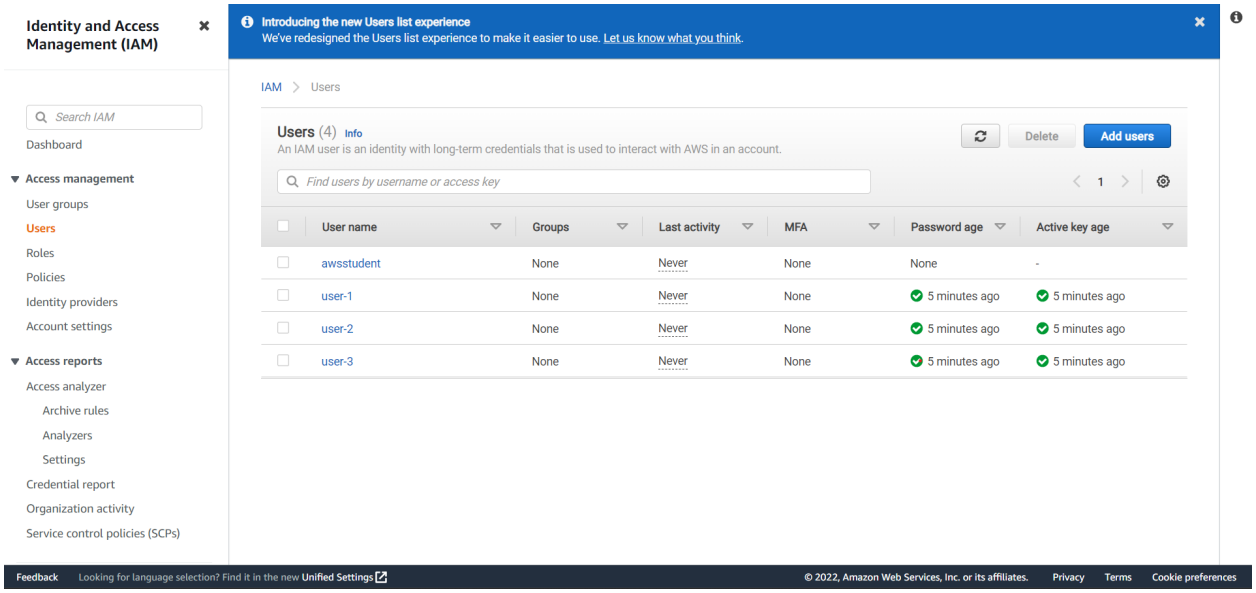
1. Introduction to AWS IAM

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



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

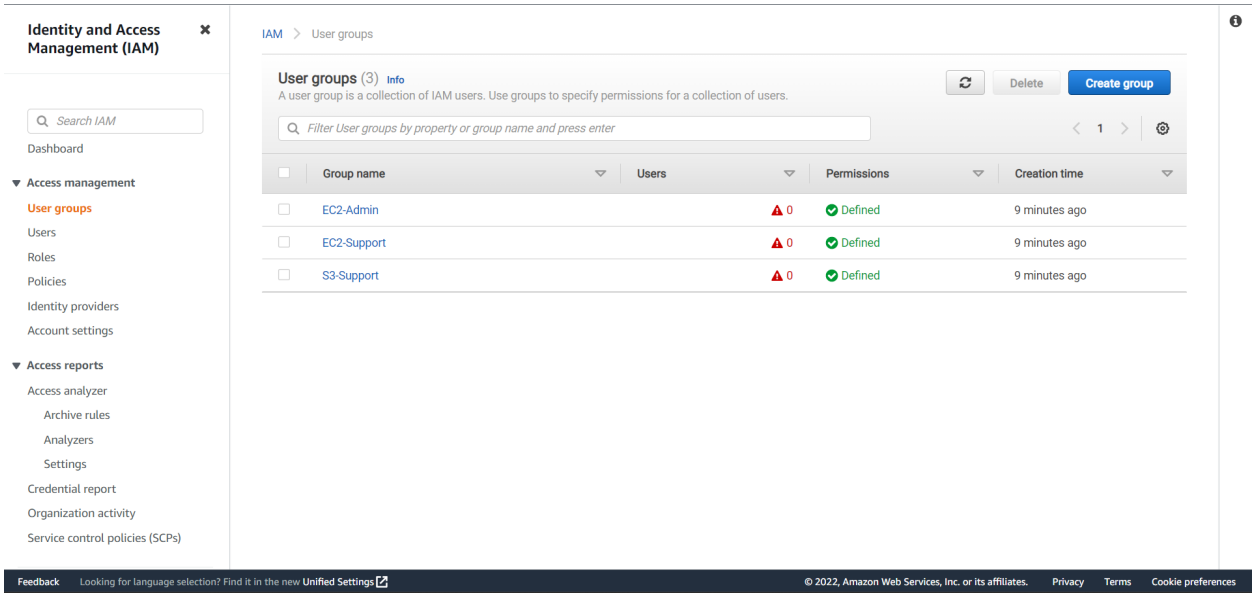
4. Notice that user-1 does not have any permissions.

