PRACTICAL NO : 10

AIM : Case study on Amazon EC2/Microsoft Azure/Google Cloud

Platform/IBM/Salesforce.com.

**Case study on: AWS**

# Introduction

Amazon web service is a platform that offers flexible, reliable, scalable, easy-to- use and cost-effective cloud computing solutions.

AWS is a comprehensive, easy to use computing platform offered Amazon. The platform is developed with a combination of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings.

## AWS Services

Amazon Web Services offers a wide range of different business purpose global cloud-based products. The products include storage, databases, analytics, networking, mobile, development tools, enterprise applications, with a pay-as- you-go pricing model.



* + AWS Compute Services
  + Storage
  + Security Services
  + Database Services
  + Analytics
  + Management Services
  + Internet of Things
  + Application Services
  + Deployment and Management
  + Developer Tools
  + Mobile Services
  + Business Productivity
  + Desktop & App Streaming
  + Artificial Intelligence
  + AR & VR (Augmented Reality & Virtual Reality)
  + Customer Engagement
  + Game Development

# Applications of AWS services

* + Web site hosting
  + Application hosting/SaaS hosting
  + Media Sharing (Image/ Video)
  + Mobile and Social Applications
  + Content delivery and Media Distribution
  + Storage, backup, and disaster recovery
  + Development and test environments
  + Academic Computing
  + Search Engines
  + Social Networking

# Companies using AWS

* + Instagram
  + Zoopla
  + Smugmug
  + Pinterest
  + Netflix
  + Dropbox
  + Etsy
  + Talkbox
  + Playfish
  + Ftopia

# Advantages of AWS

Following are the pros of using AWS services:

* + AWS allows organizations to use the already familiar programming models, operating systems, databases, and architectures.
  + It is a cost-effective service that allows you to pay only for what you use, without any up-front or long-term commitments.
  + Offers fast deployments
  + You can easily add or remove capacity.
  + You are allowed cloud access quickly with limitless capacity.
  + Offers Centralized Billing and management
  + Offers Hybrid Capabilities

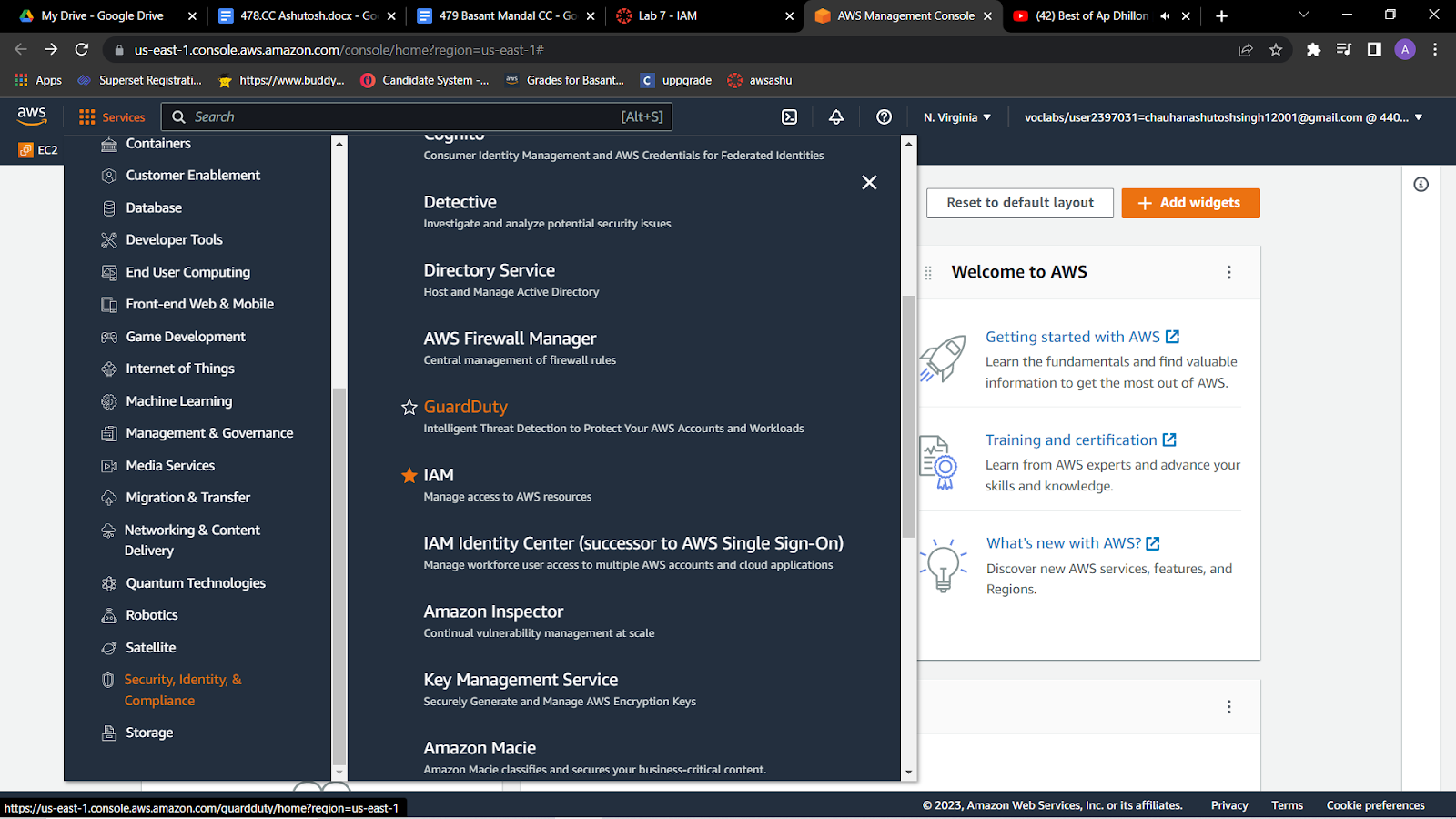
# Disadvantages of AWS

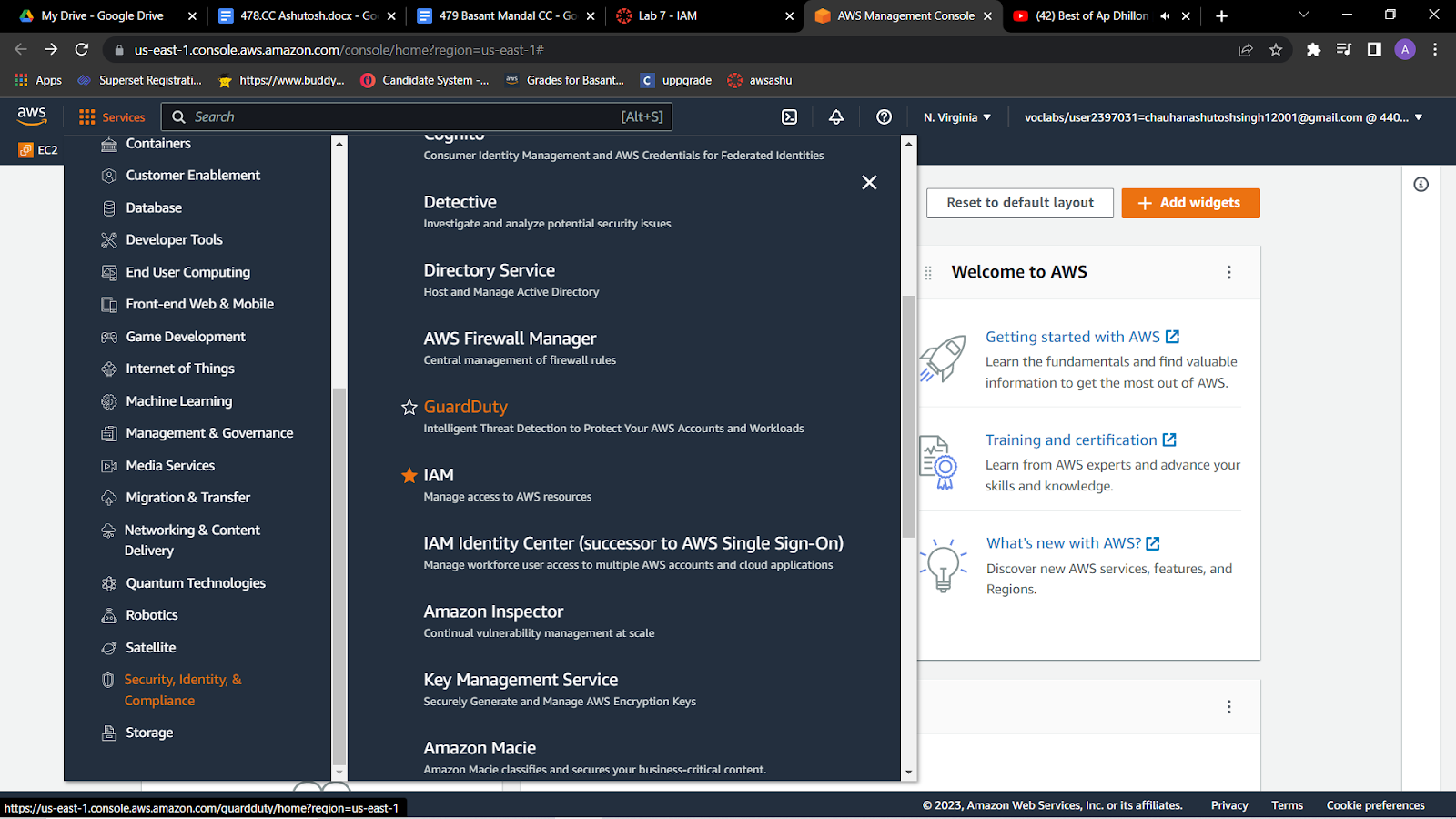
* + If you need more immediate or intensive assistance, you'll have to opt for paid support packages.
  + Amazon Web Services may have some common cloud computing issues when you move to a cloud. For example, downtime, limited control, and backup protection.

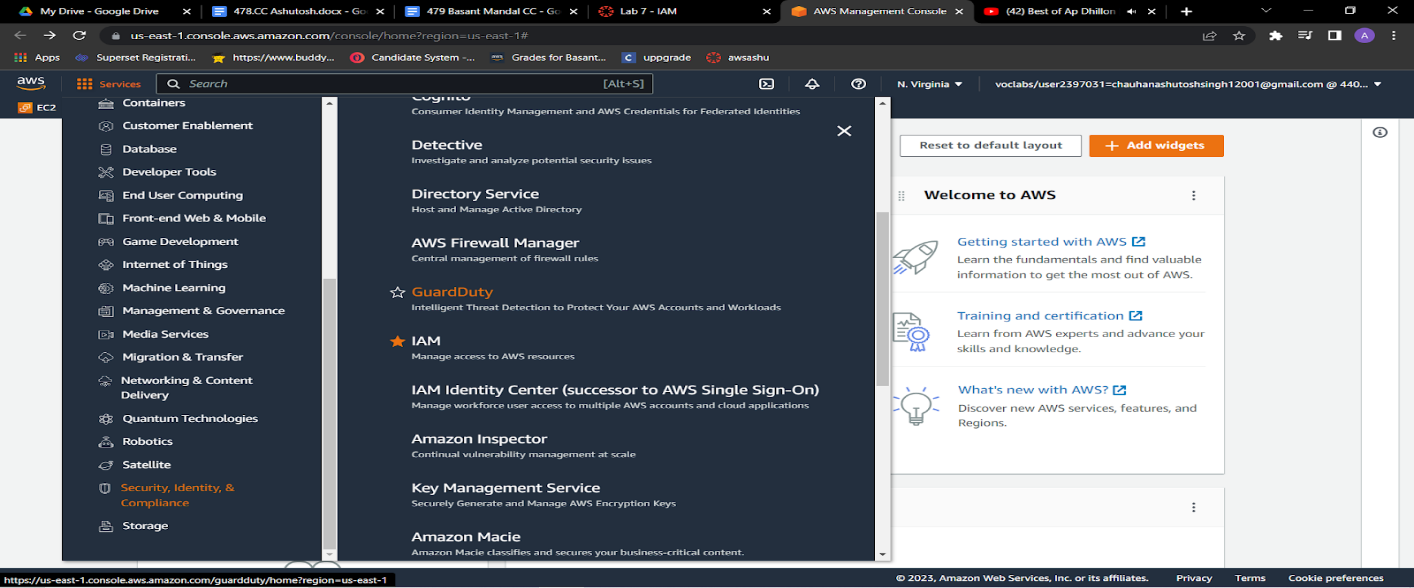
* + AWS sets default limits on resources which differ from region to region. These resources consist of images, volumes, and snapshots.
  + Hardware-level changes happen to your application which may not offer the best performance and usage of your applications.

