

Class – M.Sc. (Computer Science) Part II- Sem III

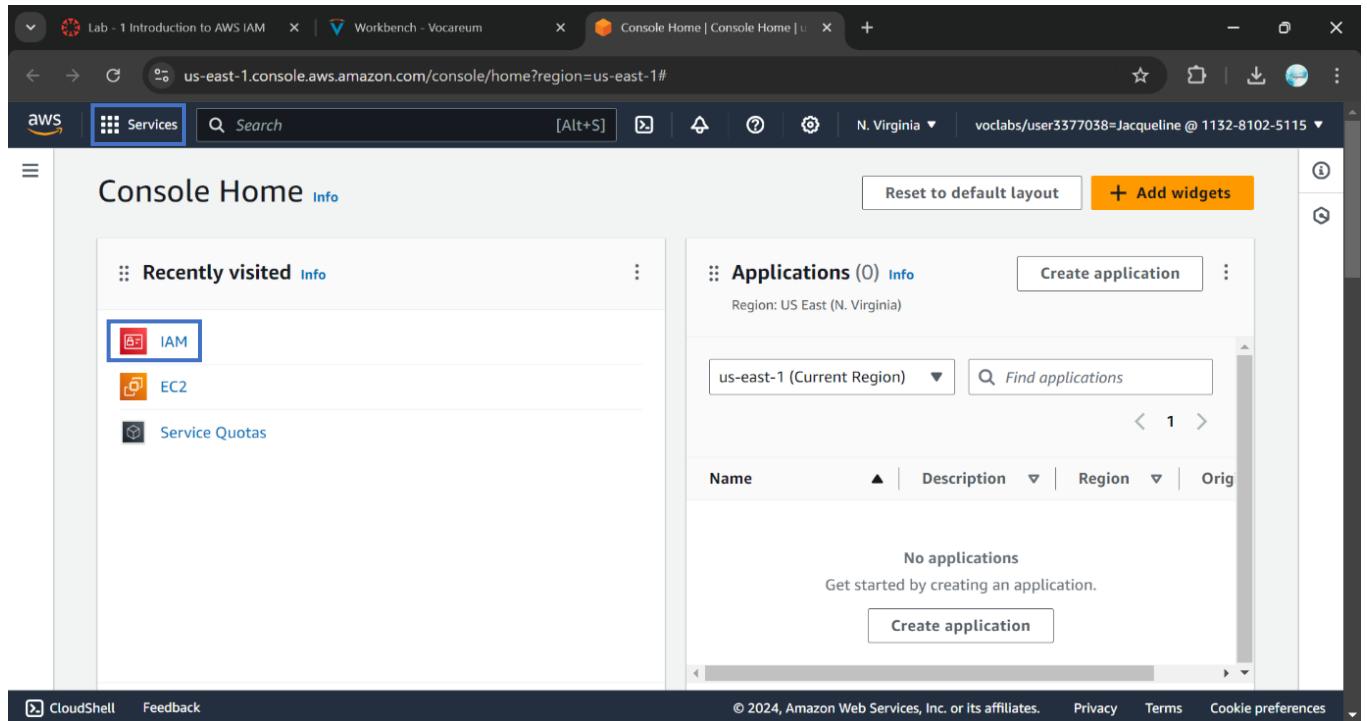
Cloud Computing Practical Assignment No 6

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

Prepare Screen shots file and write down the steps.

Make single word or PDF file.

Step 1: Search for IAM in search bar next to services tab.



Step 2: In the navigation pane on the left, choose **Users**

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu is open under 'Access management', with 'Users' selected. The main area displays 'IAM resources' with counts: User groups (3), Users (4), Roles (18), Policies (1), and Identity providers (0). Below this, a 'What's new' section lists recent updates from the AWS IAM Access Analyzer.

User groups	Users	Roles	Policies	Identity providers
3	4	18	1	0

What's new:

- AWS IAM Access Analyzer now offers policy checks for public and critical resource access. 3 months ago
- AWS IAM Access Analyzer now offers recommendations to refine unused access. 3 months ago

Step 3: These are the users which are already been created.

The screenshot shows the 'Users' page in the AWS IAM service. The sidebar menu has 'Users' selected under 'Access management'. The main table lists four users: 'awsstudent', 'user-1', 'user-2', and 'user-3'. Each user row includes columns for User name, Path, Group, Last activity, and MFA. All users show 'Access denied' in the 'Access' column.

