

**EX NO: 1A**

## **CREATION OF CLOUD ORGANIZATION IN GCP**

**DATE:**

### **AIM:**

To Create a Cloud Organization in Google Cloud platform with Role-based access control.

### **PROCEDURE:**

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

Google Cloud Platform provides infrastructure as a service, platform as a service, and server less computing environments.

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

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

### **Creating your project**

To deploy your app on App Engine, you must create a Google Cloud project, which is a top level container that holds your App Engine application resources as well as other Google Cloud resources.

In this task, you create a Google Cloud project and an App Engine application to store settings, computing resources, credentials, and metadata for your app.

If you already have a Google Cloud project with App Engine and the Cloud Build API enabled, continue to Writing Your Web Service.

### **Creating a Google Cloud project**

1. If you're new to Google Cloud, create an account to evaluate how our products perform in real-world scenarios. New customers get \$300 in free credits to run, test, and deploy workloads.

2. In the Google Cloud console, on the project selector page, select or create a Google Cloud project.

Note: If you don't plan to keep the resources that you create in this procedure, create a project instead of selecting an existing project. After you finish these steps, you can delete the project, removing all resources associated with the project.

Go to project selector

3. Make sure that billing is enabled for your Google Cloud project.

4. Enable the Cloud Build API.

Enable the API

5. Install the Google Cloud CLI.

6. To initialize the gcloud CLI, run the following command:  
gcloud init

7. Create an App Engine application for your Google Cloud project in the Google Cloud console.  
Open app creation

8. Select a region where you want your app's computing resources located.

**Note:** After you create your App Engine app, you cannot change the region. To reduce latency, choose the region closest to your app's intended users. For more information on the available regions, see App Engine Locations.

### **Next step**

Now that your Google Cloud project is set up, you're ready to write a basic web service with Node.js.

### **Setting up your development environment**

bookmark\_border

Go Java Node.js PHP Python Ruby

Use the following steps to set up your local environment for developing and deploying your App Engine services:

1. Install the latest release of Python 3.

See Python3 Runtime Environment for a list of the supported versions.

2. Install and initialize the gcloud CLI for deploying and managing your apps. If you already have the gcloud CLI installed and initialized, run the gcloud components update command to update to the latest release. By downloading, you agree to be bound by the Terms that govern use of the gcloud CLI for App Engine.

### Optional tools:

- Install Git for access to code, samples, libraries, and tools in the Google Cloud GitHub repository.
- Install your preferred tooling or framework, for example you can use any of the following frameworks

to develop your Python 3 app:

- Flask
- Django
- Pyramid
- Bottle
- web.py
- Tornado

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged if you run out of credits. [Learn more](#)

Dismiss [Start free](#)

Google Cloud My First Project creden Search

APIs & Services Credentials [+ Create credentials](#) [Delete](#) [Restore deleted credentials](#)

Enabled APIs & services  
Library  
Credentials  
OAuth consent screen  
Page usage agreements

Create credentials to access your enabled APIs. [Learn more](#)

Remember to configure the OAuth consent screen with information about your application. [Configure consent screen](#)

API Keys

<input type="checkbox"/>	Name	Creation date ↓	Restrictions	Actions
No API keys to display				

OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID	Actions
No OAuth clients to display					

Service Accounts [Manage service accounts](#)

<input type="checkbox"/>	Email	Name ↑	Actions
No service accounts to display			

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged if you run out of credits. [Learn more](#)

Dismiss [Start free](#)

Google Cloud

My First Project

top products

Search

Solutions / Solutions

All products

Jump Start Solutions

Solution deployments

Categories

Management

Compute

Storage

Analytics

Networking

Distributed Cloud

Serverless

Databases

Observability

Operations

Security

App Development

All products

Explore products from Google Cloud and recommended partners at a glance

Find and deploy over 4,500 products in Marketplace

VISIT MARKETPLACE

Name	Description
<a href="#">APIs &amp; Services</a>	API management for cloud services
<a href="#">Google Auth Platform</a>	OAuth configuration and credentials
<a href="#">Billing</a>	Assortment of billing and cost management tools
<a href="#">IAM &amp; Admin</a>	Resource access control
<a href="#">Google Cloud Setup</a>	Set up and deploy a best-practice foundation
<a href="#">Admin for Gemini</a>	Purchase and manage Gemini Products in Google Cloud
<a href="#">Cloud Hub</a>	Cloud insights, unified view.

