

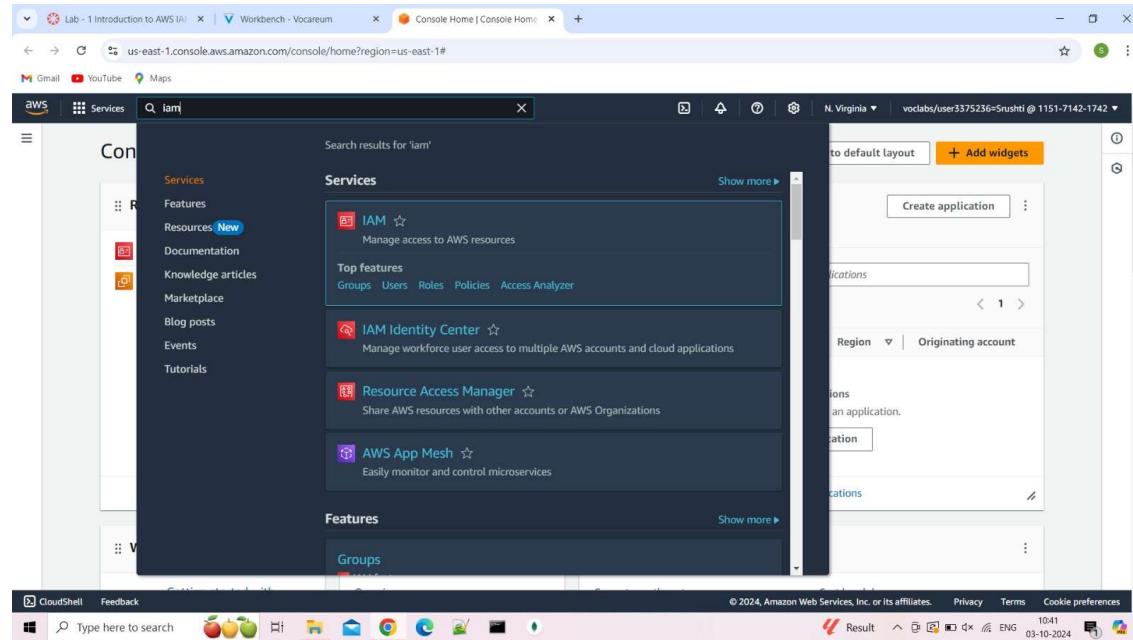
Assignment 6

Name : Srushti Dattatray Pawar

Class: Msc CS Part 2

Q.)Working and Implementation of Identity and Access Management (Using AWS)

Step 1: In the search box to the right of Services, search for and choose IAM to open the IAM console.



Step 2: In the navigation pane on the left, choose Users. The following IAM Users have been created already:

- user-1
- user-2
- user-3

The screenshot shows the AWS IAM service in the AWS Management Console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report). The main content area is titled 'Users (4) Info' and displays a table of users. The table columns are: User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. The users listed are: awsstudent (Path /), user-1 (Path /spl66/), user-2 (Path /spl66/), and user-3 (Path /spl66/). A modal window titled 'New: AWS User Notifications quick setup' is open, prompting to enable notifications for CloudWatch, EC2, and Health. A 'Create user' button is visible in the top right of the main area.

Step 3: Choose the user-1 link. This will bring to a summary page for user-1. The Permissions tab will be displayed.

The screenshot shows the AWS IAM service in the AWS Management Console, specifically for the user 'user-1'. The left sidebar is identical to the previous screenshot. The main content area is titled 'user-1 Info' and has a 'Summary' section with details like ARN, Created date, and Access keys. Below the summary is a tab bar with 'Permissions', 'Groups', 'Tags (1)', 'Security credentials', and 'Last Accessed'. The 'Permissions' tab is selected. Under 'Permissions policies (0)', it says 'Permissions are defined by policies attached to the user directly or through groups.' There is a search bar, a 'Filter by Type' dropdown set to 'All types', and a 'Policy name' input field. At the bottom of the page, there are links for CloudShell and Feedback, along with the standard AWS footer.

Step 4 :Choose the Groups tab.user-1 also is not a member of any groups.

The screenshot shows the AWS IAM User Details page for 'user-1'. The 'Groups' tab is selected. The 'User groups membership' section indicates that 'No resources' are attached to the user. The 'Summary' section shows the ARN as 'arn:aws:iam::115171421742:user/spl66/user-1', 'Console access' as 'Enabled without MFA', and two access keys: 'Access key 1' (AKIARVUGANYXE6GG6SUP4 - Active) and 'Access key 2' (Create access key). The user was created on 'October 03, 2024, 10:37 (UTC+05:30)'.

Step 5 :Choose the Security credentials tab.user-1 is assigned a Console password.

The screenshot shows the AWS IAM User Details page for 'user-1'. The 'Security credentials' tab is selected. The 'Console sign-in' section displays a 'Console sign-in link' (https://115171421742.siginn.aws.amazon.com/console) and a 'Console password' (Updated 4 minutes ago (2024-10-03 10:38 GMT+5:30)). The user was created on 'October 03, 2024, 10:37 (UTC+05:30)'.

Step 6: 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

The screenshot shows the AWS IAM User groups page. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report), CloudShell, and Feedback. The main content area is titled "User groups (3) info" and contains a table with the following data:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	4 minutes ago
EC2-Support	0	Defined	4 minutes ago
S3-Support	0	Defined	4 minutes ago

Step 7 : Choose the EC2-Support group link. This will bring you to the summary page for the EC2-Support group.

