EC-Council

codered
FROM EC-COUNCIL

CHAPTER 10

VIRTUALIZATION AND CLOUD COMPUTING

CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2022 EC-Council International Ltd.

INDEX

Chapter 10:
Virtualization and Cloud Computing

Copyrights @ 2022 EC-Council International Ltd.

SCENARIO

Modern IT environments use server virtualization, network virtualization, storage virtualization, and desktop virtualization for fast provisioning of network environments and to keep pace with modern technologies. Virtualization has been changing security concepts in modern IT environments, as the various security challenges associated with virtualization are unique and distinct from those of conventional environments.

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Its implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. Because of these benefits, many business organizations have recently been migrating their data and infrastructure to the cloud. However, the cloud environment also poses many threats and risks to organizations. Hence, as a security professional you must have the required knowledge to safeguard cloud data from cyber-attacks.

OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing cloud security controls. This includes knowledge of the following tasks:

- Auditing docker host security using tools such as Docker-Bench-Security Tool
- Creating IAM credentials using Google Cloud Platform (GCP)
- Implementation of AWS identity and access management
- Implementation of key management services in AWS platform
- Securing Amazon Web Services Storage

OVERVIEW OF CLOUD COMPUTING

Cloud computing involves on-demand delivery of IT capabilities in which an IT infrastructure and applications are provided to subscribers as metered services over a network. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce. Cloud computing delivers various types of services and applications over the Internet. These services enable users to utilize software and hardware managed by third parties at remote locations. Major cloud service providers include Google, Amazon, and Microsoft.

Copyrights @ 2022 EC-Council International Ltd.

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to secure cloud computing platforms. Recommended labs that will assist you in learning various aspects of cloud computing security include the following:

01 **Audit Docker Host Security using Docker-Bench-Security Tool**

02 **Create IAM Credentials on Google Cloud Platform**

03 **Implement AWS Identity and Access Management**

04 **Implement Key Management Services in AWS**

05 **Secure Amazon Web Services Storage**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

Docker is an open-source technology used for developing, packaging, and running applications and all their dependencies in the form of containers, which ensures that each application works in a seamless environment.

LAB SCENARIO

Docker has been used extensively by organizations that use containers for development or production. Therefore, Docker security plays a key role in safeguarding containers. Although the technology provides many security benefits, its default configuration during installation has some security issues that a security professional must fix.

OBJECTIVE

This lab will demonstrate how to audit the security of a default Docker installation on an Ubuntu host using Docker-Bench-Security Tool.
In this lab, you will learn how to do the following:

- Install Docker on Ubuntu OS
- Audit Docker Security using Docker-Bench-Security Tool

OVERVIEW OF DOCKER

Docker provides Platform-as-a-Service (PaaS) through OS-level virtualization and delivers containerized software packages. Docker-Bench-Security is a tool for auditing Docker; this tool checks the configuration of Docker and reports the status of a current setting or configuration.

Copyrights @ 2022 EC-Council International Ltd.

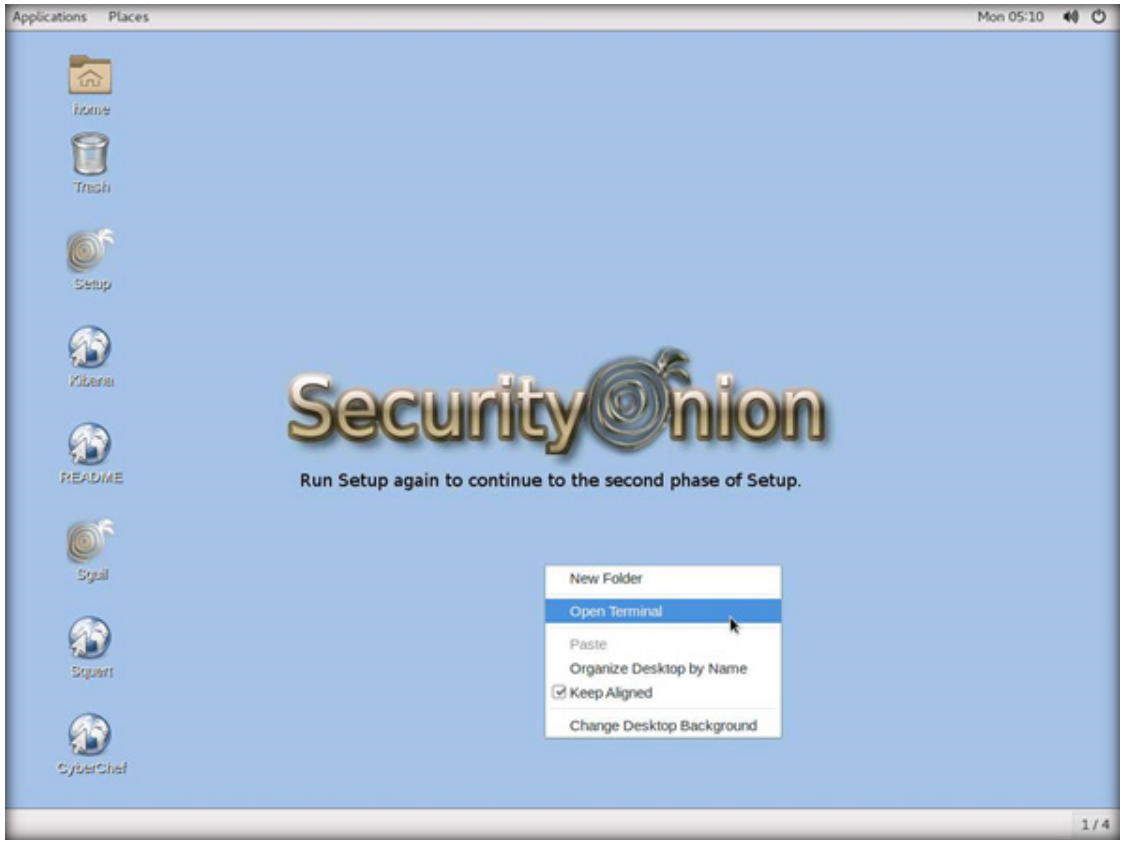
Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-2 virtual machine.

2. Log in with the credentials sam and admin@123.

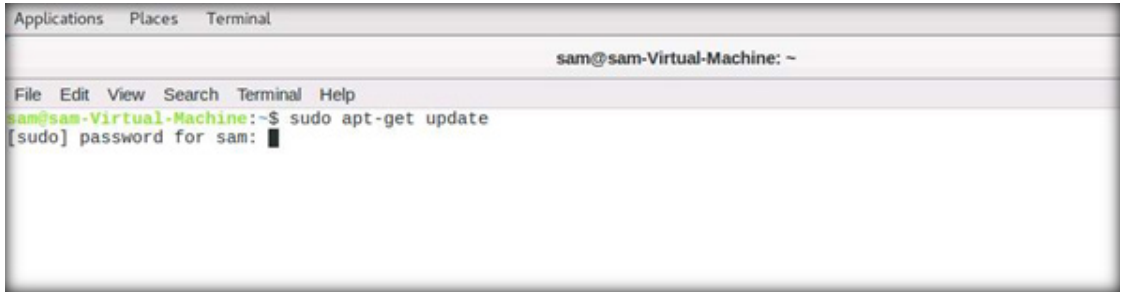
3. Right-click on the Desktop and select the Open Terminal option from the pop-up list as shown in the screenshot below.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL



4. Before installing Docker on the Ubuntu machine, we need to update the system.

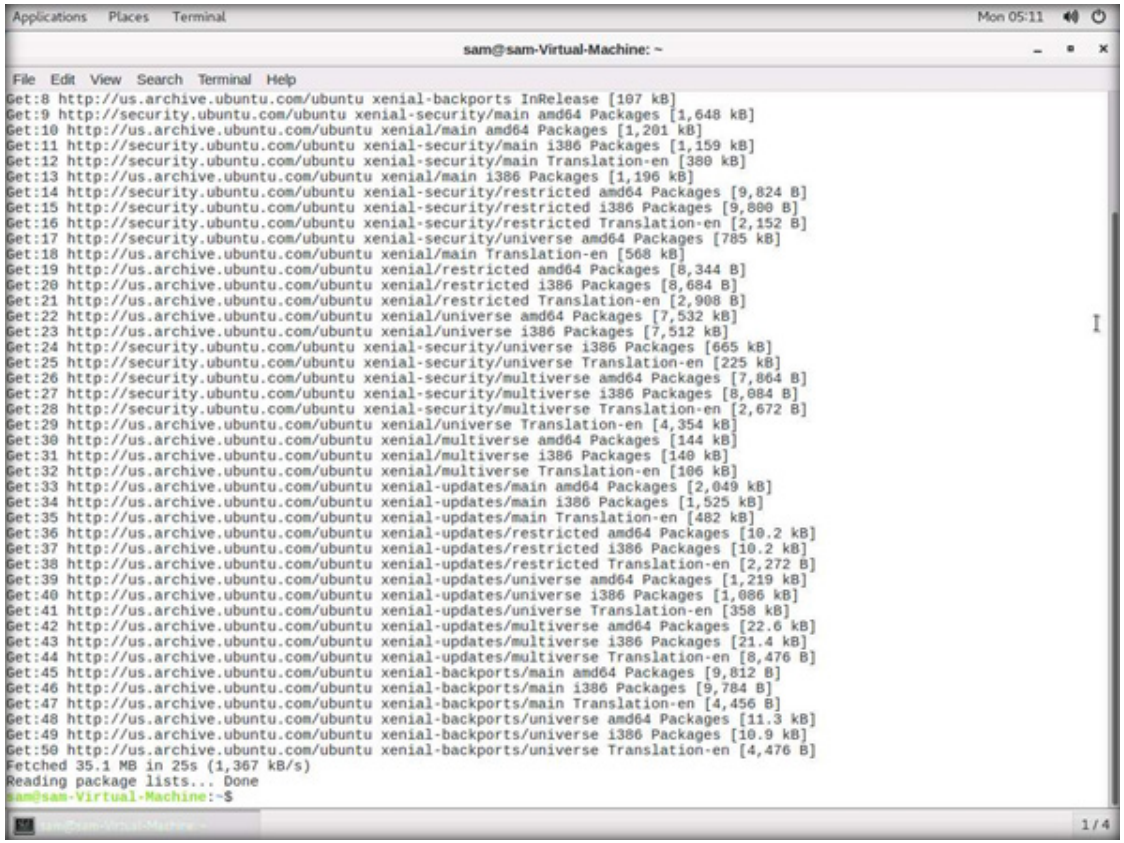
5. Type the sudo apt-get update command and press Enter button to start updating the system. If prompted for password, type admin@123 as the password for the user sam.
Note: The password that you type will not be visible.



EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

6. System update will be successfully completed.

EXERCISE 1:
AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL



Copyrights @ 2022 EC-Council International Ltd.

7. Once the system update is completed, proceed to uninstall any older version of Docker using the following command.

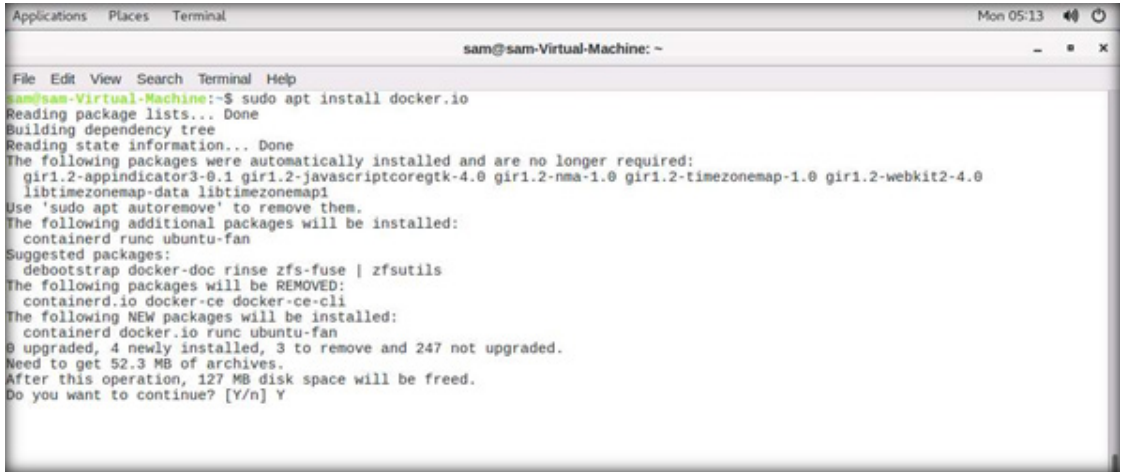
8. Type command sudo apt-get remove docker docker-engine docker.io and press Enter button.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

Copyrights @ 2022 EC-Council International Ltd.

