

1. Introduction to AWS IAM

Task 1: Explore the Users and Groups

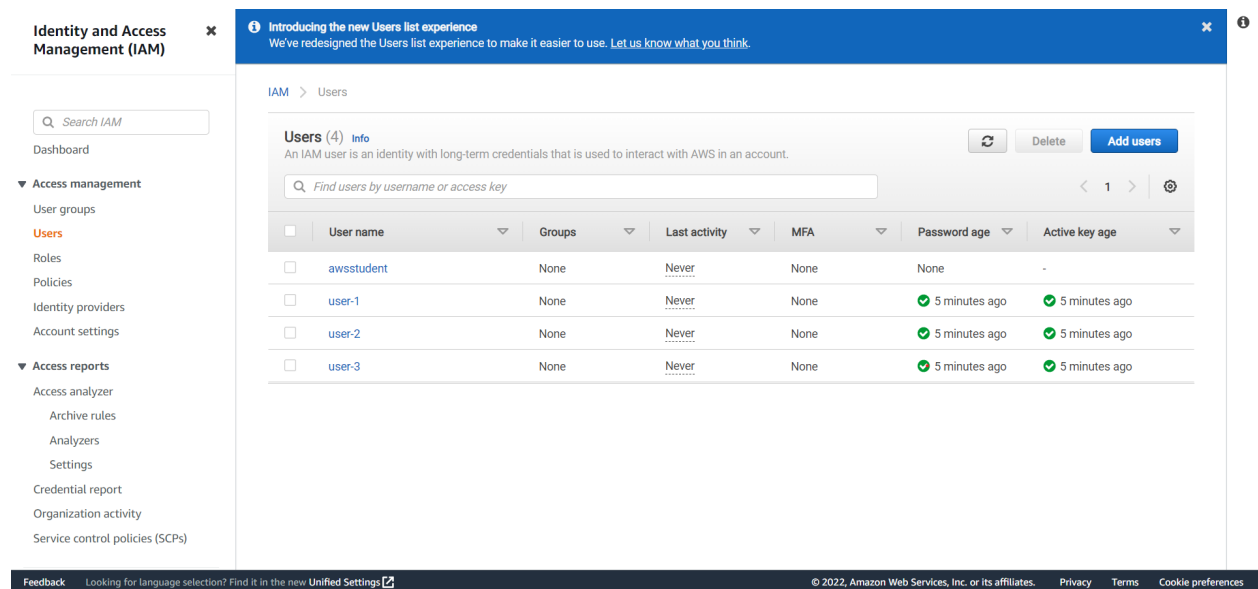
In this task, you will explore the Users and Groups that have already been created for you in IAM.

1. In the AWS Management Console, on the Services menu, select IAM.

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

The following IAM Users have been created for you:

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



The screenshot shows the AWS IAM console interface. On the left is a navigation pane with sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings) and 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The 'Users' link is highlighted. The main content area shows the 'Users (4)' list. A blue banner at the top of the main area says 'Introducing the new Users list experience'. Below the banner, there's a search bar and a table of users. The table has columns for User name, Groups, Last activity, MFA, Password age, and Active key age. The users listed are awsstudent, user-1, user-2, and user-3. user-1, user-2, and user-3 have a password age of '5 minutes ago' and an active key age of '5 minutes ago'. The footer of the console shows '© 2022, Amazon Web Services, Inc. or its affiliates.' and links for Privacy, Terms, and Cookie preferences.

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	awsstudent	None	Never	None	None	-
<input type="checkbox"/>	user-1	None	Never	None	✓ 5 minutes ago	✓ 5 minutes ago
<input type="checkbox"/>	user-2	None	Never	None	✓ 5 minutes ago	✓ 5 minutes ago
<input type="checkbox"/>	user-3	None	Never	None	✓ 5 minutes ago	✓ 5 minutes ago

3. 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.

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

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

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 console interface. On the left, the navigation pane is expanded to 'Access management' > 'User groups'. The main content area displays the 'User groups' page with a table of existing groups. The table has columns for Group name, Users, Permissions, and Creation time. Three groups are listed: EC2-Admin, EC2-Support, and S3-Support. Each group has 0 users and is marked as 'Defined' 9 minutes ago. The top of the page includes a search bar, a 'Filter User groups by property or group name and press enter' input, and buttons for 'Delete' and 'Create group'.