Steps:

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

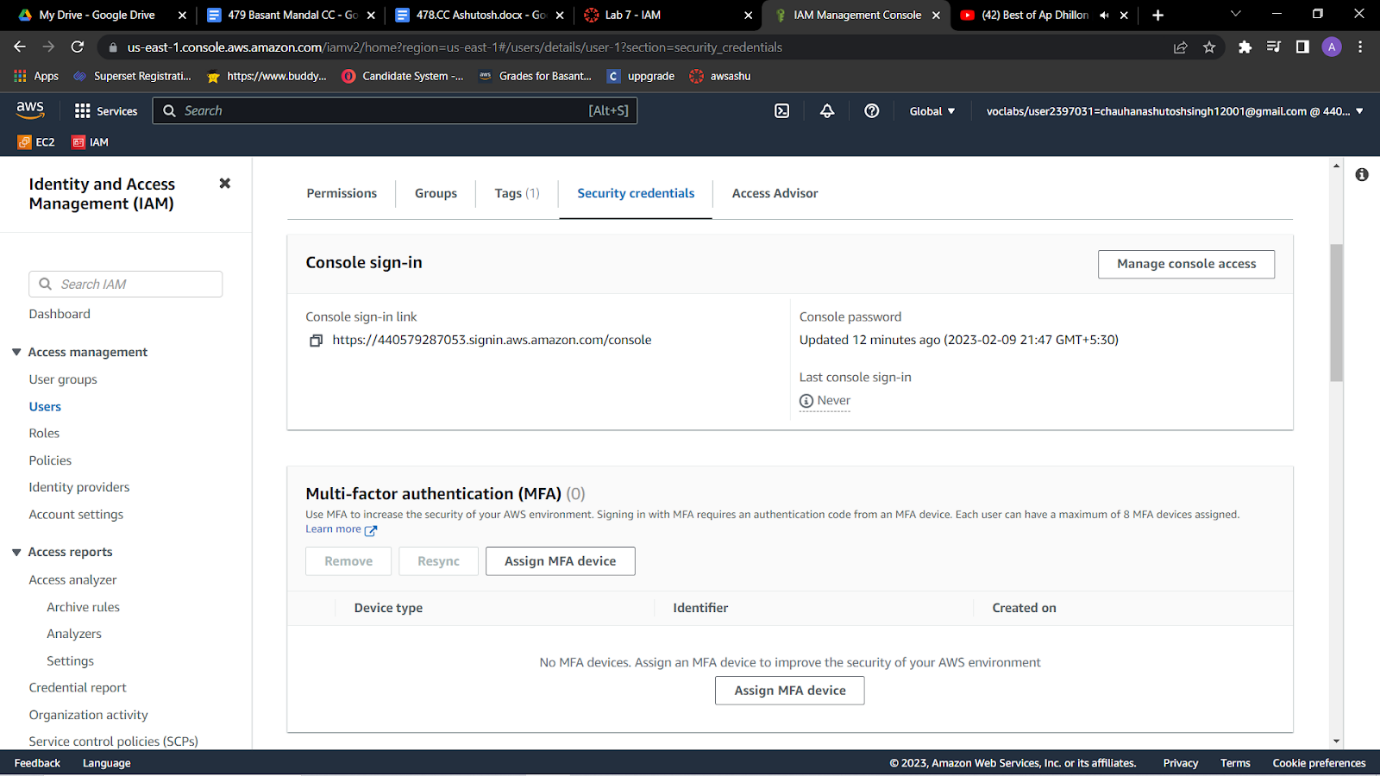




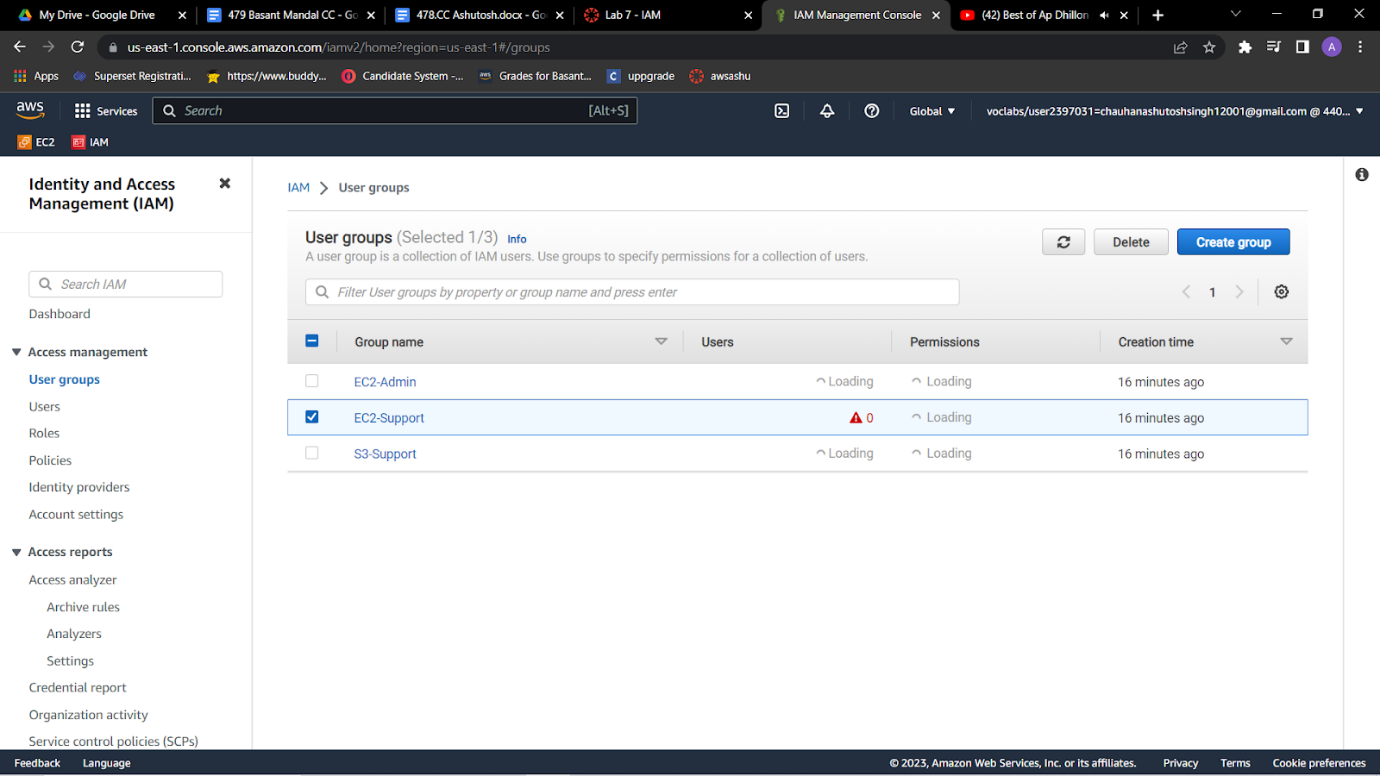


2.In the navigation pane on the left, choose **Users**.Create Users

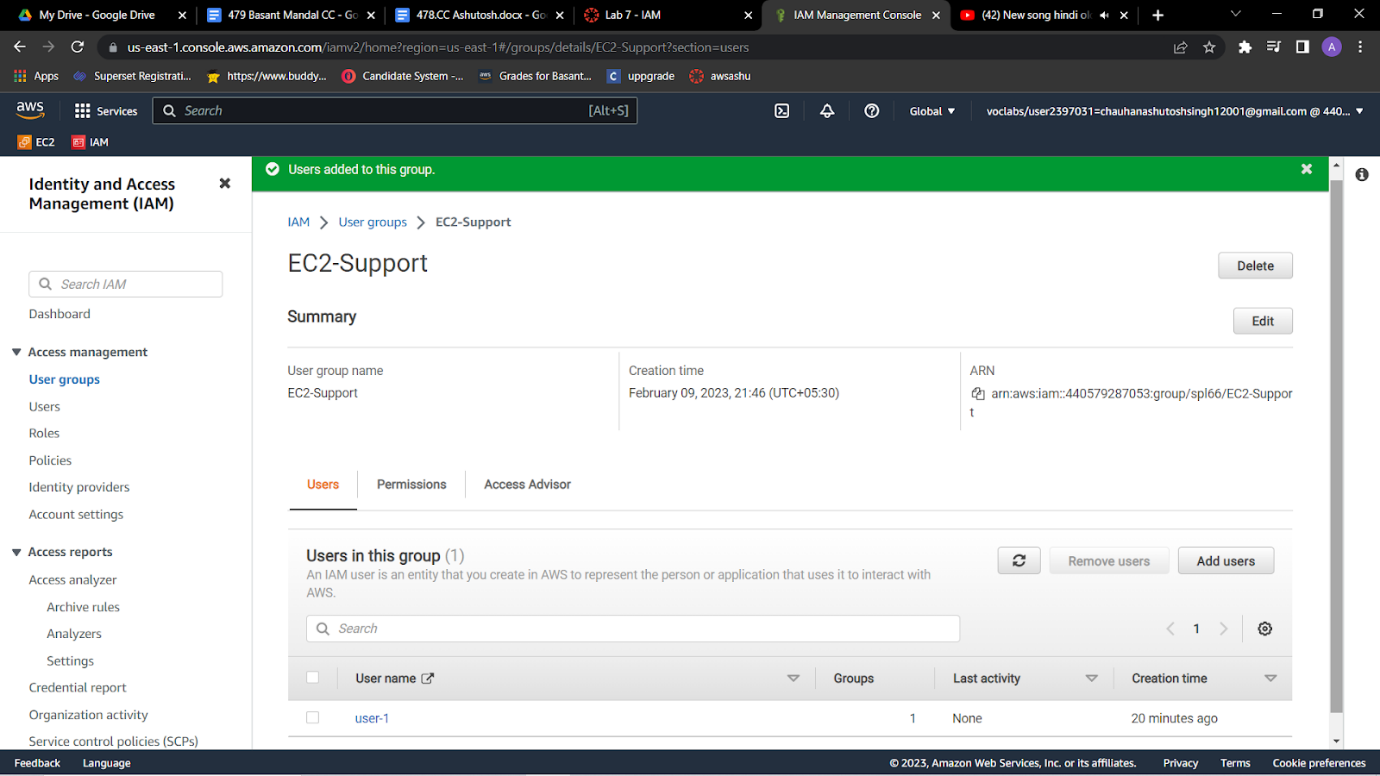
3.Choose the **Security credentials** tab.  
Notice that user-1 is assigned a **Console password**. This allows the user to access the AWS Management Console.

