Project in AWS
Practice Lab

Introduction to AWS Identity and Access Management (IAM)

Andra-Diana Popescu

2023

ABOUT THIS LAB

AWS Identity and Access Management (IAM) is a service that allows AWS customers to manage user access and permissions for the accounts and available APIs/services within AWS. IAM can manage users, security credentials (such as API access keys), and allow users to access AWS resources.

In this lab, we will walk through the foundations of IAM. We'll focus on user and group management, as well as how to assign access to specific resources using IAM-managed policies. We'll learn how to find the login URL, where AWS users can log in to their account, and explore this from a real-world use case perspective.

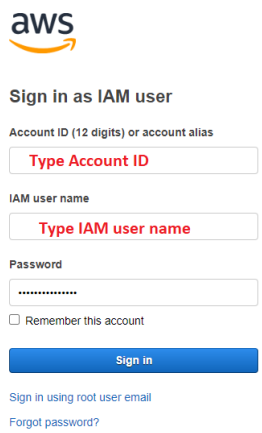
LEARNING OBJECTIVES

- Add the Users to the Proper Groups
- Use the IAM Sign-In Link to Sign-In as a User

Source: https://learn.acloud.guru/course/certified-solutions-architect-associate/

Table of Contents

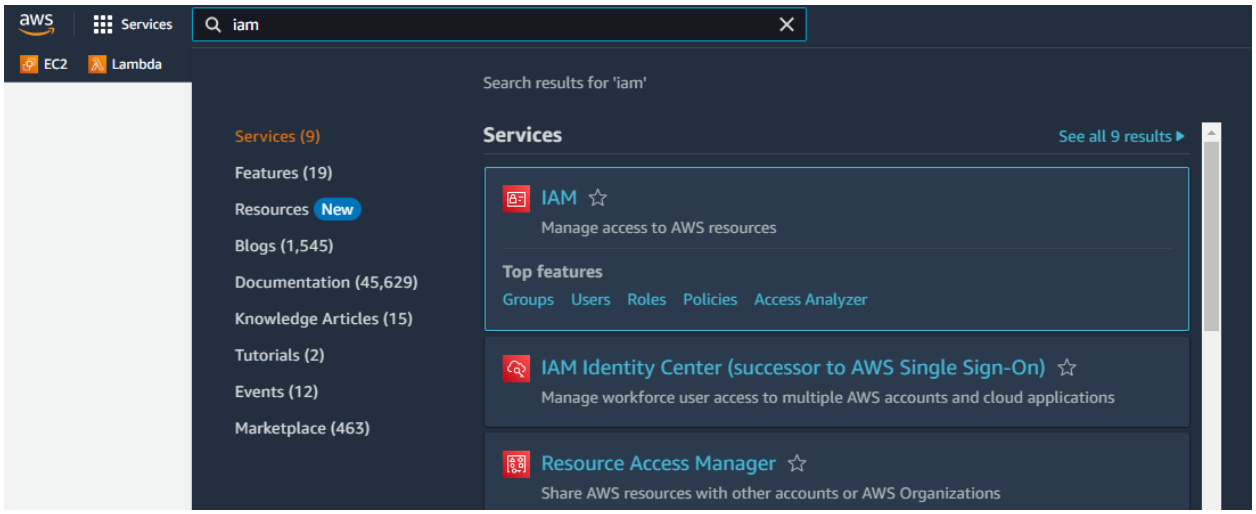
Log in to your AWS account



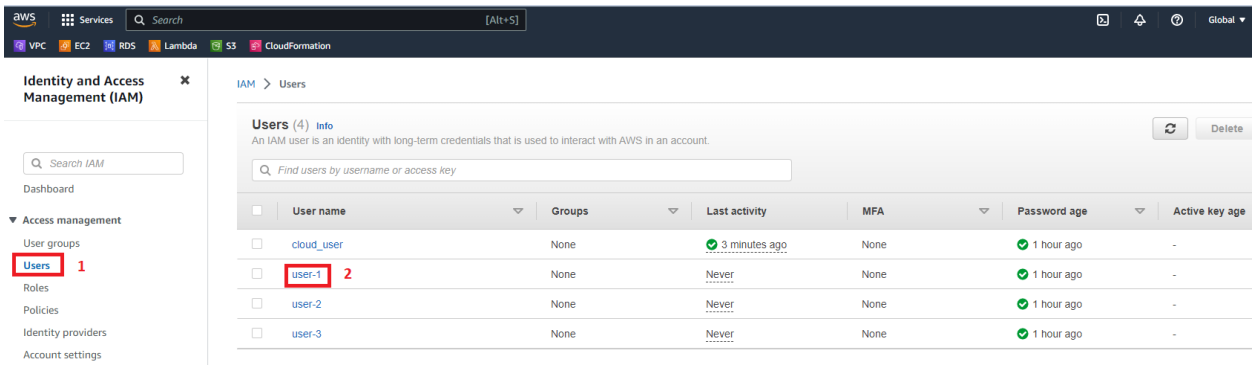
1. Explore Users and Groups

1.1. Explore the Users

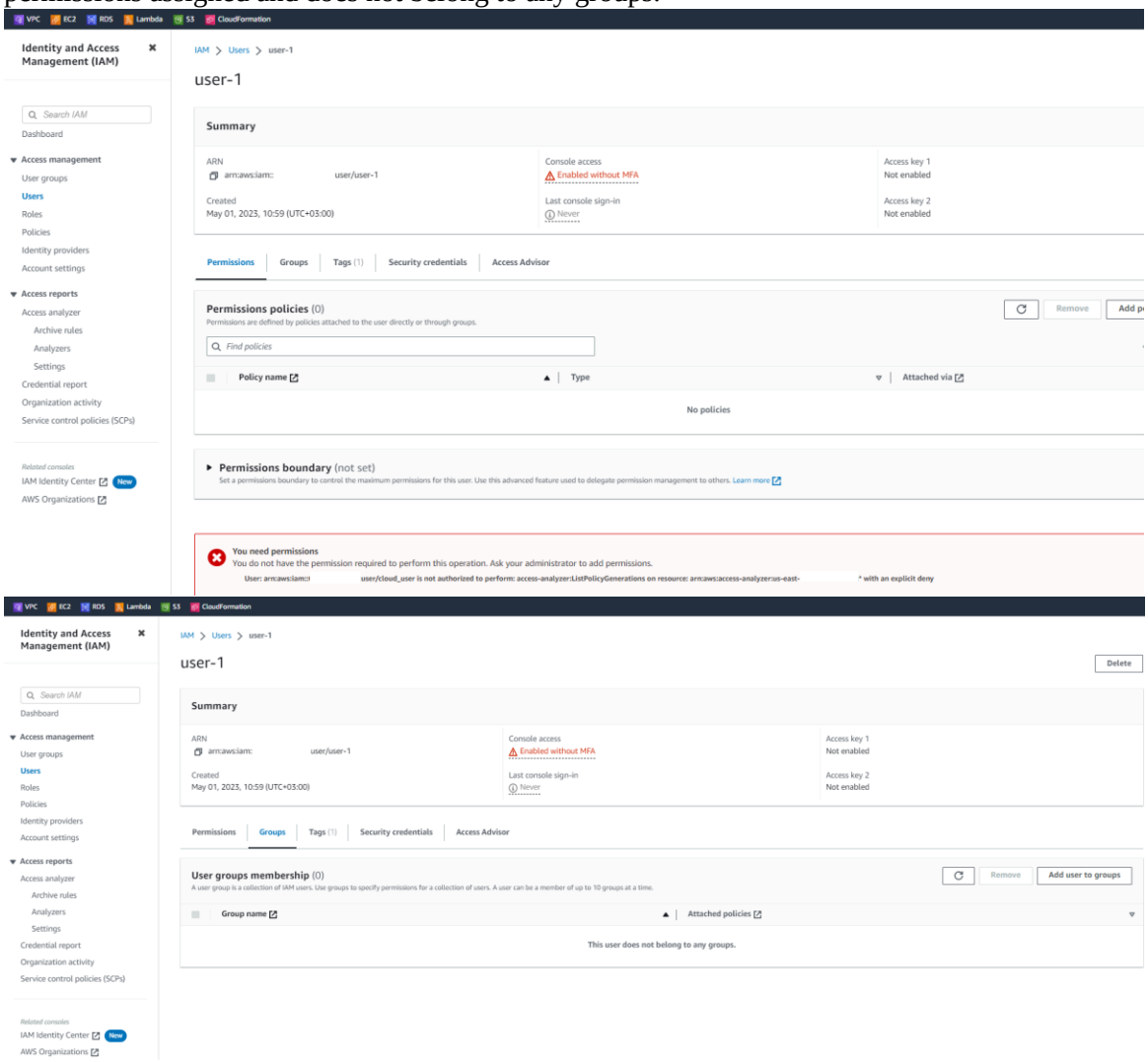
1. Once you are logged in to the AWS Management Console, navigate to IAM.