The screenshot shows the AWS IAM EC2-Support group summary page. The left sidebar is identical to the previous screenshot. The main content area is titled "EC2-Support info" and includes a "Summary" section with details: User group name (EC2-Support), Creation time (October 03, 2024, 10:58 (UTC+05:30)), and ARN (arn:aws:iam::115171421742:group/spl66/EC2-Support). Below this is a "Users" tab, which is currently selected, showing a table with no resources displayed: "No resources to display". Other tabs include "Permissions" and "Last Accessed". At the bottom right of the main content area are "Delete", "Edit", "Remove", and "Add users" buttons. The status bar at the bottom indicates it's 10:43 on 03-10-2024.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is open, showing 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is expanded, showing 'S3-Support' listed. The main content area is titled 'S3-Support' and displays the 'Summary' tab. It shows the 'User group name' as 'S3-Support', 'Creation time' as 'October 03, 2024, 10:38 (UTC+05:30)', and the 'ARN' as 'arn:aws:iam::115171421742:group/spl66/S3-Support'. Below this, there are tabs for 'Users', 'Permissions' (which is selected), and 'Last Accessed'. Under 'Permissions policies (1)', it shows a single policy named 'AmazonSS3ReadOnlyAccess' which is 'AWS managed'. At the bottom of the page, there is a footer with copyright information and a date.

Step 8: Choose the Permissions tab

This screenshot shows the same AWS IAM interface, but for the 'EC2-Admin' user group. The navigation pane and overall layout are identical to the previous screenshot. The main content area is titled 'EC2-Admin' and displays the 'Permissions' tab. It shows one permission policy named 'EC2-Admin-Policy' which is 'Customer inline'. The policy document is displayed in JSON format:

```
1< [ 2 "Version": "2012-10-17", 3 "Statement": [ 4 { 5 "Action": [ 6 "ec2:Describe*", 7 "ec2:StartInstances", 8 "ec2:StopInstances" 9 ], 10 "Resource": [ 11 "*" 12 ], 13 "Effect": "Allow" 14 } 15 ] 16 ]
```

The screenshot shows the AWS Identity and Access Management (IAM) console. In the left navigation pane, under 'Access management', the 'User groups' option is selected. A sub-menu for 'S3-Support' is open. The main content area displays the 'S3-Support' user group details. The 'Summary' section shows the user group name 'S3-Support', creation time 'October 03, 2024, 10:38 (UTC+05:30)', and ARN 'arn:aws:iam::115171421742:group/spl66/S3-Support'. Below this, the 'Users' tab is selected, showing a table with one row: 'User name' (with a search bar and filter). The table also includes columns for 'Groups', 'Last activity', and 'Creation time'. A note states 'No resources to display'.

Step 9 :In the navigation pane on the left, choose User groups. Choose the S3- Support group link and then choose the Permissions tab.

The screenshot shows the 'Add users' page for the 'S3-Support' group. The left sidebar shows the 'User groups' section with 'S3-Support' selected. The main content area has a heading 'Add users' and a sub-section 'Add users to S3-Support'. A table lists three users: 'user-1' (selected), 'user-2', and 'user-3'. Each row shows the user name, number of policies (0), permissions (None), and last activity (7 minutes ago). A 'Copy' button is located at the bottom right of the table. At the bottom of the page are 'Cancel' and 'Add users' buttons. The status bar at the bottom indicates it's 22°C Clear, 10:45, and the date is 03-10-2024.

Step 11: Choose the EC2-Admin group link and then choose the Permissions tab.

The screenshot shows the AWS IAM console with the URL us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/details/S3-Support?section=users. The main panel displays the summary for the 'S3-Support' user group, which was created on October 03, 2024, at 10:38 (UTC+05:30). It shows one user added to the group: 'user-1'. The 'Permissions' tab is visible but not selected. The ARN for the group is listed as arn:aws:iam::115171421742:group/spl66/S3-Support.

Choose the plus (+) icon to view the policy details.

The screenshot shows the AWS IAM console with the URL us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/details/EC2-Support?section=users. The main panel displays the summary for the 'EC2-Support' user group, which was created on October 03, 2024, at 10:38 (UTC+05:30). It shows zero users added to the group. The 'Permissions' tab is visible but not selected. The ARN for the group is listed as arn:aws:iam::115171421742:group/spl66/EC2-Support.

Step 12 : In the left navigation pane, choose User groups. Choose the S3- Support group link.

The screenshot shows the AWS IAM console interface. At the top, there are three tabs: 'Lab - 1 Introduction to AWS IAM' (active), 'Workbench - Vocareum', and 'Add users | IAM | Global'. The main content area displays a table of users:

User	Access Type	Last Activity
user-1	1	8 minutes ago
<input checked="" type="checkbox"/> user-2	0	8 minutes ago
user-3	0	8 minutes ago

A red box highlights the 'Copy' button at the bottom right of the table. Below this, a modal window titled 'EC2-Support' shows the summary of the user group:

Summary

User group name	Creation time	ARN
EC2-Support	October 03, 2024, 10:38 (UTC+05:30)	arn:aws:iam::115171421742:group/spl66/EC2-Support

The 'Users' tab is selected, showing one user: 'user-2'. The 'Permissions' and 'Last Accessed' tabs are also present. At the bottom of the modal, there are 'Edit', 'Delete', 'Remove', and 'Add users' buttons. The status bar at the bottom indicates 'CloudShell Feedback' and the date '03-10-2024'.

Step 13 : Choose the Users tab. In the Users tab, choose Add users.

The screenshot shows the AWS IAM console with the 'EC2-Admin' user group selected. The 'Users' tab is active, displaying a summary of the group. The ARN is listed as arn:aws:iam::115171421742:group/spl66/EC2-Admin. A search bar and a 'Remove' button are visible above the user list. The list itself is empty, showing 'No resources to display'.