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:

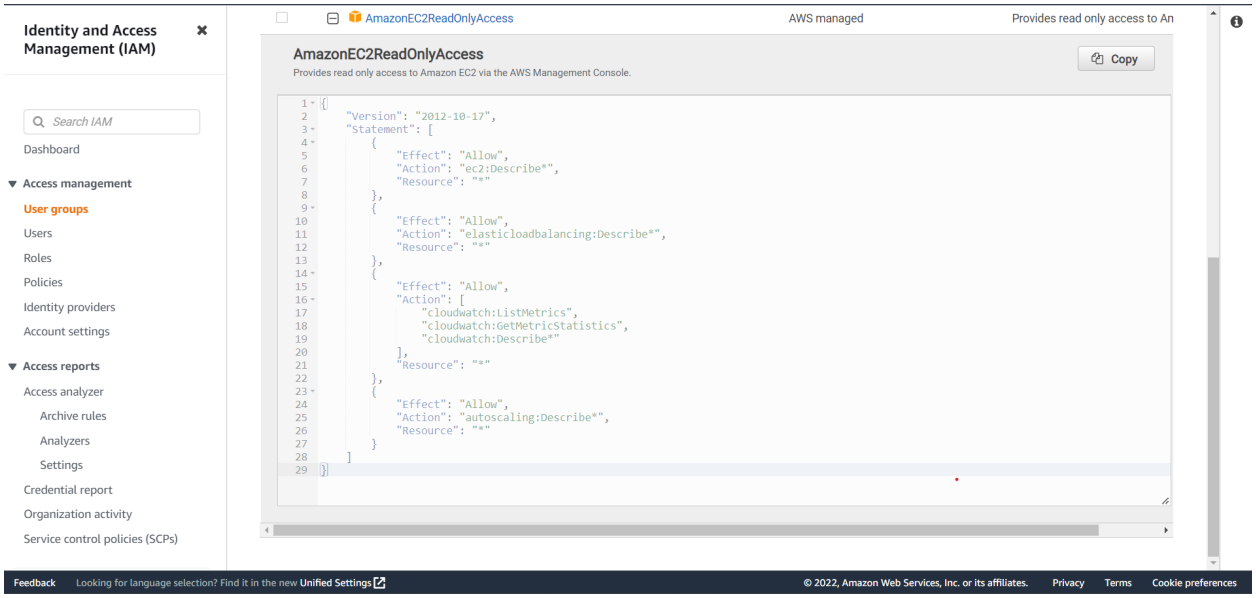
- EC2-Admin
- EC2-Support
- S3-Support



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.

