

Introduction to AWS IAM

AWS Lab 1

Evan Choi | Cisco CCNP | 4/24/2022

**Background Information**

AWS Identity and Access Management (IAM) is an amazon web service which enables AWS provides customers access to manage users and user permissions within AWS. It gives them access to specify who can access certain services and resources, and under what conditions they can do that. You can use it to manage users, security credentials like access keys, and permissions that determine what AWS resources certain users can use.

With AWS IAM you can manage IAM Users and what they can access by creating Users and assigning them specific security credentials such as multi-factor authentication devices, access keys, and passwords. You can also control what operations a User can perform. Similar, it can manage IAM Roles and what permissions they have, determining what each identity can and can’t do. These roles can be given to anyone based on what access they need. AWS IAM can also be used to manage federated users and what permissions they have. You can enable identity federation which allows users in your enterprise to have access to the management console, and access to call AWS APIs and access resources, all without needing to create separate IAM User’s for each identity.

**Configuration Steps**

Opening AWS

1. Click the start lab button until you get the **“Lab status ready”** message



1. Open the AWS Management Console by clicking the AWS button



1. Take note of the region

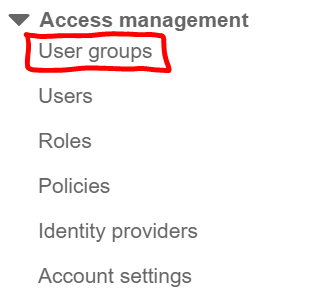


Exploring AWS

1. Click the **All services** dropdown and scroll until you see **IAM**, then click it



1. On the dashboard, click **User Groups**

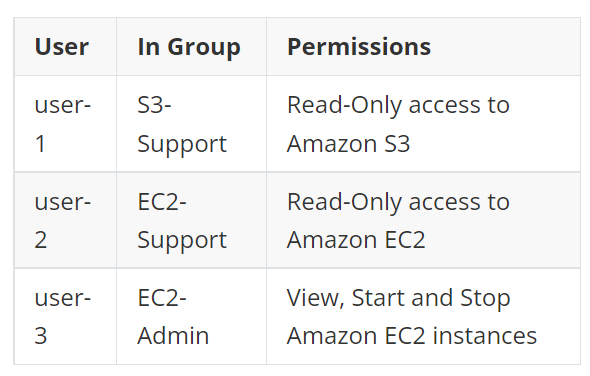


1. Select the **EC2-Support** group
2. Click the **Permissions** tab
3. Click the **+** icon next to **AmazonEC2ReadOnlyAccess** to open the policy details. The policy details tell us what actions are allowed and what actions are denied for each specific AWS resource. **Effect** tells us if the permission is Allowed or Denied, **Action** specifies what API calls can be made, and **Resource** tells us which entities are covered by the policy