Step 14 : In the Add Users to S3-Support window, configure the following:
o Select user-1.
o At the bottom of the screen, choose Add users. In the Users tab you will see that user-1 has been added to the group.

The screenshot shows the 'Add users' dialog box. The user 'user-3' is selected, indicated by a checked checkbox. At the bottom right, there is a 'Cancel' button and a highlighted 'Add users' button. Below the dialog, a message 'User-3 added successfully' is displayed.

User-3 added successfully

The screenshot shows the AWS Identity and Access Management (IAM) console. The left navigation pane is open, showing 'User groups' under 'Access management'. The main content area displays a summary of the 'EC2-Admin' user group. It shows 1 user added to the group, named 'user_3'. The ARN of the group is listed as arnawsiam::115171421742:group/spl66/EC2-Admin. The creation time is October 05, 2024, 10:38 (UTC+05:30). Below the summary, there are tabs for 'Users' (1), 'Permissions', and 'Last Accessed'. The 'Users' tab shows the single user 'user_3'.

Step 18 : In the navigation pane on the left, choose User groups. Each Group should now have a 1 in the Users column, indicating the number of Users in each Group.

The screenshot shows the AWS IAM 'User groups' page. The left navigation pane is open, showing 'User groups' under 'Access management'. The main content area displays a list of user groups. There are three groups listed: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. Each group has 1 user assigned, indicated by the number '1' in the 'Users' column. The 'Permissions' column shows 'Defined' for all groups. The 'Creation time' column shows '8 minutes ago' for all groups. The 'Group name' column lists the group names: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. The ARNs for the groups are listed as arnawsiam::115171421742:group/spl66/EC2-Admin, arnawsiam::115171421742:group/spl66/EC2-Support, and arnawsiam::115171421742:group/spl66/S3-Support respectively.

Step 19 :In the navigation pane on the left, choose Dashboard.A Sign-in URL for IAM users in this account link is displayed on the right.copy it

The screenshot shows the AWS IAM Dashboard. On the left, the navigation pane includes 'Identity and Access Management (IAM)' and several menu items under 'Dashboard' and 'Access management'. The main area displays 'IAM resources' with counts: User groups (3), Users (4), Roles (16), Policies (1), and Identity providers (0). Below this is a 'What's new' section with four bullet points about IAM Access Analyzer, Bulk Policy Migration, and IAM Roles Anywhere. To the right, there's a sidebar titled 'AWS Account' showing the Account ID (115171421742) and a 'Sign-in URL for IAM users in this account' link: <https://115171421742.signin.aws.amazon.co/m/console>. At the bottom, the status bar shows the URL https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home.

Step 20 :Open a private (Incognito) window.Paste the IAM users sign-in link into the address bar of your private browser session and press Enter.

Step 21 :Sign-in with: ● IAM user name: user-1 Password: Lab-Password1

The screenshot shows a private browser window with the URL eu-north-1.signin.aws.amazon.com. A modal dialog at the top says 'Try the new sign in UI' with a link to 'Enable new sign in'. The main form is titled 'Sign in as IAM user' and requires 'Account ID (12 digits) or account alias' (115171421742), 'IAM user name' (user-1), and 'Password' (Lab-Password1). There's also a 'Remember this account' checkbox and a 'Sign in' button. Below the form is a note about using root user email and forgot password links. To the right, there's an advertisement for 'Amazon Lightsail' featuring a cartoon robot and the text 'Lightsail is the easiest way to get started on AWS'. The status bar at the bottom shows the URL https://eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=1_emZPuSEKSYRe37JlwULEf5T_UVo-UluaVbGldQc&code_challenge

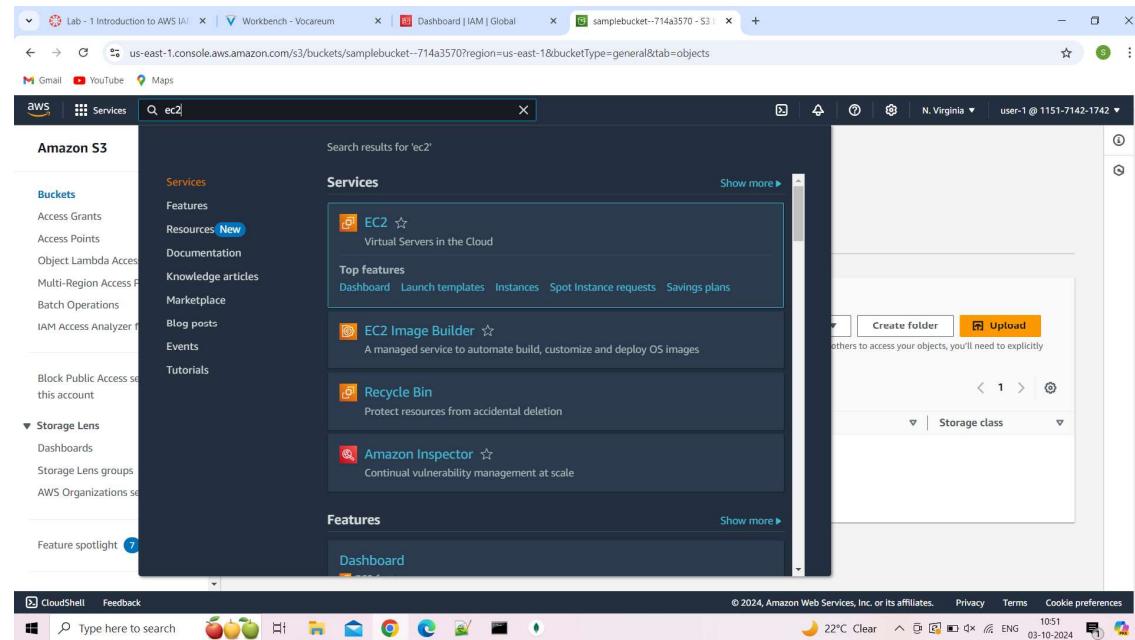
Step 22 :In the search box to the right of Services, search for and choose S3 to open

The screenshot shows the AWS Management Console search results for 's3'. The search bar at the top contains 's3'. On the left, there's a sidebar with links like 'Services', 'Features', 'Resources New', 'Documentation', 'Knowledge articles', 'Marketplace', 'Blog posts', 'Events', and 'Tutorials'. The main panel displays 'Search results for 's3'' and lists several services under 'Services': S3 (Scalable Storage in the Cloud), S3 Glacier (Archive Storage in the Cloud), AWS Snow Family (Large Scale Data Transport), and Storage Gateway (Hybrid Storage Integration). Below these, there's a section for 'Features'.