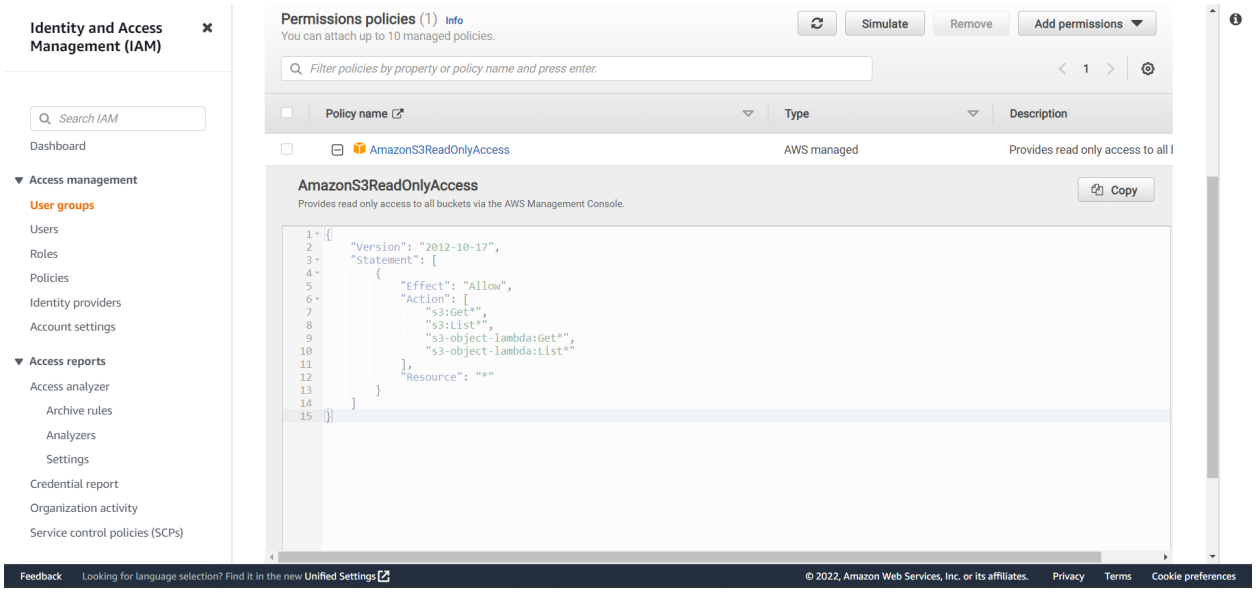


10. The basic structure of the statements in an IAM Policy is:
    - Effect says whether to Allow or Deny the permissions.
    - Action specifies the API calls that can be made against an AWS Service (eg cloudwatch:ListMetrics).
    - Resource defines the scope of entities covered by the policy rule (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

