Introduction to AWS Identity and Access Management (IAM)

In many business environments, access involves a single login to a computer or a network of computer systems that provides the user access to all resources on the network. This access includes rights to personal and shared folders on a network server, company intranets, printers, and other network resources and devices. Unauthorized users can quickly exploit these same resources if the access control and associated authentication procedures are not set up properly.

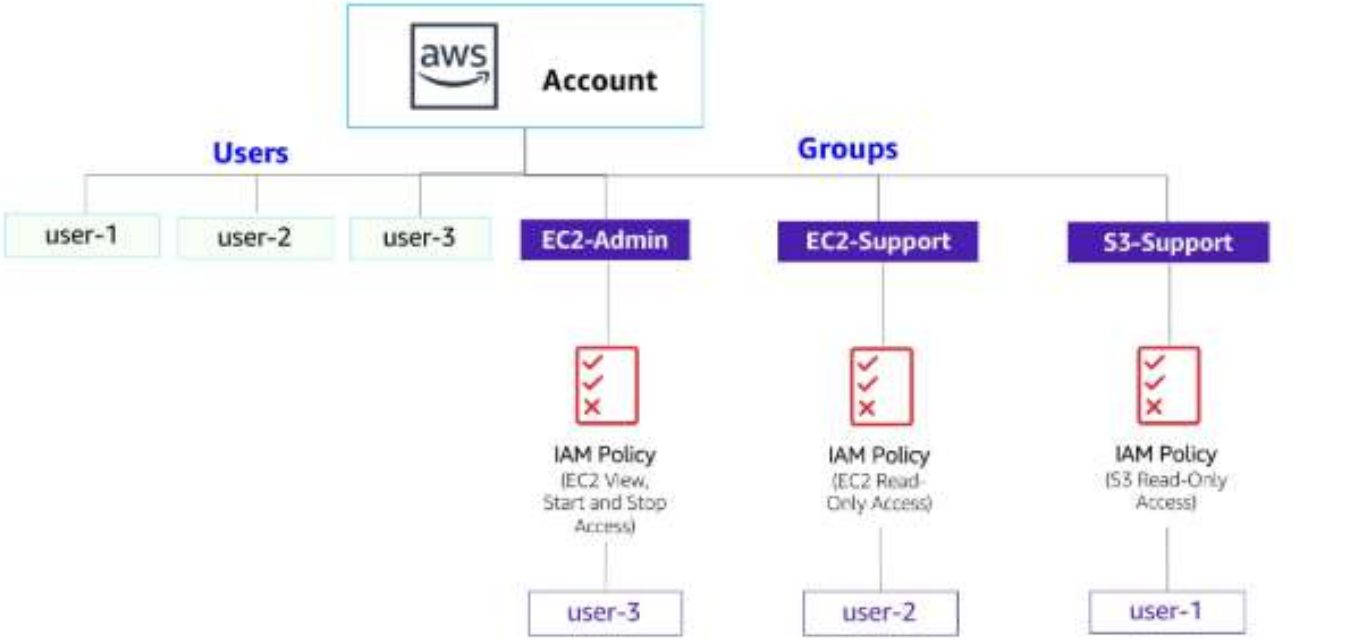
In this lab, you will explore users, user groups, and policies in the AWS Identity and Access Management (IAM) service.

Objectives

After completing this lab, you should be able to:

- Create and apply an IAM password policy
- Explore pre-created IAM users and user groups
- Inspect IAM policies as applied to the pre-created user groups
- Add users to user groups with specific capabilities active
- Locate and use the IAM sign-in URL
- Experiment with the effects of policies on service access

Here is diagram of the current environment with the listed IAM users and IAM groups.



Other AWS services

During this lab, you might receive error messages when performing actions beyond the steps in this lab. These messages will not impact your ability to complete the lab.

IAM

IAM can be used for the following:

- **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 a role is an AWS identity with permission policies that determine what the identity can and cannot do in Amazon Web Services (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 activate identity federation to allow existing users in your enterprise to access the AWS Management Console, to call AWS application programming interfaces (APIs), and to access resources without the need to create an IAM user for each identity.

Task 1: Create an account password policy

In this task, you create a custom password policy for your AWS account. This policy affects all the users associated with the account.

6. First, note the Region that you are in (for example, **Oregon**). The upper-right corner of the console page displays your Region.
7. In the AWS Management Console, in the search 🔍 box, enter `IAM` and select it.
8. In the left navigation pane, choose **Account settings**.

   Here you can see the default password policy that is currently in effect. The company that you are working for has much stricter requirements, and you need to update this policy.
9. Choose **Change password policy**.
10. Under **Select your account password policy requirements**, configure the following options:
    - For **Enforce minimum password length**, change `8` to `10` characters.
    - Select every check box except the check box for **Password expiration requires administrator reset**.
    - For **Enable password expiration**, leave the default option of **90** days.
    - For **Prevent password reuse**, leave the default option of **5** passwords.
11. Choose **Save changes**.

