**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**

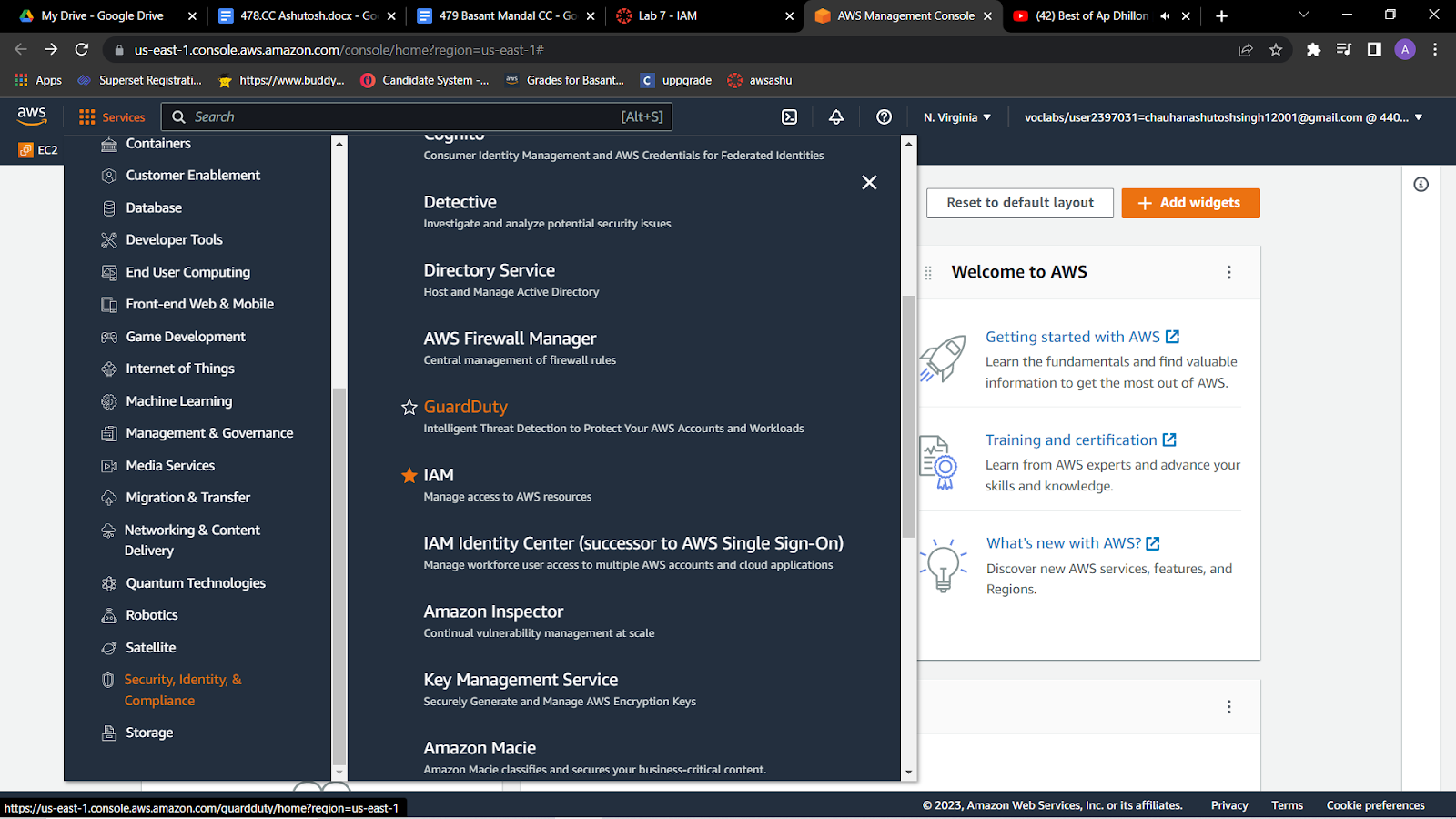
You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

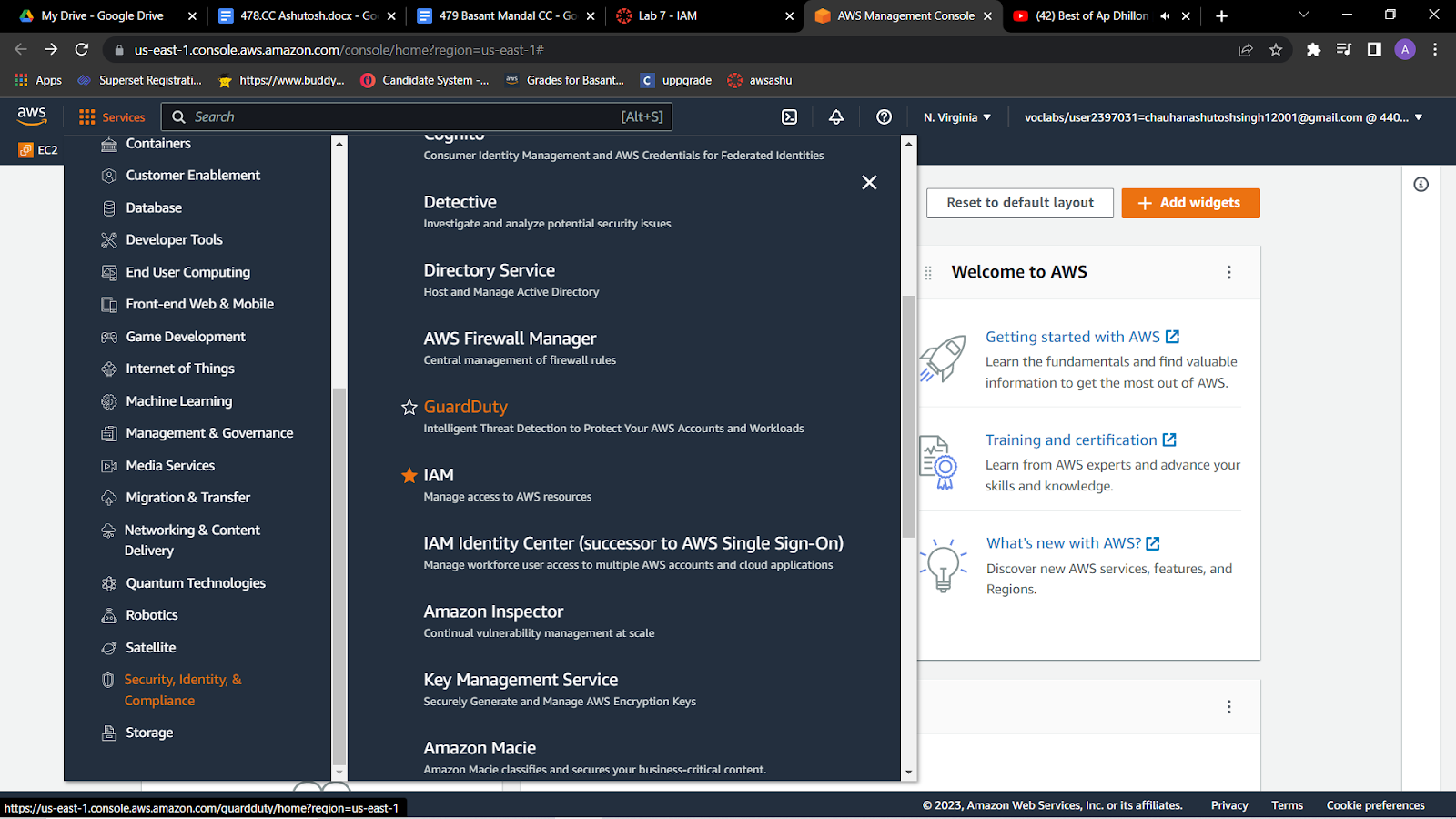
5. **Free to use**

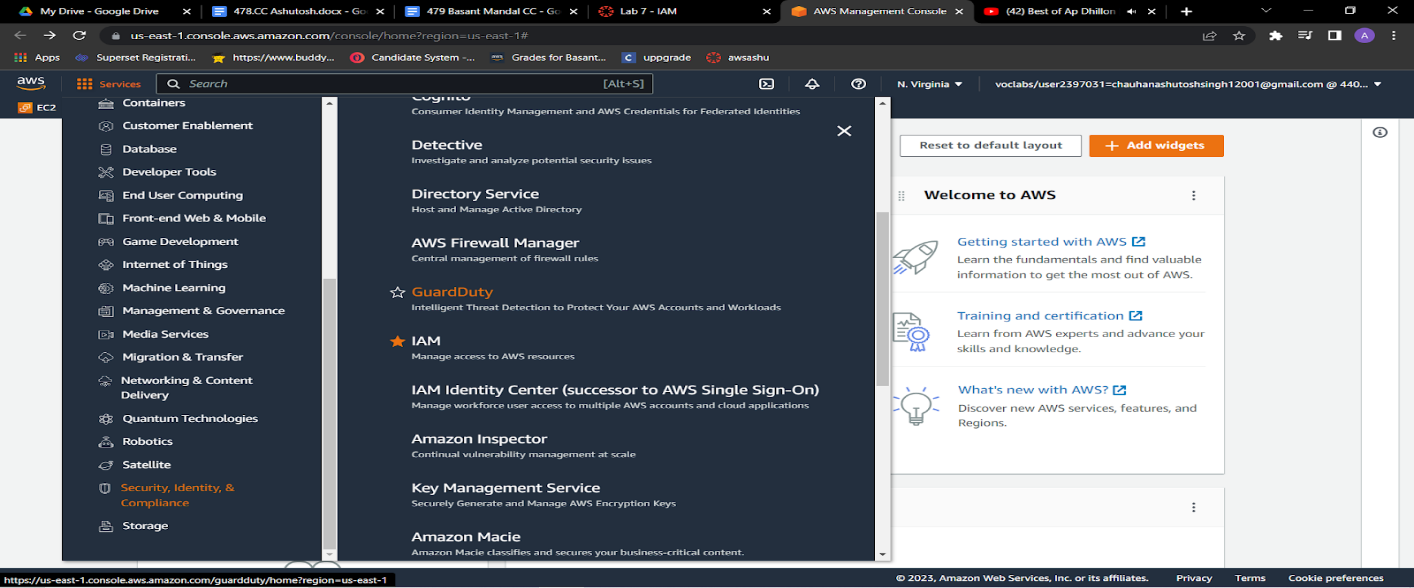
AWS Identity and Access Management (IAM) and AWS Security Token Service (AWS STS) are features of your AWS account offered at no additional charge. You are charged only when you access other AWS services using your IAM users or AWS STS temporary security credentials

Steps:

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

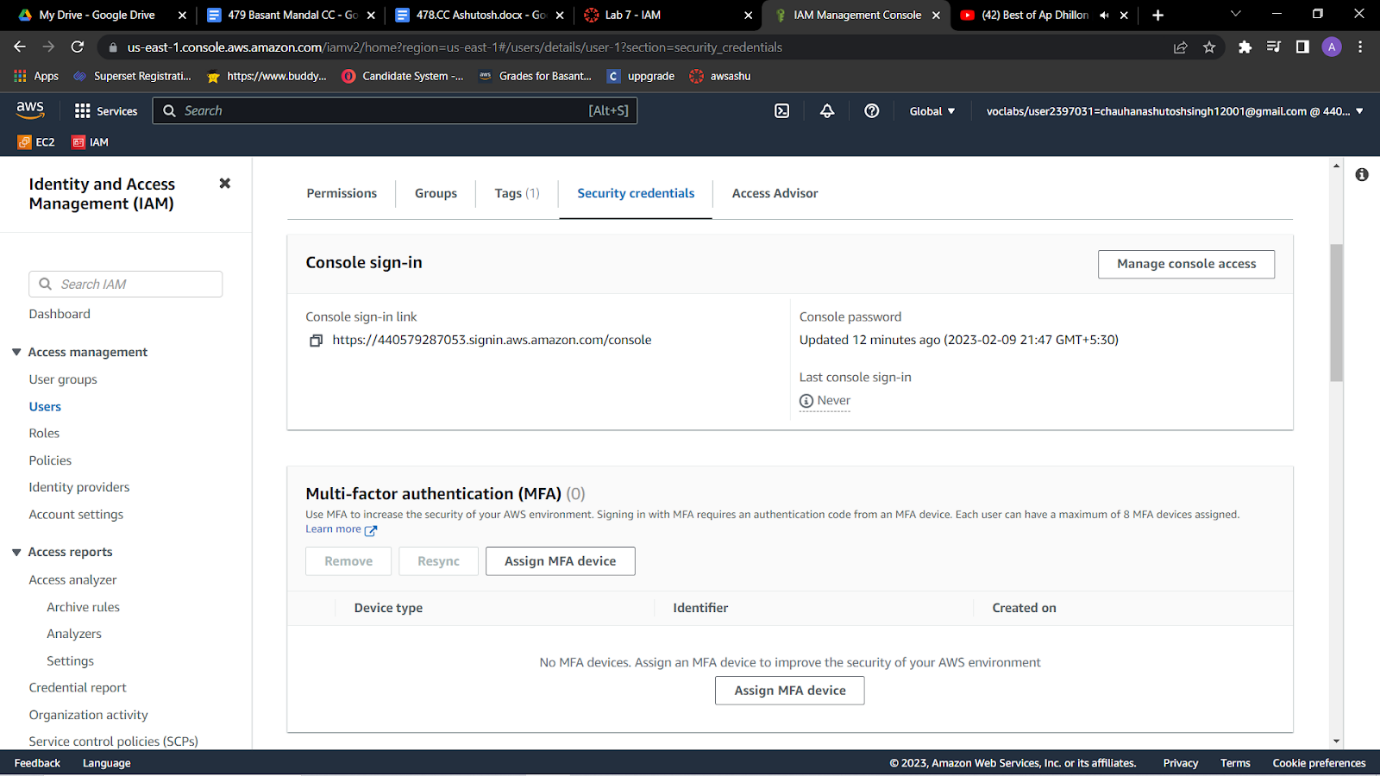




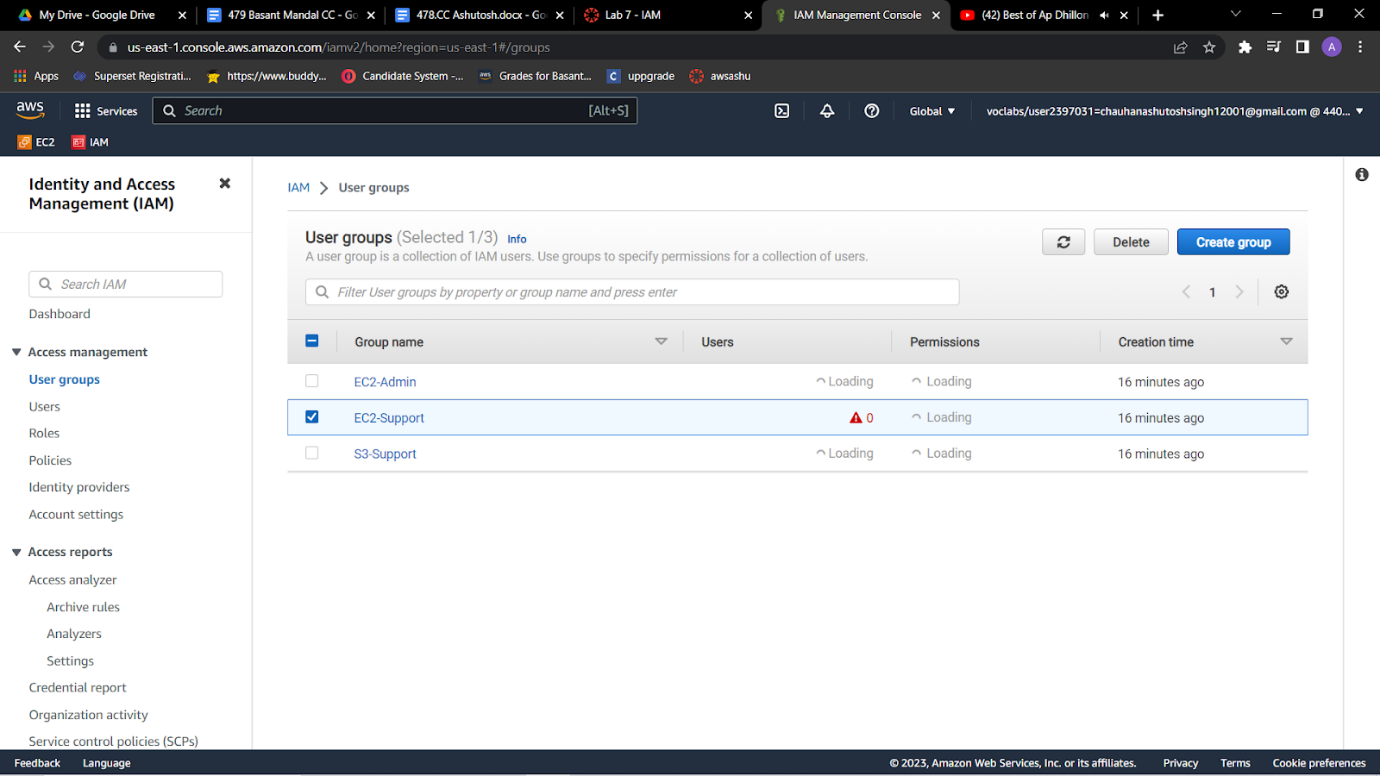


2.In the navigation pane on the left, choose **Users**.Create Users

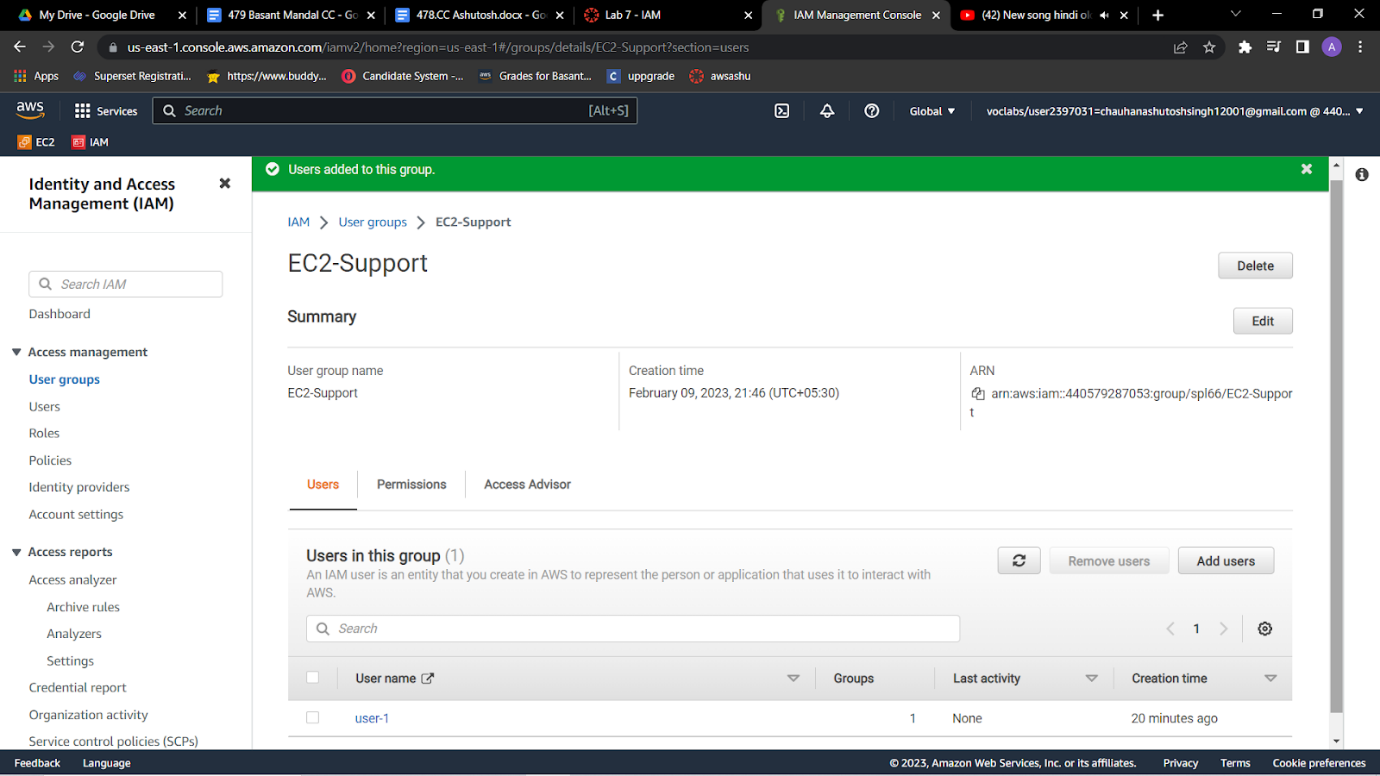
3.Choose the **Security credentials** tab.  
Notice that user-1 is assigned a **Console password**. This allows the user to access the AWS Management Console.