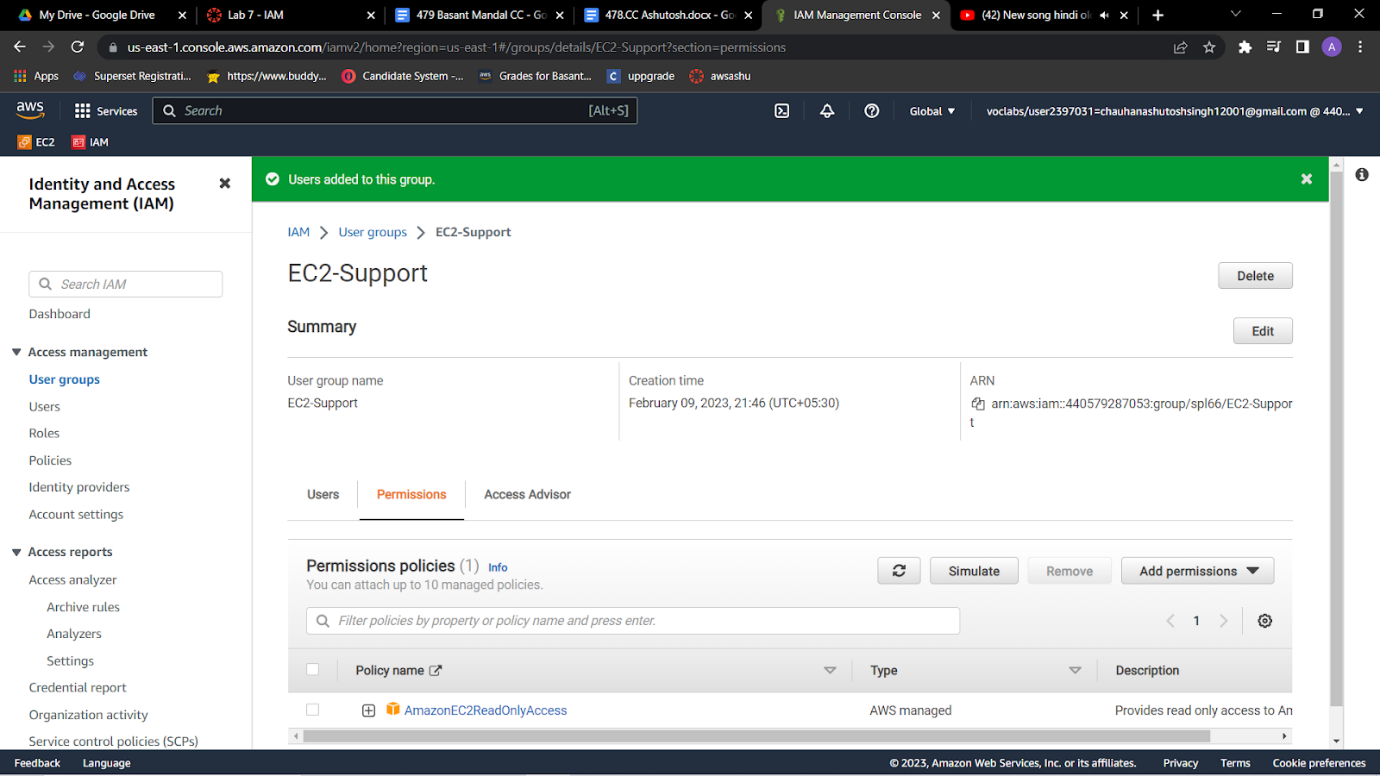


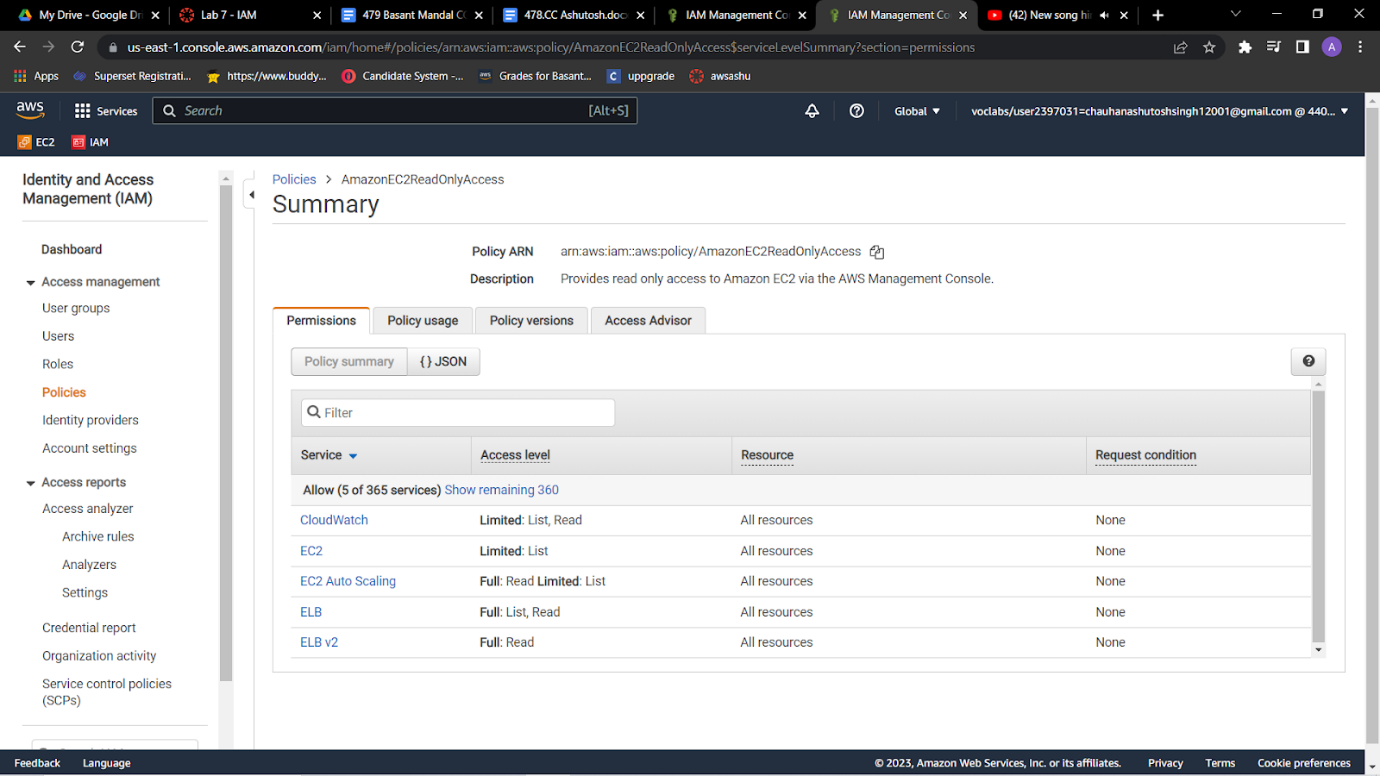
4.In the navigation pane on the left, choose **User groups**.The following groups have already been created for you:   EC2-Admin , EC2-Support , S3-Support



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



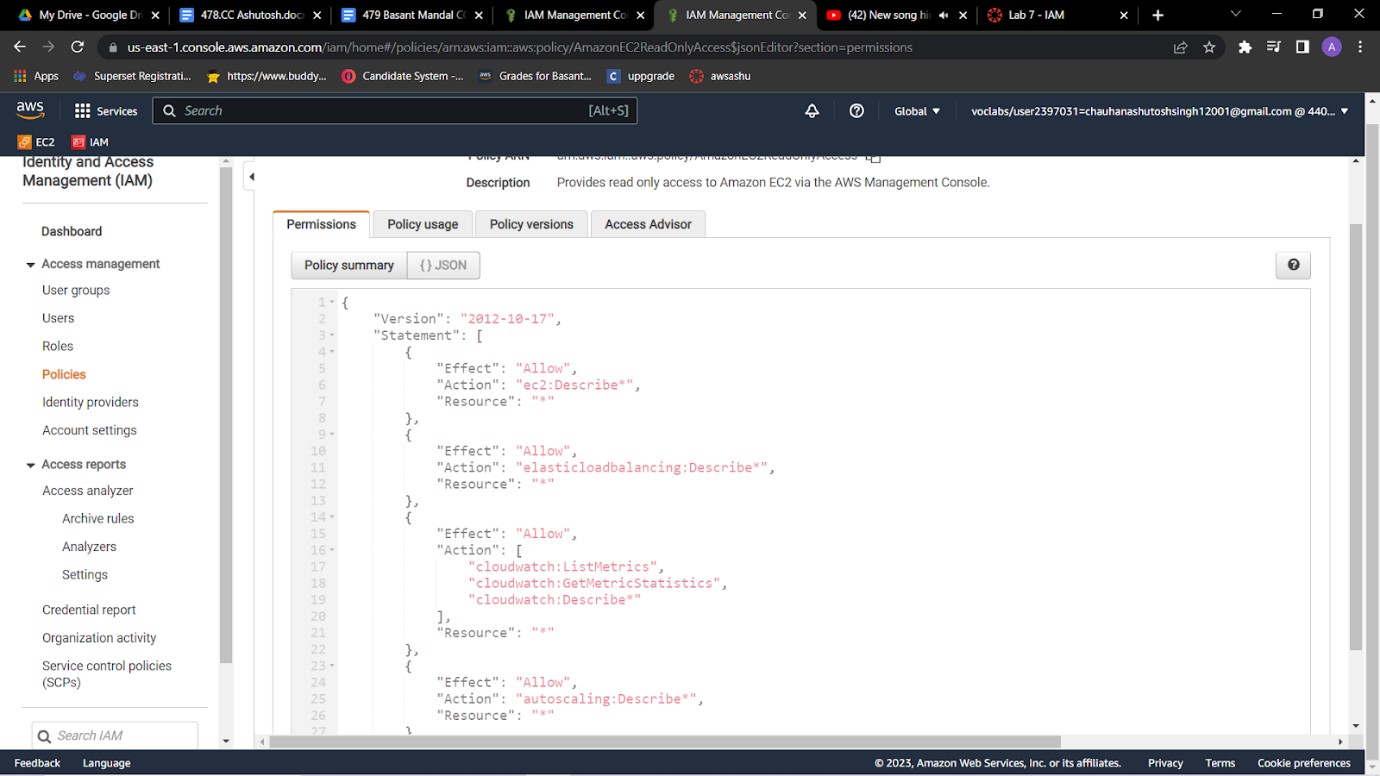
6.Choose the **Permissions** tab.  
This group has a managed policy called **AmazonEC2ReadOnlyAccess** associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the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