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged if you run out of credits. [Learn more](#)

Google Cloud

My First Project

Search (/) for resources, docs, t

IAM & Admin / IAM

IAM

PAM

Principal Access Boun...

Organizations

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Fede...

Workforce Identity Fede...

Labels

Tags

Manage Resources

Release Notes

IAM

Allow Deny Recommendations history

Access additional recommendations with Security accounts, enabling multi-factor authentication (MFA)

Upgrade Learn more

Permissions for project "My First Project"

These permissions affect this project and all of its resources. [Learn more](#)

View by principals

View by roles

Grant access

Remove access

Filter

Enter property name or value

Type	Principal	Name
<input type="checkbox"/>	johnallanmiranda.26csa@licet.ac.in	JOHN

Grant access to "My First Project"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

My First Project

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals \*  
abishekjoshua.26csa@licet.ac.in X

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role \*

Owner

IAM condition (optional) ⓘ

+ Add IAM condition

Full access to most Google Cloud resources. See the list of included permissions.

+ Add another role

Save

Cancel

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged if you run out of credits. [Learn more](#)

Dismiss [Start free](#)

Google Cloud

My First Project

Search (/) for resources, docs, products, and more

Search

IAM & Admin / IAM

IAM

PAM

Principal Access Boun...

Organizations

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Fede...

Workforce Identity Fed...

Labels

Tags

Manage Resources

Release Notes

IAM

[Learn](#)

Allow Deny Recommendations history

Access additional recommendations with Security Command Center Premium, including those for non-basic roles, removing lateral movement permissions from service accounts, enabling multi-factor authentication (MFA), and implementing other security enhancements.

[Upgrade](#) [Learn more](#)

Permissions for project "My First Project"

These permissions affect this project and all of its resources. [Learn more](#)

☐ Include Google-provided role grants

[View by principals](#)

View by roles

[Grant access](#)

[Remove access](#)

Filter Enter property name or value

☐ Type

Principal ↑

Name

Role

Security insights

☐

abishkekjoshua.26csa@licet.ac.in

ABISHEK JOSHUA C 22CSA

Owner

☐

johnallanmiranda.26csa@licet.ac.in

JOHN ALLAN MIRANDA A 22CSA

Owner

**RESULT:**

Thus Cloud Organization in Google Cloud platform with Role-based access control is created.

## **EX NO: 1B          CREATION OF CLOUD ORGANIZATION IN AWS**

**DATE:**

### **AIM:**

To Create a Cloud Organization in Amazon Web Services (AWS) with Role-based Access Control.

