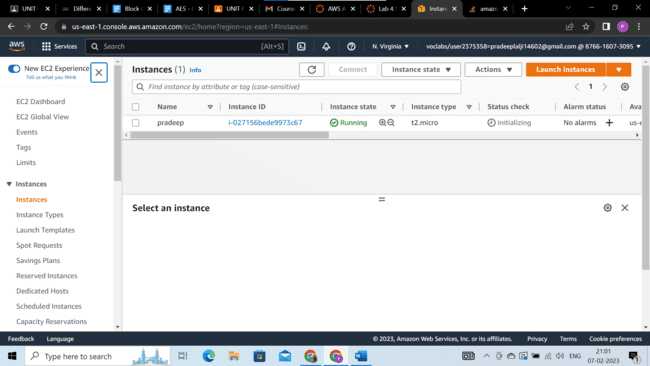


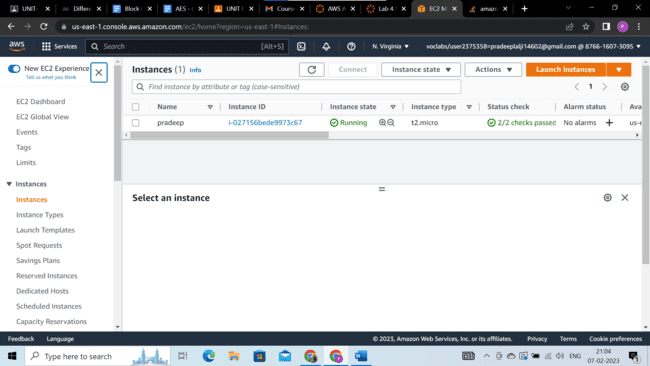


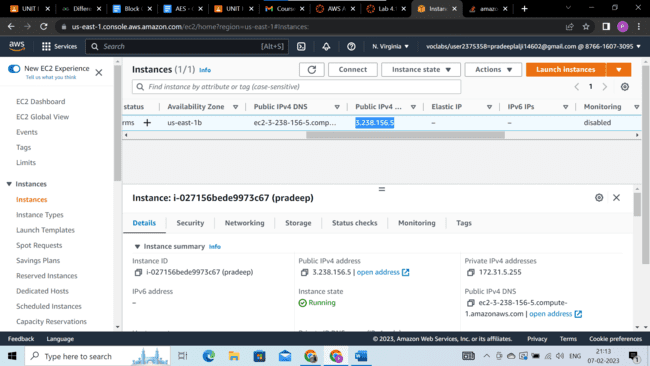


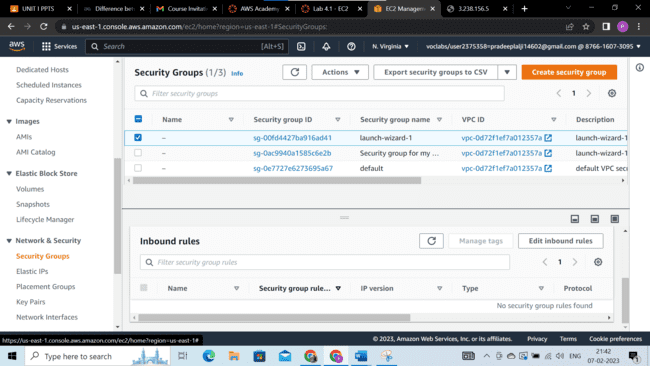


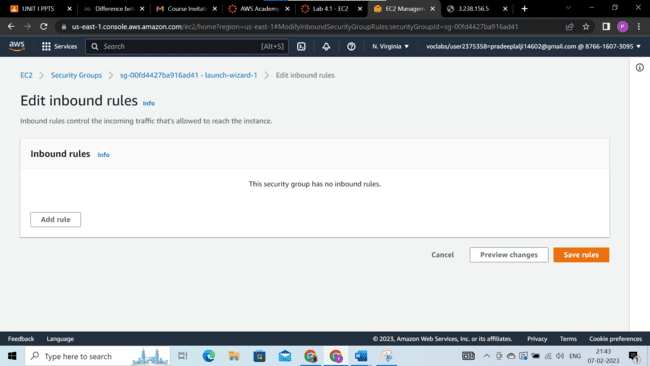


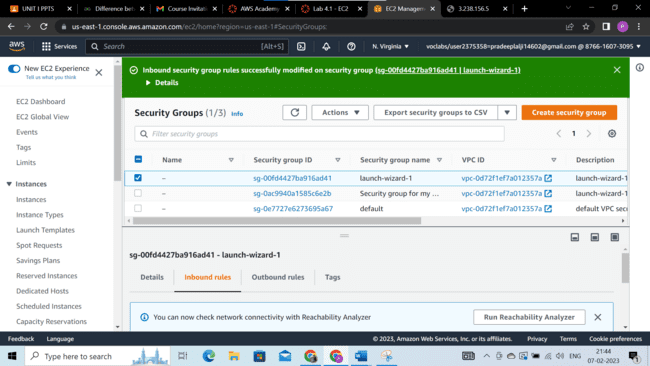


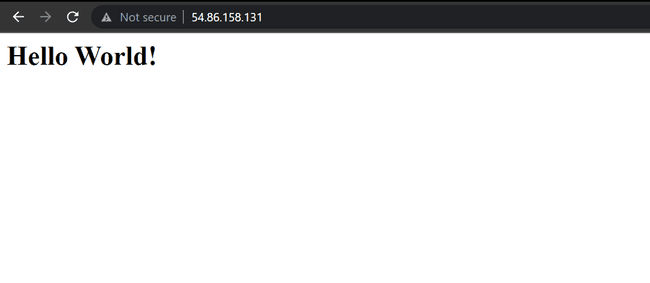












## CONCLUSION :

## Advantages of SaaS cloud computing layer :**SaaS is easy to buy,** **One to Many** ,**Less hardware required for SaaS,** **Low maintenance required for SaaS,** **No special software or hardware versions required.**

## Disadvantages of SaaS cloud computing layer :**Security,** **Latency issue,** **Total Dependency on Internet,** **Switching between SaaS vendors is difficult.**

**Practical No 4**

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

**Theory:** Storage as a service (STaaS) is a managed service in which the provider supplies the customer with access to a data storage platform. The service can be [delivered on premises](https://www.techtarget.com/searchstorage/feature/On-premises-STaaS-shifts-storage-buying-to-Opex-model) from infrastructure that is dedicated to a single customer, or it can be delivered from the public cloud as a shared service that's purchased by subscription and is billed according to one or more usage metrics.

STaaS customers access individual storage services through standard system interface protocols or application program interfaces ([APIs](https://www.techtarget.com/searchapparchitecture/definition/application-program-interface-API)). Typical offerings include bare-metal storage capacity; raw storage volumes; network file systems; storage objects; and storage applications that support file sharing and [backup](https://www.techtarget.com/searchdatabackup/definition/backup) lifecycle management.

Storage as a service was originally seen as a cost-effective way for small and mid-size businesses that lacked the technical personnel and capital budget to implement and maintain their own storage infrastructure. Today, companies of all sizes use storage as a service.

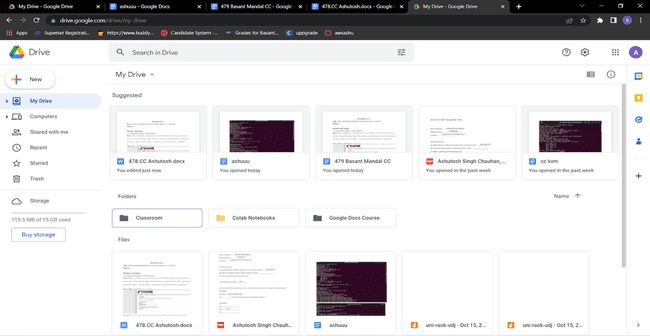
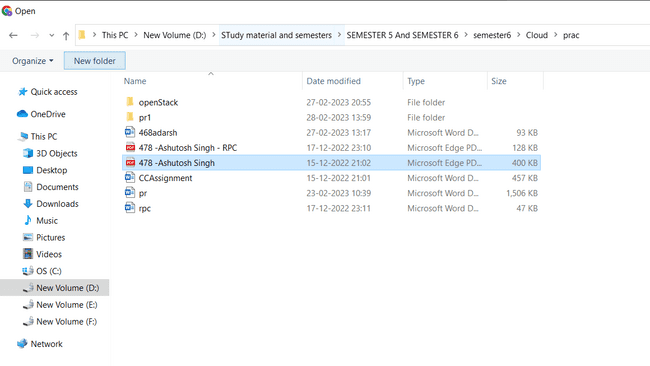
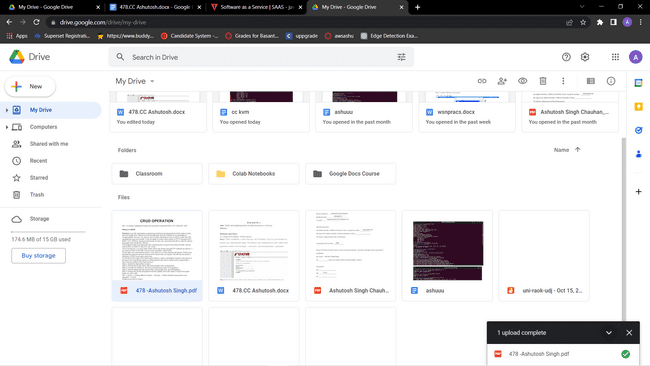
**Storage as a service in cloud computing**

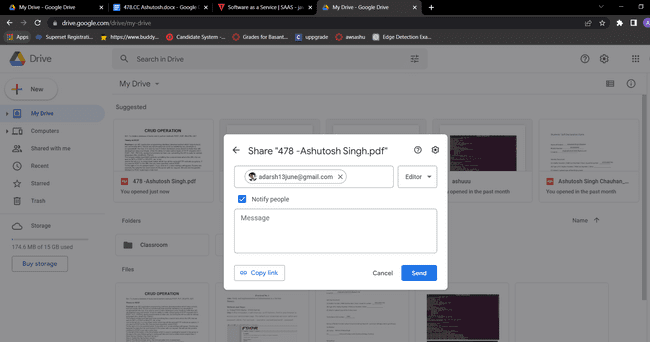
Instead of storing data on-premises, organizations that use STaaS will typically utilize a [public cloud](https://www.techtarget.com/searchcloudcomputing/definition/public-cloud) for storage and backup needs. Public cloud storage may also use different storage methods for STaaS. These storage methods include backup and restore, disaster recovery, block storage, SSD storage, object storage and bulk data transfer. Backup and restore refers to the backing up of data to the cloud, which provides protection in case of data loss. Disaster recovery may refer to protecting and replicating data from virtual machines ([VMs](https://searchservervirtualization.techtarget.com/definition/virtual-machine)).

[Block storage](https://www.techtarget.com/searchstorage/definition/block-storage) enables customers to provision block storage volumes for lower-latency [I/O](https://www.techtarget.com/whatis/definition/input-output-I-O). SSD storage is another storage type that is typically used for intensive read/write and I/O operations. Object storage systems are used in data analytics, disaster recovery and cloud applications and tend to have high latency. Cold storage is used to create and configure stored data quickly. Bulk data transfers will use disks and other hardware to transfer data.