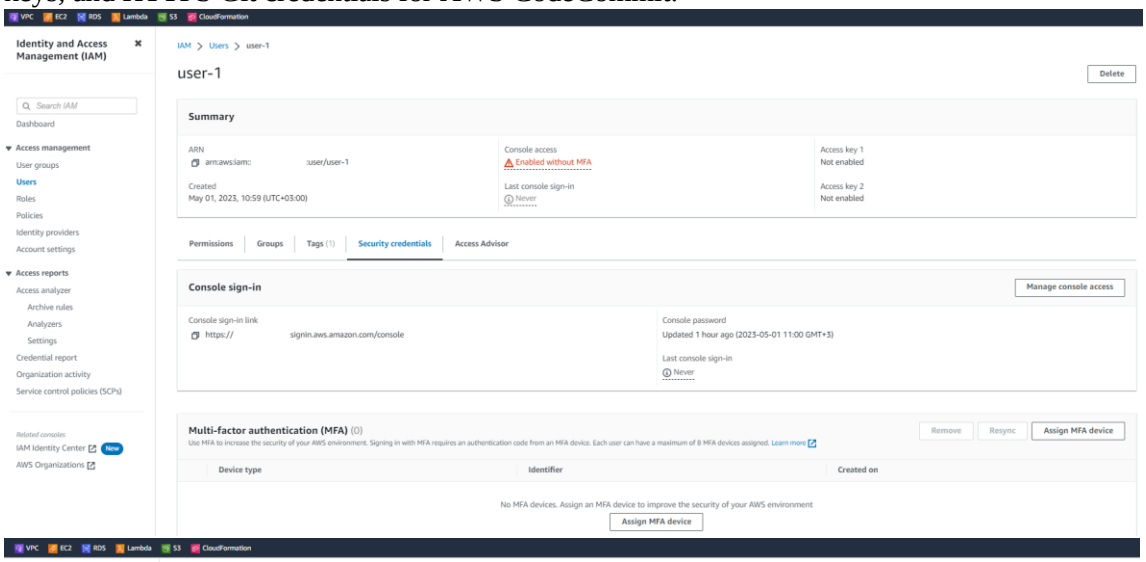
2. From the left-side menu, click **Users**.
3. Select the **user-1** user name

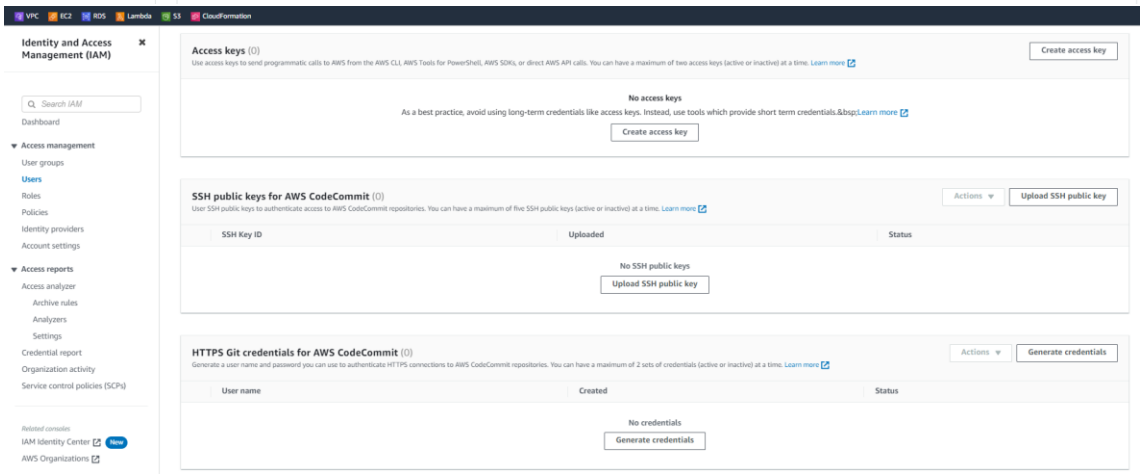


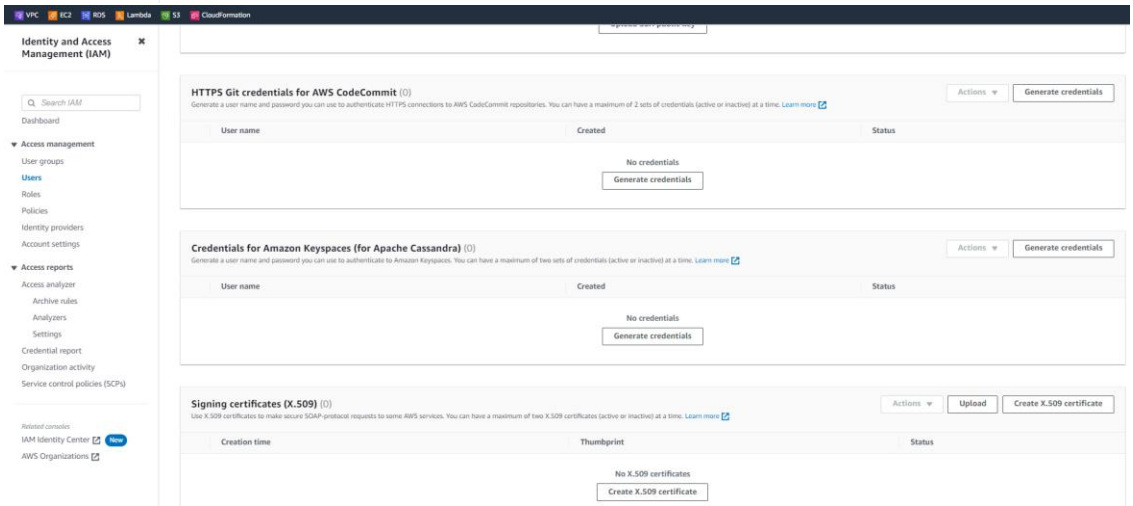
4. Review the resources associated with **user-1**:
   - Select the **Permissions** and **Groups** tabs, where you'll see **user-1** does not have any permissions assigned and does not belong to any groups.



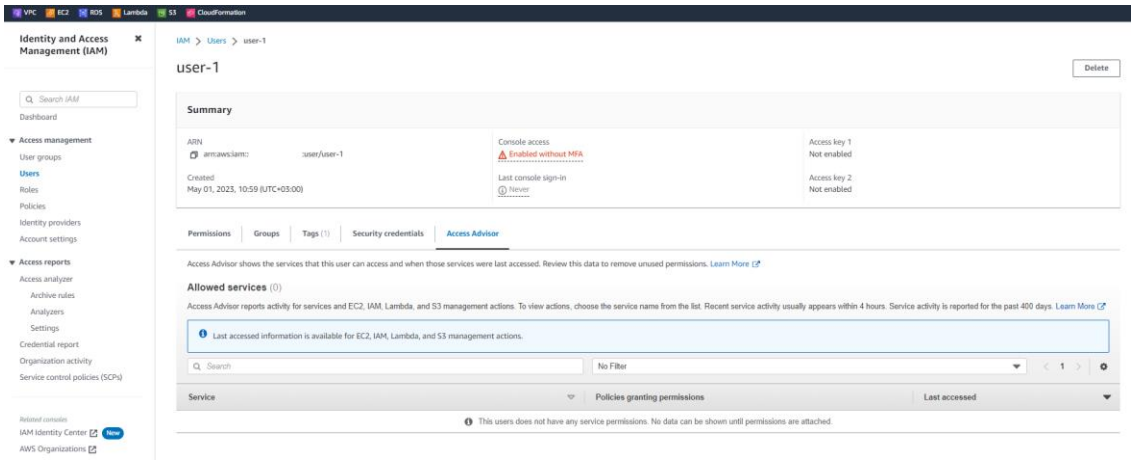
- Select the **Security credentials** tab, where you would see user access keys, SSH public keys, and HTTPS Git credentials for AWS CodeCommit.







- Select the **Access Advisor** tab to see which services the user has accessed and when.



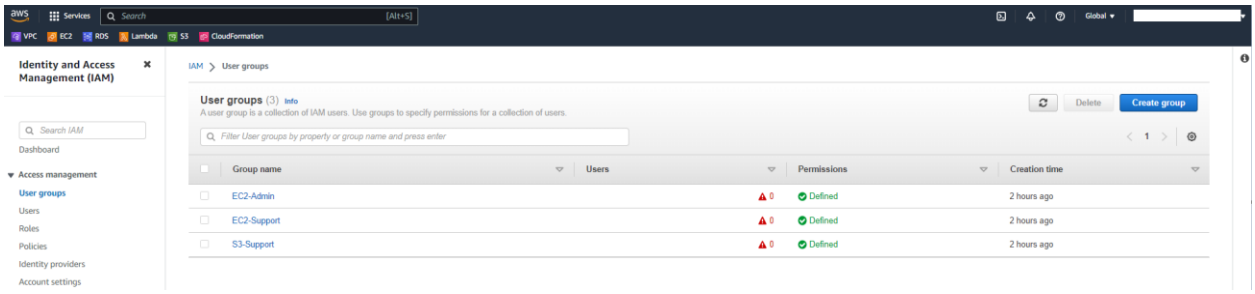
5. At the top of the page, under **Summary**, observe the user's **ARN (Amazon Resource Name)**, path, and creation time.