9. Next, to install a newer package of Docker, type command sudo apt install docker.io and press the Enter.

10. If prompted whether to continue, type Y to continue as shown in the screenshot below.

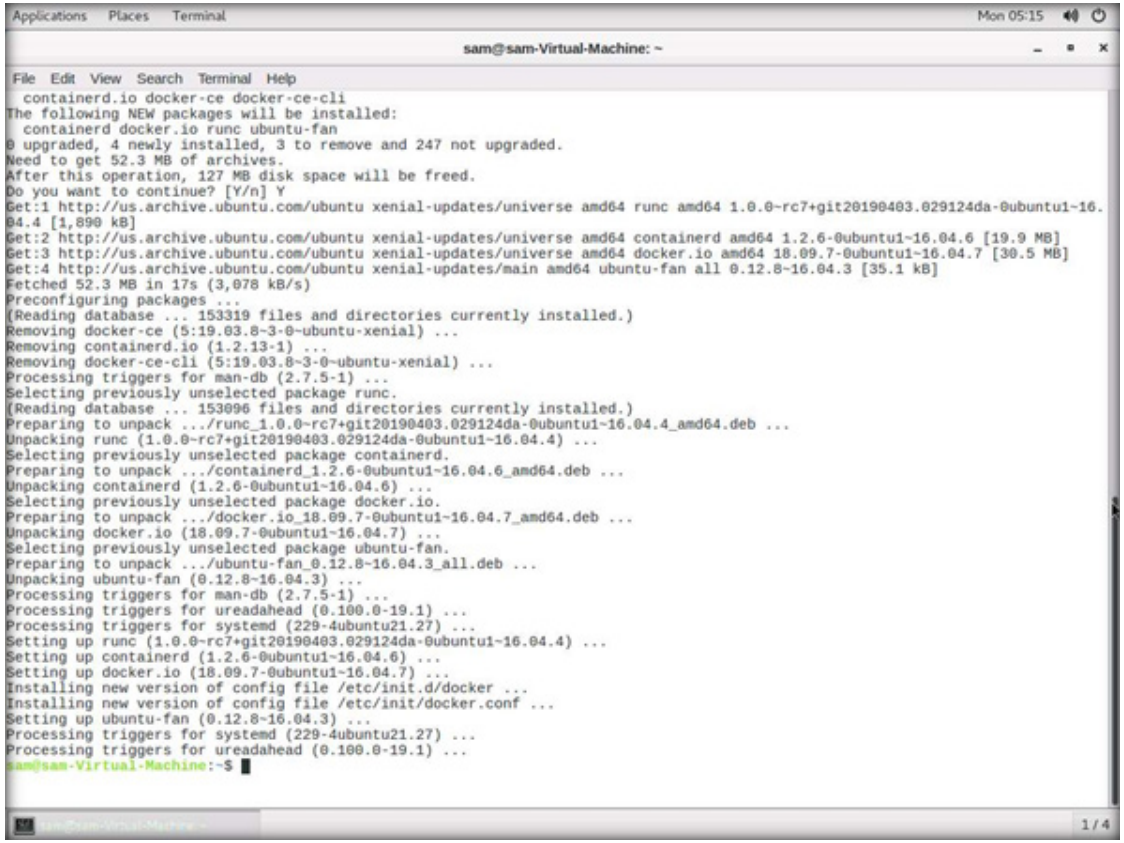


EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

Copyrights @ 2022 EC-Council International Ltd.

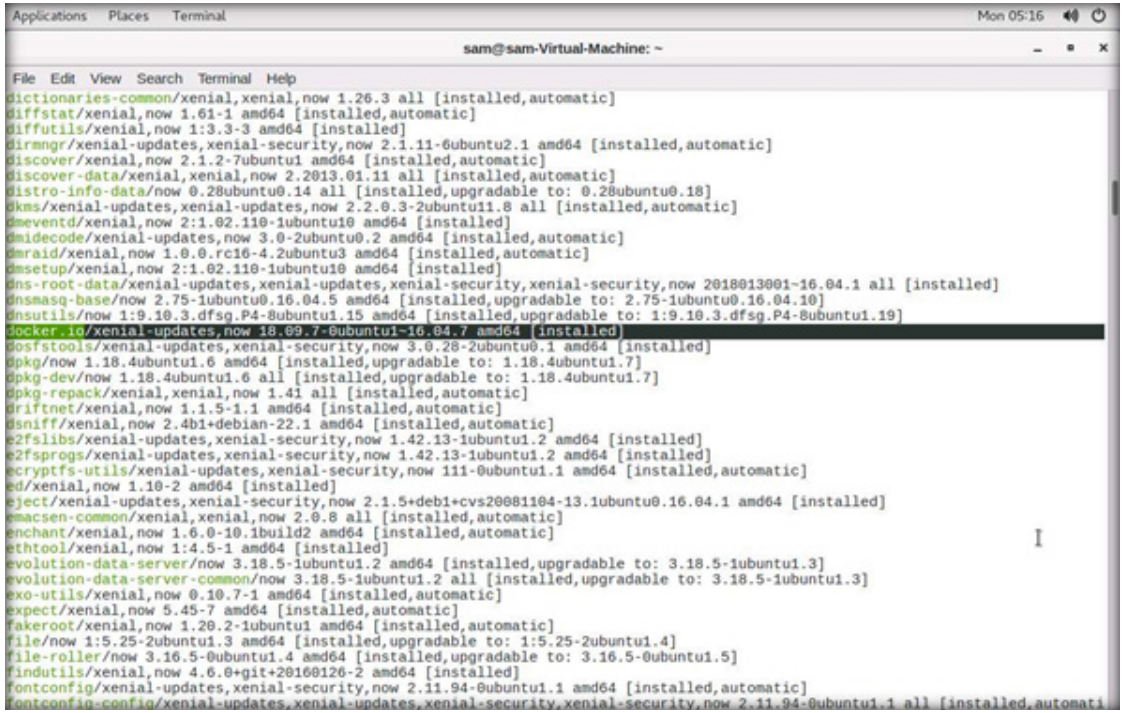
11. Wait for a few seconds till the download is completed.

EXERCISE 1:
AUDIT DOCKER
HOST SECURITY
USING DOCKER-
BENCH-SECURITY
TOOL



12. Type command apt list --installed and press Enter button. The installed packages will be listed out.

EXERCISE 1:
AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL



Copyrights @ 2022 EC-Council International Ltd.

13. Once Docker installation is completed, type command sudo docker images and press Enter.

14. Docker now displays the existing images, as shown in the screenshot below.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

Copyrights @ 2022 EC-Council International Ltd.

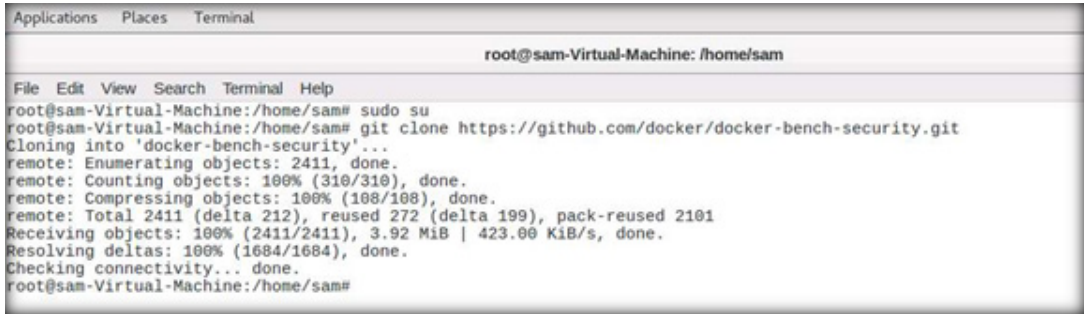
15. Docker-Bench-Security is a tool for auditing Docker.

16. Next, to install the Docker-Bench-Security tool, follow the steps outlined below.

17. The user needs root privileges to install Docker-Bench-Security tool, type sudo su command in the terminal and press the Enter button. If prompts for password, type the password as admin@123.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

18. Type command git clone https://github.com/docker/docker-bench-security.git and press the Enter button.



EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

Copyrights @ 2022 EC-Council International Ltd.

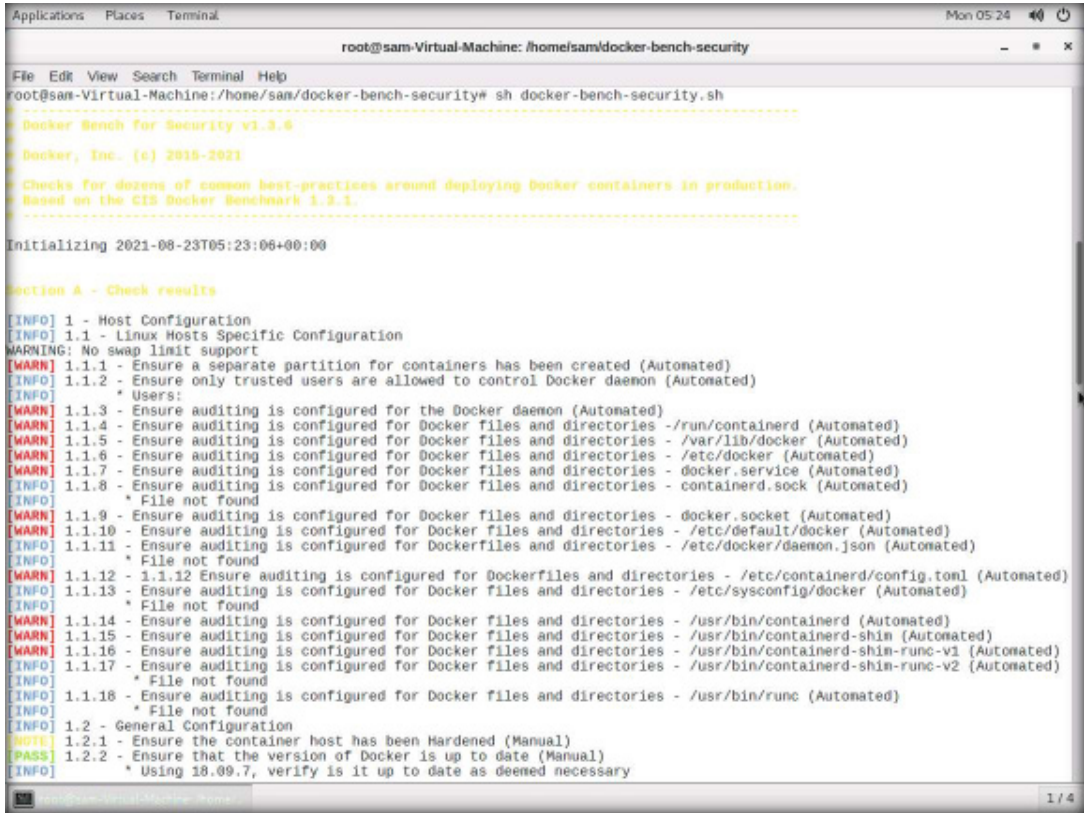
19. Docker-Bench-Security clone will be created in your current working directory.