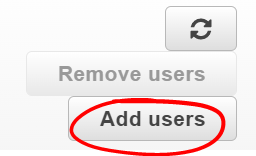


Business Scenario

1. You want to give your staff access to AWS EC2 instances based on their job function



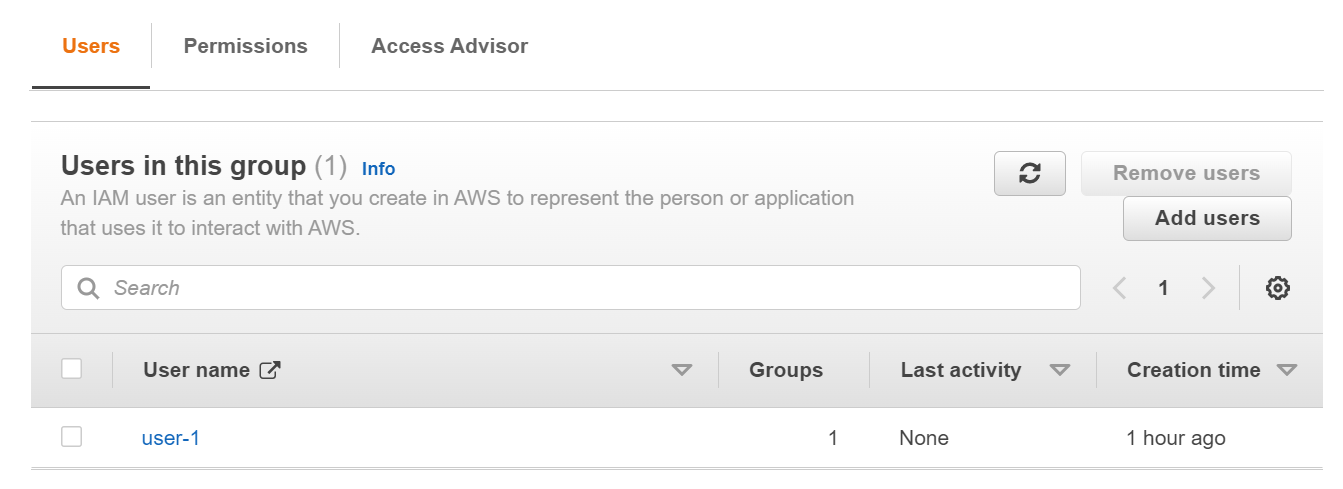
1. On the left navigation pane, select **User groups**
2. Select the **S3-Support** group
3. In the **Users tab**,select click the **Add users** button



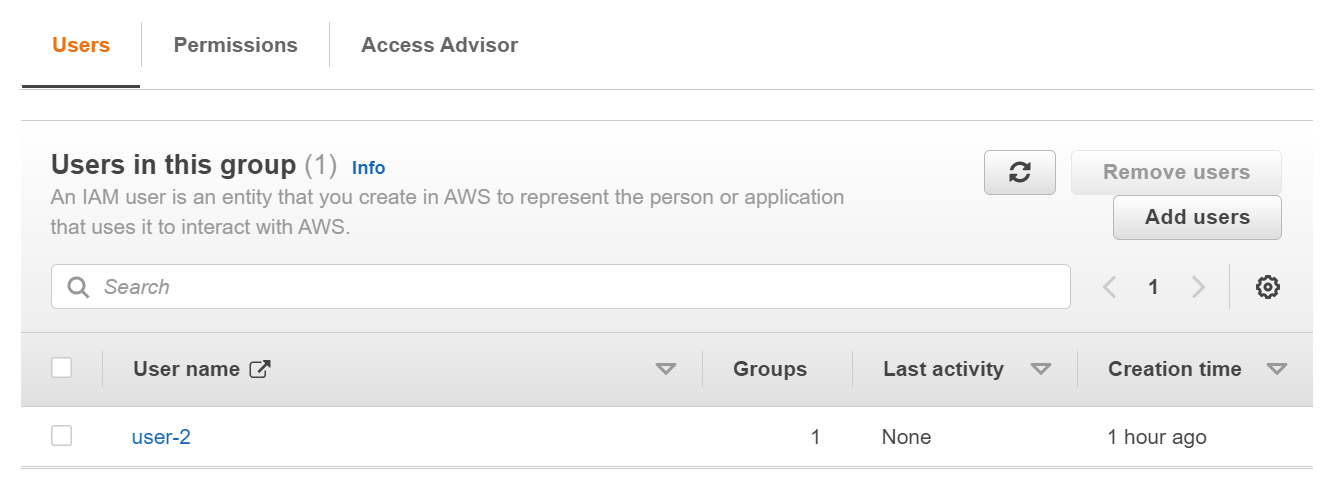
1. Click the box next to **user-1** and select **Add Users**



