

Experiment – 3

Aim: Create an AWS account, configure IAM users, create and manage S3 buckets.

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	Read-only access to Amazon EC2 instances

Task 1: Creating a custom IAM policy



Learn cloud skills at no cost with AWS Educate

-  Register with just an email address, no credit card required
-  Content and resources designed for beginners like you
-  Explore, search for, and apply for jobs through the [AWS Educate Job Board](#)
-  Gain access to the [AWS Emerging Talent Community](#) when you earn digital badges

English

Create your account

Already have a learner account? [Sign in](#)
Looking to hire cloud talent? [Register as a recruiter](#)

First name

Middle name - optional

Last name

Country

State or province

City

Birth month

FAQ Contact us Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Site terms

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 policies. 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Condition": {
        "ForAllValues":
        StringLikeIfExists": {
          "ec2:InstanceType": [
            "*.nano",
            "*.micro"
          ]
        },
        "StringEqualsIfExists": {
          "ec2:Owner":
          "amazon"
        }
      }
    }
  ]
}
```

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.

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**.

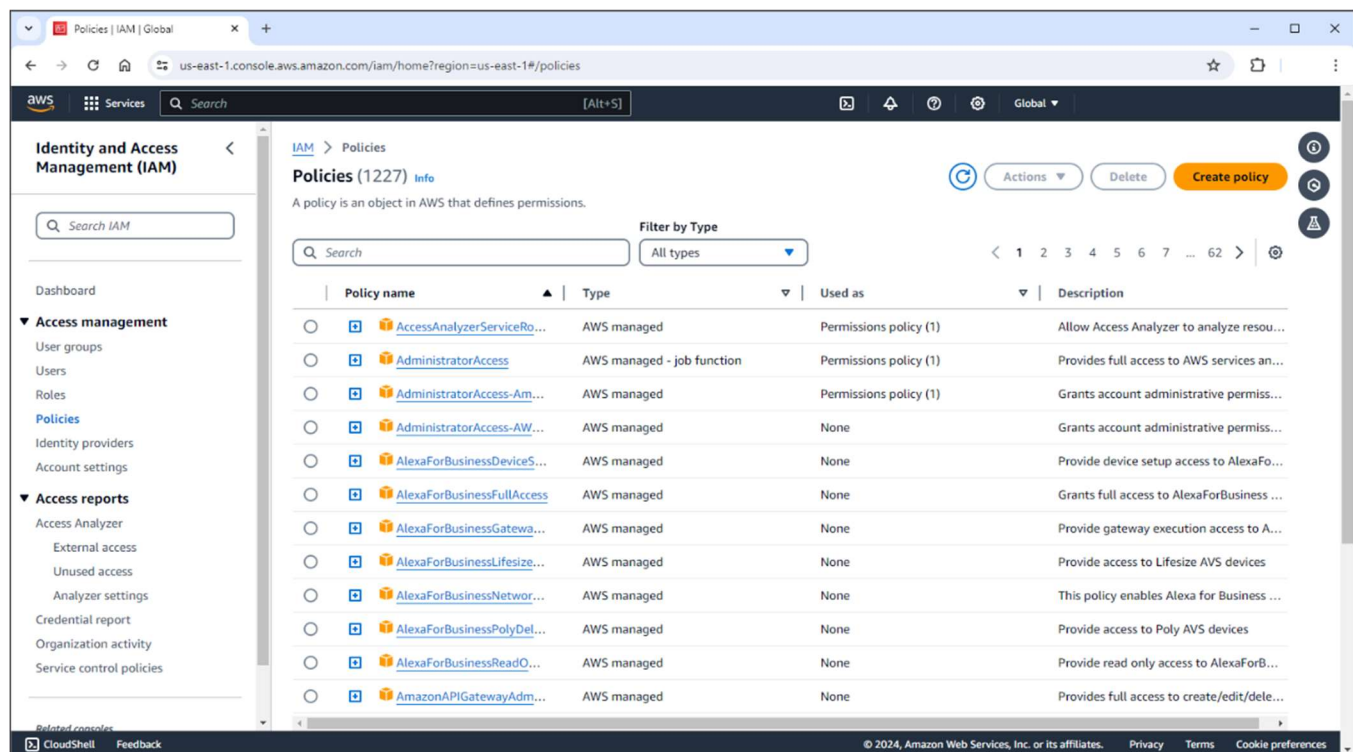
7. Choose the scroll bar to scroll down, then choose **Next**.

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.

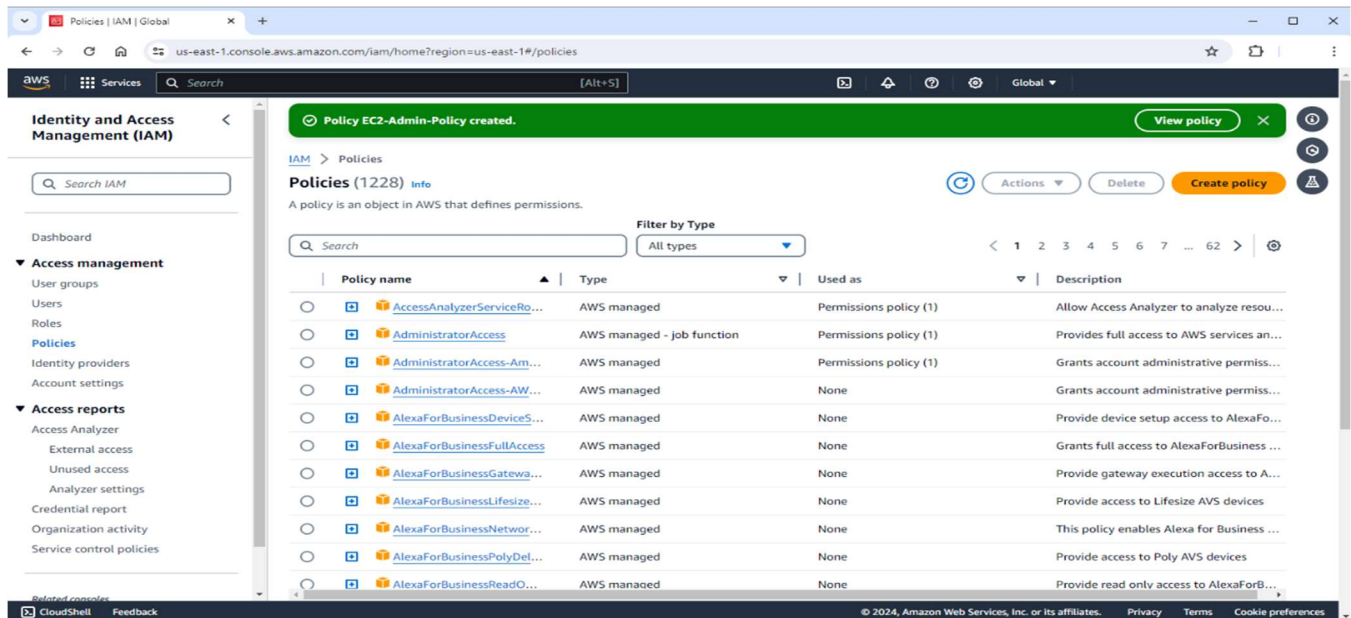


Task 2: Creating user groups with permissions

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



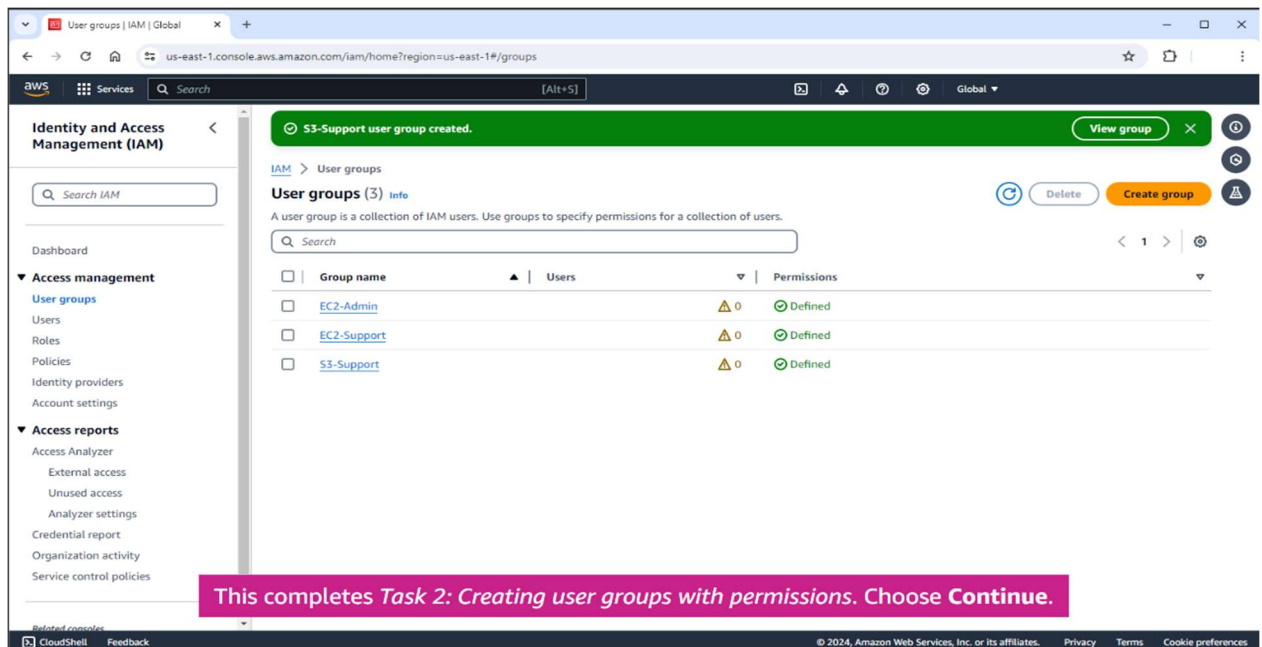
10. In the left navigation pane, choose **User groups**.
11. Choose **Create group**.
12. In the **User group name** field, enter EC2-Admin.
 - **Note:** To record your entry, press **Enter** on your keyboard or choose any place outside of the entry field.
13. Choose the scroll bar to scroll down.
14.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

The screenshot shows the AWS IAM console 'Create user' page, specifically the 'Review and create' step. The left navigation pane shows the progress: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this, there are three sections: 'User details', 'Permissions summary', and 'Tags - optional'. The 'User details' section shows 'User name' as 'user-1', 'Console password type' as 'Custom password', and 'Require password reset' as 'No'. The 'Permissions summary' section shows a table with one entry: 'S3-Support' (Name), 'Group' (Type), and 'Permissions group' (Used as). The 'Tags - optional' section states 'No tags associated with the resource.' and provides an 'Add new tag' button. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'.