User name	Path	Group	Last activity	MFA
awsstudent	/	Access denied	Access denied	Access denied
user-1	/spl66/	0	-	-
user-2	/spl66/	0	-	-
user-3	/spl66/	0	-	-

Step 4: Click on user-1 link and it will open the summary page in which there are no permissions given to user-1

The screenshot shows the AWS IAM User Details page for a user named 'user-1'. The left sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings'), and 'Access reports'. The main content area displays the 'Summary' of 'user-1'. Key details shown include:

ARN	Console access	Access key 1
arn:aws:iam::113281025115:user-/spl66/user-1	Enabled without MFA	AKIARUYATIRN5ZD2SY6J - Active Never used. Created today.
Created	Last console sign-in	Access key 2
September 10, 2024, 20:08 (UTC+05:30)	Never	Create access key

Below the summary, tabs for 'Permissions', 'Groups', 'Tags (1)', 'Security credentials', and 'Access Advisor' are visible. The 'Permissions' tab is selected. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

This screenshot is identical to the one above, showing the 'user-1' details page. However, it specifically highlights the 'Permissions' section. The 'Permissions policies (0)' section is shown, which states: 'Permissions are defined by policies attached to the user directly or through groups.' Below this, there is a search bar, a filter dropdown set to 'All types', and a table header with columns for 'Policy name', 'Type', and 'Attached via'. The table body below the header displays the message 'No resources to display'.

Step 5: Now go to groups, there are no groups created for user-1.

The screenshot shows the AWS IAM User details page for a user named 'user-1'. The 'Groups' tab is selected. Key information displayed includes:

- Created:** September 10, 2024, 20:08 (UTC+05:30)
- Last console sign-in:** Never
- Access key 2:** Access key 2 (with a 'Create access key' link)

The 'User groups membership' section indicates "No resources" and states "This user does not belong to any groups."

Navigation pane (Left):

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups
 - Users** (selected)
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports

Bottom navigation:

- CloudShell
- Feedback
- © 2024, Amazon Web Services, Inc. or its affiliates.
- Privacy
- Terms
- Cookie preferences

Step 6: Now go to the navigation pane on the left, choose **User groups**.

The screenshot shows the AWS IAM User groups page. The 'User groups' tab is selected, displaying three groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	5 minutes ago
EC2-Support	0	Defined	5 minutes ago
S3-Support	0	Defined	5 minutes ago

Navigation pane (Left):

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups** (selected)
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports

Bottom navigation:

- https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/group...
- © 2024, Amazon Web Services, Inc. or its affiliates.
- Privacy
- Terms
- Cookie preferences

Step 7: Now click on EC2 Support link and go in permissions tab it will show the summary page and then click on '+' sign in policy name tab and view the contents in it.

The screenshot shows the AWS IAM Groups Details page for the 'EC2-Support' group. The group was created on September 10, 2024, at 20:08 (UTC+05:30). It has an ARN of arn:aws:iam::113281025115:group/spl66/EC2-Support. The 'Permissions' tab is selected, showing one attached policy: 'AmazonEC2ReadOnlyAccess'. This policy is AWS managed and provides read-only access to Amazon EC2 via the AWS Management Console. The policy document is displayed below:

```
5   "Effect": "Allow",
6   "Action": "ec2:Describe*",
7   "Resource": "*"
8 },
9 {
10   "Effect": "Allow",
11   "Action": "elasticloadbalancing:Describe*",
12   "Resource": "*"
13 }
```

Step 8: Now click on ‘-’ to close the contents which are visible.

The screenshot shows the same AWS IAM Groups Details page for the 'EC2-Support' group. The 'AmazonEC2ReadOnlyAccess' policy is expanded, showing its JSON document. The 'Copy JSON' button is visible next to the policy name.

```
5   "Effect": "Allow",
6   "Action": "ec2:Describe*",
7   "Resource": "*"
8 },
9 {
10   "Effect": "Allow",
11   "Action": "elasticloadbalancing:Describe*",
12   "Resource": "*"
13 }
```

Step 9: Now click on S3 Support link from user groups and go in permissions tab it will show the summary page and then click on ‘+’ sign in policy name tab and view the contents in it.

The screenshot shows the AWS IAM Groups Details page for the 'S3-Support' group. The group was created on September 10, 2024, at 20:08 (UTC+05:30). It has an ARN of arn:aws:iam::113281025115:group/spl66/S3-Support. The 'Permissions' tab is selected, showing one attached policy: 'AmazonS3ReadOnlyAccess'. This policy is AWS managed and provides read-only access to all buckets via the AWS Management Console. The policy JSON is displayed below:

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": [
7          "s3:Get*",
8          "s3>List*",
9          "s3:Describe*",

```

Step 10: Now click on ‘-’ to close the contents which are visible.

The screenshot shows the same AWS IAM Groups Details page, but the policy content for 'AmazonS3ReadOnlyAccess' is now expanded. The JSON code is fully visible:

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": [
7          "s3:Get*",
8          "s3>List*",
9          "s3:Describe*",

```

Step 11: Now click on EC2-admin link from user groups and go in permissions tab it will show the summary page and then click on ‘+’ sign in policy name tab and view the contents in it.