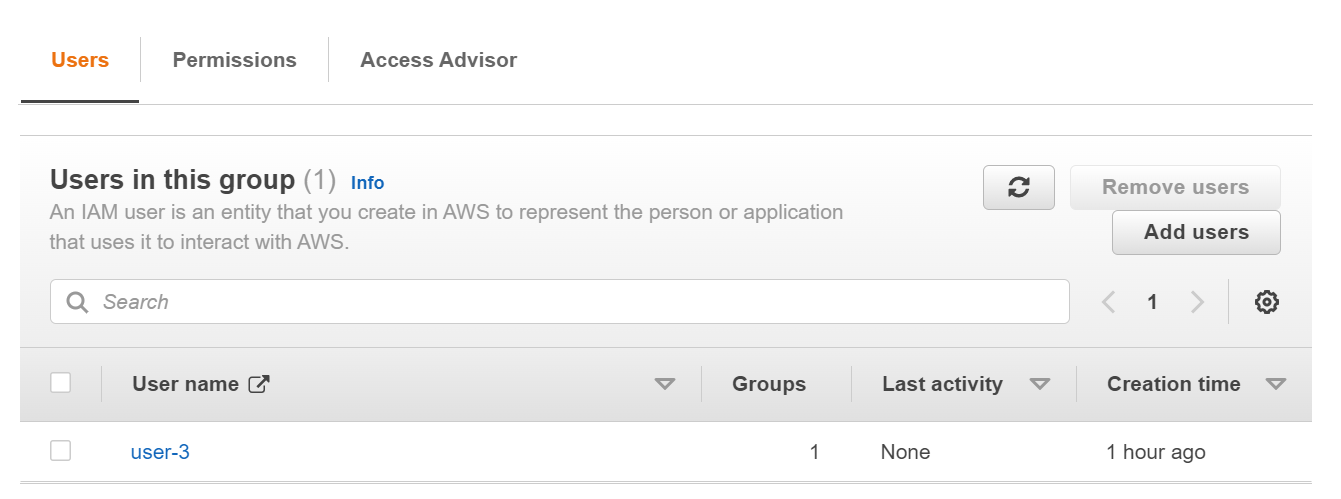
1. In the **Users** tab, **user-1** should be added to the group



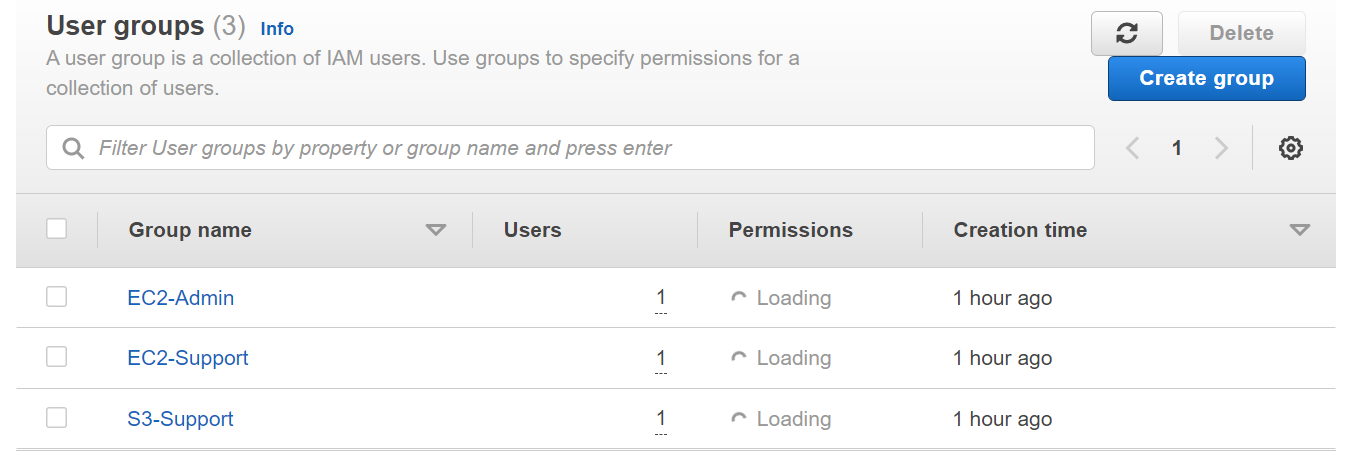
1. **User-**2 was hired into a role where they provide support for Amazon EC2. Following steps 9-13, add **user-2** to the **EC2-Support** group
2. It should look like this once **user-2** is a part of the **EC2-Support** group