20. Next, to change directory to the docker-bench-security folder, type cd docker-bench-security and press Enter.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

21. Next, to run the script, type sh docker-bench-security.sh and press the Enter button.

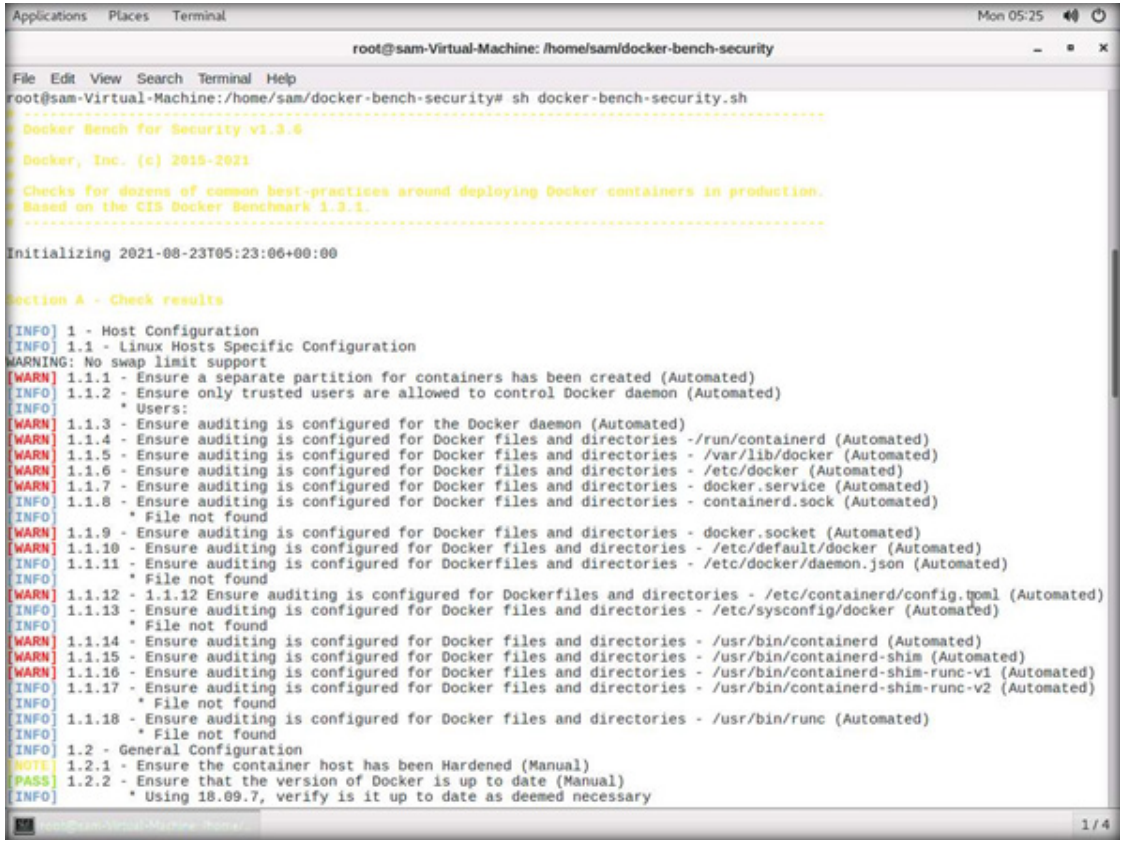
EXERCISE 1:
AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL



Copyrights @ 2022 EC-Council International Ltd.

22. Docker-Bench-Security v1.3.6 loads. Wait for a few seconds; the status of the current Docker configuration is displayed, as shown in the screenshot below.

EXERCISE 1:
AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL

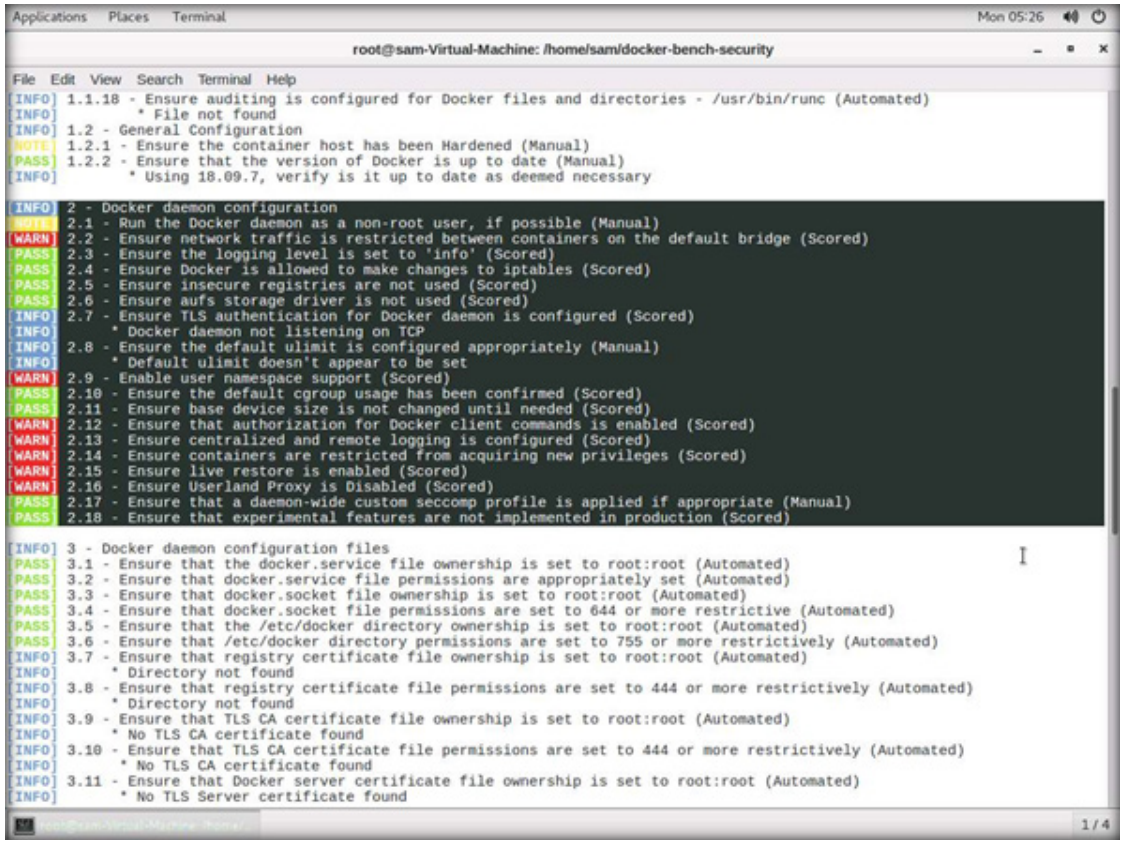


Copyrights @ 2022 EC-Council International Ltd.

23. The [WARN] line in red color indicates the security warning, and the configuration needs to be changed according to the provided information.
24. The [INFO] line in blue color provides information about the security.
25. The [PASS] line in green color shows the escaped configuration test.
26. Scroll down the terminal screen till you can see the different sections of the report.
27. Go to the Docker daemon configuration section, and you can see the warnings of Docker daemon configuration.

Note: The warnings might vary in your lab environment.

EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER-BENCH-SECURITY TOOL



Copyrights @ 2022 EC-Council International Ltd.

28. These warnings can be resolved by configuring Docker daemon securely. The Docker daemon is a service to run Docker. This service can be configured using the JSON file, which is useful for keeping all docker configurations.
Note: Docker performs various operations on the host to run containers such as Docker pull, Docker push, and Docker run. By default, Docker loads content over the network without verifying, and it is harmful to download images in Docker from untrusted sources. A security professional needs to secure the default configuration of Docker and ensure that no insecure breach left in the Docker environment.

29. Close the terminal.

30. As described above, a security professional can audit Docker security using the Docker-Bench-Security Tool.

31. Turn off the Admin Machine-2 virtual machine.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 2: **CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM**

Google Cloud Platform (GCP) provides IaaS, PaaS, and serverless computing services.

LAB SCENARIO

A security professional must have the required knowledge to create IAM credentials and assign various roles to the organization's employees according to their job demand.

OBJECTIVE

This lab will demonstrate how to create an IAM Group and IAM User, attach a role to the user and to Create a service account.

OVERVIEW OF GOOGLE CLOUD PLATFORM

The services offered by the Google Cloud Platform (GCP) include computing, data storage and analytics, machine learning, networking, bigdata, cloud AI, management tools, identity and security, IoT, and API platforms.

Copyrights @ 2022 EC-Council International Ltd.

Note: To perform this task, you must have a Gmail account.
Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.

2. Log in with the credentials Admin and admin@123.
Note: If the network screen appears, click Yes.

3. To open the browser, double-click on the Google Chrome icon on the Desktop.

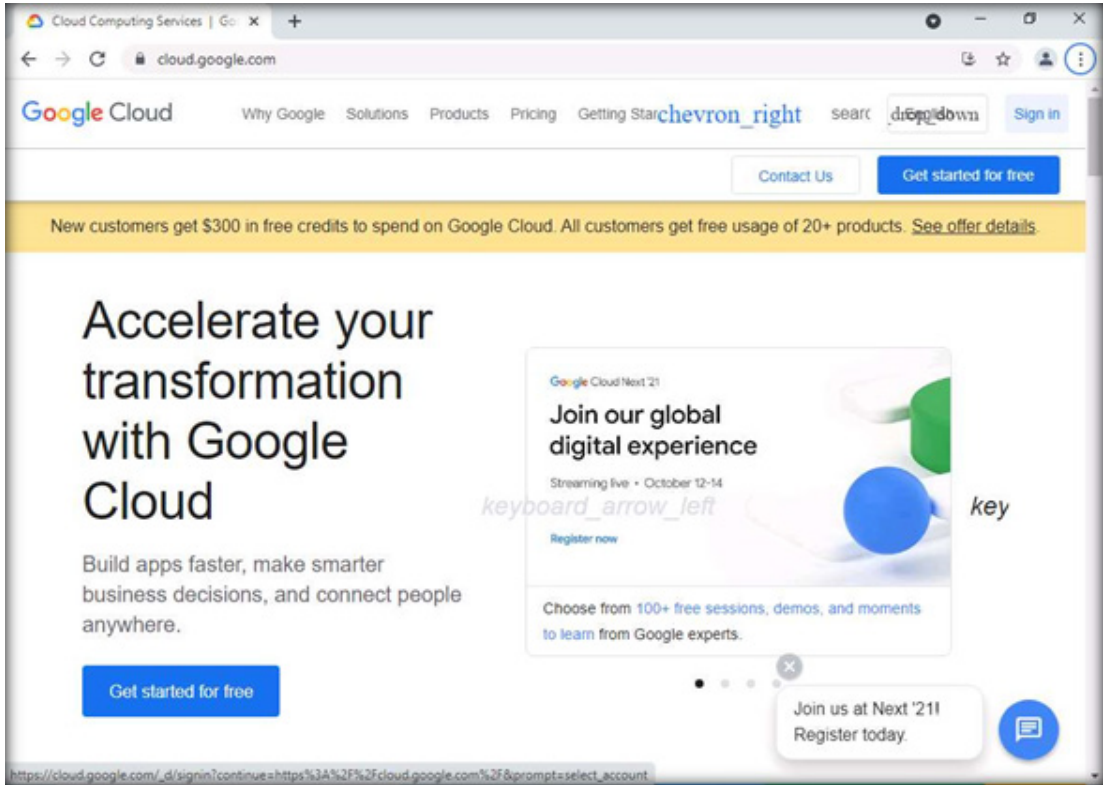
4. The Google Chrome browser opens. Go to the address bar, click https://cloud.google.com, and press Enter.

EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

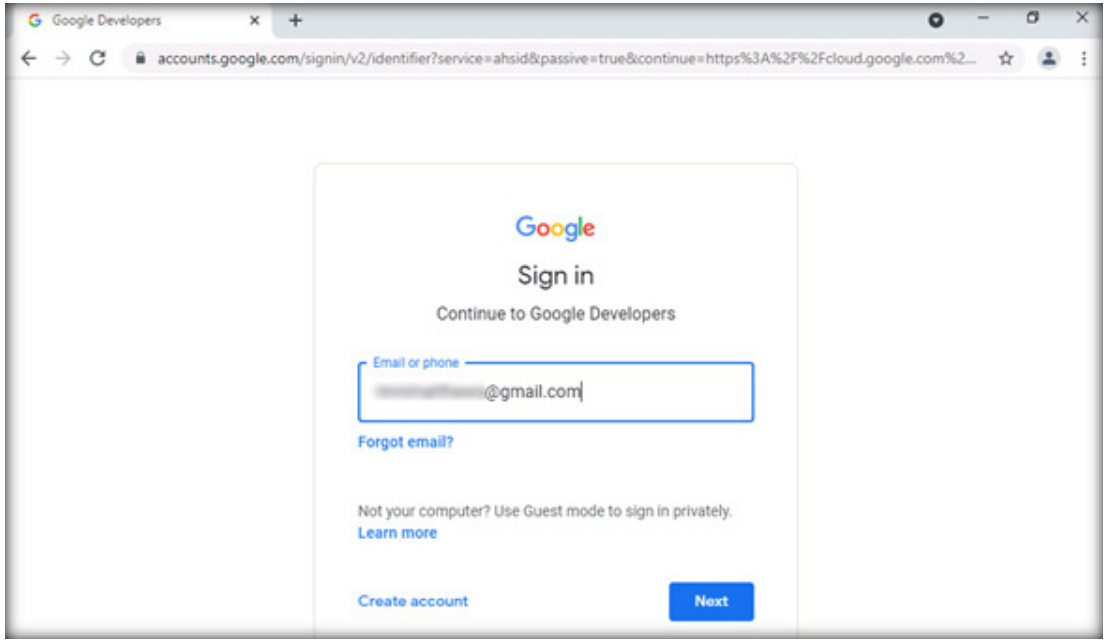
Copyrights @ 2022 EC-Council International Ltd.

