Simulation: Introduction to IAM

Simulation overview

In this simulation, you use some of the Amazon Identity and Access Management (IAM) features that you just learned about.

You will get hands-on experience with creating IAM policies, groups, and users. You will experience logging in as users with different permissions. You will learn how groups can be used to manage permissions for users, based on their job role.

Objectives

After completing this simulation, you will know how to do the following:

- Create a custom managed policy.
- Create IAM user groups with permission policies.
- Create IAM users and assign users to groups.
- Use user groups to add users to a group.
- Explore policy permissions that users inherit from groups.
- Log in as users to test the user's permissions.
- Modify a user's permission to provide additional access.

Duration

This simulation requires approximately **40 minutes** to complete. You can take as long as you need.

Prerequisites

Before you begin this simulation, you should complete the Getting Started with Security course content.

AWS service restrictions

In this simulation environment, you will be guided on which actions to perform. Because this is not a live environment, you can only perform the actions you are instructed to perform. If you choose any other actions, an error message will

prompt you to the right actions. It is highly recommended that you review *How to use this simulation* in the introduction of the simulation.

Simulation scenario

For this simulation, you create users and groups to enable permissions that support the following business scenario.

Your company is growing its use of AWS services, and is using many Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon Simple Storage Service (Amazon S3) buckets. You hire three new employees and want to give access to new staff, based on their job function, as indicated in the following table.

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 Amazon EC2 instances

Task 1: Creating a custom IAM policy

In this task, you create a custom IAM policy for limited administrative Amazon EC2 access. The permissions will give any user attached to the policy access to view, start, and stop EC2 instances. You will create the policy now, so that you can use it later.

1. In the **AWS Management Console**, enter `IAM` in the search field.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
2. Then, choose **IAM** from search results.
3. In the left navigation pane, choose **Policies**.

IAM offers a wide variety of AWS managed polices. These are created and administered by AWS. However, you can create your own policies that meet your specific needs.

4. Choose **Create policy**.
5. For the **Policy editor**, choose **JSON**.

The policy editor field generates a policy template where you can start editing your code. You can also delete the existing code and paste your own code into the policy editor.