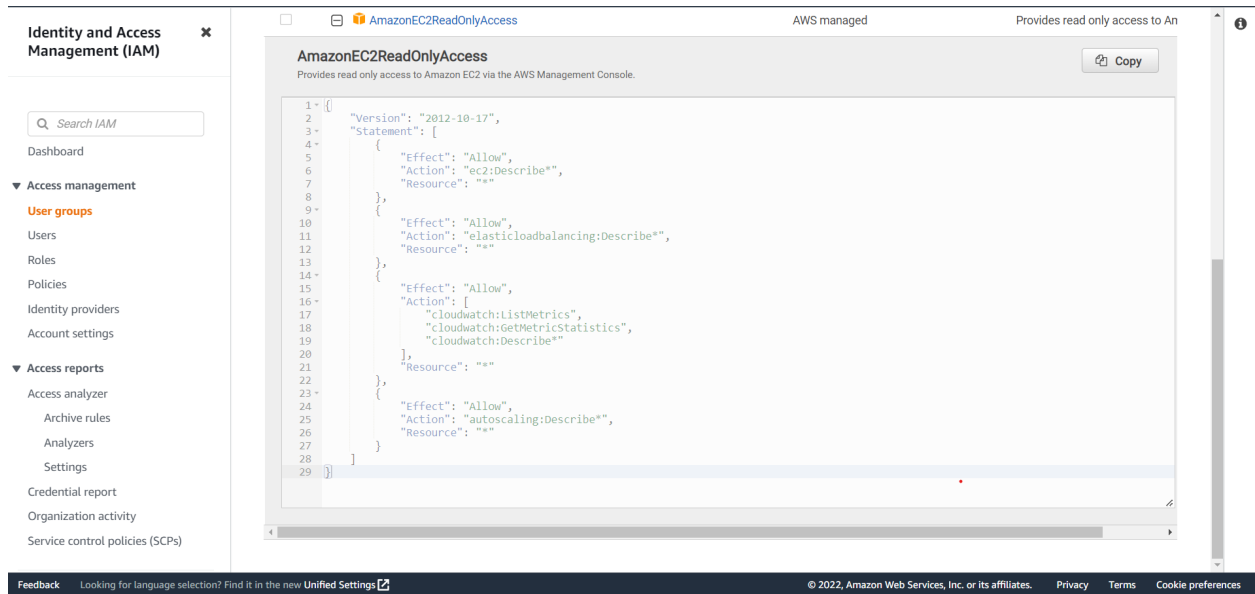
Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	9 minutes ago
EC2-Support	0	Defined	9 minutes ago
S3-Support	0	Defined	9 minutes ago

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

8. 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 are immediately apply against all Users and Groups that are attached to the policy.

9. Choose the plus (+) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.



10. 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).

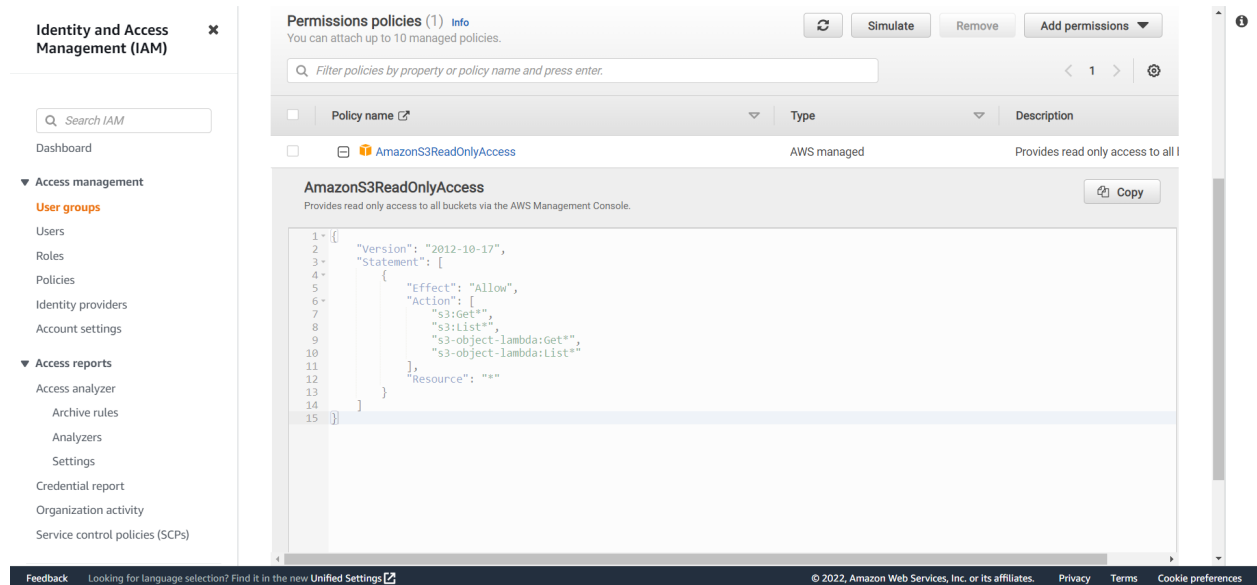
11. Choose the minus icon (-) to hide the policy details.

