|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | AWS Lab 1 | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

# Lab 1: Introduction to AWS IAM

**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.

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.

**The purpose**

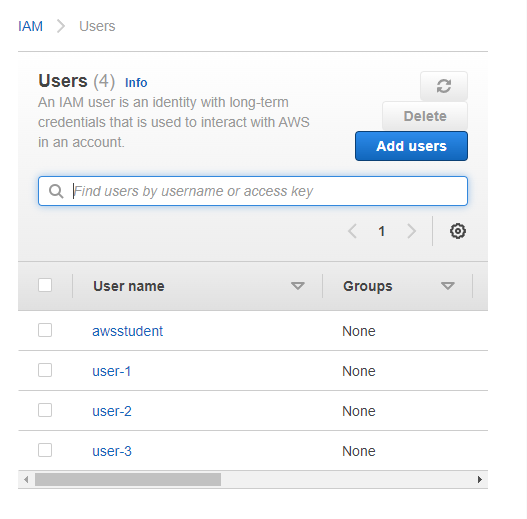
To explore pre-created **IAM Users and Groups,** inspect **IAM policies** as applied to the pre-created groups, follow a **real-world scenario**, add users to groups with specific capabilities enabled, Locate and use the **IAM sign-in URL Experimenting** with the effects of policies on service access

**Task 1: Explore the Users and Groups**

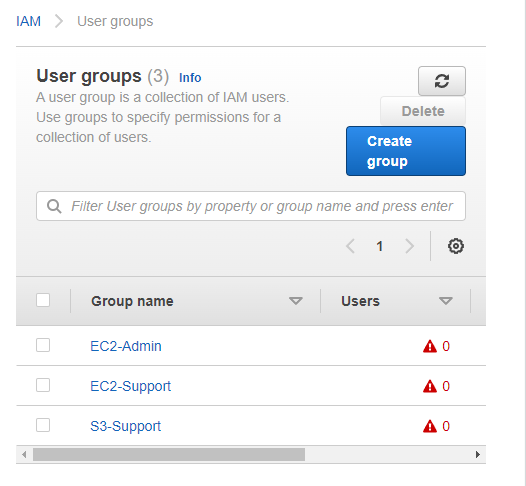
1. In the **AWS Management Console**, on the **Services** menu, click **IAM**.
2. In the navigation pane on the left, choose Instances **Users**

The following IAM Users have been created:

* User-1
* User-2
* User-3



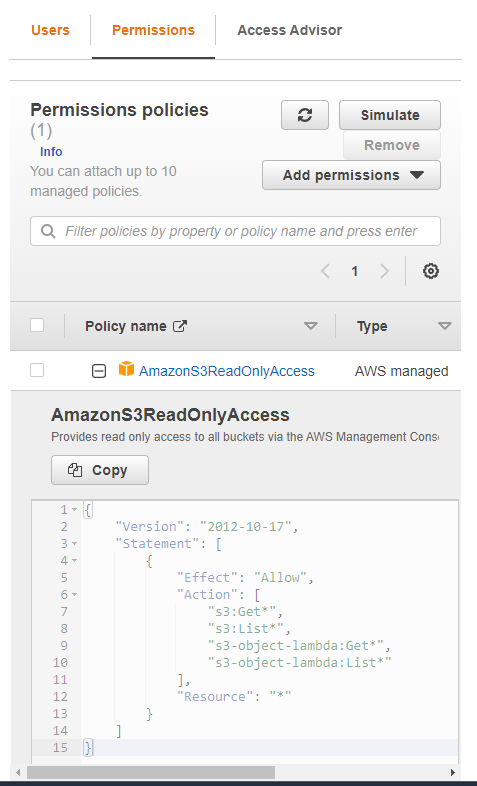
1. Choose **user-1.** User-1 does not have any permissions**.**
2. Choose **Groups** tab