1.2. Explore the Groups

1. In the IAM sidebar menu, select **User groups**.

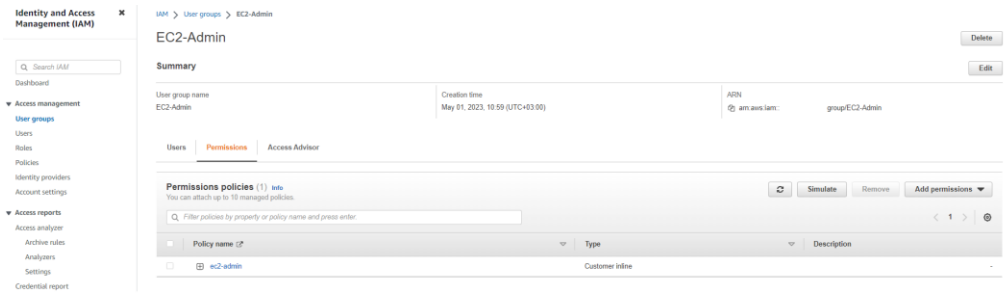
   You should see three provided user groups for this lab:

   - **EC2-Admin**: Provides permissions to view, start, and stop EC2 instances
   - **EC2-Support**: Provides read-only access to EC2
   - **S3-Support**: Provides read-only access to S3

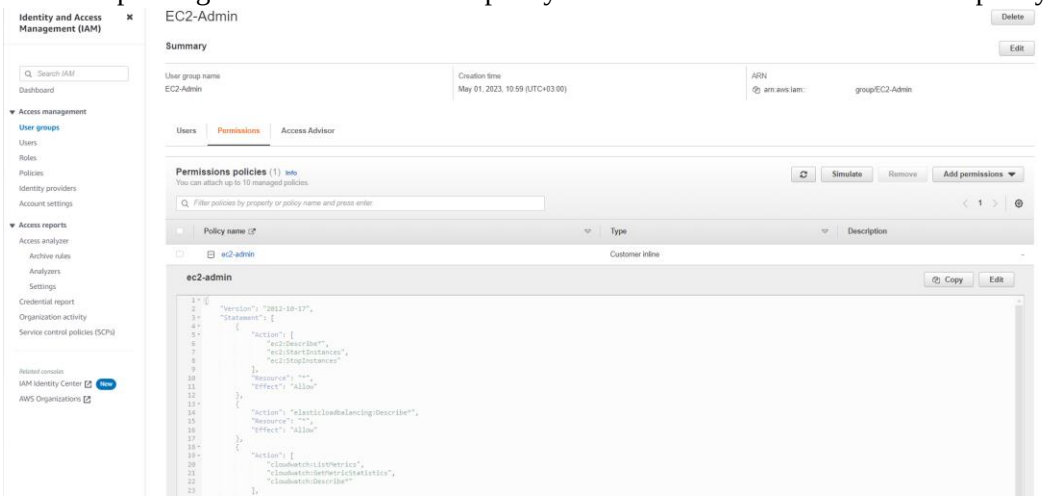


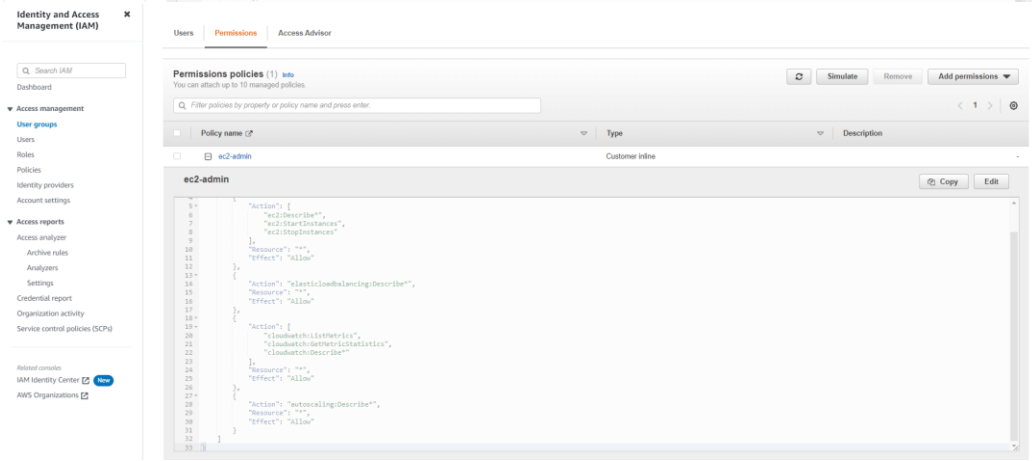
2. Select the **EC2-Admin** group name.
3. Review the resources associated with **EC2-Admin**:

   - Select the **Permissions** tab, where you can see that there is an inline policy associated with the group.



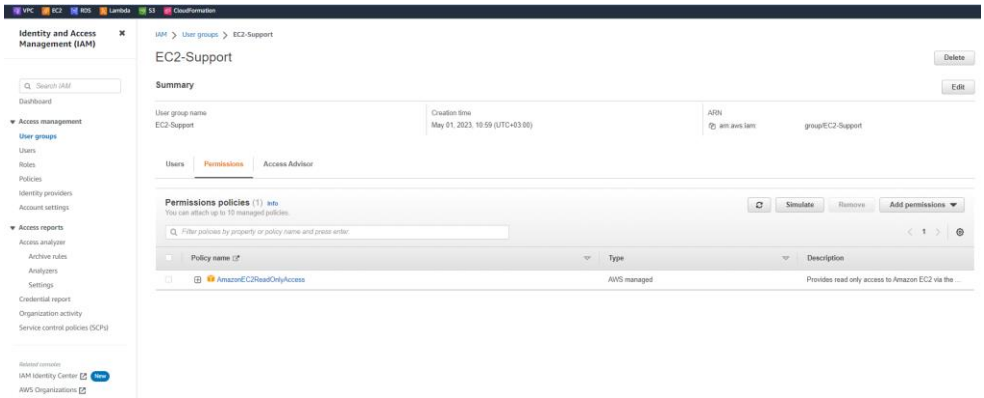
- Click the plus-sign icon to the left of the policy name to view the associated inline policy.



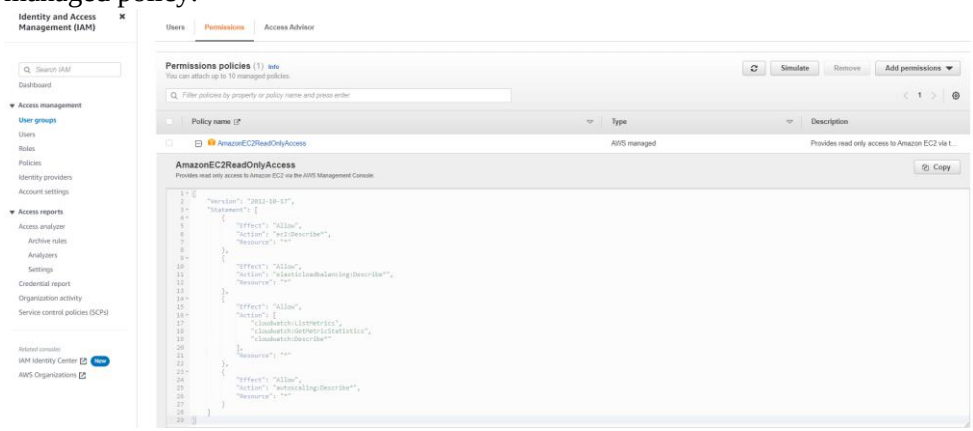


4. Use the breadcrumb along the top of the page to select **User groups**.
5. Select the **EC2-Support** group name.
6. Review the resources associated with **EC2-Support**:

    - Select the **Permissions** tab, where you'll see that the group has an AWS managed policy.

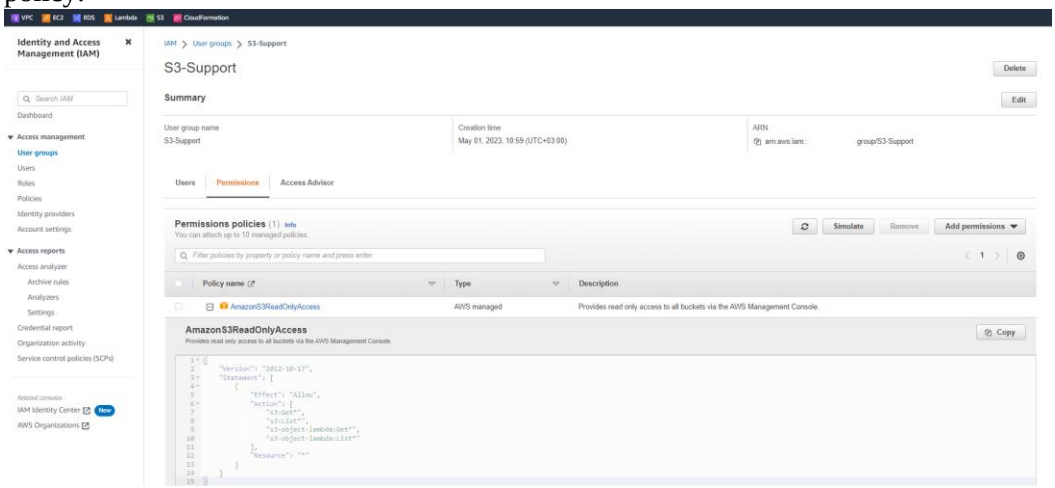


- Click the plus-sign icon to the left of the policy name to view the associated AWS managed policy.



