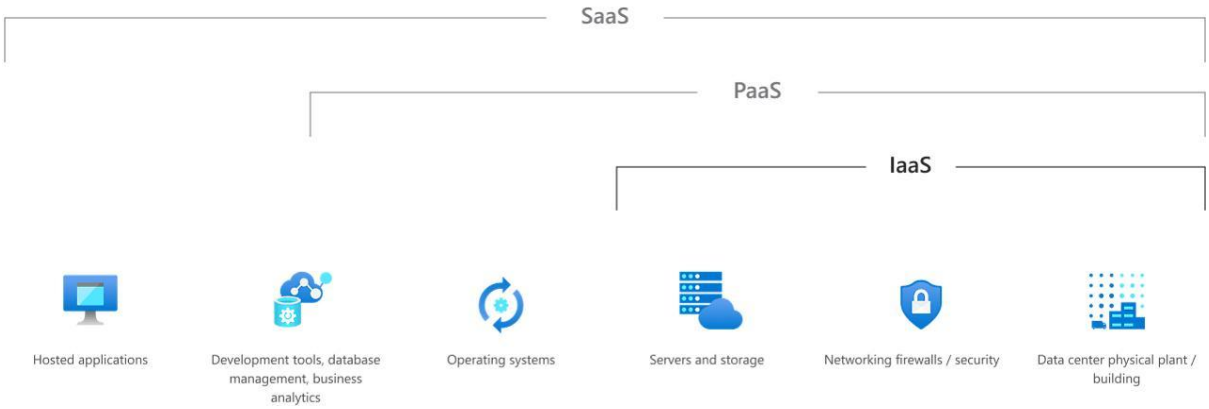
Experiment 4:

Aim: To study and implement Infrastructure as a Service using AWS/Microsoft Azure.

Theory:

Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualized computing resources over the internet. It offers fundamental infrastructure components such as virtual machines, storage, networking, and sometimes load balancers and firewalls. IaaS allows businesses to avoid the expense and complexity of buying and managing physical servers and data center infrastructure. Instead, users rent computing resources on a pay-as-you-go basis.

IaaS providers, such as **Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)**, manage the infrastructure, while users maintain control over their operating systems, applications, and middleware.



Advantages of IaaS

1. **Cost Savings** – No need for upfront capital investment in hardware; businesses only pay for what they use.
2. **Scalability** – Easily scale up or down based on demand without over-provisioning resources.
3. **Flexibility** – Users can deploy and configure infrastructure according to their needs.
4. **Reliability** – Cloud providers offer high availability, disaster recovery, and automatic backups.
5. **Security** – Leading providers offer advanced security features, including encryption and identity management.
6. **Focus on Core Business** – Companies can focus on developing applications instead of managing hardware.

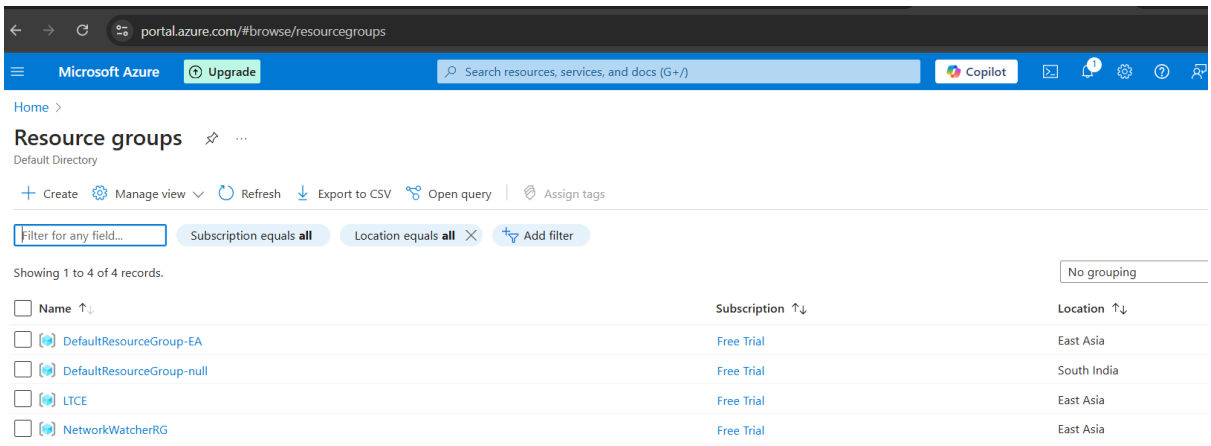
Disadvantages of IaaS

1. **Security Risks** – Since infrastructure is managed by a third party, there is a potential risk of data breaches.
2. **Downtime & Reliability Issues** – If the cloud provider experiences downtime, businesses may suffer disruptions.
3. **Hidden Costs** – While IaaS reduces capital expenses, improper resource management can lead to high operational costs.
4. **Complexity in Management** – Managing virtual infrastructure requires skilled IT professionals.
5. **Vendor Lock-in** – Migrating from one IaaS provider to another can be challenging due to compatibility issues.

Implementation:

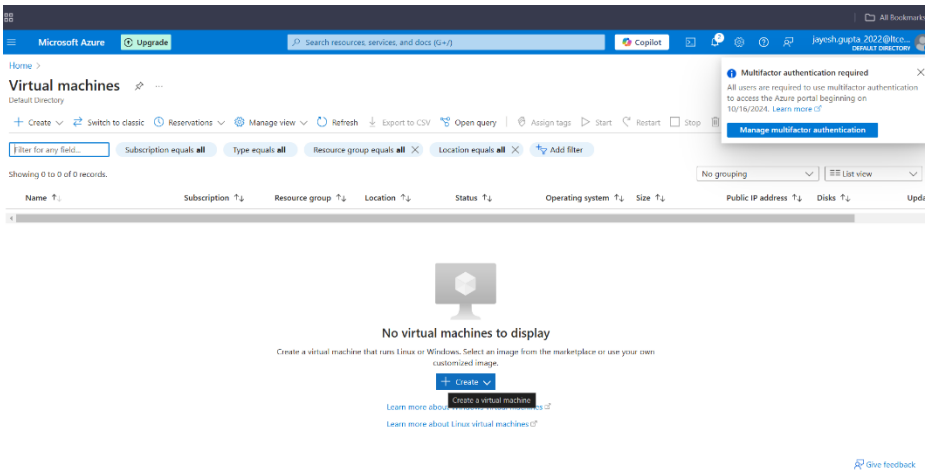
Step 1: **Create a Resource Group**

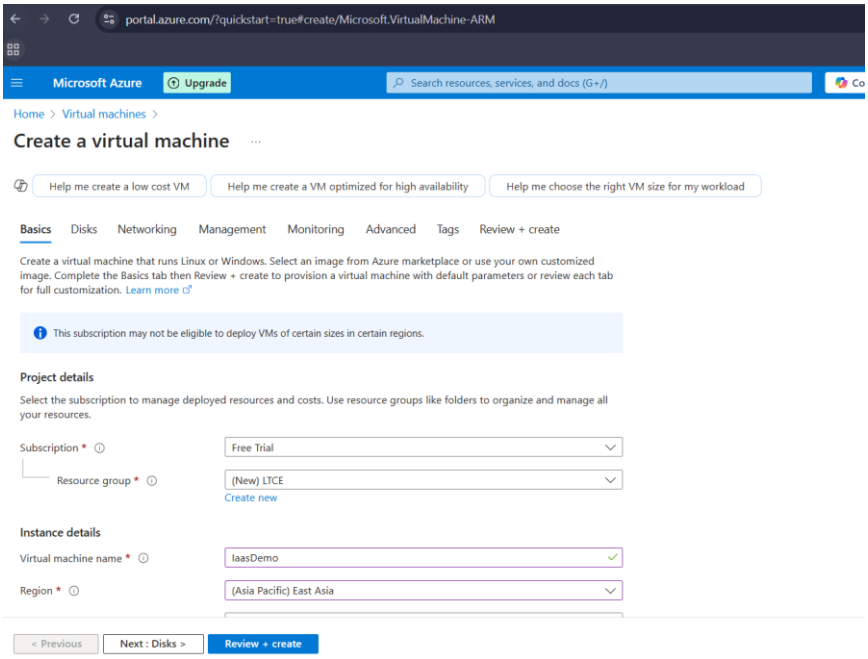
- **Navigate to:** *Home > Resource groups*
- Click **Create** and provide:
  - **Subscription**: Select your Azure subscription.
  - **Resource Group Name**: Enter a unique name.
  - **Region**: Choose a region closest to your users for better performance.
- Click **Review + Create → Create**.



Step 2: **Create a Virtual Machine (VM)**

- **Go to:** *Home > Virtual Machines > Create*
- Fill in the details:
  - **Subscription & Resource Group**: Choose the ones created earlier.
  - **Name**: Enter a name for your VM.
  - **Region**: Keep it consistent with the previous resources.
  - **Image**: Select the OS (e.g. Ubuntu).
  - **Size**: Choose the VM size based on your workload (e.g., B2s for small workloads).
  - **Authentication**: Select **Password** or **SSH Key**.
- Click **Review + Create → Create**.





Microsoft Azure | Upgrade | Search resources, services, and docs (G+/)

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Region * (Asia Pacific) East Asia

Availability options Availability zone

Zone options
- Self-selected zone
  Choose up to 3 availability zones, one VM per zone
- Azure-selected zone (Preview)
  Let Azure assign the best zone for your needs

Availability zone * Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type Trusted launch virtual machines

Configure security features

Image * Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)

See all images | Configure VM generation

VM architecture
- Arm64
- x64

Run with Azure Spot discount

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot

Home > Virtual machines >

Create a virtual machine

Validation passed

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Price

1 X Standard B1s
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
1.2146 INR/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name: Jayesh Gupta

Preferred e-mail address: jayesh.gupta_2022@ltce.in

< Previous | Next > | Create

Download a ter

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot

Home >

CreateVm-canonical.ubuntu-24_04-lts-server-20250207221123 | Overview

Deployment

Search

- Overview
- Inputs
- Outputs
- Template

Delete | Cancel | Redeploy | Download | Refresh

Your deployment is complete

Deployment name: CreateVm-canonical.ubuntu-24_04-lts-server-2...
Subscription: Free Trial
Resource group: LTCE

Start time: 2/7/2025, 10:19:12 PM
Correlation ID: 154ee92b-2954-440a-af48-bb08330c64c1