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.

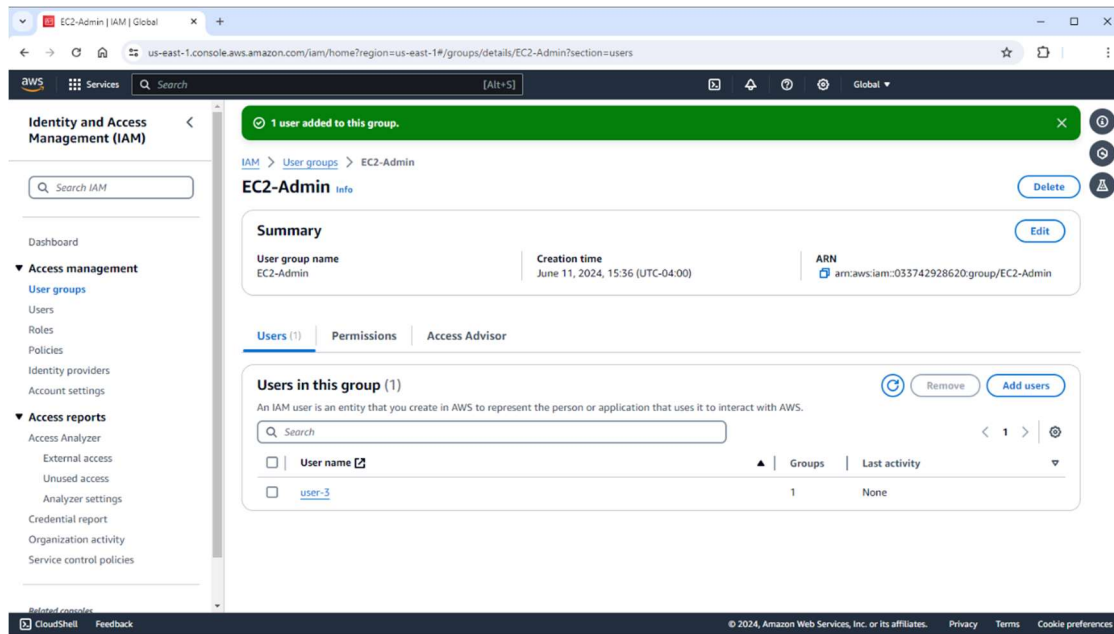
The screenshot shows the AWS IAM console interface. At the top, a green banner indicates 'User created successfully'. Below this, the 'Users' page is displayed, showing a table of three users: user-1, user-2, and user-3. The table has columns for 'User name', 'Groups', and 'Console access'. user-1 and user-2 are associated with 1 group each, while user-3 is associated with 0 groups. All three users have 'Enabled' console access. A pink banner at the bottom of the console area states: 'This completes Task 3: Creating users and adding them to user groups. Choose Continue.'

<input type="checkbox"/>	User name	Groups	Console access
<input type="checkbox"/>	user-1	1	Enabled
<input type="checkbox"/>	user-2	1	Enabled
<input type="checkbox"/>	user-3	0	Enabled

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 policies 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.

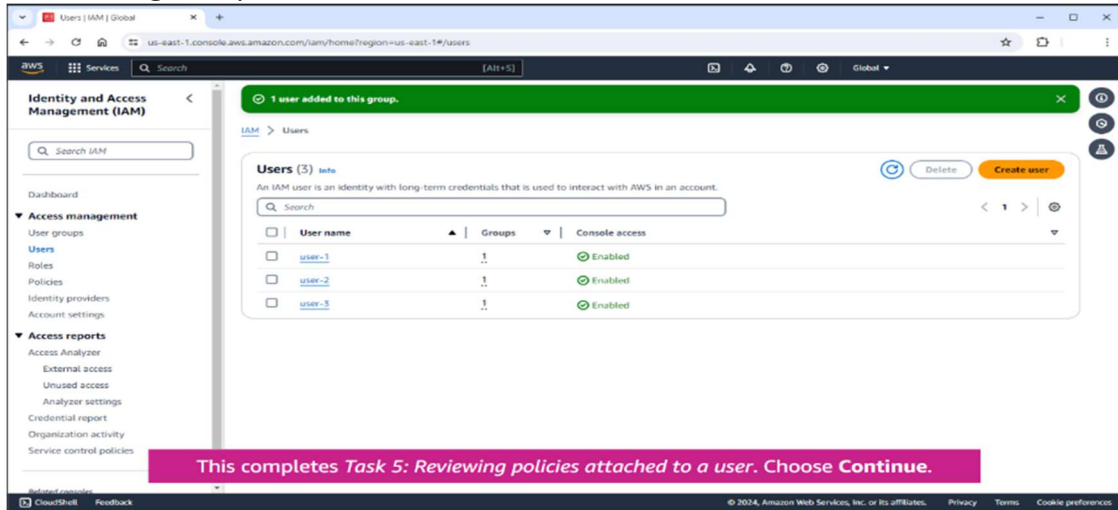
70. On the **Permissions defined in this policy** pane, choose **JSON**.

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.

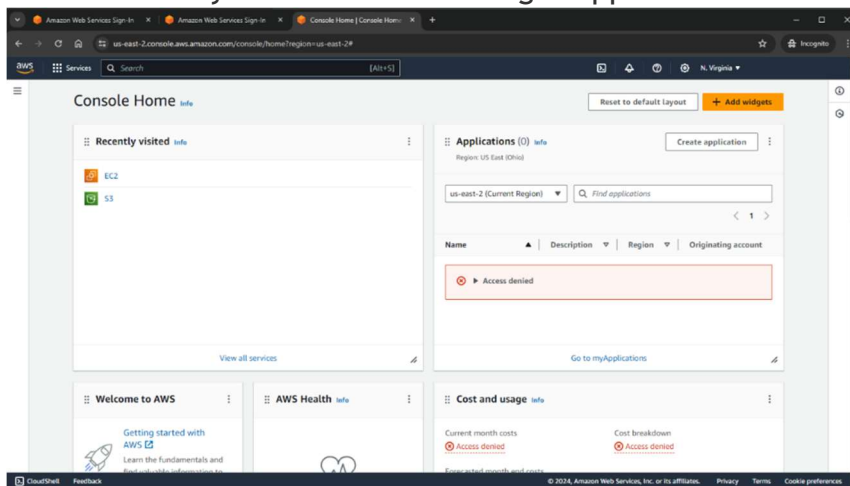
78. Open the context (right-click) menu for your browser tab.

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**.

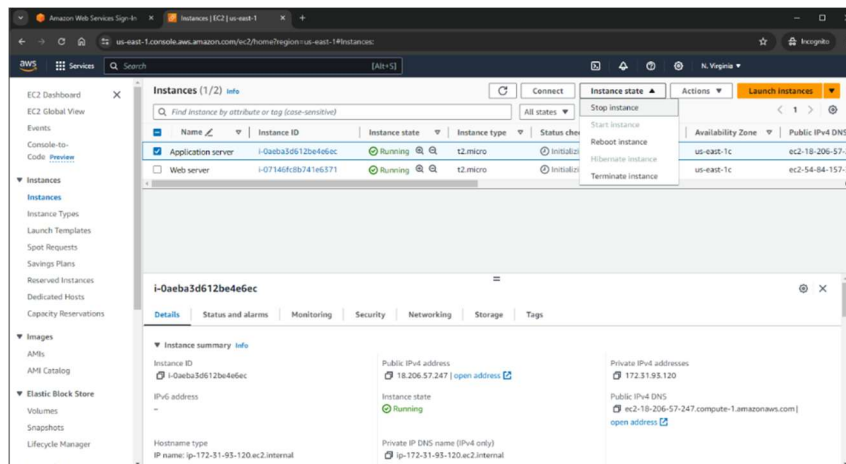
You can see two EC2 instances. However, you cannot make any changes to

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.

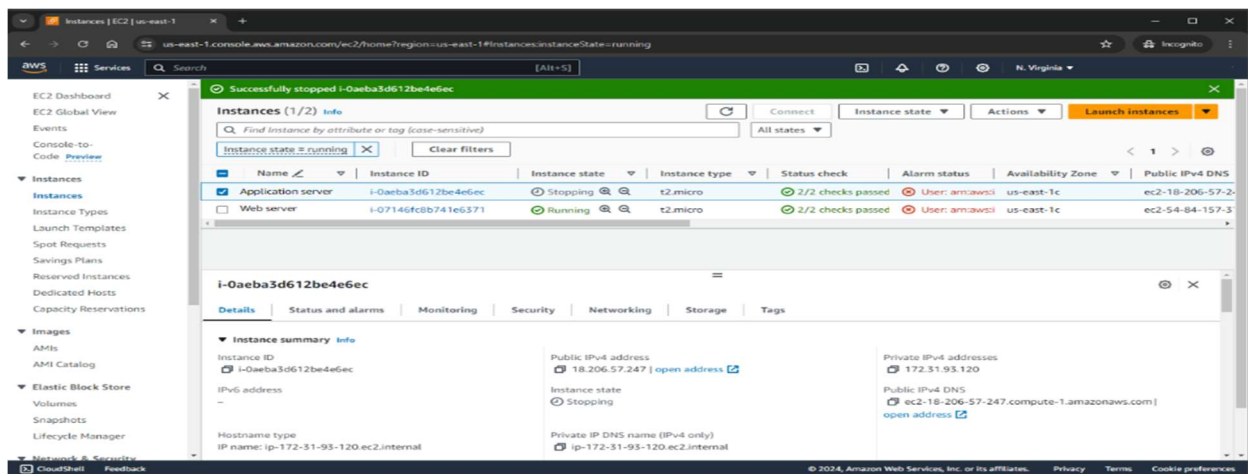
99. In the **Recently visited** section, choose **EC2**.
100. In the **Resources** pane, choose **Instances (running)**.

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**.

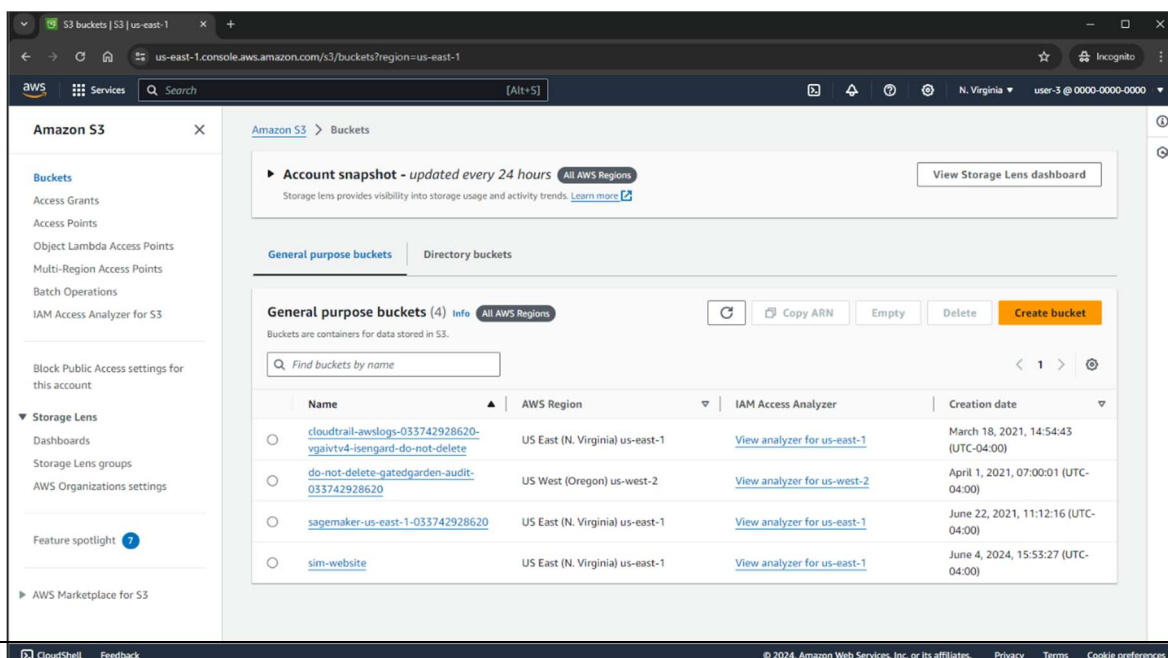
The new access is available immediately. There is no requirement for the user to log out and log back in for the changes to take effect. User-3 now has the same access to S3 that user-1 has. However, user-1 cannot access EC2.

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**.



The screenshot shows the Amazon S3 console interface. The left sidebar contains navigation links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area displays the 'Buckets' page with an 'Account snapshot' section and a 'General purpose buckets' table. The table lists four buckets with their names, AWS Regions, IAM Access Analyzer links, and creation dates.

Name	AWS Region	IAM Access Analyzer	Creation date
cloudtrail-awslogs-033742928620-vgaivtv4-isengard-do-not-delete	US East (N. Virginia) us-east-1	View analyzer for us-east-1	March 18, 2021, 14:54:43 (UTC-04:00)
do-not-delete-gatedgarden-audit-033742928620	US West (Oregon) us-west-2	View analyzer for us-west-2	April 1, 2021, 07:00:01 (UTC-04:00)