12. In the navigation pane on the left, choose User groups.

Choose the S3-Support group and then choose the Permissions tab.

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

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



14. This policy grants permissions to Get and List resources in Amazon S3. Choose the minus icon (-) to hide the policy details.

15. In the navigation pane on the left, choose User groups. Choose the EC2-Admin group and then choose the Permissions tab.

16. 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.

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

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

18. Choose the minus icon (-) to hide the policy details.

Task 2: Add Users to Groups

Add user-1 to the S3-Support Group

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

20. Choose the **S3-Support** group.

21. Choose the **Users** tab.

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

The screenshot shows the 'Add user' form in the AWS IAM console. At the top, there's a progress bar with five steps, where step 1 is highlighted. The form is titled 'Add user' and has a section 'Set user details'. Below this, there's a text input field for 'User name*' and a link 'Add another user'. The next section is 'Select AWS access type', which includes a note about programmatic access and a link 'Learn more'. Under this, there are two radio button options: 'Access key - Programmatic access' (selected) and 'Password - AWS Management Console access'. The bottom of the form has a 'Cancel' button and a 'Next: Permissions' button. A footer bar contains links for 'Feedback', 'Looking for language selection? Find it in the new Unified Settings', and copyright information for Amazon Web Services, Inc.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☒ Access key - Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ Password - AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

[Cancel](#) [Next: Permissions](#)

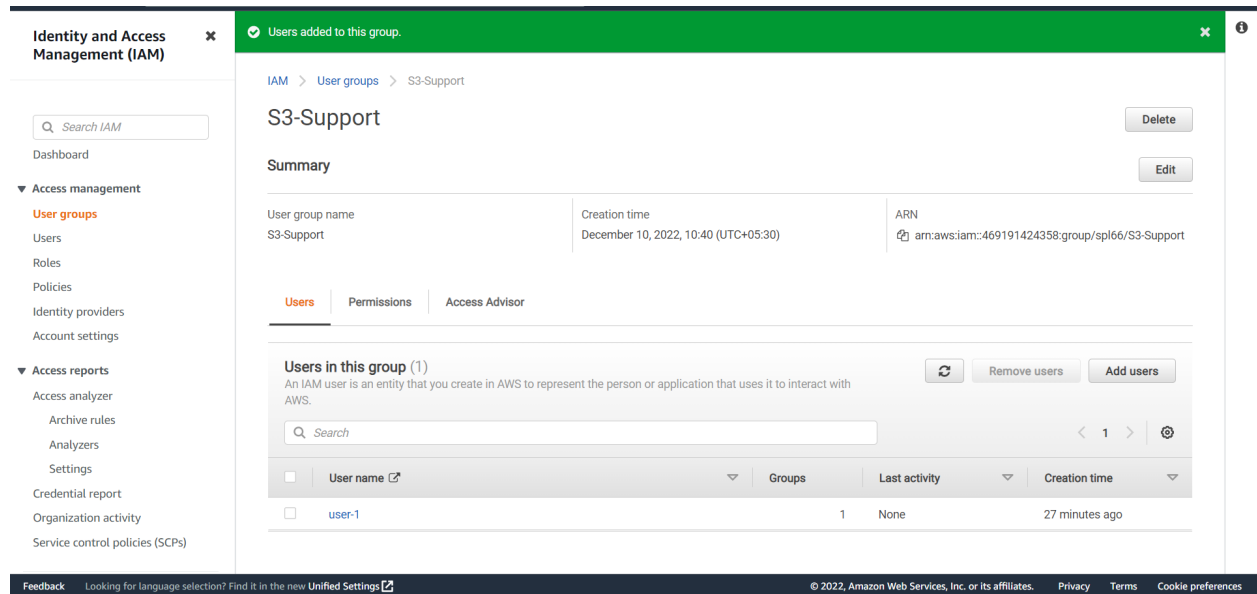
[Feedback](#) Looking for language selection? Find it in the new Unified Settings [Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