    These changes take affect at the AWS account level and apply to every user associated with the account.

Task 2: Explore users and user groups

In this task, you explore the users and user groups that have already been created for you in IAM.

12. In the left navigation pane, choose **Users**.

    The following IAM users have been created for you:

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

13. Choose **user-1**.

    This option bring you to a **Summary** page for **user-1**. The **Permissions** tab is displayed.

    Notice that user-1 does not have any permissions.

14. Choose the **Groups** tab.

    user-1 is also is not a member of any user groups.

    ℹ A user group consists of several users who need access to the same data. Privileges can be distributed to the entire group of users rather than to each individual. This option is much more efficient when applying permissions and provides greater overall control of access to resources than applying permissions to individuals.

15. Choose the **Security credentials** tab.

    user-1 is assigned a **Console password**.

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

    The following user groups have already been created for you:

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

17. Choose the **EC2-Support** group.

    This option brings you to the **Summary** page for the **EC2-Support** group.

18. 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 user groups. When the policy is updated, the changes to the policy are immediately applied to all users and user groups that are attached to the policy.

19. Next to the **AmazonEC2ReadOnlyAccess** policy, select the plus sign to show the policy.

    A policy defines what actions are allowed or denied for specific AWS resources. This policy grants permission to list and describe information about Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources but not modify them is ideal for assigning to a support role.

    The following is the basic structure of the statements in an IAM policy:

    - **Effect** indicates whether to **Allow** or **Deny** the permissions.
    - **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
    - **Resource** defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket, EC2 instance, or * which means *any resource*).

20. In the left navigation pane, choose **User groups**.
21. Choose the **S3-Support** group.
22. Choose the **Permissions** tab.

    The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.
23. Next to the **AmazonS3ReadOnlyAccess** policy, select the plus sign to show the policy.

    This policy has permissions to get and list resources in Amazon S3.
24. In the left navigation pane, choose **User groups**.
25. Choose the **EC2-Admin** group.
26. Choose the **Permissions** tab.

    This group is slightly different from the other two. Instead of a managed policy, it has a **Customer inline** policy, which is a policy assigned to only one user or group. Inline policies are typically used to apply permissions for one-off situations.
27. Next to the **EC2-Admin-Policy** policy, select the plus sign to show the policy.

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

Summary of task 2

In this task, you were able to view pre-created users along with the pre-created user groups. You learned about the attached polices to the user groups and what the differences between the user groups and their permissions are.

28. Under **Actions**, choose the **Show Policy** link.

    A policy defines what actions are allowed or denied for specific AWS resources. This policy grants permission to list and describe information about Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources but not modify them is ideal for assigning to a support role.

    The following is the basic structure of the statements in an IAM policy:

    - **Effect** indicates whether to **Allow** or **Deny** the permissions.
    - **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
    - **Resource** defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket, EC2 instance, or * which means *any resource*).
29. To close the **Show Policy** window, choose the **✕**
30. In the left navigation pane, choose **User groups**.
31. Choose the **S3-Support** group.

    The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.
32. From the **Actions** menu, choose the **Show Policy** link.

    This policy has permissions to get and list resources in Amazon S3.
33. To close the **Show Policy** window, choose the **✕**
34. In the left navigation pane, choose **User groups**.

35. Choose the **EC2-Admin** group.

    This group is slightly different from the other two. Instead of a managed policy, it has a **Customer inline** policy, which is a policy assigned to only one user or group. Inline policies are typically used to apply permissions for one-off situations.

36. Under **Actions**, choose **Show Policy** to view the policy.

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

37. At the bottom of the screen, choose **Cancel** to close the policy.

Summary of task 2

In this task, you were able to view pre-created users along with the pre-created user groups. You learned about the attached polices to the user groups and the differences between the user groups and their permissions.

Business scenario

For the remainder of this lab, you work with these users and user groups to activate permissions supporting the following business scenario:

Your company is growing its use of AWS and is using many EC2 instances and a great deal of Amazon S3 storage. You want to give access to new staff members depending upon their job function:

User	In Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	View, start, and stop EC2 instances

Task 3: Add users to user groups

You have recently hired **user-1** into a role where they will provide support for Amazon S3. You add them to the **S3-Support** group so that they inherit the necessary permissions via the attached **AmazonS3ReadOnlyAccess** policy.

💬 You can ignore any **not authorized** errors that appear during this task. They are caused by your lab account having limited permissions and should not impact your ability to complete the lab.