sagemaker-us-east-1-033742928620	US East (N. Virginia) us-east-1	View analyzer for us-east-1	June 22, 2021, 11:12:16 (UTC-04:00)
sim-website	US East (N. Virginia) us-east-1	View analyzer for us-east-1	June 4, 2024, 15:53:27 (UTC-04:00)

Simulation: Getting Started with Amazon S3

Simulation overview and objectives

In this simulation, you use some of the Amazon Simple Storage Service (Amazon S3) features that you just learned about to create a static website.

Static websites can contain HTML pages, images, style sheets, and all files that are needed to render a website. Static websites do not use server-side scripting or a database. However, they might contain client-side scripts that run in a user's web browser.

You can host a static website on Amazon S3 by uploading the content and making it readable by users. No servers are needed, and you can use Amazon S3 to store and retrieve any amount of data anytime from anywhere on the web.

Objectives

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

- Create a bucket in Amazon S3.
- Configure a bucket to host a static website.
- Upload content to a bucket.
- Turn on public access to bucket objects.
- Securely share a bucket object by using a presigned URL.
- Secure a bucket by using a bucket policy.
- Update the website.
- View object versions in the Amazon S3 console.

Duration

This simulation requires approximately **30 minutes** to complete. You can take as long as you need.

Prerequisites

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

Amazon Web Services (AWS) service restrictions

In this simulation environment, you will be guided on which actions to perform. Because this environment is not live, you can only perform the actions that 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.

Task 1: Creating a bucket in Amazon S3

In this task, you create an S3 bucket that you will use for static website hosting.

1. In the **AWS Management Console**, choose the search bar and enter **S3**.

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

2. Then choose **S3** from the search results.
3. Choose **Create bucket**.

An S3 bucket name is globally unique, and all AWS accounts share the namespace. After you create a bucket, no other AWS accounts in any AWS Regions can use the name of that bucket unless you delete the bucket.

4. For **Bucket name**, enter **sim-website**.

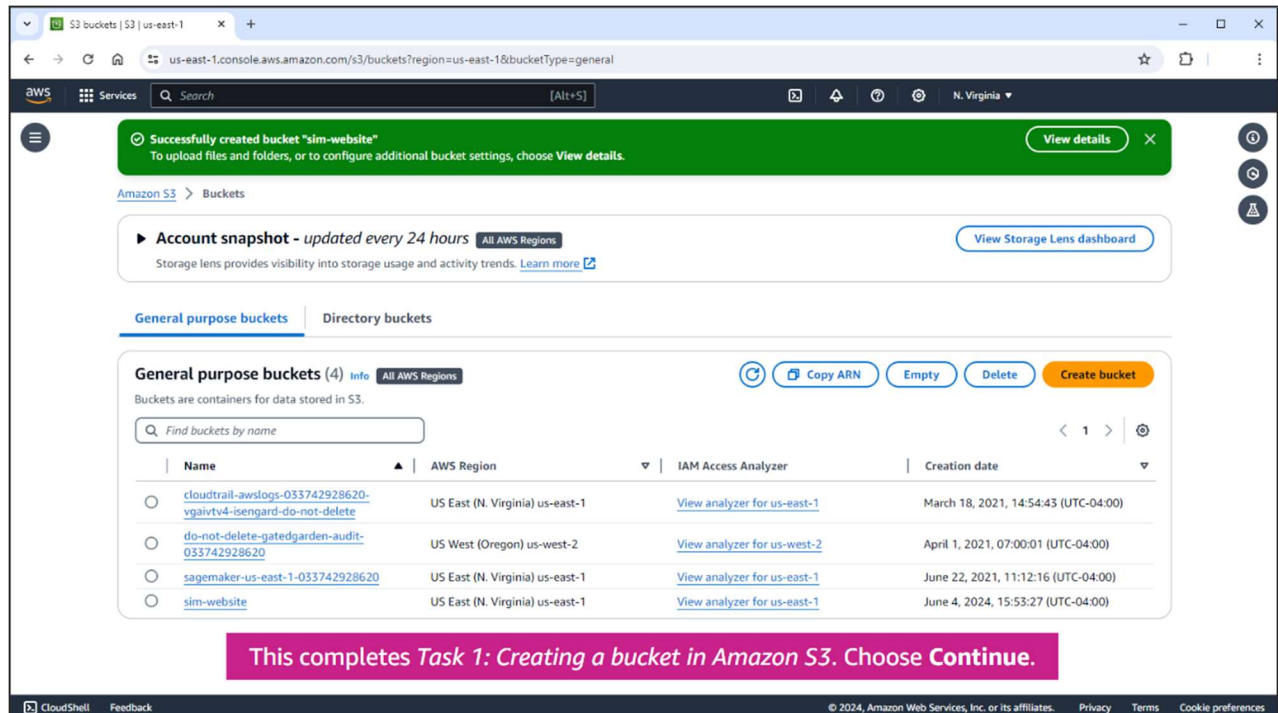
Note: To record your entry, press **Enter** on your keyboard or choose any place outside the entry field.

5. Choose the scroll bar to scroll down to **Object Ownership**.
6. For **Object Ownership**, choose **ACLs enabled**. Keep the default **Bucket owner preferred** selected.
7. Choose the scroll bar to scroll down to **Block Public Access settings for this bucket**.