Deployment details

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

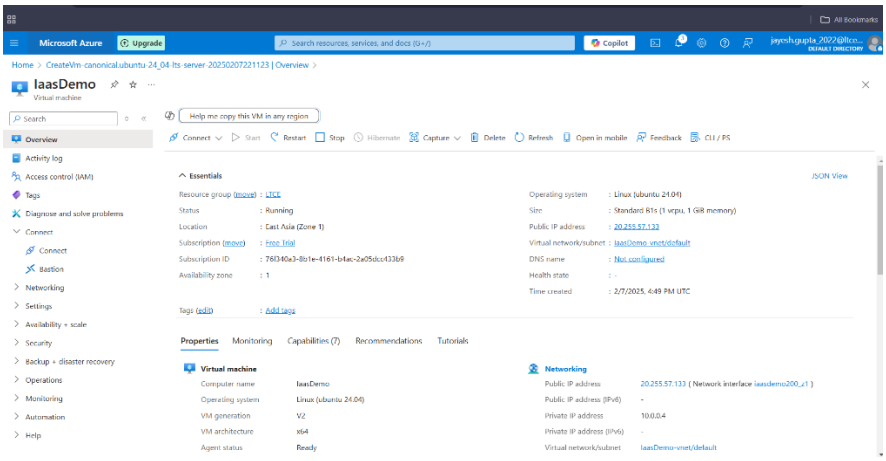
Run a script inside the virtual machine Recommended

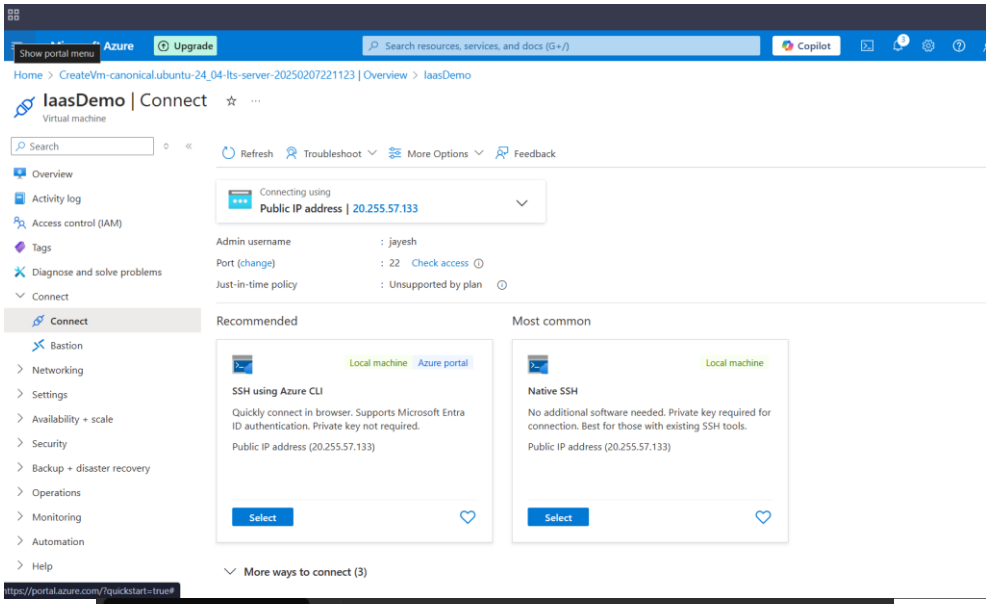
Go to resource | Create another VM

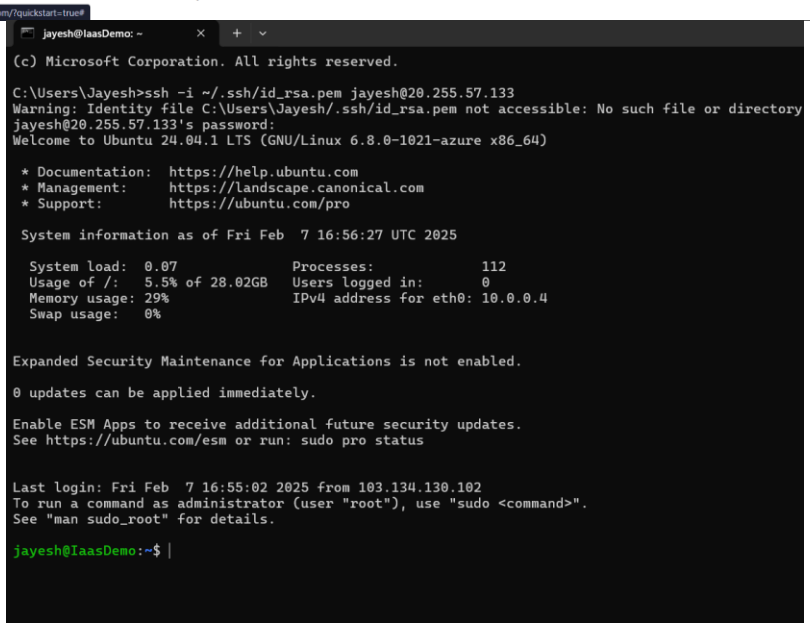
Give feedback

Tell us about your experience with deployment

Step 3: Check Whether it is working, by connecting it through the public IP.







Connected Successfully through the terminal to the deployed Service.

Experiment 5:

Aim: To study and implement Platform as a Service using AWS Elastic Beanstalk/ Microsoft Azure App Service.

Theory:

Platform as a Service (PaaS) is a cloud computing model that provides a **managed platform** for developing, running, and managing applications. Unlike **Infrastructure as a Service (IaaS),** where users control the infrastructure, **PaaS abstracts infrastructure complexities** by providing a **fully managed environment** for application deployment.

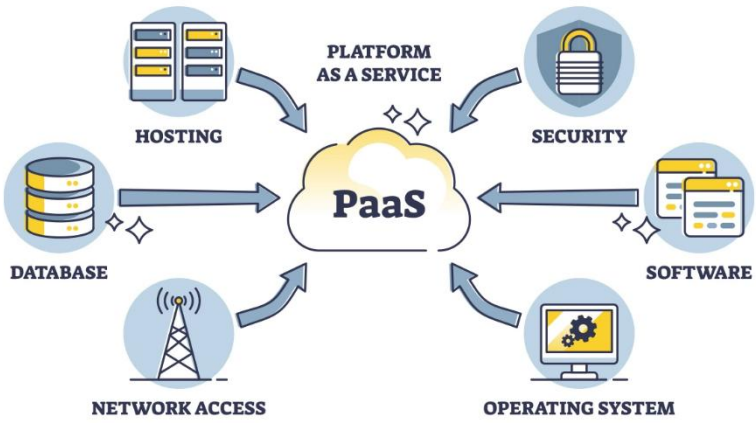
With PaaS, developers can focus on writing code while the cloud provider manages the underlying infrastructure, OS, runtime, middleware, and security updates.

Advantages of PaaS

- **Faster Development** – Developers focus on coding instead of managing infrastructure.
- **Automatic Scaling** – Resources are adjusted based on demand.
- **Cost-Efficient** – No need to manage hardware or infrastructure, reducing operational costs.
- **Managed Security** – Cloud providers handle security updates and patches.
- **Built-in DevOps Tools** – Supports continuous integration & deployment (CI/CD).
- **Supports Multiple Languages** – Deploy applications in various programming languages.

Disadvantages of PaaS

- **Limited Control** – Users cannot configure underlying infrastructure.
- **Vendor Lock-in** – Migrating applications between providers can be challenging.
- **Security Risks** – Sensitive data is stored on third-party servers.
- **Performance Variability** – Performance depends on the provider's shared resources.
- **Compatibility Issues** – Not all legacy applications work smoothly on PaaS platforms.



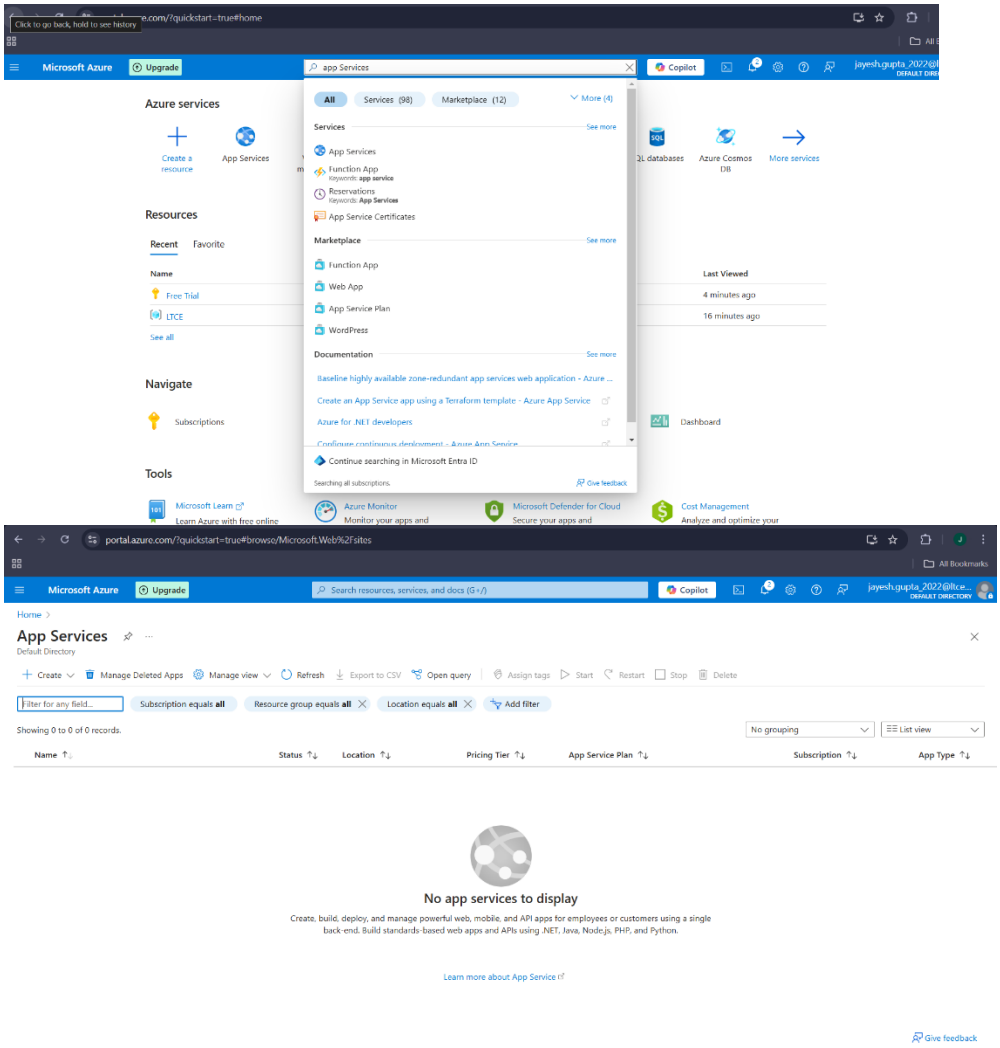
Implementation:

Step 1: **Create an Azure App Service**

- **Go to**: *Home > App Services > Create*
- Select **Web App** (for deploying a website or API).