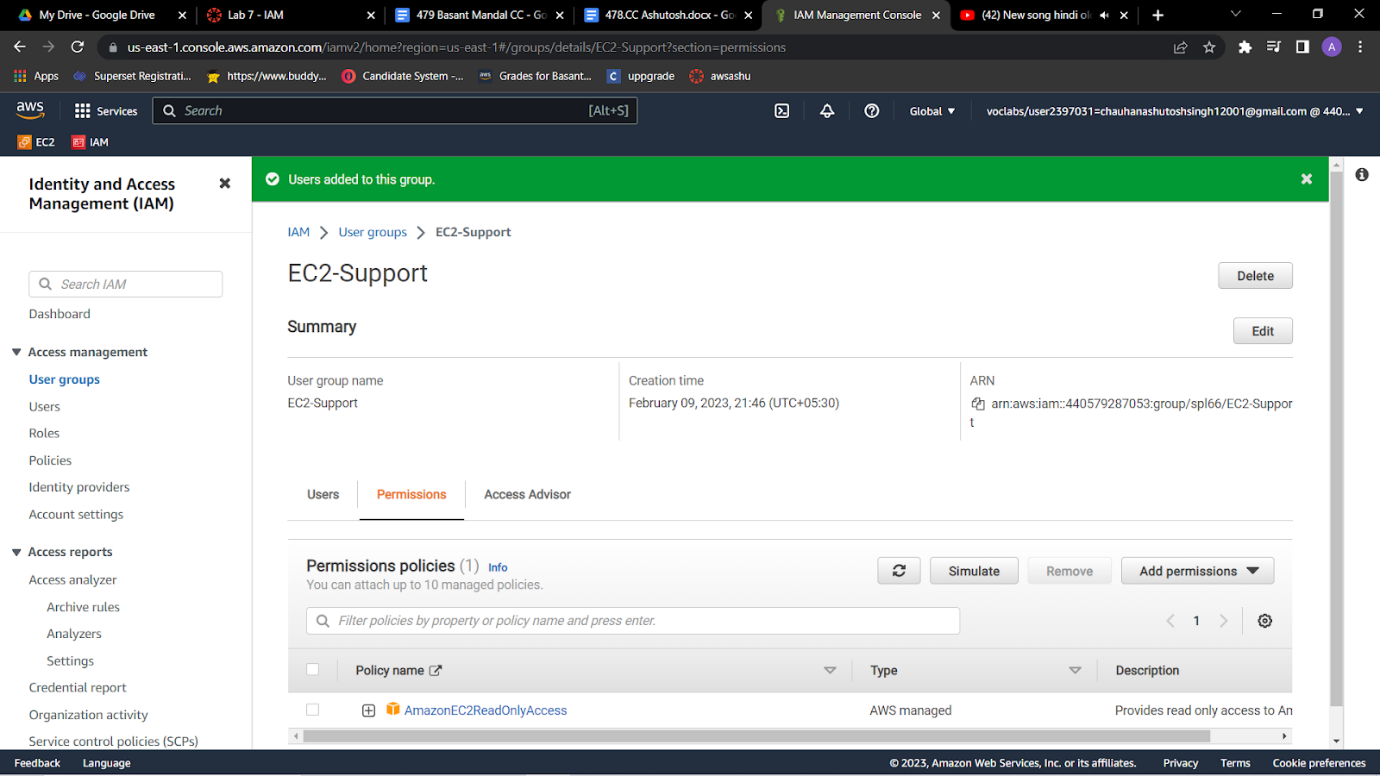


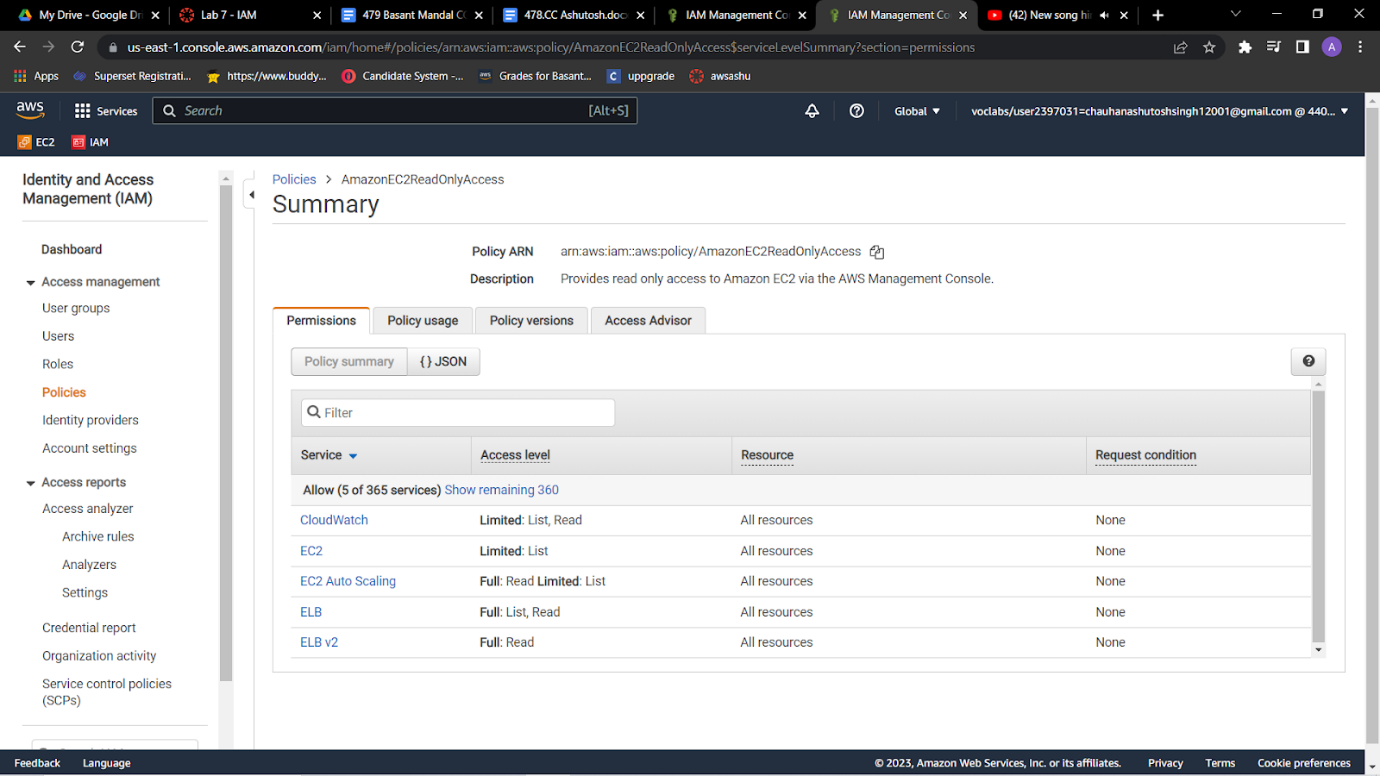
4.In the navigation pane on the left, choose **User groups**.The following groups have already been created for you:   EC2-Admin , EC2-Support , S3-Support



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



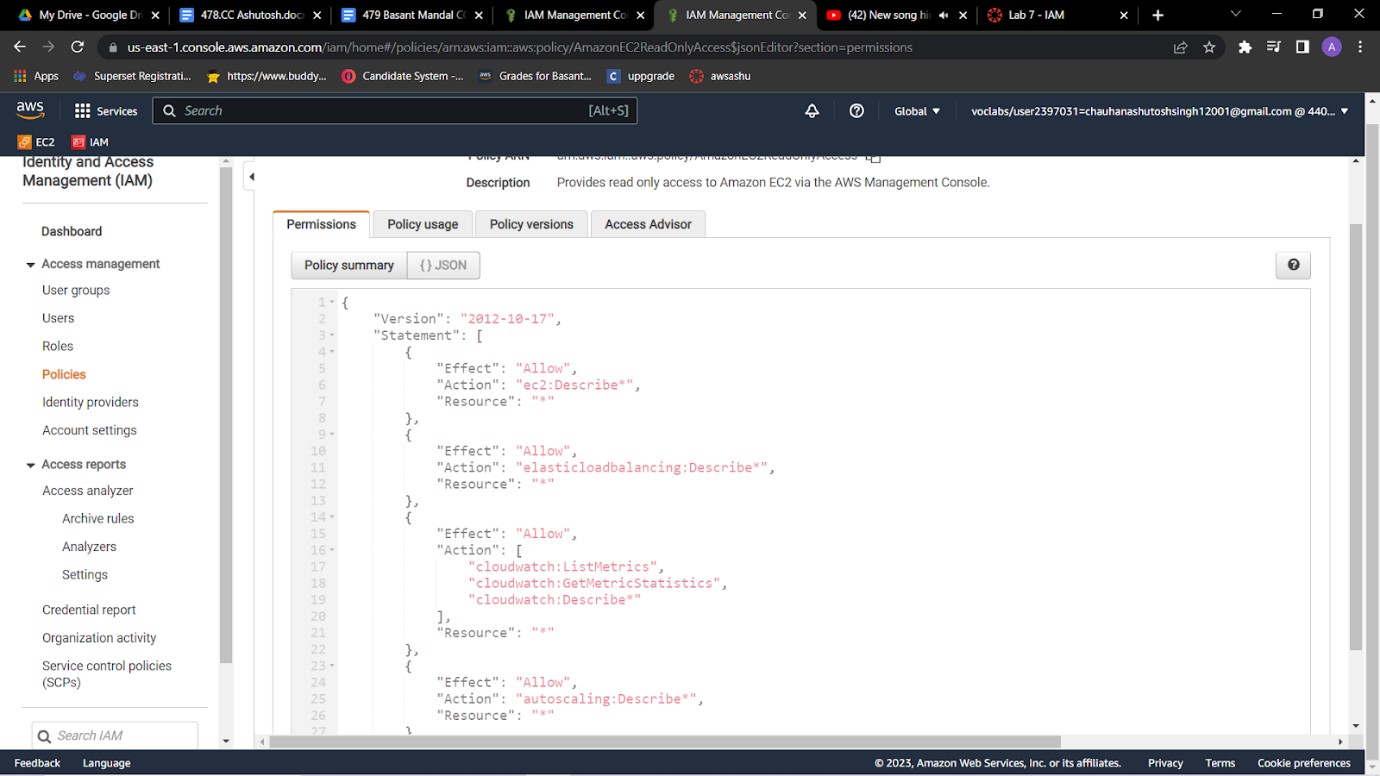
6.Choose the **Permissions** tab.  
This group has a managed policy called **AmazonEC2ReadOnlyAccess** associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the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