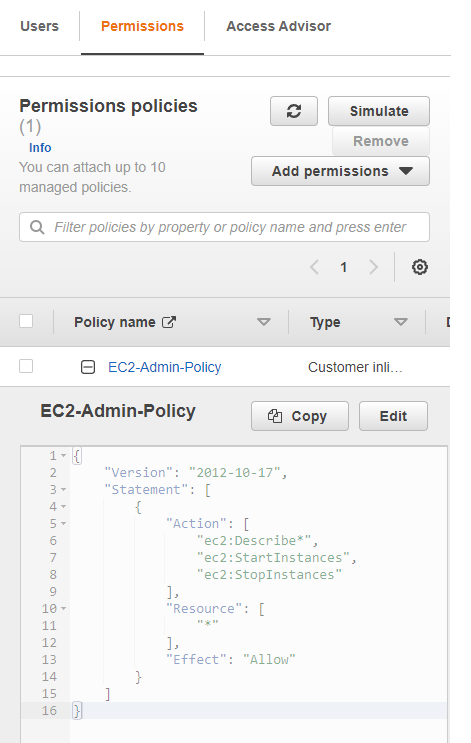
1. Choose the **Security credentials** tab.
2. In the navigation pane on the left, choose **User groups**.
3. Choose the **EC2-Support** group.
4. Choose the **Permissions** tab to view policy details



1. In the navigation pane on the left, choose **User groups**.
2. Choose the **S3-Support** group and choose the **Permissions** tab to view policy details



1. In the navigation pane on the left, choose **User groups**.
2. Choose the **EC2-Admin** and choose **Permissions** tab to view policy details

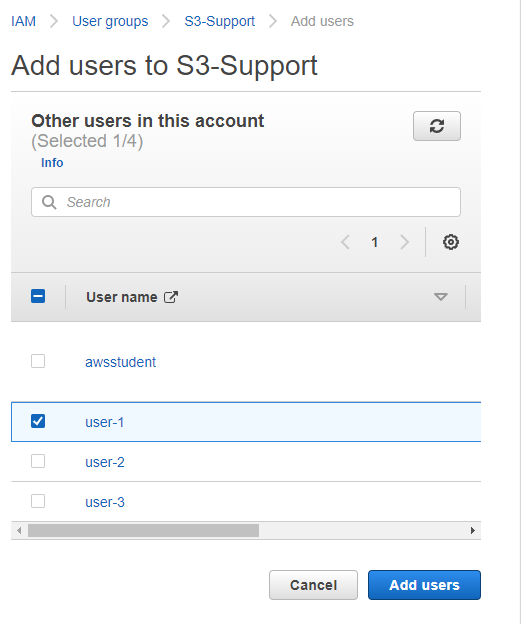


## Task 2: Add Users to Groups

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

1. In the left navigation pane, choose **User Groups**.
2. Choosethe **S3-Support** group
3. Choose the **Users** tab, choose **Add users**.
4. In the Add Users to S3-Support window, configure:

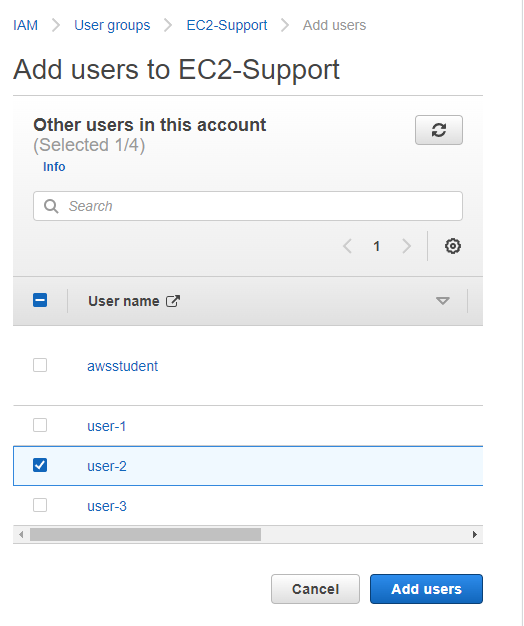
* Select **User-1**
* Choose **Add Users**



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

1. In the left navigation pane, choose **User Groups**.
2. Choosethe **EC2-support** group
3. Choose the **Users** tab, choose **Add users**.
4. In the Add Users to S3-Support window, configure:

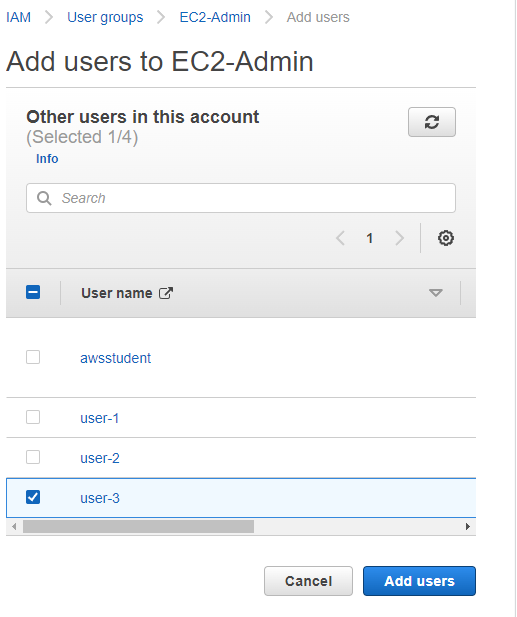
* Select **User-2**
* Choose **Add Users**



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

1. In the left navigation pane, choose **User Groups**.
2. Choosethe **EC2-Admin** group
3. Choose the **Users** tab, choose **Add users**.
4. In the Add Users to S3-Support window, configure:

* Select **User-2**
* Choose **Add Users**

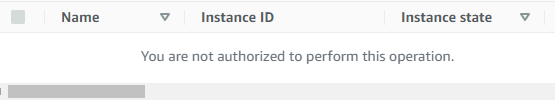


## Task 3: Sign-In and Test Users

1. In the navigation pane on the left, choose **Dashboard**.
2. Save the **Sign-in URL for IAM users in this account**
3. Open a private (Incognito) window.
4. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.
5. Sign-in with:

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

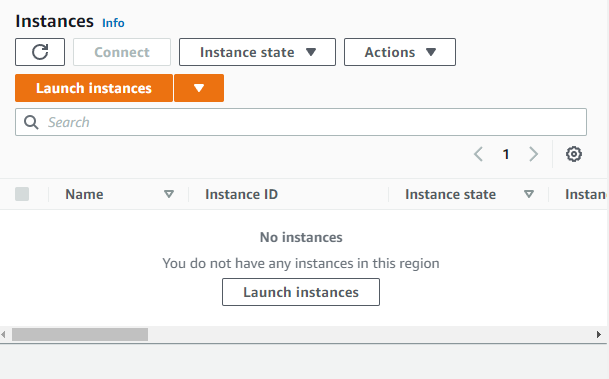
1. In the **Services** menu, choose **S3.** Choose the name of the bucket that exists in the account and browse the contents.
2. In the **Services** menu, choose **EC2**.
3. In the left navigation pane, choose **Instances**.



1. **Sign Out**
2. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.
3. Sign-in with:

* **IAM user name:** user-2
* **Password:** Lab-Password2

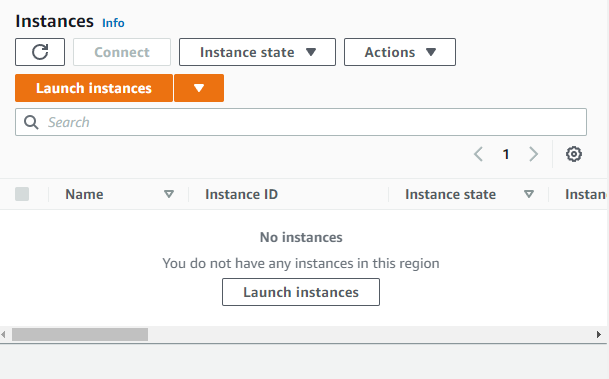
1. In the **Services** menu, choose **EC2**.
2. In the navigation pane on the left, choose **Instances**
3. In the **Instance state** menu above, select **Stop instance** and click **stop**
4. In the **Services**, choose **S3**.



1. **Sign out**
2. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.
3. Sign-in with:

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

1. In the navigation pane on the left, choose **Instance**
2. In the **Instance state** menu above, select **Stop instance** and click **stop**



1. Close Window