### **PROCEDURE:**

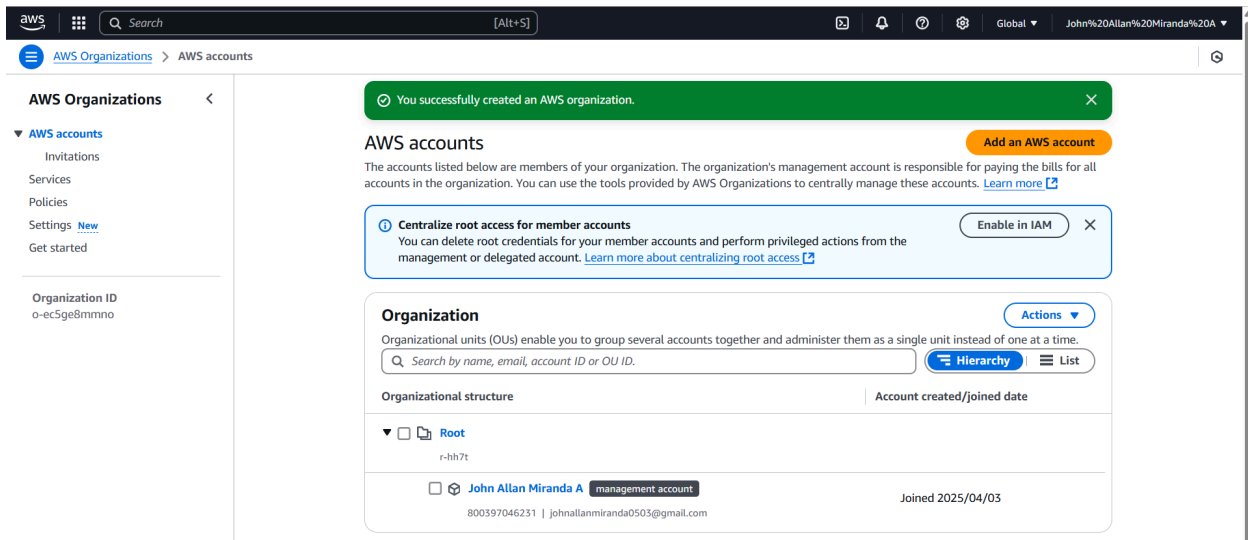
**Amazon Web Services (AWS)**, offered by Amazon, is a comprehensive cloud computing platform that provides infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). AWS provides scalable cloud computing services, including computing power, storage, databases, machine learning, and analytics, to customers across various industries.

Creating an AWS Organization allows businesses to centrally manage multiple AWS accounts, enforce security policies, and optimize resource utilization. AWS Organizations enable Role-Based Access Control (RBAC), ensuring secure and efficient access management.

#### **Creating Your AWS Organization and Setting Up an Account**

1. **Sign Up for AWS:**  
Go to the AWS website and create an AWS account.
2. **Access the AWS Management Console:**  
Log in to the AWS Management Console.  
Navigate to the AWS Organizations service.
3. **Create an AWS Organization:**  
Click on "Create an Organization."
4. **Create AWS Accounts within the Organization:**  
In AWS Organizations, click Add an AWS Account to create or invite existing AWS accounts.
5. **Enable and Configure IAM Policies for Role-Based Access Control (RBAC):**  
Navigate to IAM (Identity and Access Management).  
Create Users, Groups, and Roles with specific permissions.  
Attach predefined or custom IAM Policies to enforce access control.
6. **Enable AWS CLI for Command-Line Access:**  
Download and install the AWS Command Line Interface (CLI).

7. Configure the CLI using the following command:  
aws configure  
Enter your AWS Access Key, Secret Access Key, Region, and Output format.
8. Create and Deploy an Application in AWS:  
Choose a computing service such as Amazon EC2, AWS Lambda, or Elastic Beanstalk.  
Set up the required storage services like Amazon S3 or Amazon RDS.  
Deploy the application using AWS Management Console, AWS CLI, or Infrastructure as Code (IaC) tools like AWS CloudFormation or Terraform.
9. Select an AWS Region for Your Application:  
Choose a region closest to your users to minimize latency.  
Ensure compliance with data residency requirements.



**AWS Organizations** > **AWS accounts**

**AWS accounts**

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. [Learn more](#)

**Centralize root access for member accounts** Enable in IAM ×

You can delete root credentials for your member accounts and perform privileged actions from the management or delegated account. [Learn more about centralizing root access](#)

**Organization** Actions

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Hierarchy List

**Organizational structure** Account created/joined date

Organizational unit	Account created/joined date
<b>Root</b> r-hh7t	
<input type="checkbox"/> <b>AbiJoshua</b> 145107590821   abijoshua234@gmail.com	Joined 2025/04/03
<input type="checkbox"/> <b>John Allan Miranda A</b> <span>management account</span> 800397046231   johnallanmiranda0503@gmail.com	Joined 2025/04/03

**IAM** > **Roles** > **AWSServiceRoleForOrganizations**

**AWSServiceRoleForOrganizations** Info Delete

Service-linked role used by AWS Organizations to enable integration of other AWS services with Organizations.