23. In the **Add Users to S3-Support** window, configure the following:

- Select **user-1**.
- At the bottom of the screen, choose **Add Users**.

24. In the **Users** tab you will see that user-1 has been added to the group.



Add user-2 to the EC2-Support Group

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

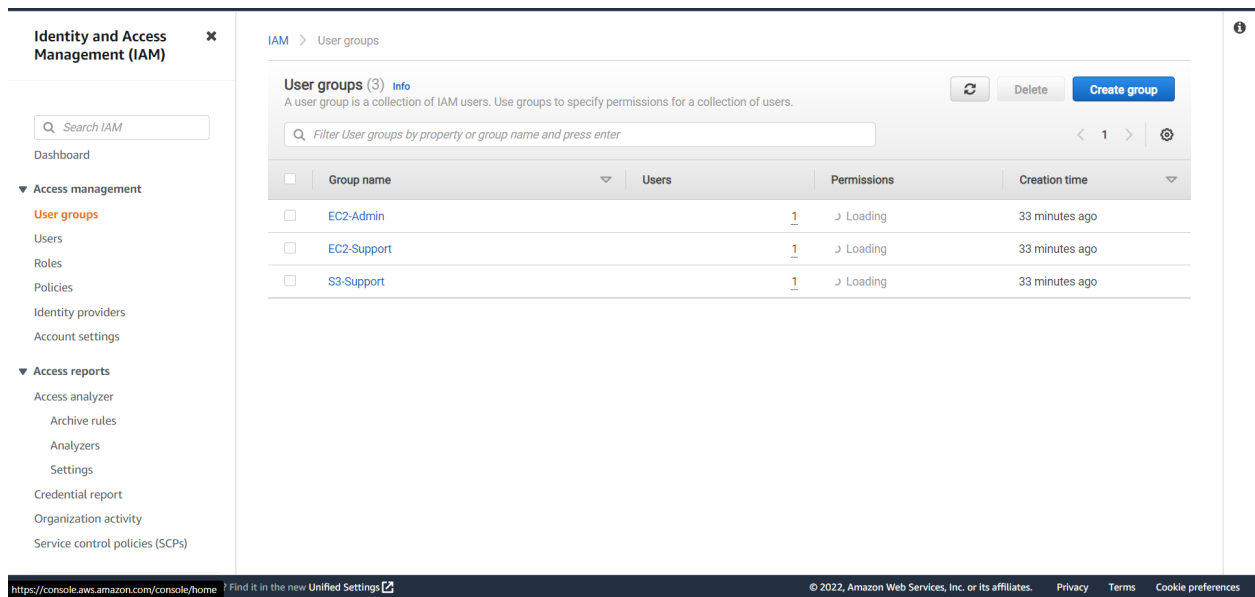
25. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group. user-2 should now be part of the **EC2-Support** group.

Add user-3 to the EC2-Admin Group

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

26. 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.

27. In the navigation pane on the left, choose **User groups**. Each Group should now have a **1** in the Users column for the number of Users in each Group.



Task 3: Sign-In and Test Users

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

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

An **IAM users sign-in link** is displayed on the right. 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.

29. Copy the **Sign-in URL for IAM users in this account** to a text editor.

30. Open a private (Incognito) window

Google Chrome

- Choose the ellipsis at the top-right of the screen
- Select **New Incognito Window**

31. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.