5. The Google Cloud page appears. Click on Sign in present at the top-right corner of the page.

EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM



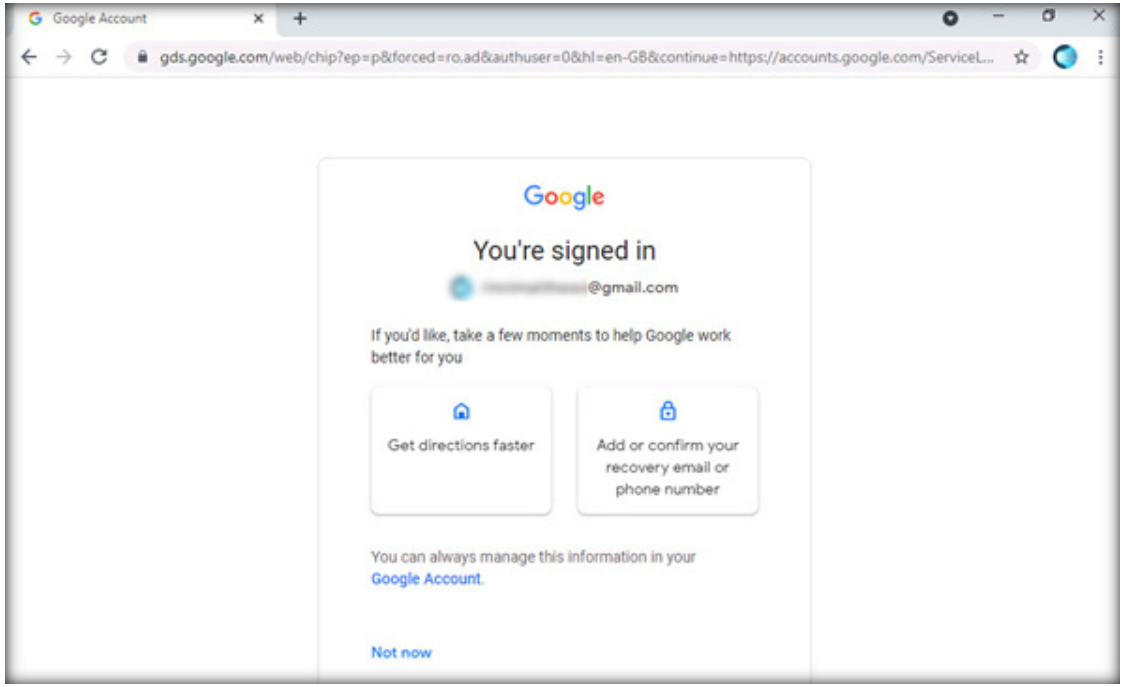
6. Sign in page appears, in the Email or phone field, enter your Gmail account ID and click Next.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

7. In the next page, enter your password and click Next.

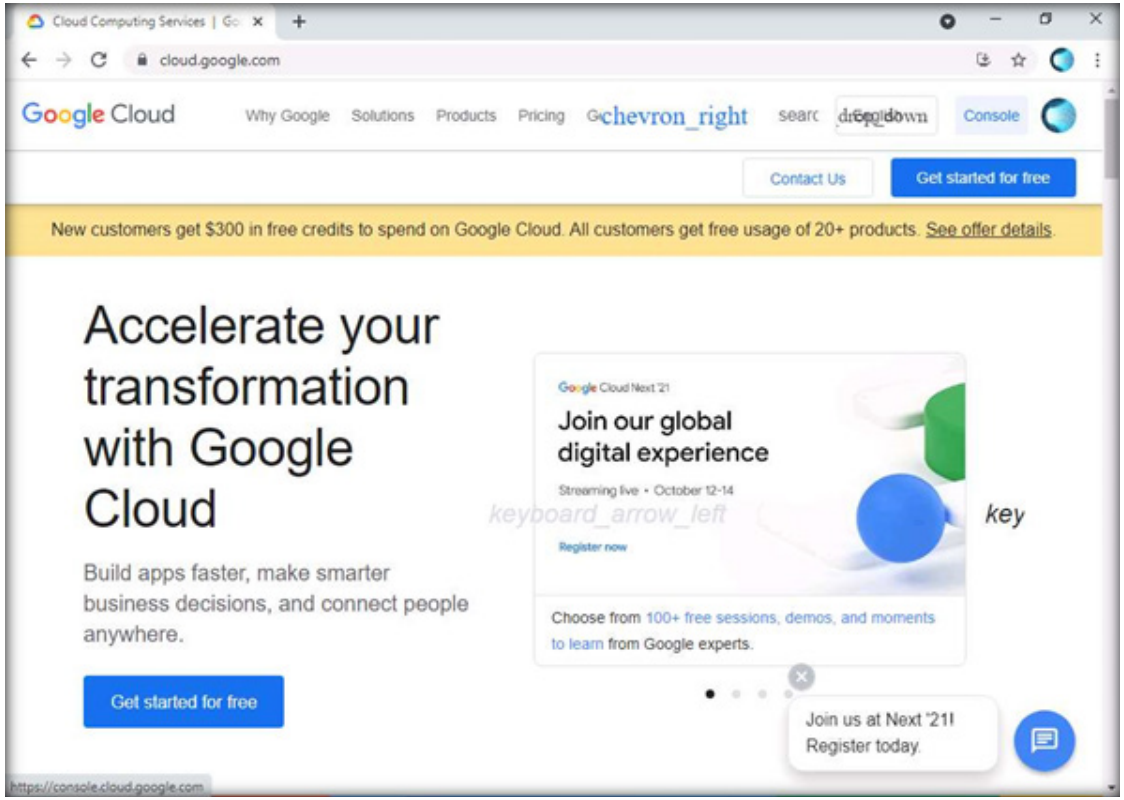
8. You're signed in page appears, click Not now to continue.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

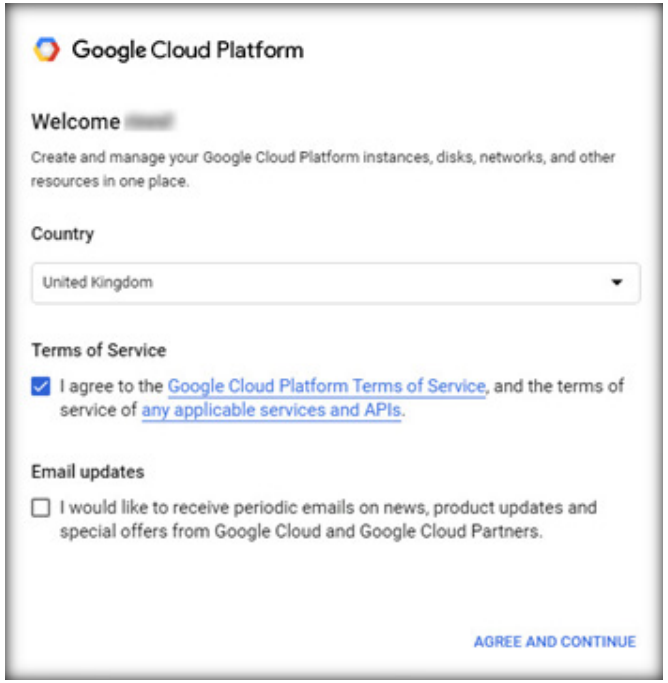
9. Google Cloud platform appears, click Console present at the top-right corner of the page.

EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM



10. A welcome page appears. Under the Terms of Service section, select I agree checkbox and click AGREE AND CONTINUE.
Note: The options in the screenshot might differ in your lab environment.

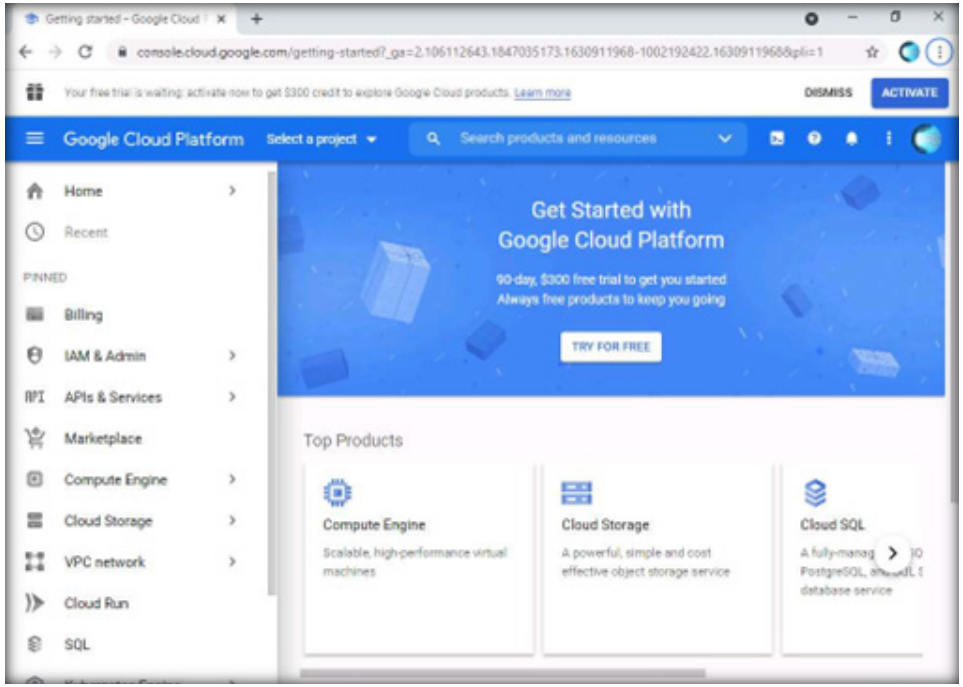
EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM



Copyrights @ 2022 EC-Council International Ltd.

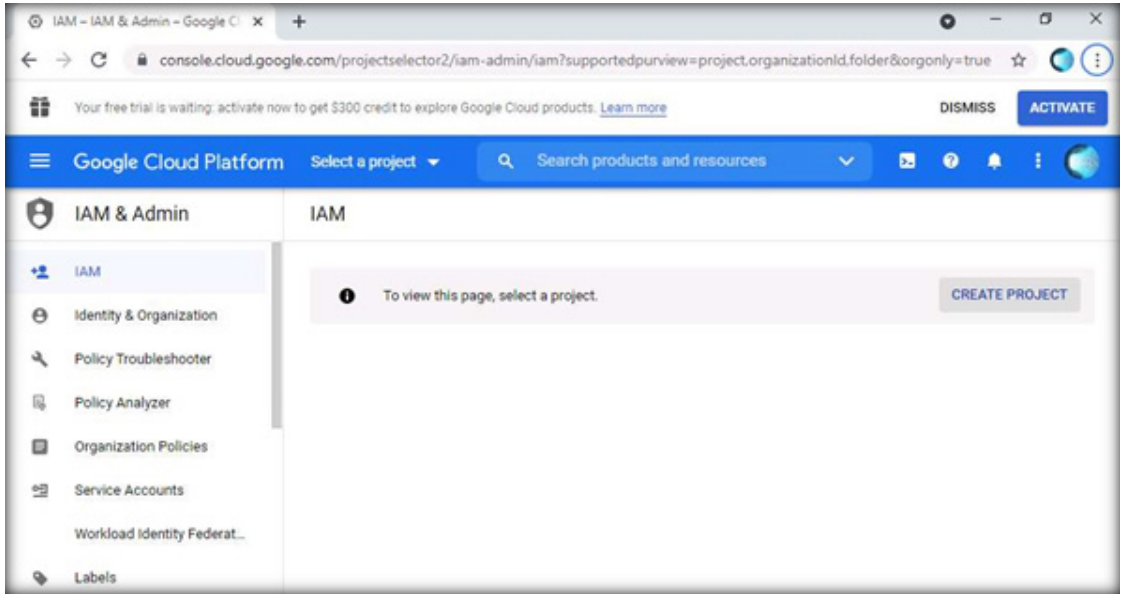
11. How are you planning to use Google Cloud? page appears, click SKIP.

