

## Lab Overview

**AWS Identity and Access Management (IAM)** is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage **users**, **security credentials** such as access keys, and **permissions** that control which AWS resources users can access.

### Topics covered

This lab will demonstrate:

- Exploring pre-created **IAM Users and Groups**
- Inspecting **IAM policies** as applied to the pre-created groups
- Following a **real-world scenario**, adding users to groups with specific capabilities enabled
- Locating and using the **IAM sign-in URL**
- **Experimenting** with the effects of policies on service access

## AWS Identity and Access Management

AWS Identity and Access Management (IAM) can be used to:

- **Manage IAM Users and their access:** You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
- **Manage IAM Roles and their permissions:** An IAM Role is similar to a User, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be *assumable* by anyone who needs it.
- **Manage federated users and their permissions:** You can enable *identity federation* to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.

## Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

**Caution:** You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Warning:** Do not change the **Region** unless instructed.

## Task 1: Explore the Users and Groups

In this task, you will explore the Users and Groups that have already been created for you in IAM.

- At the top of the AWS Management Console, in the search bar, search for and choose IAM

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top contains 'IAM'. Below the search bar, the 'Services' section is expanded, showing three items: 'IAM' (selected), 'IAM Identity Center', and 'Resource Access Manager'. The 'Features' section below shows 'IAM Access analyzer for S3'. A sidebar on the left lists recent services: Services, Features, Resources (New), Documentation, Knowledge articles, Marketplace, Blog posts, Events, and Tutorials. At the bottom of the sidebar, there are 'Were these results helpful?' buttons for 'Yes' and 'No'.

- In the navigation pane on the left, choose **Users**.

The following IAM Users have been created for you:

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

The screenshot shows the IAM Users page. The left navigation pane is collapsed, showing 'Identity and Access Management (IAM)' and 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management). The main content area shows a table titled 'Users (3)'. The table has columns: User name, Path, Group, Last activity, MFA, and Password age. The data is as follows:

User name	Path	Group	Last activity	MFA	Password age
user-1	/spl66/	-	-	-	15 minutes
user-2	/spl66/	-	-	-	15 minutes
user-3	/spl66/	-	-	-	15 minutes

- Choose **user-1**.

This will bring to a summary page for user-1. The **Permissions** tab will be displayed.

4. Notice that user-1 does not have any permissions.

**Note:** You should see an **Unexpected error** message. This is normal.

The screenshot shows two side-by-side views of the AWS IAM User Details page for a user named "user-1".

**Left View (Top):** The "Permissions" tab is selected. It displays the "Permissions policies (0)" section, which states: "Permissions are defined by policies attached to the user directly or through groups." Below this is a search bar and a filter section labeled "Filter by Type". A note at the bottom says "No resources to display".

**Right View (Bottom):** The "Permissions boundary (not set)" section is shown. It contains a red-bordered box with the following error message:  
- **Access denied to access-analyzer>ListPolicyGenerations**  
- You don't have permission to `access-analyzer>ListPolicyGenerations`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors](#).  
- **User:** arn:aws:sts::042022252145:assumed-role/AWSLabsUser-ttWUNESeY5XCISYpdJENor/01599bbc-ff95-45 d8-9817-7c16a4975cb4  
- **Action:** access-analyzer>ListPolicyGenerations  
- **On resource(s):** arn:aws:access-analyzer:us-east-1:042022252145:  
- **Context:** a policy explicitly denies the action

5. 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 left navigation pane is visible with options like Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, Resource analysis). The main content area is titled 'Summary' and shows ARN (arn:aws:iam::042022252145:user/spl66/user-1), Console access (Enabled without MFA), and Last console sign-in (Never). Below this is a 'User groups membership' section with tabs for Permissions, Groups (which is selected), Tags, Security credentials, and Last Accessed. The 'Attached policies' table is empty, showing 'No resources' and the message 'This user does not belong to any groups.' There is a 'Remove' button and an 'Add user to groups' button. At the bottom right are links for CloudShell, Feedback, and the AWS footer with copyright information.

6. Choose the **Security credentials** tab.

user-1 is assigned a **Console password**

The screenshot shows the AWS IAM User Details page for user-1, with the Security credentials tab selected. The left navigation pane is identical to the previous screenshot. The main content area is titled 'user-1 Info' and shows the same summary information as the Groups tab. Below this is a 'Console sign-in' section with a 'Console sign-in link' (https://042022252145.signin.aws.amazon.com/console) and a 'Manage console access' button. To the right is a 'Console password' section showing it was updated 18 minutes ago (2025-09-11 15:09 GMT+5:30). Below this is a 'Last console sign-in' section showing it has never occurred. The bottom right corner includes the AWS footer.

7. In the navigation pane on the left, choose **User groups**.

The following groups have already been created for you:

- 1 EC2-Admin
- 2 EC2-Support
- 3 S3-Support

The screenshot shows the AWS IAM User groups page. On the left, there's a navigation sidebar with options like Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, Resource analysis). The main content area is titled "User groups (3) Info". It says "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." Below this is a search bar and a table with three rows:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	19 minutes ago
EC2-Support	0	Defined	19 minutes ago
S3-Support	0	Defined	19 minutes ago

At the bottom right of the table are "Delete" and "Create group" buttons. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

## 8. Choose the **EC2-Support** group.

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". It shows the "Summary" section with the user group name "EC2-Support", creation time "September 11, 2025, 15:09 (UTC+05:30)", and ARN "arn:aws:iam:042022252145:group/spl66/EC2-Support". Below this are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is selected, showing a table with one row: "Users in this group (0)". A note says "An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS." At the bottom right of the table are "Edit", "Delete", "Remove", and "Add users" buttons. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

## 9. Choose the **Permissions** tab.

This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. Managed Policies are pre-built 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 immediately apply against all Users and Groups to which the policy is attached.

The screenshot shows the AWS IAM User Groups page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is expanded, showing 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'. Under 'Access reports', 'Access Analyzer' and 'Resource analysis' are listed. The main content area is titled 'Summary' for the 'EC2-Support' user group. It shows the 'User group name' as 'EC2-Support', 'Creation time' as 'September 11, 2025, 15:09 (UTC+05:30)', and the 'ARN' as 'arn:aws:iam::042022252145:group/spl66/EC2-Support'. Below this, tabs for 'Users', 'Permissions', and 'Access Advisor' are visible, with 'Permissions' selected. A section titled 'Permissions policies (1) Info' shows one policy attached: 'AmazonEC2ReadOnlyAccess'. Buttons for 'Edit', 'Simulate', 'Remove', and 'Add permissions' are available. A search bar and a filter dropdown for 'Policy name' and 'Type' are also present.

- Choose **AmazonEC2ReadOnlyAccess** under the **Permissions** tab and a new browser window opens. Now choose **JSON**.

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

The basic structure of the statements in an IAM Policy is:

- Effect** says whether to *Allow* or *Deny* the permissions.
- Action** specifies the API calls that can be made against an AWS Service (eg *cloudwatch:ListMetrics*).
- Resource** defines the scope of entities covered by the policy rule (eg a specific Amazon S3 bucket or Amazon EC2 instance, or \* which means *any resource*).