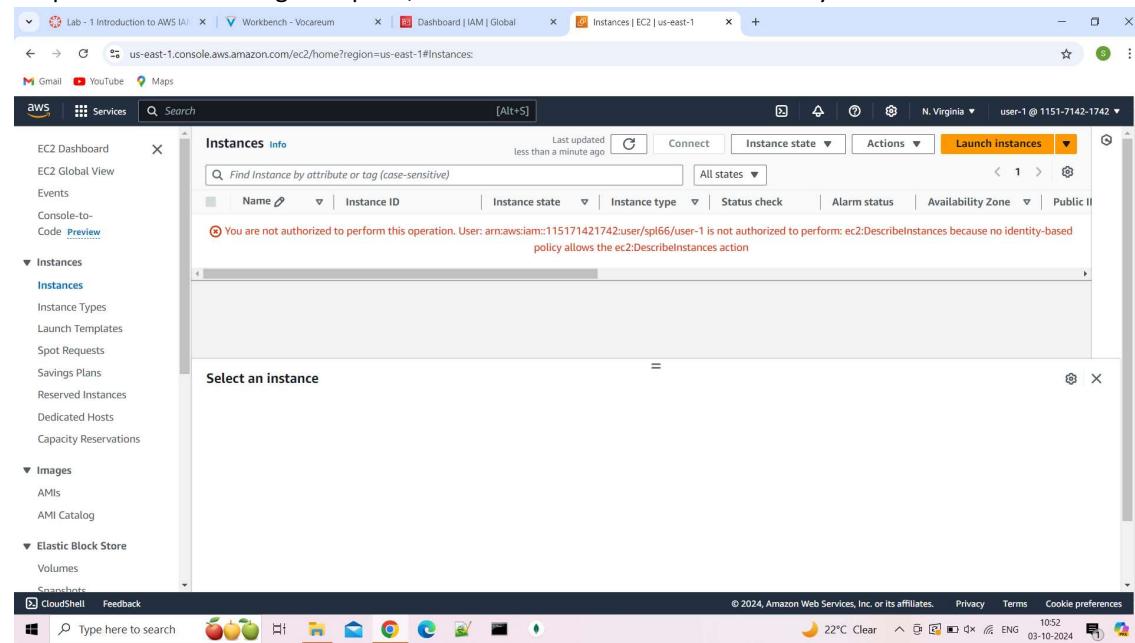
Step 23 :Choose the name of the bucket that exists in the account and browse the contents.The bucket does not contain any objects.

The screenshot shows the AWS S3 bucket details page for 'samplebucket--714a3570'. The URL in the address bar is 'us-east-1.console.aws.amazon.com/s3/buckets/samplebucket--714a3570?region=us-east-1&bucketType=general&tab=objects'. The left sidebar has 'Amazon S3' selected, with 'Buckets' expanded, showing options like 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', and 'Block Public Access settings for this account'. The main content area shows the 'samplebucket--714a3570' bucket. It has tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under 'Objects', it says '(0)' and 'No objects'. There are buttons for 'Upload' and 'Create folder'. A note says 'Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 Inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.' The status bar at the bottom shows '22°C Clear' and the date '03-10-2024'.

Step 24 :In the search box to the right of Services, search for and choose EC2 to open the EC2 console.

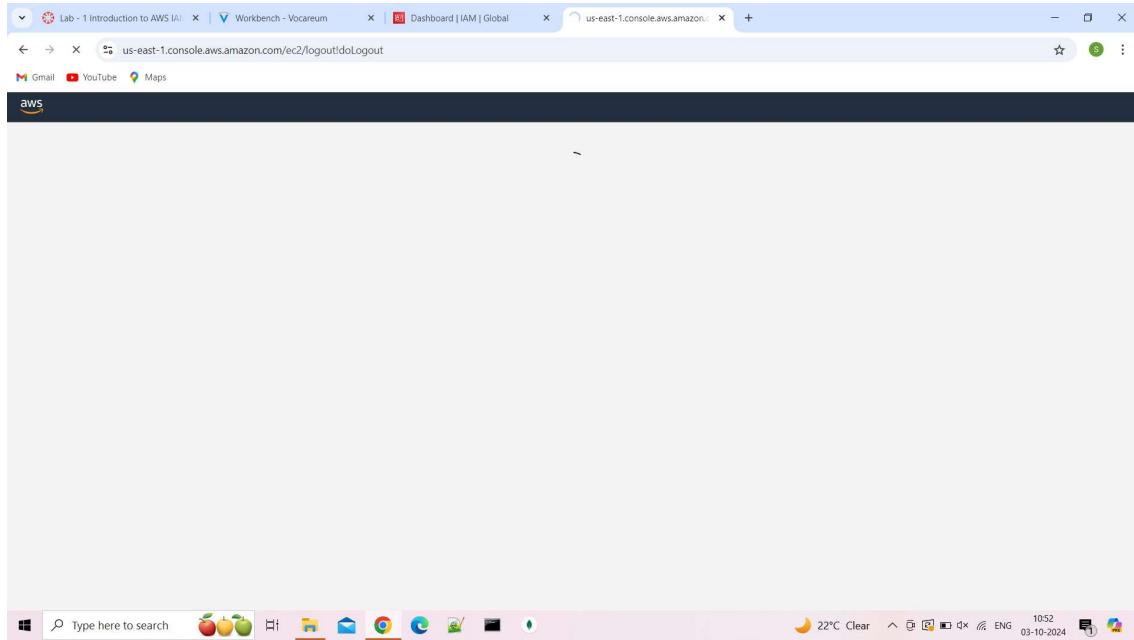


Step 25 :In the left navigation pane, choose Instances.You cannot see any instances.