12. The main dashboard page appears, click IAM & Admin option from the left-pane.



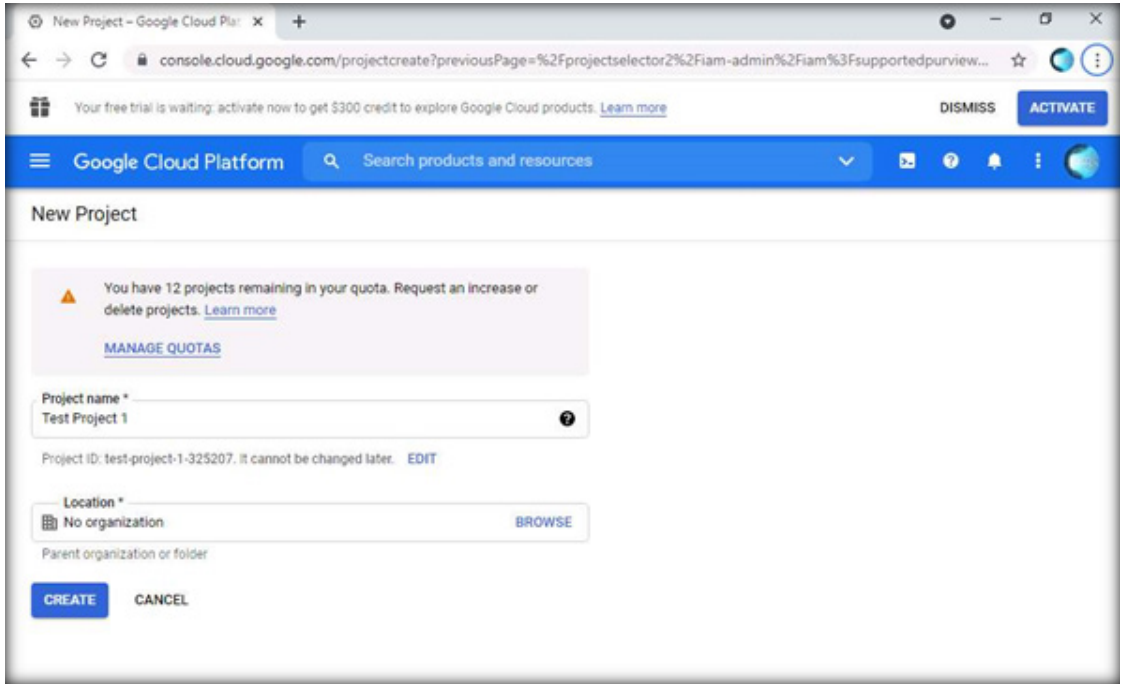
EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

13. Now, click CREATE PROJECT under the IAM section in the right-pane.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

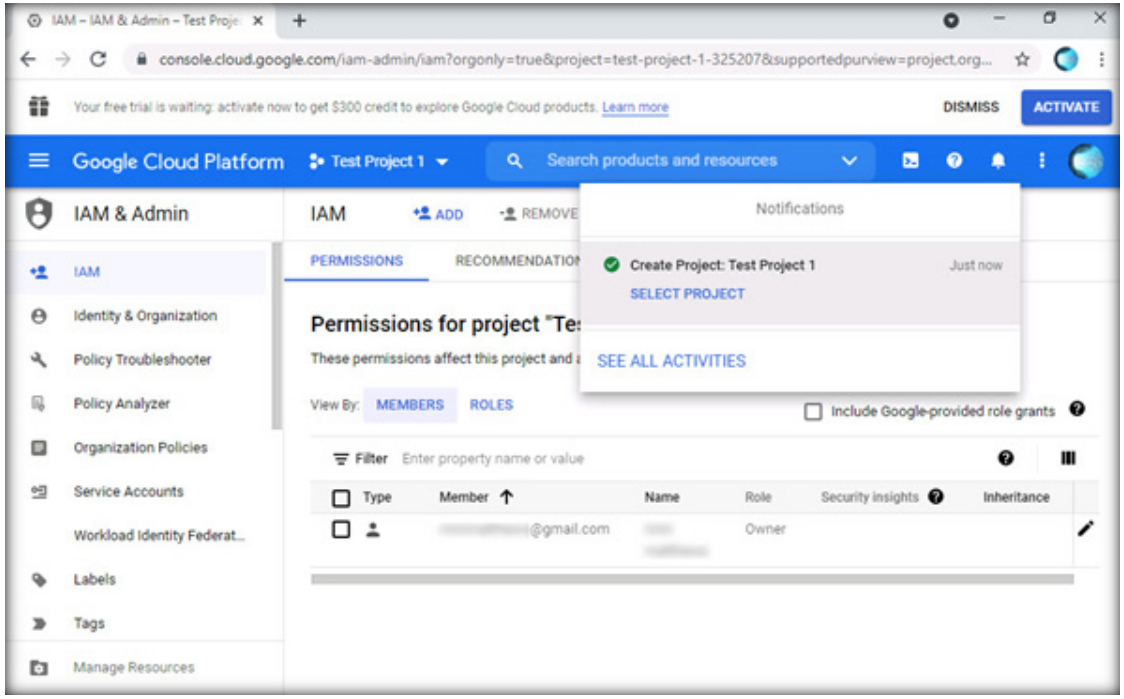
14. New Project page appears, enter the Project name as Test Project 1 and click CREATE.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

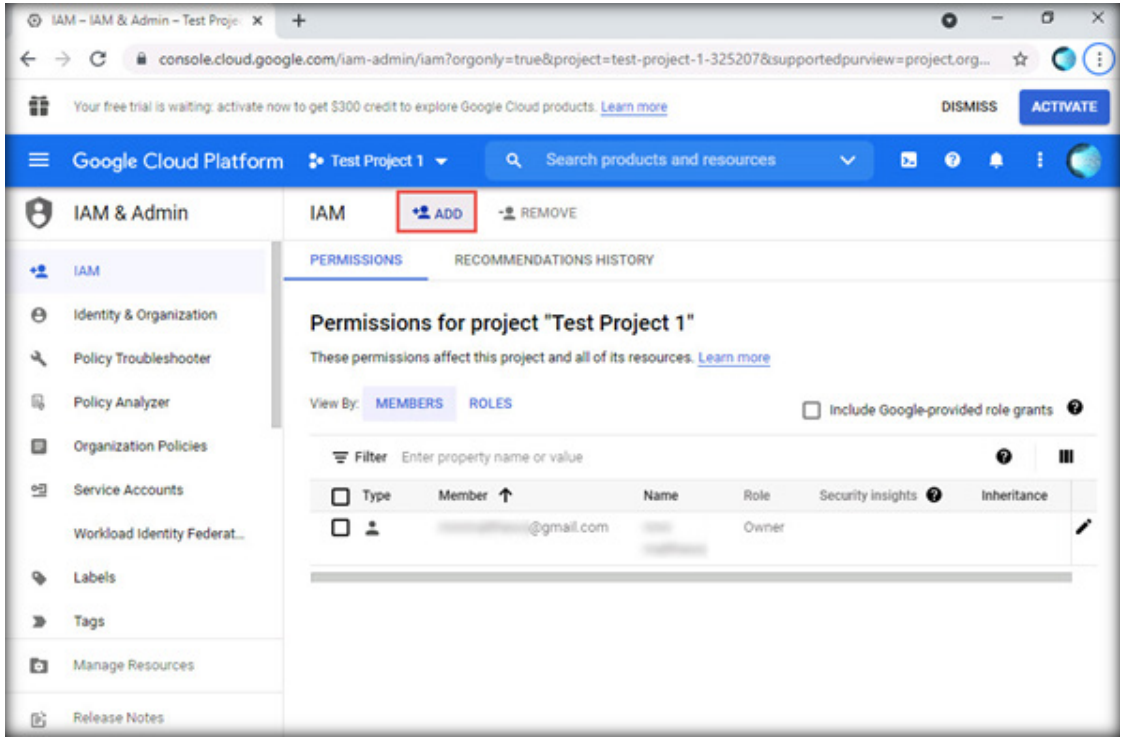
Copyrights @ 2022 EC-Council International Ltd.

15. A new project has now been created successfully, as shown in the screenshot below.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

16. Now, click ADD button present at the top of the page.

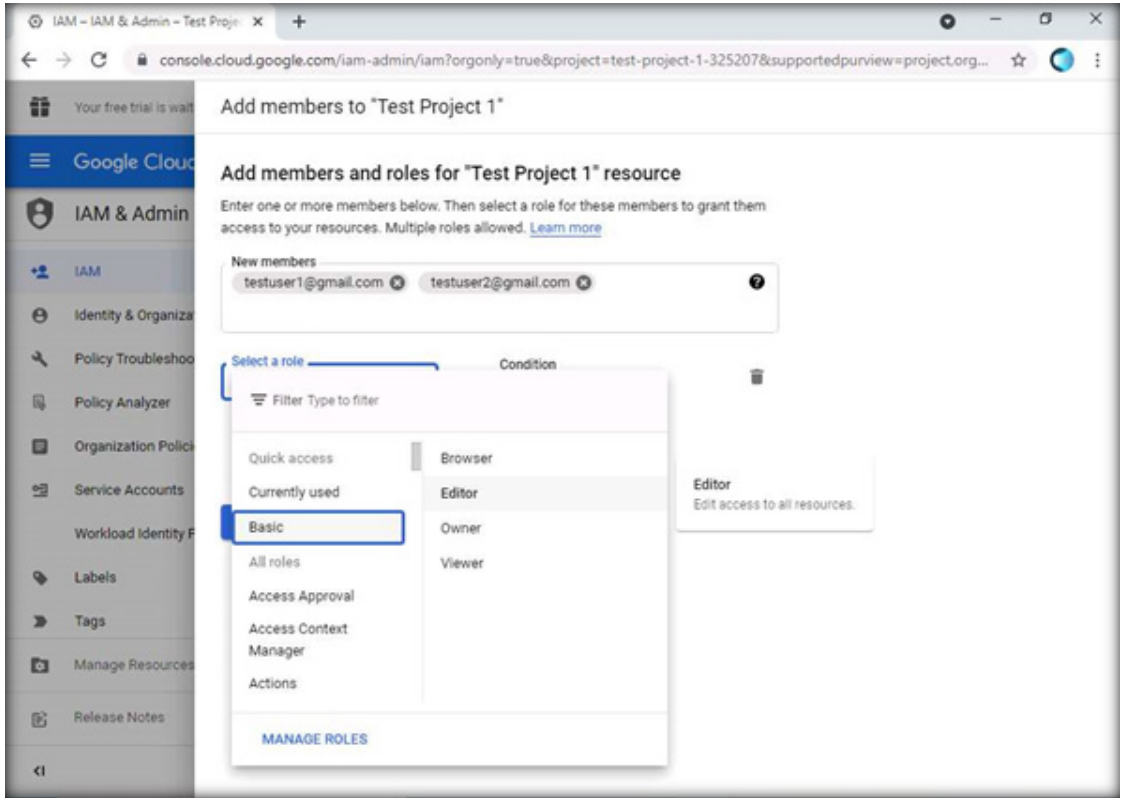


EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

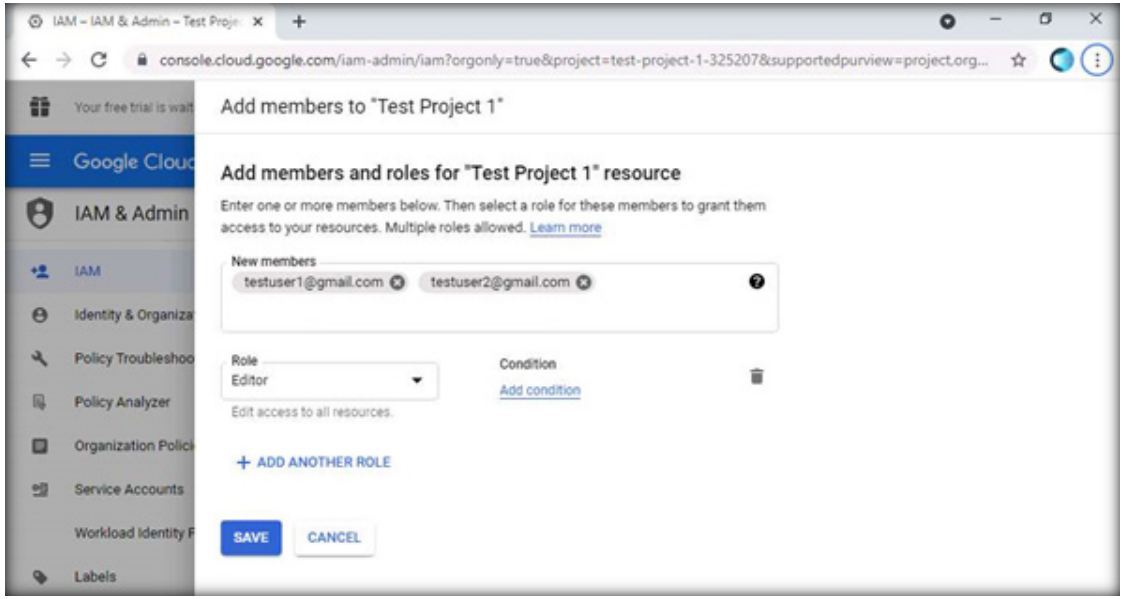
17. The Add members and roles for “Test Project 1” resource page appears. In the New members field, add the members (here, two members are added testuser1@gmail.com and testuser2@gmail.com).
Note: If Add principals and roles for “Test Project 1” resource page appears. In the New principals field, add the principals (here, two principals are added testuser1@gmail.com and testuser2@gmail.com).
Note: The users testuser1@gmail.com and testuser2@gmail.com are demo users, you can add users of your choice.