The screenshot shows the AWS IAM Policies page. The 'Policies' tab is selected. The 'AmazonEC2ReadOnlyAccess' policy is shown in detail. The 'Policy details' section indicates it is an 'AWS managed' policy, created on February 07, 2015, at 00:10 (UTC+05:30), and last edited on December 27, 2024, at 15:37 (UTC+05:30). The ARN is 'arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess'. Below this, tabs for 'Permissions', 'Entities attached', 'Policy versions (3)', and 'Last Accessed' are visible, with 'Permissions' selected. A section titled 'Permissions defined in this policy' shows the JSON code for the policy:

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:Describe",
8                  "ec2:GetSecurityGroupsForVpc"
9              ],
10             "Resource": "*"
11         },
12         {
13             "Effect": "Allow",
14             "Action": [
15                 "logs:CreateLogGroup",
16                 "logs:CreateLogStream",
17                 "logs:PutLogEvents"
18             ],
19             "Resource": "*"
20         }
21     ]
22 }

```

The screenshot shows the AWS IAM Policies details page for the 'AmazonEC2ReadOnlyAccess' policy. The left navigation pane is visible with 'User groups' selected under 'Access management'. The main content area displays the JSON code for the policy:

```

1  {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Effect": "Allow",
6             "Action": [
7                 "ec2:Describe",
8                 "ec2:GetSecurityGroupsForVpc"
9             ],
10            "Resource": "*"
11        },
12        {
13            "Effect": "Allow",
14            "Action": "elasticloadbalancing:Describe",
15            "Resource": "*"
16        },
17        {
18            "Effect": "Allow",
19            "Action": [
20                "cloudwatch:listMetrics",
21                "cloudwatch:GetMetricStatistics",
22                "cloudwatch:Describe"
23            ],
24            "Resource": "*"
25        },
26        {
27            "Effect": "Allow",
28            "Action": "autoscaling:Describe",
29            "Resource": "*"
30        }
31    ]
32 }

```

11. In the navigation pane on the left, choose **User groups**.
12. Choose the **S3-Support** group.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

The screenshot shows the AWS IAM User Groups page. The left navigation pane is visible with 'User groups' selected under 'Access management'. The main content area displays a table of user groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	26 minutes ago
EC2-Support	0	Defined	26 minutes ago
S3-Support	0	Defined	26 minutes ago

The screenshot shows the AWS IAM User Groups page for the 'S3-Support' group. The left navigation pane is collapsed. The main content area displays the 'Summary' of the 'S3-Support' group, showing its creation time (September 11, 2025, 15:09 UTC+05:30) and ARN (arn:aws:iam::042022252145:group/spl66/S3-Support). Below this, the 'Permissions' tab is selected, showing one attached policy: 'AmazonS3ReadOnlyAccess'. A search bar and filter options are available for managing policies.

13. Choose **AmazonS3ReadOnlyAccess** under the **Permissions** tab and a new browser window opens. Now choose **JSON**.

This policy has permissions to Get and List resources in Amazon S3.