Fill in the Details:

- **Subscription** – Choose your Azure subscription.
- **Resource Group** – Create a new one or use an existing one.
- **Name** – Enter a unique name for your web app.
- **Publish Type** – Select **Code** (for deploying your own code) or **Docker** (for container-based apps).
- **Runtime Stack** – Choose the programming language (e.g., .NET, Node.js, Python, PHP).
- **Region** – Pick the closest data center for better performance.
- **Pricing Plan** – Choose **Free (F1)** or a **Basic/Premium plan** for production use.
- Click **Review + Create → Create**.



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/)

Home > App Services >

Create Web App

Basics | Database | Deployment | Networking | Monitor + secure | Tags | Review + create

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. Learn more

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Free Trial

Resource Group * : LTCE

Create new

Instance Details

Name : jayesh445 .azurewebsites.net

Try a secure unique default hostname. More about this update

Publish * : Code / Container

Runtime stack * : Java 21

Java web server stack * : Java SE (Embedded Web Server)

Review + create | < Previous | Next : Database >

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/)

Home > App Services >

Create Web App

Publish * : Code / Container

Runtime stack * : Java 21

Java web server stack * : Java SE (Embedded Web Server)

Operating System * : Linux / Windows

Region * : West India

Not finding your App Service Plan? Try a different region or select your App Service Environment.

Pricing plans

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app.
Learn more

Linux Plan (West India) * : (New) ASP-LTCE-9c45

Create new

Pricing plan : Basic B1 (100 total ACU, 1.75 GB memory, 1 vCPU)

Explore pricing plans

Zone redundancy

Review + create | < Previous | Next : Database >

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/)

Home > App Services >

Create Web App

Basics | Database | Deployment | Networking | Monitor + secure | Tags | Review + create

Summary

Web App
by Microsoft

Basic (B1) sku
Estimated price - 1153.91 INR/Month

Basic authentication for this app is currently disabled and may impact deployments. Click to learn more.

Details

Subscription	76f340a3-8b1e-4161-b4ac-2a05dcc433b9
Resource Group	LTCE
Name	jayesh445
Publish	Code
Runtime stack	Java 21
Java web server stack	Java SE (Embedded Web Server)

App Service Plan (New)

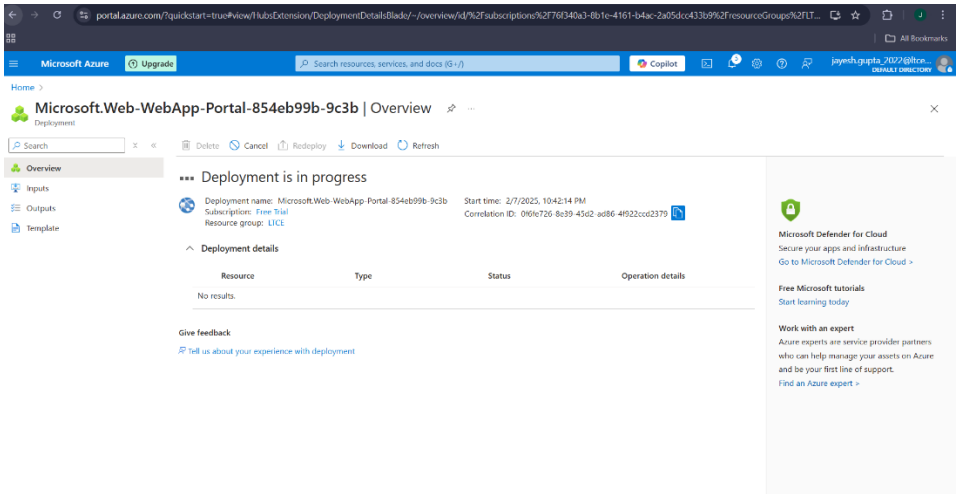
Name	ASP-LTCE-9c45

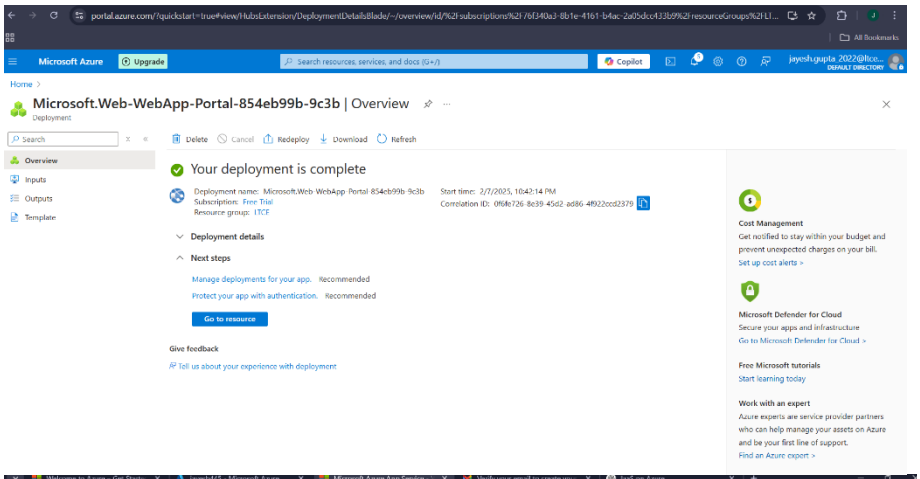
Create | < Previous | Next > | Download a template for automation

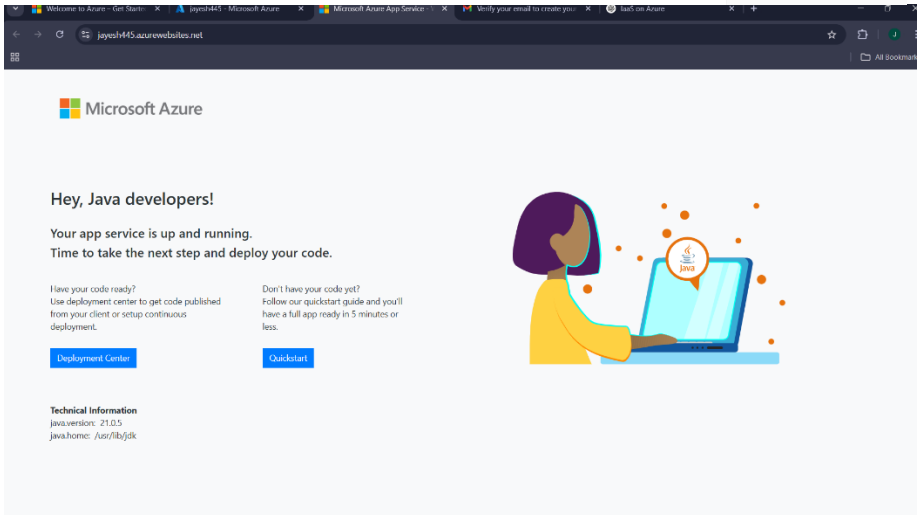
Step 3: **Deploy the Application**

You can deploy your application in several ways:

- Using Azure Portal
- Using GitHub Actions
- Using Visual Studio Code
- Using Azure C







Experiment 6:

Aim: To study and implement Software as a Service using Own Cloud/ AWS S3, Glaciers/ Azure Storage.

Theory:

Software as a Service (SaaS) is a cloud computing model where software applications are hosted and managed by a service provider and accessed over the internet. Unlike **Infrastructure as a Service (IaaS)** and **Platform as a Service (PaaS),** SaaS eliminates the need for users to install, maintain, or manage software on their local devices.

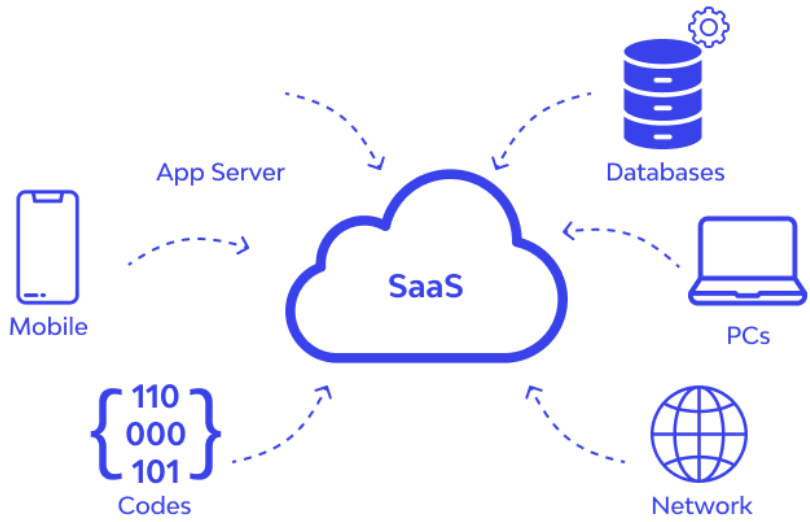
SaaS applications are typically **subscription-based** and can be accessed from anywhere using a web browser. Examples include **Google Drive, Microsoft Office 365, Dropbox, and Salesforce.**

Advantages of SaaS

- Cost-Effective – No upfront cost for hardware or software; users pay only for the subscription.
- Easy Accessibility – Access applications from anywhere with an internet connection.
- Automatic Updates – Providers handle maintenance, security patches, and updates.
- Scalability – Users can scale up or down based on their needs.
- Multi-Device Support – Works on desktops, tablets, and mobile devices.
- Security & Backup – Cloud providers manage security and data recovery.

Disadvantages of SaaS

- Limited Control – Users have minimal control over software updates and configurations.
- Internet Dependency – Requires a stable internet connection for access.
- Security & Privacy Concerns – Data is stored on third-party servers, posing potential risks.
- Vendor Lock-in – Switching from one provider to another can be difficult.
- Performance Issues – High latency may occur depending on internet speed and provider load.

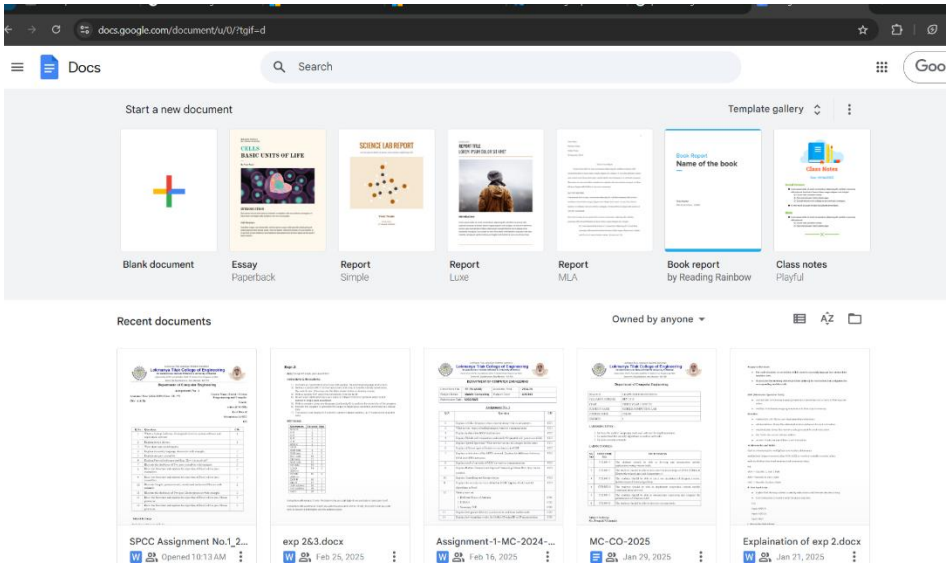


Implementation:

Google Docs: Google Docs is a perfect example of **Software as a Service (SaaS)** because it is cloud-based, requires no installation, and allows real-time collaboration.