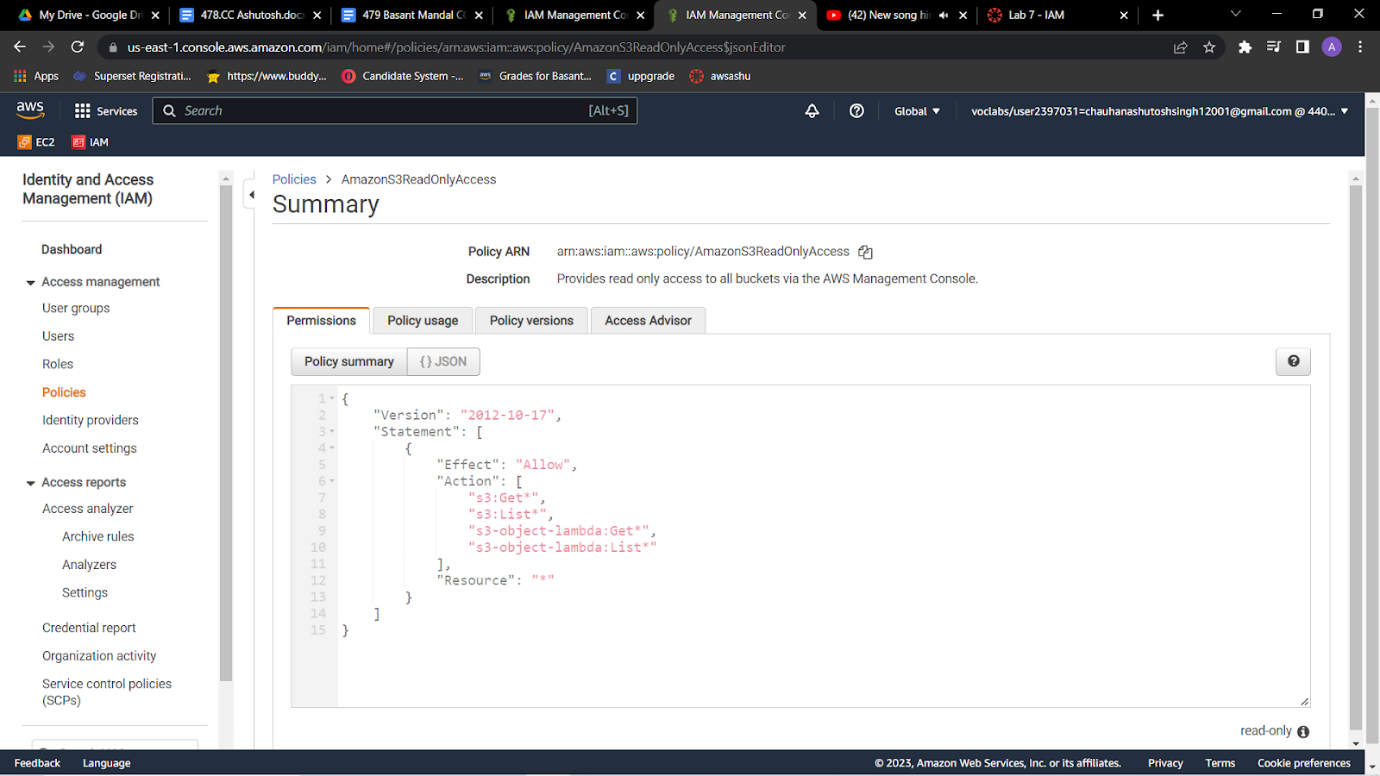
7.Choose the **{} JSON** tab.

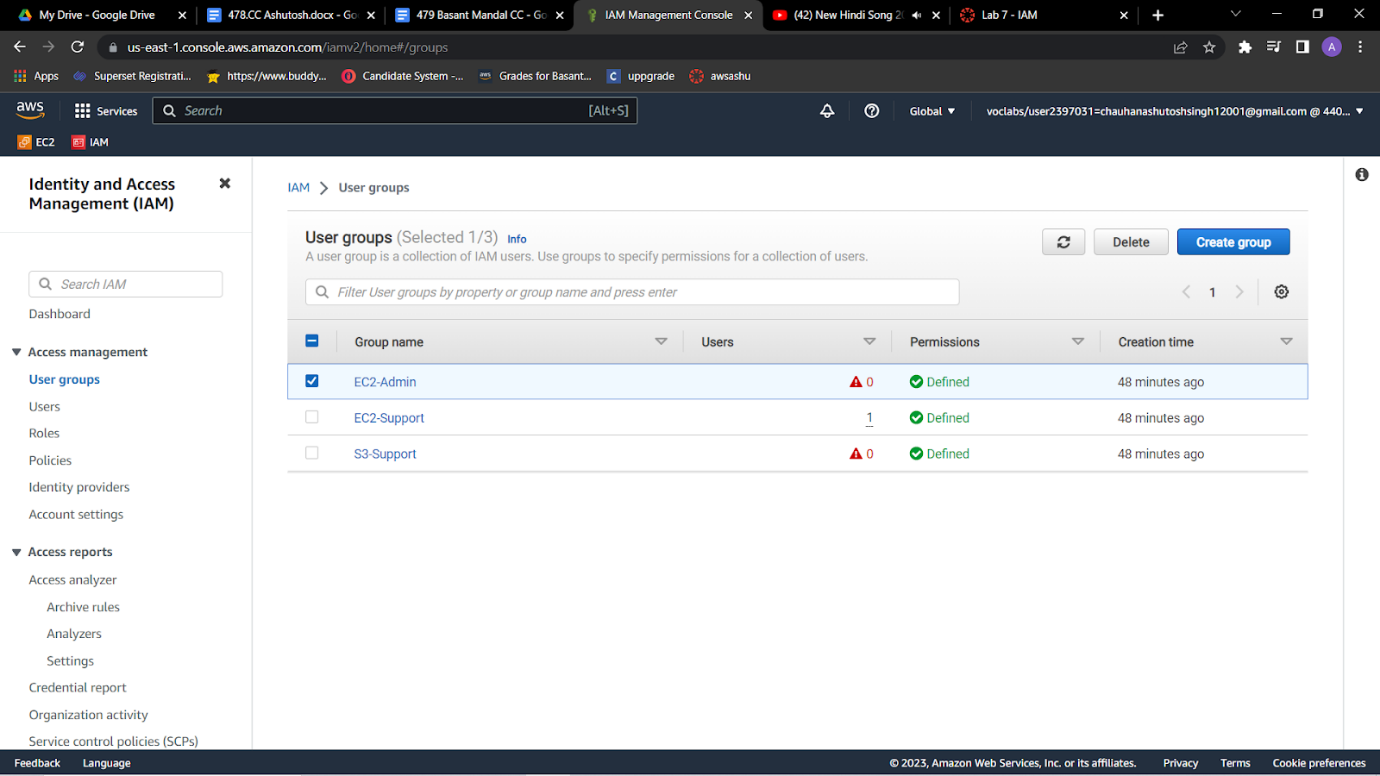
A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to *List* and *Describe* (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view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

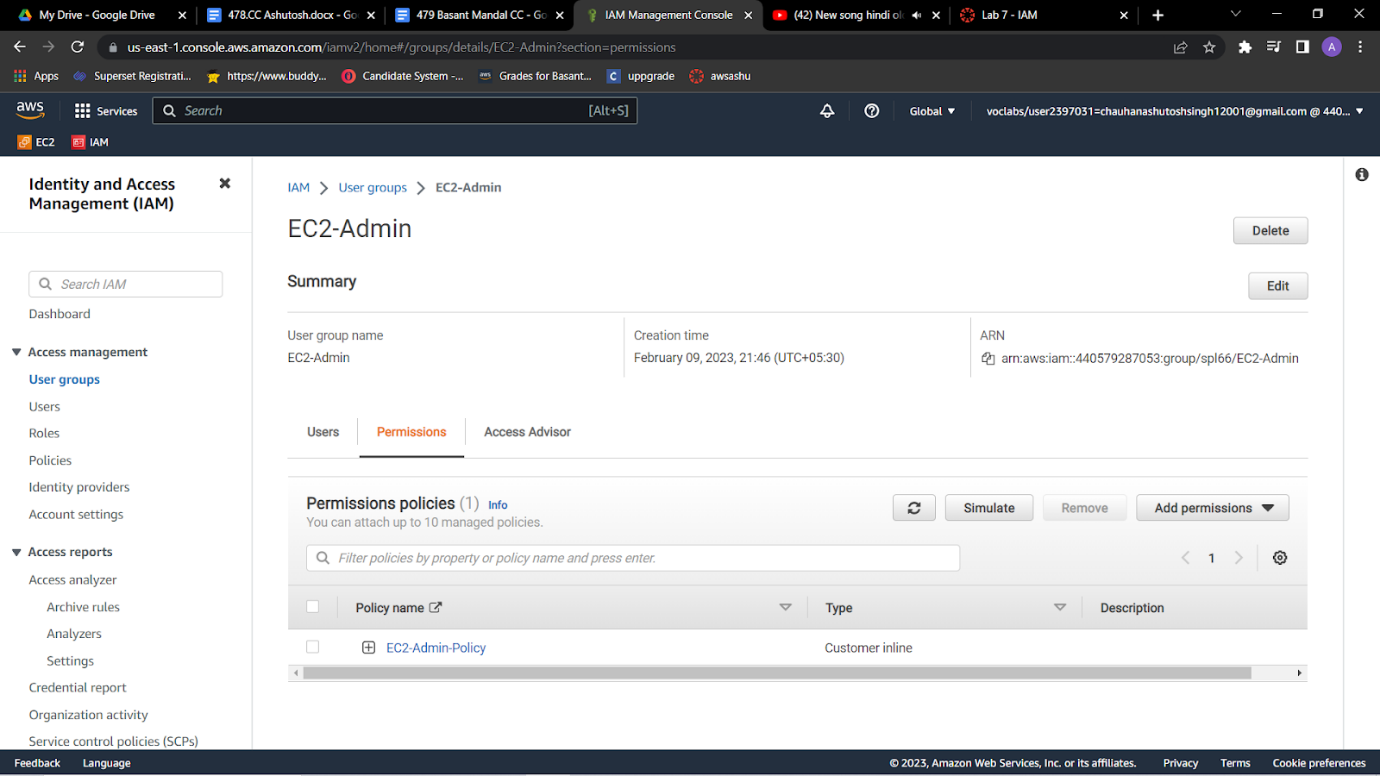
* Statements in an IAM policy have the following basic structure:
  + **Effect** says whether to *Allow* or *Deny* the permissions.
  + **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
  + **Resource** defines the scope of entities covered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