The screenshot shows the AWS IAM Groups Details page for the 'EC2-Admin' group. The 'Permissions' tab is selected. Under 'Permissions policies', there is one policy named 'EC2-Admin-Policy'. The policy details are shown as follows:

```
1: { "Version": "2012-10-17", "Statement": [ 2: { "Action": [ "ec2:Describe*", "ec2:StartInstances", "ec2:StopInstances" ], "Resource": [ "*" ], "Effect": "Allow" } ] }
```

Step 12: Now click on ‘-’ to close the contents which are visible.

The screenshot shows the same AWS IAM Groups Details page for the 'EC2-Admin' group. The 'Permissions' tab is selected. Under 'Permissions policies', the 'EC2-Admin-Policy' is expanded, showing its JSON content. The policy details are identical to the previous screenshot.

```
1: { "Version": "2012-10-17", "Statement": [ 2: { "Action": [ "ec2:Describe*", "ec2:StartInstances", "ec2:StopInstances" ], "Resource": [ "*" ], "Effect": "Allow" } ] }
```

Step 13: Now in the left navigation pane, choose **User groups** and click on S3-Support group link and click on ‘Add users’ to add users in it.

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 left sidebar is open, showing 'Access management' with 'User groups' selected. The main content area displays the 'S3-Support' user group details under the 'Summary' tab. It shows the user group name 'S3-Support', creation time 'September 10, 2024, 20:08 (UTC+05:30)', and ARN 'arn:aws:iam::113281025115:group/spl66/S3-Support'. Below this, there are tabs for 'Users' (selected), 'Permissions', and 'Access Advisor'. A section titled 'Users in this group (0)' has a 'Add users' button highlighted with a red box.

Step 14: Select user-1 and then click on Add users.

The screenshot shows the 'Add users' dialog box from the AWS IAM console. The URL is us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/details/S3-Support/add-users. On the left, a list of users is shown: 'user-1' (selected and highlighted with a blue border), 'user-2', and 'user-3'. To the right of the list, there are columns for 'Actions', 'Count', 'Last modified', and 'Last modified ago'. At the bottom right of the dialog, there are 'Cancel' and 'Add users' buttons, with 'Add users' also highlighted with a red box.

Step 15: Now the user-1 is been added to S3-Support group.

Identity and Access Management (IAM)

1 user added to this group.

S3-Support	September 10, 2024, 20:08 (UTC+05:30)	arn:aws:iam::113281025115:group/spl66/S3-Support
------------	------------------------------------------	--------------------------------------------------

Users (1) Permissions Access Advisor

Users in this group (1)

User name	Groups	Last activity	Creation time
user-1	1	None	9 minutes ago

CloudShell Feedback

Step 16: Now in the left navigation pane, choose **User groups** and click on EC2-Support group link and click on ‘Add users’ to add users in it.

Identity and Access Management (IAM)

IAM > User groups > EC2-Support

EC2-Support Info

Delete Edit

Summary

User group name	Creation time	ARN
EC2-Support	September 10, 2024, 20:08 (UTC+05:30)	arn:aws:iam::113281025115:group/spl66/EC2-Support

Users Permissions Access Advisor

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

CloudShell Feedback

Step 17: Select user-2 and then click on Add users.

The screenshot shows the 'Add users' dialog in the AWS IAM console. A list of users is displayed, with 'user-2' selected. The 'Add users' button is visible at the bottom right.

User	Count	Last Activity
user-1	1	None 15 minutes ago
user-2	0	None 15 minutes ago
user-3	0	None 15 minutes ago

Add users

Step 18: Now the user-2 is been added to EC2-Support group.

The screenshot shows the 'EC2-Support' group details page in the AWS IAM console. It displays the summary information for the group and a list of users in the group.

Summary

User group name	Creation time	ARN
EC2-Support	September 03, 2024, 12:05 (UTC+05:30)	arn:aws:iam::430254637503:group/spl66/EC2-Support

Users (1)

User name	Count	Last activity
user-2	1	None 16 minutes ago

Add users

Step 19: Now in the left navigation pane, choose **User groups** and click on EC2-Admin group link and click on 'Add users' to add users in it.