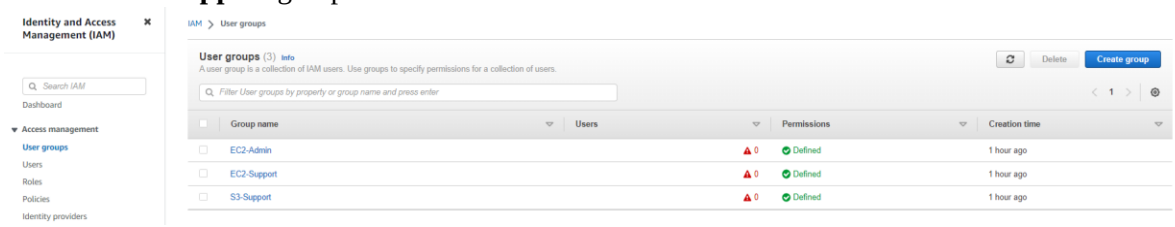
7. Use the breadcrumb along the top of the page to select **User groups**.
8. Select the **S3-Support** group name.
9. Review the resources associated with **S3-Support**:

    - Select the **Permissions** tab, where you'll see that the group is only allowed read-only access.
    - Click the plus-sign icon to the left of the policy name to view the associated read-only policy.

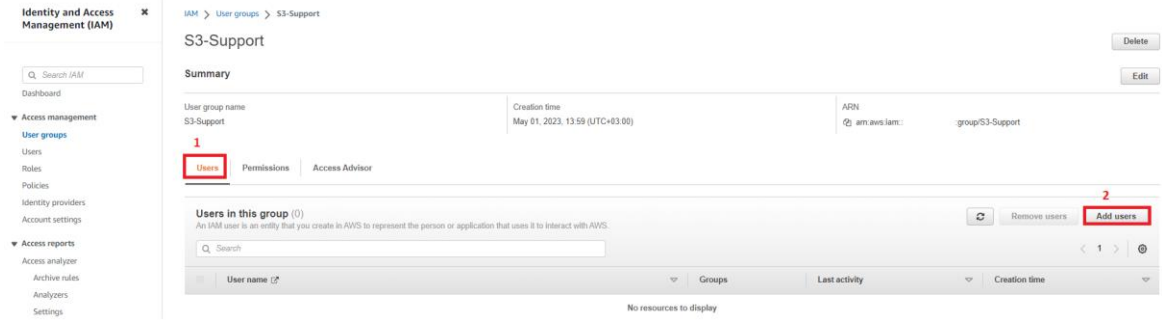


2. Add the Users to the Proper Groups

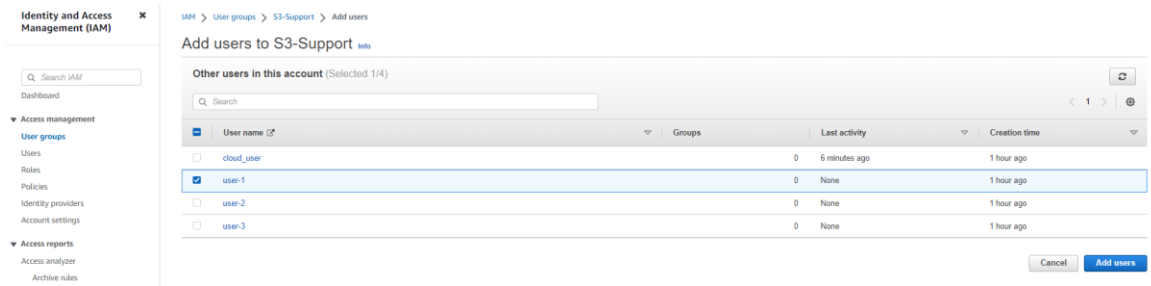
1. Navigate to **IAM**.
2. In the IAM sidebar menu, select **User groups**.
3. Add **user-1** to the **S3-Support** group:
    - Select the **S3-Support** group name.



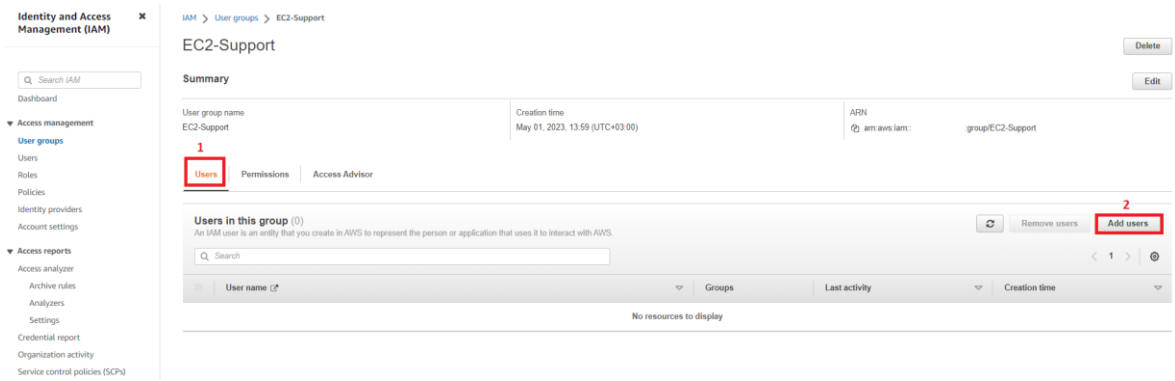
    - Ensure the **Users** tab is selected and then click **Add users** on the right.



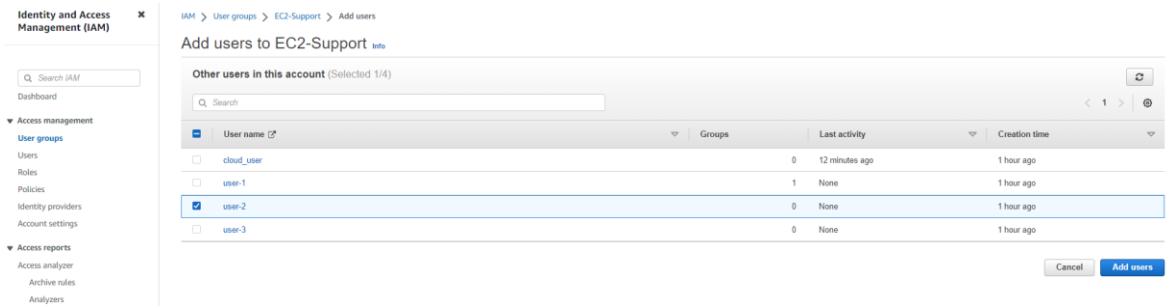
    - From the list of available users, check the checkbox next to **user-1**.
    - Click **Add users**.



4. Use the breadcrumb along the top of the page to select **User groups**.
5. Add **user-2** to the **EC2-Support** group:
    - Select the **EC2-Support** group name.
    - Ensure the **Users** tab is selected and then click **Add users** on the right.

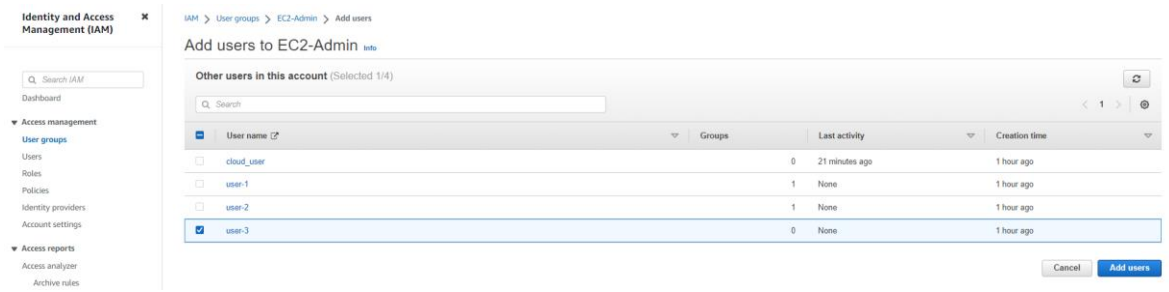


- From the list of available users, check the checkbox next to **user-2**.
- Click **Add users**.

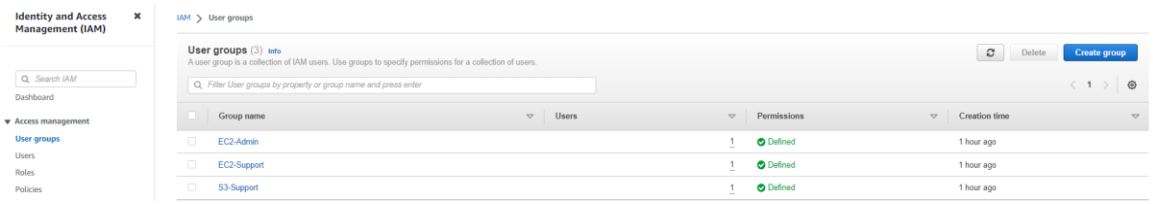


6. Use the breadcrumb along the top of the page to select **User groups**.
7. Add **user-3** to the **EC2-Admin** group:
   - Select the **EC2-Admin** group name.
   - Ensure the **Users** tab is selected and then click **Add users** on the right.