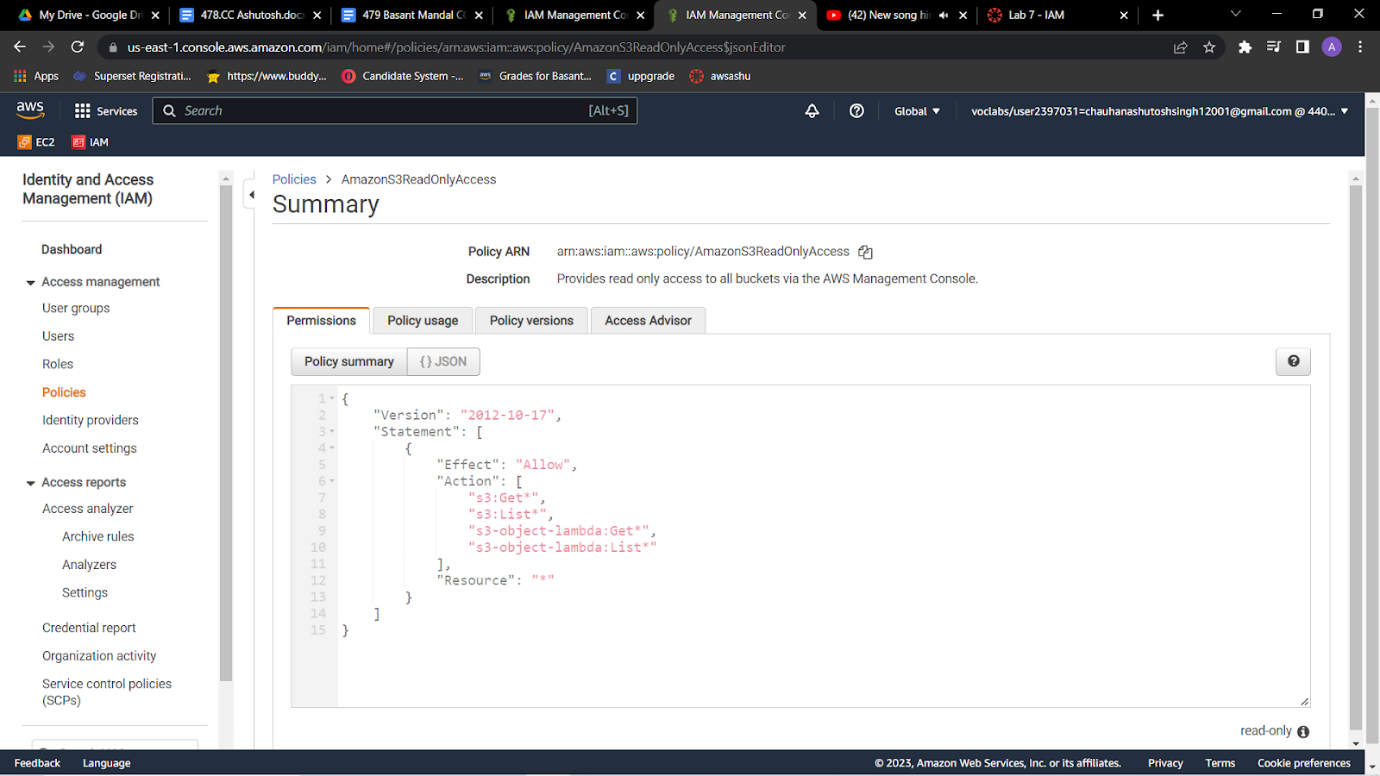
7.Choose the **{} JSON** tab.

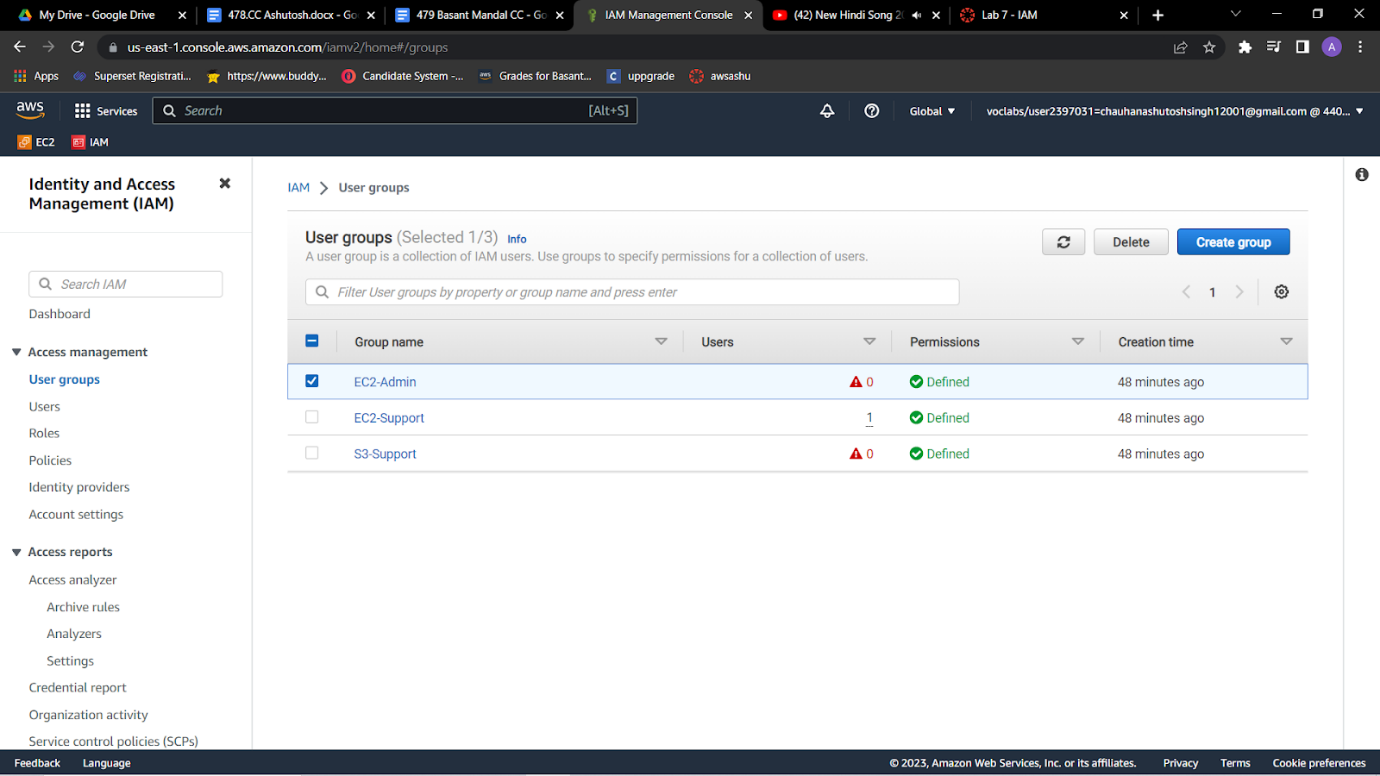
A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to *List* and *Describe* (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view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

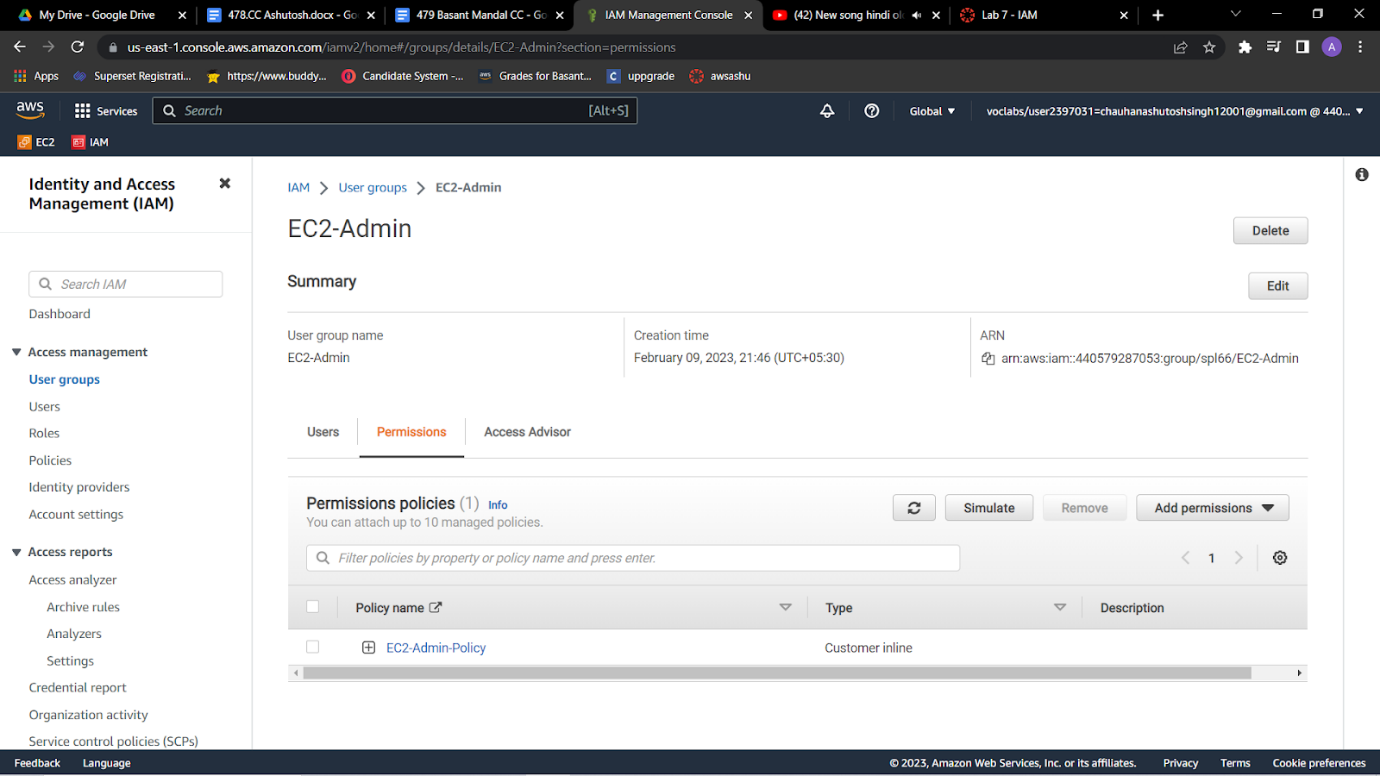
* Statements in an IAM policy have the following basic structure:
  + **Effect** says whether to *Allow* or *Deny* the permissions.
  + **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
  + **Resource** defines the scope of entities covered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