Public access to buckets is blocked by default. Because the files in your static website must be accessible through the internet, you must permit public access.

8. For **Block Public Access settings for this bucket**, clear the checkbox for **Block all public access**. Then, select the box that states **I acknowledge that the current settings might result in this bucket and the objects within becoming public**.
9. Choose the scroll bar to scroll down to **Bucket Versioning**.
10. For **Bucket Versioning**, choose **Enable**.

Note: As soon as you turn on (enable) bucket versioning, you can't turn it off.



11. For **Tags**, choose **Add tag**, and enter the following:

- **Key:** Department
- **Value:** Marketing

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

You can use tags to add additional information to a bucket, such as a project code, cost center, or owner.

12. Choose the scroll bar to scroll down.

13. Choose **Create bucket**.

Your bucket appears in the list of buckets for your AWS account.

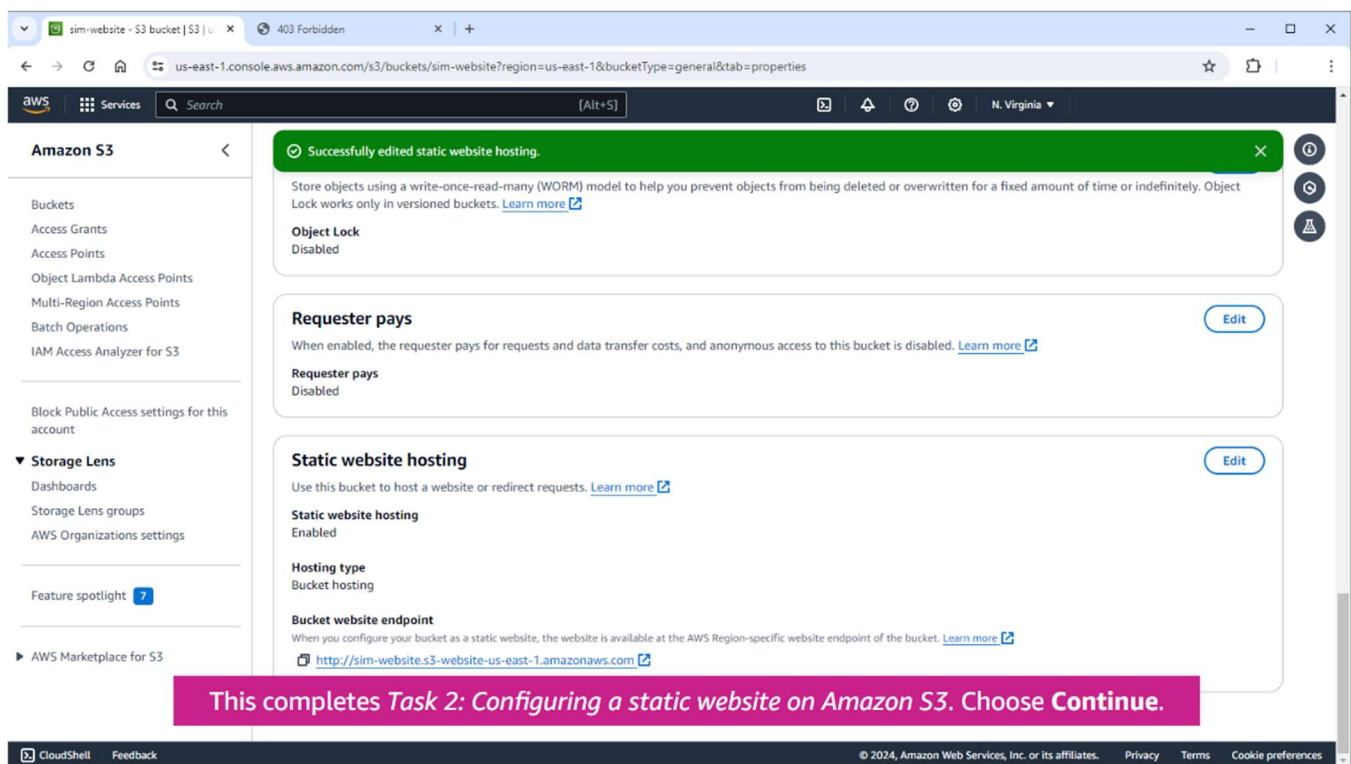
Task 2: Configuring a static website on Amazon S3

You will now configure the bucket for static website hosting.

17. In the list of your buckets, choose the name of the bucket that you just created, **sim- website**.

18. Choose the **Properties** tab.
19. Choose the scroll bar to scroll to the **Static website hosting** panel.
20. Choose **Edit** to the **Static website hosting** panel.
21. Choose **Enable**.
22. For **Hosting type**, keep the default setting **Host a static website**.
23. Configure the following settings:
 - **Index document:** Enter Index.html
 - **Error document:** Enter error.html

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



24. Choose the scroll bar to scroll down.
25. Choose **Save changes**.
26. Choose the scroll bar to scroll to the **Static website hosting** panel.
27. In the **Static website hosting** panel under **Bucket website endpoint**, choose the link.

A new tab opens where you receive a **403 Forbidden** message because you have not yet configured the bucket permissions. You can return to it later.

28. Choose the **AWS Management Console** tab on your browser.

You have configured your bucket to host a static website.

Task 3: Uploading content to your bucket

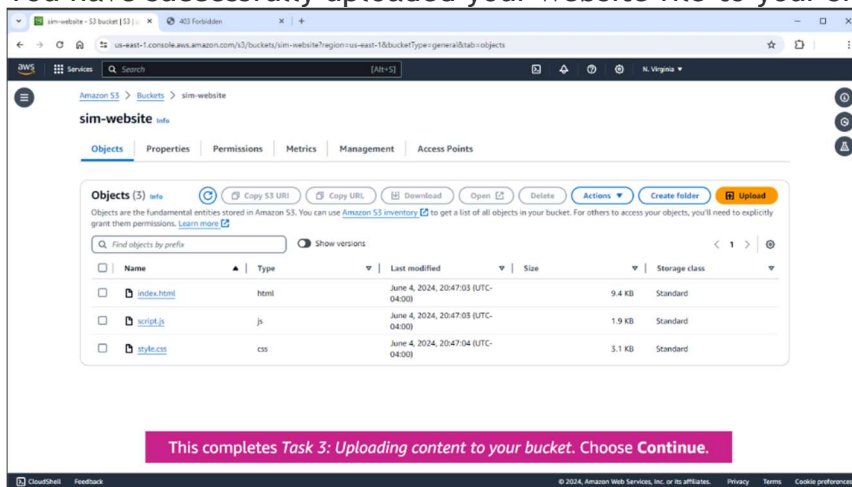
In this task, you upload the static files to your bucket.

22. Choose the scroll bar to scroll to the top of the page, and choose the **Objects** tab.
23. Choose **Upload**.
24. Choose **Add files**.
25. Choose the **Website files** folder, and choose **Open** to open the folder.
26. Use your mouse to choose each of the following files: **index.html**, **script.js**, and **style.css** (order does not matter). Then choose **Open**.