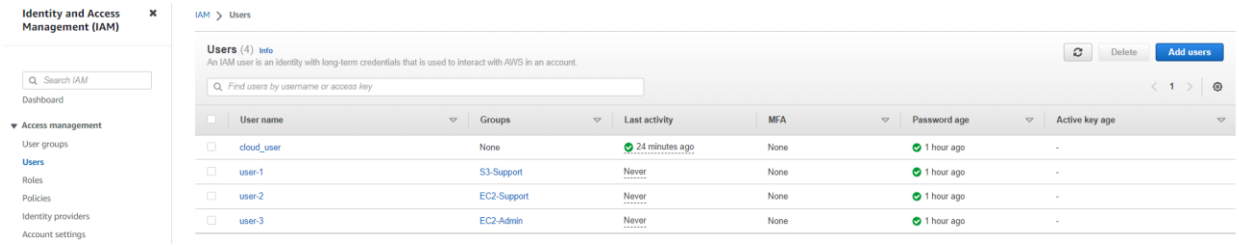
- From the list of available users, check the checkbox next to **user-3**.
- Click **Add users**.



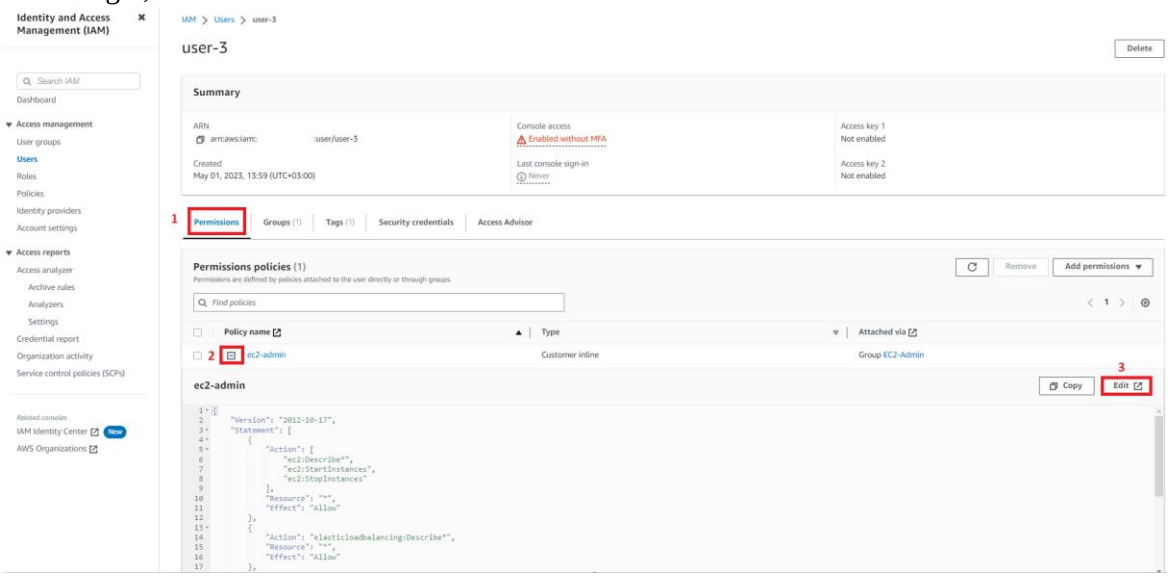
Now we have one user for each of these groups.



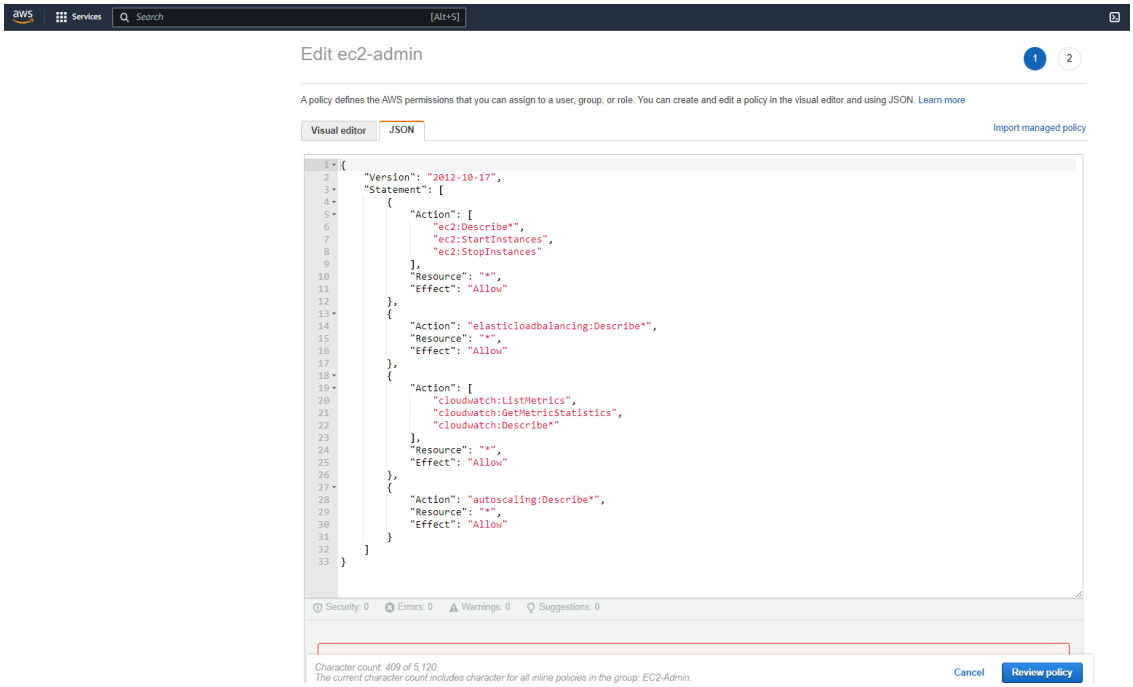
8. In the IAM sidebar menu, select **Users**.



9. Review the permissions for **user-3**:
   - Select the **user-3** user name.
   - Select the **Permissions** tab and then click the plus-sign icon to expand the customer inline policy associated with **user-3**.
   - On the right, click **Edit**.



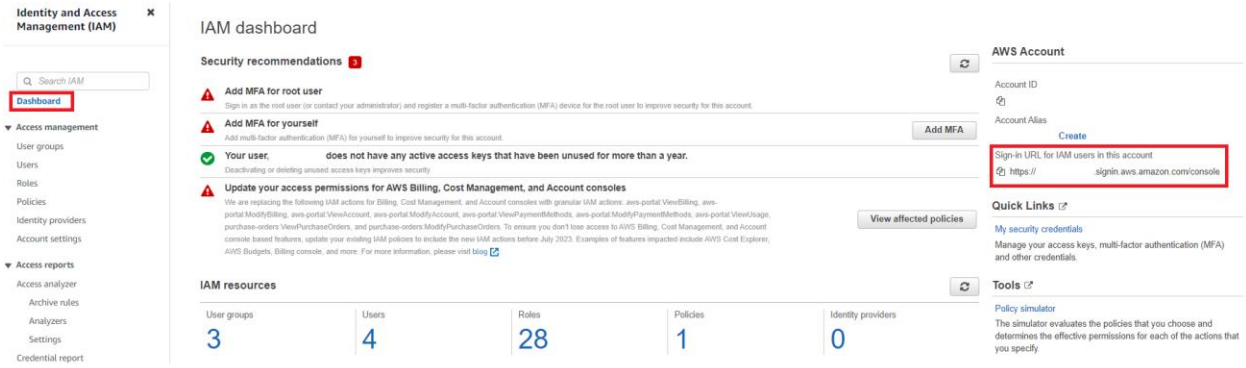
   - Select the **JSON** tab and review the policy permissions, but do not make any changes.
   - Click **Cancel**.