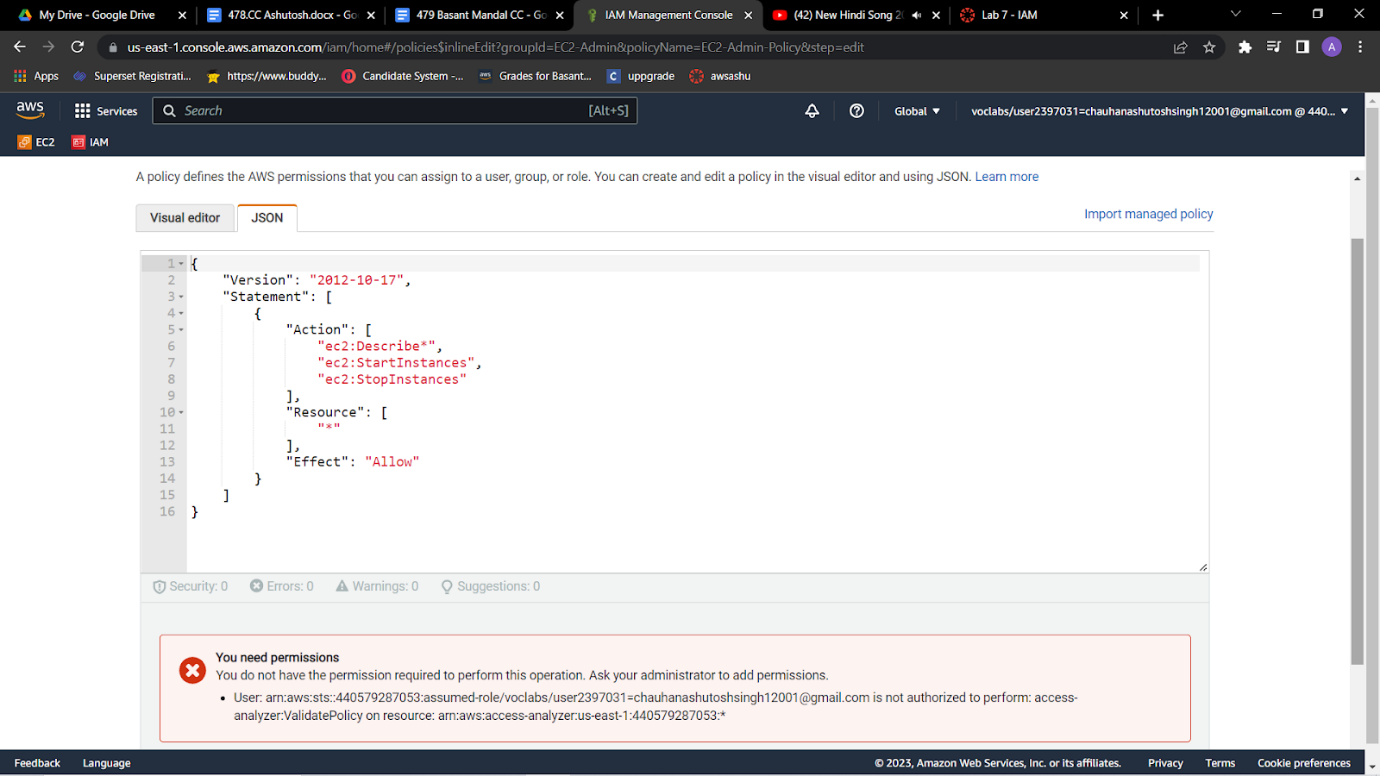


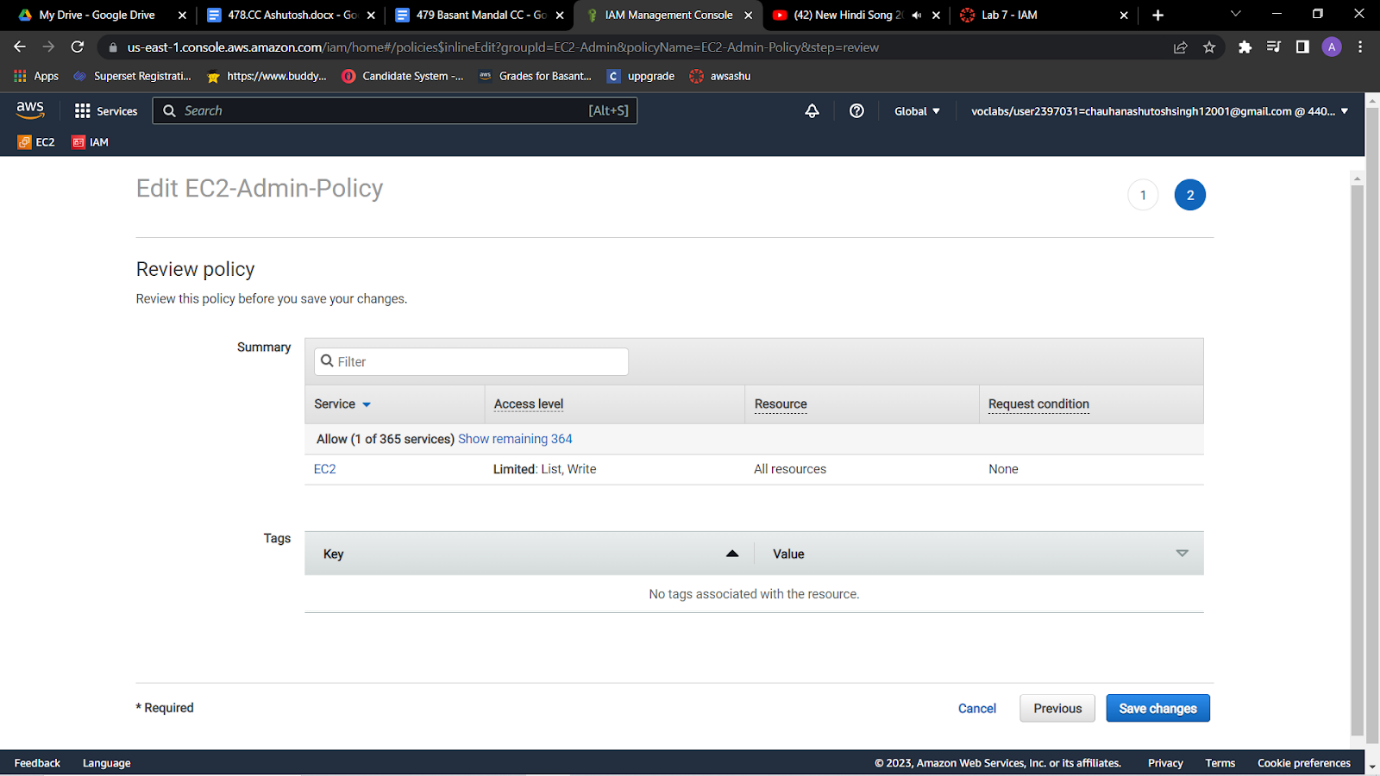
8.In the navigation pane on the left, choose **User groups**.Choose the name of the **S3-Support** group.Choose the **Permissions** tab.  
The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.    Under **Policy Name**, choose the link for the **AmazonS3ReadOnlyAccess** policy.Choose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

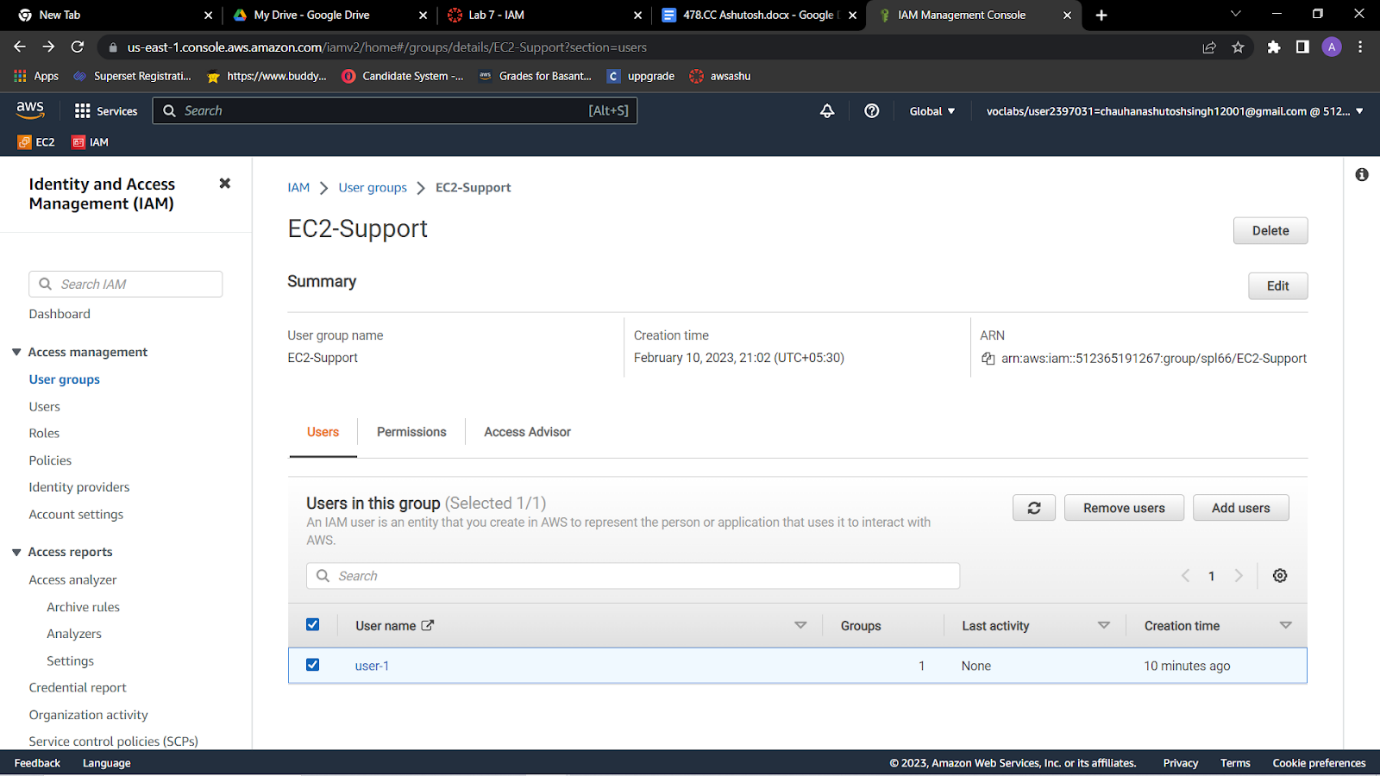
10.Choose the **Permissions** tab.  
This group is different from the other two. Instead of a managed policy, the group has an *inline policy*, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.

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. 



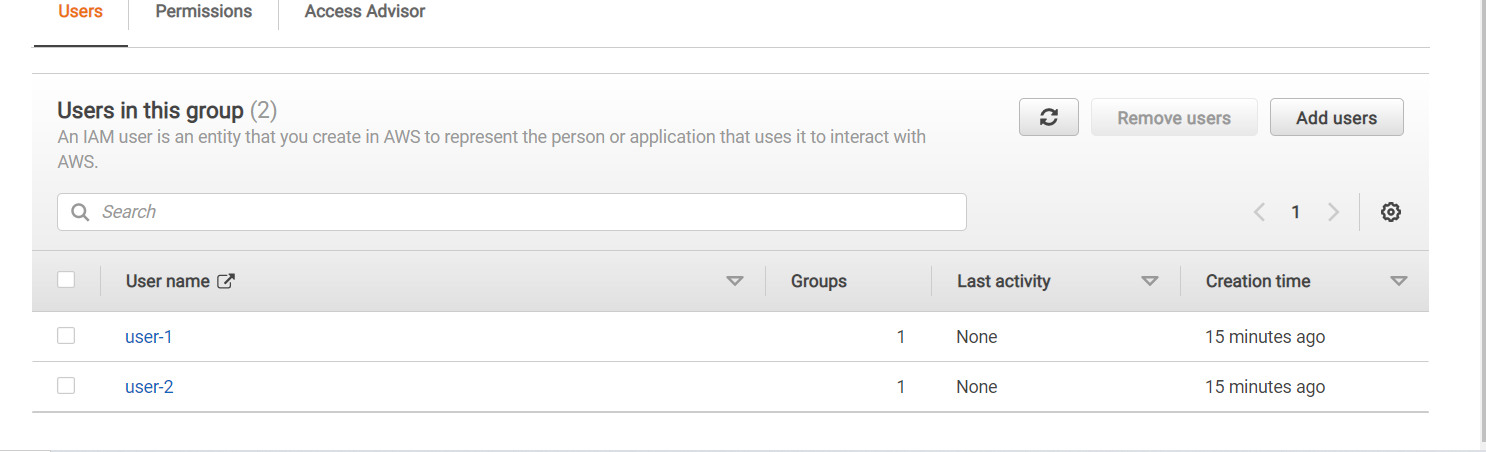
12.At the bottom of the screen, choose **Cancel** to close the policy.