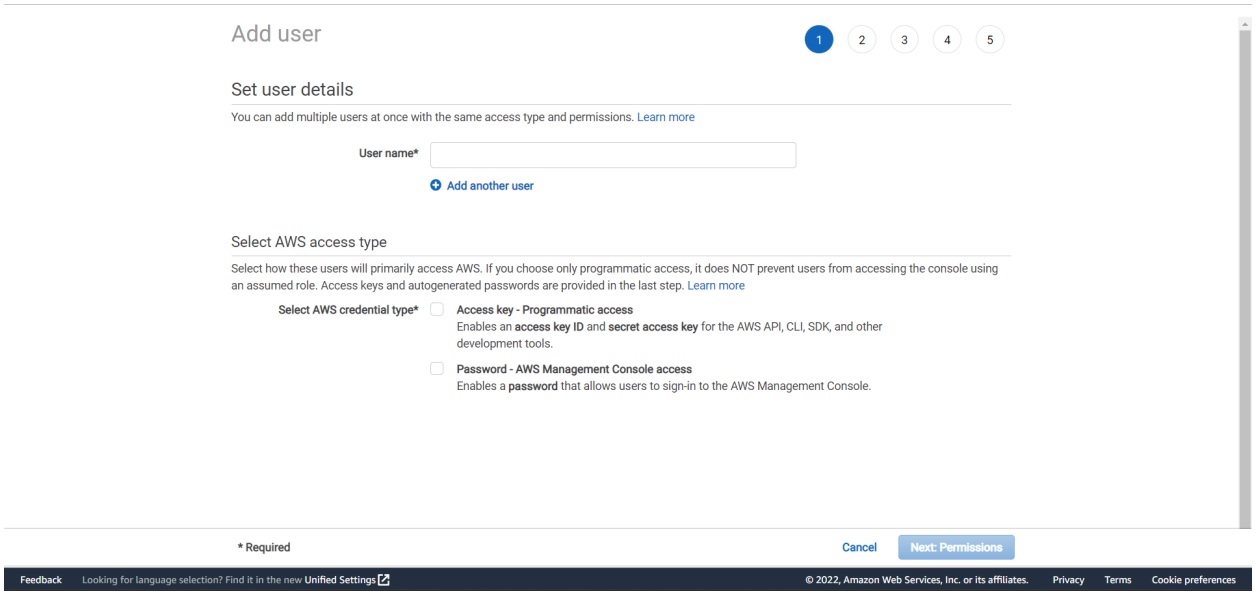
Add user-1 to the S3-Support Group

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

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

21. Choose the **Users** tab.

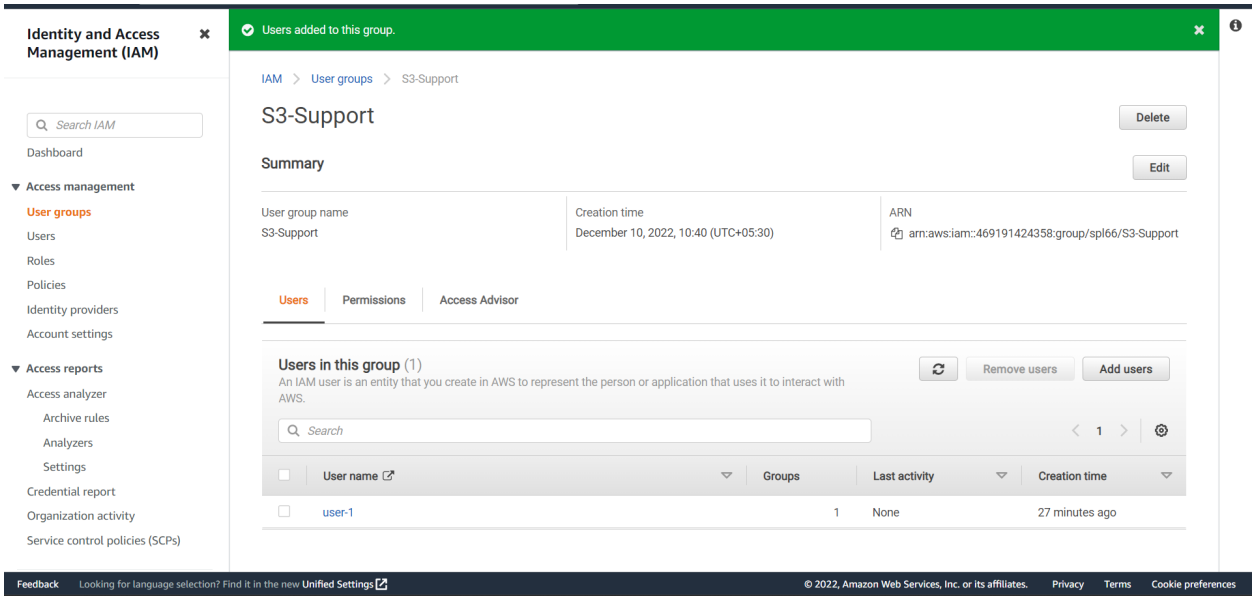
22. In the **Users** tab, choose **Add users**.



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.