27. Choose the scroll bar to scroll down.
28. Choose **Upload**.

Your files are uploaded to the bucket.

27. Choose **Close**.

You have successfully uploaded your website file to your sim-website bucket.



Task 4: Turning on public access to the objects

Objects that are stored in Amazon S3 are private by default. This setting helps keep your organization's data secure.

In this task, you make the uploaded objects publicly accessible so users can view your website.

First, confirm that the objects are currently private.

28. Return to the browser tab that showed the *403 Forbidden* message.
29. Choose the **Refresh** button for the webpage.

You should still see a *403 Forbidden* message. This response is expected. This

message indicates that your static website is being hosted by Amazon S3 but that the content is private.

You can make Amazon S3 objects public in two different ways:

- To make either a whole bucket public or a specific directory in a bucket public, use a bucket policy.
- To make individual objects in a bucket public, use an access control list (ACL).

It is normally safer to make individual objects public because doing so avoids accidentally making other objects public. However, if you know that the entire bucket contains no sensitive information, you can use a bucket policy.

You now configure the individual objects to be publicly accessible.

30. Keep the website tab open, and return to the web browser tab with the **Amazon S3 console**.

31. Choose the **Name** checkbox to select all three objects.

32. In the **Actions** menu, choose **Make public using ACL**. A list

of the three objects is displayed.

33. Choose **Make public**.

Your static website is now publicly accessible.

34. Choose **Close**.

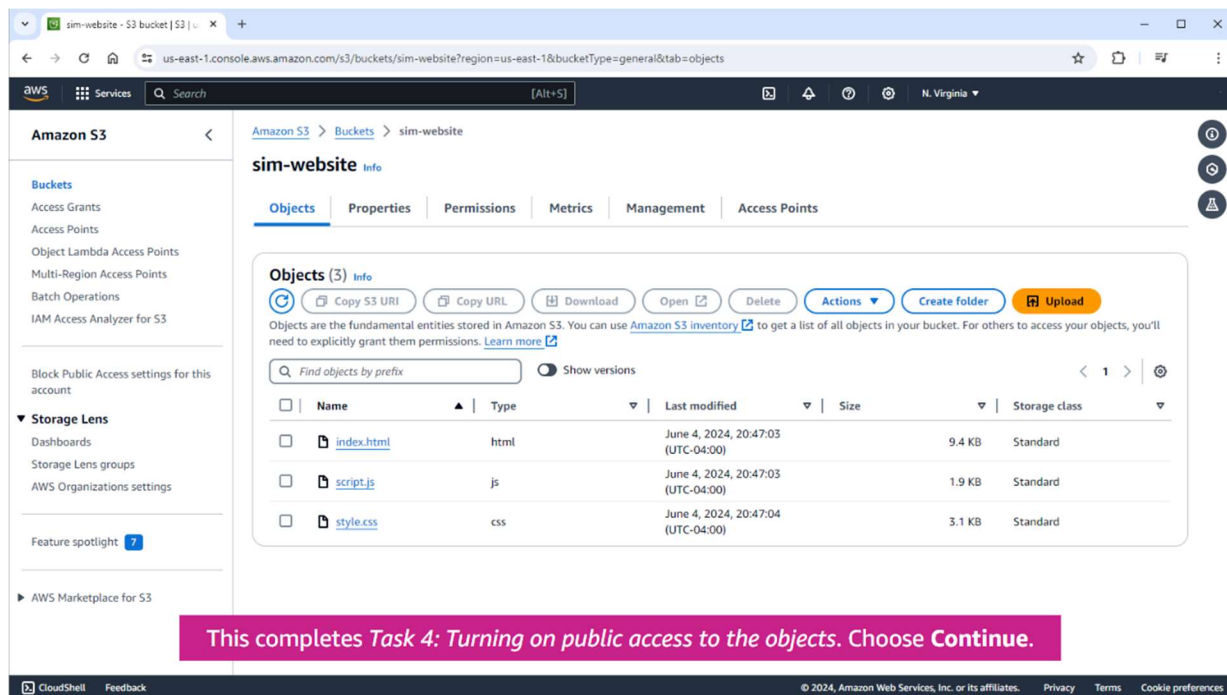
35. Return to the web browser tab that has the *403 Forbidden* message.

36. Refresh the webpage.

You should now see the static website that Amazon S3 is hosting.

37. On your browser, choose the **x** on the **My Static Website** tab.

Now you know how to share objects with everyone by making them public. However, at times, you might need to share an individual object for a limited amount of time. In the next task, you learn how to temporarily share an object.



Task 5: Securely sharing an object by using a presigned URL

When you must temporarily and securely share an object with a person or group of people, you can create a presigned URL. When you create the URL, you must configure how long the URL will be valid. Then, you can share this URL with the users who should have access to the object.

If the presigned URL is valid, anyone who has it can get to the object. Avoid keeping the URL active longer than necessary, and only share the URL with people you trust.