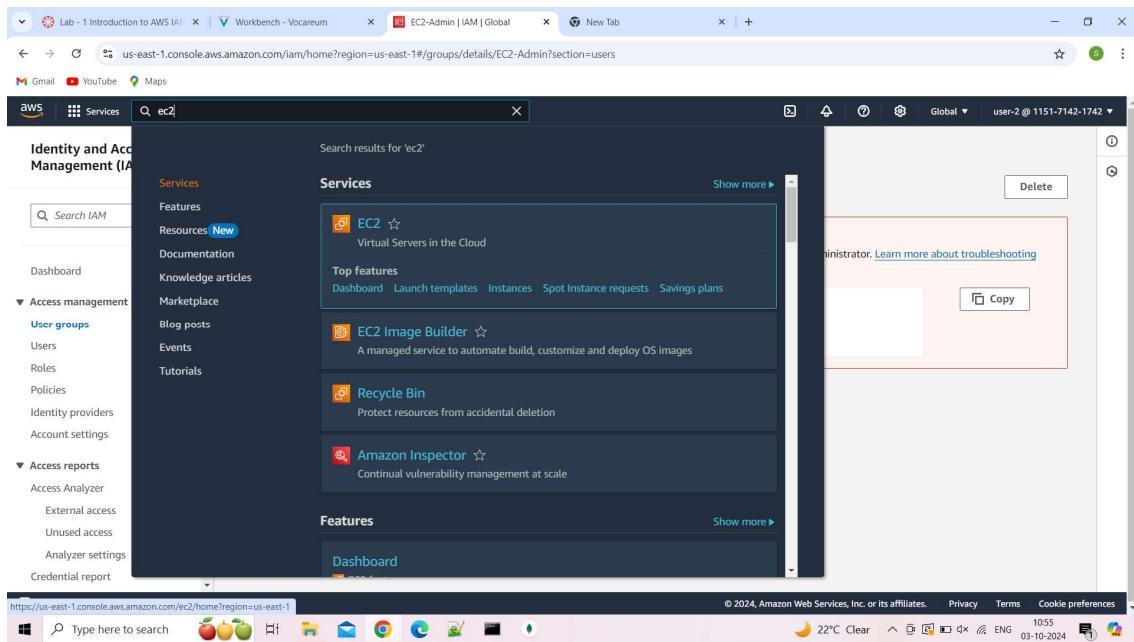


Step 26: Choose Sign Out Step

27: Paste the IAM users sign-in link into your private browser tab's address bar and press Enter. Sign-in with: IAM user name: user-2 Password: Lab-Password2



Step 28 :In the search box to the right of Services, search for and choose EC2 to open the EC2 console.



Step 29 :In the navigation pane on the left, choose Instances.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed, and the main content area displays a table of instances. There are two rows in the table:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
LabHost	i-04ffaa08c7b5bdf67	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-98-1
Bastion Host	i-079b7f1cb2fc734bd	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-

Below the table, a detailed view for the first instance (i-04ffaa08c7b5bdf67) is expanded. It shows the following details:

- Instance ID: i-04ffaa08c7b5bdf67 (LabHost)
- Public IPv4 address: 98.81.250.57 [open address]
- Private IPv4 addresses: 10.11.139
- Public IPv4 DNS: ec2-98-81-250-57.compute-1.amazonaws.com [open address]
- Instance state: Running
- Hostname type: Private IP DNS name (IPv4 only)

The bottom of the screen includes a search bar, a toolbar with various icons, and a footer with copyright information and system status.

Step 30 : Select the instance named LabHost, In the Instance state menu above, select Stop instance.

The screenshot shows the AWS EC2 Instances page. There are two instances listed:

- LabHost**: Instance ID i-04ffaa08c7b5bdf67, Running, t2.micro
- Bastion Host**: Instance ID i-079b7f1cb2fc734bd, Running, t2.micro

The 'Actions' dropdown for the LabHost instance is open, and the 'Stop instance' option is highlighted.

The screenshot shows the 'Stop instance' confirmation dialog for the LabHost instance. The dialog includes the following information:

- Instance ID: i-04ffaa08c7b5bdf67 (LabHost)
- Stop protection: Off (Can stop instance)
- Warning message: You will be billed for associated resources. After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.
- Associated resources: You will continue to incur charges for these resources while the instance is stopped.

At the bottom right of the dialog are 'Cancel' and 'Stop' buttons.

Step 31: You will receive an error stating You are not authorized to perform this operation. This demonstrates that the policy only allows you to view information, without making changes.