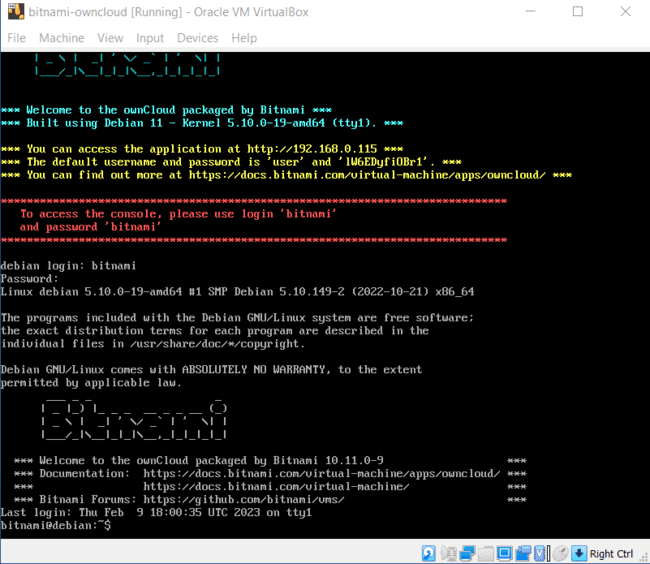
**Methods and Steps:**

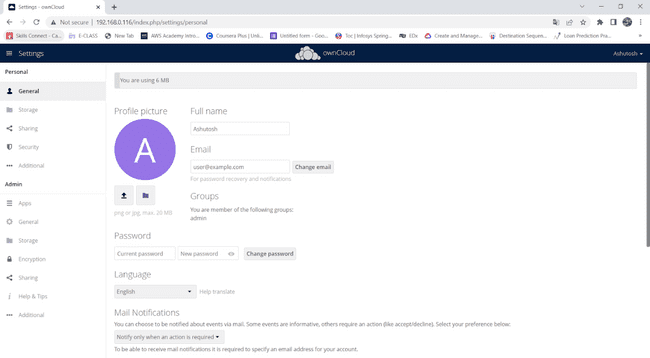
1. Google Drive

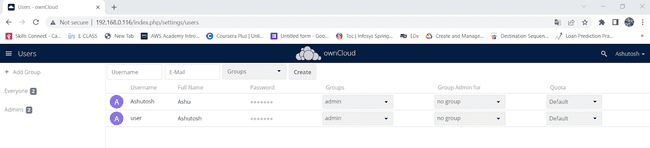
  

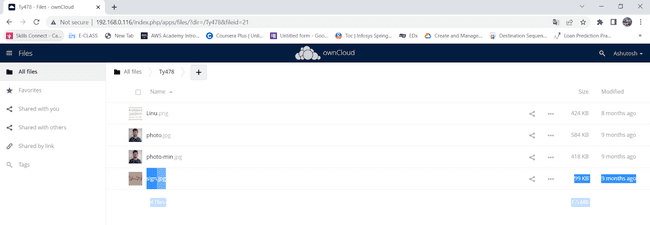


B. OwnCloud (Offline)



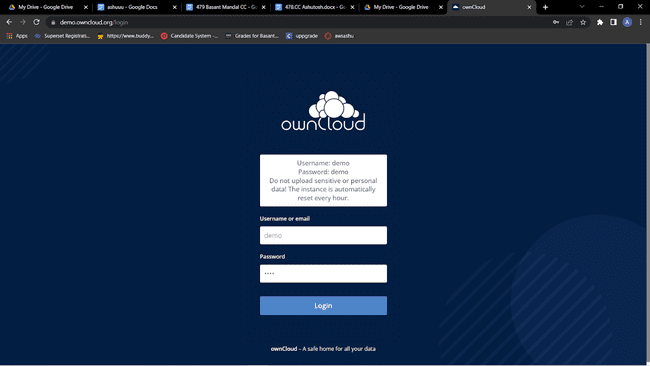


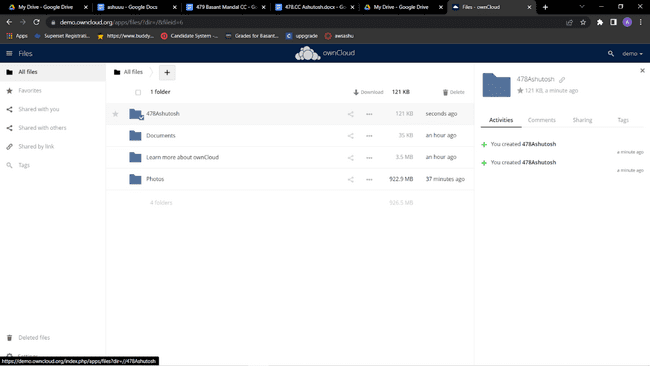


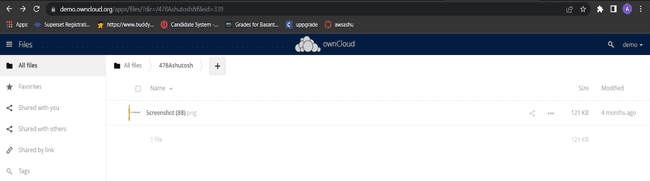


C. Owncloud (Online)

Demo.owncloud.org







**CONCLUSION :**

**Advantages of STaaS**

Key advantages to STaaS in the enterprise include the following:

* Storage costs. Personnel, hardware and physical storage space expenses are reduced.
* Disaster recovery. Having multiple copies of data stored in different locations can better enable disaster recovery measures.
* Scalability. With most public cloud services, users only pay for the resources that they use.
* Syncing. Files can be automatically synced across multiple devices.
* Security. Security can be both an advantage and a disadvantage, as security methods may change per vendor. Data tends to be encrypted during transmission and while at rest.

**Practical No. 5**

**Aim: User Management in Cloud .**

**Theory**: 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 the IT admin had dictated.

• Traditionally, user management has been grounded with on-prem servers, databases, and closed virtual 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.

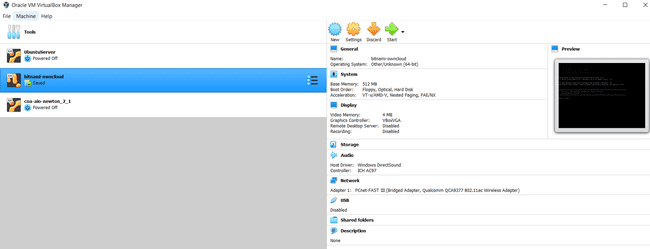
User management allows administrators to manage resources and organize users according to their needs and roles while maintaining the security of IT systems. Administrators need powerful user management capabilities that can allow them to group users and define flexible access policies.

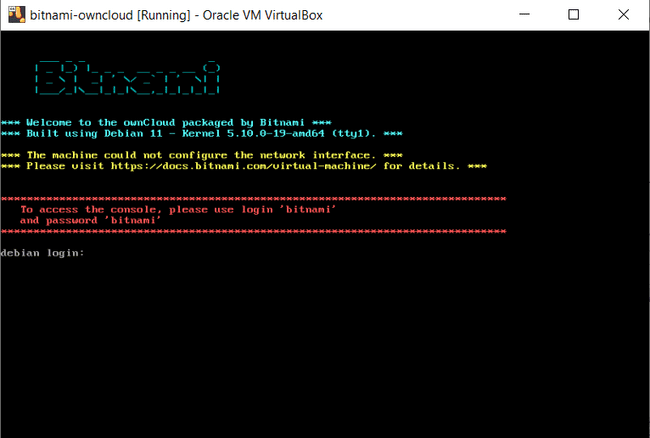
For end-users, many parts of user management are invisible. When users are exposed to user management—for example, when they use a login box to access an application—they expect the interaction to be simple and seamless. Login is a frequently-performed, critical operation, meaning that any delay or malfunction annoys users and hurts productivity.Many organizations recognize that on-premise IdP solutions are insufficient for the modern IT environment. Users increasingly rely on cloud services and access corporate systems remotely, often via personal devices, and traditional IdP cannot address these use cases.

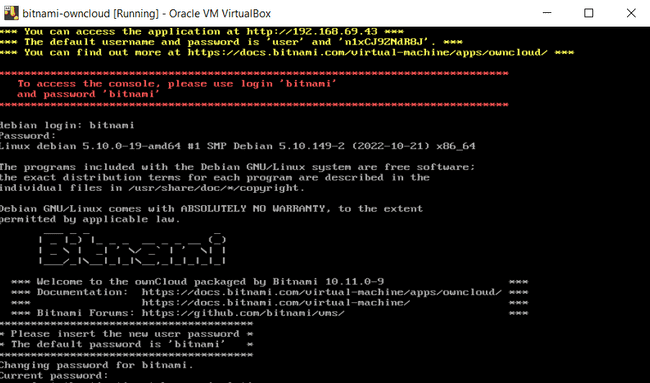
Organizations must find a way to manage secure access for a distributed environment. At the same time, users demand the same simplicity of popular services like Google and Facebook in their work environment. These challenges are making user management more important and more complex than ever before.

**Methods and Steps:**

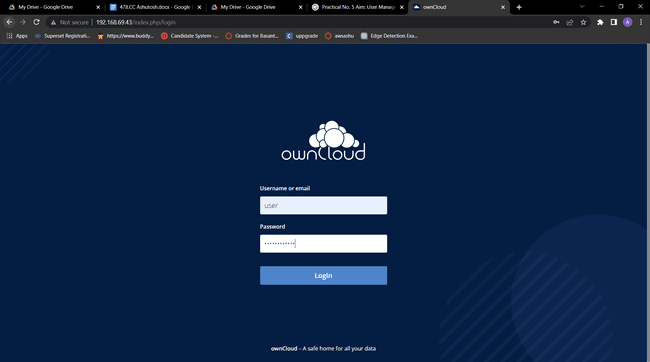
1. OwnCloud(local)