38. Choose **Upload**.
39. Choose **Add files**.
40. Choose the file **new-report** file and choose **Open**.
41. Choose the scroll bar to scroll down.
42. Choose **Upload**.

You have uploaded your file to the bucket.

43. Choose **Close**.

Like when you first uploaded the website files, the **new-report.png** file is private by default. This time, instead of making the object public, you create a presigned URL to access the file.

44. In the **Objects** tab, choose **new-report.png**.
45. From the **Actions** menu, select **Share with a presigned URL**.

46. In the pop-up window, keep the default **Minutes** selected for the **Time interval until the presigned URL expires**.

47. For **Number of minutes**, enter 2.

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

48. Choose **Create presigned URL**.

49. From the banner at the top of the page, choose **Copy presigned URL**.

50. Open a new browser tab.

51. Paste the URL that you copied into the address bar. Use these specific steps to paste and launch the URL:

- Choose the browser URL search bar.
- Press **Ctrl + v** on your keyboard.
 - **Note:** Mac users should also press **Ctrl + v** on their keyboard. This command is not the pasting command for Mac keyboards, but this simulation requires you to use your keyboard as a Windows keyboard.
- Press **Enter** to load the page.

A report is displayed in the web browser.

If you wait 2 minutes and use the link again, you will find that the URL has expired and no longer works. Note: for the sake of the simulation, you do not need to wait 2 minutes.

52. Choose the Refresh icon on the browser.

Now that the presigned URL is expired, you get an Access denied page.

53. Choose **x** to close the Access denied tab.

The screenshot displays the AWS IAM console interface. On the left, the 'Upload' section shows a successful upload of 'new-report.png' (84.0 KB) to the 's3://my-website' bucket. The 'Files and folders' tab is active, showing a list of files and folders. The 'Access Logs' tab is also visible, showing a list of log entries for the 'my-website' bucket.

File	Folder	Type	Size	Status	Error
new-report.png	-	Image/png	84.0 KB	Successful	-

Task 6: Using a bucket policy to secure your bucket

You want to protect your website files and make sure that no one can delete them. To do so, you apply a bucket policy that denies delete privileges on your website files.

50. Choose the **Permissions** tab.

51. Choose the scroll bar to scroll down to the **Bucket policy** panel.

52. In the **Bucket policy** panel, choose **Edit**.

53. Copy the following policy text and paste it in the **Policy** text editor field. To do so, follow these specific steps:

- Open the context (right-click) menu for the Policy text editor field.
- Choose **Paste**.