The screenshot shows a browser window with the AWS CloudWatch Errors interface. The main content area displays an error message: "Failed to stop the Instance i-04ffaa08c7b5bdf67". The message states that the user is not authorized to perform this operation, specifically the EC2:StopInstances action, due to a lack of identity-based policy allowing it. The error code is ec2:StopInstances and the full message is: "User: arn:aws:sts::115171421742:assumed-role/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:115171421742:instance/i-04ffaa08c7b5bdf67 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: vpp80bEtqy5n8OKVSYALf6sbuCtByxb8Dov6hdj1dWr-dNRhb0UDehWThTgFxsymb6EgjFACBY1MndvJKm90dmF-VmBa0xCaucR6LNVTaJ1ep0QsgoyXjYfuyglg10Egi_QXq0R05af0kLcY8o5Tc_uMdpr1ePjX35a0KwHgiacBqn67jbBrk3x2HJLD025EvAknWofsTh eRRBixEvWW-tb0iMH0sZwc2zC4zt2jDLve0lx8t3K2C8wdoZniGQIAcBGYUH3GVDVVGQ1bN4Uf4leyQkEL5doTw90tzkMopJz71uMyI2k7BTlyxtMMx8ZQbmQHe6k4 RMBzV2huwH1J9r7vJ2TON3Dyq_G_oq5hixXcEUMGX_gyevx5xIUEb6J1EB2ZORM5YTgxewp_TFKJ7esym76W6unFuFYyzAm41L4_GtQj2IRZ5KgllEmry8XM75Ku9nCPaBQ_uxqT olE1qjPARCVoSwKhvqZEHwVxKjB9VOTLOxmJ_I3yra6aCnCo5yG-e5PhKnr03murnf1xuKzNlyppUj529nKvKDceQsGpx-9KDfEm4JNH_QKieg0ub3hVc4WfSmLFe3faAsvq_jp8083JtPgeMnwuWz2ADrnihOkidzj2Lnmc0lcnQmNRuVChgp0JbV2J0XA-uAnM3CCSgfmklnh0Elhbe2VHDCLGliodQ_Ygywofk62ROgFG-BKxa14Jstefq65QCKmt5PxgKk6p1b0Ar4un-vjDbw9Jlu_Vpa0dStgExQ1AnzGLqdDA1tPf5GdbtuGVKLVLNUtwDIZ2Im05P6g05cS9JzgmnctQpusBcPvJCold.ttM_nGDWMDqyjdNQicTRGPg3 2grZt_5SDPgvJbbNUHKGYBOu1AWsjkVrdkmnw1A2njz5oUjdttsxQFWHMz8FblbNj-2Q4mNGYlOfZaqwy-slRnuSU3cvwpypC7b2SaXHICoH3icyyPdjFN1zbAFE-9xgcYwEnb5APfHsBnlojMaTCMo6Kn1To413M4Z1uo_zw

The sidebar on the left lists various AWS services like EC2 Dashboard, EC2 Global View, Events, Console-to-Code, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, and Snapshots. At the bottom of the sidebar, there are CloudShell and Feedback links.

Step 32 : In the search box to the right of Services, search for and choose S3 to open the S3 console.

The screenshot shows a browser window with the AWS Services menu open. The search bar at the top right contains the text "S3". The results list includes "Recently visited" (EC2, IAM, Console Home), "Favorites" (Analytics, Application Integration, Blockchain, Business Applications, Cloud Financial Management, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, Front-end Web & Mobile), and "All services" (Analytics, Application Integration, Blockchain, Business Applications, Cloud Financial Management, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, Front-end Web & Mobile, IAM, Kinesis, Lambda, Machine Learning, Media Services, Mobile, Organizations, Personalize, Rekognition, Route 53, S3, SageMaker, Security, Systems Manager, Transfer, VPC, WAF, WorkLink, WorkSpaces). The "S3" entry is highlighted with a yellow star icon. The right side of the screen shows the same error message as in Step 31, indicating unauthorized access to the S3 service.

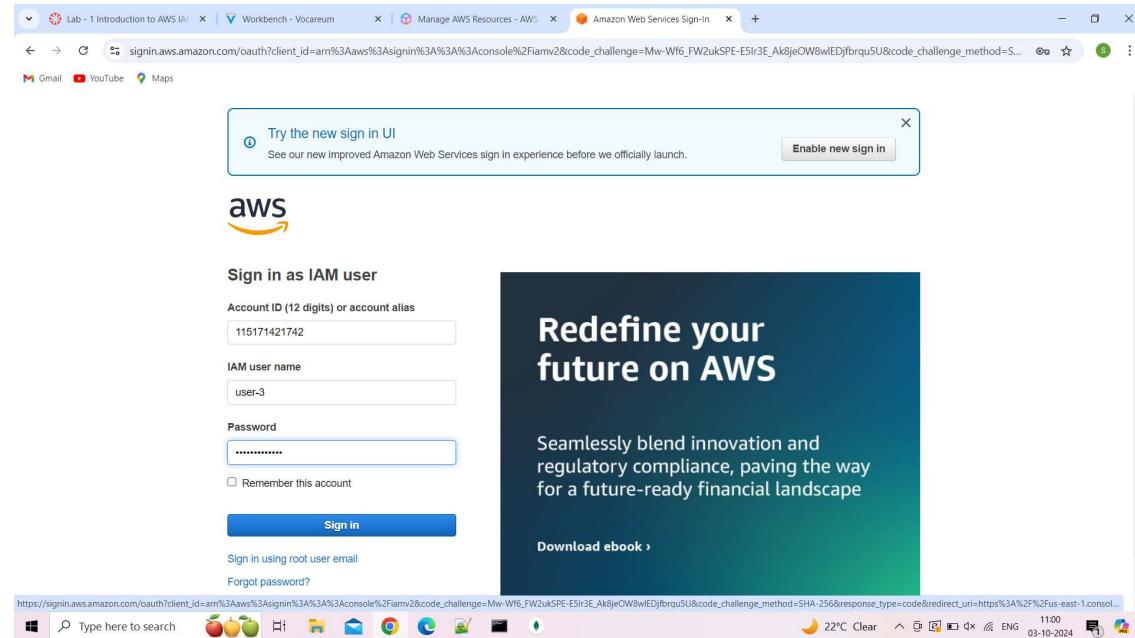
You will see the message You don't have permissions to list buckets because user-2 does not have permission to access Amazon S3.