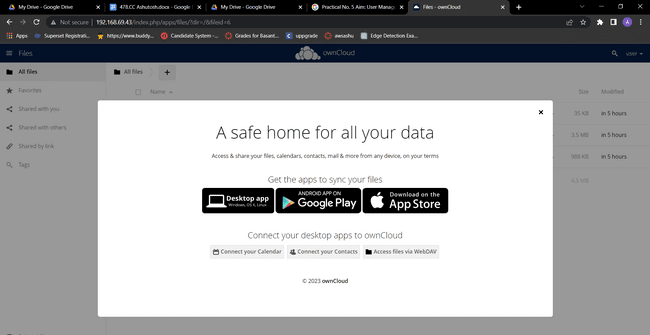


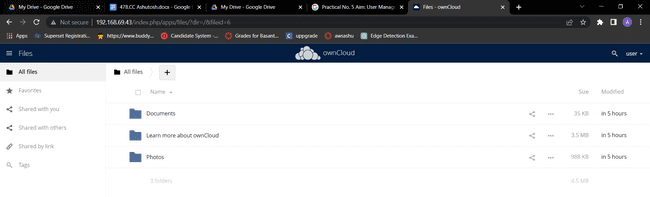


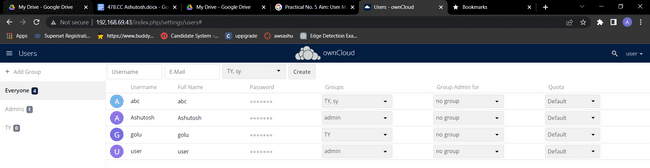


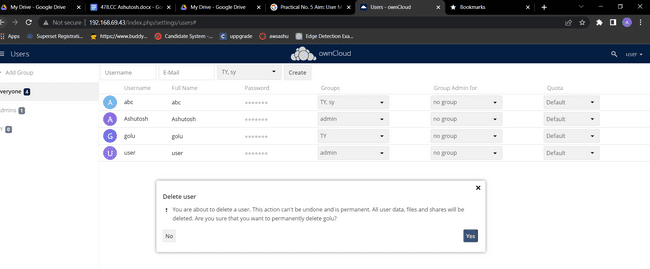




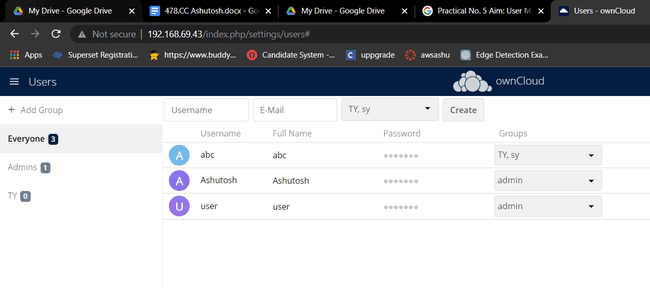




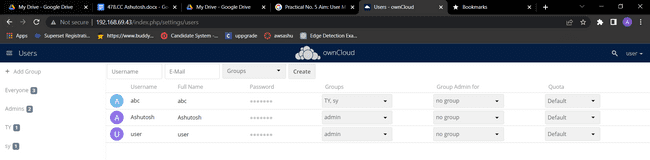


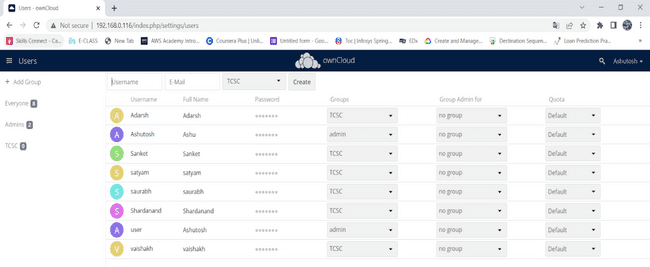
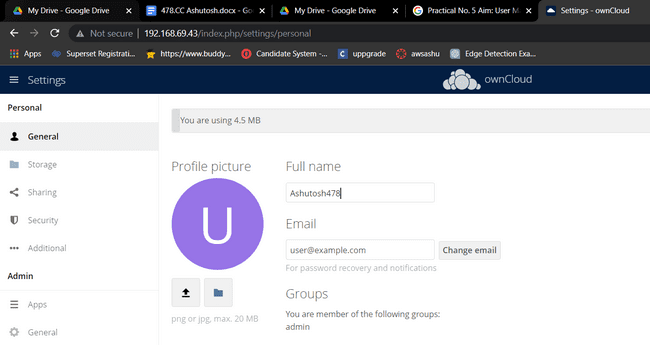


DELETE USER GOLU:



USERS :



**CONCLUSION :** Successfully Performed User Management in Cloud…..

**Practical No.6**

**Aim:** Study and implement Identity and Access Management (IAM) in AWS..

**Theory:**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

**IAM features**

IAM gives you the following features:

**1.Shared access to your AWS account**

You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

**2.Granular permissions**

You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift, and other AWS services. For other users, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but nothing else.

**3.Secure access to AWS resources for applications that run on Amazon EC2**

You can use IAM features to securely provide credentials for applications that run on EC2 instances. These credentials provide permissions for your application to access other AWS resources. Examples include S3 buckets and DynamoDB tables.

4. **Identity federation**

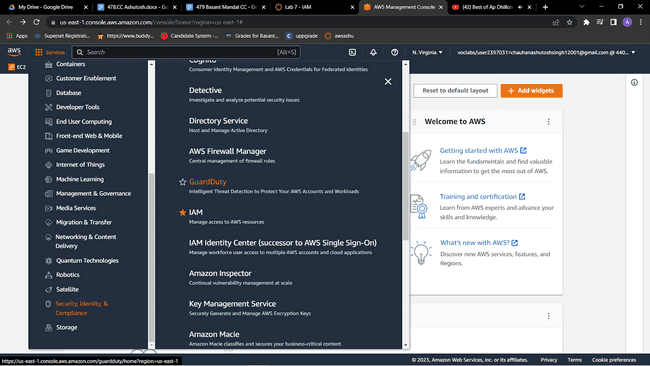
You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

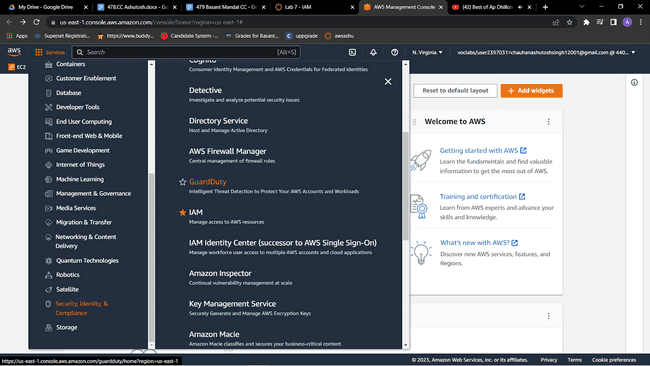
5. **Free to use**

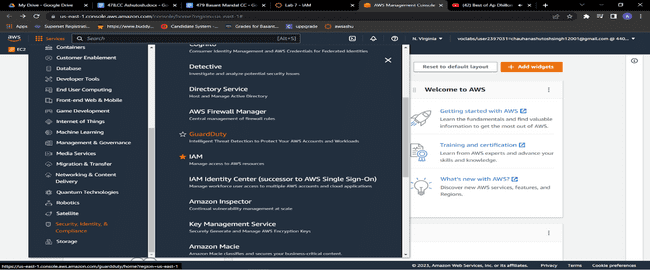
AWS Identity and Access Management (IAM) and AWS Security Token Service (AWS STS) are features of your AWS account offered at no additional charge. You are charged only when you access other AWS services using your IAM users or AWS STS temporary security credentials

Steps:

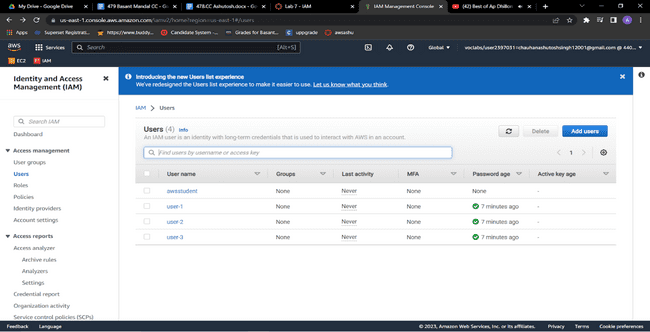
1. Choose the **Services** menu, locate the **Security, Identity, & Compliance** services, and choose **IAM**

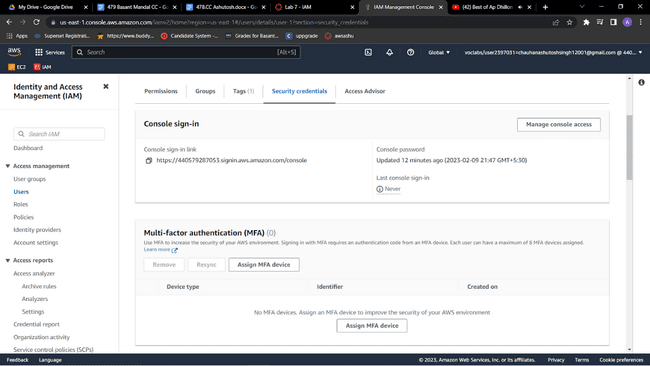




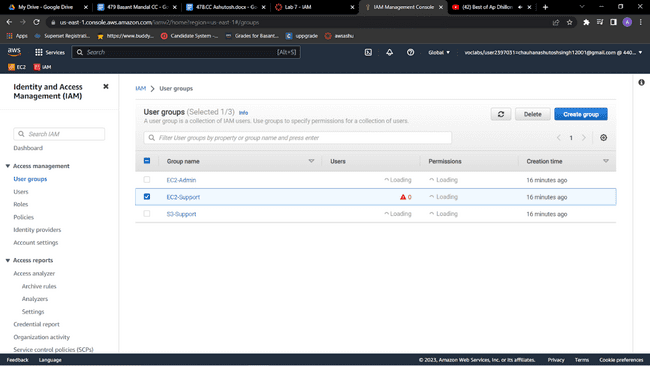


2.In the navigation pane on the left, choose **Users**.Create Users

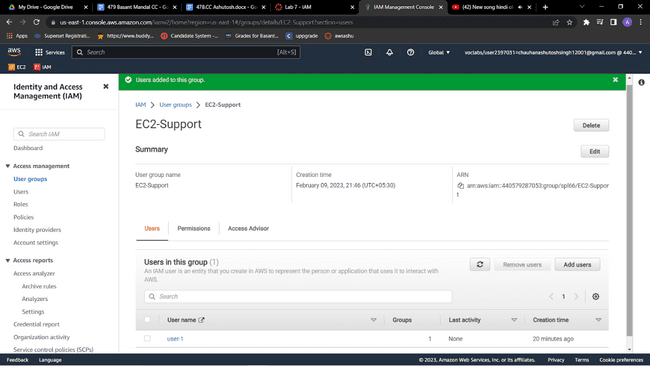
3.Choose the **Security credentials** tab.  
Notice that user-1 is assigned a **Console password**. This allows the user to access the AWS Management Console.

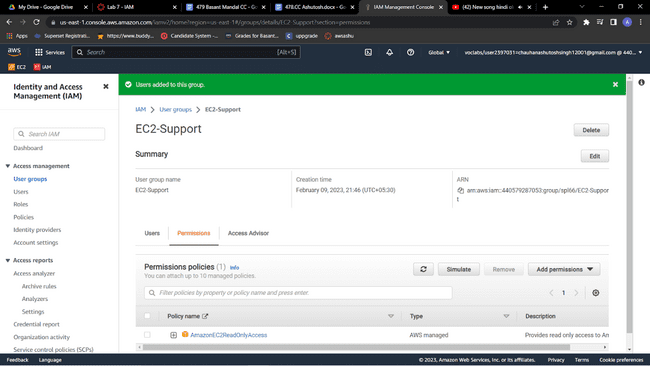


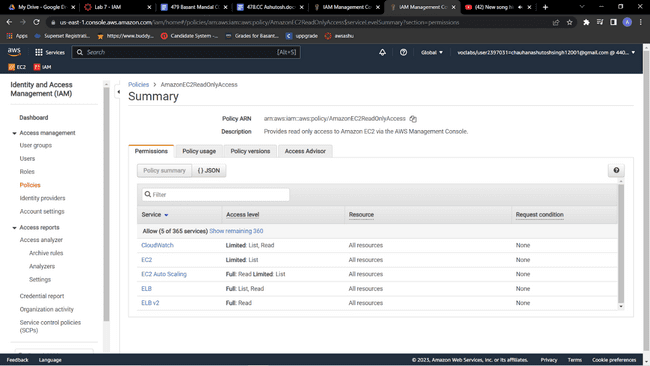
4.In the navigation pane on the left, choose **User groups**.The following groups have already been created for you:   EC2-Admin , EC2-Support , S3-Support



5.Choose the name of the **EC2-Support** group.  
This brings you to the summary page for the **EC2-Support** group.



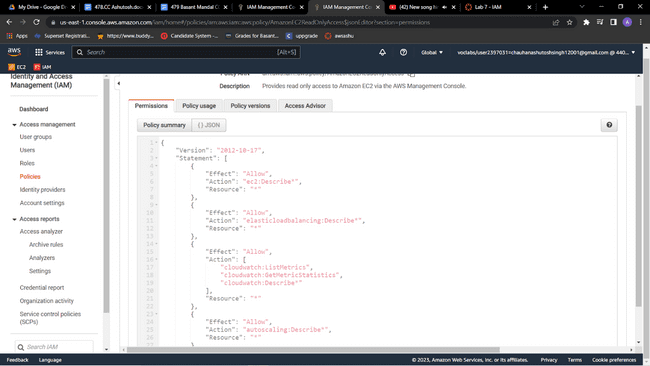
6.Choose the **Permissions** tab.  
This group has a managed policy called **AmazonEC2ReadOnlyAccess** associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the policy are immediately applied against all users and groups that are attached to the policy.