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-Admin?section=users. The left sidebar is open, showing 'Access management' with 'User groups' selected. The main content area displays the 'EC2-Admin' user group details. The 'Summary' section shows the group name 'EC2-Admin', creation time 'September 10, 2024, 20:08 (UTC+05:30)', and ARN 'arn:aws:iam::113281025115:group/spl66/EC2-Admin'. Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor', with 'Users' selected. A table titled 'Users in this group (0)' is shown, along with 'Add users' and 'Remove' buttons. The bottom navigation bar includes CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

Step 20: Select user-3 and then click on Add users.

The screenshot shows the 'Add users' page for the EC2-Admin group. The URL is us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/details/EC2-Admin/add-users. On the left, a sidebar shows 'User groups' with 'User groups' selected. The main area lists three users: 'user-1', 'user-2', and 'user-3'. The checkbox next to 'user-3' is checked, and the entire row is highlighted with a blue border. To the right of the table, there are columns for 'Count', 'Last modified', and 'Last modified ago'. At the bottom right are 'Cancel' and 'Add users' buttons. A red box highlights the 'user-3' row.

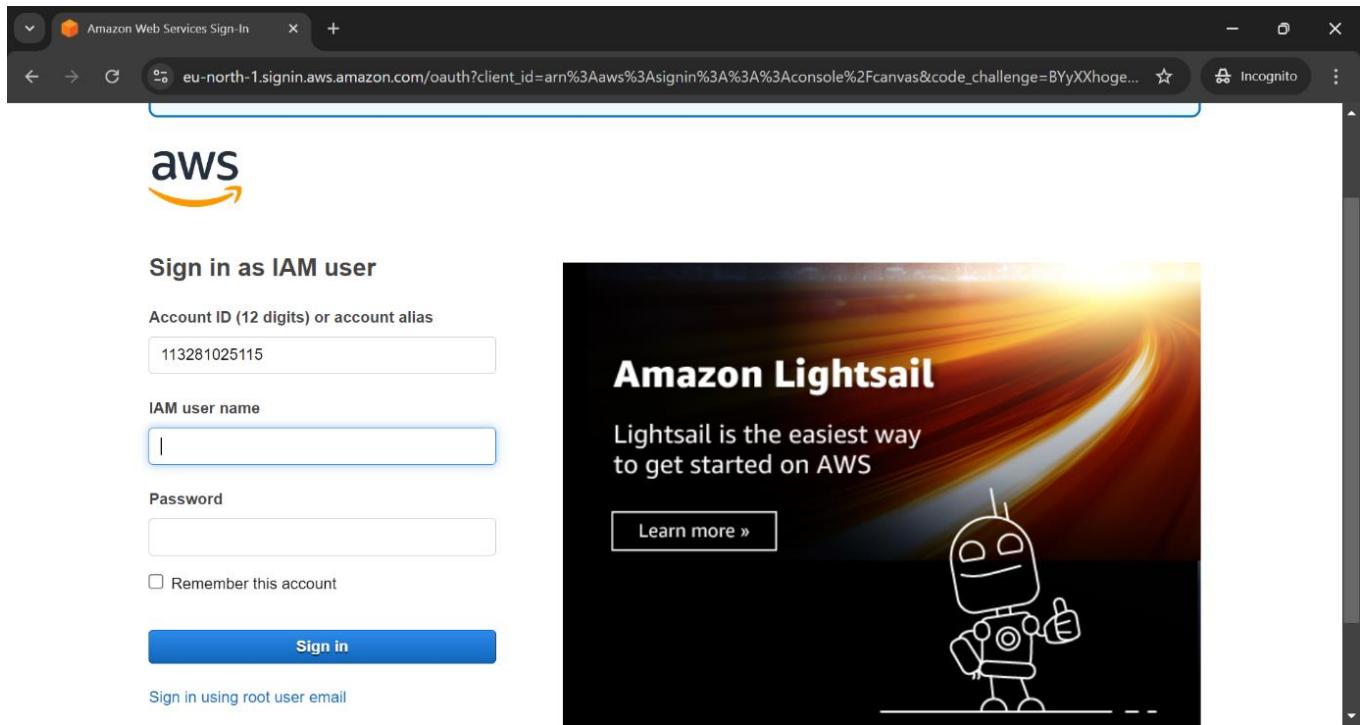
Step 21: Now the user-3 is been added to EC2-Admin group.