The following custom JSON policy provided for you grants the user the access to start, stop, and view nano-type and micro-type instances. If this is the only policy that is attached to the user, the user will not have access to perform any other actions.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Condition": {
"ForAllValues:StringLikeIfExists": {
"ec2:InstanceType": [
"*.nano",
"*.micro"
]
},
"StringEqualsIfExists": {
"ec2:Owner": "amazon"
}
},
"Action": [
"ec2:Describe*",
"ec2:StartInstances",
"ec2:StopInstances"
],
"Resource": [
"*"
],
"Effect": "Allow"
}
]
}
```

6. Copy and paste the preceding code into the policy editor field. **NOTE:** Keyboard shortcuts won't work for this simulation. To simulate replacing the existing code with the preceding code, follow these specific steps:
    - Open the context (right-click) menu for the policy editor field.
    - From the menu, choose **Select all**.
    - Open the context (right-click) menu for the highlighted text.

- From the menu, choose **Paste**.

7. Choose the scroll bar to scroll down, then choose **Next**.
8. In the Policy name field, enter `EC2-Admin-Policy` .
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
9. Choose the scroll bar to scroll down, then choose **Create policy**.

You have just created a custom managed policy that provides a user with the ability to start, stop, and view instances. This policy will be used for the EC2-Admin group.

Task 2: Creating user groups with permissions

In this task, you create a user group for each of the three roles and attach the appropriate permission to the group. Users will inherit the permissions of the group or groups that they are added to. You can attach permissions directly to a user. However, it is generally a best practice to manage permission by adding users to user groups, especially when there are multiple users with the same set of permissions.

Create the EC2-Admin user group

10. In the left navigation pane, choose **User groups**.
11. Choose **Create group**.
12. In the **User group name** field, enter `EC2-Admin`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
13. Choose the scroll bar to scroll down.
14. In the **Attach permissions policies** search field, enter `EC2-Admin-Policy`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.

This is the policy that you created in task 1.

15. Select the **EC2-Admin-Policy** check box.
16. Choose **Create user group**.

Create the EC2-Support group

17. Use what you learned from the previous steps to create the *EC2-Support* group. For the name of the group, use `EC2-Support`. For the policy, use `AmazonEC2ReadOnlyAccess`. If you need assistance, use the following steps:
    - Choose **Create group**.
    - In the **User group name** field, enter `EC2-Support`.
        - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
    - Choose the scroll bar to scroll down.
    - In the **Attach permissions policies** search field, enter `AmazonEC2ReadOnlyAccess`.
        - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
    - Select the **AmazonEC2ReadOnlyAccess** check box.
    - Choose **Create user group**.

Create the S3-Support group

18. Use what you learned from the previous steps to create the *S3-Support* group. For the name of the group use `S3-Support` and for the policy use `AmazonS3ReadOnlyAccess`. If you need assistance, use the following steps:
    - Choose **Create group**.
    - In the **User group name** field, enter `S3-Support`.
        - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
    - Choose the scroll bar to scroll down.
    - In the **Attach permissions policies** search field, enter `AmazonS3ReadOnlyAccess`.
        - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
    - Select the **AmazonS3ReadOnlyAccess** check box.
    - Choose **Create user group**.

Task 3: Creating users and adding them to groups

In this task, you will create three users based on the *Simulation business scenario*. As you create each user, you add the user to a group that aligns with their job role. The user will inherit the permissions that are attached to the group. If you need to re-familiarize yourself with the group that each user belongs in, review the *Business scenario*.

Create user-1 and add to the S3-Support user group

19. In the left navigation pane, choose **Users**.
20. Choose **Create user**.
21. In the **User name** field, enter `user-1`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
22. Select the **Provide user access to the AWS Management Console** check box.

It is recommended that you use AWS IAM Identity Center to provide console access to a person. IAM Identity Center is used to connect your existing workforce identity source and centrally manage access to AWS. For this simulation, there is no existing identity source. Therefore, you create IAM users. Permissions will work the same.

23. For **User type,** choose **I want to create an IAM user**.
24. Choose the scroll bar and scroll down. Then, for **Console password**, choose **Custom password**.
25. Select the **Show password** check box.
26. In the **Custom password** field, enter `Sim-Password1`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
27. Clear the **User must create a new password at next sign-in** check box.

It is a best practice to make users create a new password when the user logs in for the first time. But to avoid the steps of creating a new password when you log in as each user, this configuration will be cleared. If you were to leave the check box selected, the user would automatically be provided a policy that allows the user to create a new password.

28. Choose **Next**.
29. Keep the **Permissions options** default setting **Add user to group** selected. In the **User groups** list, select the **S3-Support** check box.
30. Choose **Next**.

Take a moment to review the user details.

31. Choose **Create User**.

Now that the user is created, you are provided with an opportunity to review the Console password and to email sign-in instructions to the user.

32. On the **Console sign-in details** panel, choose **Show** to review the **Console password**.
33. Choose **Return to users list**.

Create user-2 and add to the S3-Support user group

34. Choose **Create user**.
35. In the **User name** field, enter `user-2`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
36. Select the **Provide user access to the AWS Management Console** check box.