18. In a Select a role field, click drop-down icon and hover the mouse-cursor over Basic option. Under Basic option, select Editor option.

EXERCISE 2:
CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

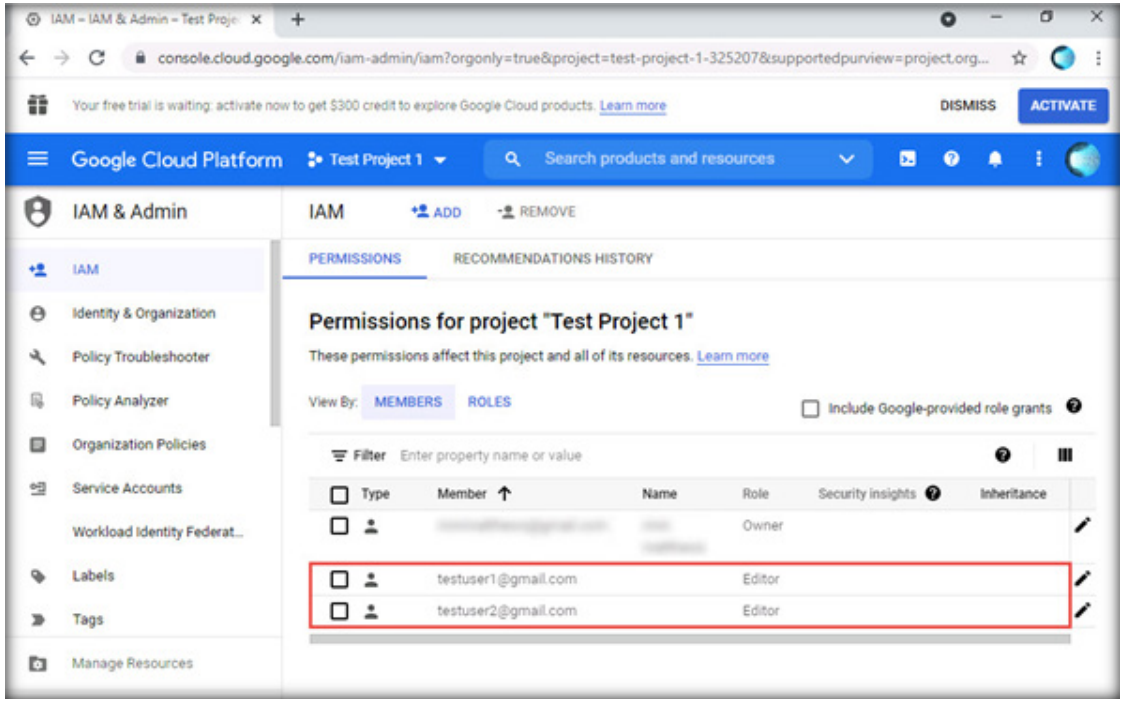


19. Click SAVE to save the settings.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

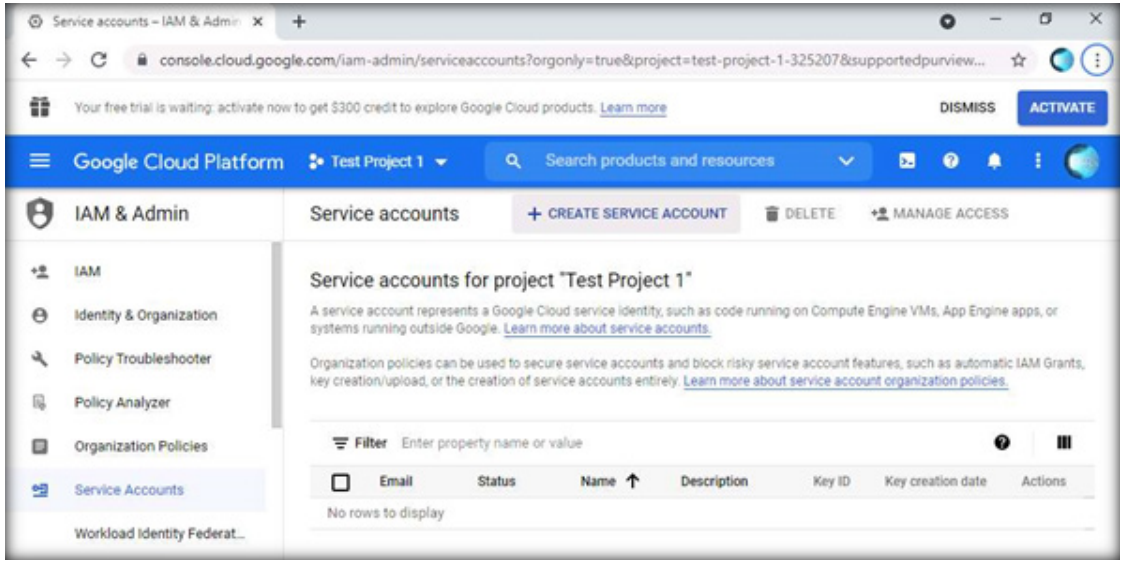
20. You can observe that the members, along with the assigned Roles have been added successfully, as shown in the screenshot below.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

21. Now, we will create a service account. To do so, click Service Accounts option from the left-pane.
Note: A service account is a type of Google account that grants permissions to the virtual machines instead of end users.

22. The Service accounts page appears; click on CREATE SERVICE ACCOUNT from the top-section of the page, as shown in the screenshot below.
Note: If Google tutorial pop-up appears, click GOT IT to close it.

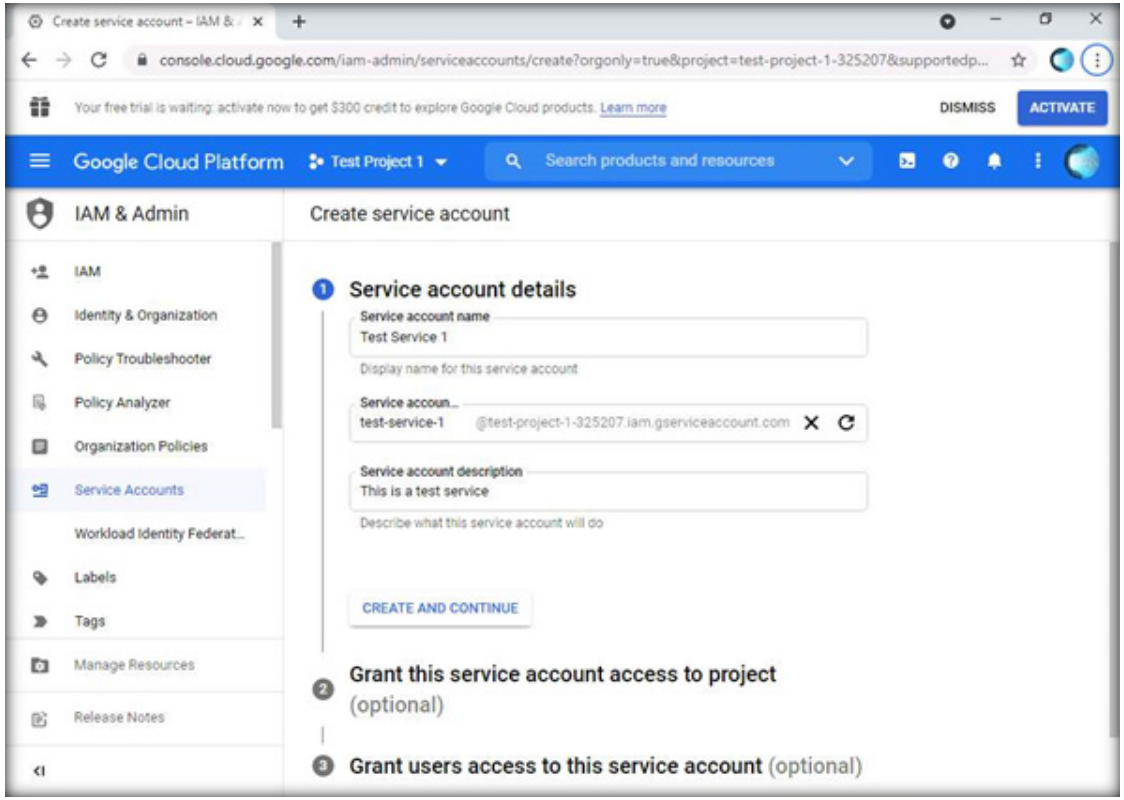


EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

Copyrights @ 2022 EC-Council International Ltd.

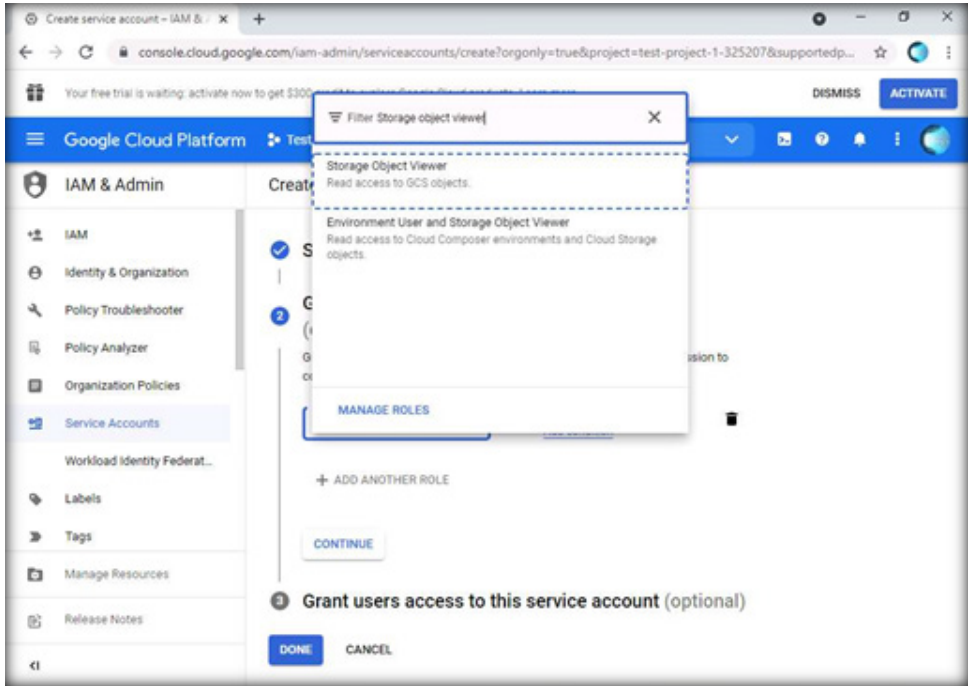
23. The Create service account page appears, in the Service account name field, enter Test Service 1. In the Service account description, enter This is a test service and click CREATE AND CONTINUE.

EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM



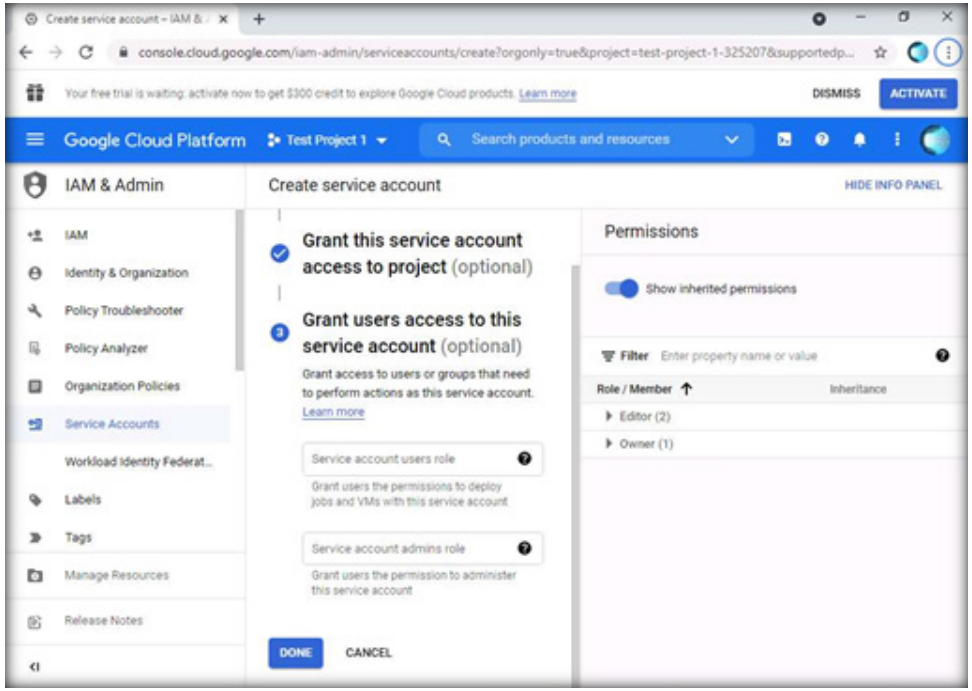
24. The Grant this service account access to project section appears, click Select a role field. A drop-down with options appears, in the Type to filter field, enter Storage object viewer. Select Storage object viewer from the options.

EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM



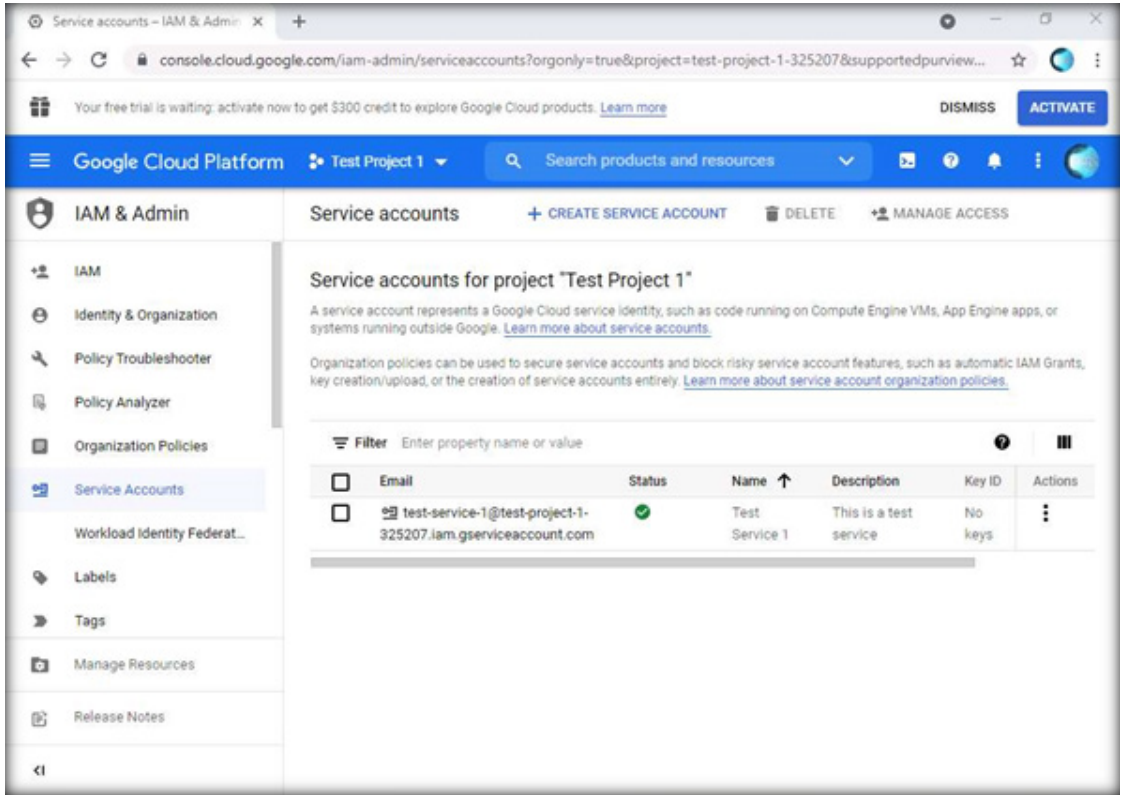
25. Click CONTINUE.

26. Now, click DONE to create the service account.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

27. A service account has been created successfully, as shown in the screenshot below.



EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

28. Using this custom service account, we can then create a virtual machine inside the platform.

29. You can further explore the various other options provided by Google Cloud Platform.

30. This concludes the demonstration showing how to create IAM credentials on Google Cloud Platform.

31. Close all open windows.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 3: **IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT**

Amazon Web Services (AWS) provides on-demand cloud computing services to individuals, organizations, the government, etc. on a pay-per-use basis.

LAB SCENARIO

AWS IAM enables security professionals to control access to AWS services and resources securely. It allows establishment of access rules and permissions for specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) for resource access. This helps security professionals assign role-based access control for accessing critical information within the enterprise.

OBJECTIVE

This lab will demonstrate how to create an IAM group and IAM user, attach a policy to the user, and enable Multi-Factor Authentication (MFA) that enables adding two-factor authentication for individual users in order to ensure additional security for the user accounts in AWS.
In this lab, you will learn to do the following:

- Create IAM Group in AWS
- Create IAM User in AWS
- Assign permission policy to user
- Create custom IAM policy in AWS
- Enable MFA

OVERVIEW OF IAM

IAM enables role-based access control for accessing critical information within the enterprise. It comprises business processes, policies, and technologies that allow monitoring electronic or digital identities. IAM provides tools and technologies to regulate user access (creating, managing, and removing access) to systems or networks based on the roles of individual users within the enterprise. Organizations generally prefer all-in-one authentication, which can be extended to Identity Federation. Identity Federation includes IAM with single sign-on (SSO) and centralized Active directory (AD) account for secure management. For the root user account of cloud, and its associated user accounts, MFA is enabled. MFA is used to control access to Cloud Service APIs. However, the best option is choosing either Virtual MFA or a hardware device.

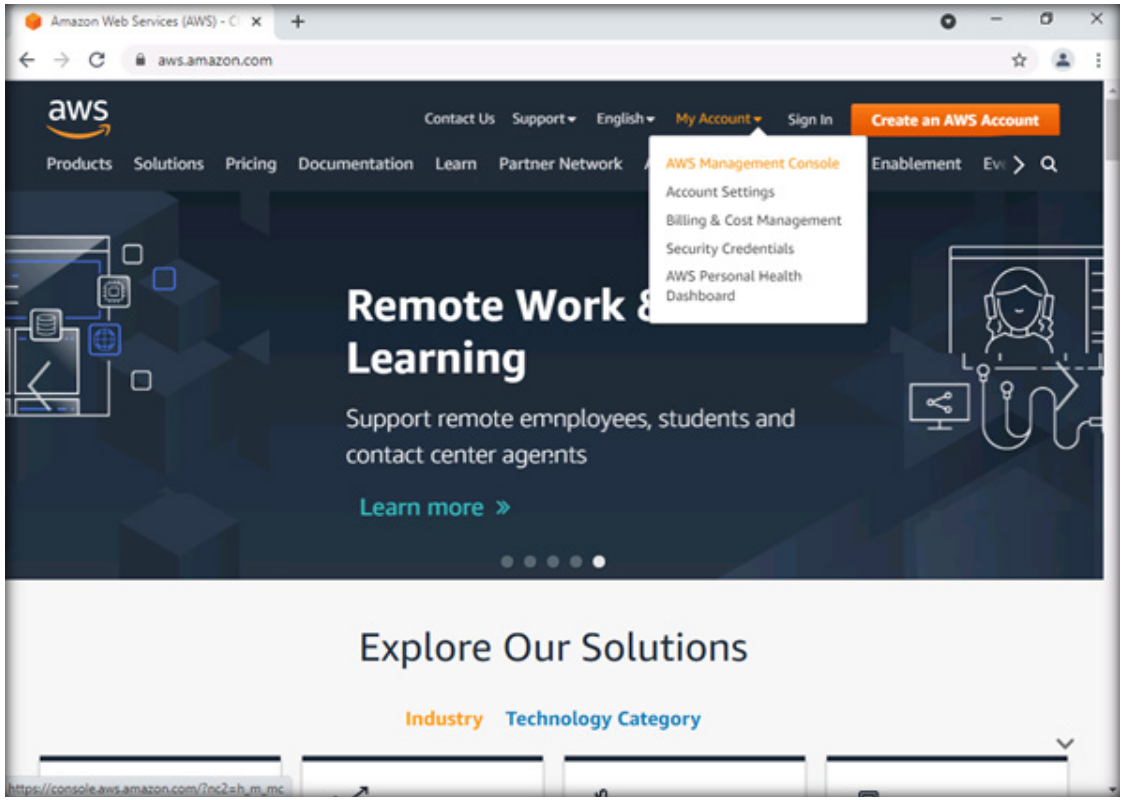
Copyrights @ 2022 EC-Council International Ltd.

Note: Before starting this lab, you should create an AWS account using the following: https://portal.aws.amazon.com/billing/signup. Once the registration is completed, perform the following tasks.
Note: Ensure that PfSense Firewall and Admin Machine-1 virtual machines are running.
1. In the Admin Machine-1 virtual machine, double-click on the Google Chrome icon on the Desktop to open the browser.

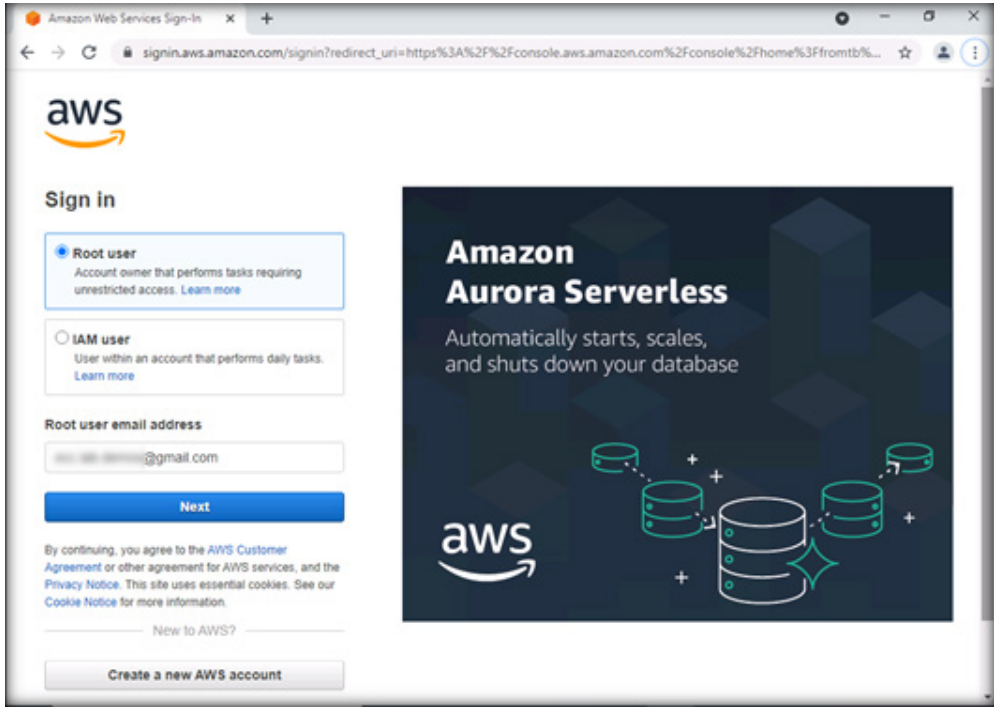
2. The Google Chrome browser opens. Go to the address bar, type https://aws.amazon.com/, and press Enter.

3. The AWS Web Services - Cloud Computing Services page appears. Click on AWS Management Console from the My Account drop-down menu as shown in the screenshot below.