The screenshot shows the AWS IAM Groups details page. A green banner at the top states "1 user added to this group." Below it, a table lists the user "EC2-Admin" who was added on "September 10, 2024, 20:08 (UTC+05:30)" with the ARN "arn:aws:iam::113281025115:group/spl66/EC2-Admin". The main content area shows a table titled "Users in this group (1)". The table has columns for User name, Groups, Last activity, and Creation time. It shows one user named "user-3".

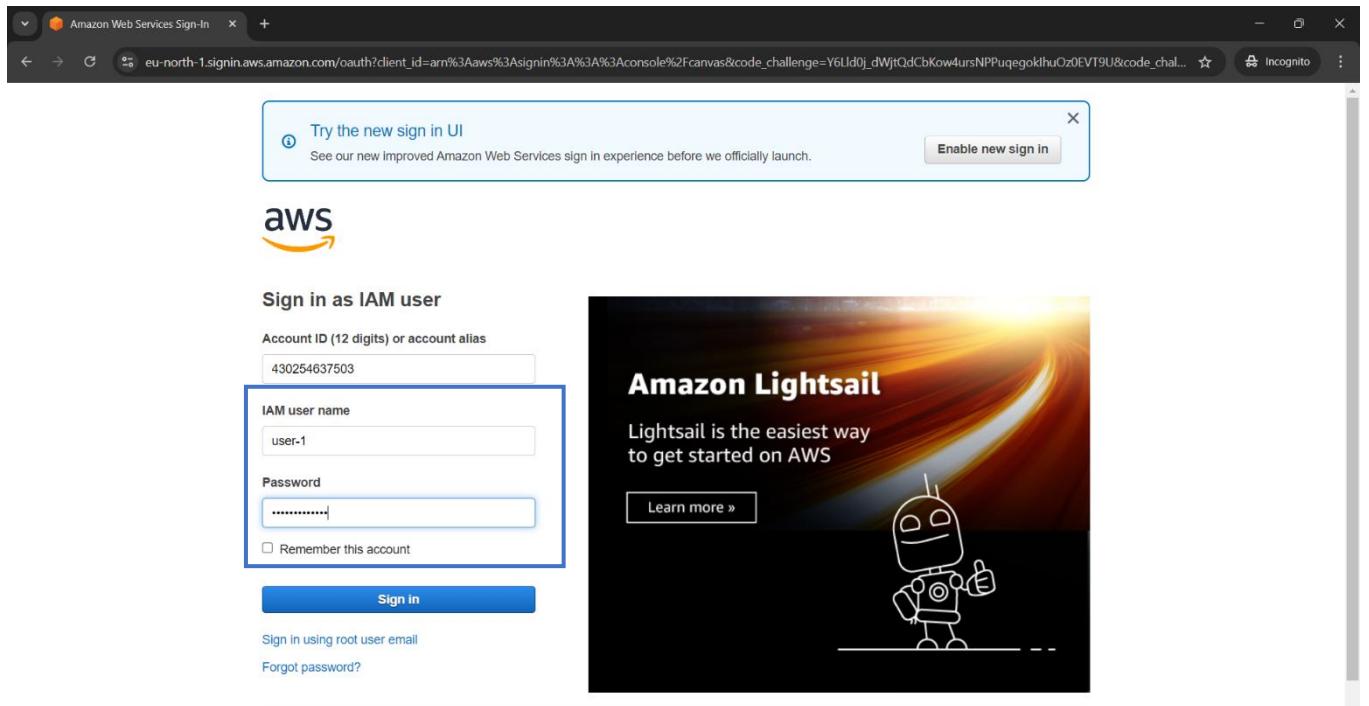
Step 22: Now go to dashboard and copy the Sign-in link provided on the right side.

The screenshot shows the AWS IAM Dashboard. In the "AWS Account" section, the "Sign-in URL for IAM users in this account" is displayed as a blue-bordered box: <https://113281025115signin.aws.amazon.com/console>.

Step 23: Paste this link in New incognito tab of google chrome.



Step 24: Now sign in using user-1 credentials.



Step 25: Now search for S3 in search bar next to services.

The screenshot shows the AWS Console Home page. On the left, under 'Recently visited', the 'S3' icon is highlighted with a blue border. The main content area displays various services: Applications (0), AWS Health, Cost and usage, and Welcome to AWS. The Applications section shows a single entry with an 'Access denied' message. The bottom navigation bar includes CloudShell, Feedback, and links to 2024 Amazon terms and cookie preferences.

Step 26: Select the name of the bucket that exists in the account and browse the contents. Since your user is part of the S3-Support Group, they have permission to view a list of Amazon S3 buckets and the contents.