The screenshot shows the AWS S3 console with a modal dialog. The dialog title is "Create S3 bucket | S3 | us-east-1". It contains a "Bucket Key" section with a note about SSE-KMS and two radio buttons: "Disable" and "Enable" (selected). Below this is an "Advanced settings" section with a note about uploading files after creation. A large error message box is present, stating "Failed to create bucket" with the sub-note "To create a bucket, the s3:CreateBucket permission is required." It includes a "Diagnose with Amazon Q" button and links to the IAM console and Identity and Access Management in Amazon S3. At the bottom are "Cancel" and "Create bucket" buttons. The background shows the AWS navigation bar and a taskbar at the bottom.

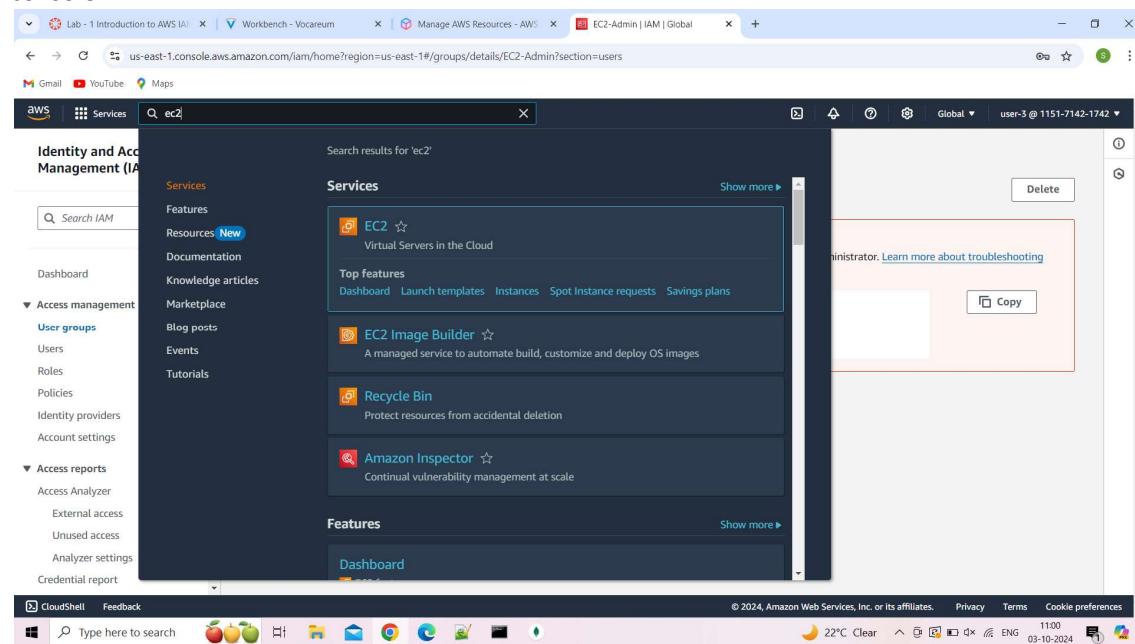
Step 33 : Choose Sign Out

This screenshot is identical to the previous one, showing the failed bucket creation dialog. However, the "Sign out" button in the bottom right corner of the dialog is now highlighted with a red box, indicating it is the next step to take.

Step 34 :Paste the IAM users sign-in link into your private window and press Enter.Signin with: IAM user name: user-3 Password: Lab-Password3



Step 35: In the search box to the right of Services, search for and choose EC2 to open the EC2 console.



The screenshot shows the AWS Management Console with the EC2 Instances page open. There are two instances listed: 'LabHost' and 'Bastion Host'. The 'LabHost' instance is selected. A context menu is open over the 'LabHost' row, with the 'Stop instance' option highlighted.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
LabHost	i-04ffaa08c7b5bdf67	Running	t2.micro	2/2 checks passed	User: amznaws: us-east-1a	ec2-98-81-250-37	98.81.250.37
Bastion Host	i-079b7f1cb2fc734bd	Running	t2.micro	2/2 checks passed	User: amznaws: us-east-1a	ec2-54-151-110-111	54.151.110.111

