Introduction to IAM

Lab overview

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

Duration

This lab requires approximately 40 minutes to complete.

Access the AWS Management Console

- 1. To start the lab session, choose Start Lab in the upper-right corner of the page.
 - The lab session starts.
 - A timer displays in the upper-right corner of the page and shows the time remaining in the session.
 Tip: To refresh the session length at any time, choose Start Lab again before the timer

Tip: To refresh the session length at any time, choose Start Lab again before the timer reaches 0:00.

- 2. Before continuing, wait until the lab environment is ready. The environment is ready when the lab details appear on the right side of the page and the circle icon next to the AWS link in the upper-left corner turns green.
- 3. To return to these instructions, choose the Readme link in the upper-right corner.
- 4. To connect to the AWS Management Console, choose the AWS link in the upper-left corner, above the terminal window.

A new browser tab opens and connects you to the AWS Management Console. Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose Allow pop-ups.

Note: You are using the console through the lab environment, so you are not incurring any actual costs. However, in the real world, when using a personal or business account to access the console, users incur charges for use of specific AWS services.

Task 1. Explore the users and groups

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

- First, note the Region that you are in; for example, N. Virginia. The Region is displayed in the upper-right corner of the console page.
 You might need this information later in the lab.
- 5. Choose the Services menu, locate the Security, Identity, & Compliance services, and choose IAM.

- 6. In the navigation pane on the left, choose Users. The following IAM users have been created for you:
 - user-1
 - user-2
 - user-3
- 7. Choose the name of user-1.
 - This brings you to a summary page for user-1. The Permissions tab will be displayed.
 - Notice that user-1 does not have any permissions.
- Choose the Groups tab. Notice that user-1 also is not a member of any groups.
- Choose the Security credentials tab. Notice that user-1 is assigned a Console password. This allows the user to access the AWS Management Console.
- 10. In the navigation pane on the left, choose User groups. The following groups have already been created for you:
 - EC2-Admin
 - EC2-Support
 - S3-Support
- 11. Choose the name of the EC2-Support group.

This brings you to the summary page for the EC2-Support group.

12. Choose the Permissions tab.

This group has a managed policy called AmazonEC2ReadOnlyAccess associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the policy are immediately applied against all users and groups that are attached to the policy.

- 13. Under Policy Name, choose the link for the AmazonEC2ReadOnlyAccess policy.
- 14. Choose the {} JSON tab.
 - A policy defines what actions are allowed or denied for specific AWS resources. This
 policy is granting permission to List and Describe (view) information about Amazon
 Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and
 Amazon EC2 Auto Scaling. This ability to view resources, but not modify them, is ideal for
 assigning to a support role.
 - Statements in an IAM policy have the following basic structure:
 - Effect says 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 or Amazon EC2 instance; an asterisk [*] means any resource).
- 15. In the navigation pane on the left, choose User groups.
- 16. Choose the name of the S3-Support group.
- 17. Choose the Permissions tab. The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.
- 18. Under Policy Name, choose the link for the AmazonS3ReadOnlyAccess policy.
- Choose the {} JSON tab.
 This policy has permissions to Get and List for all resources in Amazon S3.
- 20. In the navigation pane on the left, choose User groups.
- 21. Choose the name of the EC2-Admin group.
- 22. Choose the Permissions tab.

This group is different from the other two. Instead of a managed policy, the group has an inline policy, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.

- 23. Under Policy Name, choose the name of the EC2-Admin-Policy policy.
- 24. Choose the JSON tab.

This policy grants permission to Describe information about Amazon EC2 instances, and also the ability to Start and Stop instances.

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

Business scenario

For the remainder of this lab, you will work with these 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 EC2 instances and Amazon S3 buckets. You want to give access to new staff depending upon 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-Suppor t	Read-only access to Amazon EC2
user-3	EC2-Admin	View, Start, and Stop Amazon EC2 instances

Task 2. Add users to groups

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

Ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

Add user-1 to the S3-Support group

- 26. In the left navigation pane, choose User groups.
- 27. Choose the name of the S3-Support group.
- 28. On the Users tab, choose Add users.
- 29. Select user-1, and choose Add users.On the Users tab, notice 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 will provide support for Amazon EC2. You will add them to the EC2-Support group so that they inherit the necessary permissions via the attached AmazonEC2ReadOnlyAccess policy.