Add user-1 to the S3-Support group

38. In the left navigation pane, choose **User groups**.
39. Choose the **S3-Support** group.
40. Choose the **Users** tab.
41. In the **Users** tab, choose **Add users**.
42. In the **Add users to S3-Support** window, configure the following options:
    - Select the check box for **user-1**.
    - Choose **Add Users**.

    In the **Users** tab, you 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 provide support for Amazon EC2.

43. Using the previous steps in this task, 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 to manage your EC2 instances.

44. Using the previous steps in this task, add **user-3** to the **EC2-Admin** group.

    user-3 should now be part of the **EC2-Admin** group.

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

    Each group should have a **1** in the **Users** column for the number of users in each group.

    If there is not a **1** beside each group, revisit the previous instructions in this task to confirm that each user is assigned to a group as shown in the table at the beginning of the **Business scenario** section.

Summary of task 3

In this task, you added all the associated users to the user groups.

Task 4: Sign in and test user permissions

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

46. In the left navigation pane, choose **Dashboard**.

    The **AWS Account** section includes a **Sign-in URL for IAM users in this account**. This link should look similar to the following: **https://123456789012.signin.aws.amazon.com/console**

    You can use this link to sign in to the AWS account that you are currently using.

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

48. Open a private window using the following instructions for your web browser:

    Mozilla Firefox

    - Choose the menu bars ☰ at the upper-right of the screen.
    - Choose **New Private Window**.

    Google Chrome

    - Choose the ellipsis ⋮ at the upper-right of the screen.
    - Choose **New Incognito window**.

    Microsoft Edge

    - Choose the ellipsis ••• at the upper-right of the screen.
    - Choose **New InPrivate window**.

    Microsoft Internet Explorer

    - Choose the **Tools** menu option.
    - Choose **InPrivate Browsing**.

49. Paste the **Sign-in URL for IAM users in this account** into your private window, and press Enter.

    You now sign in as **user-1**, who has been hired as your Amazon S3 storage support staff.

50. Sign in using the following credentials:

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

51. Choose **Sign in**.

    If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.

52. From the **Services** menu, choose **S3**.

53. Choose the name of one of your buckets, and browse the contents.

    Because your user is part of the **S3-Support** group in IAM, they have permission to view a list of S3 buckets and their contents.

    Now, test whether they have access to Amazon EC2.

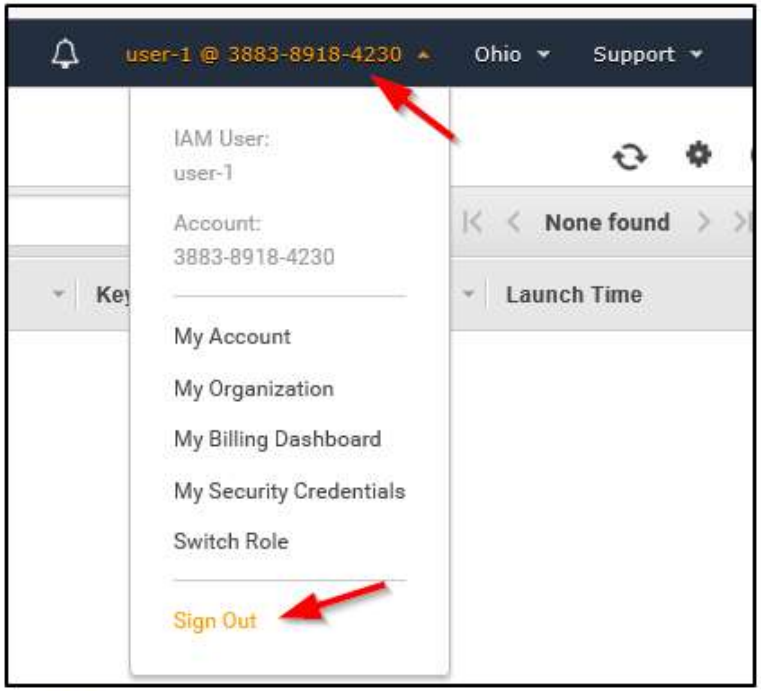
54. From the **Services** menu, choose **EC2**.

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

    You cannot see any instances. Instead, you see a message that says, **You are not authorized to perform this operation.** This message appears because your user has not been assigned any permissions to use Amazon EC2.

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

56. Sign user-1 out of the **AWS Management Console** by following these steps:
    - At the top of the screen, choose **user-1**.
    - Choose **Sign out**.



57. Paste the **Sign-in URL for IAM users in this account** into your private window, and press Enter.

    This link should be in your text editor.