The screenshot shows the AWS S3 home page. The left sidebar includes options like Buckets, Access Grants, and Storage Lens. The main area displays an 'Account snapshot' and a table for 'General purpose buckets'. One bucket, 'samplebucket--a5c441e0', is listed with details: Name (samplebucket--a5c441e0), AWS Region (US East (N. Virginia) us-east-1), IAM Access Analyzer (View analyzer for us-east-1), and Creation date (September 3, 2024, 12:05:11 (UTC+05:30)).

Name	AWS Region	IAM Access Analyzer	Creation date
samplebucket--a5c441e0	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 3, 2024, 12:05:11 (UTC+05:30)

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled "Amazon S3" contains sections for "Buckets", "Access Grants", "Access Points", "Object Lambda Access Points", "Multi-Region Access Points", "Batch Operations", "IAM Access Analyzer for S3", and "Storage Lens". Under "Storage Lens", there are links for "Dashboards", "Storage Lens groups", and "AWS Organizations settings". A "Feature spotlight" section is also present. At the bottom of the sidebar are links for "CloudShell" and "Feedback". The main content area shows the "samplebucket--a5c441e0" bucket. The "Objects" tab is selected, showing a table with one row: "No objects". Below the table, it says "You don't have any objects in this bucket." There are buttons for "Upload" and "Find objects by prefix". The top navigation bar shows the URL "us-east-1.console.aws.amazon.com/s3/buckets/samplebucket--a5c441e0?region=us-east-1&bucketType=general&tab=objects". The top right corner shows the user "user-1 @ 4302-5463-7503" and the region "N. Virginia".

Step 27: Now search for EC2 console and see if you have permission or not. It will give error messages as it states You are not authorized to perform this operation. This is because this user has not been granted any permissions to access Amazon EC2.

The screenshot shows the AWS EC2 console interface. The left sidebar includes sections for "EC2 Dashboard", "Instances", "Images", and "Elastic Block Store". The main content area features a "Resources" summary card with various metrics like Instances (running), Auto Scaling Groups, Capacity Reservations, etc., each followed by an "API Error" message. Below this are "Launch instance" and "Service health" cards, both of which also display "API Error" messages. A prominent red error box on the right side states "An error occurred" and "An error occurred checking for a default VPC", with a "Diagnose with Amazon Q" button. The top navigation bar shows the URL "us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home". The top right corner shows the user "user-1 @ 4302-5463-7503" and the region "N. Virginia".

Step 28: Now sign out of user-1.

The screenshot shows the AWS EC2 Dashboard in the N. Virginia region. The top right corner displays the account ID (1132-8102-5115) and IAM user (user-1). A sidebar on the left lists various EC2 services and resources. In the center, a 'Resources' section shows a grid of status cards for Instances (running: 0), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Key pairs, Load balancers, Security groups, and Snapshots. Below this is a 'Launch instance' button and a 'Service health' section. On the far right, a vertical sidebar provides links to Account, Organization, Service Quotas, Billing and Cost Management, and Security credentials. At the bottom right, there are 'Switch role' and 'Sign out' buttons.

Step 29: Now sign in as user-2 again in the same link which was earlier copied.

The screenshot shows the AWS Sign-In page for user-2. The top bar indicates the user is signing in as 'user-2'. The main form asks for an 'Account ID (12 digits) or account alias' (430254637503) and 'IAM user name' (user-2). It includes fields for 'Password' and a 'Remember this account' checkbox. A 'Sign in' button is at the bottom. To the right, there's a promotional banner for 'Amazon Lightsail' featuring a cartoon robot and the text 'Lightsail is the easiest way to get started on AWS'. A 'Learn more »' link is also present.

The screenshot shows the AWS Console Home page. On the left, there's a 'Recently visited' section with links to S3 and EC2. Below it are sections for 'Welcome to AWS', 'AWS Health', and 'Cost and usage'. The main focus is the 'Applications' section, which displays a single item: 'Access denied'. A 'Create application' button is available at the top right of this section. The bottom of the page includes standard navigation links like CloudShell, Feedback, and copyright information for 2024.

Step 30: Now go to instances and select the instance as Labhost and stop that instance. It will give error message as user-2 only has read only permission.