**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.****

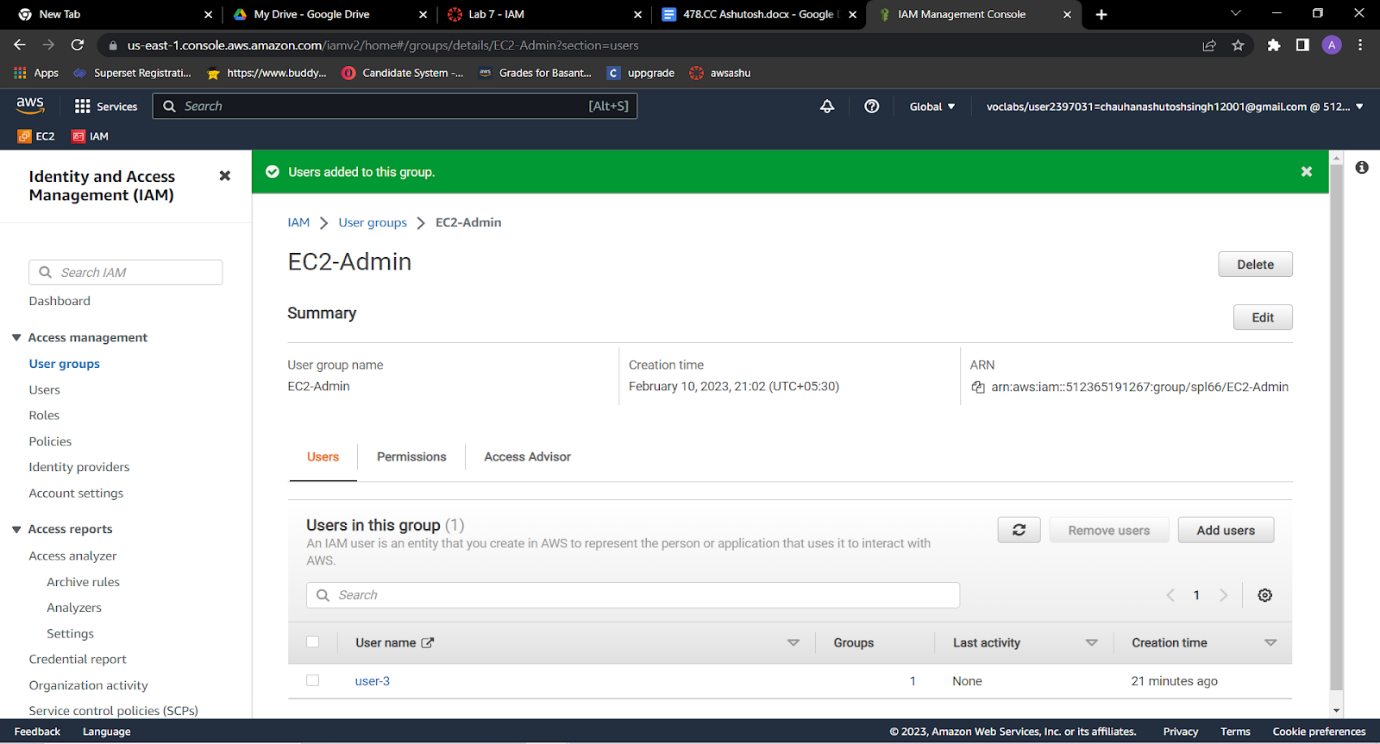
**Add user-2 to the EC2-Support group**

**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**

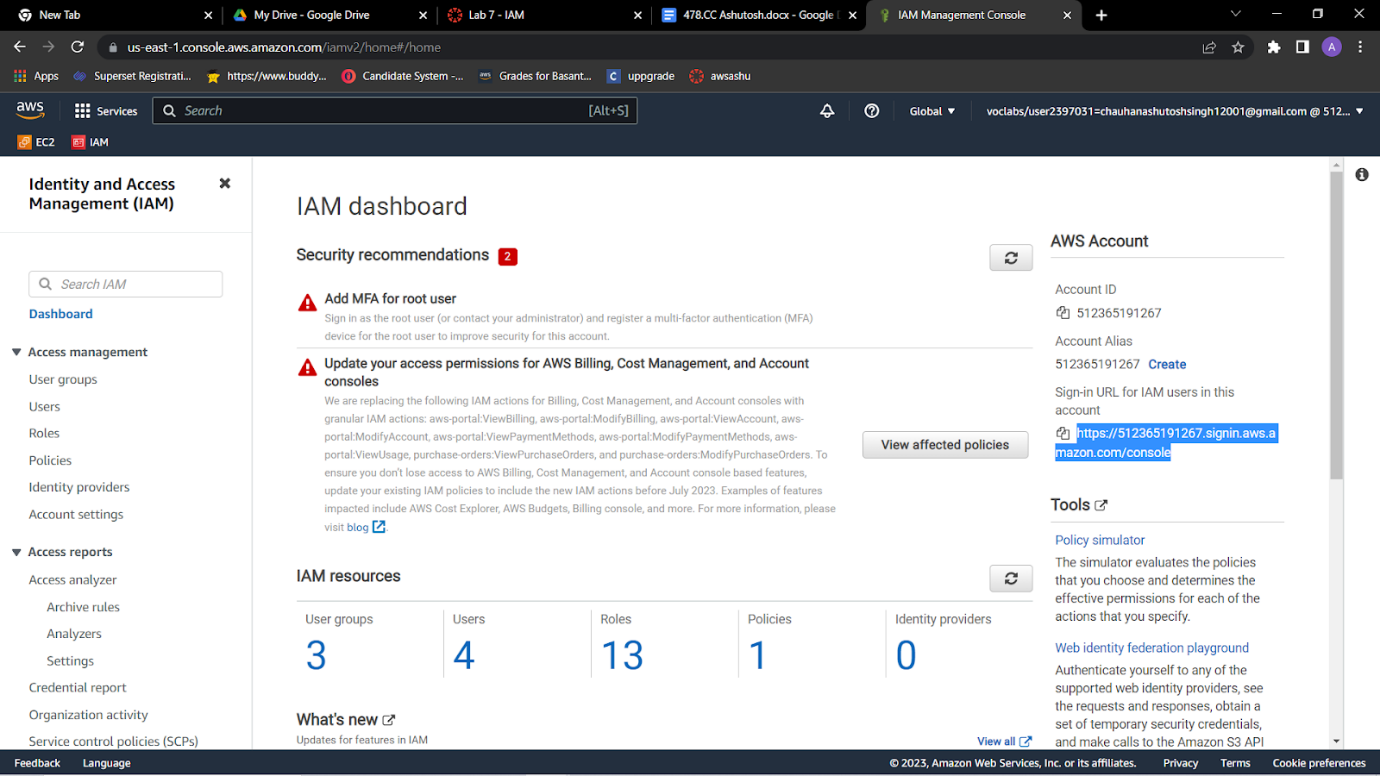
You have hired *user-3* as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the *EC2-Admin* group so that they inherit the necessary permissions via the attached *EC2-Admin-Policy*.