The screenshot shows the AWS IAM Policies page for the 'AmazonS3ReadOnlyAccess' policy. The left navigation pane is collapsed. The main content area displays the 'Policy details' for 'AmazonS3ReadOnlyAccess', including its type (AWS managed), creation time (February 07, 2015, 00:10 UTC+05:30), edited time (August 11, 2023, 03:01 UTC+05:30), and ARN (arn:aws:iam::aws:policy/AmazonS3ReadonlyAccess). Below this, the 'Permissions' tab is selected, showing the 'Permissions defined in this policy' table. The table lists two services: 'S3' and 'S3 Object Lambda', both with 'Full: List, Read' access level and 'All resources' resource. A link to 'Show remaining 448 services' is also present.

14. In the navigation pane on the left, choose **User groups**.  
15. Choose the **EC2-Admin** group.

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, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report). The main content area is titled "User groups (3) Info" and contains a table with three rows:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	29 minutes ago
EC2-Support	0	Defined	29 minutes ago
S3-Support	0	Defined	29 minutes ago

At the top right, there are "Delete" and "Create group" buttons. The bottom right corner shows copyright information: © 2025, Amazon Web Services, Inc. or its affiliates.

This Group is slightly different from the other two. Instead of a *Managed Policy*, it has an **Inline Policy**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.

The screenshot shows the AWS IAM EC2-Admin user group details page. The left sidebar is identical to the previous screenshot. The main content area is titled "EC2-Admin Info" and includes a "Summary" section with the user group name "EC2-Admin" and creation time "September 11, 2025, 15:09 (UTC+05:30)". It also shows the ARN "arn:aws:iam::042022252145:group/spl66/EC2-Admin". Below this is a "Users" tab, which is currently selected, showing a table with zero users. The table has columns for "User name" and sorting options for "Groups", "Last activity", and "Creation time". At the top right of the table, there are "Edit", "Remove", and "Add users" buttons. The bottom right corner shows copyright information: © 2025, Amazon Web Services, Inc. or its affiliates.

## 16. Choose **EC2-Admin-Policy** under the **Permissions** tab. Now choose **JSON** tab.

This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.

The screenshot shows the AWS IAM Modify permissions in EC2-Admin-Policy page. The JSON editor tab is selected. The policy document is as follows:

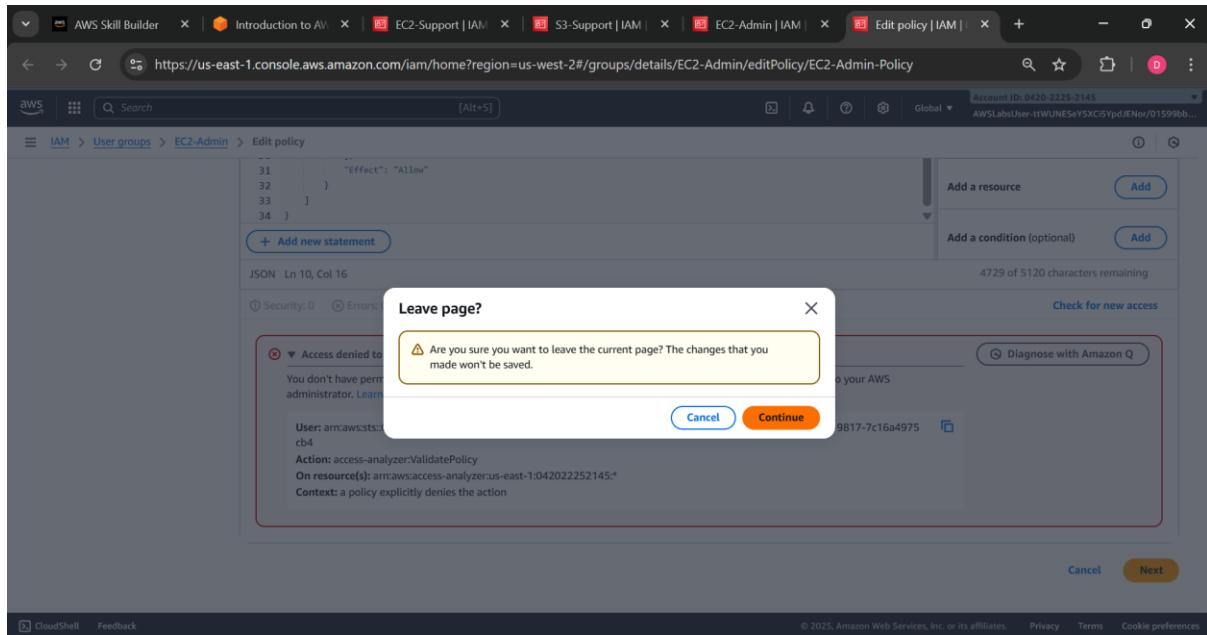
```
1 Version: "2012-10-17",
2 Statement: [
3     {
4         Action: [
5             "ec2:Describe",
6             "ec2:StopInstances",
7             "ec2:StartInstances"
8         ],
9         Resource: [
10            "arn:aws:ec2:/*:instance/*"
11        ],
12        Effect: "Allow"
13    },
14    {
15        Action: [
16            "ec2:DescribeInstances",
17            "ec2:DescribeInstanceStatus",
18            "ec2:DescribeVolumes"
19        ],
20        Resource: "*",
21        Effect: "Allow"
22    }
]
```

The sidebar includes tabs for Visual, JSON, Actions, and Remove. It also lists services like EC2, AI Operations, AMP, API Gateway, API Gateway V2, ARC Region switch, and ARC Zonal Shift.