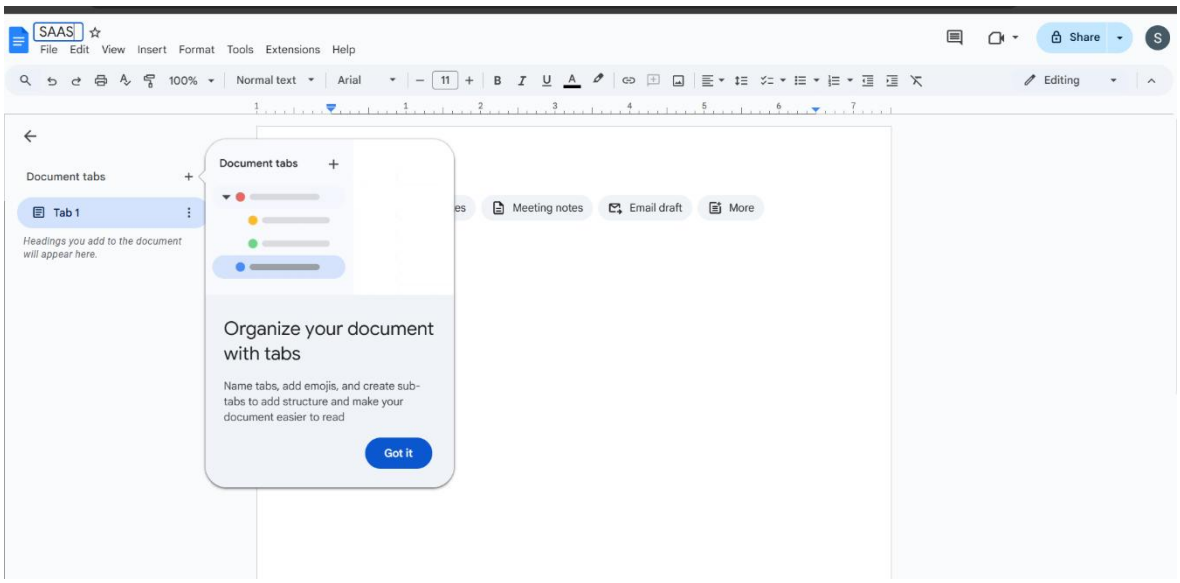
Step 1: **Sign in to Google Docs**

- Open a web browser and go to docs.google.com.
- Sign in with your **Google account**.



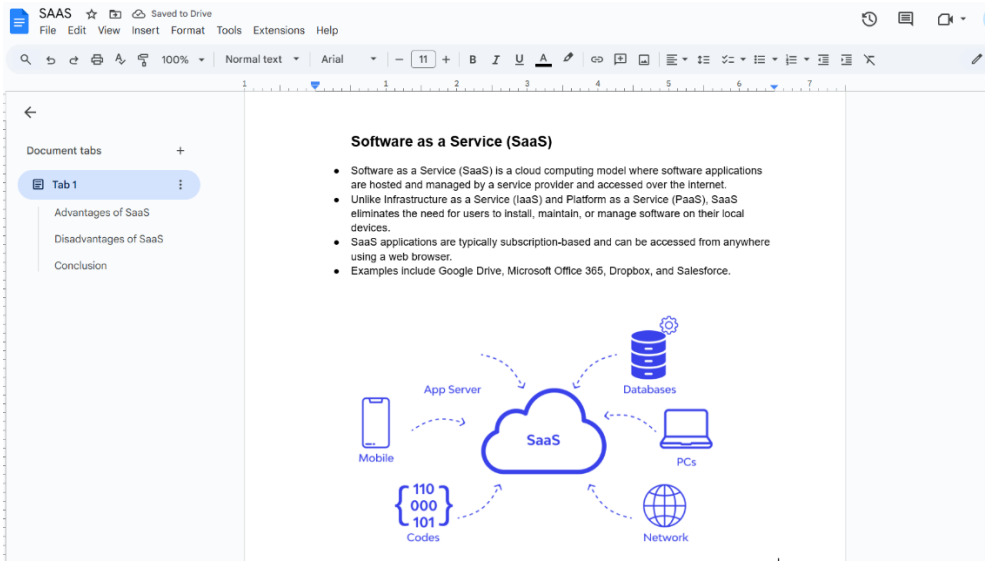
Step 2: **Create a New Document**

- Click on **Blank Document** or choose a **template** from the options.
- A new document will open, similar to Microsoft Word but in a browser.



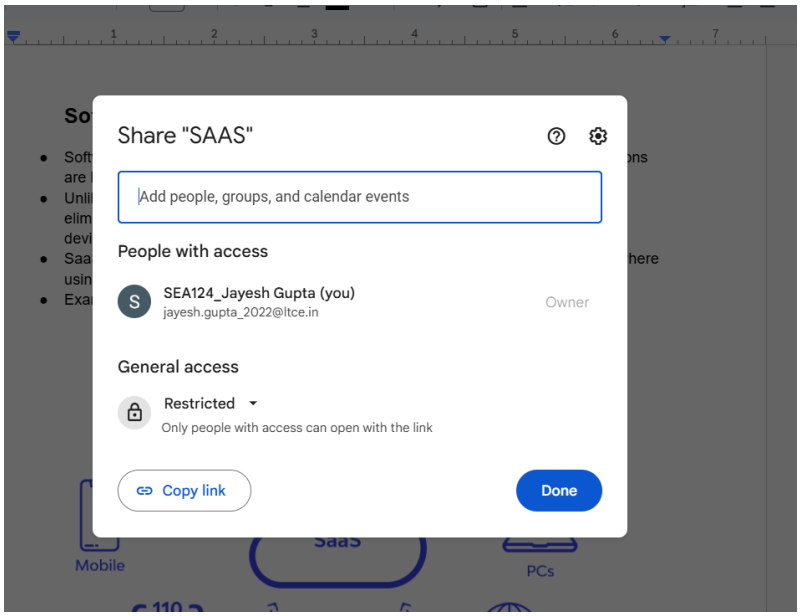
Step 3: **Edit the Document Online**

- Type text, insert images, and format the content.
- No need to save manually – all changes are **automatically saved** in Google Drive.



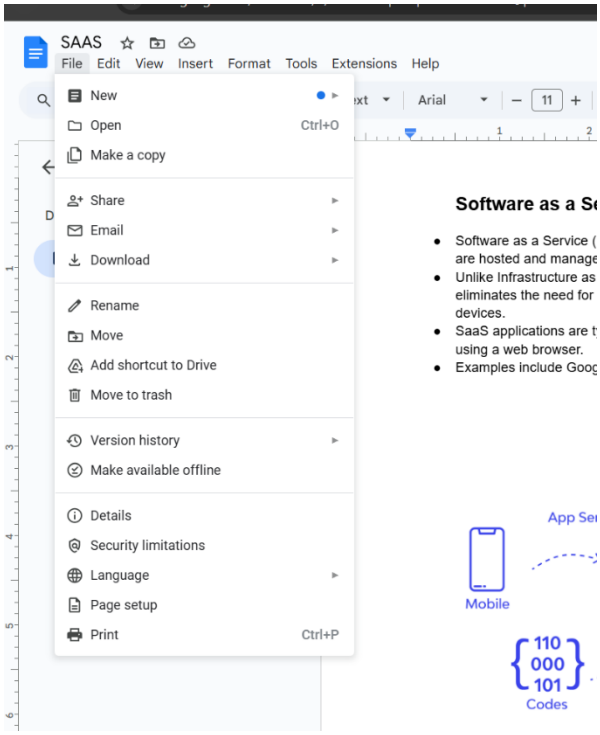
Step 4: **Share and Collaborate in Real-Time**

- Click the **"Share"** button in the top-right corner.
- Enter the **email addresses** of people you want to collaborate with.
- Set **permissions**:
  - **Viewer** – Can only read the document.
  - **Commenter** – Can add comments but not edit.
  - **Editor** – Can make changes to the document.
- Click **Send** or copy the **sharing link** to share manually.



Step 5: **Export and Download**

- Click **File > Download As** to save the document in different formats like **PDF, DOCX, TXT**.
- You can also **print** the document directly.



Conclusion:

By demonstrating **Google Docs**, you can showcase how SaaS applications:

- Work **entirely online** without installation.
- Allow **real-time collaboration** from different locations.
- Provide **automatic updates and cloud storage**.

Experiment 7:

Aim: To study and implement Database as a Service on SQL/NOSQL databases like AWS RDS, AZURE SQL/ MongoDB Lab/ Firebase.

Theory:

- **Database as a Service (DBaaS)** is a cloud computing service where a database is hosted, managed, and maintained by a cloud provider.
- It eliminates the need for businesses to set up and manage their own database infrastructure.
- DBaaS provides **automated backups, scaling, security, and maintenance**, allowing developers to focus on application development.
- It supports **SQL (Relational Databases) and NoSQL (Non-Relational Databases)**.

Advantages of DBaaS

1. **Fully Managed Service** – No need for database maintenance, backups, or security patches.
2. **Scalability** – Databases automatically scale based on demand.
3. **High Availability** – Cloud providers ensure uptime with redundancy and failover mechanisms.
4. **Cost-Efficient** – Pay only for what you use; no need for physical database servers.
5. **Security & Compliance** – Providers handle encryption, authentication, and compliance certifications.
6. **Easy Integration** – Can be easily integrated with cloud applications and analytics tools.

Disadvantages of DBaaS

1. **Less Control** – Limited customization options compared to self-managed databases.
2. **Vendor Lock-in** – Migrating databases from one provider to another can be complex.
3. **Security Concerns** – Sensitive data is stored on third-party cloud servers.
4. **Internet Dependency** – Requires a stable internet connection for access.
5. **Cost Overhead** – Long-term costs may increase based on storage and compute usage.