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

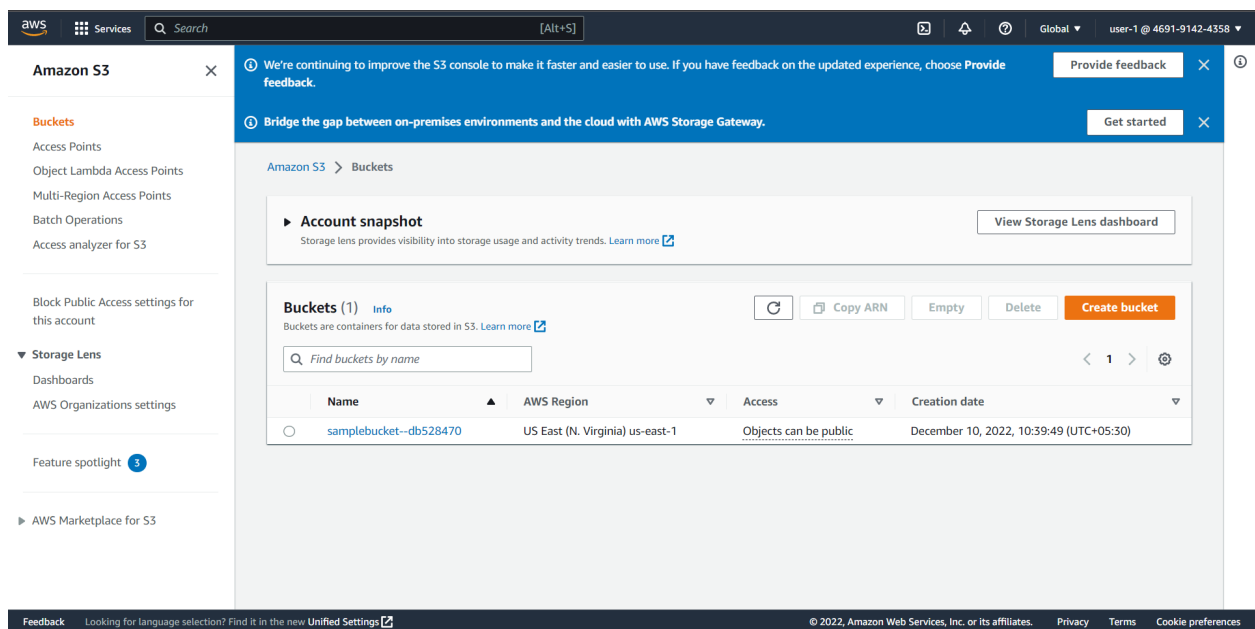
32. Sign-in with:

- **IAM user name:** user-1
- **Password:** Lab-Password1

34. In the **Services** menu, choose **S3**.

35. Choose the name of the bucket that exists in the account and browse the contents.

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.



36. In the **Services** menu, choose **EC2**.

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

You cannot see any instances. Instead, you see a message that states *You are not authorized to perform this operation*. This is because this user has not been granted any permissions to access Amazon EC2.

You will now sign-in as **user-2**, who has been hired as your Amazon EC2 support person.