7.Under **Policy Name**, choose the link for the **AmazonEC2ReadOnlyAccess** policy.

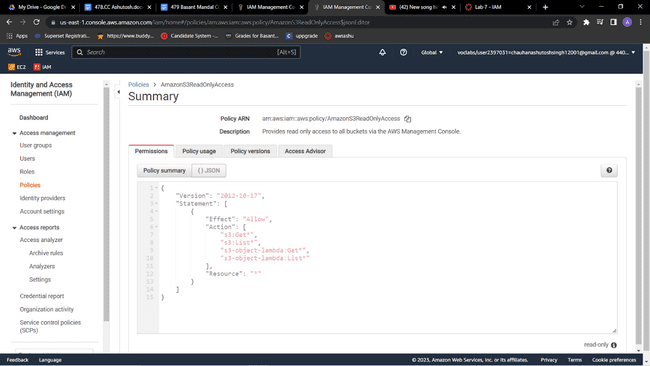
7.Choose the **{} JSON** tab.

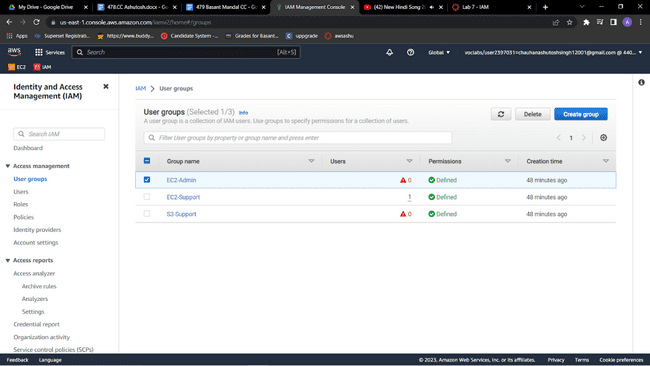
A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to *List* and *Describe* (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a support role.

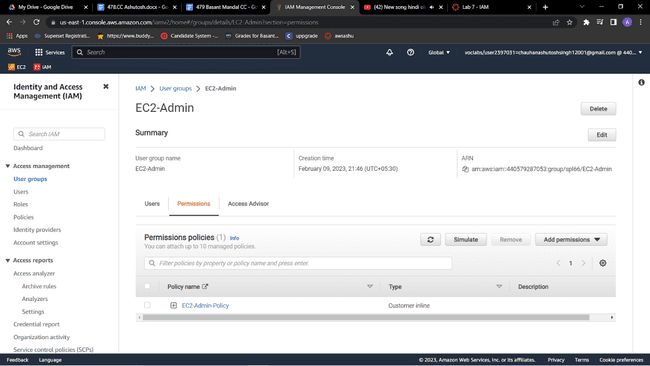
* Statements in an IAM policy have the following basic structure:
  + **Effect** says whether to *Allow* or *Deny* the permissions.
  + **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
  + **Resource** defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket or Amazon EC2 instance; an asterisk [ \* ] means *any resource*).

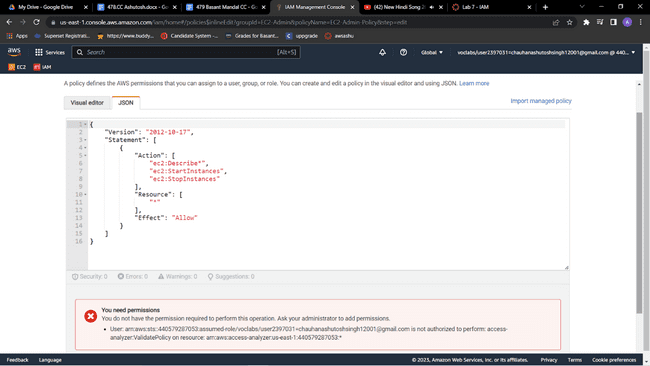


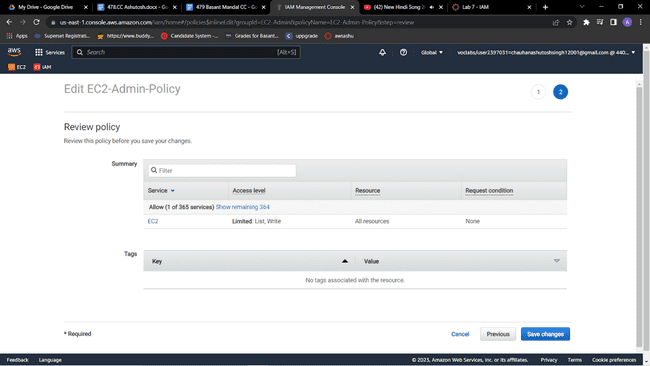
8.In the navigation pane on the left, choose **User groups**.Choose the name of the **S3-Support** group.Choose the **Permissions** tab.  
The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.    Under **Policy Name**, choose the link for the **AmazonS3ReadOnlyAccess** policy.Choose the **{} JSON** tab.  
This policy has permissions to *Get* and *List* for *all* resources in Amazon S3.



9.In the navigation pane on the left, choose **User groups**.Choose the name of the **EC2-Admin** group.

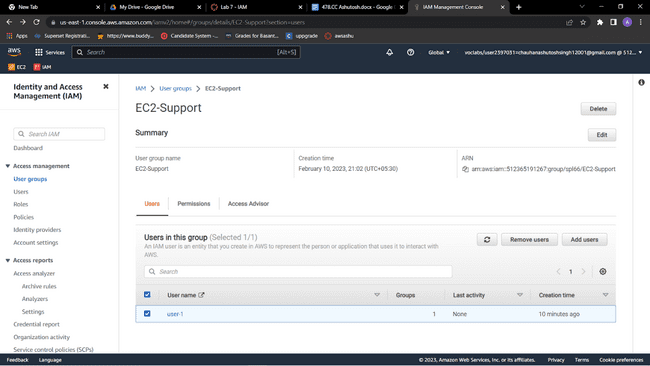
10.Choose the **Permissions** tab.  
This group is different from the other two. Instead of a managed policy, the group has an *inline policy*, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.

11.Under **Policy Name**, choose the name of the **EC2-Admin-Policy** policy.Choose the **JSON** tab.  
This policy grants permission to *Describe* information about Amazon EC2 instances, and also the ability to *Start* and *Stop* instances. 



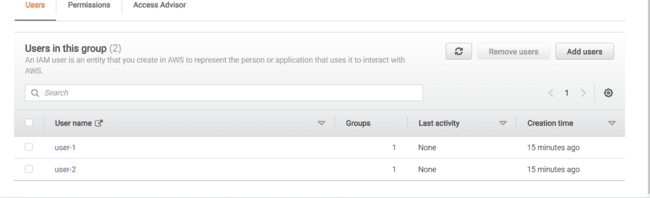
12.At the bottom of the screen, choose **Cancel** to close the policy.

**Add user-1 to the S3-Support group**

**13.**In the left navigation pane, choose User groups.Choose the name of the S3-Support group.On the Users tab, choose Add users.Select  user-1, and choose Add usersOn the Users tab, notice that *user-1* has been added to the group.****

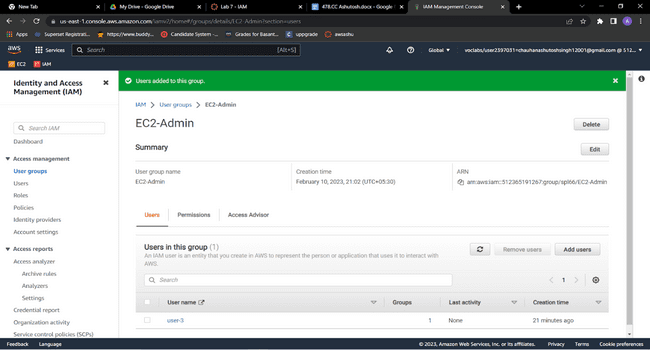
**Add user-2 to the EC2-Support group**

**You have hired *user-2* into a role where they will provide support for Amazon EC2. You will add them to the *EC2-Support* group so that they inherit the necessary permissions via the attached *AmazonEC2ReadOnlyAccess* policy.**

**14**.Use what you learned from the previous steps to add *user-2* to the *EC2-Support* group.*user-2* should now be part of the *EC2-Support* group.****

**Add user-3 to the EC2-Admin group**

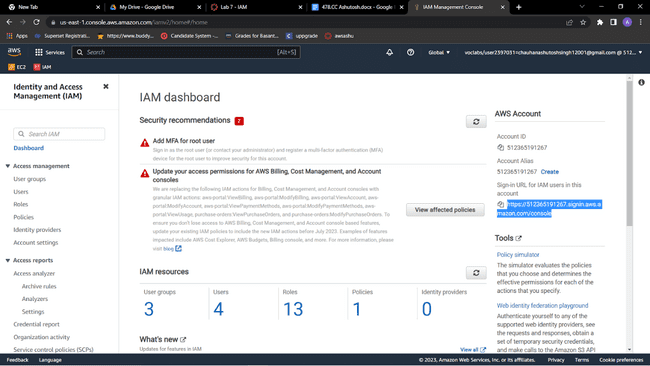
You have hired *user-3* as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the *EC2-Admin* group so that they inherit the necessary permissions via the attached *EC2-Admin-Policy*.

15.Use what you learned from the previous steps to add *user-3* to the *EC2-Admin* group.*user-3* should now be part of the *EC2-Admin* group.In the navigation pane on the left, choose **User groups**.Each group should have a **1** in the **Users** column. This indicates the number of users in each group.If you do not have a **1** for the **Users** column for a group, revisit the previous steps to ensure that each user is assigned to a group, as shown in the table in the **Business scenario** section.

**Sign in and test users**

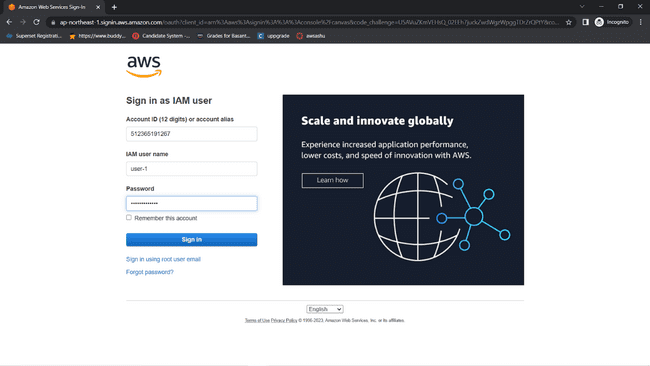
**Get the console sign-in URL**

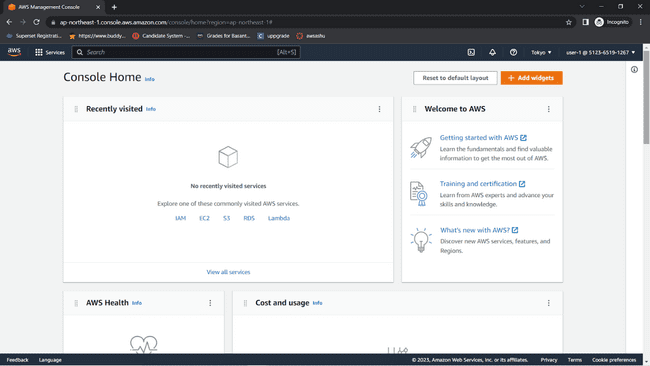
**16.**In the navigation pane on the left, choose Dashboard.Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: https://123456789012.signin.aws.amazon.com/console  
This link can be used to sign in to the AWS account that you are currently using.Copy the sign-in link to a text editor.