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**

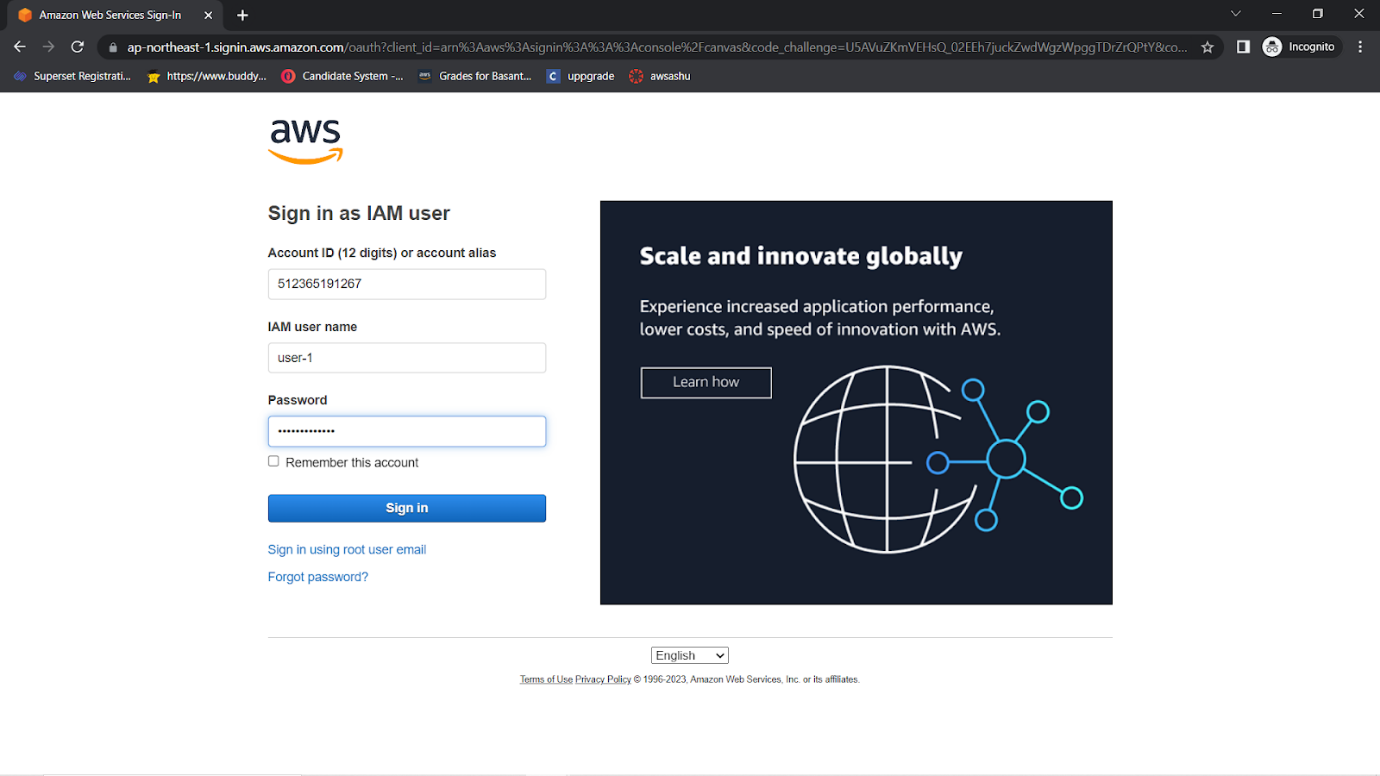
**Get the console sign-in URL**

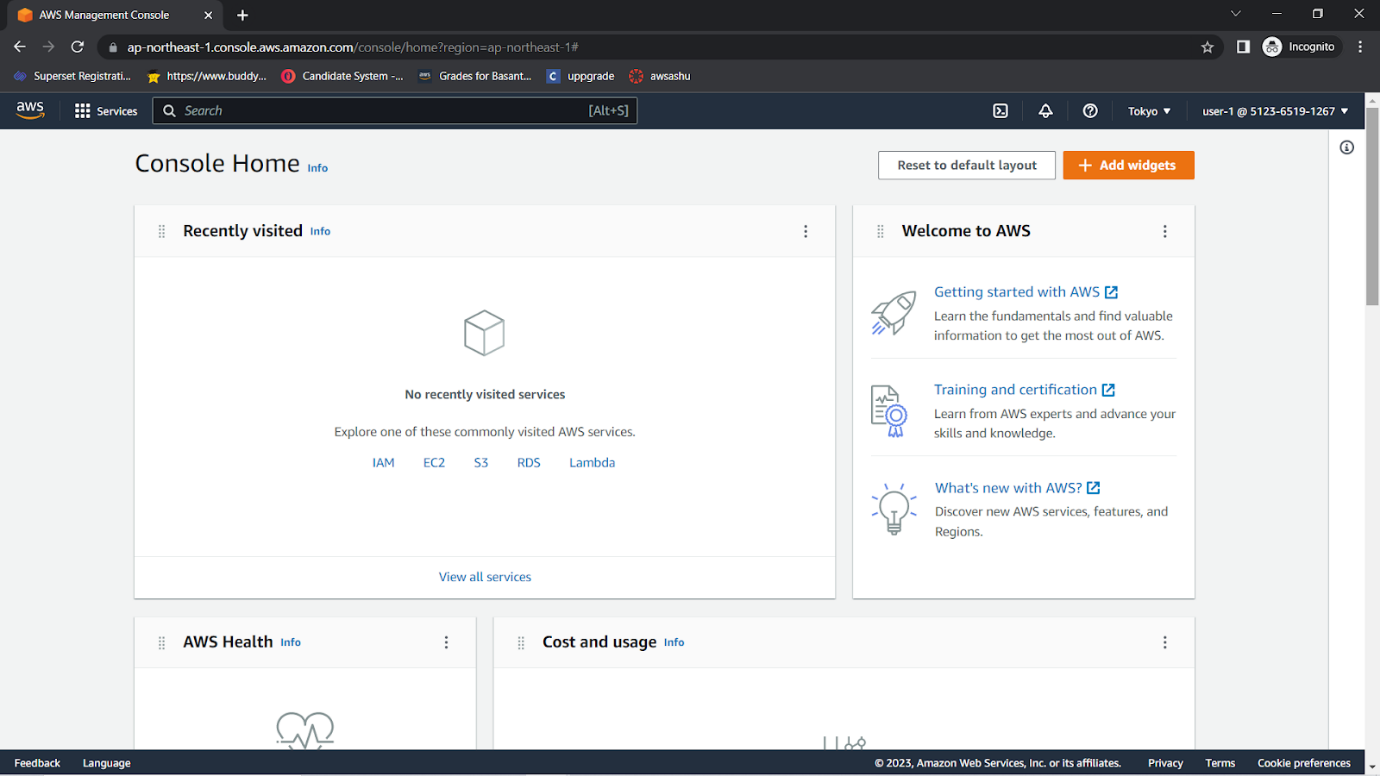
**16.**In the navigation pane on the left, choose Dashboard.Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: https://123456789012.signin.aws.amazon.com/console  
This link can be used to sign in to the AWS account that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

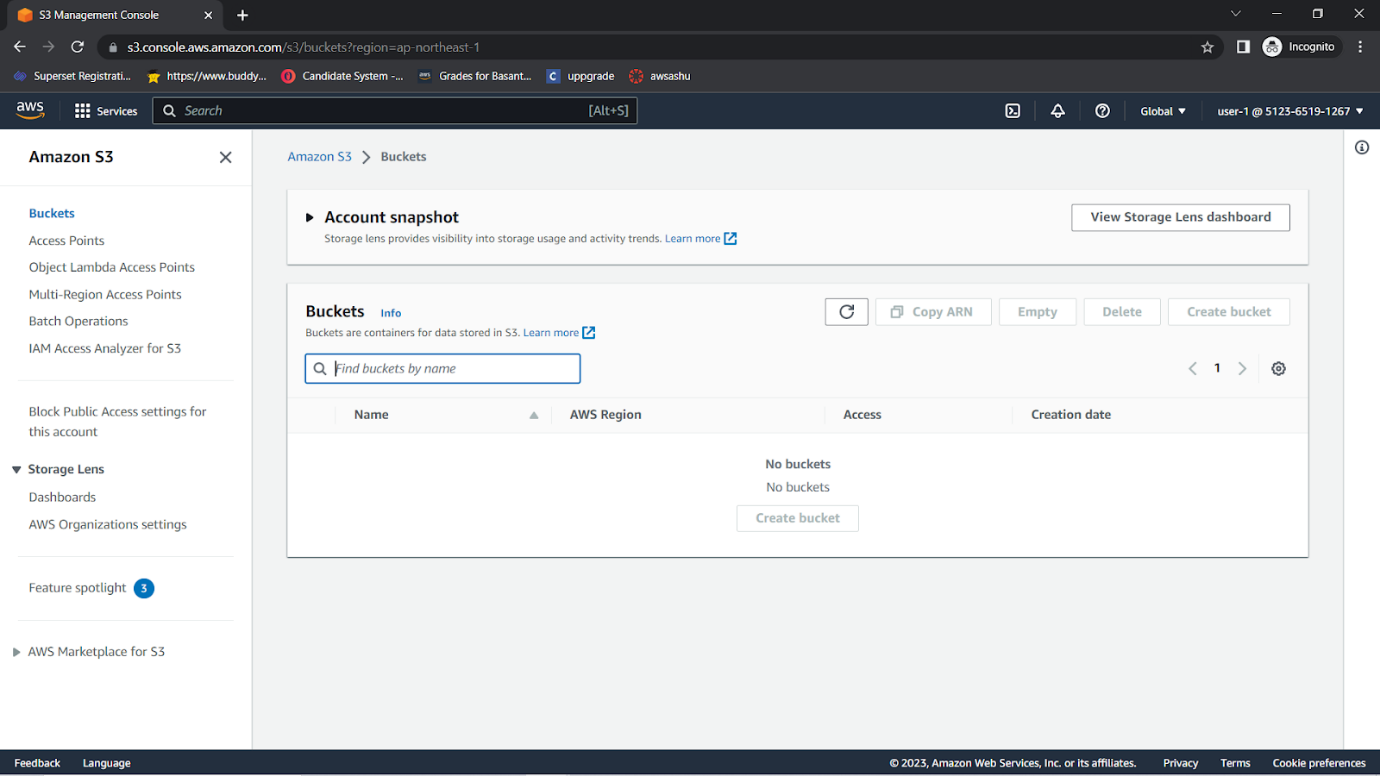


**Test user-1 permissions**

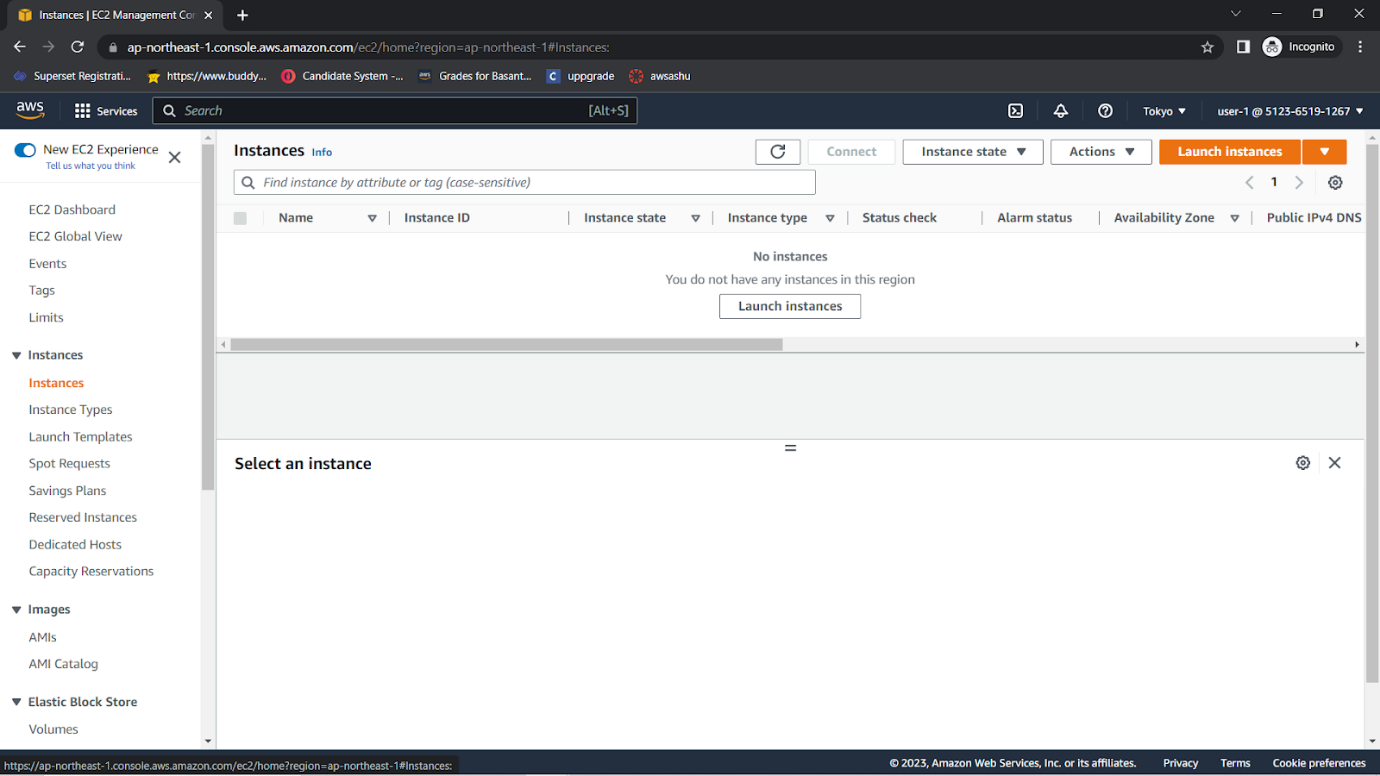
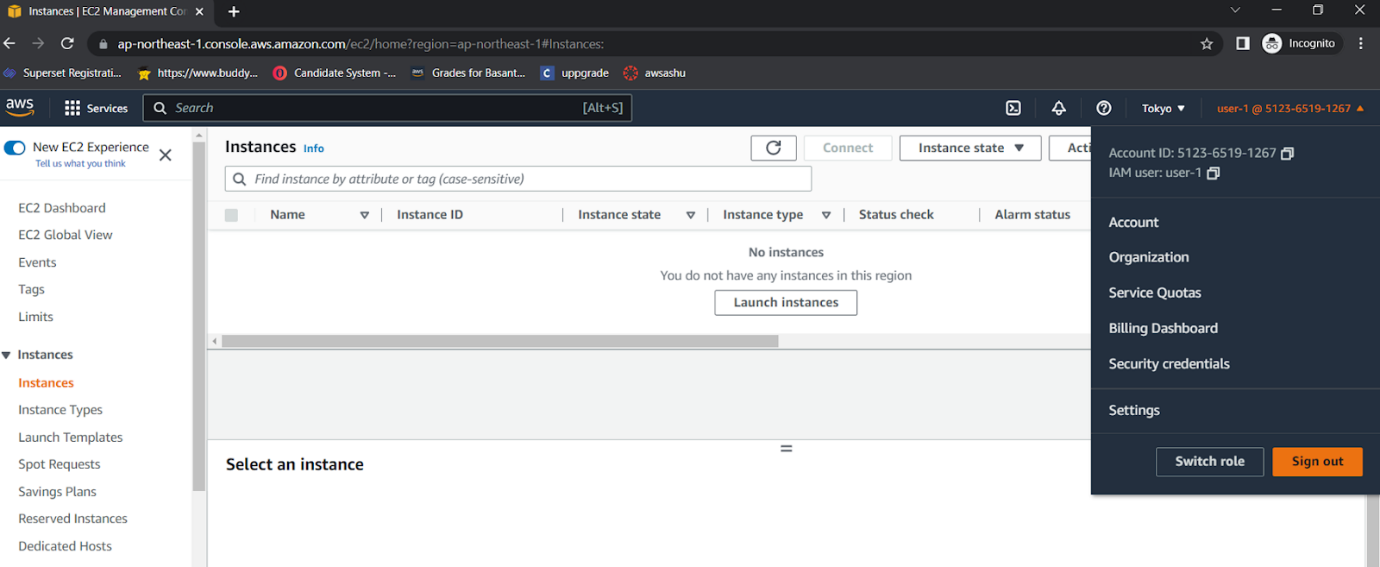
17.Open a private or incognito window in your browser.Paste the sign-in link into the private browser, and press ENTER.You will now sign-in as *user-1*, who has been hired as your Amazon S3 storage support staff.Sign in with the following credentials:**IAM user name:** user-1,**Password:** Lab-Password1