58. Sign in using the following credentials:
    - **IAM user name:** Enter `user-2`
    - **Password:** Enter `Lab-Password2`

59. Choose **Sign in**.

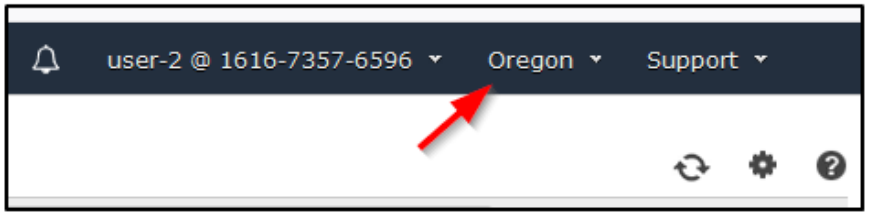
    If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.

60. From the **Services** menu, choose **EC2**.

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

    You are now able to see an EC2 instance because you have read-only permissions. However, you are not be able to make any changes to Amazon EC2 resources.

    ⚠ If you cannot see an EC2 instance, then your Region may be incorrect. In the upper-right of the screen, choose the **Region** menu, and select the Region that you noted at the start of the lab (for example, **Oregon**).



    Your EC2 instance should be selected. If it is not, choose it.

62. From the **Instance state** dropdown list, choose **Stop instance**.

63. In the **Stop instance?** window, choose **Stop**.

You receive an error that says, **Failed to stop the instance. You are not authorized to perform this operation**. This message demonstrates that the policy gives you permission to only view information and does not give you permission to make changes.

64. At the **Stop Instances** window, choose **Cancel**.

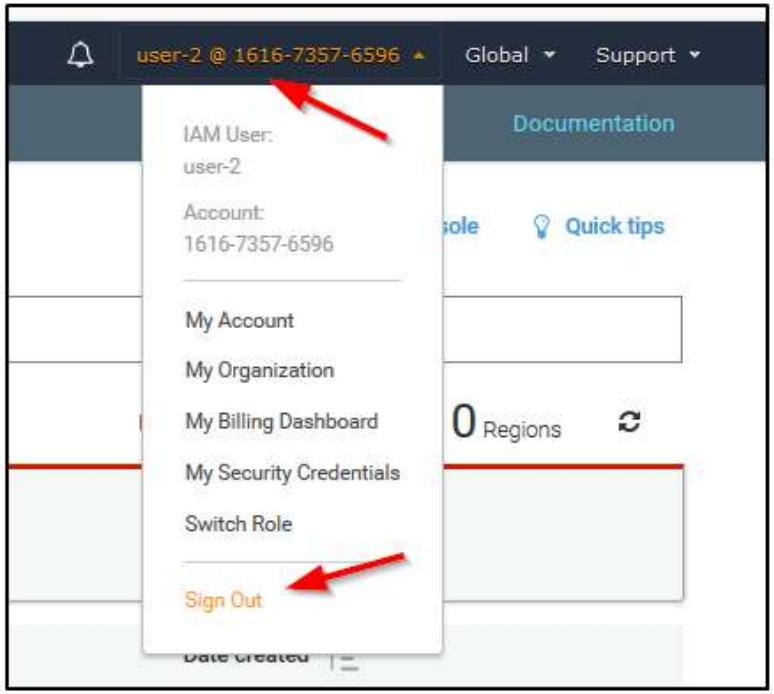
    Next, check if user-2 can access Amazon S3.

65. From the **Services** menu, choose **S3**.

    You receive an **You don't have permissions to list buckets** message because user-2 does not have permission to use Amazon S3.

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

66. Sign user-2 out of the **AWS Management Console** by following these steps:
    - At the top of the screen, choose **user-2**.
    - Choose **Sign out**.



67. Paste the **Sign-in URL for IAM users in this account** into your private window, and press Enter.

    If this link is not in your clipboard, retrieve it from the text editor where you pasted it earlier.

68. Sign in using the following credentials:
    - **IAM user name:** Enter `user-3`
    - **Password:** Enter `Lab-Password3`
69. Choose **Sign in**.

If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.

70. From the **Services** menu, choose **EC2**.
71. In the left navigation pane, choose **Instances**.

    As an EC2 administrator, you should now have permissions to stop the EC2 instance.

    Your EC2 instance should be selected. If it is not, choose it.

    ⚠ If you cannot see an EC2 instance, then your Region may be incorrect. In the upper-right of the screen, choose the **Region** menu, and select the Region that you noted at the start of the lab (for example, **Oregon**).
72. From the **Instance state** dropdown list, choose **Stop instance**.
73. In the **Stop instance?** window, choose **Stop**.

    The instance should enter the **Stopping** state and will shut down.
74. Close your private window.

Summary of task 4

In this task, you were able to sign in as all three users. You verified that user-1 was able to view S3 buckets but unable to view EC2 instances. You then signed in as user-2 and verified that they were able to view EC2 instances but unable to perform the stop instance action. user-2 was also unable to view S3 buckets. After signing in as user-3, you were able to view EC2 instances and perform the stop instance action.