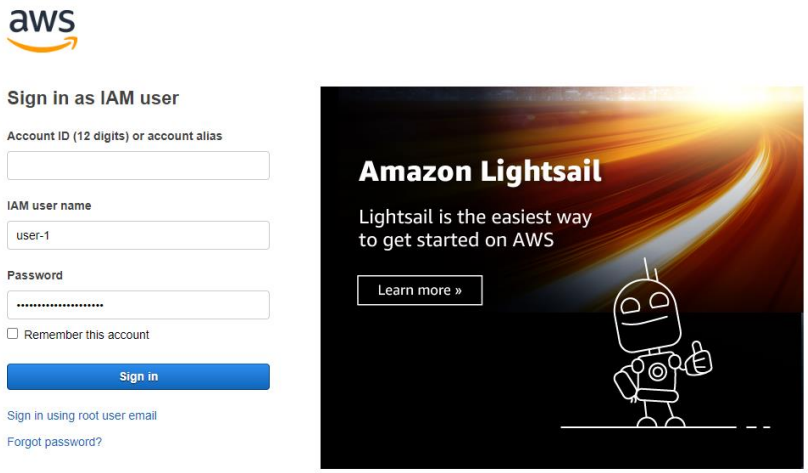
3. Use the IAM Sign-In Link to Sign-In as Each User

3.1. Sign-In as user-1

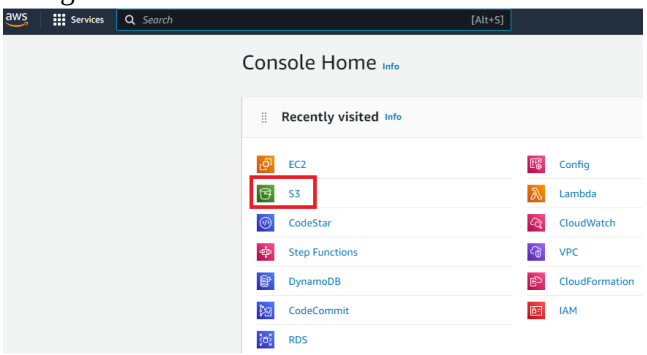
1. In the IAM sidebar menu, select **Dashboard**.
2. In the **AWS Account** section on the right, copy the sign-in URL.



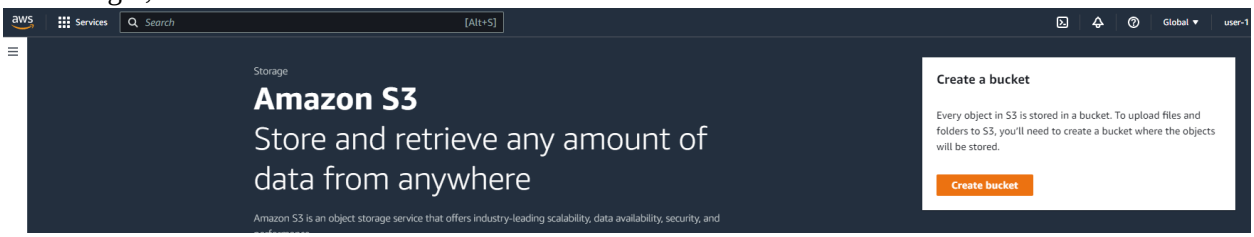
3. In a new browser tab, navigate to the URL.
4. Log in to the AWS Management Console as **user-1** using the password provided in the lab's resources. Remember that this user only has read-only access to S3.



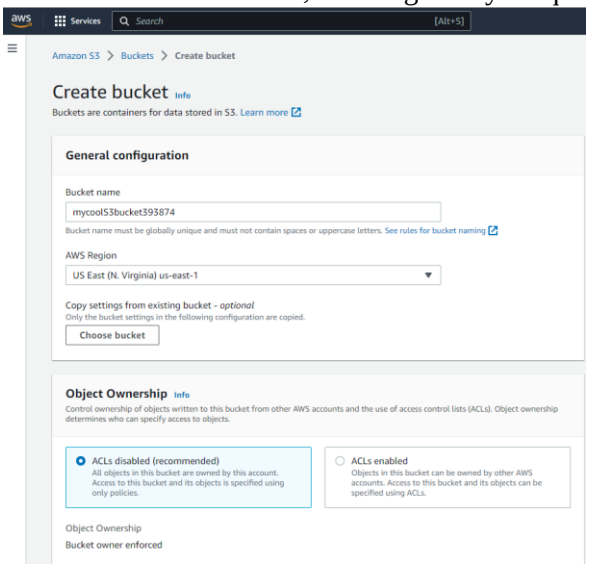
5. Navigate to **S3**.



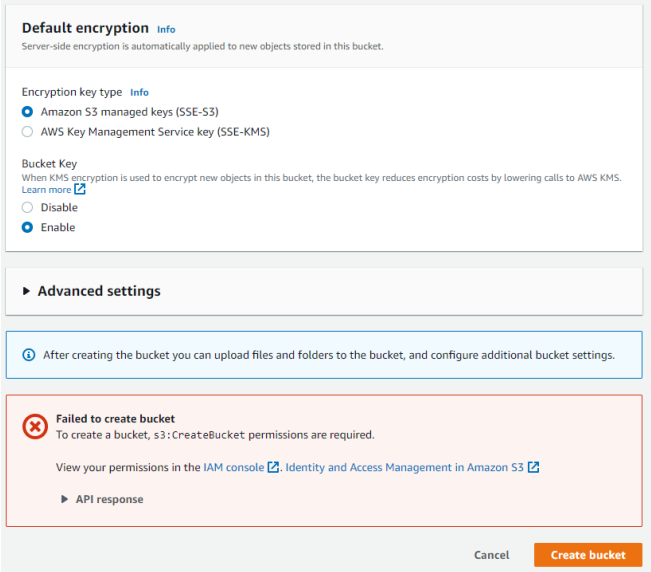
6. On the right, click **Create bucket**.



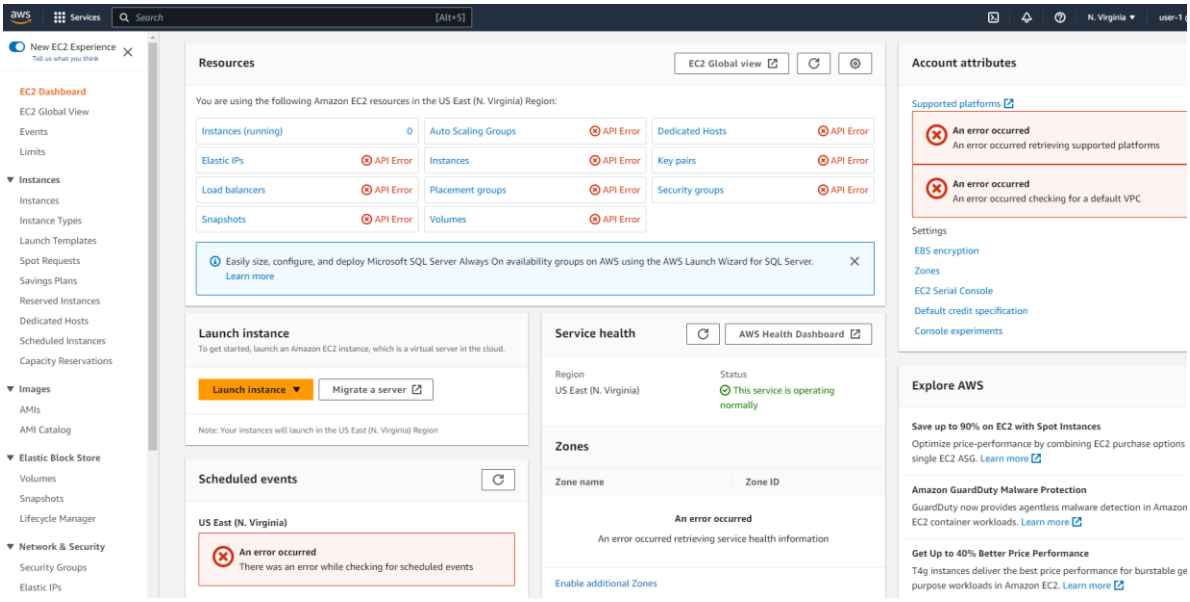
7. In the **Bucket name** field, enter a globally unique bucket name (e.g., mycools3bucket393874).



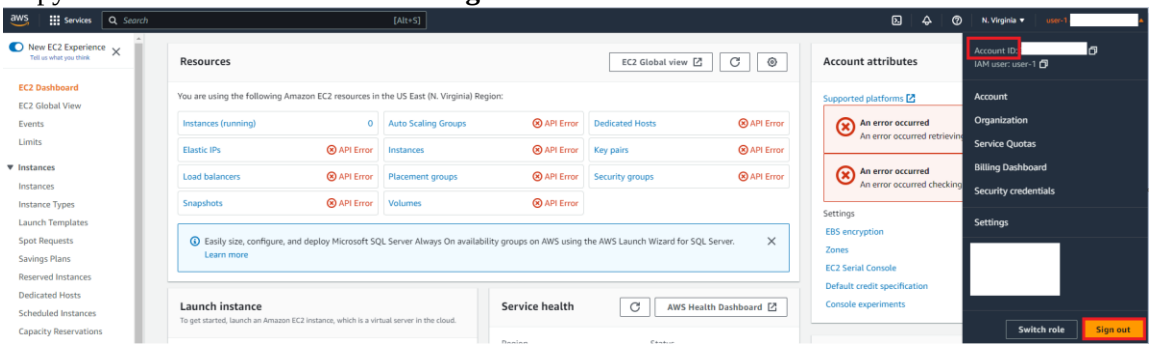
8. Leave all other default settings and click **Create bucket**. You should receive an Access Denied error, indicating that your group policy is in effect.