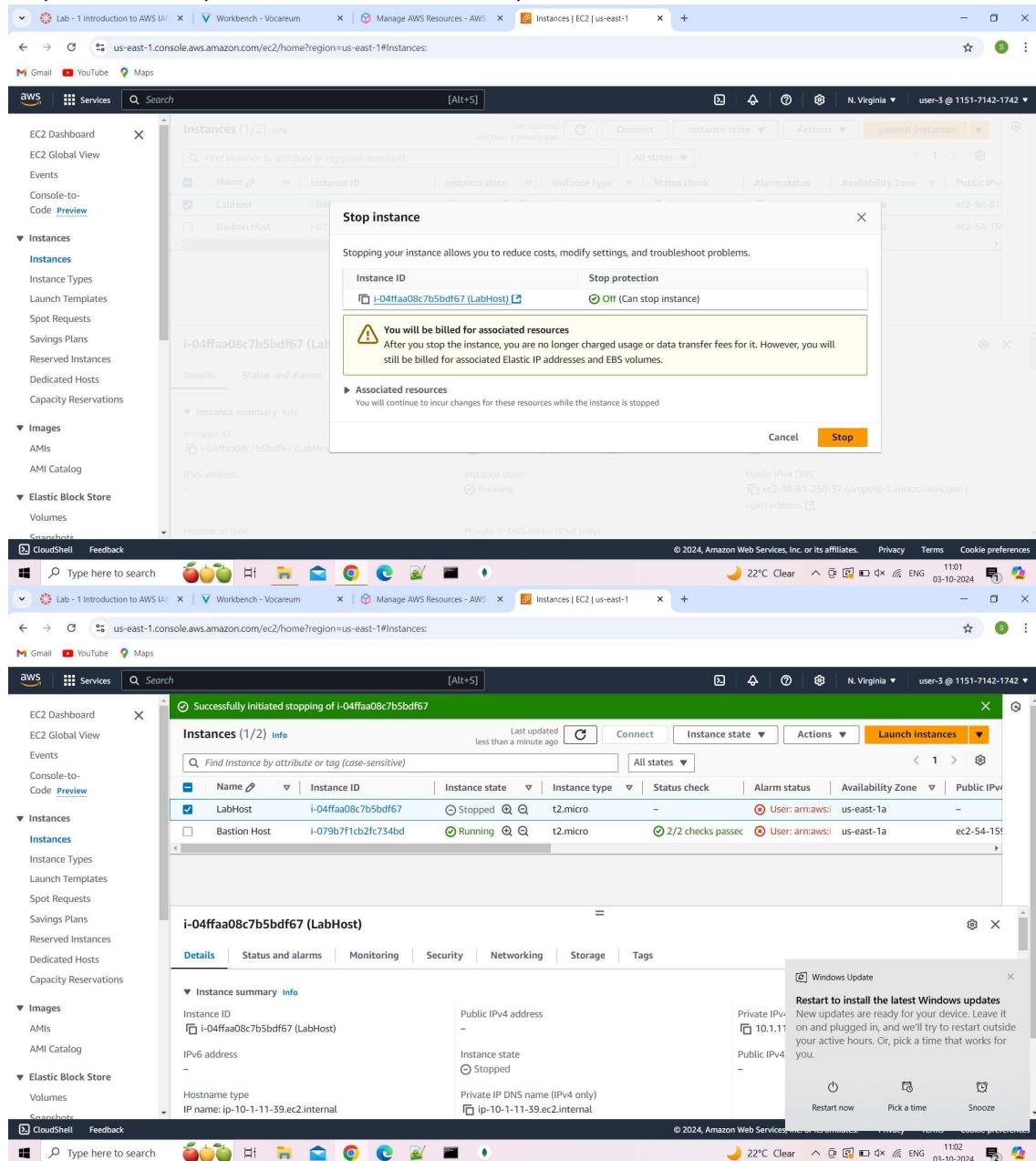
Step 36 :Select the instance named LabHost .

Step 37 : In the Instance state menu, choose Stop instance.

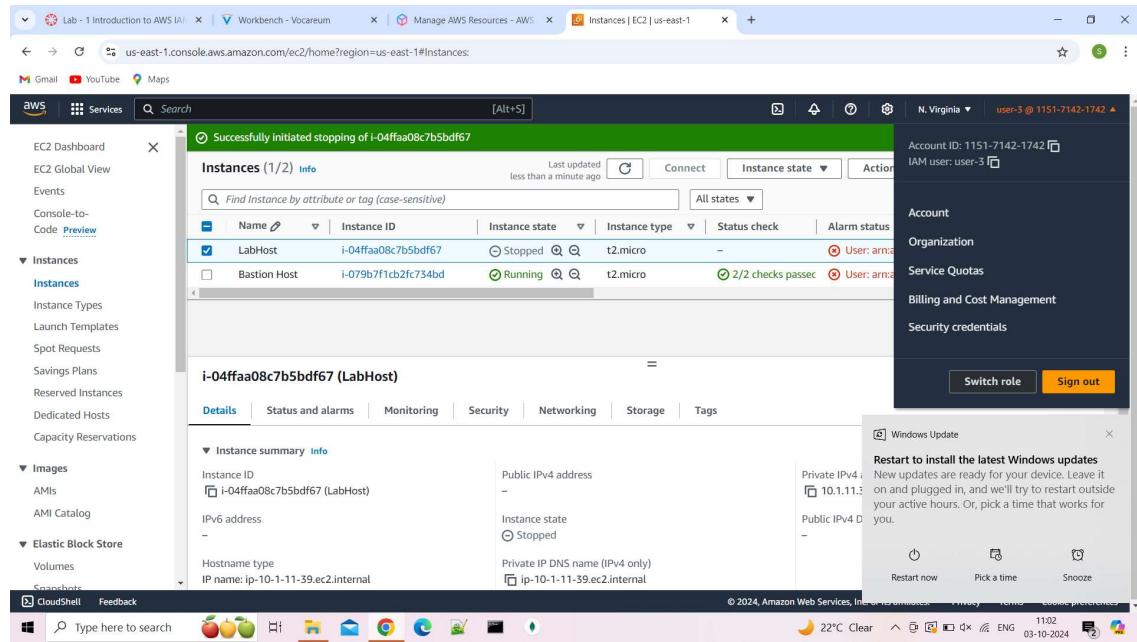
The screenshot shows the AWS Management Console with the EC2 Instances page open. The 'LabHost' instance is selected. A context menu is open over the 'LabHost' row, with the 'Stop instance' option highlighted.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
LabHost	i-04ffaa08c7b5bdf67	Running	t2.micro	2/2 checks passed	User: amznaws: us-east-1a	ec2-98-81-250-37	98.81.250.37
Bastion Host	i-079b7f1cb2fc734bd	Running	t2.micro	2/2 checks passed	User: amznaws: us-east-1a	ec2-54-151-110-111	54.151.110.111

Step 38 : In the Stop instance window, choose Stop.



Step 39 : Click on Sign Out .



Step 40: Close your private window