The screenshot shows the AWS IAM EC2-Admin page under the Permissions tab. The ARN is listed as arn:aws:iam::042022252145:group/spl66/EC2-Admin. The Permissions section shows the attached policy EC2-Admin-Policy.

Policy name	Type	Attached entities
EC2-Admin-Policy	Customer inline	0

17. At the bottom of the screen, choose **Cancel** and then choose **Continue** to close the policy.



## Business Scenario

For the remainder of this lab, we will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many Amazon EC2 instances and a great deal of Amazon S3 storage. You wish to give access to new staff depending upon their job function:

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

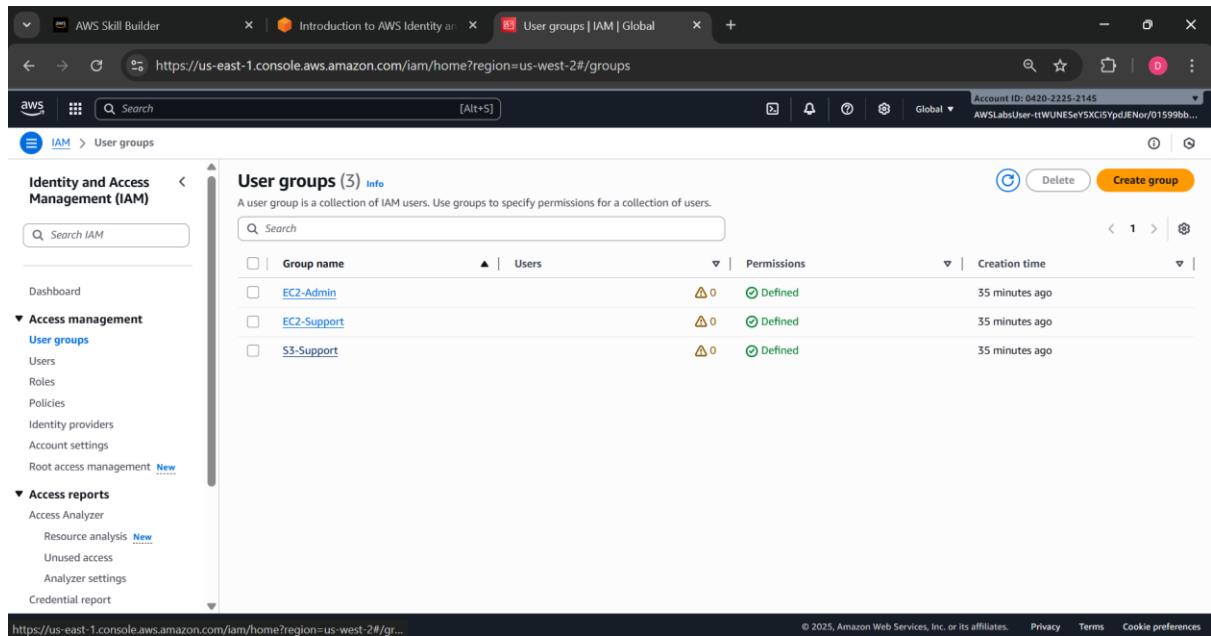
## Task 2: Add Users to Groups

You have recently hired **user-1** into a role where they will provide support for Amazon S3. You will add them to the **S3-Support** group so that they inherit the necessary permissions via the attached *AmazonS3ReadOnlyAccess* policy.

You can ignore any “not authorized” errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

## Add user-1 to the S3-Support Group

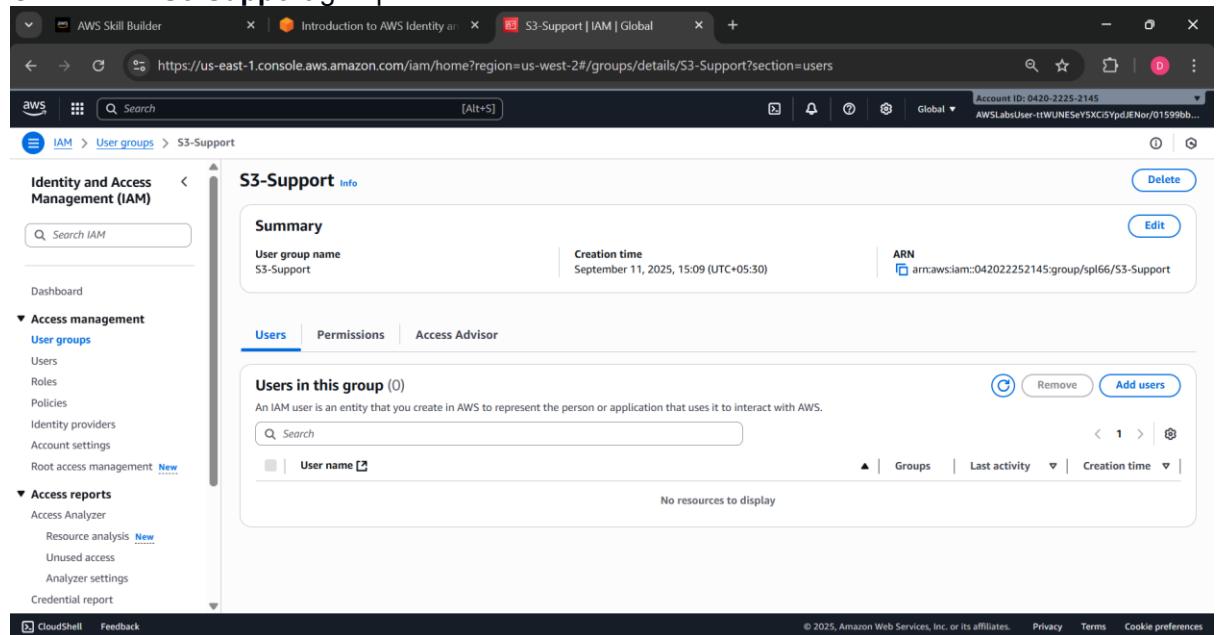
18. In the left navigation pane, choose **User groups**.



The screenshot shows the AWS IAM User Groups page. The left sidebar is collapsed, and the main content area displays a table of user groups. The table has columns for Group name, Users, Permissions, and Creation time. Three groups are listed: EC2-Admin, EC2-Support, and S3-Support, all created 35 minutes ago with defined permissions.

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	35 minutes ago
EC2-Support	0	Defined	35 minutes ago
S3-Support	0	Defined	35 minutes ago

19. Choose the S3-Support group.



The screenshot shows the AWS IAM S3-Support Group Details page. The left sidebar is collapsed, and the main content area shows the group's summary and its users. The summary section includes the user group name (S3-Support), creation time (September 11, 2025, 15:09 UTC+05:30), and ARN (arn:aws:iam::042022252145:group/spl66/S3-Support). The users tab is selected, showing a table with a single row: "No resources to display".

User name
No resources to display

20. Choose the **Users** tab.

21. In the **Users** tab, choose **Add users**.

The screenshot shows the 'Add users to S3-Support' page. At the top, there's a search bar and a 'User name' dropdown. Below is a table listing three users: 'user-1', 'user-2', and 'user-3'. Each user has a checkbox next to their name. The table includes columns for Groups, Last activity, and Creation time. At the bottom right are 'Cancel' and 'Add users' buttons.

User name	Groups	Last activity	Creation time
user-1	0	None	38 minutes ago
user-2	0	None	38 minutes ago
user-3	0	None	38 minutes ago

22. In the **Add users to Group** window, configure the following:

- 1 Select **user-1**.
- 2 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 same 'Add users to S3-Support' page, but now 'user-1' is selected, indicated by a checked checkbox. The 'Add users' button at the bottom is highlighted with an orange border.

User name	Groups	Last activity	Creation time
user-1	0	None	39 minutes ago
user-2	0	None	39 minutes ago
user-3	0	None	39 minutes ago

The screenshot shows the AWS IAM Groups page for the 'S3-Support' group. The group was created on September 11, 2025, at 15:09 UTC+05:30. It contains one user, 'user-1'. The ARN for the group is arn:aws:iam::042022252145:group/spl66/S3-Support.