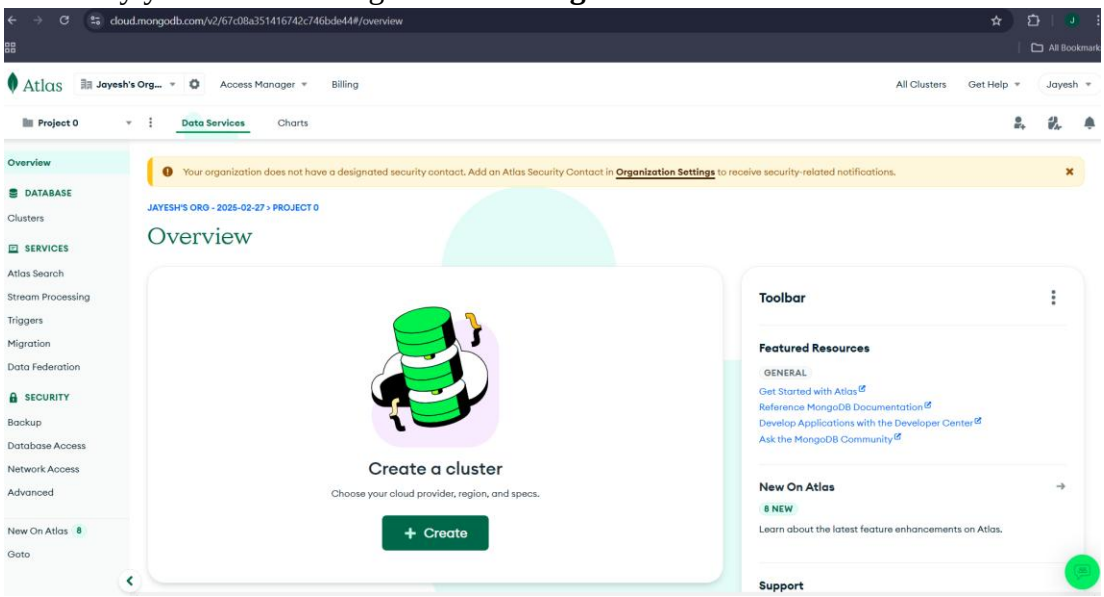
Implementation:

Steps to Implement DBaas in MongoDB Atlas (DBaaS)

MongoDB Atlas is a **cloud-based NoSQL database** that allows developers to store and manage data without managing infrastructure. Follow these steps to create and connect to a **MongoDB Atlas database.**

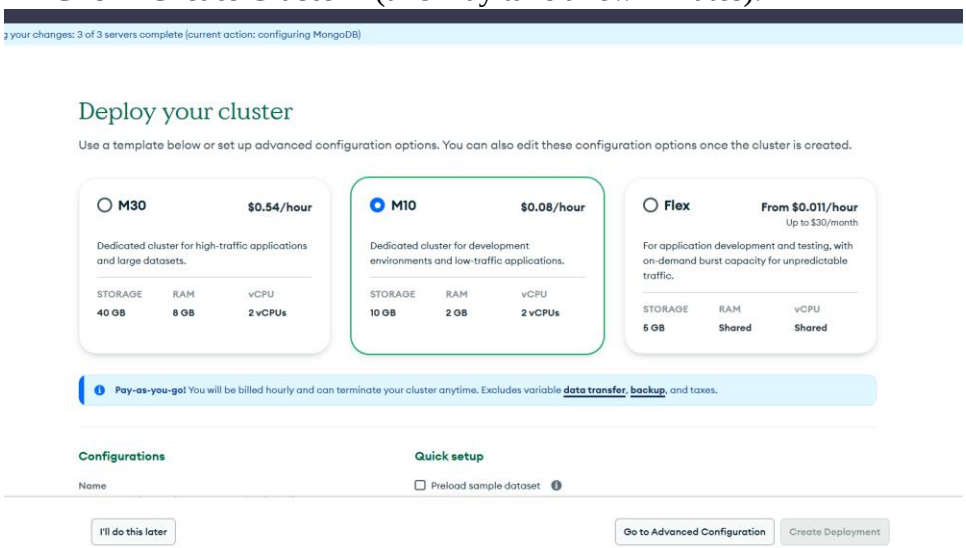
Step 1:**Sign Up and Create an Account**

- Go to [MongoDB Atlas](#).
- Click **Sign Up** and create a free account.
- Verify your email and log in to the **MongoDB Atlas Dashboard**.



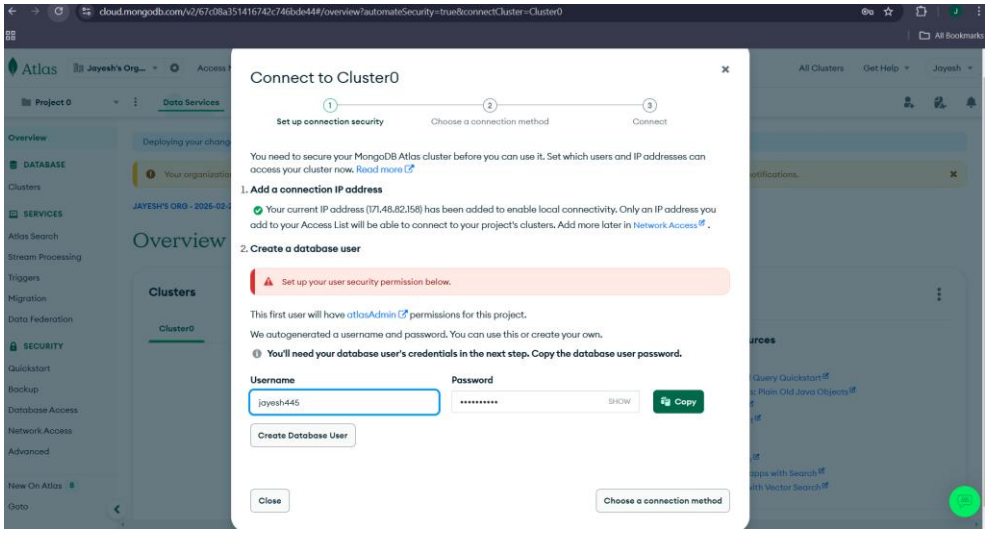
Step 2: **Create a New Cluster**

- Click **"Create a New Cluster"**.
- Select a **Cloud Provider** (AWS, Azure, or Google Cloud).
- Choose a **Free Cluster (M0 Sandbox)** for testing.
- Pick a **region** closest to your location for low latency.
- Click **"Create Cluster"** (this may take a few minutes).



Step 3**: Configure Database Access**

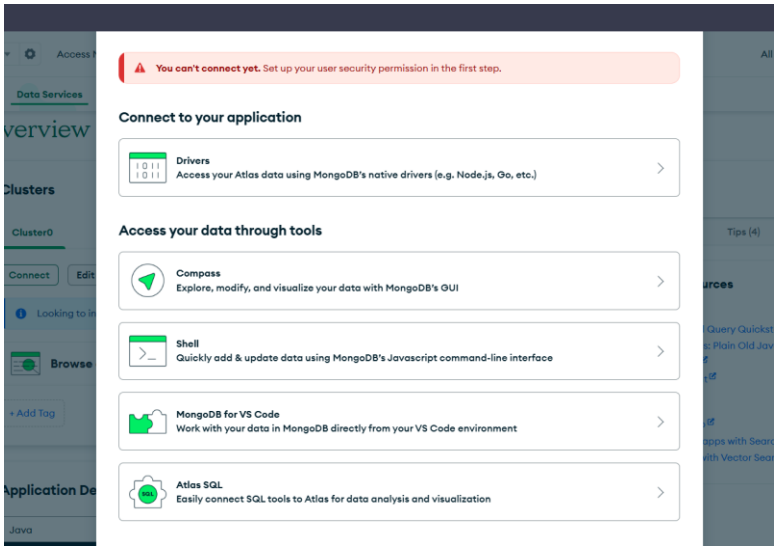
- Go to **"Database Access"** in the left menu.
- Click **"Add New Database User"**.
- Set a **username and password** (keep them safe for connection).
- Choose **"Read and Write"** access.
- Click **"Create User"**.



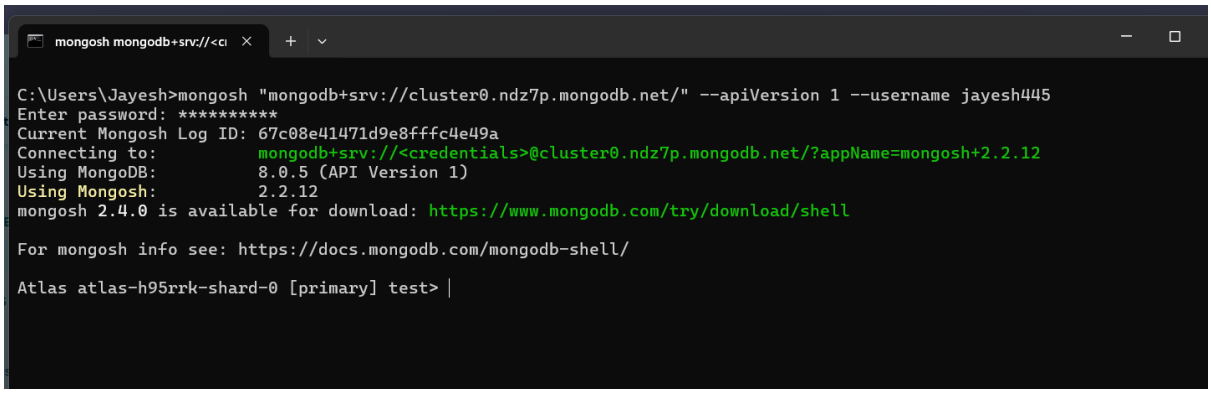
Step 4: **Connect to the Database**

- Go to **"Clusters"**, then click **"Connect"**.
- Select **"Connect Your Application"**.
- Choose **Shell** to connect through CLI.
- Copy the **Connection String** (it looks like this):

mongosh "mongodb+srv://cluster0.ndz7p.mongodb.net/" --apiVersion 1 --username <db_username> #Replace username and password with your database credentials.



Step 5: Paste the command in the CLI or Powershell and enter it will then connect to the Cluster created with default database as test.



Experiment 8:

Aim: To study and implement Security as a Service on AWS/Azure.

Theory:

- **Security as a Service (SECaaS)** is a cloud-based model that delivers **security solutions** on a subscription basis.
- Instead of maintaining **on-premise security infrastructure**, organizations use SECaaS to access advanced security tools **managed by cloud providers**.
- SECaaS solutions protect against **cyber threats, data breaches, unauthorized access, and malware**.
- Leading providers include **AWS Security Services, Microsoft Azure Security Center, and Google Cloud Security**.

Advantages of SECaaS

1. **Cost-Effective** – Reduces costs by eliminating the need for expensive security hardware.
2. **Scalability** – Easily scales security services as business needs grow.
3. **Automated Updates** – Cloud providers handle software updates and patches.
4. **Advanced Threat Protection** – Uses AI and machine learning for real-time threat detection.
5. **Compliance Management** – Helps businesses meet security regulations (GDPR, HIPAA, PCI DSS).
6. **Centralized Security Management** – Provides a unified dashboard for monitoring threats.