38. Sign-in with:

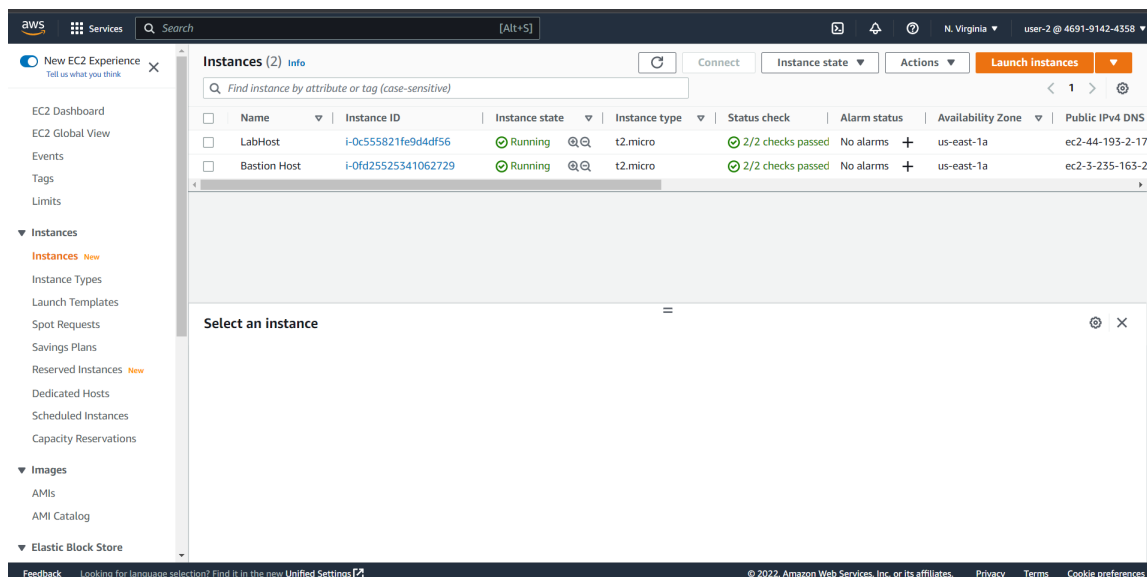
- a. **IAM user name:** user-2
- b. **Password:** Lab-Password2

39. In the **Services** menu, choose **EC2**.

40. 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.

- c. Select the instance named *LabHost*.



41. In the **Instance state** menu above, select **Stop instance**.

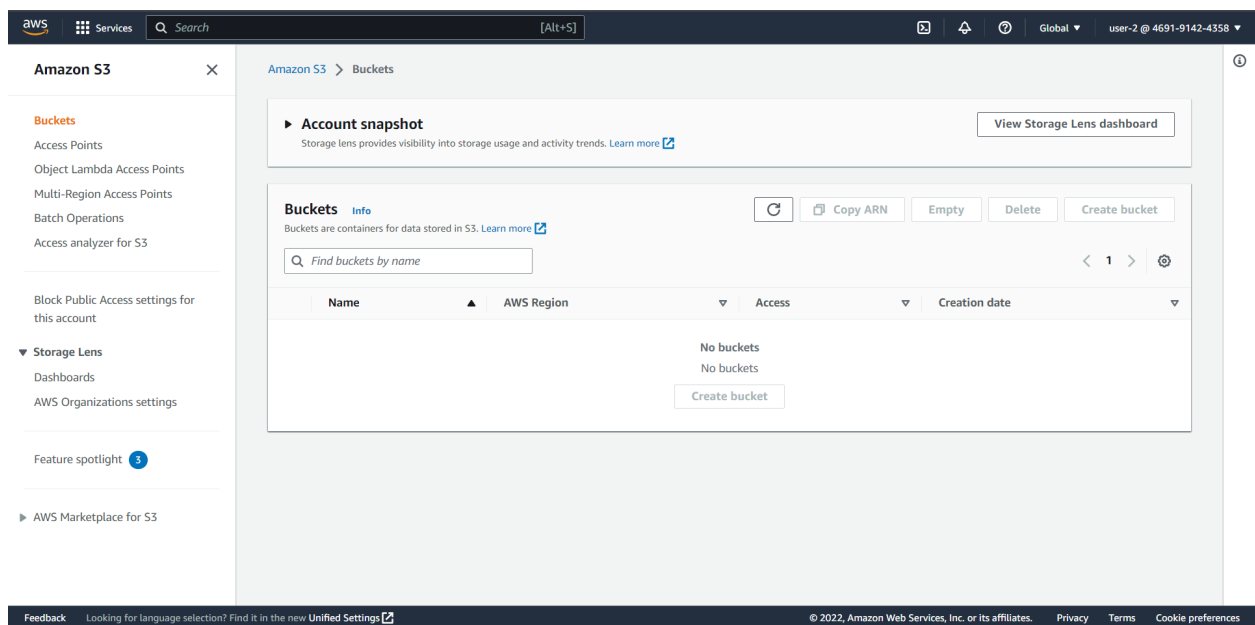
42. In the **Stop Instance** window, select **Stop**.

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.