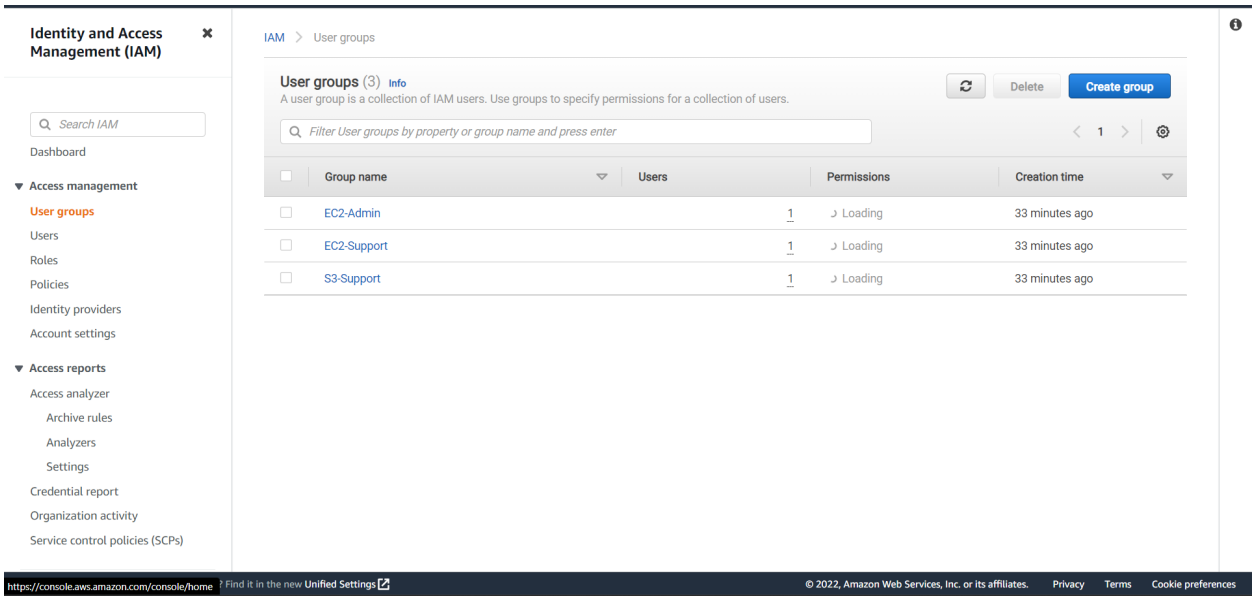
25. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.
user-2 should now be part of the **EC2-Support** group.

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**

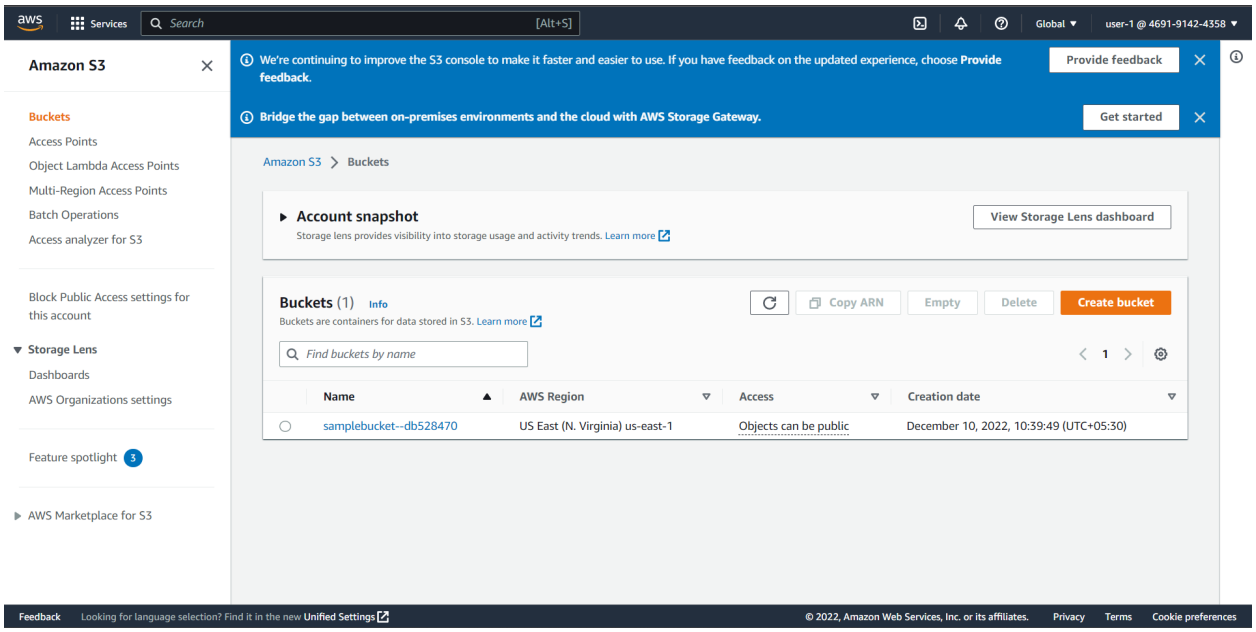
31. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.
Next, you will sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

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.