Disadvantages of SECaaS

1. **Data Privacy Risks** – Sensitive data is stored on third-party cloud servers.
2. **Dependence on Internet** – Requires a stable internet connection for real-time security.
3. **Limited Customization** – Less control over security settings compared to in-house security.
4. **Vendor Lock-in** – Switching security providers can be challenging.
5. **Latency Issues** – Real-time threat detection may cause slight delays.

Implementation for DDoS:

Distributed Denial of Services (DDoS): A **DDoS attack** is a cyberattack where multiple compromised systems flood a target (such as a website or application) with excessive requests, **overloading resources and causing downtime**. The primary goal of a DDoS attack is to make the service unavailable to legitimate users.

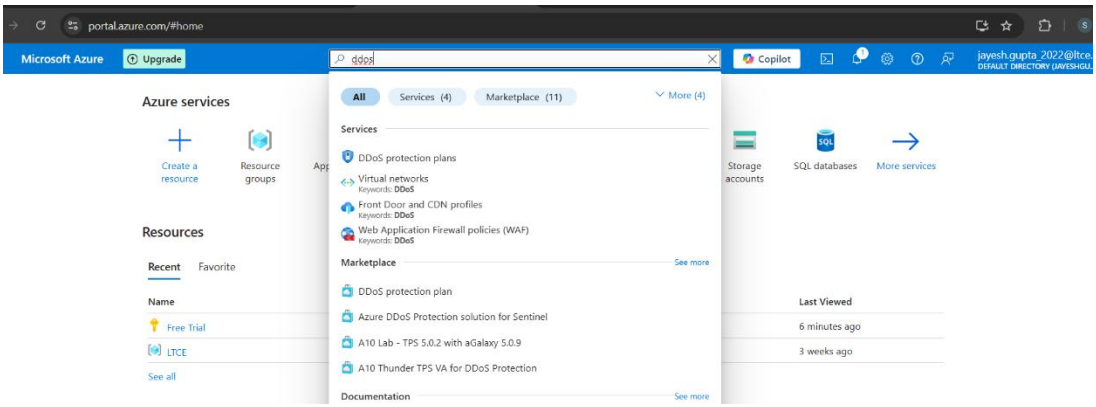
Azure provides Security as a Service (SECaaS) solutions to protect cloud applications, data, and networks. One of the key SECaaS offerings is **Azure DDoS Protection**, which helps businesses defend against cyber threats.

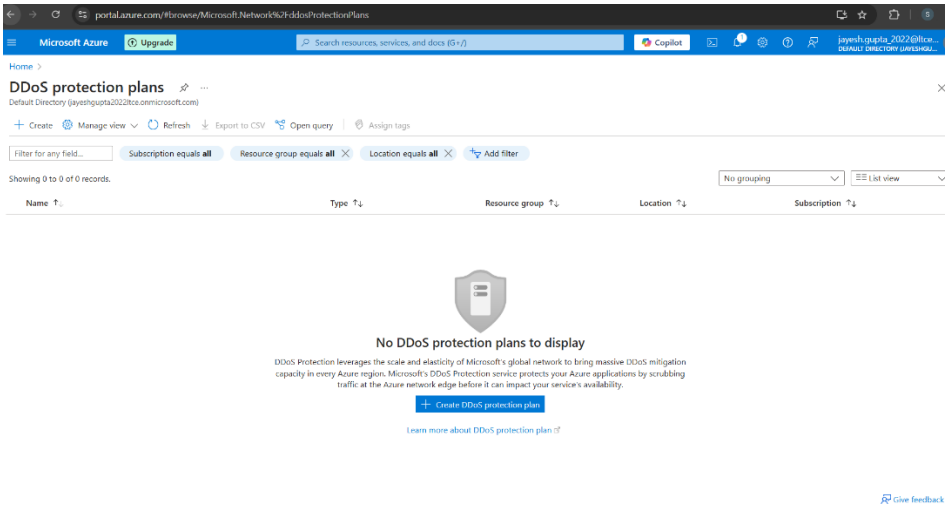
How Azure DDoS Protection Works

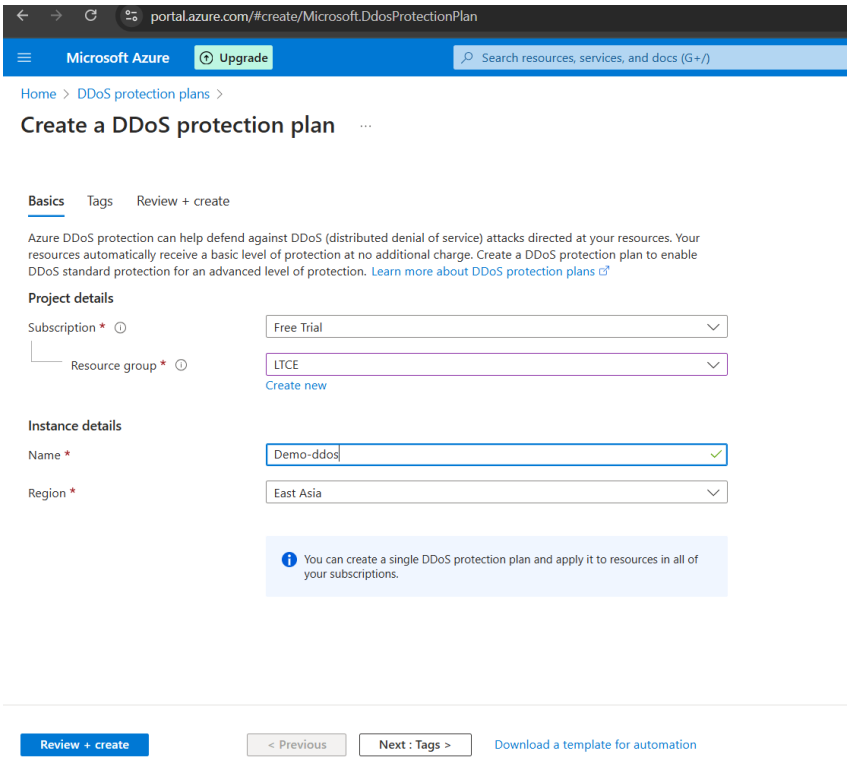
1. **Traffic Monitoring**: Azure constantly monitors network traffic.
2. **Automatic Detection**: If unusual traffic spikes are detected, mitigation is triggered.
3. **Real-Time Filtering**: Malicious traffic is blocked, while legitimate traffic remains unaffected.
4. **Post-Attack Analytics**: Provides reports via **Azure Monitor**.

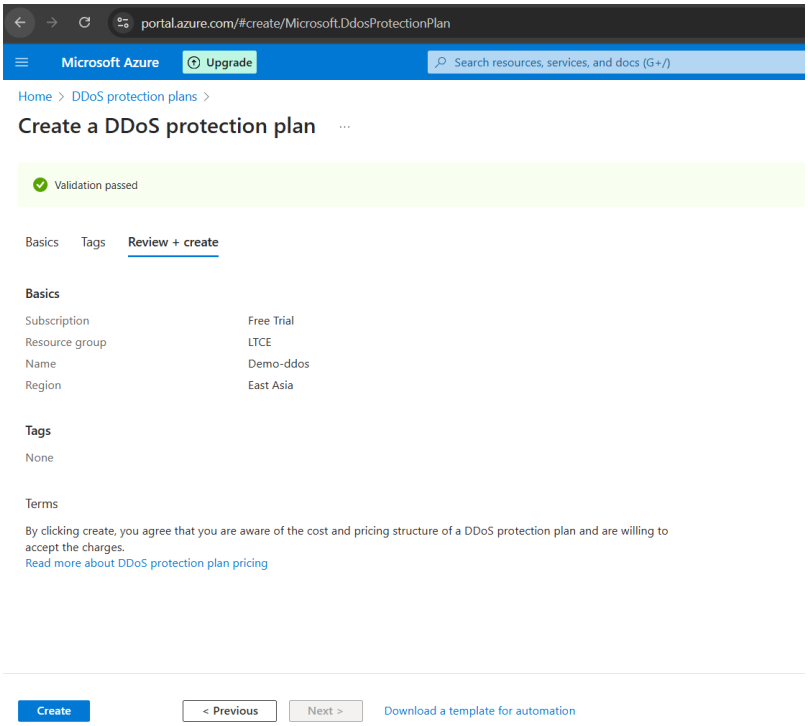
Step 1: **Create a DDoS Protection Plan**

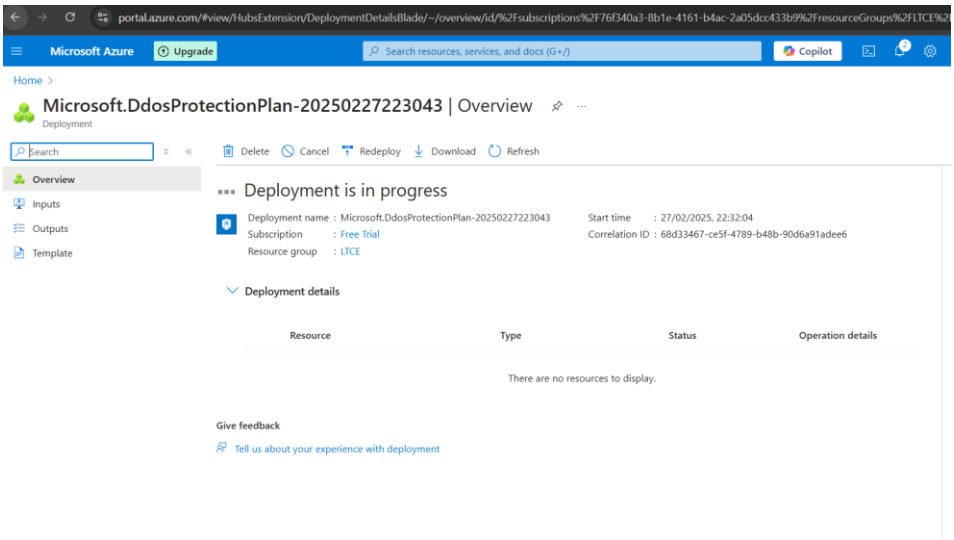
1. In the **Azure Portal**, search for **DDoS Protection Plans** in the top search bar.
2. Click **"Create DDoS Protection Plan"**.
3. Fill in the required details:
   - **Subscription**: Choose the Azure subscription where you want to deploy DDoS protection.
   - **Resource Group**: Either create a new resource group or use an existing one.
   - **Name**: Give a name to your DDoS Protection Plan (e.g., MyDDoSProtectionPlan).
   - **Region**: Select a region (e.g., East US).
4. Click **"Review + Create"**, then **"Create"**.