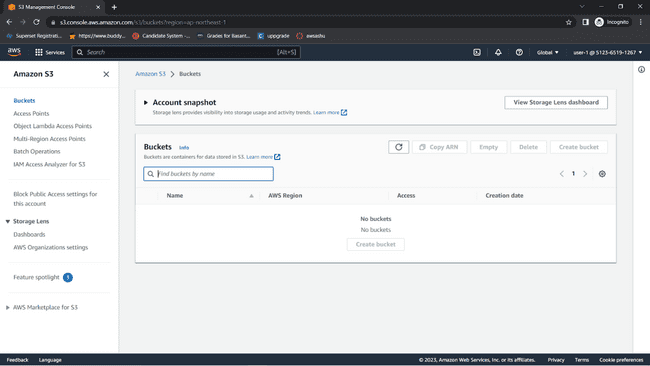


**Test user-1 permissions**

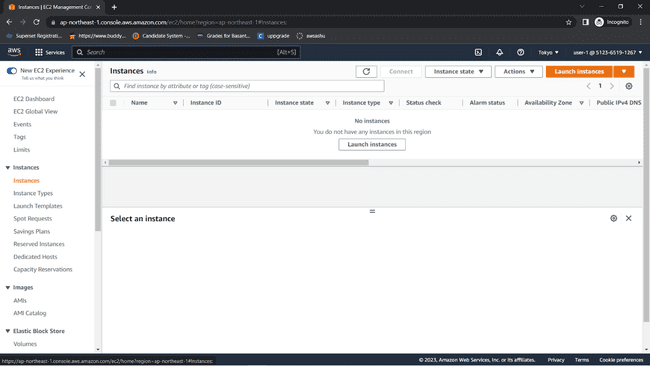
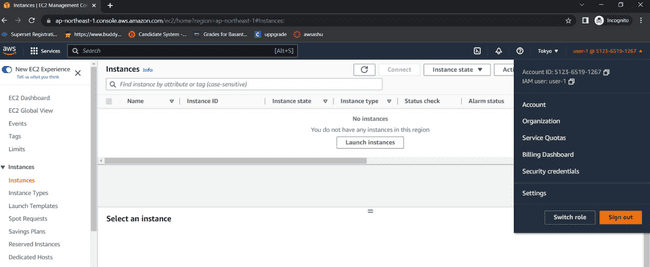
17.Open a private or incognito window in your browser.Paste the sign-in link into the private browser, and press ENTER.You will now sign-in as *user-1*, who has been hired as your Amazon S3 storage support staff.Sign in with the following credentials:**IAM user name:** user-1,**Password:** Lab-Password1

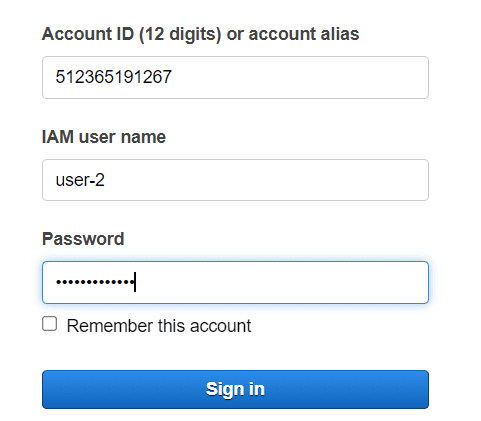




18.Choose the **Services** menu, and choose **S3**.Choose the name of one of your buckets, and browse the contents.Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.Now, test whether the user has access to Amazon EC2.

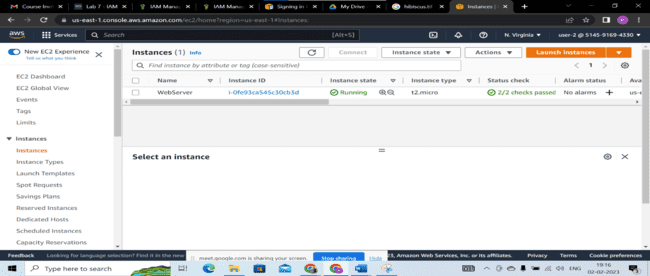
19.Choose the **Services** menu, and choose **EC2**.In the left navigation pane, choose **Instances**.You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2.You will now sign in as *user-2*, who has been hired as your Amazon EC2 support person.

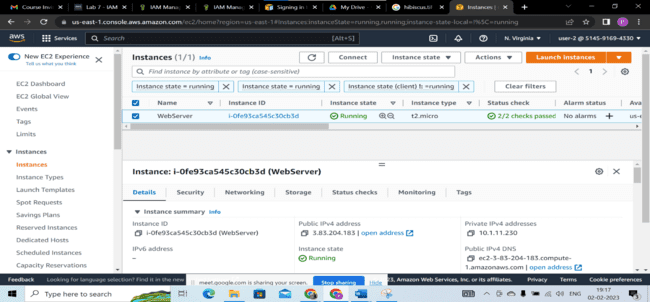
Sign Out

20.Paste the sign-in link into the private browser again, and press ENTER.Sign in with the following credentials:**IAM user name:** user-2  **Password:** Lab-Password2

21.Choose the **Services** menu, and choose **EC2**.In the navigation pane on the left, choose **Instances**.You are now able to see an EC2 instance. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions.If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, **N. Virginia**).

22.Select the EC2 instance.Choose the **Instance state** menu, and then choose **Stop instance**.To confirm that you want to stop the instance, choose **Stop**.  
An error message appears and says that *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information without making changes.Next, check if *user-2* can access Amazon S3.





**CONCLUSION :** Identity and access management (IAM) is one of the foundations of [**cloud security**](https://www.cassinfo.com/cloud-management/services/cloud-security). As more organizations turn to mobile-friendly and cloud-based platforms, the need to provide a safe and secure place to store identifiable information becomes more important.

**Practical No.7**

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

**THEORY :**

[AWS multi-factor authentication](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users) (MFA) is an [AWS Identity and Access Management (IAM)](https://aws.amazon.com/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](https://aws.amazon.com/security/amazon-security-initiatives/free-mfa-security-key/).

With MFA enabled, when a user signs in to the [AWS Management Console](https://console.aws.amazon.com/console/home), 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](https://aws.amazon.com/iam/identity-center/). For more information, see the [IAM Identity Center User Guide](https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html).

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.

Available MFA methods for IAM

You can manage your MFA devices in the [IAM console](https://console.aws.amazon.com/iam/). The following options are the MFA methods that IAM supports.

FIDO security keys

FIDO-certified hardware security keys are provided by third-party providers such as Yubico. The FIDO Alliance maintains a list of all [FIDO-certified products](https://fidoalliance.org/certification/fido-certified-products/)  that are compatible with FIDO specifications. FIDO authentication standards are based on public key cryptography, which enables strong, phishing-resistant authentication that is more secure than passwords. FIDO security keys support multiple root accounts and IAM users using a single security key. For more information about enabling FIDO security keys, see [Enabling a FIDO security key](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_fido.html).

AWS offers a [free MFA security key](https://aws.amazon.com/security/amazon-security-initiatives/free-mfa-security-key/) to eligible AWS account owners in the United States. To determine eligibility and order a key, see the [Security Hub console](https://console.aws.amazon.com/securityhub/home/#/free-mfa-security-key).

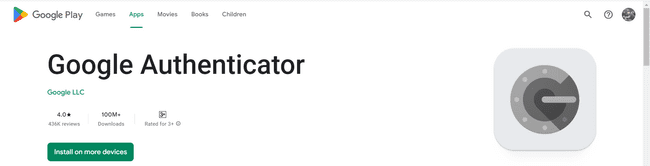
Virtual authenticator apps

Virtual authenticator apps implement the [time-based one-time password](https://datatracker.ietf.org/doc/html/rfc6238) (TOTP) algorithm and support multiple tokens on a single device. Virtual authenticators are supported for IAM users in the [AWS GovCloud (US) Regions](https://aws.amazon.com/govcloud-us/) and in other AWS Regions. For more information about enabling virtual authenticators, see [Enabling a virtual multi-factor authentication (MFA) device](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html).You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

|  |  |
| --- | --- |
| Android | [Twilio Authy Authenticator](https://play.google.com/store/apps/details?id=com.authy.authy), [Duo Mobile](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile), [LastPass Authenticator](https://play.google.com/store/apps/details?id=com.lastpass.authenticator), [Microsoft Authenticator](https://play.google.com/store/apps/details?id=com.azure.authenticator), [Google Authenticator](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2), [Symantec VIP](https://m.vip.symantec.com/home.v#searchwebsite) |
| iOS | [Twilio Authy Authenticator](https://apps.apple.com/us/app/authy/id494168017), [Duo Mobile](https://apps.apple.com/us/app/duo-mobile/id422663827), [LastPass Authenticator](https://apps.apple.com/us/app/lastpass-authenticator/id1079110004), [Microsoft Authenticator](https://apps.apple.com/us/app/microsoft-authenticator/id983156458), [Google Authenticator](https://apps.apple.com/us/app/google-authenticator/id388497605), [Symantec VIP](https://m.vip.symantec.com/home.v#searchwebsite) |

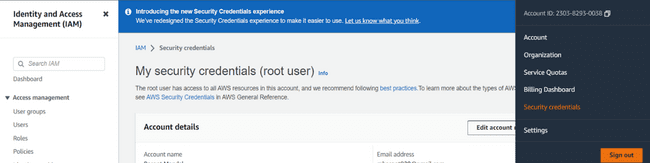
**GOOGLE APP FOR AUTHENTICATION :**

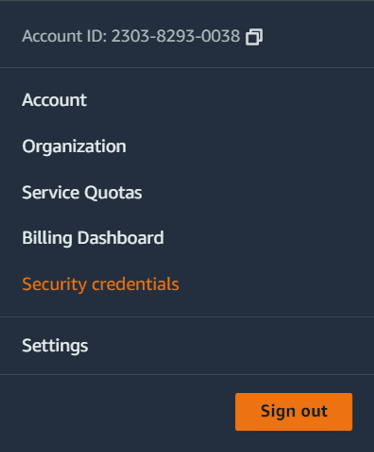
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>