9. Navigate to **EC2**. You should see a number of API errors, indicating that you do not have access to EC2.

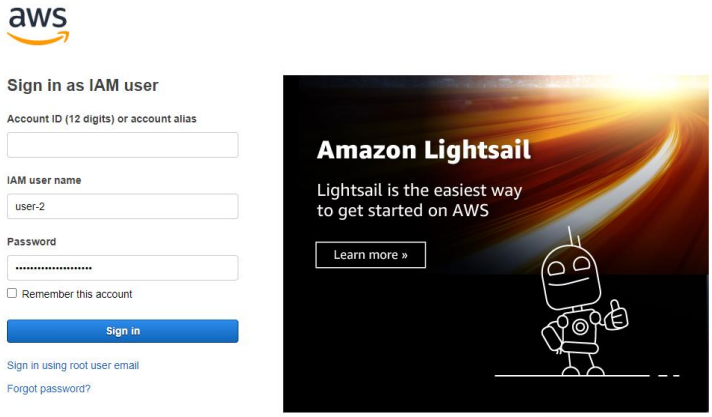


10. In the top right corner of the page, expand the **user-1** dropdown menu.
11. Copy the **Account ID** and then click **Sign out**.

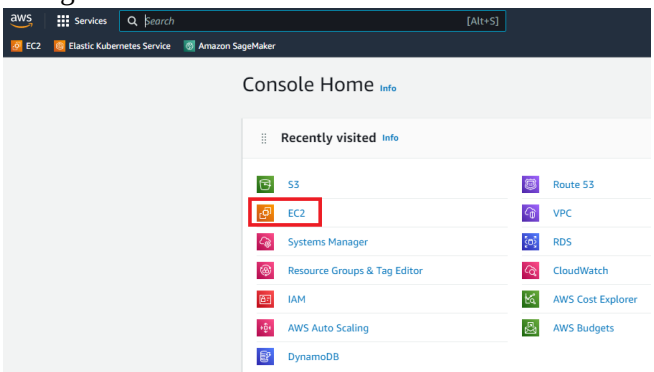


3.2. Sign-In as user-2

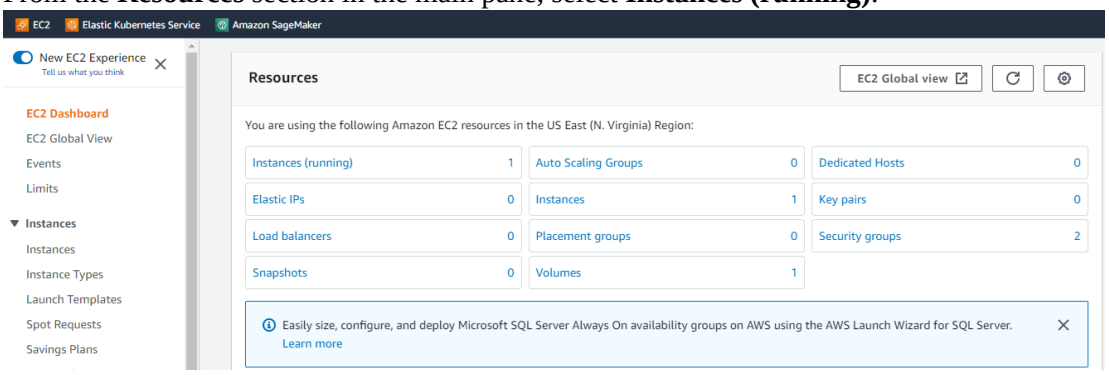
1. Click **Log back** in and then paste your copied account ID in the **Account ID** field.
2. Log in to the AWS Management Console as **user-2** using the password provided in the lab's resources. Remember that this user only has read-only access to EC2.



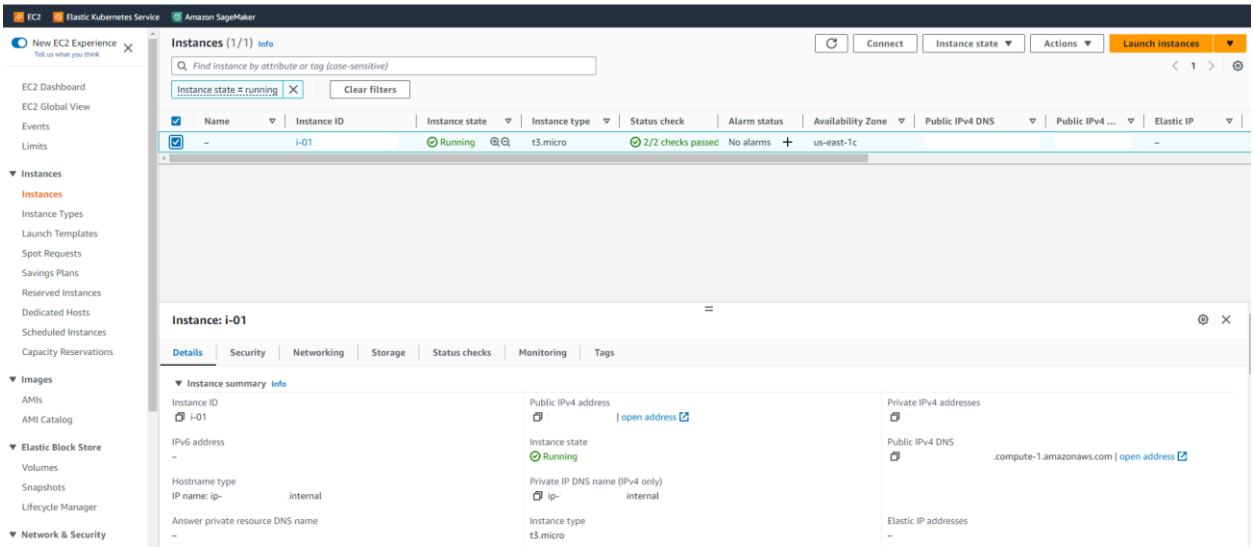
3. Navigate to **EC2**.



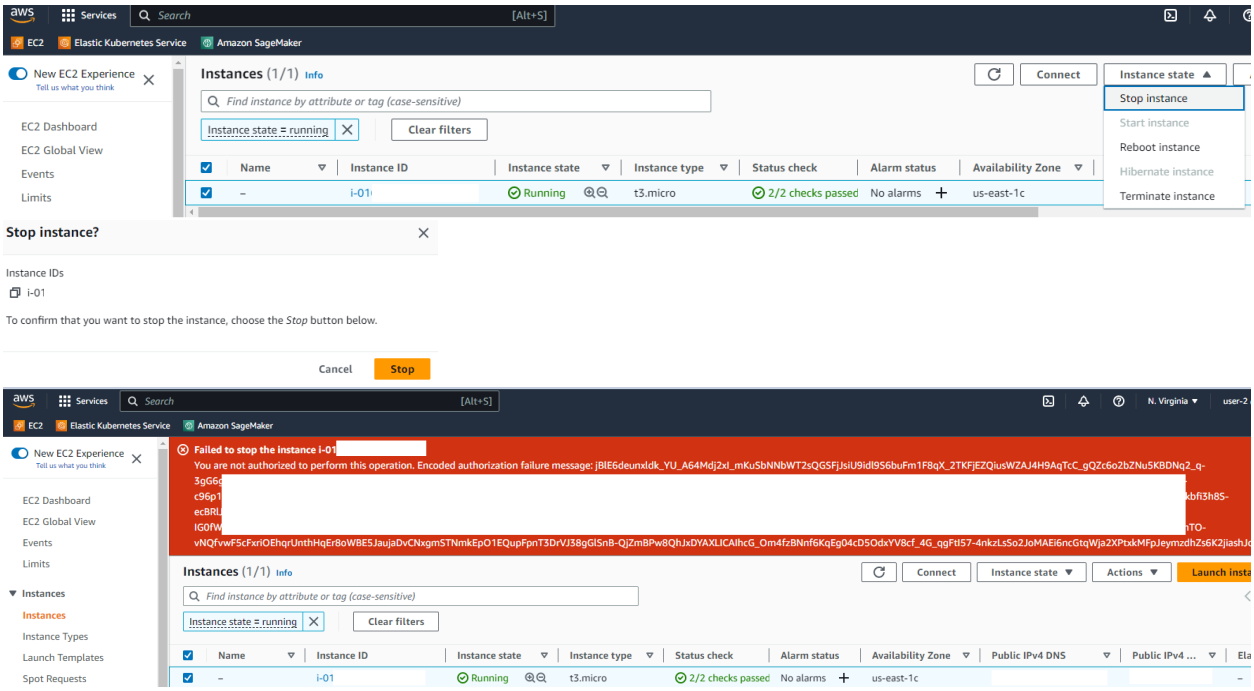
4. From the **Resources** section in the main pane, select **Instances (running)**.



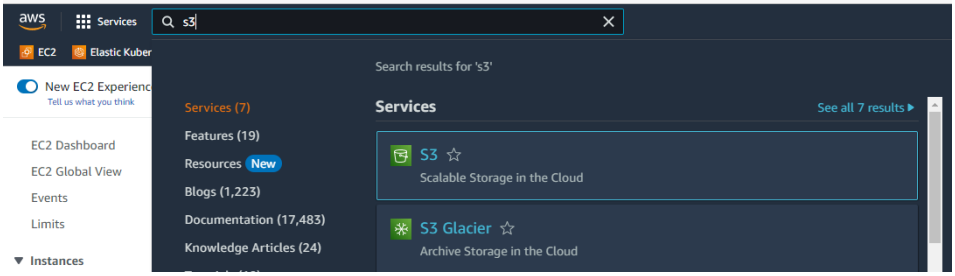
5. Check the checkbox to the left of the running instance and review the instance details.