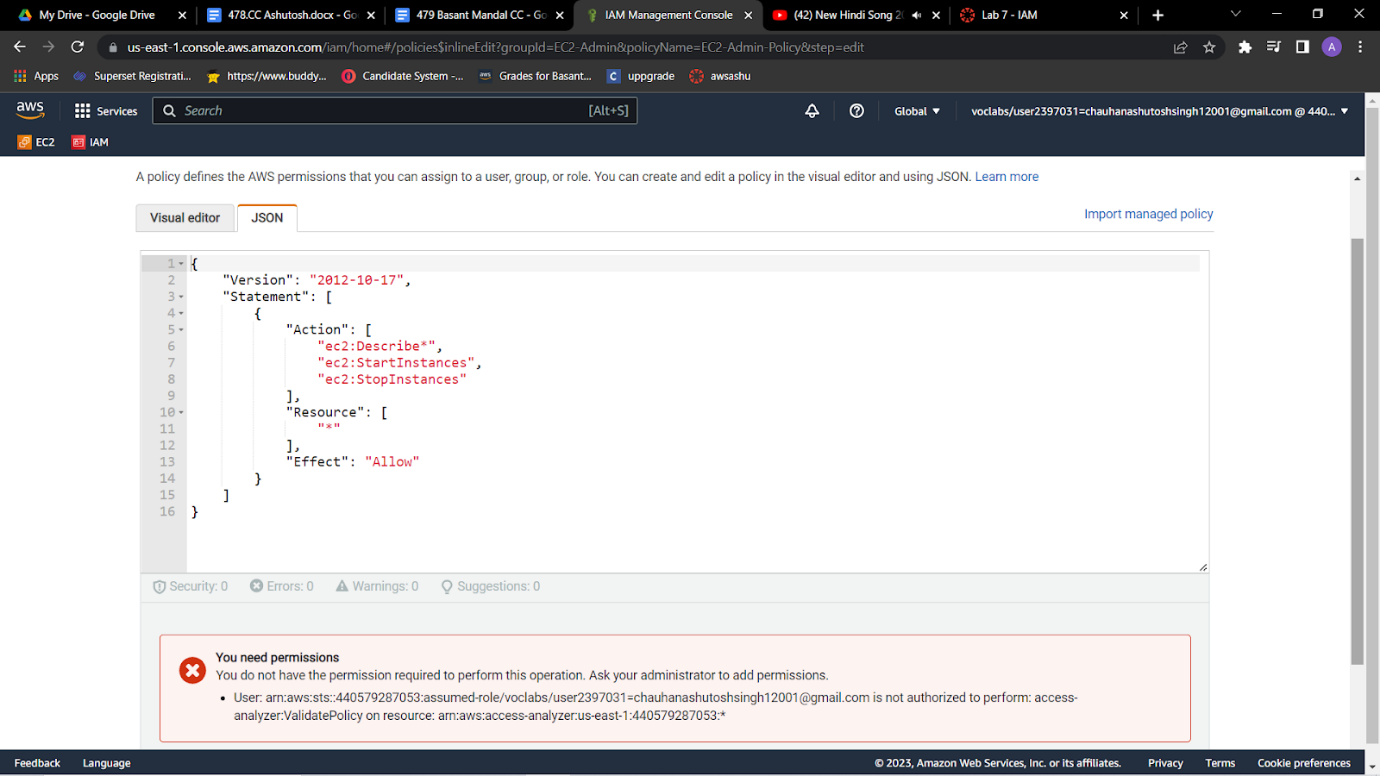


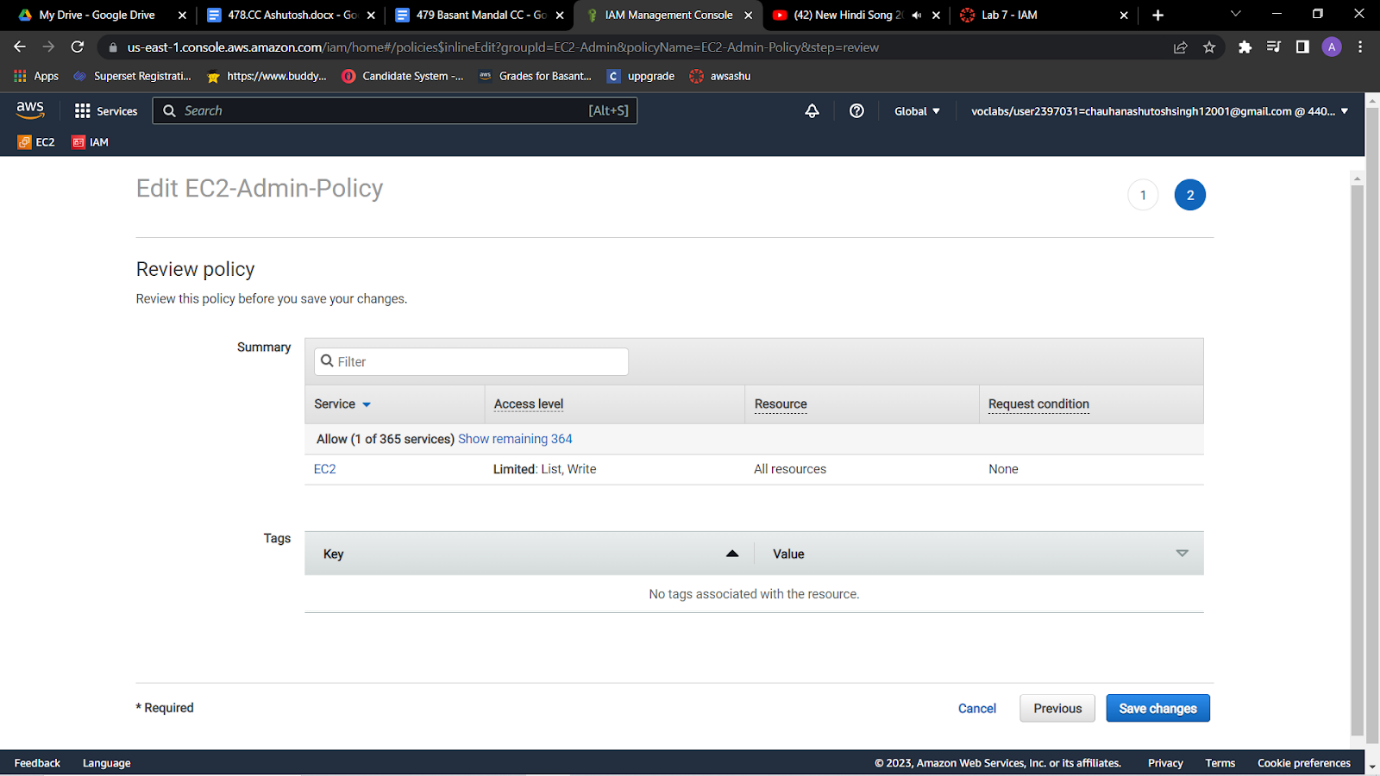
8.In the navigation pane on the left, choose **User groups**.Choose the name of the **S3-Support** group.Choose the **Permissions** tab.  
The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.    Under **Policy Name**, choose the link for the **AmazonS3ReadOnlyAccess** policy.Choose 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.

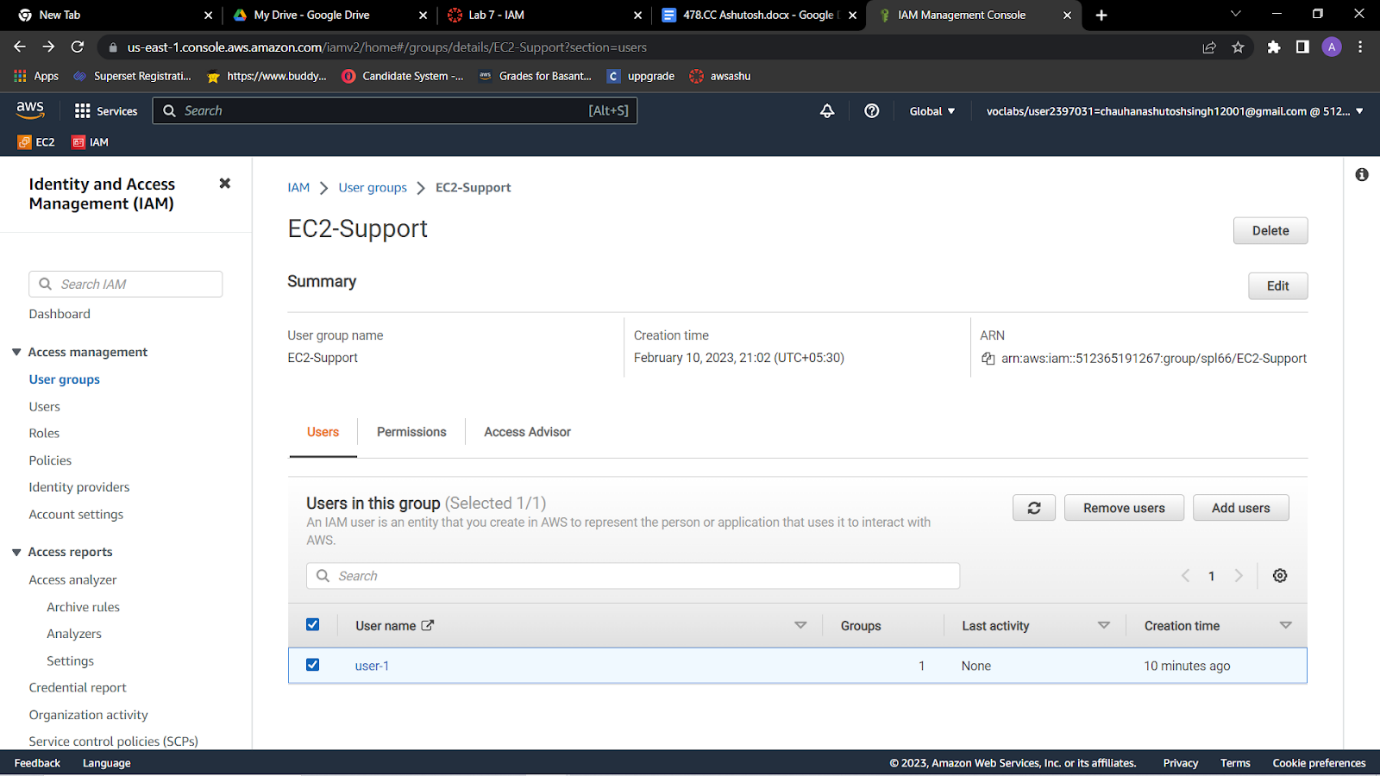
10.Choose the **Permissions** tab.  
This group is different from the other two. Instead of a managed policy, the group has an *inline policy*, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.

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. 



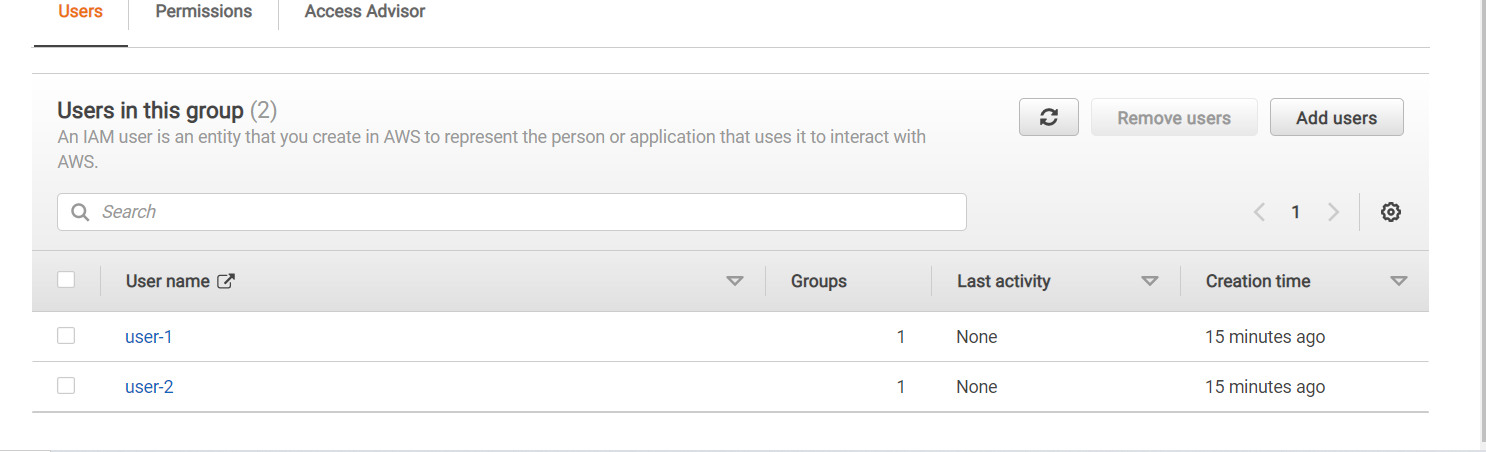
12.At the bottom of the screen, choose **Cancel** to close the policy.