43. Choose the X to close the *Failed to stop the instance* message.
Next, check if user-2 can access Amazon S3.

44. In the **Services**, choose **S3**.

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



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

45. Sign-in with:

- **IAM user name:** user-3
- **Password:** Lab-Password3

46. In the **Services** menu, choose **EC2**.

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

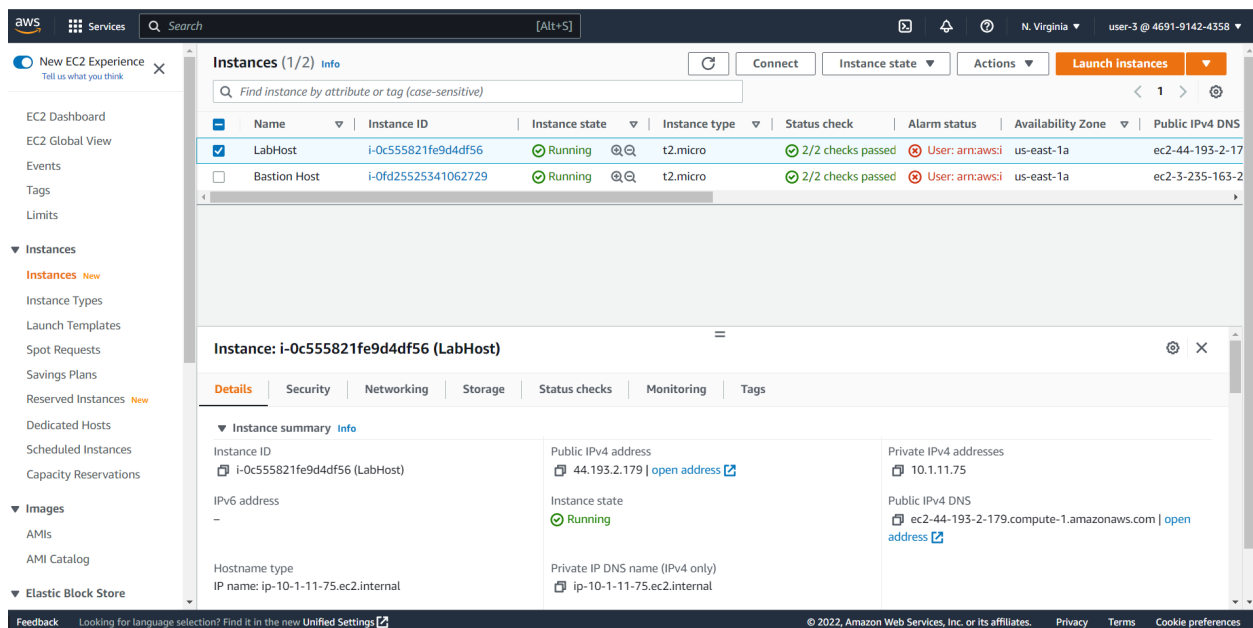
As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.

Select the instance named *LabHost* .

48. In the **Instance state** menu, choose **Stop instance**.

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

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



The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, showing the 'Instances' section. The main content area displays a list of EC2 instances. Two instances are listed: 'LabHost' (Instance ID: i-0c555821fe9d4df56) and 'Bastion Host' (Instance ID: i-0fd25525341062729). Both instances are in the 'Running' state. The 'LabHost' instance is selected. Below the list, the details for the 'LabHost' instance are shown. The 'Instance state' dropdown menu is open, showing the 'Stop instance' option.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
LabHost	i-0c555821fe9d4df56	Running	t2.micro	2/2 checks passed	User: arn:aws:us-east-1a	us-east-1a	ec2-44-193-2-17
Bastion Host	i-0fd25525341062729	Running	t2.micro	2/2 checks passed	User: arn:aws:us-east-1a	us-east-1a	ec2-3-235-163-2

Instance: i-0c555821fe9d4df56 (LabHost)

Instance summary

Property	Value
Instance ID	i-0c555821fe9d4df56 (LabHost)
Public IPv4 address	44.193.2.179 open address
Private IPv4 addresses	10.1.11.75
Instance state	Running
Public IPv4 DNS	ec2-44-193-2-179.compute-1.amazonaws.com open address
Private IP DNS name (IPv4 only)	ip-10-1-11-75.ec2.internal

50. Close your private browser window.