1. **User-3** was hired as the Amazon EC2 administrator, who will be managing your EC2 instances. Following steps 9-13, add **user-3** to the **EC2-Admin** group.
2. It should look like this once **user-3** is a part of the **EC2-Admin** group

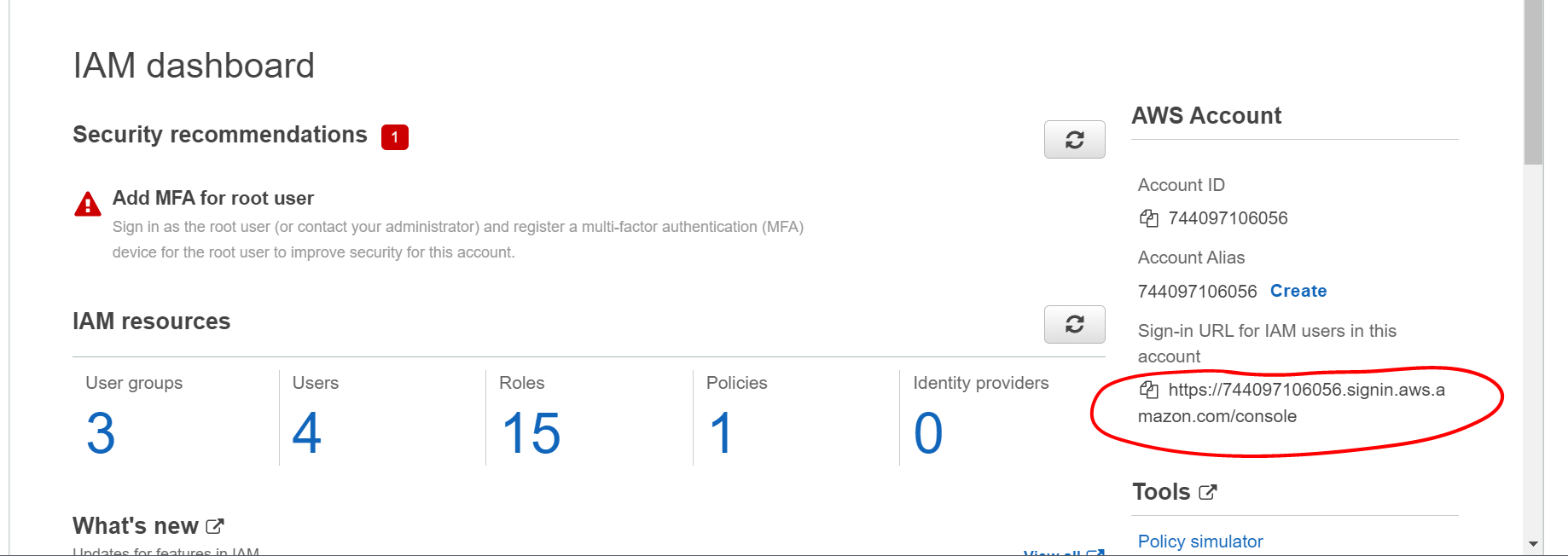


1. To verify you did it right, choose **User groups** in the navigation pane. There should be a **1** in the Users column for each group. If there isn’t go back to the steps above

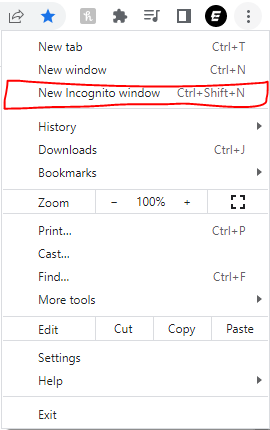


Sign-In and Test Users

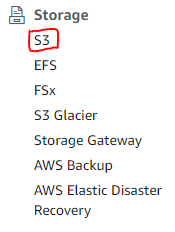
1. Choose **Dashboard** in the navigation pane
2. Find the **IAM users sign-in link** on the right side of your screen and copy it