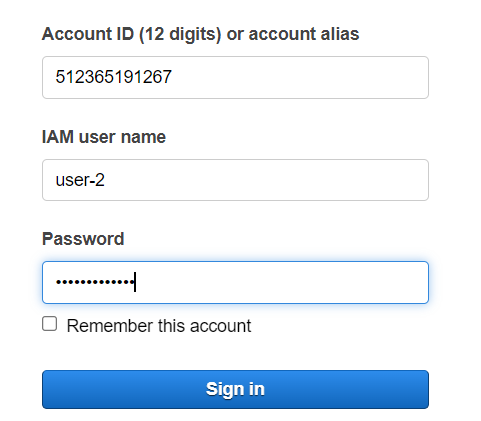




18.Choose the **Services** menu, and choose **S3**.Choose the name of one of your buckets, and browse the contents.Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.Now, test whether the user has access to Amazon EC2.

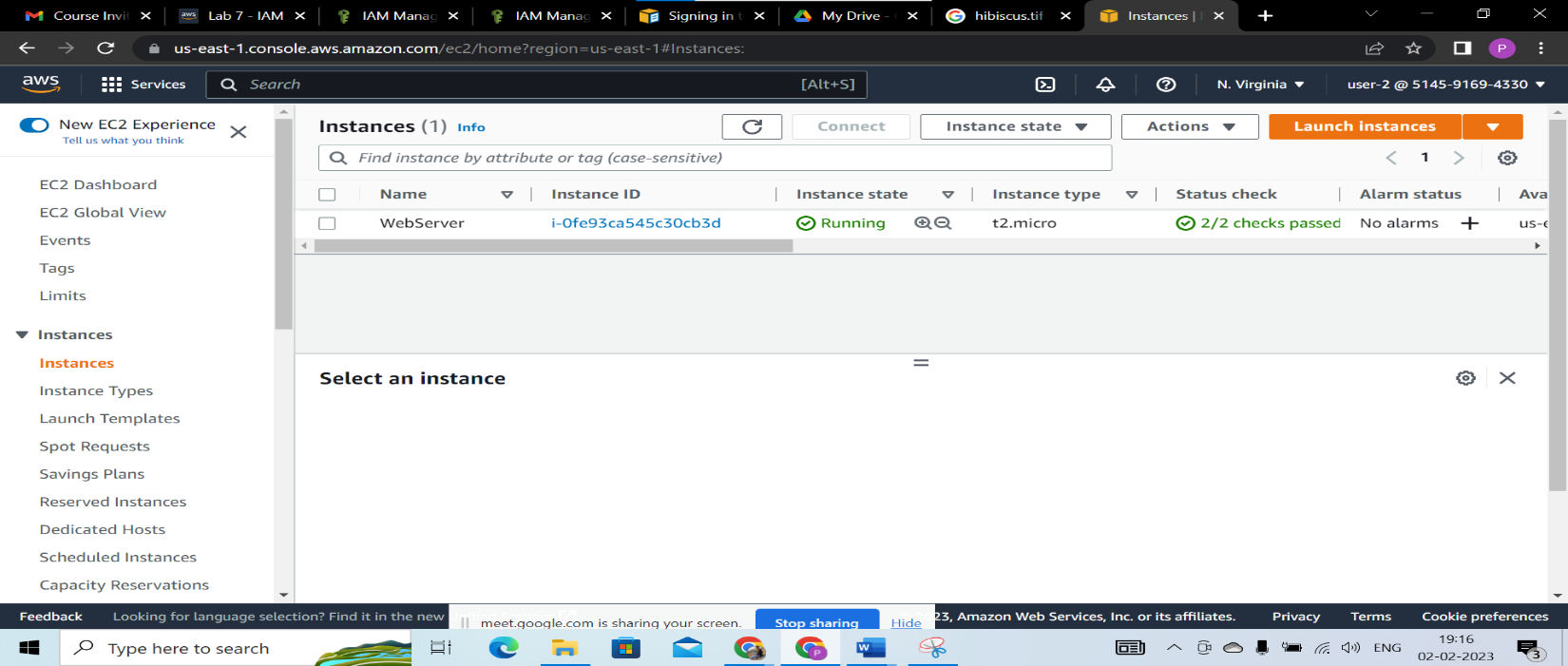
19.Choose the **Services** menu, and choose **EC2**.In the left navigation pane, choose **Instances**.You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2.You will now sign in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

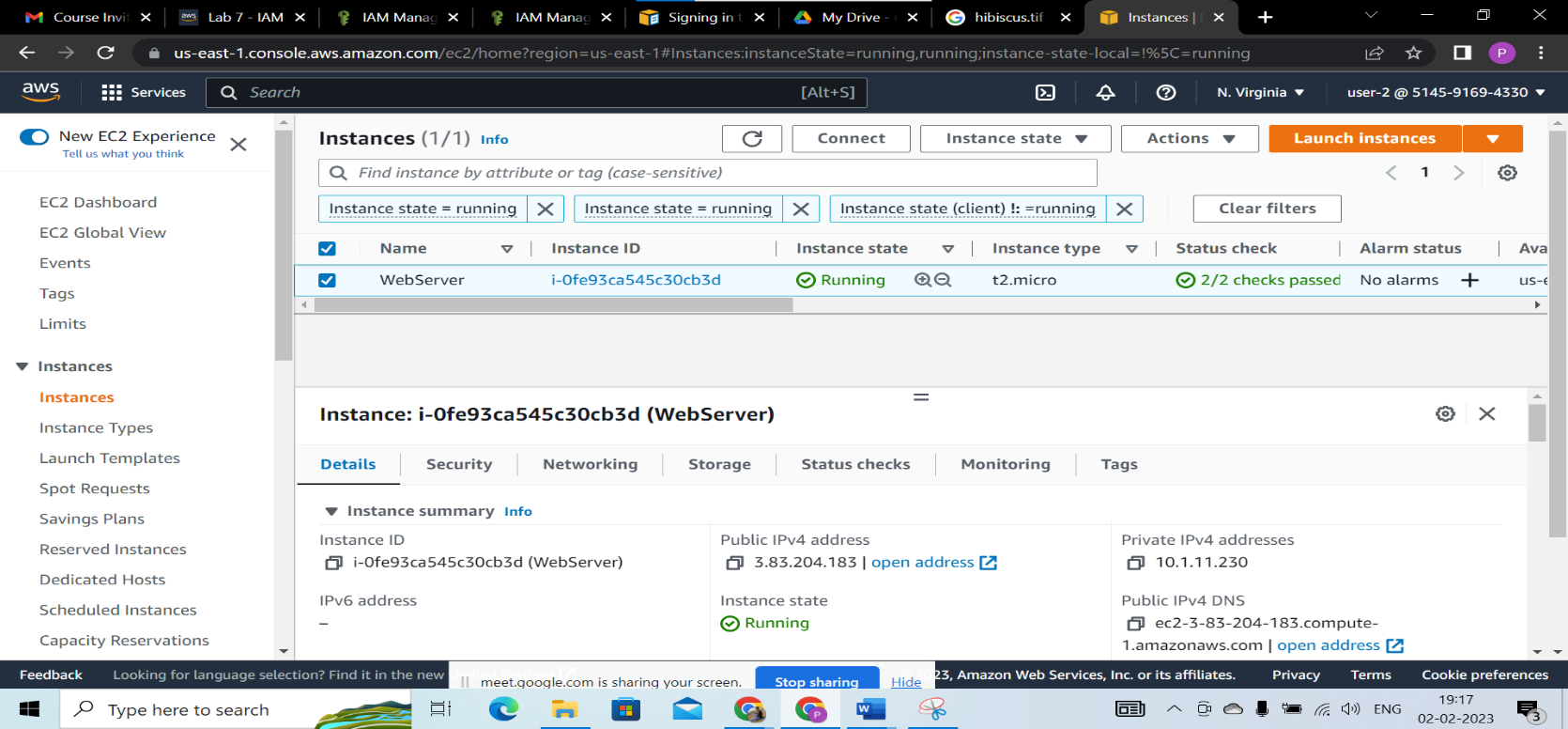
Sign Out

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.