```
{
  "Version": "2012-10-17",
  "Id": "MyBucketPolicy", "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:DeleteObject",
      "Resource": [
        "arn:aws:s3:::sim-website/index.html",
        "arn:aws:s3:::sim-website/script.js",
        "arn:aws:s3:::sim-website/style.css"
      ]
    }
  ]
}
```

This policy prevents everyone from deleting the three files that make your website work.

Note: If you use this code in your own AWS account, you must use the name of your bucket in place of this simulation's **sim-website** bucket.

53. Choose the scroll bar to scroll down.

54. Choose **Save changes**.

55. Return to the **Objects** tab.

56. Select **index.html**.

57. Choose **Delete**.

58. In the **Delete objects** panel, enter delete to confirm that you want to remove this file.

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

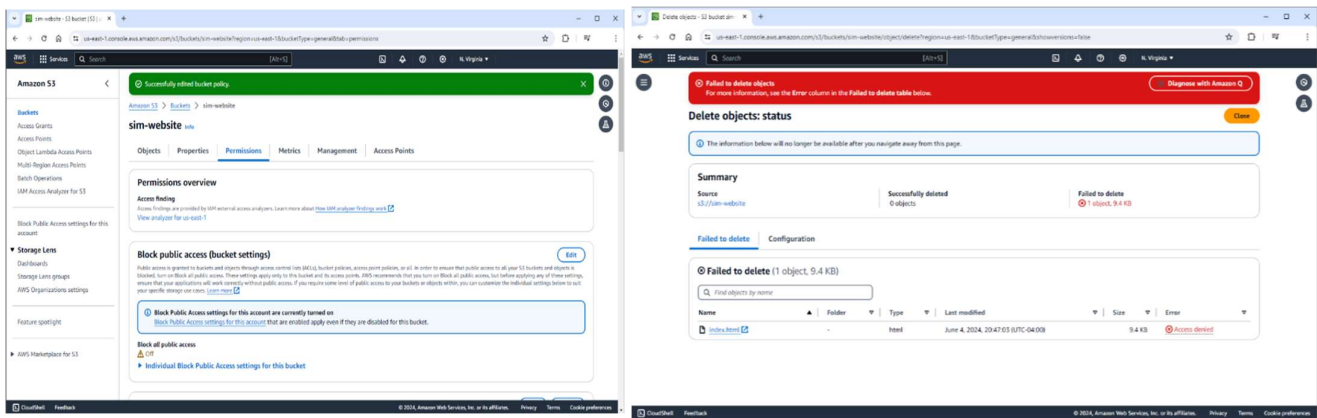
59. Choose **Delete objects**.

60. Notice that the **index.html** file is listed in the **Failed to delete** pane.

This entry confirms that your policy is working and preventing the website's files from being deleted.

61. Choose **Close** to return to the **Objects** tab.

Your bucket policy is now protecting your website files from being deleted.



Task 7: Updating the website

Although you have configured a policy to prevent deletion of website files, you can still update the website. You can do so by editing the HTML file and uploading it to the S3 bucket again.

Amazon S3 is an object storage service, so you must upload the whole file. This action replaces the existing object in your bucket. You cannot edit the contents of an object; instead, you must replace the whole object.

Next you edit the existing **index.html** file.

62. On your computer, load the **index.html** file into a text editor (in this simulation, you use Notepad). Follow these specific steps:

1. Open the context (right-click) menu for the **index.html** file.
2. Choose **Open with**.
3. Choose **Notepad**.

63. Find the text **Served from Amazon S3**, and replace it with Created by Jane. Follow these specific steps:

1. Choose the text **Served from Amazon S3**.
2. Enter Created by Jane.

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

entry field.

64. Save the file. Follow these specific steps:

1. Choose **File** from the Notepad menu.
2. Choose **Save**.

65. Return to the **Amazon S3 console** by selecting the **Amazon S3 console** window in the background.

Now you review the current website version.

66. Choose the **index.html** file name (choose the link, not the checkbox).

67. Choose the **Object URL** link.

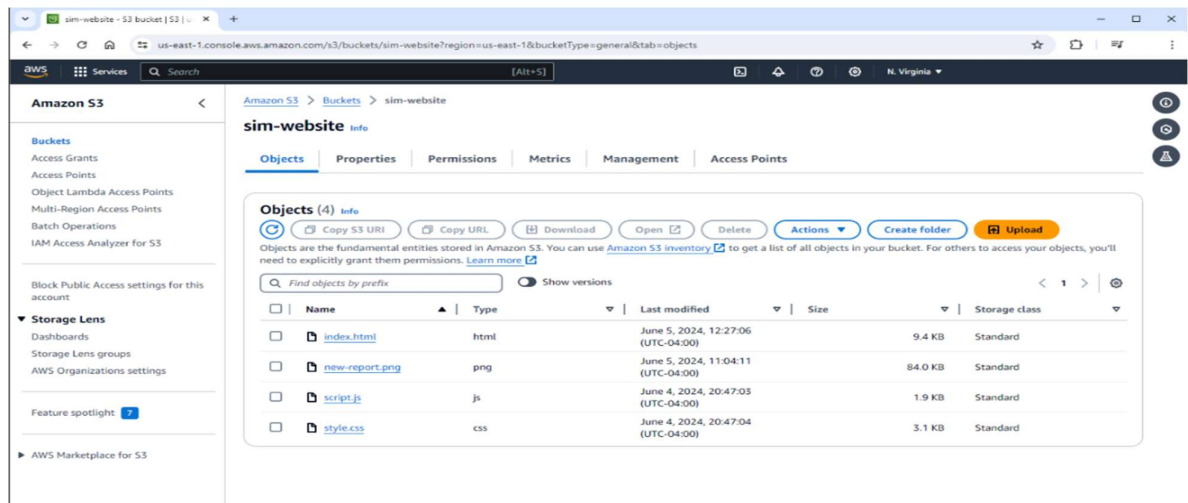
Served from Amazon S3 should still be visible on your website page because you have not yet uploaded the new version and made it public. Next, you will upload the index.html file that you edited and make it public.

68. Choose the **Back** arrow on your browser to return to the **Amazon S3 console**.

69. Choose the **sim-website** link from the navigation at the top of the page.

70. Upload the **index.html** file that you just edited. Follow these specific steps:

1. Choose **Upload**.