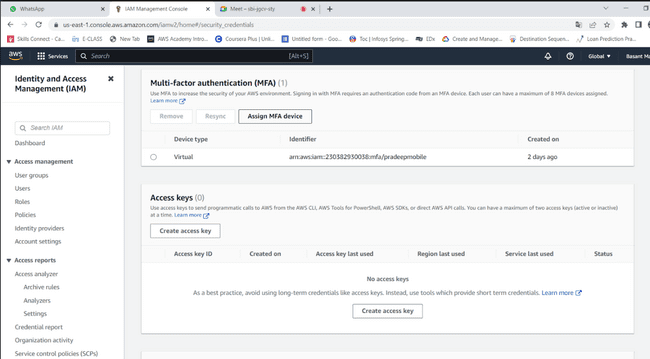
 **IMPLEMENTATION:**

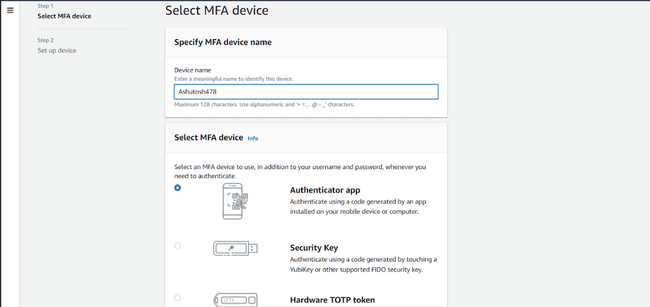


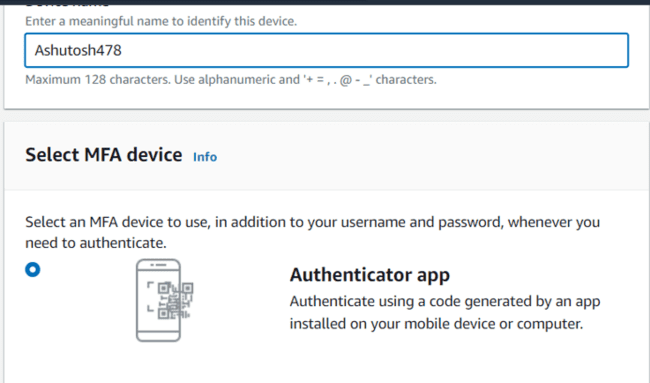




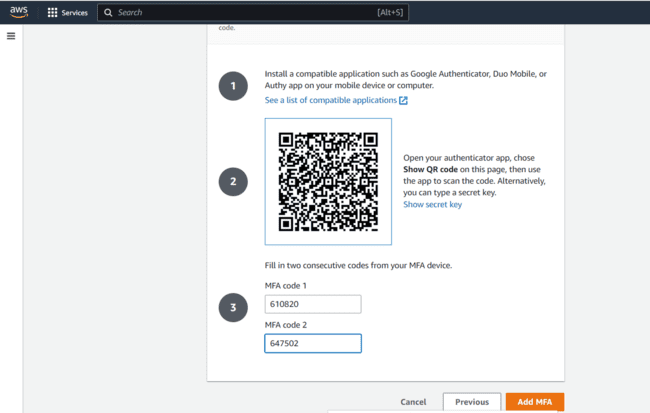


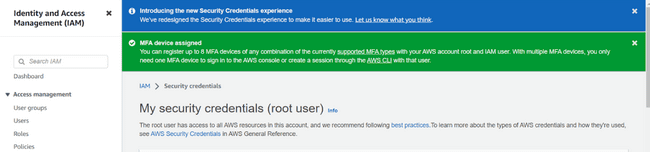






**USE GOOGLE AUTHENTICATOR APP FOR OTP:**





**CONCLUSION** : Successfully Implemented [AWS multi-factor authentication](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users) (MFA).

**Practical No.8**

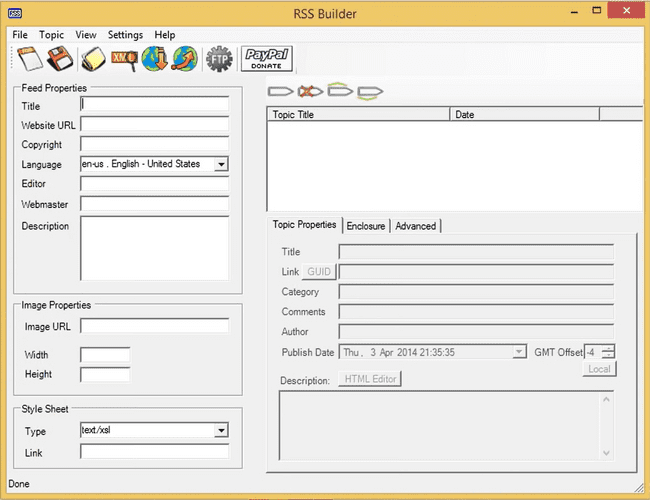
**AIM**: Write a program for web feed.

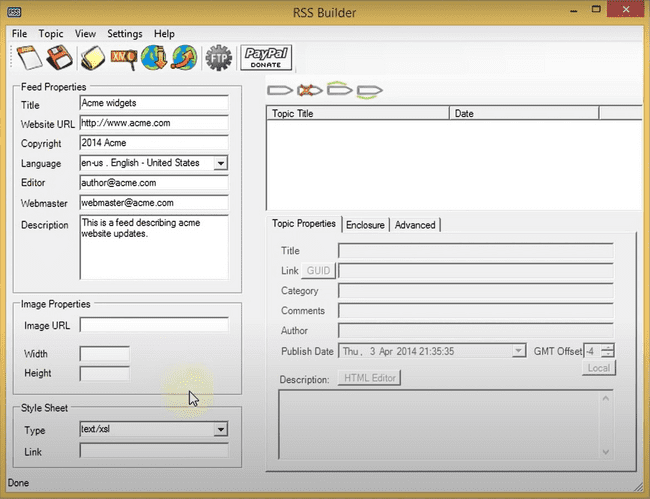
THEORY: RSS builder allows you to create a feed from specific sections of the webpage. You can generate a feed using RSS builder in two modes: **Quick mode**and**Advanced mode.**

An RSS feed is a feed that delivers **auto-updated** content to users without having to manually go to a specific website. It is formatted into an XML file that can be read in an RSS reader or embedded into your website.

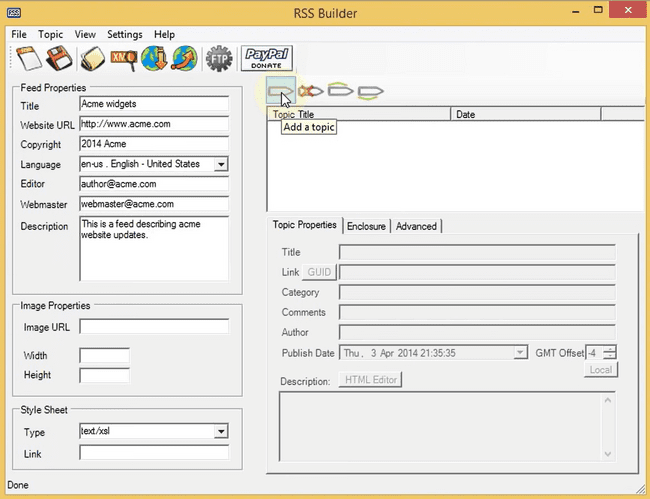
**IMPLEMENTATION:**

Step 01: Open RSS builder



Step 02: Fill the Feed properties 

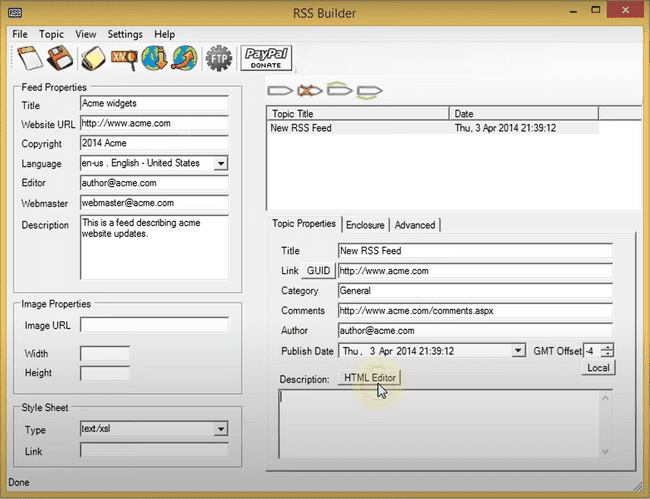
Step 03: Click on Add a Topic to add new topic to your feed



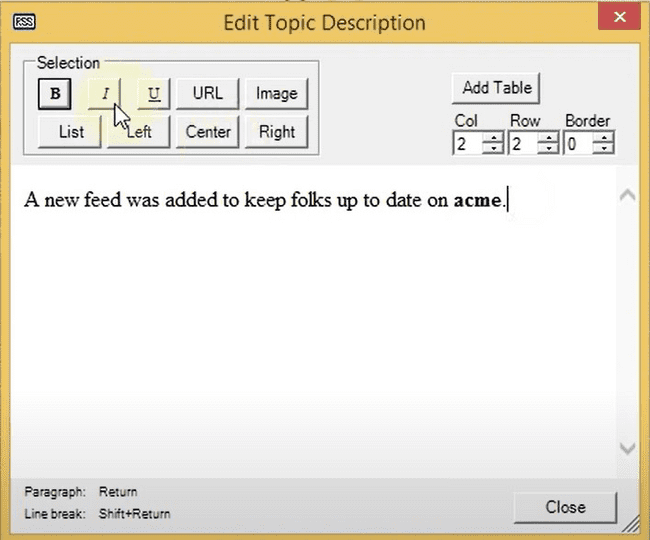
Step 04: Fill the topic properties



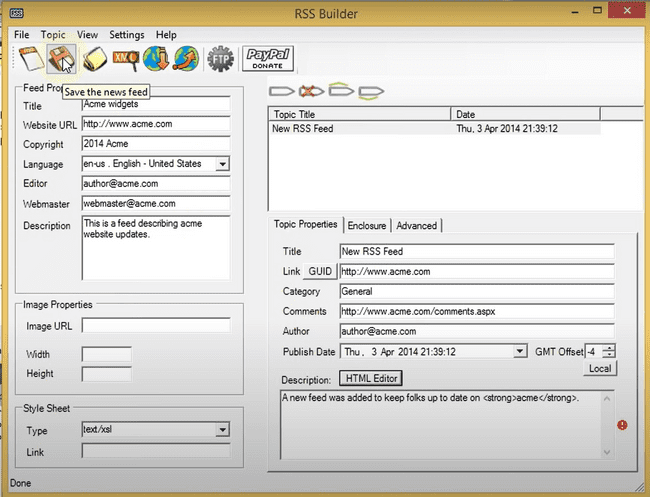
Step 05:To add description on web feed click on HTML editor



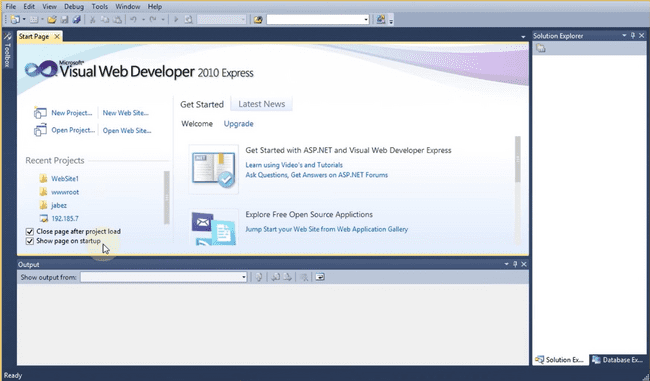
Step 06:Add topic description to show in feed



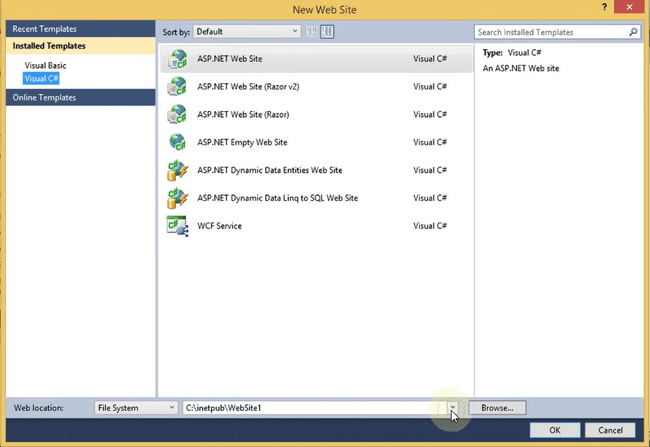
Step 07:Save the feed in xml format(defaultly saved in .xml)