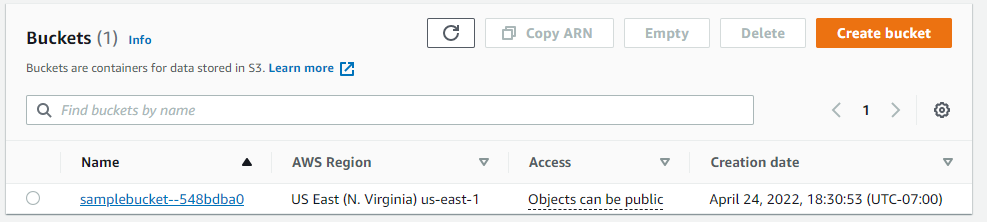
1. Open an Incognito window by clicking on the 3 dots at the top-right of your screen, then select **New Incognito Window**



1. Paste the **IAM users sign-in** link into the address bar
2. Sign-in as **user-1** using the **IAM user name:** user-1 and the **password:** Lab-Password1
3. Click the **All Services** menu, and choose **S3**



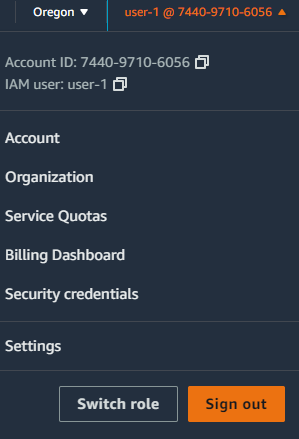
1. Click the bucket in the account. Because **user-1** is in the **S3-Support** Group in IAM, it has permission to view a list of Amazon S3 buckets. It doesn’t have any objects.



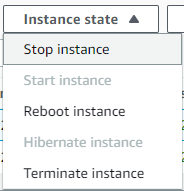
1. Now click the **Services** menu and choose **EC2**



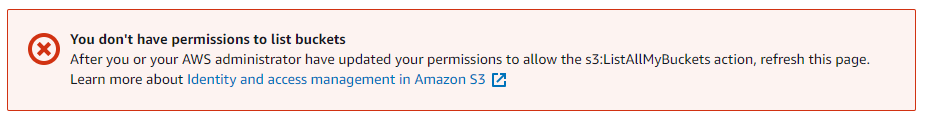
1. Now sign-out of **user-1.** At the top right click **user-1** and click sign out.



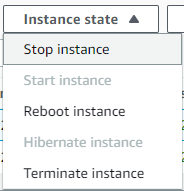
1. Paste the **IAM users sign-in** link into the address bar
2. Sign-in as **user-2** using the **IAM user name:** user-2 and the **password:** Lab-Password2
3. Click the **All Services** menu, and choose **EC2**
4. Choose **Instances.** If there are no instances, look at the top right where a region is listed, and click it and change it to the region you noted in step 3.
5. Select the **LabHost** instance
6. In the **Instance state** menu, select, **Stop instance.** You will receive an error message.



1. Now, check if user-2 can access Amazon S3
2. Click the **Services** menu at the top left and choose S3. You should receive this message since user-2 doesn’t have permission to Amazon S3



1. Now, sign-in as user-3. Follow steps 28-30, with the **IAM user name:** user-3 and **Password:** Lab-Password3
2. Click the **All Services** menu, and choose **EC2**
3. Choose **Instances.** If there are no instances, look at the top right where a region is listed, and click it and change it to the region you noted in step 3. You should have permissions to Stop the Amazon EC2 instance this time because user-3 is an EC2 Administrator
4. Select the **LabHost** instance
5. In the **Instance state** menu, select, **Stop instance.** This will stop the instance



You have finished this lab!

1. Click the **End Lab** button and select the blue **Yes** button.



**Conclusion**

In this lab you explored existing IAM users and groups, inspected IAM policies, used a real-world scenario to add users to certain groups, used the IAM sign-in URL, and experimented the effects that the policies on service access had on each user.