The screenshot shows the AWS Instances page. The left sidebar lists various EC2 management options like Dashboard, Global View, Events, and Instances. Under Instances, it shows sub-options for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, and Reservations. The main content area shows a specific instance named 'i-071a9a5112b078c2b'. A large red error message box is displayed, stating: 'Failed to stop the instance i-071a9a5112b078c2b. You are not authorized to perform this operation. User: arn:aws:iam:430254637503:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:430254637503:instance/-071a9a5112b078c2b because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: 9U23TL9sYuyKXFG1mAMToINCMHWEzy-3fxON2qifgyMqlA3Zbsvll_COUG1Gpz2MaLGlfPvx_d0M25wqNebf4jRBG-CmdT6xhJ2zHXDNQYBpHqpxOjjpdCYUEMRxHL7nm5iyVJ4ALUAavI2qqRXjgmgssYpVwmsxf7XhfnUslylhqOc3_DPJMk2tQZNJdn7D-SZ8_p1965TZQvSoD5V9xvNIPRuuOJzdee6PouXbxvHmzqkRemhM2J9JhbL5aGncwihN7rCYFZU6jjabesj7sbyCFHXIDLT5FMUQyeVwc4fLF-6BVXynPi7M-Jb7_EETbeArDR3YiWPLF9-1809CQyqp2oSwW1lygSaM0G6TelORuCltyJ4HN0001mzjArI9_hk5tLTvhHhT0IU1MigSBwvSsm_CBOE14u3leog2xf0G9o4P6fz8dyb_w_Uw50LdWBeEbZDtD4T7562ZHGrpTq9s3tL-GirdmDfub7WQd0l7XY20nPo4S8wzIgtghpMax62E4s4H5Zj3GFa5Q-psgwZvkyFlep-4HSni3ZuBcMRNzq4N70yCZUUbddYOuQfTeCfX61em8kwuOpurn680jEM5LW_Byt76fCOSVbGz_7e_6p2nwlfNed713.nJKOrYHCSw.jpgz64lVMN7wvEPQnxWDv8hjCeeBlyPubrnWzq2uY_K9ugn7nTclLeCYEB8UsjkVv1ajYohCku0OQYs4aber4xfhKLdn34NBAHHKEK0db2vT9JrBruGJVLlwPl6fAC9qvksJupq4cvnct10my6Kx8ycht8Duxiu66Zc-prHPLGLMd68hyaM69MWPyFwuqxqfwmXRig5H4722GaxsIMxAyGf_koyX1oJekAMchlx55-PhmLuB30sK7zQW344Y8EW6Cob7dbggSj4AS5FLyUdtRwmBjm-Fyq_z-G705Vq7K3Ub_p8KO2G6V32P_tcbWJ2DXWGA6sSwdyenXOsxhi373oS2ay1QVYqyVm4bDzjJ291gCdDqkaRg'. Below the error message, the instance details are shown, including its ID, IP addresses, state, and DNS name.

Step 31: Now sign out of user-2.

The screenshot shows the AWS Management Console for EC2. A modal window displays an error message: "Failed to stop the instance i-0746b9f6291600da5". The message states: "You are not authorized to perform this operation. User: arn:aws:iam::113281025115:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:113281025115:instance/i-0746b9f6291600da5 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: ecFqAJseE3EDqcC2xAg9UNK_WHatxDV63wYH8nj7zRY9cwtsM5VrUsOzfGVSa19Zz8IDL1qeZDSN3hOlD02PmXWpVytJdZLremYa4hmq6zQs5t6ioYvhQXYi49g2EVL6clVS2cDoQVHPpdMSrYcra7hKg113N13kdOFmdlid_RbqpGA5q8EGtSsMjZa64dTjRwnn9_BaZcP8RZNEA4cgNSVRofvILMuGHcepWB2JV02ATBjVgP0O5ffyXfJEvfRfdPNXj7L2-ZygTkn6R5LlnU2esbvwlkLTMr6EQJLzL7-ESE-cYhcoUoieNrzsbQbjm4e9c1QT9dgxDoiFa1rv_WltzP-oi8SXkneaxdtpeni75x7NvgDdvEpDxyS4e5J9OUUGo15bnmT3LW2wJpo_-mLfXJqBuV28w0gsdoygnO32V2uHi-peCyVLdmepsY7hAxDHzd_dxUfBev22djduBjFLsNCNF193FVjfCZ-skU6q7cTe4EUdb_SRmolzPjjDhRZXogIdue1xreyFRNRalYxbYLts0FLGxLLi3zKeEvu8V9Bhisaxi9mdDSi5PTZklyJuE9FFCTPo9d95nPNh5-feLOULtJT8bOku9LUAc7ju87Wqx12WaWmfAXCB4q_QF9QKTdp7b2bFwNculuiPBY1KrPQ7lrQSf-A-r653EqjsSj-K37iwxmSe4bomeMklBbgmqdsM4hWcvZ-8VntibXRlb_mZ975OTJynwnMb3QkQduRQRptYpiBbpbt4oXduAdHtO8KvhioAK0yWUL_-HL4IKU27OS9_CnzMRkx6B2f56Dv3xQDIQH5AEFIh7N8vyORBgWj-iog-boyEhDwf_jukMvX8VY-61oasicX0ZA22S_Fe-C43LDGkaP58oFFY5alrOZVc698D4La_iYHTZ_tGMwriSMa1mF7KsxwP7rZ5-".