**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.****

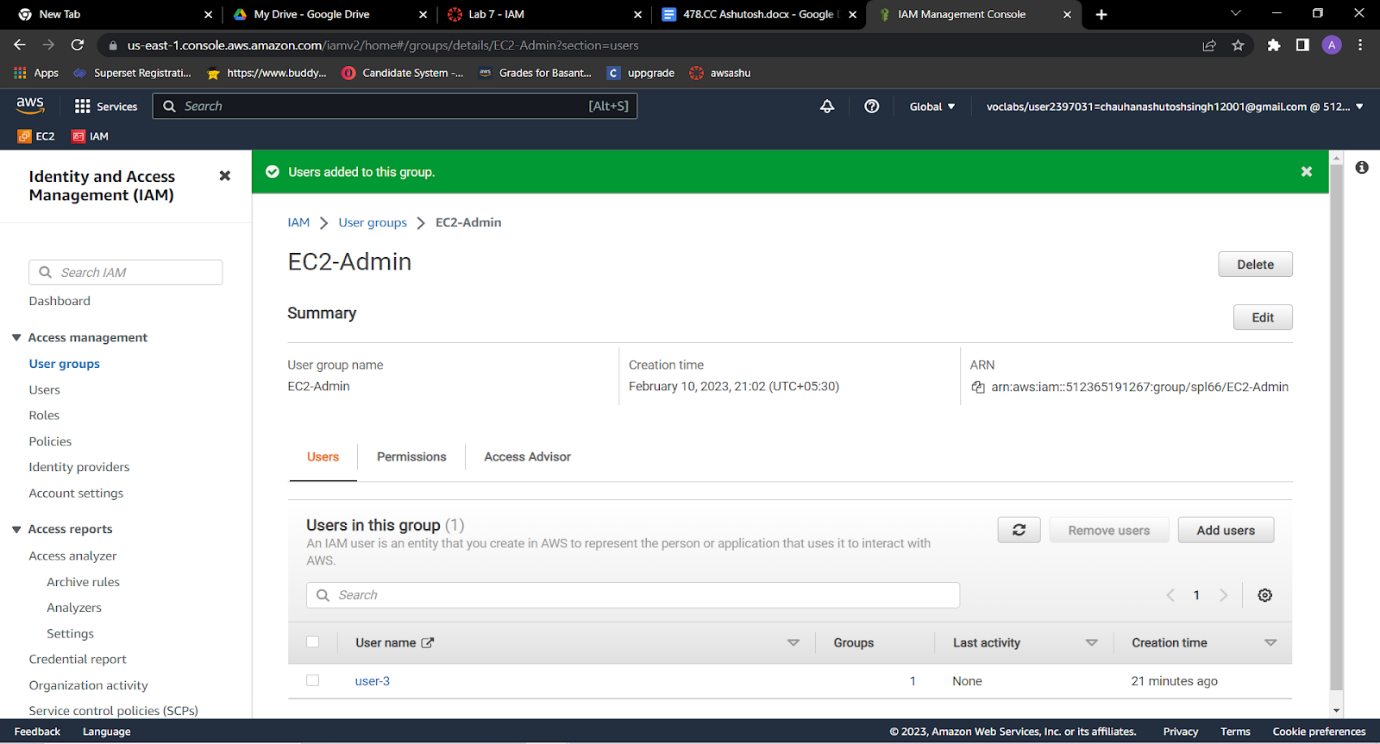
**Add user-2 to the EC2-Support group**

**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**

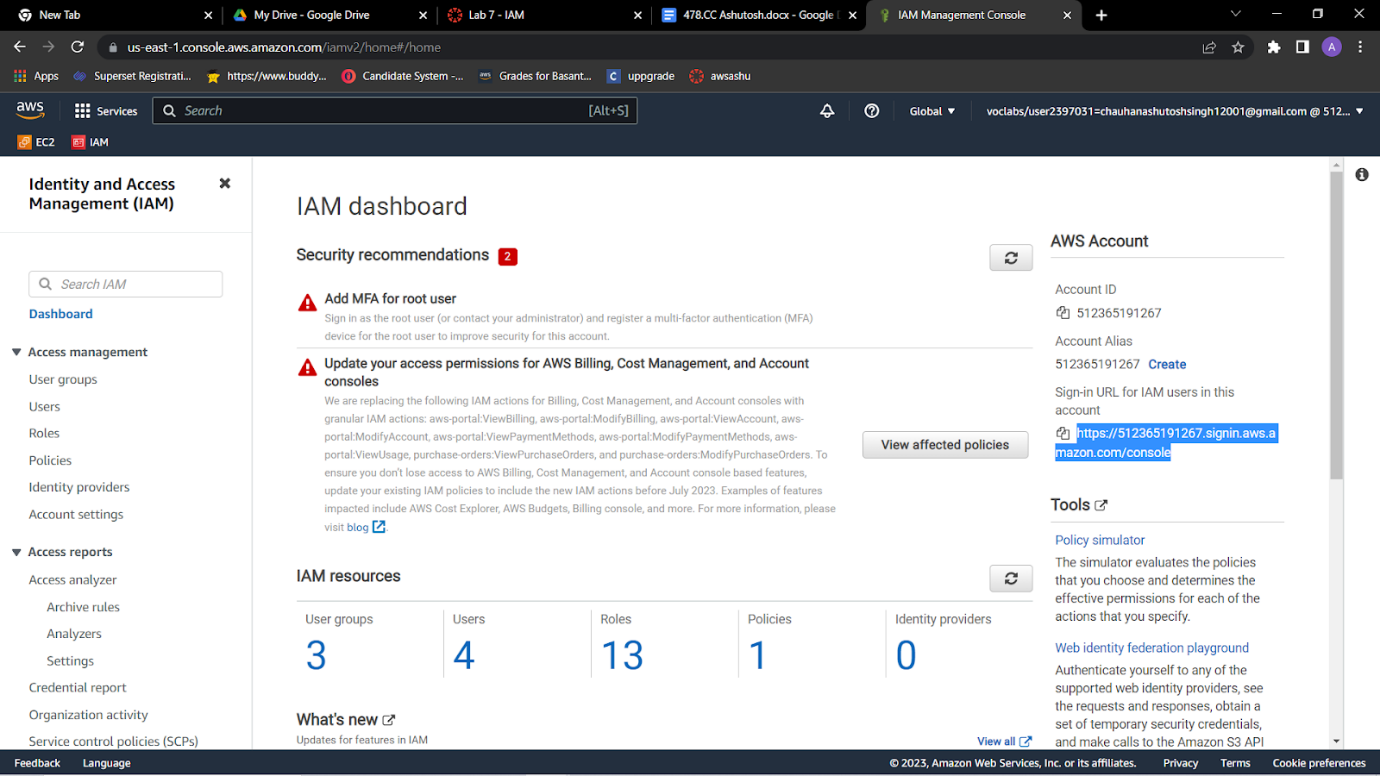
You have hired *user-3* as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the *EC2-Admin* group so that they inherit the necessary permissions via the attached *EC2-Admin-Policy*.

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**

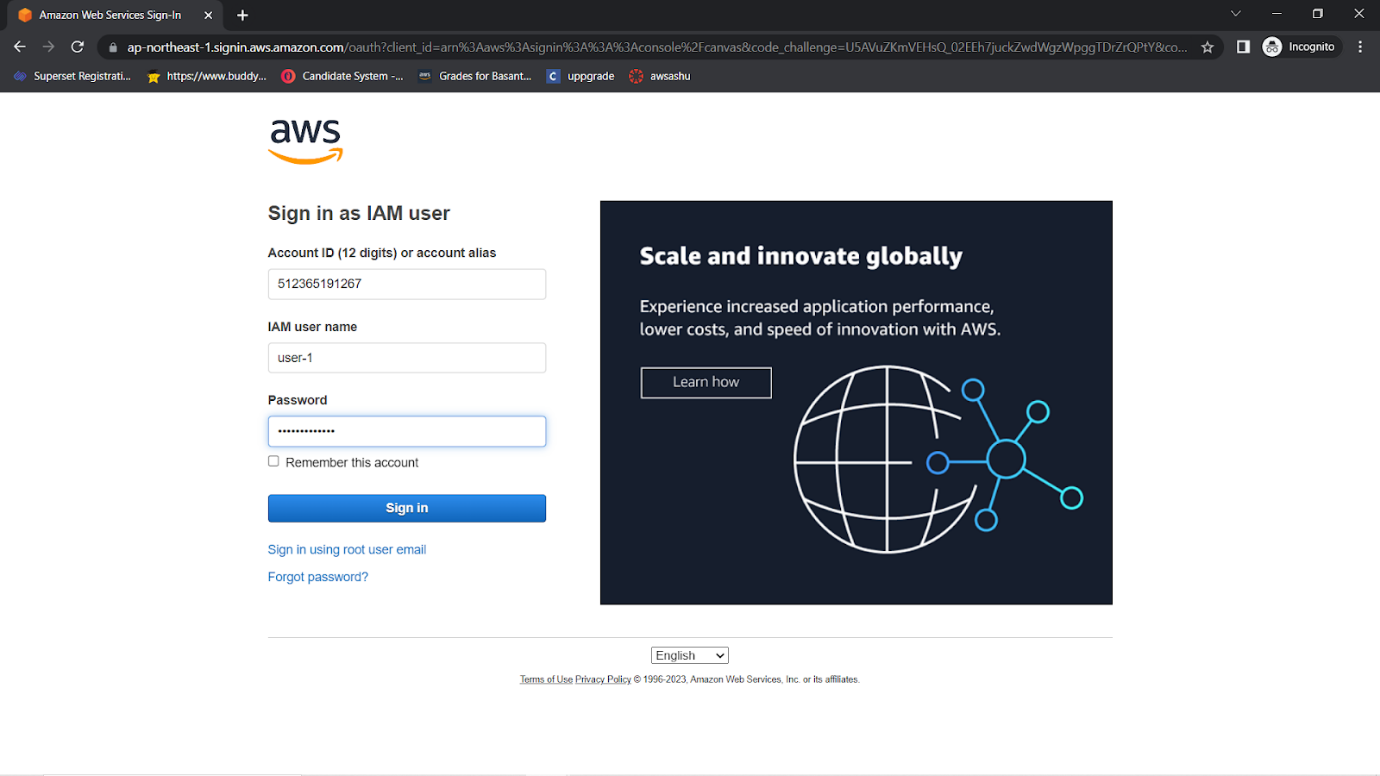
**Get the console sign-in URL**

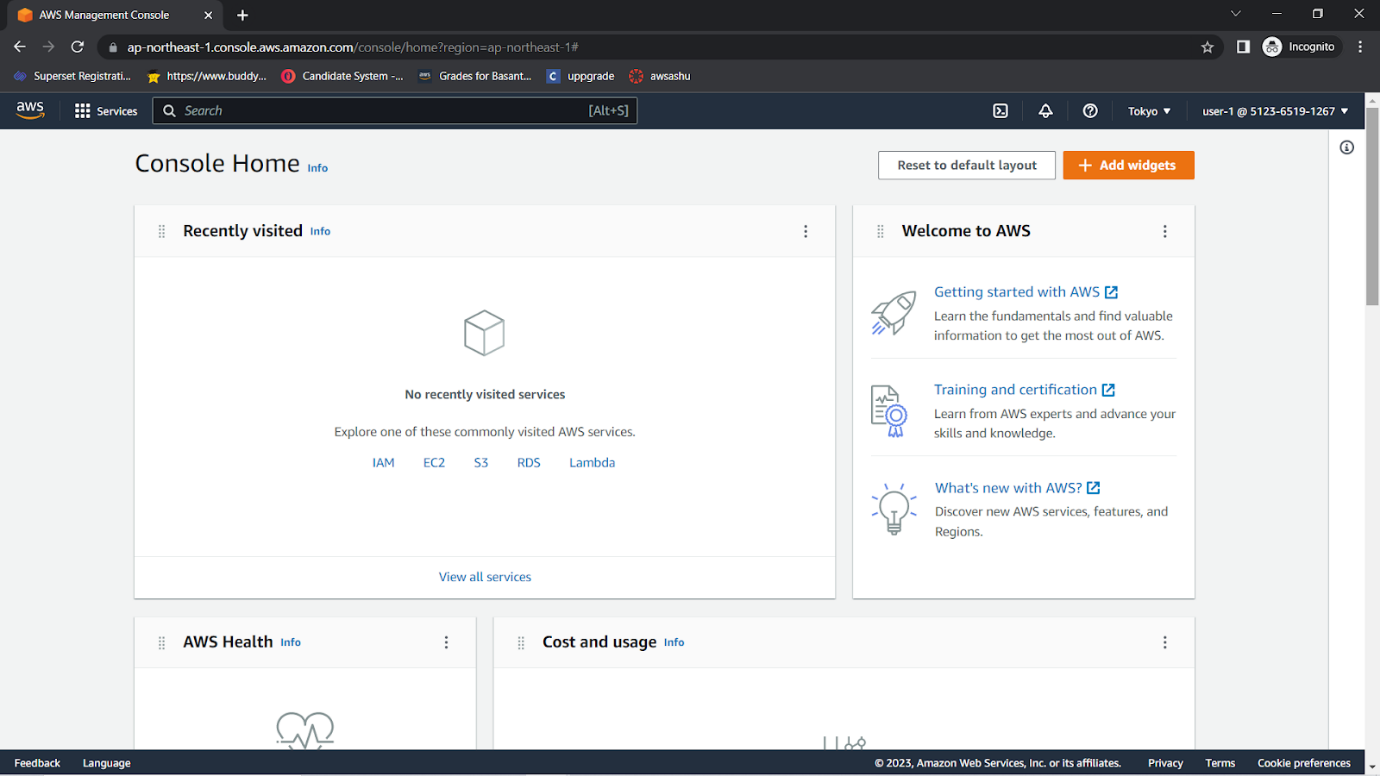
**16.**In the navigation pane on the left, choose Dashboard.Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: https://123456789012.signin.aws.amazon.com/console  
This link can be used to sign in to the AWS account that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