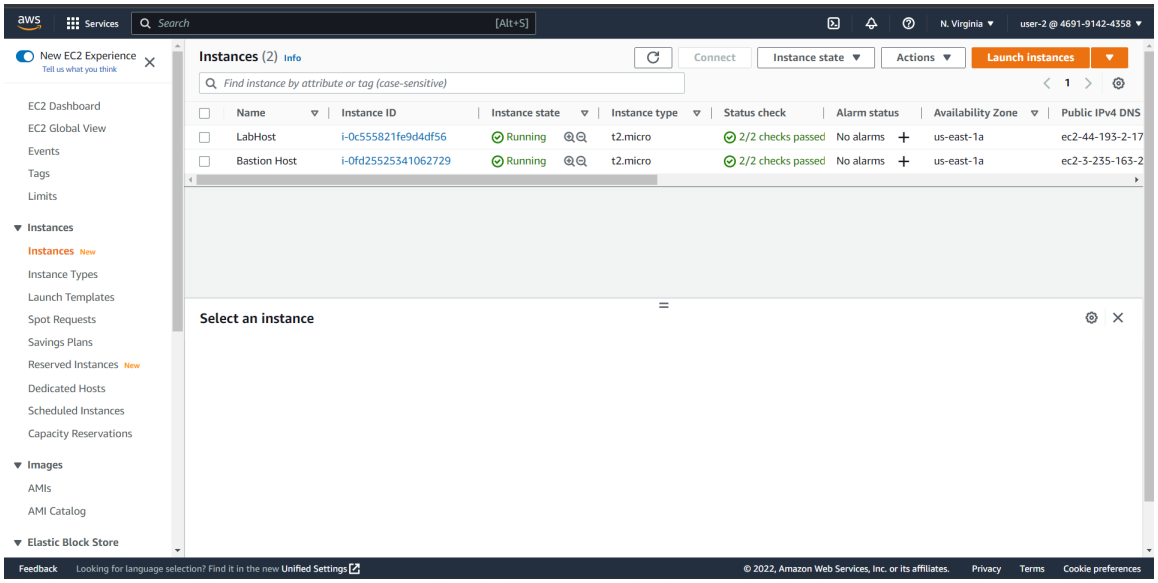
38. Sign-in with:

    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**.