30. Use what you learned from the previous steps to 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. You will add them to the EC2-Admin group so that they inherit the necessary permissions via the attached EC2-Admin-Policy.

- 31. Use what you learned from the previous steps to add user-3 to the EC2-Admin group. user-3 should now be part of the EC2-Admin group.
- In the navigation pane on the left, choose User groups.
 Each group should have a 1 in the Users column. This indicates the number of users in each group.

If you do not have a 1 for the Users column for a group, revisit the previous steps to ensure that each user is assigned to a group, as shown in the table in the Business scenario section.

Task 3. Sign in and test users

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

Get the console sign-in URL

33. In the navigation pane on the left, choose Dashboard.

Notice the Sign-in URL for IAM users in this account section at the top 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.

34. Copy the sign-in link to a text editor.

Test user-1 permissions

- 35. Open a private or incognito window in your browser.
- 36. Paste the sign-in link into the private browser, and press ENTER. You will now sign-in as user-1, who has been hired as your Amazon S3 storage support staff.
- 37. Sign in with the following credentials:
 - IAM user name: user-1
 - Password: Lab-Password1
- 38. Choose the Services menu, and choose S3.
- 39. Choose the name of one of your buckets, and browse the contents. Because this user is part of the S3-Support group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents. Now, test whether the user has access to Amazon EC2.
- 40. Choose the Services menu, and choose EC2.
- 41. In the left navigation pane, choose Instances. You cannot see any instances. Instead, an error message says you are not authorized to perform this operation. This user has not been assigned any permissions to use Amazon EC2. You will now sign in as user-2, who has been hired as your Amazon EC2 support person.
- 42. First, sign out user-1 from the console:
 - In the upper-right corner of the page, choose user-1.
 - Choose Sign Out.

Test user-2 permissions

- 43. Paste the sign-in link into the private browser again, and press ENTER.
- 44. Sign in with the following credentials:
 - IAM user name: user-2
 - Password: Lab-Password2
- 45. Choose the Services menu, and choose EC2.
- 46. In the navigation pane on the left, choose Instances.
 - You are now able to see an EC2 instance. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions.
 - If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, N. Virginia).
- 47. Select the EC2 instance.
- 48. Choose the Instance state menu, and then choose Stop instance.
- 49. To confirm that you want to stop the instance, choose Stop. An error message appears and says that You are not authorized to perform this operation. This

demonstrates that the policy only allows you to view information without making changes. Next, check if user-2 can access Amazon S3.

- 50. Choose the Services menu, and choose S3. An error message says You don't have permissions to list buckets because user-2 does not have permissions to use Amazon S3. You will now sign-in as user-3, who has been hired as your Amazon EC2 administrator.
- 51. First, sign out user-2 from the console:
 - In the upper-right corner of the page, choose user-2.
 - Choose Sign Out.

Test user-3 permissions

- 52. Paste the sign-in link into the private browser again, and press ENTER.
- 53. Sign in with the following credentials:
 - IAM user name: user-3
 - Password: Lab-Password3
- 54. Choose the Services menu, and choose EC2.
- 55. In the navigation pane on the left, choose Instances.
 - An EC2 instance is listed. As an Amazon EC2 Administrator, this user should have permissions to Stop the EC2 instance.
 - If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, N. Virginia).
- 56. Select the EC2 instance.
- 57. Choose the Instance state menu, and then choose Stop instance.
- 58. 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 starts to shut down.
- 59. Close your private browser window.

Lab complete

Congratulations! You have completed the lab.

- 60. Log out of the AWS Management Console.
 - In the upper-right corner of the page, choose your user name. Your user name begins with voclabs/user.
 - Choose Sign Out.
- 61. Choose End Lab at the top of this page, and then select Yes to confirm that you want to end the lab.