37. For **User type**, choose **I want to create an IAM user**.
38. Choose the scroll bar and scroll down. Then for **Console password**, choose **Custom password**.
39. Select the **Show password** check box.
40. In the **Custom password** field, enter `Sim-Password2`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
41. Clear the **User must create a new password at next sign-in** check box.
42. Choose **Next**.
43. Keep the **Permissions options** default setting **Add user to group** selected.
44. In the **User groups** list, select the **EC2-Support** check box.
45. Choose **Next**.
46. Choose **Create User**.
47. Choose **Return to users list**.

You didn't receive this warning for user-1, because you reviewed the password by choosing **Show**. But you are confident that you know the password, so you continue to the user lists.

48. On the **Continue without viewing or downloading console password** pop-up box, choose **Continue**.

Create user-3 without adding the user to a group

49. Choose **Create user**.
50. In the **User name** field, enter `user-3`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
51. Select the **Provide user access to the AWS Management Console** check box.
52. For **User type**, choose **I want to create an IAM user**.

53. Choose the scroll bar and scroll down. Then for **Console password**, choose **Custom password**.
54. Select the **Show password** check box.
55. In the **Custom password** field, enter `Sim-Password3`.
    - **Note**: To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
56. Clear the **User must create a new password at next sign-in** check box.
57. Choose **Next**.

In task 4, you will explore another way to add users to a group. Therefore, you will not select a group to add user-3 to at this point.

58. Choose **Next**.

Notice that the user has no permissions. This user will not be able to do anything in the AWS Management Console at this point.

59. Choose **Create User**.
60. Choose **Return to users list**.
61. On the **Continue without viewing or downloading console password** pop-up box, choose **Continue**.

You have created the three users that are required for the *Business scenario*. You have added user-1 and user-2 to their job-role related group. Both user-1 and user-2 have a 1 in the **Groups** column. This indicates how many groups each user is in. User-3 has a 0 in the **Groups** column, because you did not add the user to a group. You will add user-3 to a group in the next task.

Task 4: Using the user group to add users

An alternative way to add users to groups is to go into the group and add users. You will do this with our user-3 user.

62. In the left navigation pane, choose **User groups**.
63. Choose the **EC2-Admin** group name.
64. Choose **Add users**.
65. From the list of users, select the **user-3** check box.

Adding users in this way can save a lot of time because you can add many users at once, instead of going into each user one by one. From here, you can also remove multiple users from a group at once.

66. Choose **Add users**.
67. In the left navigation pane, choose **Users**.

Notice that user-3 is now showing a 1 in the **Groups** column. This confirms that the user is now in a group.

Task 5: Reviewing polices attached to a user

If you need to confirm access that any user has, you can review the policies attached to a user. Next, you will review the permission for user-2.

68. On the Users page, choose **user-2** from the **User name** column.

The **Permissions policy** pane lists all of the policies that are attached to the user in the **Policy name** section. Policies that are directly attached to a user and policies that are inherited from the user belonging to a group will appear here.

69. In the **Policy name** section, choose **AmazonEC2ReadOnlyAccess.**

A new tab opens displaying the **AmazonEC2ReadOnlyAccess** information page.

70. On the **Permissions defined in this policy** pane, choose **JSON**.
71. Choose the scroll bar to scroll down.

From here, you can review the permission that this AWS managed policy grants to the user.

72. Close the **AmazonEC2ReadOnlyAccess** browser tab.
73. In the navigation pane on the left, choose **Users**.

Task 6: Testing the access of user-1

In this task, you will log in to the AWS Management Console as user-1 and test the permissions. User-1 is in the S3-Support group.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached to it. Therefore, user-1 should be able to go to the S3 console page and view buckets and content in the buckets. However, the user should not be able to upload or delete objects.

Get the console sign-in URL

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

Notice the **Sign-in URL for IAM users in this account** section at the top right of the page. The sign-in URL looks similar to the following:
https://123456789012.signin.aws.amazon.com/console

This link can be used to sign in to the AWS account that you are currently using. (The account number is blurred out for security reasons).

75. On the **AWS Account** pane, choose the copy icon for **Sign-in URL for IAM users in this account** to copy the link.

Open an incognito window

76. Open a private or incognito window in your browser. To do this, follow these specific instructions:
    - In the top right corner of your browser, choose the vertical ellipsis.
    - Choose **New Incognito window**.
77. Simulate pasting the sign in browser URL in the incognito window's search bar. To do this, follow these specific instructions:
    - Choose the browser's URL search bar.
    - Press **Ctrl** + **v** on your keyboard.
        - **Note**: Mac users should also press **Ctrl** + **v** on their keyboard. This is not the pasting command for Mac keyboards, but this simulation requires you to use your keyboard as a Windows keyboard.
    - Choose the highlighted URL to load the page.

Next, you will duplicate the **Sign in as IAM user** page so that you have three duplicate tabs open. You will use the tabs to sign in as each of your three users.

78. Open the context (right-click) menu for your browser tab.
79. Choose **Duplicate**.
80. Open the context (right-click) menu for your second browser tab.
81. Choose **Duplicate**.

You now have three duplicate tabs open. You will now sign in as *user-1*, who has been hired as your Amazon S3 storage support staff.

Test user-1 permissions

82. Sign in with the following credentials:
    - **IAM user name:** user-1
    - **Password:** Sim-Password1

Note: To record each entry, press **Enter** on your keyboard or choose any place outside of the entry field.

    -
83. In the **Recently visited** section, choose **S3**.
84. Choose the **sim-website** bucket.

Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of the Amazon S3 buckets and their contents. However, the user cannot create buckets. The user is also restricted from deleting or uploading files. Next, you test the restrictions by trying to upload a file.

85. Choose **Upload**.
86. Choose **Add files**.
87. Select the **Index.html** file.
88. Choose **Open**.
89. Choose the scroll bar to scroll down. Then, choose **Upload**.

The failed upload message confirms that the user's permissions are working as expected.

90. Close the browser tab.

Task 7: Testing the access of user-2

In this task, you will log into the AWS Management Console as user-2 and test the permissions. User-2 has been hired as an Amazon EC2 support person and is therefore in the EC2-Support group.

The EC2-Support group has the **AmazonEC2ReadOnlyAccess** policy attached to it. Therefore, user-2 should be able to go to the EC2 dashboard and view instances. However, the user should not be able to stop and start the instance.

91. Sign in with the following credentials:
    - **IAM user name:** user-2
    - **Password:** Sim-Password2

Note: To record each entry, press **Enter** on your keyboard or choose any place outside of the entry field.

92. In the **Recently visited** section, choose **EC2**.
93. In the left navigation pane, choose **Instances**.

You can see two EC2 instances. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions.

94. Select the **Application server** instance check box.
95. Choose the **Instance state** menu. Then, choose **Stop instance**.
96. To confirm you want to stop the instance, choose **Stop**.

An error message appears that says, *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information without making changes.

97. Close the **Instances** browser tab.

Task 8: Testing the access of user-3

In this task, you will log into the AWS Management Console as user-3 and test the permissions. User-3 has been hired as an Amazon EC2 admin person and is therefore in the EC2-Admin group.

The EC2-Admin group has the **EC2-Admin-Policy** policy attached to it. This is the custom policy that you created in task 1. Therefore, user-3 should be able to go to the EC2 dashboard and view instances. However, unlike user-2, user-3 should be able to stop and start instance.

98. Sign in with the following credentials:
    - **IAM user name:** user-3
    - **Password:** Sim-Password3

Note: To record each entry, press **Enter** on your keyboard or choose any place outside of the entry field.

99. In the **Recently visited** section, choose **EC2**.
100. In the **Resources** pane, choose **Instances (running)**.

EC2 instances are listed. As an Amazon EC2 Administrator, this user should have permissions to *Stop* the EC2 instance.

101. Select the **Application server** instance check box.
102. Choose the **Instance state** menu. Then choose **Stop instance**.
103. To confirm that you want to stop the instance, choose **Stop**.

This time, the action is successful because *user-3* has permissions to stop EC2 instances. The **Instance state** changes to *Stopping* and begins to shut down.

Modifying access to grant user-3 read only access to Amazon S3

Next, you will test whether the **EC2-Admin-Policy** that user-3 inherits from the **EC2-Admin** group provides any access to view buckets in Amazon S3.

104. To return to the **AWS Management Console Home** page, choose the **AWS** icon in the top left corner. In the **Recently visited** section, choose **S3**.
105. In the left navigation pane, choose **Buckets**.

An error message appears that says, *You don't have permissions to list buckets*. This demonstrates that the policy does not grant any access for S3.

If you wanted to give your EC2 administrator access to view buckets and bucket objects, you could add the user to the S3-Support group. Next, you will update the user-3 permissions so that the user can view buckets, in addition to having administrative access to EC2.

106. Return to your normal browser window, where you are logged into the IAM console. To do this, do the following:
    - Hover near the bottom of the browser to bring up the task bar, then choose the **Google Chrome** icon.
107. Choose **User groups**.
108. In the list of user groups, choose **S3-Support**.

The group provides a list of users that are in the group already.

109. Choose **Add users**.

Notice that user-1 is not among the list of users on the **Add users to S3-Support** page. That is because this page does not show users that are already in the group.

110. On the **Other users in this account** pane, select the **user-3** check box.
111. Choose **Add users**.
112. Return to the incognito window, by closing the current window.
113. On the top left of your browser, choose **Refresh**.

The new access is available immediately. There is no requirement for the user to log out and log back in for the changes to take effect. User-3 now has the same access to S3 that user-1 has. However, user-1 cannot access EC2.

Conclude the simulation by logging out.

114. Choose the user-3 account dropdown list.

Note: The account number **0000-0000-0000-0000** is a fictitious account number that is used for security purposes. Only share your account number with trusted sources.

115. Choose **Sign out**.

Wrap up

In this simulation, you created a custom managed IAM policy. You created user groups that had permission policies based on job roles. You created users and assigned them to the appropriate group. You learned how to review the policies that a user inherits from a group or policies that are directly attached to the user. You discovered how to add many users to a group to save time. You also logged in as each user and tested the permission. Excellent work!

Simulation complete

Congratulations! You have completed the simulation.

For more information about AWS Training and Certification, see AWS Training and Certification.

Your feedback is welcome and appreciated.

If you would like to share any suggestions or corrections, please provide the details in our AWS Training and Certification Contact Form at https://support.aws.amazon.com/#/contacts/aws-training.