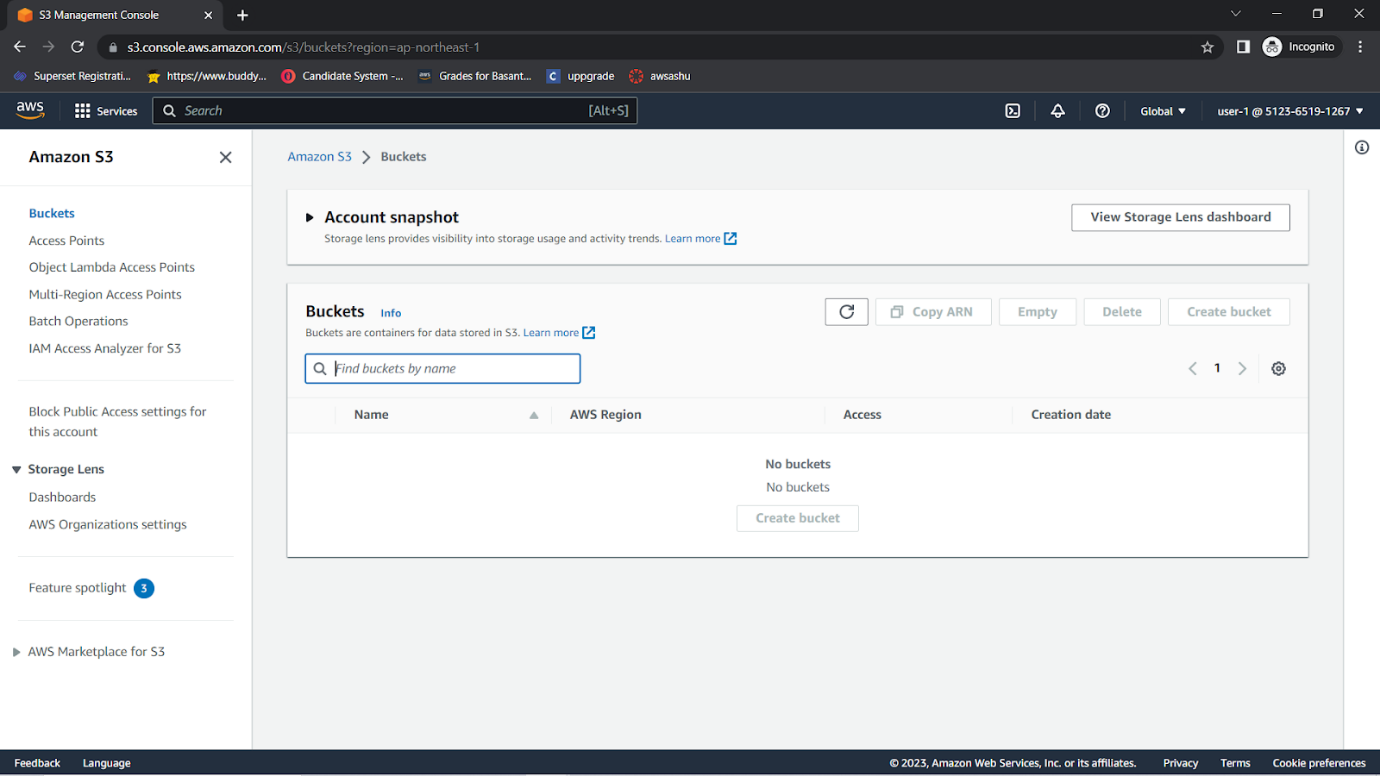


**Test user-1 permissions**

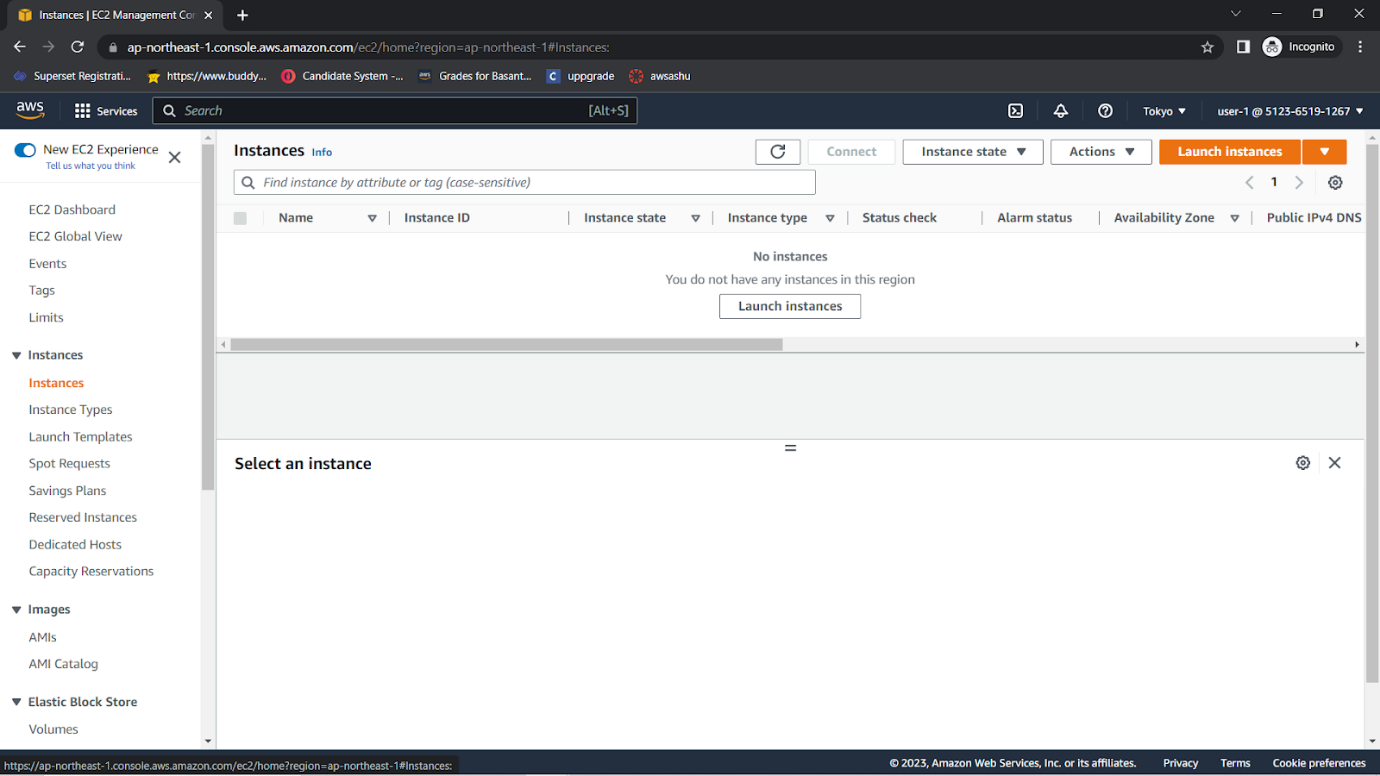
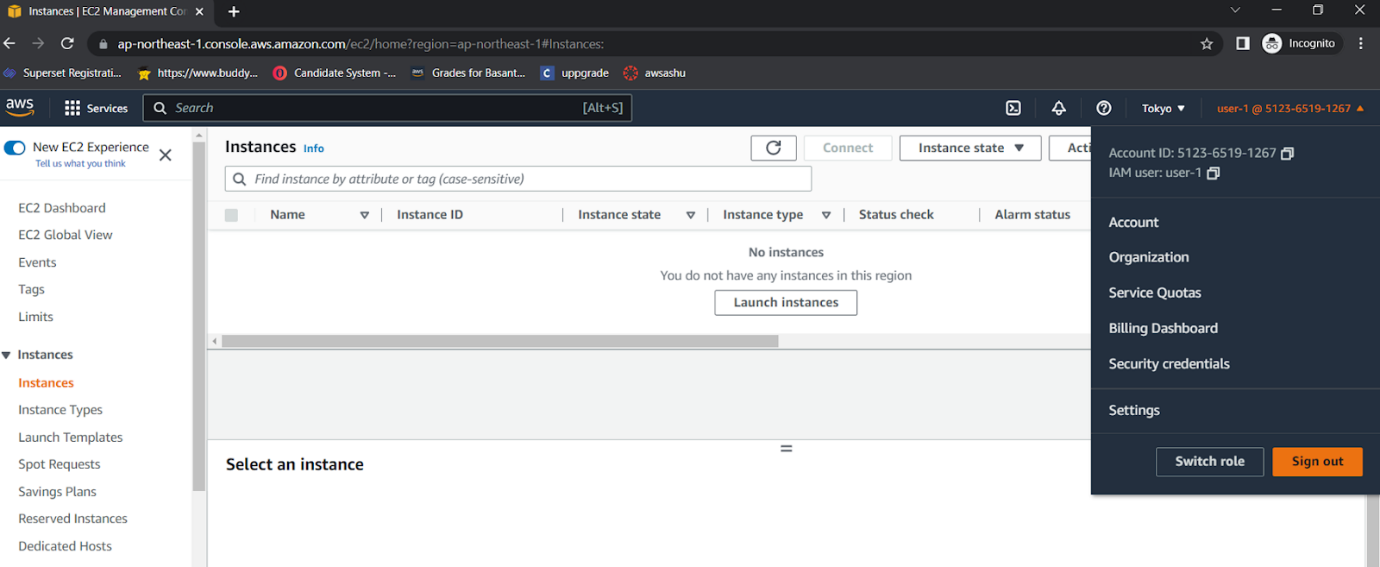
17.Open a private or incognito window in your browser.Paste the sign-in link into the private browser, and press ENTER.You will now sign-in as *user-1*, who has been hired as your Amazon S3 storage support staff.Sign in with the following credentials:**IAM user name:** user-1,**Password:** Lab-Password1

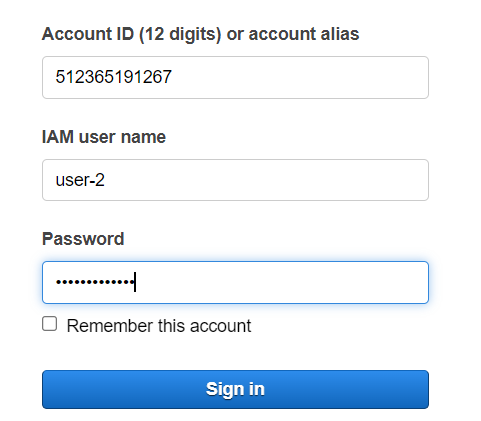




18.Choose the **Services** menu, and choose **S3**.Choose the name of one of your buckets, and browse the contents.Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.Now, test whether the user has access to Amazon EC2.