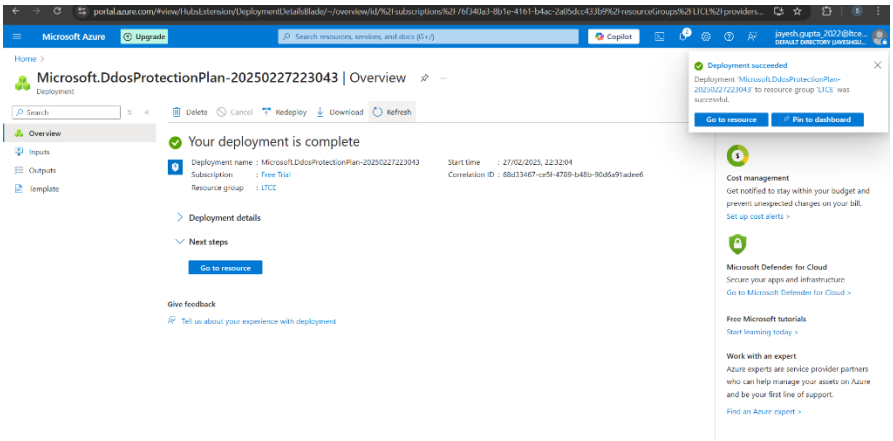



portal.azure.com/#browse/Microsoft.Network%2Fddosprotectionplans
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
DDoS protection plans
Default Directory (jayeshgupta2022ltce.onmicrosoft.com)
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 0 to 0 of 0 records.
No grouping
List view
Name
Type
Resource group
Location
Subscription
No DDoS protection plans to display
DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring massive DDoS mitigation capacity in every Azure region. Microsoft's DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.
Create DDoS protection plan
Learn more about DDoS protection plan
Give feedback


portal.azure.com/#create/Microsoft.DdosProtectionPlan
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > DDoS protection plans >
Create a DDoS protection plan
Basics
Tags
Review + create
Azure DDoS protection can help defend against DDoS (distributed denial of service) attacks directed at your resources. Your resources automatically receive a basic level of protection at no additional charge. Create a DDoS protection plan to enable DDoS standard protection for an advanced level of protection. Learn more about DDoS protection plans
Project details
Subscription *
Free Trial
Resource group *
LTCE
Create new
Instance details
Name *
Demo-ddos
Region *
East Asia
You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.
Review + create
< Previous
Next : Tags >
Download a template for automation


portal.azure.com/#create/Microsoft.DdosProtectionPlan
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > DDoS protection plans >
Create a DDoS protection plan
Validation passed
Basics
Tags
Review + create
Basics
Subscription
Free Trial
Resource group
LTCE
Name
Demo-ddos
Region
East Asia
Tags
None
Terms
By clicking create, you agree that you are aware of the cost and pricing structure of a DDoS protection plan and are willing to accept the charges.
Read more about DDoS protection plan pricing
Create
< Previous
Next >
Download a template for automation


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home >
Microsoft.DdosProtectionPlan-20250227223043 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name : Microsoft.DdosProtectionPlan-20250227223043
Subscription : Free Trial
Resource group : LTCE
Start time : 27/02/2025, 22:32:04
Correlation ID : 68d33467-ce5f-4789-b48b-90d6a91adee6
Deployment details
Resource
Type
Status
Operation details
There are no resources to display.
Give feedback
Tell us about your experience with deployment


Microsoft Azure
Upgrade
Copilot
Home >
Microsoft.DdosProtectionPlan-20250227223043 | Overview
Deployment
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : Microsoft.DdosProtectionPlan-20250227223043
Subscription : Free Trial
Resource group : LTCE
Start time : 27/02/2025, 22:32:04
Correlation ID : 68d33467-ce5f-4789-b48b-90d6a91adee6
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Deployment succeeded
Go to resource
Pin to dashboard
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Experiment 9:

Aim: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

Theory:

What is IAM (Identity and Access Management)?

Identity and Access Management (IAM) in Azure is a security framework that ensures the right users have the right access to cloud resources. It controls authentication (who can log in) and authorization (what they can do) in Azure Active Directory (Azure AD).

Features of IAM in Azure

- **Azure Active Directory (Azure AD)** – Central identity management service.
- **Role-Based Access Control (RBAC)** – Assigns permissions based on roles.
- **Multi-Factor Authentication (MFA)** – Adds an extra layer of security.
- **Conditional Access** – Allows access based on specific conditions (e.g., location, device).
- **Privileged Identity Management (PIM)** – Controls and monitors privileged accounts.

Advantages of Azure IAM

- **Centralized User Management** – All users are managed in Azure AD.
- **Granular Access Control** – RBAC allows fine-tuned permission assignments.
- **Increased Security** – MFA, Conditional Access, and PIM reduce unauthorized access.
- **Scalability** – Can be applied across multiple applications and services.

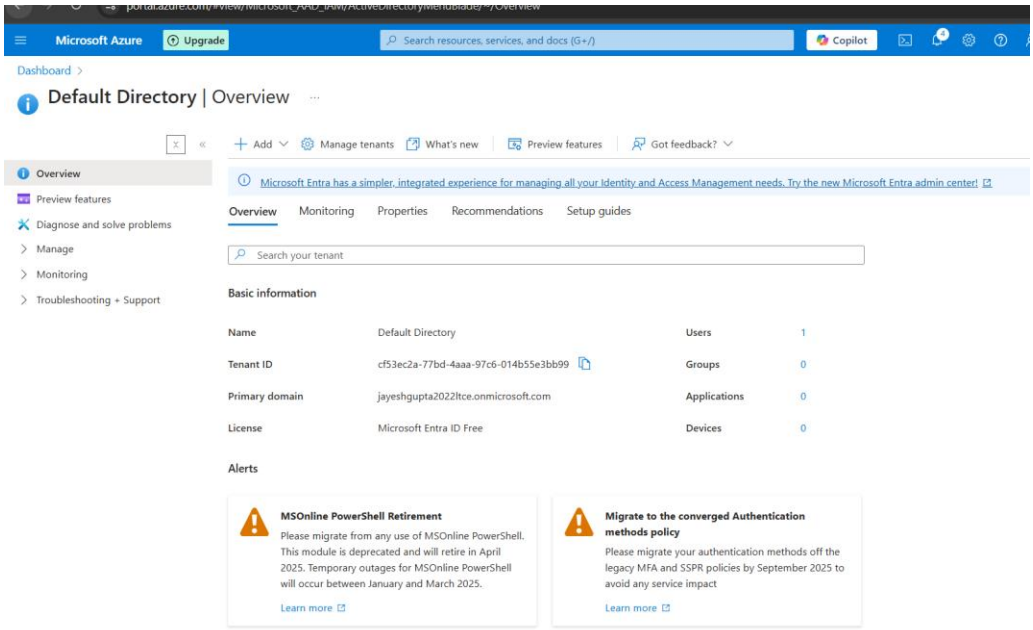
Disadvantages of Azure IAM

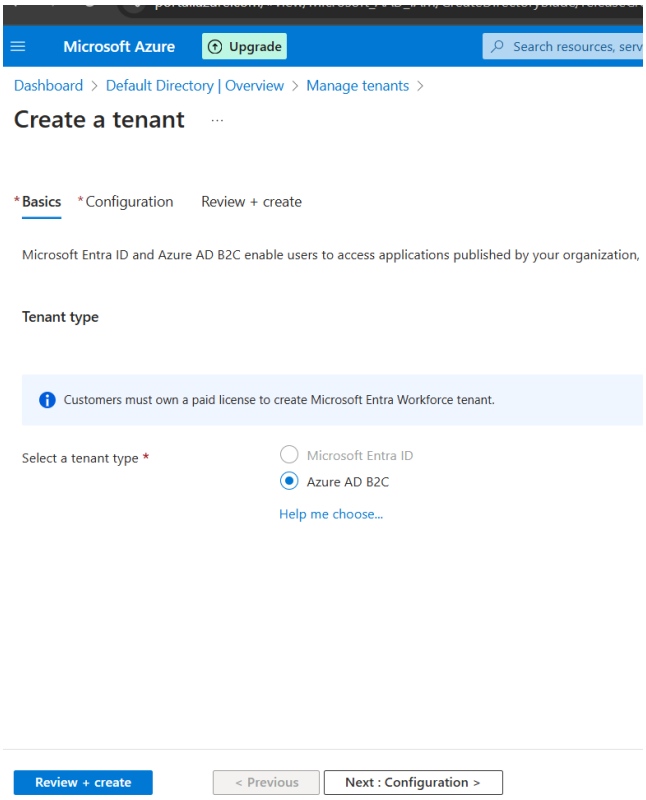
- **Complex Setup** – Requires proper configuration to avoid misconfigurations.
- **License Cost** – Advanced IAM features like PIM require Azure AD Premium.
- **Role Overhead** – Managing multiple roles can become difficult in large organizations.

Implementation:

Step 1: **Set Up Azure Active Directory (Azure AD)**

1. **Search for "Azure Active Directory"** in the portal.
2. Click **Create a new tenant** if you don't have one.
3. Choose **Directory Type** as **Azure AD**.
4. Provide an **Organization Name** and **Domain Name** (e.g., mycompany.onmicrosoft.com).
5. Click **Create**.





Microsoft Azure | Upgrade | Search resources, services, and docs (G+/)

Dashboard > Default Directory | Overview > Manage tenants >

Create a tenant

*Basics *Configuration Review + create

Directory details

Configure your new directory

Organization name * LTCoE

Initial domain name * jayeshgpt

Country/Region United States

Geographic location - United States

The location selected above will determine the geographic location where Azure AD
AD B2C region availability and data residency.

Subscription

Choose the subscription to use for Azure AD B2C. See pricing details

Subscription * Free Trial

Resource group * LTCE

Create new

Review + create | < Previous | Next : Review + create >

https://portal.azure.com/#

Dashboard > Default Directory | Overview > Manage tenants >

Create a tenant

Validation passed.