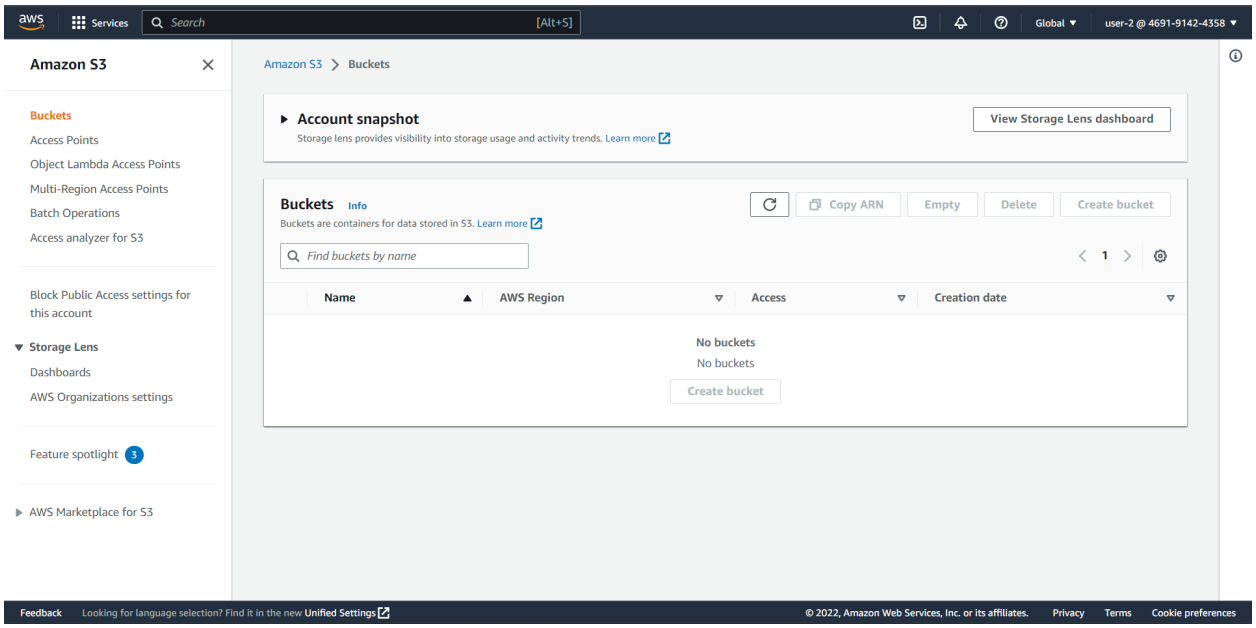
42. In the **Stop Instance** window, select **Stop**.

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**.

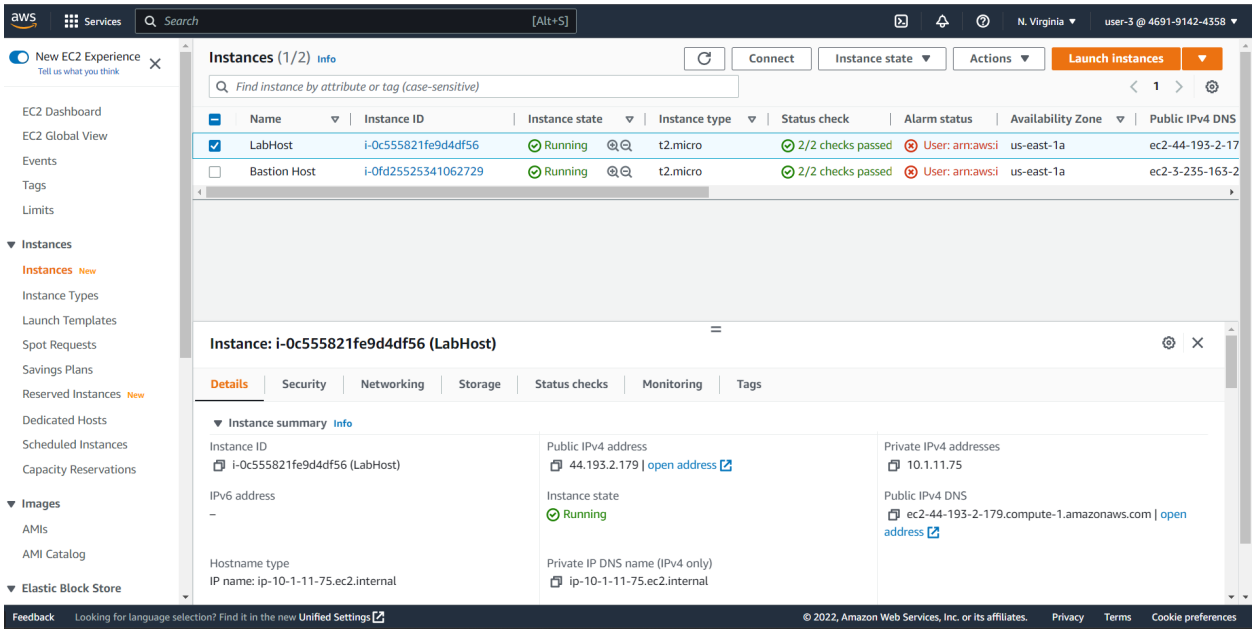
47. In the navigation pane on the left, choose **Instances**.

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.



50. Close your private browser window.