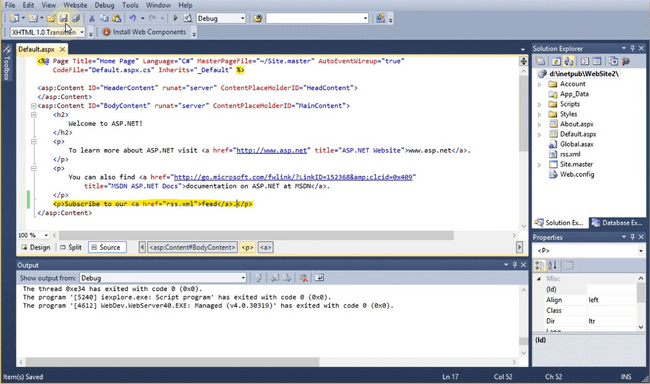
Step 08:launch Visual Studios 2010 to launch the sample website



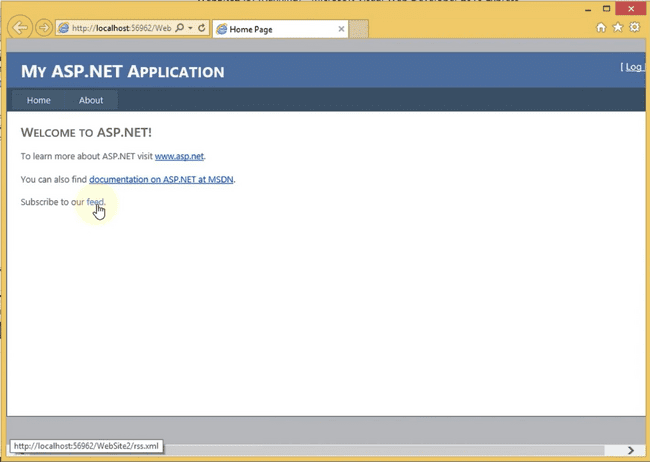
Step 09:Create new website on asp.net web site



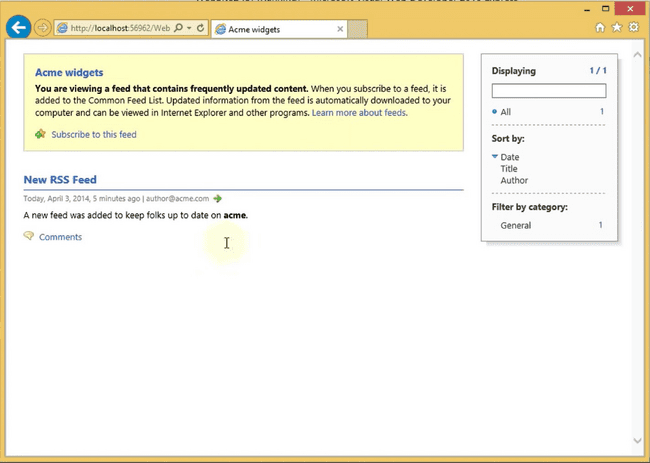
Step 10:Add new paragraph in default.aspx file and provide a link to server to access your website



Step 11:Run the program the page will appear as shown in the figure where the given link is provided click on it.



Step 12:New RSS feed will be created after clicking on the link to see the final output.



CONCLUSION :Successfully Performed, Your feed is now ready to be embedded and shared.

**PRACTICAL NO : 09**

**Aim:** Study and implementation of Single-Sign-On

(SSO).

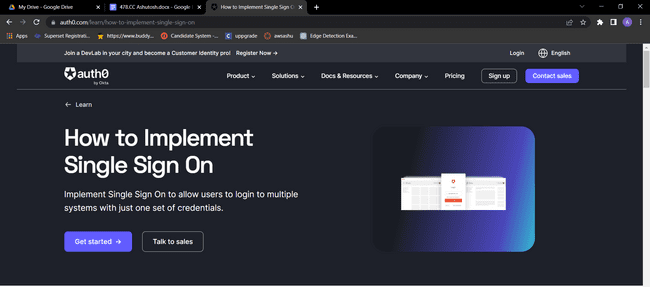
**THEORY :**

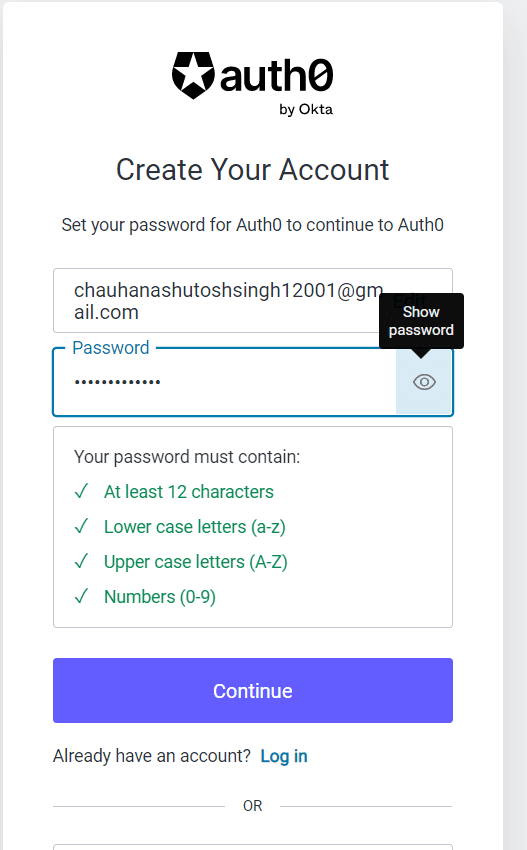
• Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications

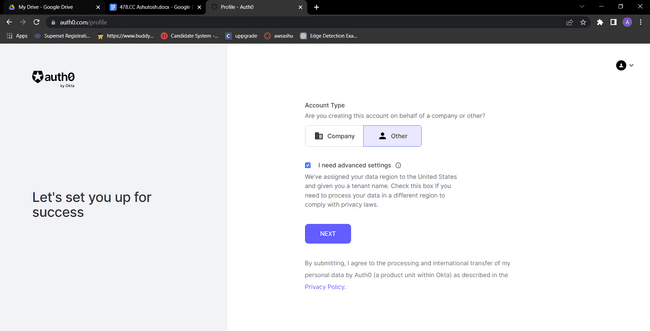
• The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.

• In a basic web SSO service, an agent module on the application server retrieves the specific authentication credentials for an individual user from a dedicated SSO policy server, while authenticating the user against a user repositorysuch as a lightweight directory access protocol (LDAP) directory.

Procedure:- Step1:got to the following link <https://auth0.com/learn/how-to-implement> single-sign-on/

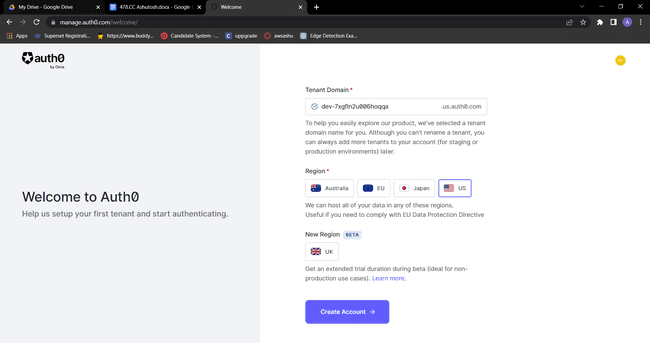
Step2:click on try autho for free → fill the details

Step3: Provide the username and Password and click on Signup

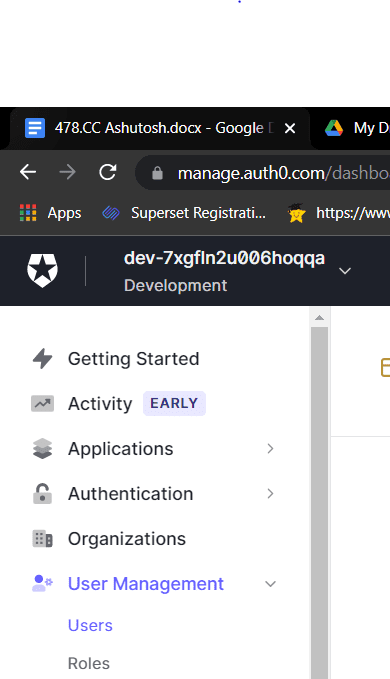


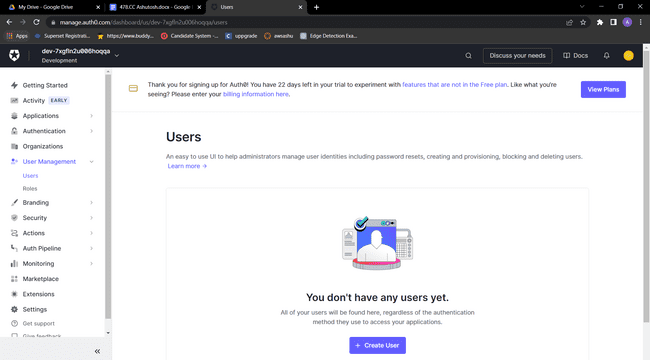
Step 4: Provide the tenant name and click on next

Step5: Fill all the Details and click on create account

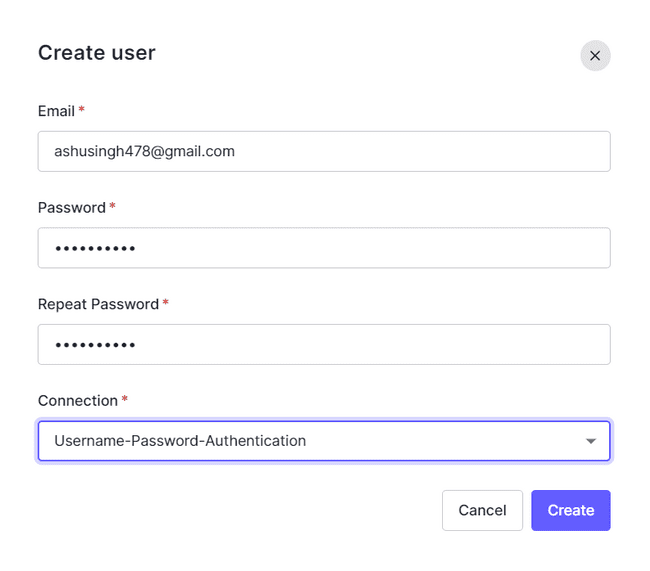


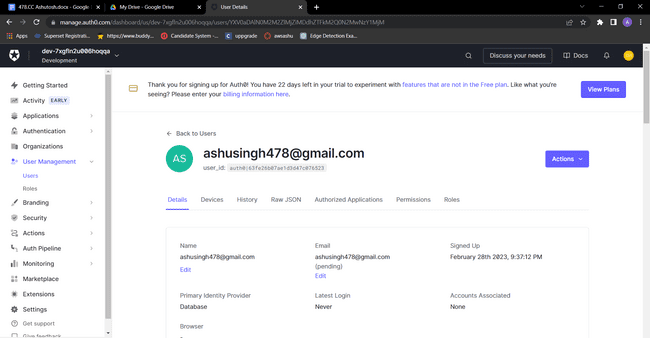
Step6: In this step you will get Dashbord . First create one user