On the right side of the console, there is a sidebar with navigation links: Account ID: 1132-8102-5115, IAM user: user-2, Account, Organization, Service Quotas, Billing and Cost Management, Security credentials, Switch role, and Sign out.

Step 32: Now sign in again as user-3 from the link that was earlier copied and choose instances and select the instance as Labhost.

The screenshot shows the AWS Sign-In page for user-3. The page includes a "Try the new sign in UI" banner with a "Enable new sign in" button. The main sign-in form has fields for "Account ID (12 digits) or account alias" (430254637503), "IAM user name" (user-3), "Password" (redacted), and a "Remember this account" checkbox. Below the form is a "Sign in" button. At the bottom of the page are links for "Sign in using root user email" and "Forgot password?". To the right of the sign-in form is an advertisement for Amazon Lightsail, featuring a cartoon character and the text "Amazon Lightsail" and "Lightsail is the easiest way to get started on AWS".

The screenshot shows the AWS Console Home page. On the left, there's a 'Recently visited' section with links to EC2 and S3. Below it are sections for 'Welcome to AWS' and 'AWS Health'. On the right, there's an 'Applications' section with a table header for Name, Description, Region, and Originating account. A single row is shown with a red border and the message 'Access denied'. At the bottom, there are links for 'View all services', 'Go to myApplications', and navigation links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Step 33: Now say stop instance, the instance will stop as user-3 is an EC2 Administrator, so you now have permissions to Stop the Amazon EC2 instance.

The screenshot shows the AWS Instances EC2 page. The left sidebar includes options like EC2 Dashboard, EC2 Global View, Events, and various instance-related links. The main area displays a table of instances with two entries: 'Bastion Host' and 'LabHost'. The 'LabHost' row is selected. A context menu is open over the 'Actions' button, with 'Stop instance' highlighted. The 'Details' tab of the instance card for 'i-071a9a5112b078c2b (LabHost)' is visible, showing basic details like Instance ID, Public IPv4 address (54.88.219.36), and Instance state (Running).

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

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Bastion Host	i-024268985b9cdb6c6	Running	t2.micro	2/2 checks passed	User: arm:aws:1	us-east-1a	ec2-54-
LabHost	i-071a9a5112b078c2b	Stopped	t2.micro	-	User: arm:aws:1	us-east-1a	-

A modal window titled "Select an instance" is overlaid on the list, indicating that an action is being performed on the selected instance.

Step 34: Now sign out of user-3 and close the private window tab.

The screenshot shows the AWS Management Console with the EC2 Instances page. A success message at the top indicates that the instance was stopped successfully:

Successfully initiated stopping of i-0746b9f6291600da5

The instance list shows the "LabHost" instance is now in the "Stopped" state:

Name	Instance ID	Instance state	Instance type
Bastion Host	i-0a0c6eef6d58a2d71	Running	t2.micro
LabHost	i-0746b9f6291600da5	Stopped	t2.micro

The instance details page for "i-0746b9f6291600da5 (LabHost)" is displayed. In the top right corner of the sidebar, the "Sign out" button is highlighted.

Step 35: Now sign out of your account and end the lab.

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and links for 'Dashboard', 'Access management', 'Access reports', and 'Account settings'. The main area displays 'IAM resources' with counts: 3 User groups, 4 Users, 18 Roles, and 1 Policies. Below this is a 'What's new' section with two items about AWS IAM Access Analyzer. On the right, there's a sidebar with 'Account', 'Organization', 'Service Quotas', and 'Billing and Cost Management'. At the bottom right are 'Switch role' and 'Sign out' buttons. The URL in the address bar is <https://console.aws.amazon.com/iam/home?region=us-east-1#/home>.

The screenshot shows the AWS Academy Learner Lab interface. On the left, there's a sidebar with 'Home', 'Modules', 'Discussions', 'Grades', 'Lucid', 'Courses', 'Calendar', 'Inbox', 'History', and 'Help'. The main area has a terminal window showing a session for user 'eee_W_3374460@runweb133396:~\$'. To the right of the terminal is a code editor with a snippet of Python code related to AWS Lambda and CodeWhisperer. At the bottom are 'Previous' and 'Next' buttons. The URL in the address bar is <https://awsacademy.instructure.com/courses/86436/modules/items/7859818>.