## Add user-2 to the EC2-Support Group

You have hired **user-2** into a role where they will provide support for Amazon EC2.

23. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.

**user-2** should now be part of the **EC2-Support** group.

The screenshot shows the AWS IAM Groups page for the 'EC2-Support' group. The group was created on September 11, 2025, at 15:09 UTC+05:30. It contains one user, 'user-2'. A green notification bar at the top indicates '1 user added to this group.' The ARN for the group is arn:aws:iam::042022252145:group/spl66/EC2-Support.

## Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

24. Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.

**user-3** should now be part of the **EC2-Admin** group.

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The navigation pane on the left is expanded, showing 'User groups' selected under 'Access management'. The main content area displays the 'EC2-Admin' group details, including its creation time (September 11, 2025, 15:09 UTC+05:30) and ARN (arn:aws:iam:042022252145:group/spl66/EC2-Admin). The 'Users' tab is selected, showing one user ('user-3') assigned to the group. The user table includes columns for User name, Groups, Last activity, and Creation time.

25. In the navigation pane on the left, choose **User groups**.

Each Group should have a **1** in the Users column for the number of Users in each Group.

If you do not have a **1** beside each group, revisit the above instructions to ensure that each user is assigned to a Group, as shown in the table in the Business Scenario section.

The screenshot shows the AWS IAM User Groups page displaying three groups: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. The 'User groups' tab is selected. The table lists the group names, the number of users (all show 1), the status (Defined), and the creation time (all show 42 minutes ago).

Group name	Users	Permissions	Creation time
EC2-Admin	1	Defined	42 minutes ago
EC2-Support	1	Defined	42 minutes ago
S3-Support	1	Defined	42 minutes ago

### Task 3: Sign-In and Test Users

In this task, you will test the permissions of each IAM User.

26. In the navigation pane on the left, choose **Dashboard**.

An **IAM users Sign-in URL** is displayed It will look similar to: <https://123456789012.signin.aws.amazon.com/console>

This link can be used to sign-in to the AWS Account you are currently using.

The screenshot shows the AWS IAM Dashboard. On the left, there is a navigation pane with sections like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Tools'. The main area displays 'IAM resources' with counts: 3 User groups, 3 Users, 26 Roles, 3 Policies, and 0 Identity providers. Below this is a 'What's new' section with a list of recent changes:

- Amazon Bedrock introduces API keys for streamlined development. 2 months ago
- AWS Service Reference now supports annotations for service actions. 3 months ago
- AWS expands resource control policies (RCPs) support to two additional services. 3 months ago
- AWS IAM now enforces MFA for root users across all account types. 3 months ago