2. Choose **Add files**.
3. Choose the **Website files** folder, and choose **Open**.
4. Choose the **index** file and choose **Open**.
5. Choose the scroll bar to scroll down.
6. Choose **Upload**.
7. Choose **Close**.



71. Select the **index.html** checkbox, and in the **Actions** menu, choose the **Make public using ACL** option again.

72. Choose **Make public**, and choose **Close**.

Now you verify that your website is updated with your edits.

73. Choose the **index.html** file name (choose the link, not the checkbox).

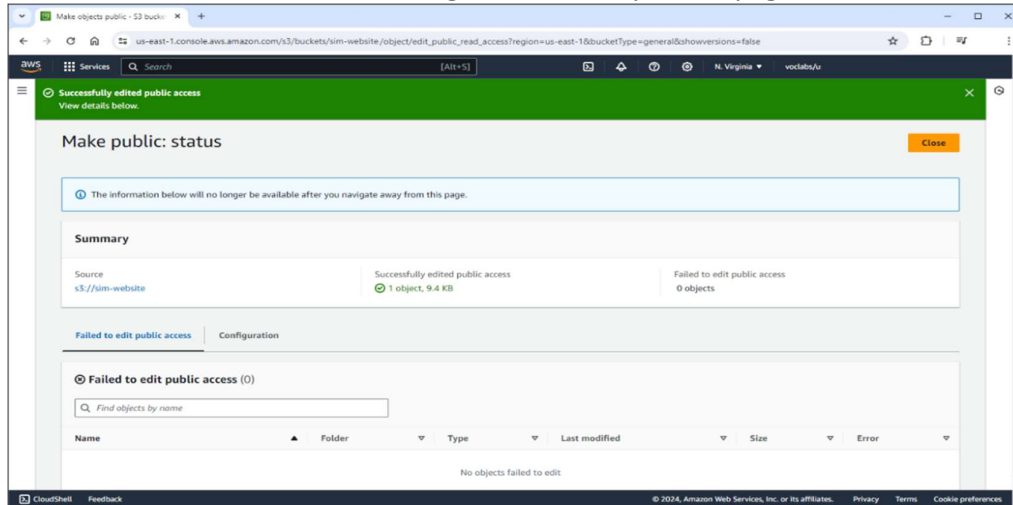
74. Choose the **Object URL** link.

Created by Jane should now be on the page in place of *Served from Amazon S3*.

Your static website is now accessible on the internet. Because it is hosted on Amazon S3, the website has high availability and can serve high volumes of traffic without using any servers.

75. Choose the Back arrow on your browser to return to the Amazon S3 console.

76. Choose the **sim-website** link from the navigation at the top of the page.



Task 8: Exploring file versions

Bucket versioning is turned off by default. When versioning is turned off, changes to objects can't be undone. For example, if you upload a new version of a file, the old file is replaced with the new one. The original file is lost. If you delete a file, it is permanently deleted, and you can't get it back.

However, when versioning is turned on, changed and deleted versions of files are saved. Previous versions of objects are not presented by default, but you can access them by using the console or programmatically. Because you are keeping earlier versions of objects, you can recover them if you need to.

It is important to remember that as soon as you turn on versioning, you cannot turn it off. However, you can suspend versioning. For more information about bucket versioning, see "Using versioning in S3 buckets" in the *Amazon Simple Storage Service Users Guide* at <https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>.

Recall that when you created your bucket, you turned on versioning. In this task, you view the object versions available in your bucket.

77. Choose **Show versions** to see which files have multiple versions.

78. Choose the scroll bar to scroll down.

79. Review the list of objects in the bucket.

sim-website - S3 bucket | S3 | X +

us-east-1.console.aws.amazon.com/s3/buckets/sim-website?region=us-east-1&bucketType=general&tab=objects

Services Search [Alt+S] N. Virginia

Amazon S3 > Buckets > sim-website

sim-website Info

Objects Properties Permissions Metrics Management Access Points

Objects (4) Info Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix Show versions < 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	index.html	html	June 5, 2024, 12:27:06 (UTC-04:00)	9.4 KB	Standard
<input type="checkbox"/>	new-report.png	png	June 5, 2024, 11:04:11 (UTC-04:00)	84.0 KB	Standard
<input type="checkbox"/>	script.js	js	June 4, 2024, 20:47:03 (UTC-04:00)	1.9 KB	Standard
<input type="checkbox"/>	style.css	css	June 4, 2024, 20:47:04 (UTC-04:00)	3.1 KB	Standard

Name :- Vinayak kumar
Regd no.:- 2201020593
Group :- 7
Branch :- COE