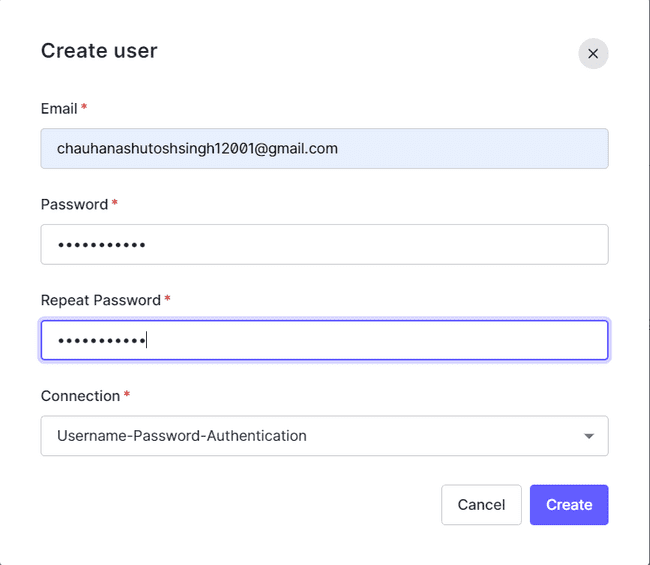




Step 7: click on create user

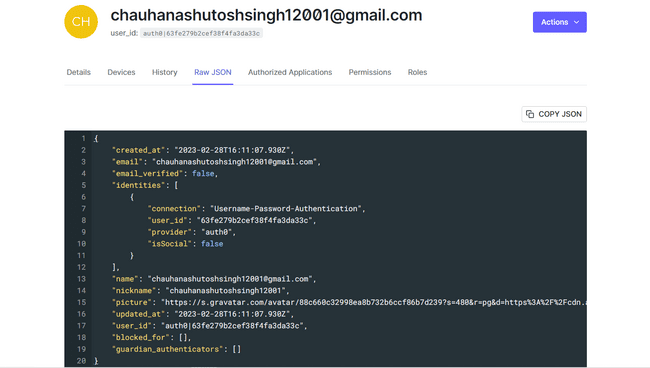
Step 8: fill all the details and click on save



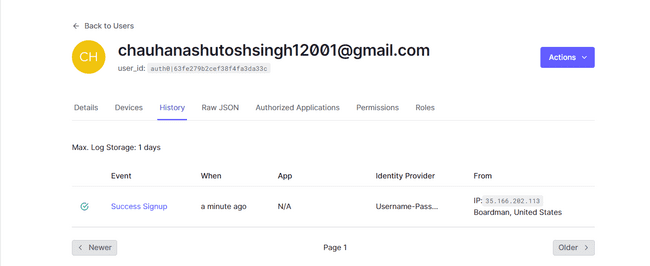




**RESULTS :**

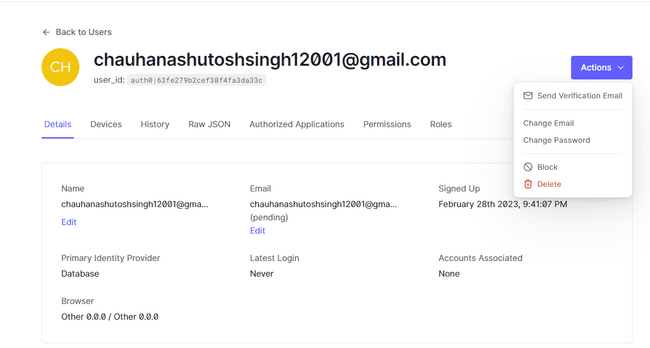




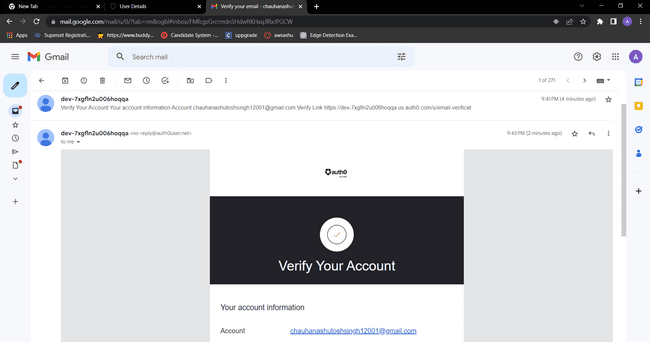




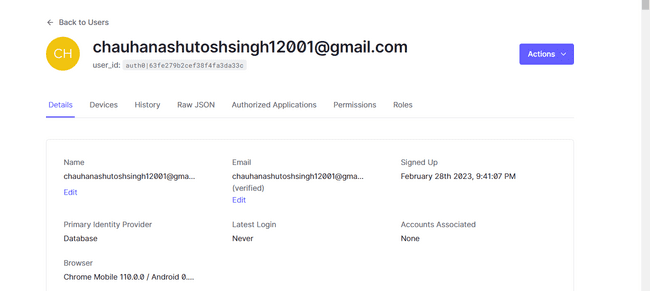
**Verification Mail :**



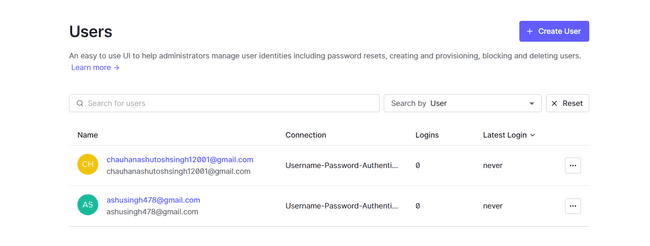




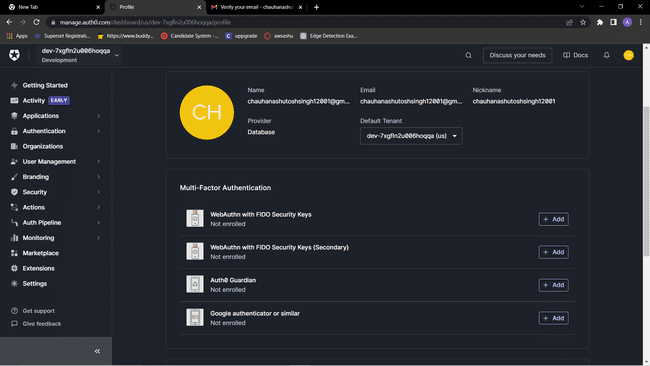
**MAIL VERIFIED:**







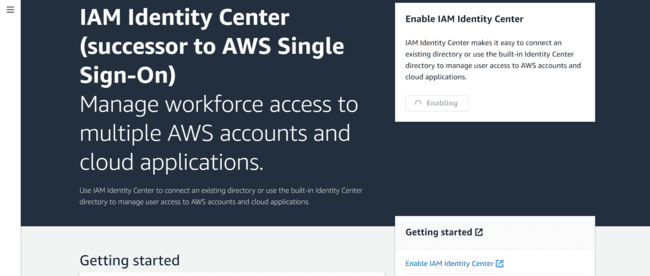


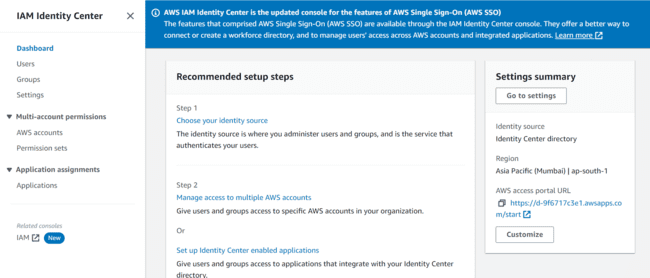


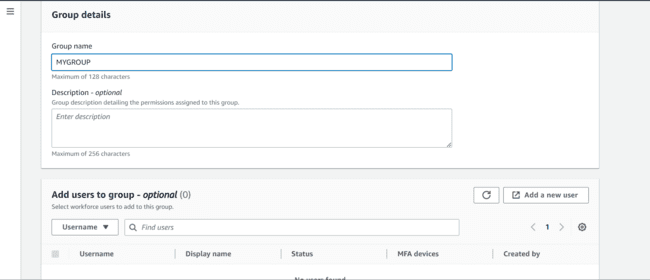


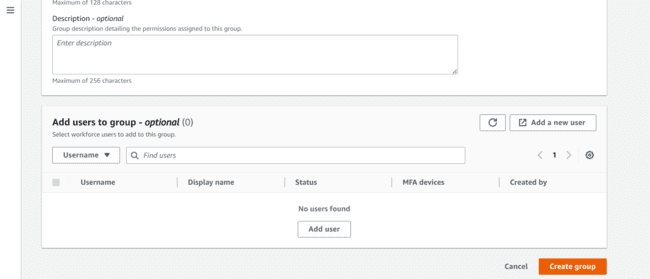
**BYAWS/.**

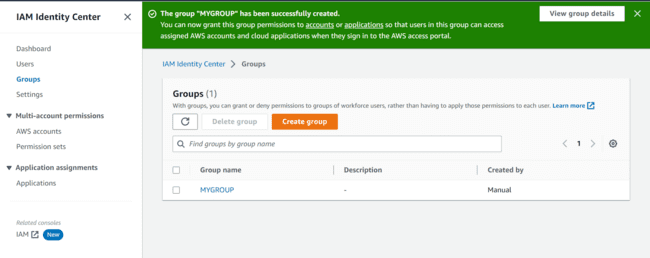




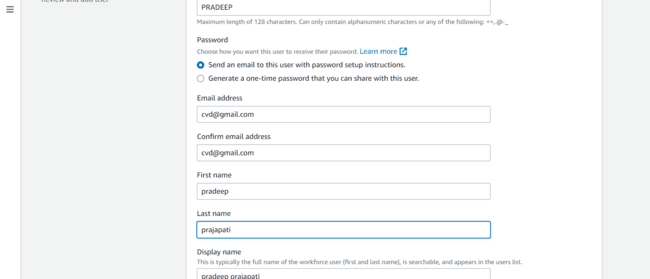


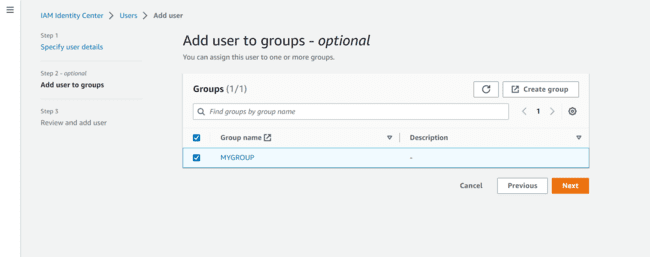


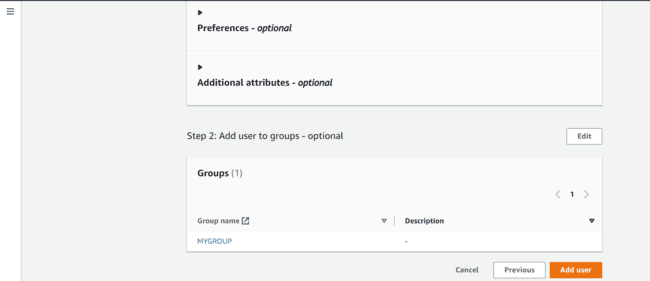


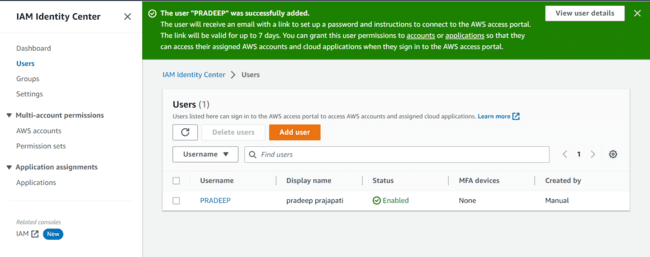


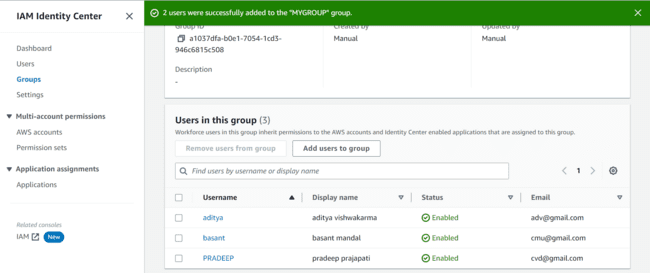
Create users











**CONCLUSION** : Succesfully implemented Single-Sign-On(SSO).