On the right, there is a 'AWS Account' summary with the Account ID (042022252145), Account Alias (Create), and a 'Sign-in URL for IAM users in this account' link (<https://042022252145.signin.aws.amazon.com/console>). At the bottom, there are links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

27. Copy the **IAM users Sign-in URL** to a text editor.

28. Open a private window.

#### Mozilla Firefox

- 1 Choose the menu bars at the top-right of the screen
- 2 Select **New Private Window**

#### Google Chrome

- 1 Choose the ellipsis at the top-right of the screen
- 2 Choose **New Incognito window**

#### Microsoft Edge

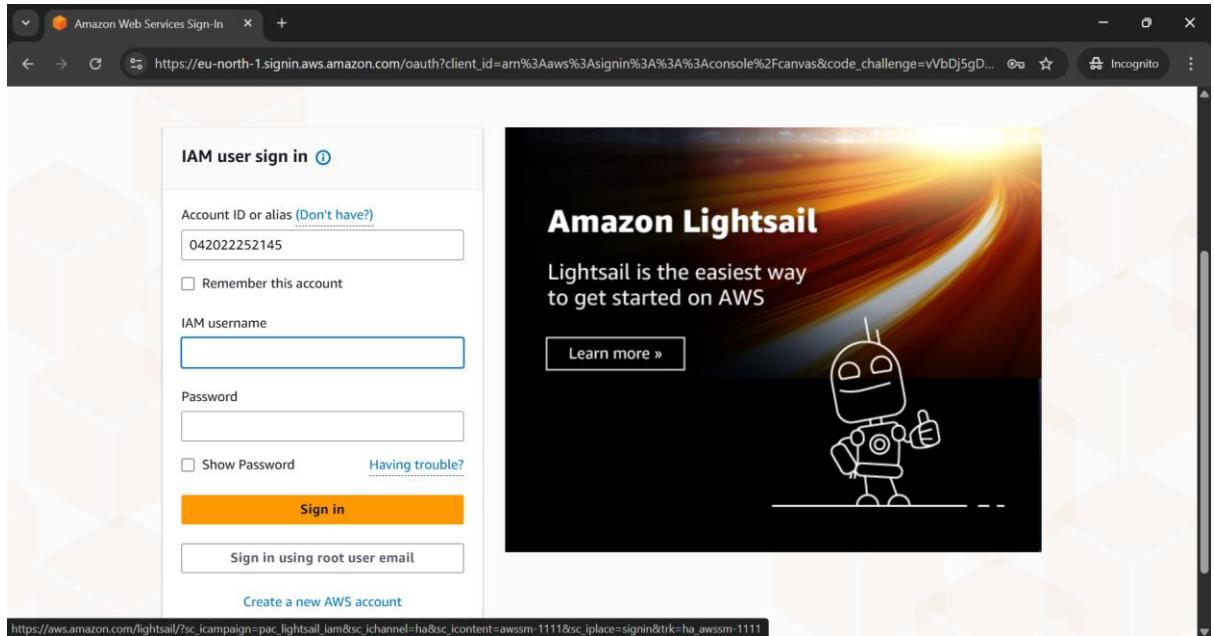
- 1 Choose the ellipsis at the top-right of the screen
- 2 Choose **New InPrivate window**

#### Microsoft Internet Explorer

- 1 Choose the **Tools** menu option
- 2 Choose **InPrivate Browsing**

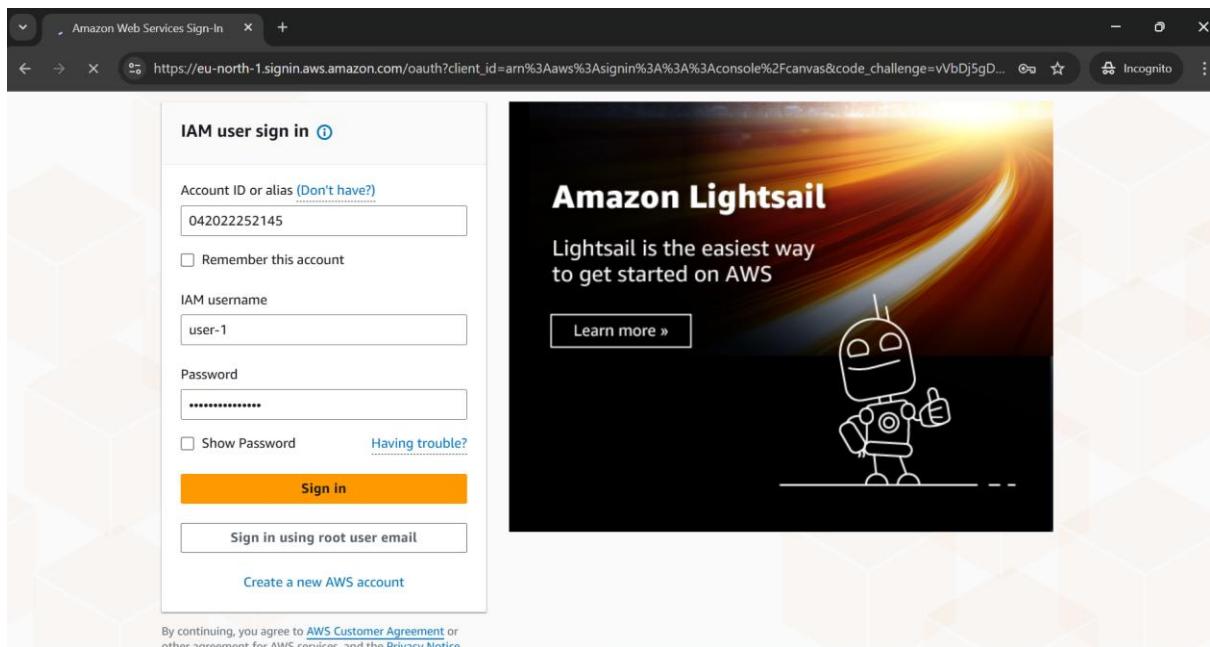
29. Paste the **IAM users sign-in** link into your private window and press **Enter**.

You will now sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.



30. Sign-in with:

- 1 **IAM username:**
  1. **user-1**
- 2 **Password:** Paste the value of *AdministratorPassword* located to the left of these instructions.



31. At the top of the AWS Management Console, in the search bar, search for and choose S3

The screenshot shows the AWS Management Console search results for 's3'. The search bar at the top contains 's3'. Below it, the 'Services' section lists 'S3 Scalable Storage in the Cloud', 'S3 Glacier Archive Storage in the Cloud', and 'AWS Snow Family Large Scale Data Transport'. The 'Features' section lists 'S3 on Outposts' as an 'AWS Outposts feature'. A sidebar on the left shows recent items like 'CloudShell' and 'Feedback'. A right-hand panel has a red box highlighting the 'Create application' button.

32. Choose the bucket that has **s3bucket** in its name.

The name of your S3 bucket is also located to the left of these instructions.

Since your user is part of the **S3-Support** Group in IAM, they have permission to view a list of Amazon S3 buckets and the contents of the **s3bucket**.

Now, test whether they have access to Amazon EC2.

The screenshot shows the AWS Management Console for an S3 bucket named 'labstack-01599bbc-ff95-45d8-9817-7c16a497-s3bucket-xgdntrd5hkbv'. The left sidebar shows 'General purpose buckets' with options like 'Directory buckets', 'Table buckets', and 'Vector buckets'. The main area shows 'Objects (0)' with buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', and 'Actions'. A message states 'No objects' and 'You don't have any objects in this bucket.' The bottom right corner has a red box highlighting the 'Upload' button.

33. At the top of the AWS Management Console, in the search bar, search for and choose **EC2**

34. Navigate to the region that your lab was launched in by:

- 1 Choosing the drop-down arrow at the top of the screen, to the left of **Support**
- 2 Selecting the region value that matches the value of **Region** to the left of these instructions

35. In the left navigation pane, choose **Instances**.

You cannot see any instances. This is because your 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.

36. Sign user-1 out of the **AWS Management Console** by completing the following actions:

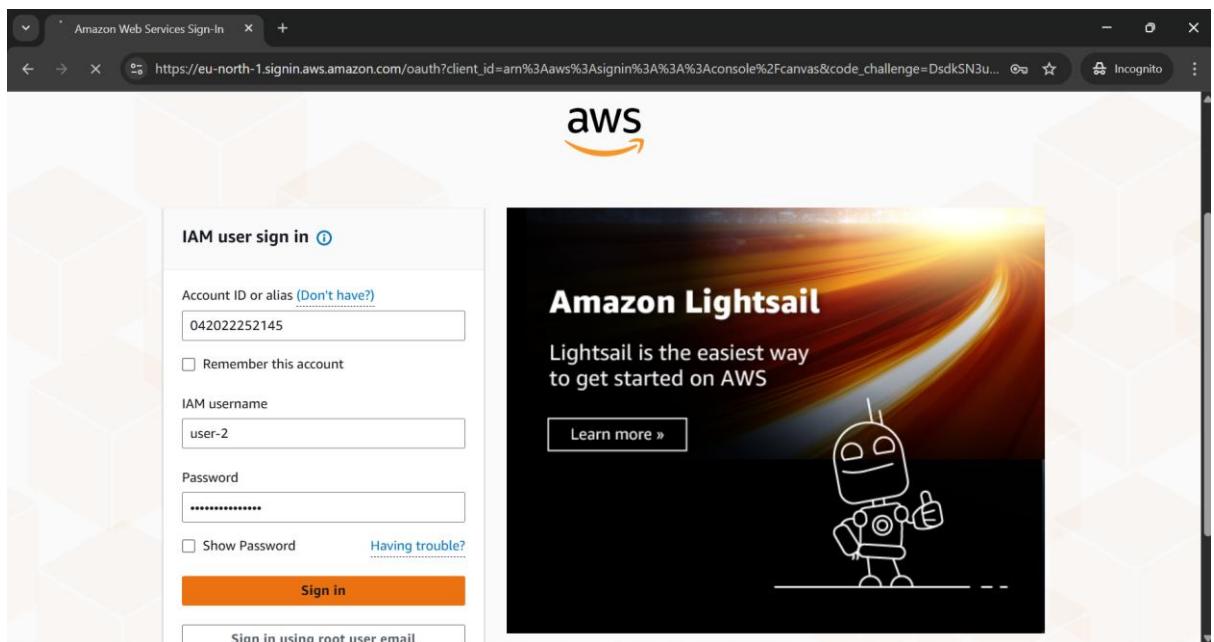
- 1 At the top of the screen, choose **user-1**
- 2 Choose **Sign out**