*Basics *Configuration Review + create

Summary

Basics

Tenant type	Azure AD B2C

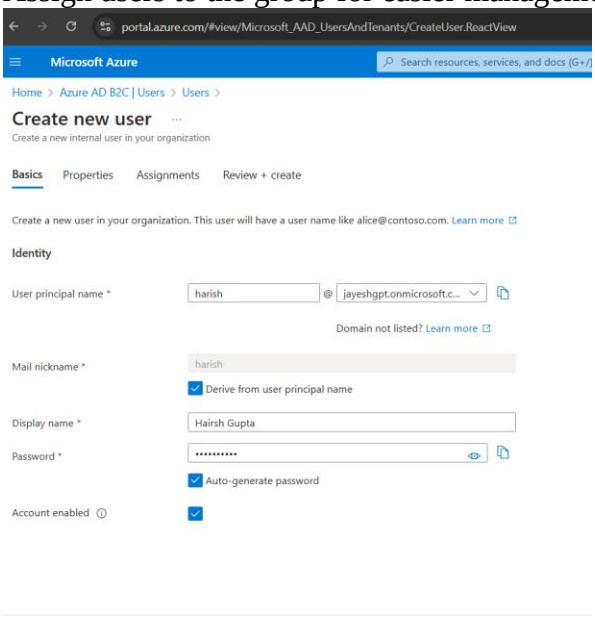
Configuration

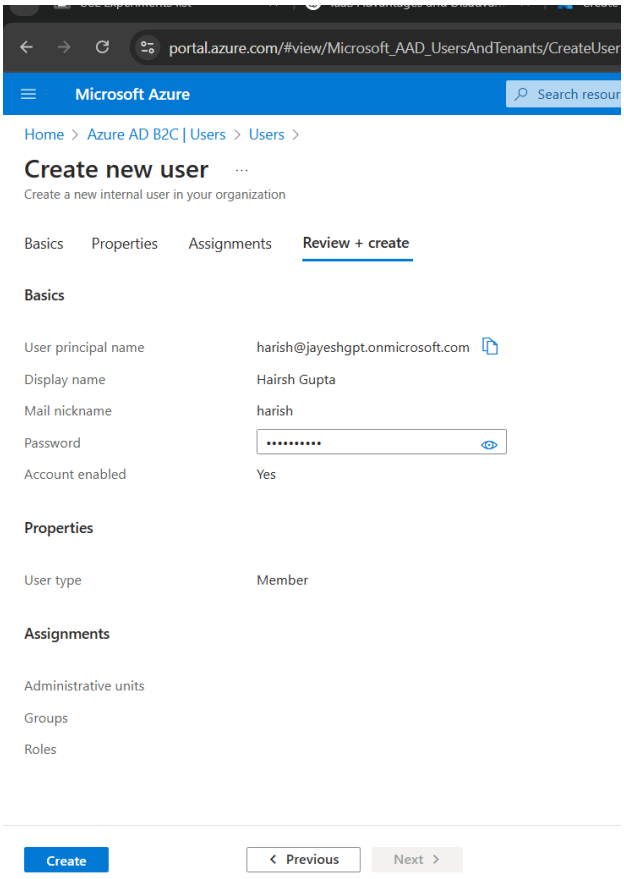
Organization name	LTCoE
Initial domain name	jayeshgpt.onmicrosoft.com
Country/Region	United States
Subscription	Free Trial
Resource group	LTCE

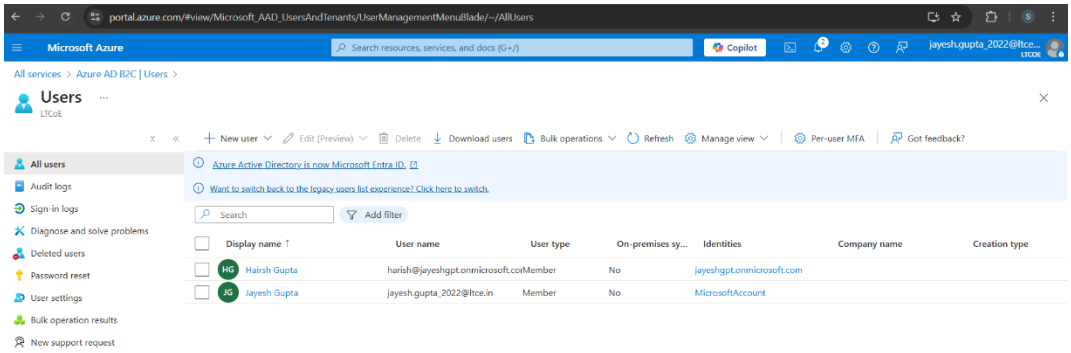
Create | < Previous | Next >

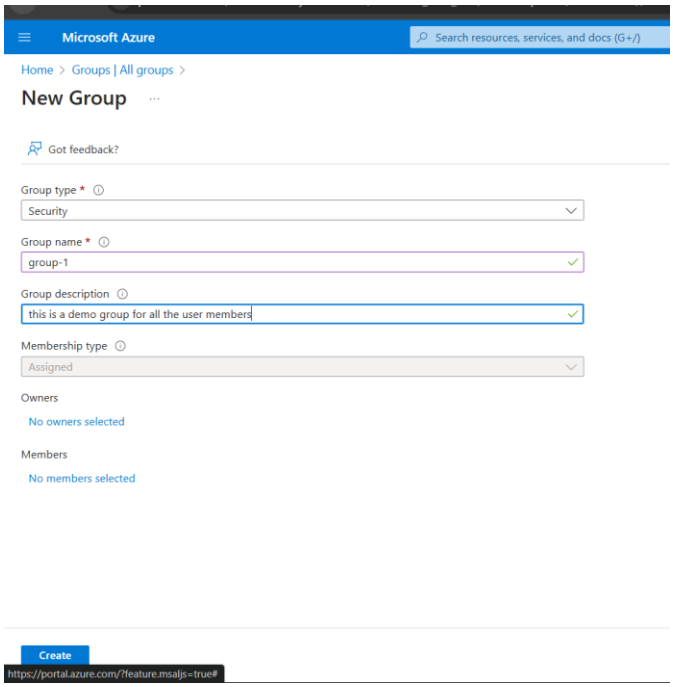
Step 2: **Add Users and Groups**

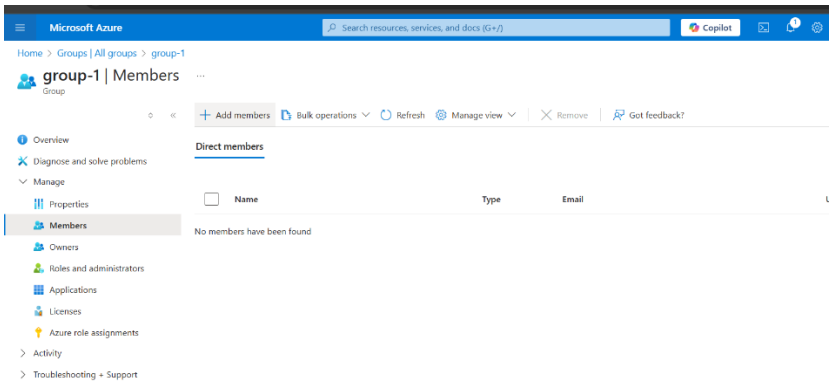
1. Go to **Azure AD → Users** → Click **+ New user**.
2. Fill in user details and set a password.
3. Click **Create**.
4. To create a group, go to **Azure AD → Groups → + New Group**.
5. Assign users to the group for easier management.

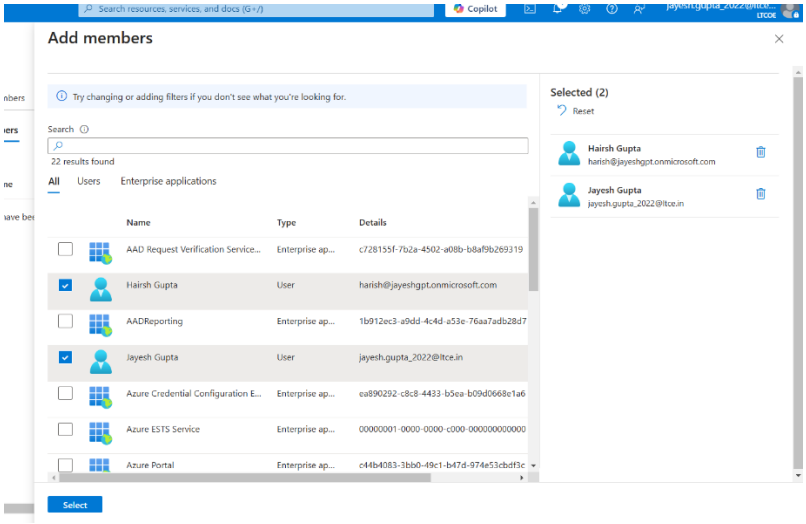


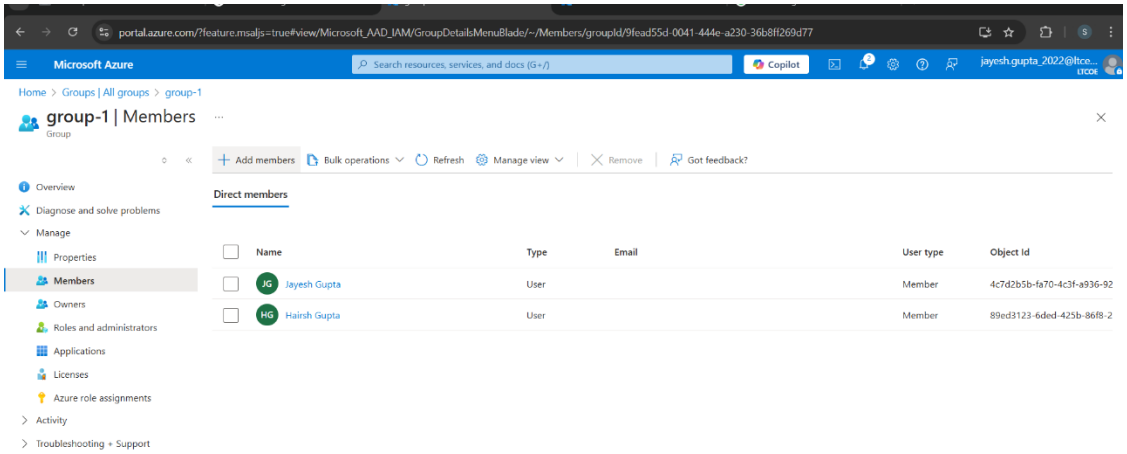



portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/AllUsers
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
jayesh.gupta_2022@ltce...
All services > Azure AD B2C | Users >
Users
LTCoE
New user
Edit (Preview)
Delete
Download users
Bulk operations
Refresh
Manage view
Per-user MFA
Got feedback?
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
New support request
Azure Active Directory is now Microsoft Entra ID.
Want to switch back to the legacy users list experience? Click here to switch.
Search
Add filter
Display name
User name
User type
On-premises sy...
Identities
Company name
Creation type
Hairsh Gupta
harish@jayeshgpt.onmicrosoft.com
Member
No
jayeshgpt.onmicrosoft.com
Jayesh Gupta
jayesh.gupta_2022@ltce.in
Member
No
MicrosoftAccount


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Groups | All groups >
New Group
Got feedback?
Group type *
Security
Group name *
group-1
Group description
this is a demo group for all the user members
Membership type
Assigned
Owners
No owners selected
Members
No members selected
Create
https://portal.azure.com/?feature.msaljs=true#


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Groups | All groups > group-1
group-1 | Members
Group
Add members
Bulk operations
Refresh
Manage view
Remove
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Applications
Licenses
Azure role assignments
Activity
Troubleshooting + Support
Direct members
Name
Type
Email
No members have been found





Conclusion:

- IAM in Azure provides secure authentication, role-based access, and identity protection.
- Azure AD, RBAC, MFA, Conditional Access, and PIM are key IAM implementations.
- Proper IAM policies help organizations protect their cloud resources from unauthorized access.