**Summary** Edit

<b>Creation date</b> April 03, 2025, 19:45 (UTC+05:30)	<b>ARN</b> arn:aws:iam::800397046231:role/aws-service-role/organizations.amazonaws.com/AWSServiceRoleForOrganizations
<b>Last activity</b> -	<b>Maximum session duration</b> 1 hour

**Permissions** Trust relationships Tags Last Accessed

**Permissions policies (1)** Info

Filter by Type All types

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<b>AWSOrganizationsServiceTrustPolicy</b>	AWS managed	1

## RESULT :

Thus to Create a Cloud Organization in Amazon Web Services (AWS) with Role-based Access Control is created.



## **EX NO: 1C          CREATION OF CLOUD ORGANIZATION IN AZURE**

**DATE:**

**AIM:**

To Create a Cloud Organization in Azure with Role-based Access Control.

**PROCEDURE:**

**Microsoft Azure**, offered by Microsoft, is a cloud computing platform providing IaaS, PaaS, and SaaS solutions. Azure enables businesses to manage resources efficiently with secure role-based access control.

### **Creating an Azure Organization and Setting Up an Account**

1. Sign Up for Azure:  
Go to the Azure website and create an account.  
New users get free credits for testing services.
2. Access Azure Portal:  
Log in to the Azure Portal.  
Navigate to Azure Active Directory (Azure AD).
3. Create an Azure Tenant:  
Go to Azure AD > Manage Tenants > Create a Tenant.  
Choose an organization name and set up the domain.
4. Create and Manage Azure Subscriptions:  
Go to Subscriptions in the Azure Portal.  
Click Add Subscription to create a new one.
5. Enable and Configure RBAC (Role-Based Access Control):  
Navigate to Azure AD > Users and Groups.  
Create Users, Groups, and Roles with specific permissions.  
Assign RBAC roles using Azure IAM (Identity and Access Management).
6. Create and Deploy an Application in Azure:  
Choose a service like Azure Virtual Machines (VMs), Azure Functions, or App Services.  
Set up storage using Azure Blob Storage or Azure SQL Database.  
Deploy using the Azure Portal, CLI, or Infrastructure as Code (Bicep, ARM templates, Terraform).

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

johnnallanmiranda.26csa...  
DEFAULT DIRECTORY

Home > Azure for Students | Access control (IAM) >

Add role assignment

RoleMembersConditionsReview + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function rolesPrivileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search by role name, description, permission, or IDType: AllCategory: All

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	<a href="#">View</a>
AcrDelete	acr delete	BuiltinRole	Containers	<a href="#">View</a>
AcrImageSigner	acr image signer	BuiltinRole	Containers	<a href="#">View</a>
AcrPull	acr pull	BuiltinRole	Containers	<a href="#">View</a>
AcrPush	acr push	BuiltinRole	Containers	<a href="#">View</a>
AcrQuarantineReader	acr quarantine data reader	BuiltinRole	Containers	<a href="#">View</a>
AcrQuarantineWriter	acr quarantine data writer	BuiltinRole	Containers	<a href="#">View</a>

Review + assignPreviousNext

Feedback

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

johnnallanmiranda.26csa...  
DEFAULT DIRECTORY

Home > Azure for Students | Access control (IAM) >

Add role assignment

RoleMembersConditionsReview + assign

RoleReader

Scope/subscriptions/a5cf36fd-3581-479e-9e53-4dcbef90d9cb

Members

Name	Object ID	Type
abishekjoshua.26csa@licet.ac.in	--	User

DescriptionNo description

Review + assignPreviousNext

Adding Role assignment

abishekjoshua.26csa@licet.ac.in is being added as Reader for Azure for Students.

Inited user

abishekjoshua.26csa@licet.ac.in was added to the Default Directory directory as a guest. abishekjoshua.26csa@licet.ac.in was also sent an invitation link they must accept.  
To manually invite:  
1. Right-click and copy this [invitation link](#). (Do not click the link because it starts the invitation process.)  
2. Send the invitation link to the invited user.

Feedback

## RESULT:

Thus to Create a Cloud Organization in Azure with Role-based Access Control is created.