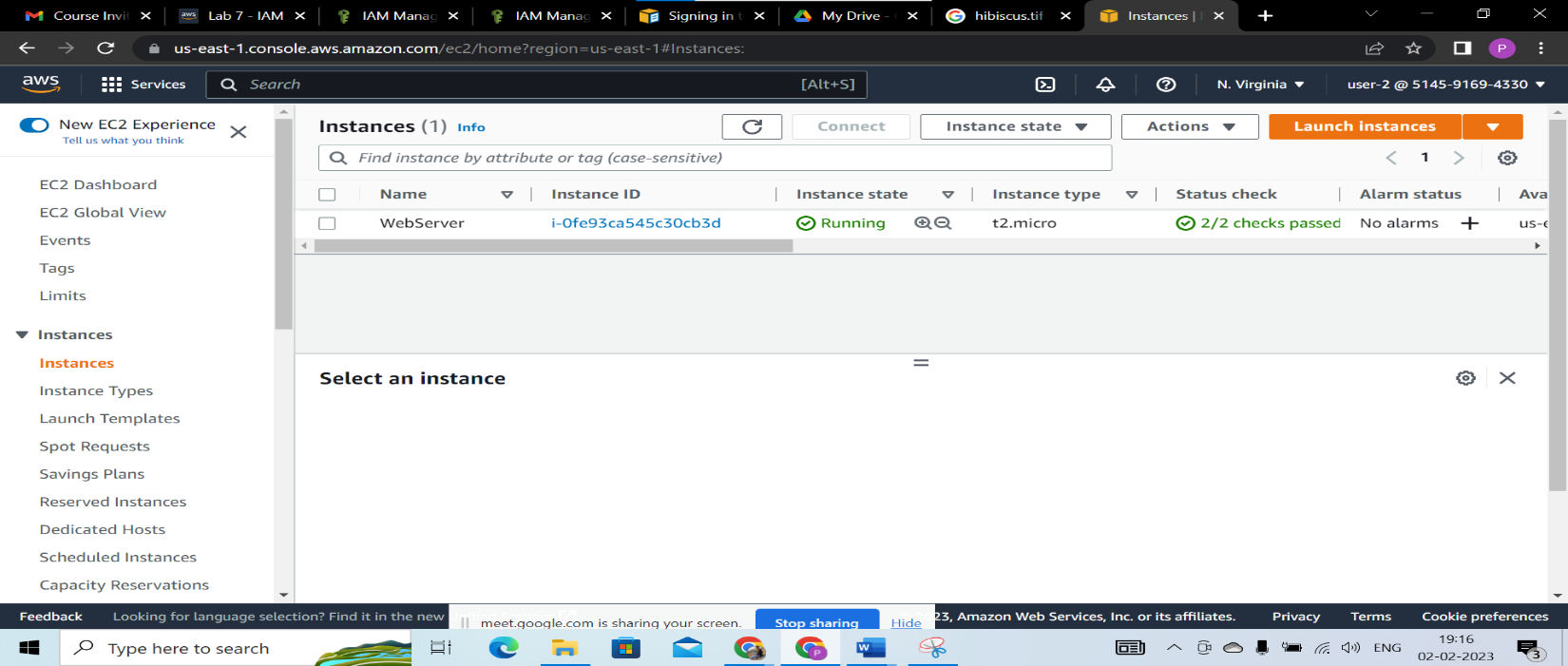
19.Choose the **Services** menu, and choose **EC2**.In the left navigation pane, choose **Instances**.You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2.You will now sign in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

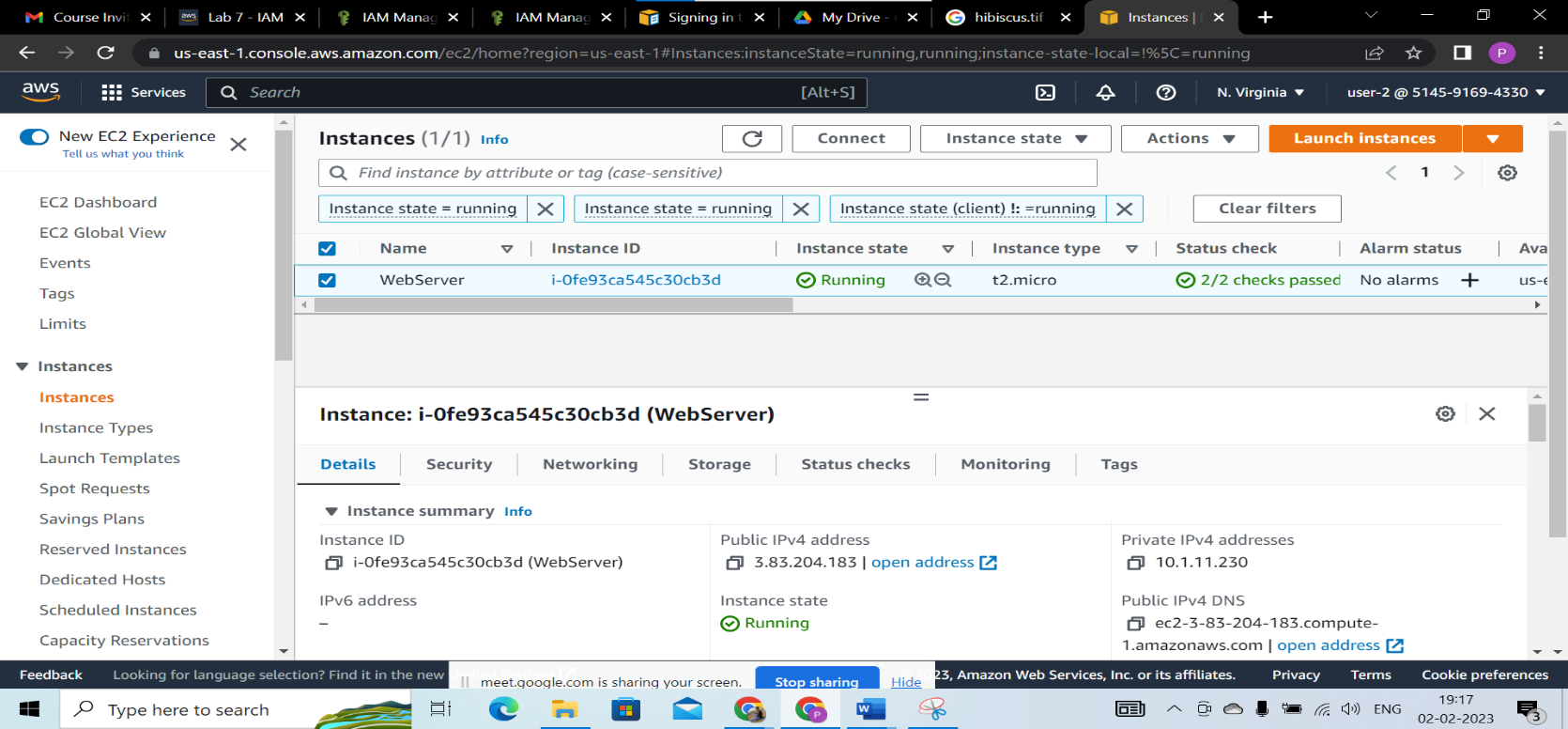
Sign Out

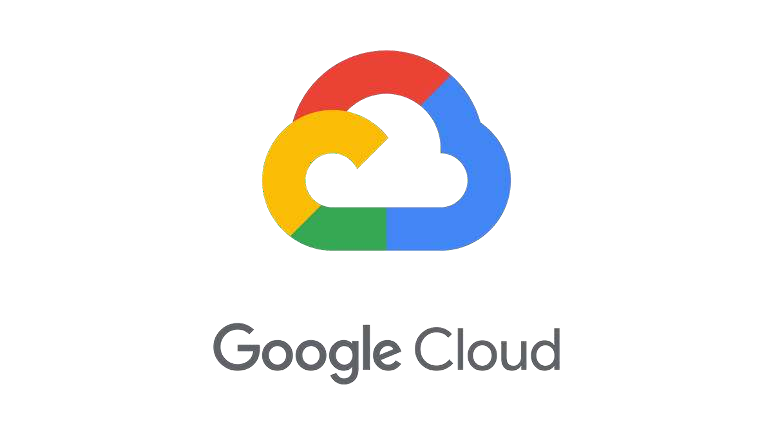
20.Paste the sign-in link into the private browser again, and press ENTER.Sign in with the following credentials:**IAM user name:** user-2  **Password:** Lab-Password2

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.







# Introduction

Google Cloud Platform, offered by Google, is a suite of cloud computing services that run on the same infrastructure that Google uses internally for its end-user products. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning.

# Google Cloud services

* + Artificial intelligence & Machine Learning
  + API management
  + Compute
  + Data Analytics
  + Databases
  + Developer Tools
  + Internet of Things (IoT)
  + Hybrid and multi-cloud
  + Management Tools
  + Media
  + Migration
  + Networking
  + Security
  + Storage

**Features of Google Cloud Platform**

* + Pricing
  + Hosting
  + Containers
  + Big Data
  + Andromeda
  + Load Balancing
  + Cloud Debugger
  + Cloud Trace
  + Maintenance
  + Cloud Save



# Introduction

Azure is a cloud computing platform which was launched by Microsoft in February 2010. It is an open and flexible cloud platform which helps in development, data storage, service hosting, and service management. The Azure tool hosts web applications over the internet with the help of Microsoft data centers.

# Types of Azure Clouds

1. PAAS
2. SAAS
3. IASS

### Azure as PaaS

PaaS is a computing platform which includes an operating system, programming language execution environment, database or web services. This Azure service is used by developers and application providers.

### Azure As SaaS

SaaS (Software as a Service) is software which is centrally hosted and managed. It is a single version of the application is used for all customers. You can scale out to multiple instances. This helps you to ensure the best performance in all locations. The software is licensed through a monthly or annual subscription.

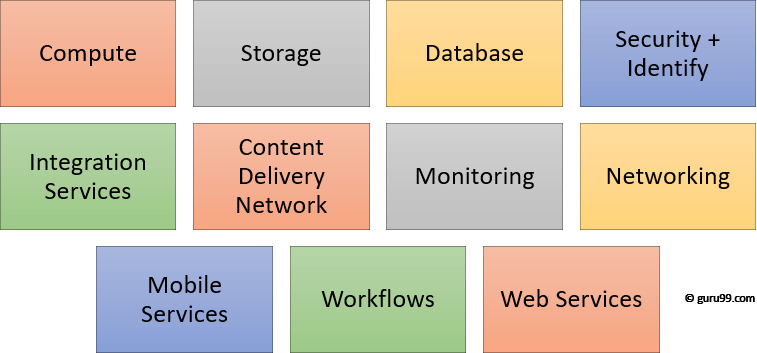
MS Exchange, Office, Dynamics are offered as a SaaS

**SUB: CLOUD COMPUTING**

### Azure as IaaS

IaaS(Infrastructure as a Service) is the foundational cloud platform layer. This Azure service is used by IT administrators for processing, storage, networks or any other fundamental computer operations. It is one of the Azure topics to learn that allows users to run arbitrary software.

**Azure Services**



* + Compute
  + Storage
  + Database
  + Content Delivery Network
  + Security + Identify sevices
  + Enterprise Integration Services:
  + Monitoring + Management Services
  + Azure Networking
  + Web and Mobile Services:
  + Workflows in the cloud
  + Migration

# Applications of Azure

* + Infrastructure Services
  + Mobile Apps
  + Web Applications
  + Cloud Services
  + Storage, Backup, and Recovery
  + Data Management
  + Media Services

# Advantages of Azure

* + Azure infrastructure will cost-effectively enhance your business continuity strategy
  + It allows you to access the application without buying a license for the individual machine
  + Windows Azure offers the best solution for your data needs, from SQL database to blobs to tables
  + Offers scalability, flexibility, and cost-effectiveness
  + Helps you to maintain consistency across clouds with familiar tools and resources
  + Helps you to scale your IT resources up and down based on your needs
  + You will not require processing power or hard disk space if you are using Azure
  + Cloud computing offers virtually limitless storage
  + Sharing documents leads directly to better collaboration

# Disadvantages of Azure

* + Cloud computing is not possible if you can't connect to the Internet
  + Azure is a web-based application which requires a lot of bandwidth to download, as do large documents
  + Web-based applications can sometimes be slower compared to accessing a similar software program on your desktop PC