37. Paste the **IAM users sign-in** link into your private window and press **Enter**.

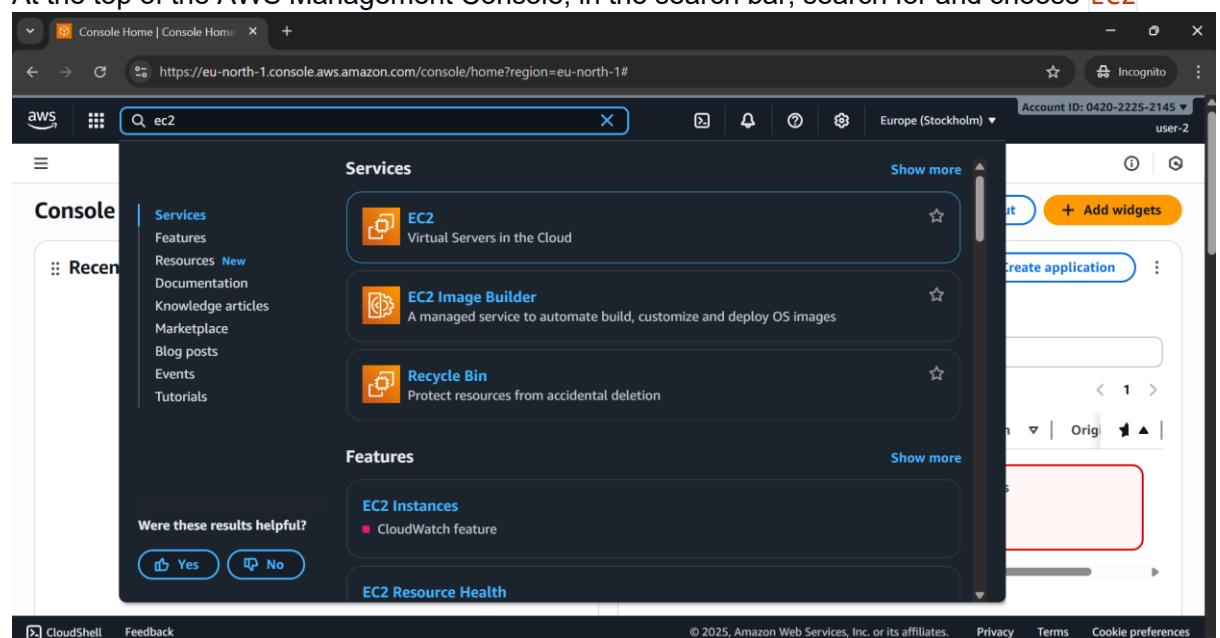
This links should be in your text editor.

38. Sign-in with:

- 1 **IAM user name:** **user-2**
- 2 **Password:** Paste the value of *AdministratorPassword* located to the left of these instructions.



39. At the top of the AWS Management Console, in the search bar, search for and choose **EC2**



40. Navigate to the region that your lab was launched in by:

- 1 Choosing the drop-down arrow at the top of the screen, to the left of **Support**
- 2 Selecting the region value that matches the value of **Region** to the left of these instructions

The screenshot shows the AWS EC2 Dashboard for the us-west-2 region. A blue banner at the top right says "You can change your default landing page for EC2." Below it are "Permanently dismiss" and "Change landing page" buttons. The main area displays "Resources" and "Account attributes".

Instances (running)	1	Auto Scaling Groups	0
Capacity Reservations	0	Dedicated Hosts	0
Elastic IPs	0	Instances	1
Key pairs	0	Load balancers	-
Placement groups	0	Security groups	4
Snapshots	0	Volumes	1

**Account attributes**

- Default VPC: vpc-00ac0c3b953b5b868
- Settings
  - Data protection and security
  - Allowed AMIs
  - Zones
  - EC2 Serial Console
  - Default credit specification
  - EC2 console preferences

Explore AWS Privacy Terms Cookie preferences

41. In the navigation pane on the left, choose **Instances**.

You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make any changes to Amazon EC2 resources.

Your EC2 instance should be selected. If it is not selected, select it.

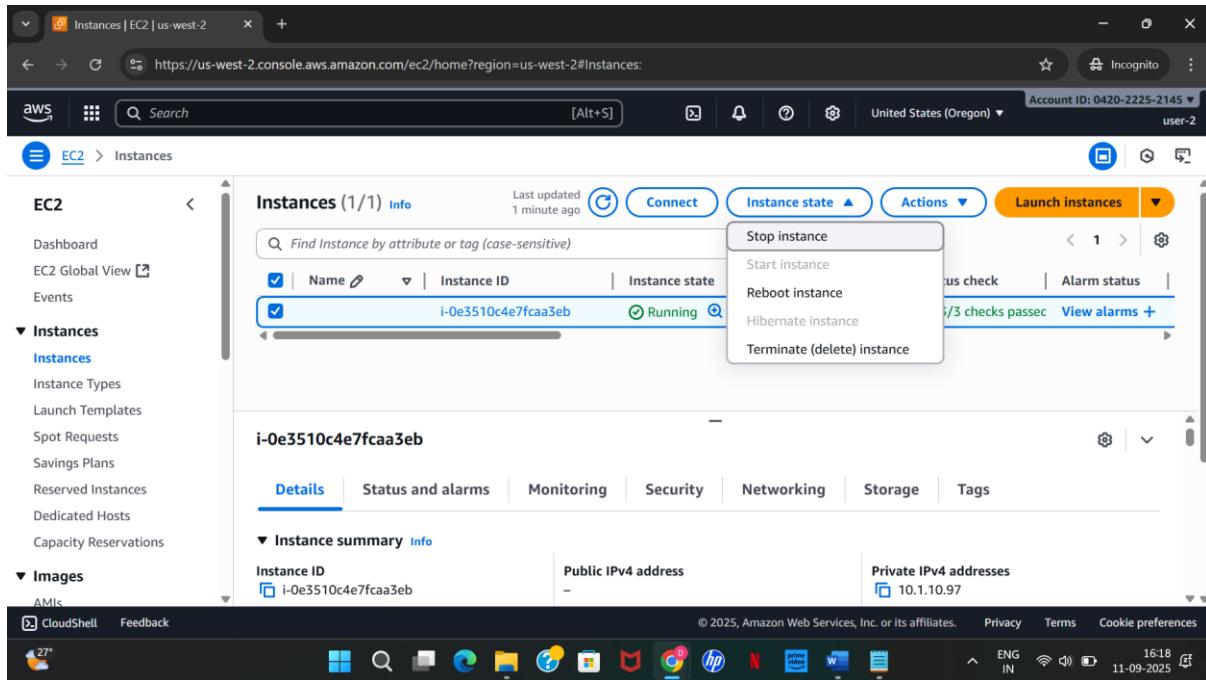
The screenshot shows the AWS EC2 Instances page. It lists one instance: i-0e3510c4e7fcaa3eb, which is running and of type t3.micro. The "Actions" dropdown menu is open, showing options like "Stop", "Start", "Reboot", "Termination protection", and "Launch instances".

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
i-0e3510c4e7fcaa3eb	i-0e3510c4e7fcaa3eb	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>

Select an instance

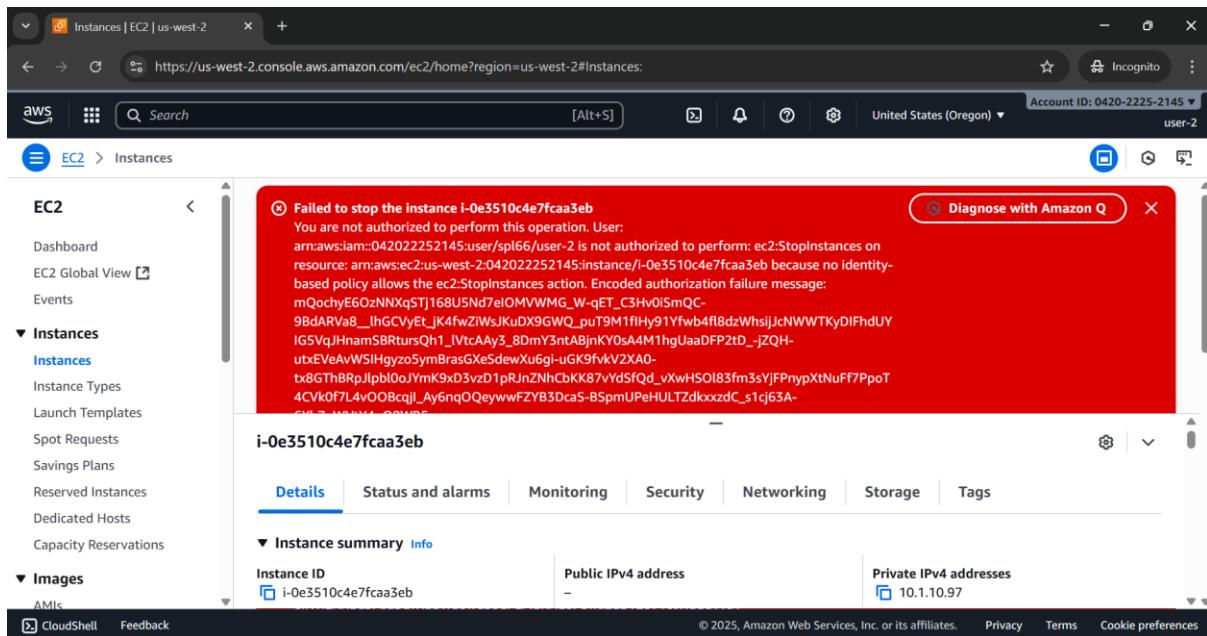
CloudShell Feedback

42. In **Instance state**, menu choose **Stop instance**.



43. In the **Stop instance** window, choose **Stop**.

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



44. Close the displayed error message.

Next, check if user-2 can access Amazon S3.

45. At the top of the AWS Management Console, in the search bar, search for and choose **S3**. You will receive an **Error Access Denied** because user-2 does not permission to use Amazon S3.

46. You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

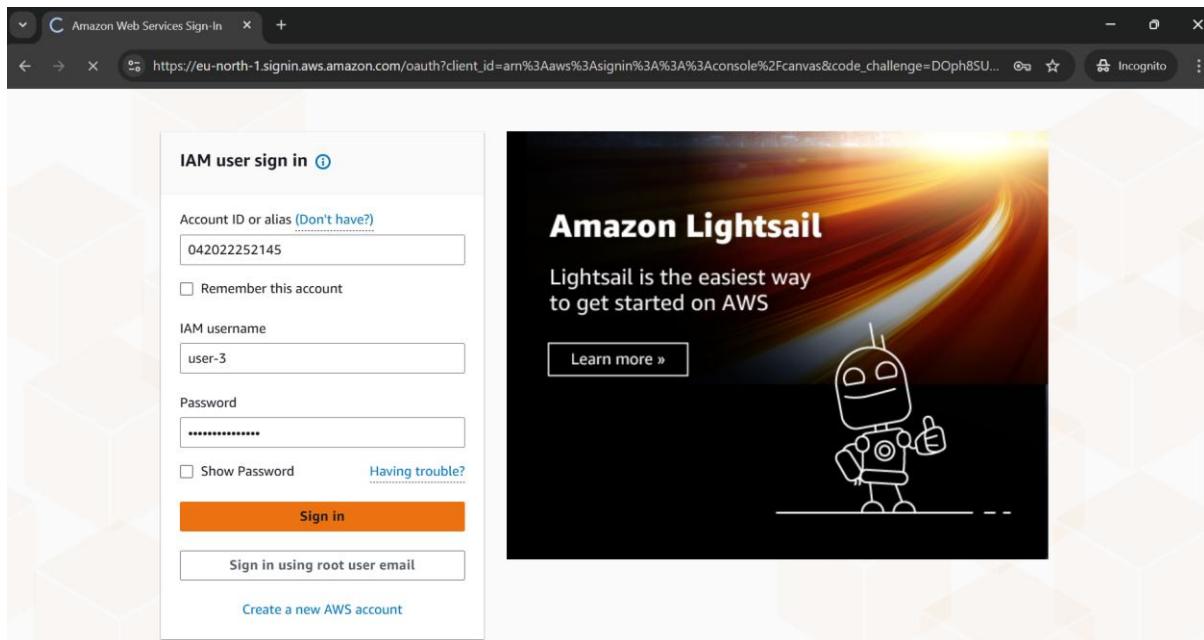
47. Sign user-2 out of the **AWS Management Console** by completing the following actions:
- 1 At the top of the screen, choose **user-2**
  - 2 Choose **Sign out**

48. Paste the **IAM users sign-in** link into your private window and press **Enter**.

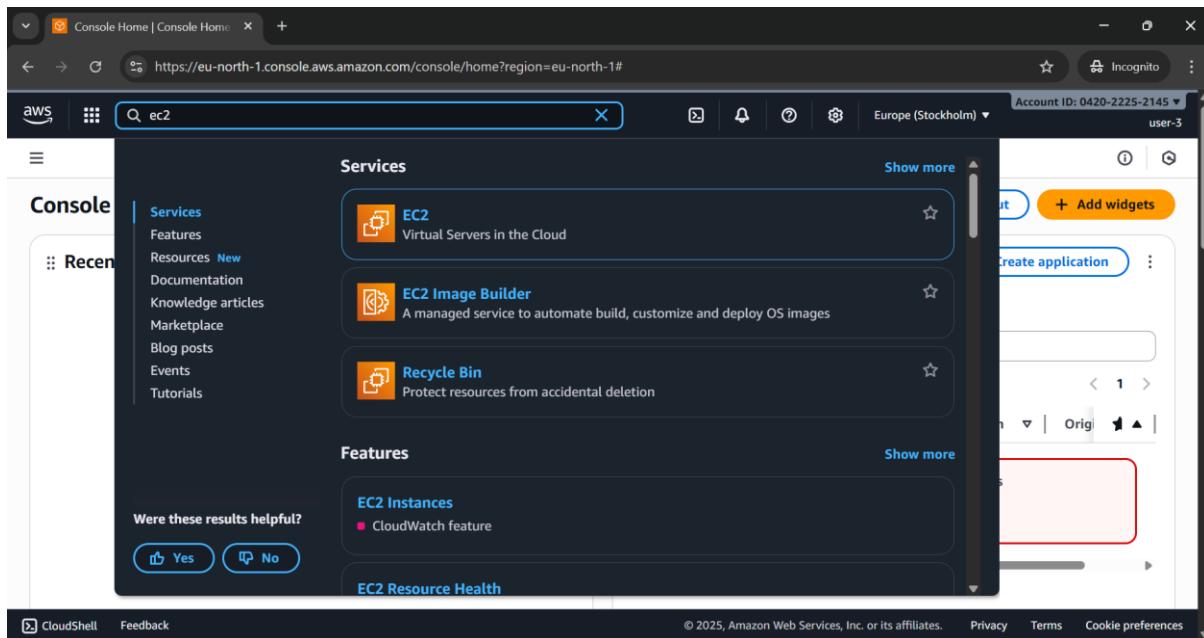
49. Paste the sign-in link into your web browser address bar again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

50. Sign-in with:

- 1 **IAM user name:** **user-3**
- 2 **Password:** Paste the value of *AdministratorPassword* located to the left of these instructions.