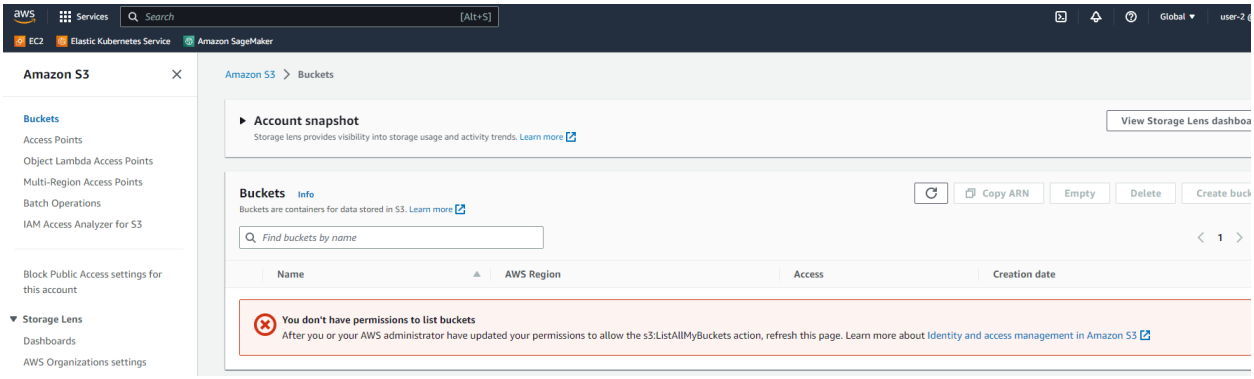


6. Along the top of the page, use the **Instance state** dropdown to select **Stop instance**, and then click **Stop**. You should see an error message, since this user doesn't have the permissions to stop instances.

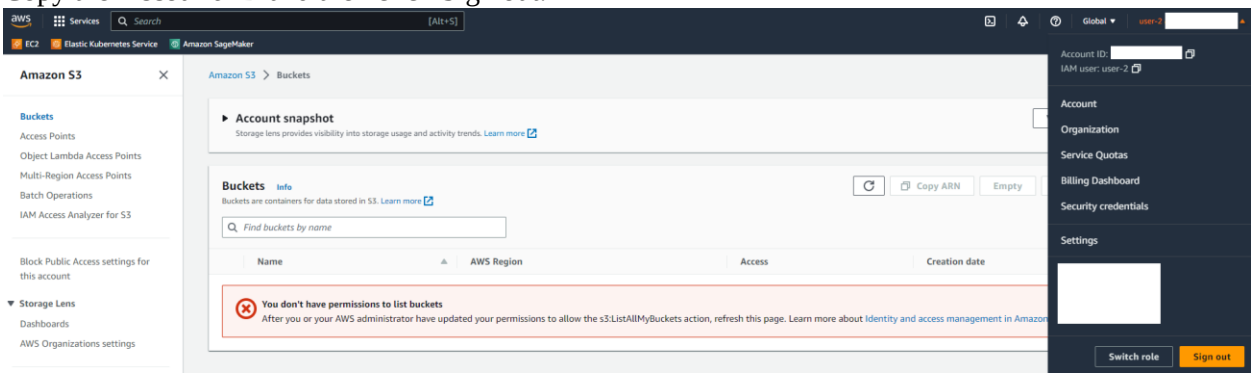


7. Navigate to **S3**. You should see that S3 is unavailable for **user-2** because this user doesn't have any permissions outside of EC2.





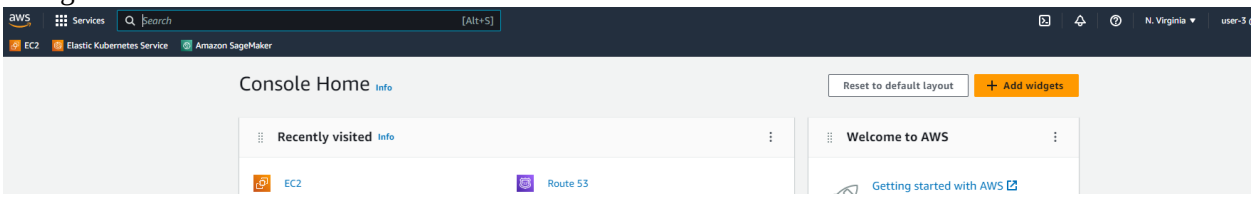
8. In the top right corner of the page, expand the **user-2** dropdown menu.
9. Copy the **Account ID** and then click Sign out.



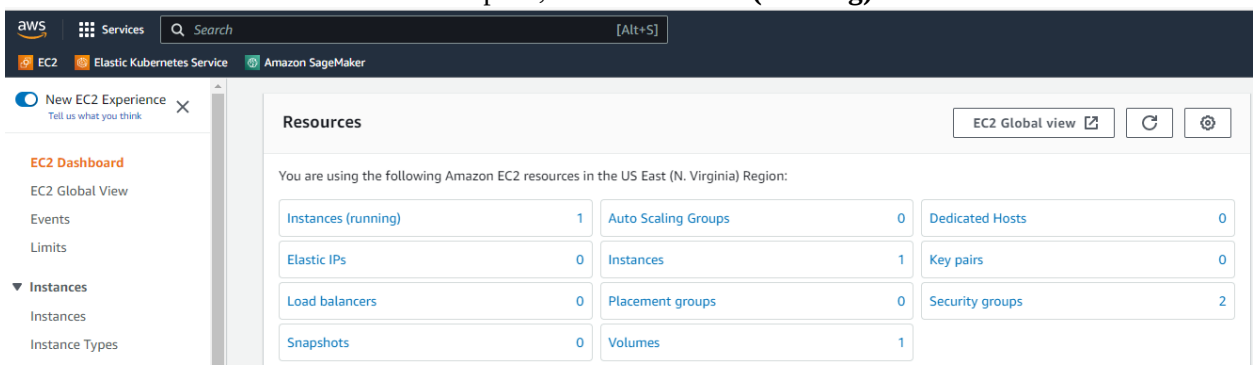
3.3. Sign-In as user-3

1. Click **Log back in** and then paste your copied account ID in the **Account ID** field.
2. Log in to the AWS Management Console as **user-3** using the password provided in the lab's resources. Remember that this user can view, start, and stop EC2 instances.

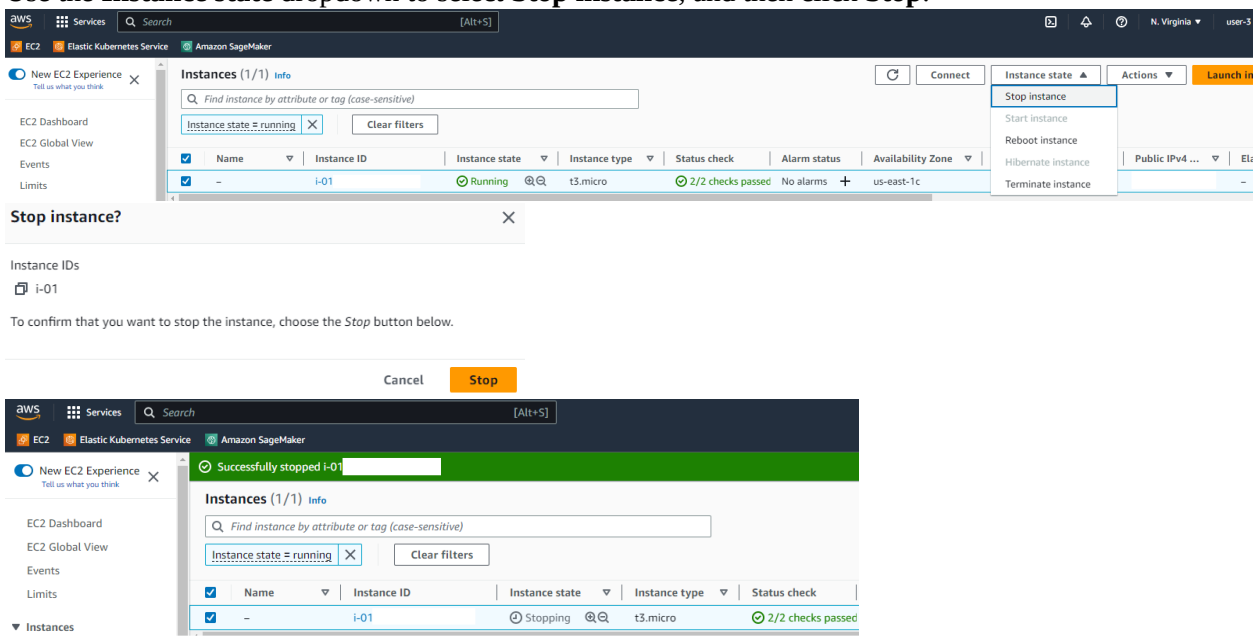
3. Navigate to **EC2**.



4. From the **Resources** section in the main pane, select **Instances (running)**.



5. Check the checkbox to the left of the running instance.
6. Use the **Instance state** dropdown to select **Stop instance**, and then click **Stop**.



7. After a minute, refresh the instances page to verify the instance is now in a **Stopped** state.