51. At the top of the AWS Management Console, in the search bar, search for and choose **EC2**



52. Navigate to the region that your lab was launched in by:

- 1 Choosing the drop-down arrow at the top of the screen, to the left of **Support**

2 Selecting the region value that matches the value of **Region** to the left of these instructions

The screenshot shows the AWS EC2 Dashboard for the us-west-2 region. The left sidebar includes links for EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), and Images (with sub-links for AMIs). A blue banner at the top says "You can change your default landing page for EC2." Below it, there's a "Resources" section showing counts for various EC2 services, many of which have "API Error" status indicators. To the right is the "Account attributes" section, which has a red box around an error message: "An error occurred: An error occurred checking for a default VPC. Diagnose with Amazon Q". Other account settings like Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, and Default credit specification are listed below.

53. In the navigation pane on the left, choose **Instances**.

- 1 As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.
- 2 Your EC2 instance should be selected . If it is not, please select it.

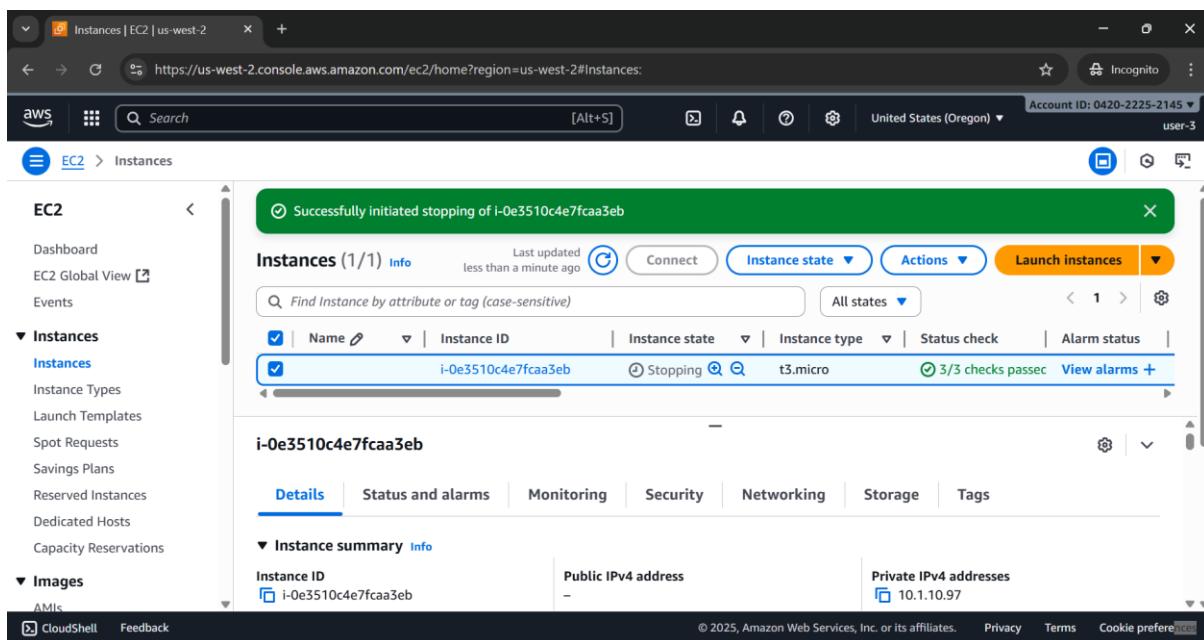
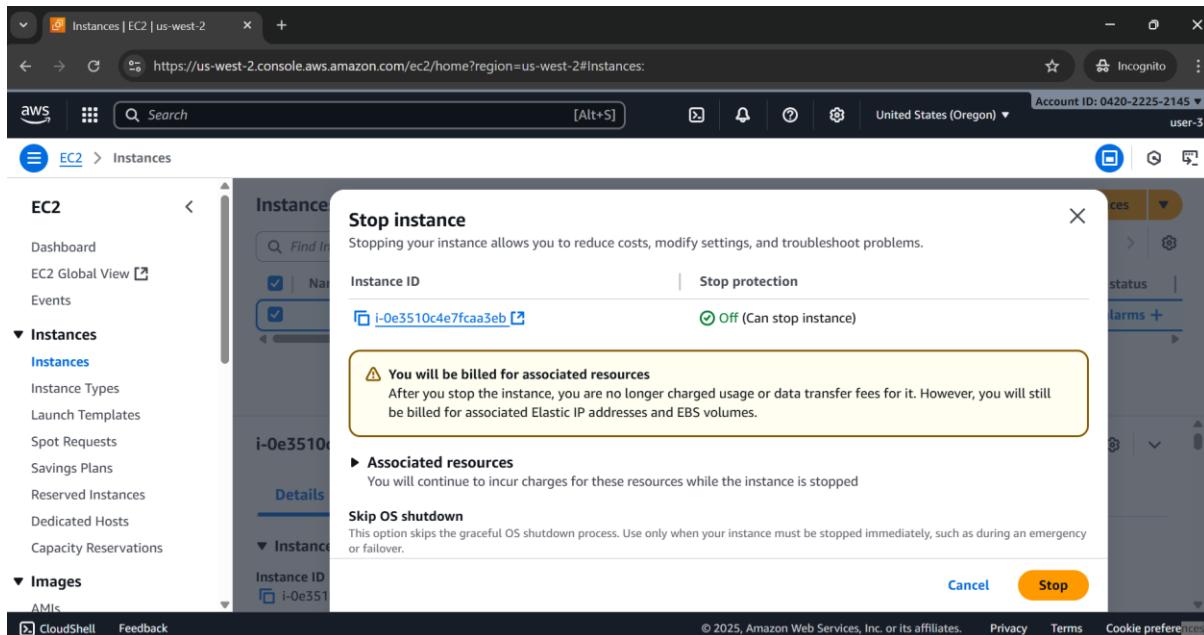
The screenshot shows the AWS EC2 Instances page. The left sidebar lists Instances, Images, and CloudShell. The main area displays a table of instances with one row selected: "i-0e3510c4e7fcaa3eb" (Status: Running, Type: t3.micro, Health: 3/3 checks passed). Below the table is a detailed view for the selected instance, showing tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, the Instance ID is i-0e3510c4e7fcaa3eb, and the Public IPv4 address is 10.1.10.97.

54. In **Instance state**, menu choose **Stop instance**.

55. In the **Stop Instance** window, choose **Stop**.

- 1 The instance will enter the *stopping* state and will shutdown.

## 56. Close your private window.



## Conclusion

Congratulations! You now have successfully:

- Explored pre-created IAM users and groups
- Inspected IAM policies as applied to the pre-created groups
- Followed a real-world scenario, adding users to groups with specific capabilities enabled
- Located and used the IAM sign-in URL
- Experimented with the effects of policies on service access

## End lab

Follow these steps to close the console and end your lab.

57. Return to the **AWS Management Console**.
58. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
59. Choose **End Lab** and then confirm that you want to end your lab.

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'AWS CloudTrail'. The main area displays 'IAM resources' with counts: User groups (3), Users (3), Roles (26), Policies (3), and Identity providers (0). Below this is a 'What's new' section with a list of recent updates. To the right, there's a sidebar with account details: Account ID (0420-2225-2145), Federated user (AWSLabsUser), and a note about not having permission to see the color for this account. There are also sections for 'Tools' (with 'Policy simulator' and 'Switch role' buttons) and 'Additional information' (with 'Security best practices in IAM'). The URL in the browser bar is <https://us-east-1.console.aws.amazon.com/iam/logout/doLogout>.