EXERCISE 3:
IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



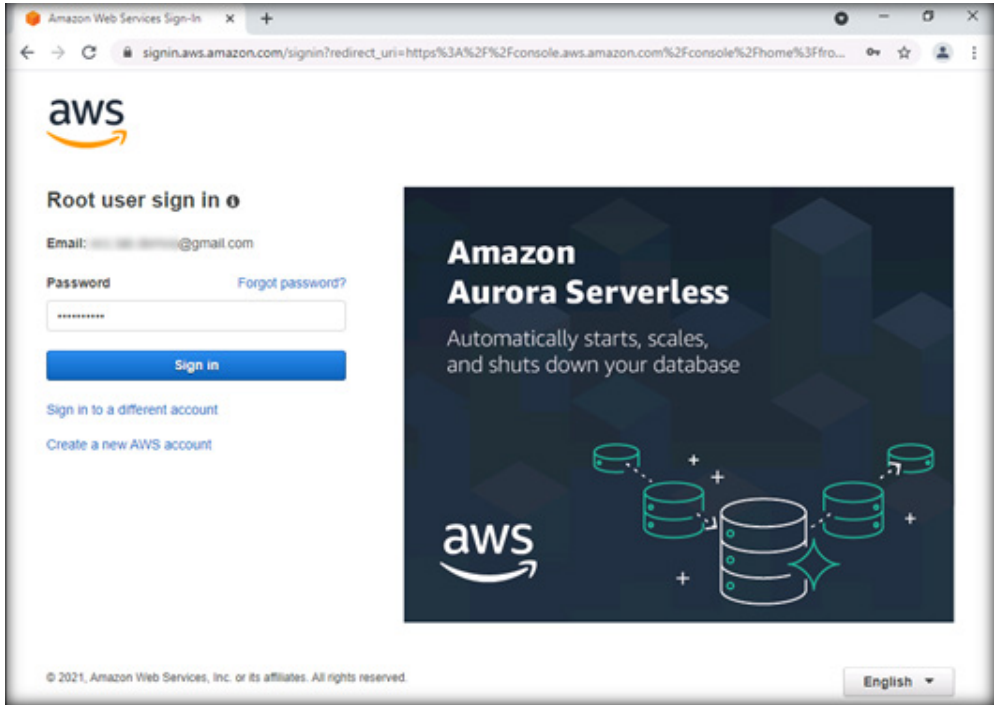
4. The AWS Web Services Sign-in page appears. Type the AWS administrator account ID and click on Next.
Note: In the next window, type the characters seen in the image and click on submit.



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

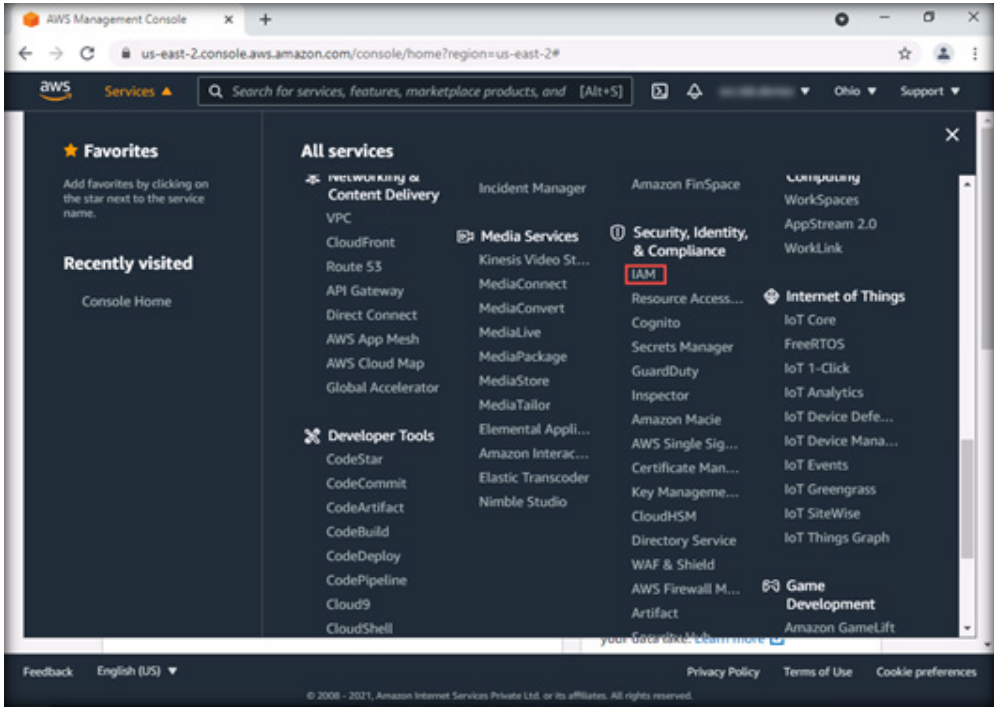
Copyrights @ 2022 EC-Council International Ltd.

5. In the Password field, type the password, and click on Sign-in.



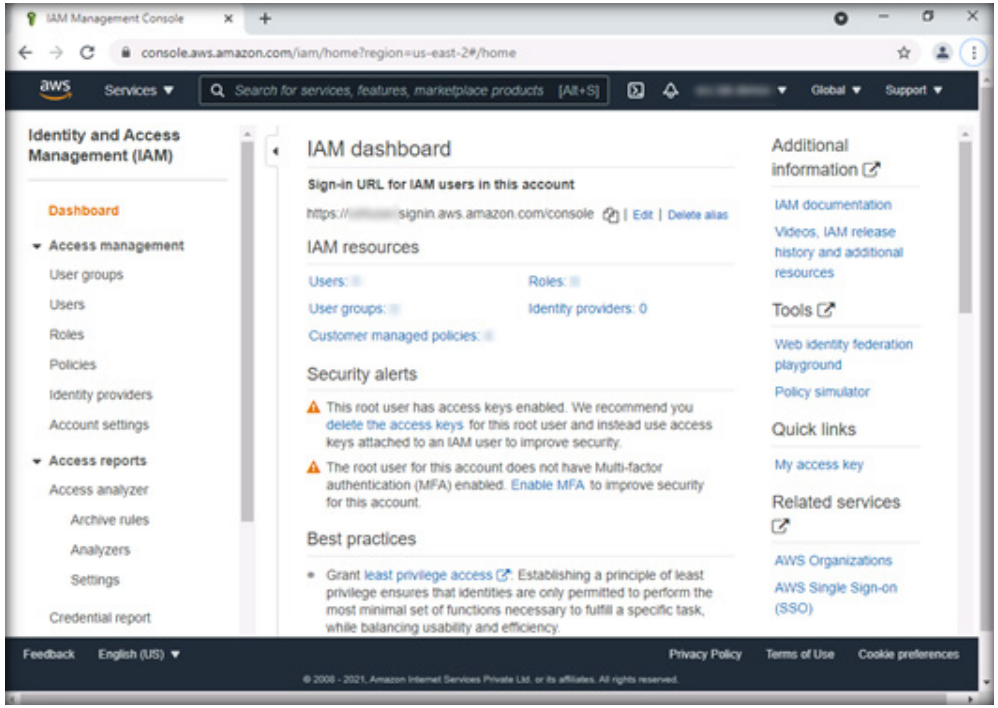
EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

6. Select Services from the menu bar and click on IAM under the Security, Identity, & Compliance section.



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

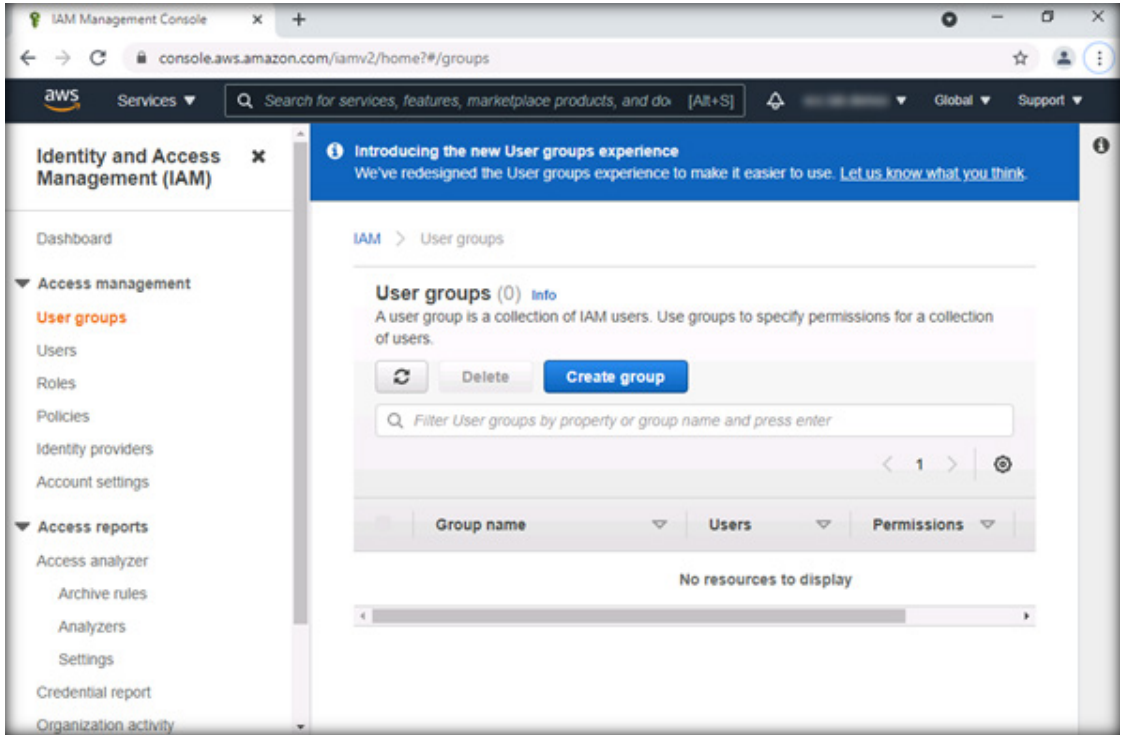
7. The Welcome to the Identity and Access Management (IAM) page appears. Click on User groups in the left pane under Access management.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

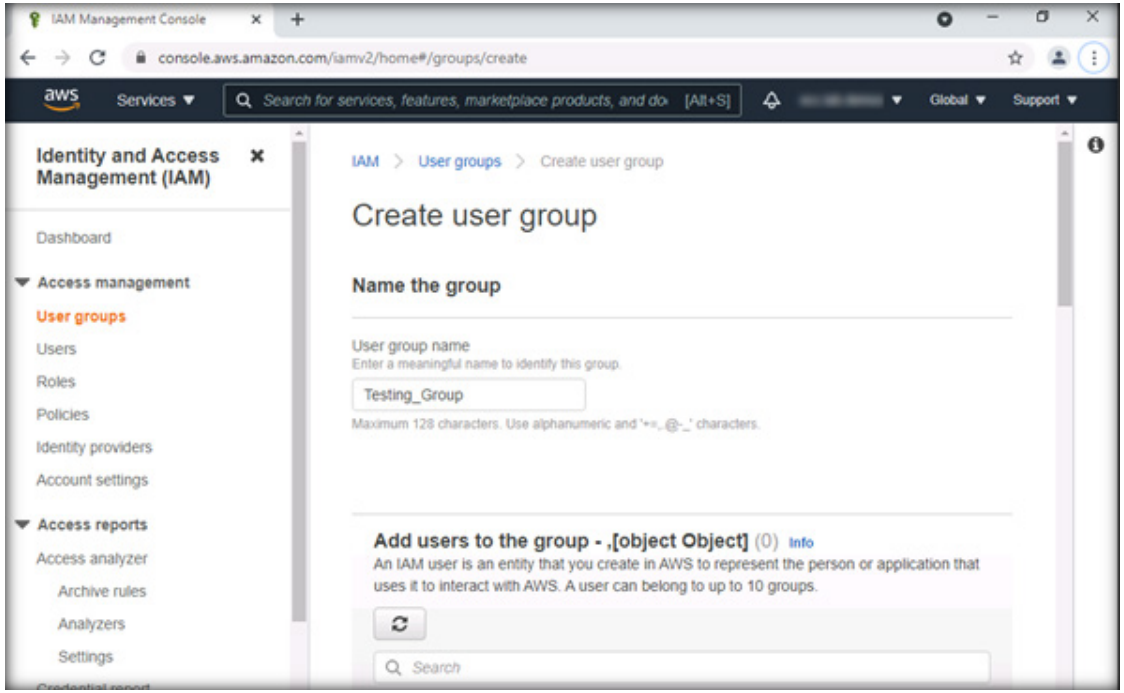
Copyrights @ 2022 EC-Council International Ltd.

8. Now, click on Create group.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

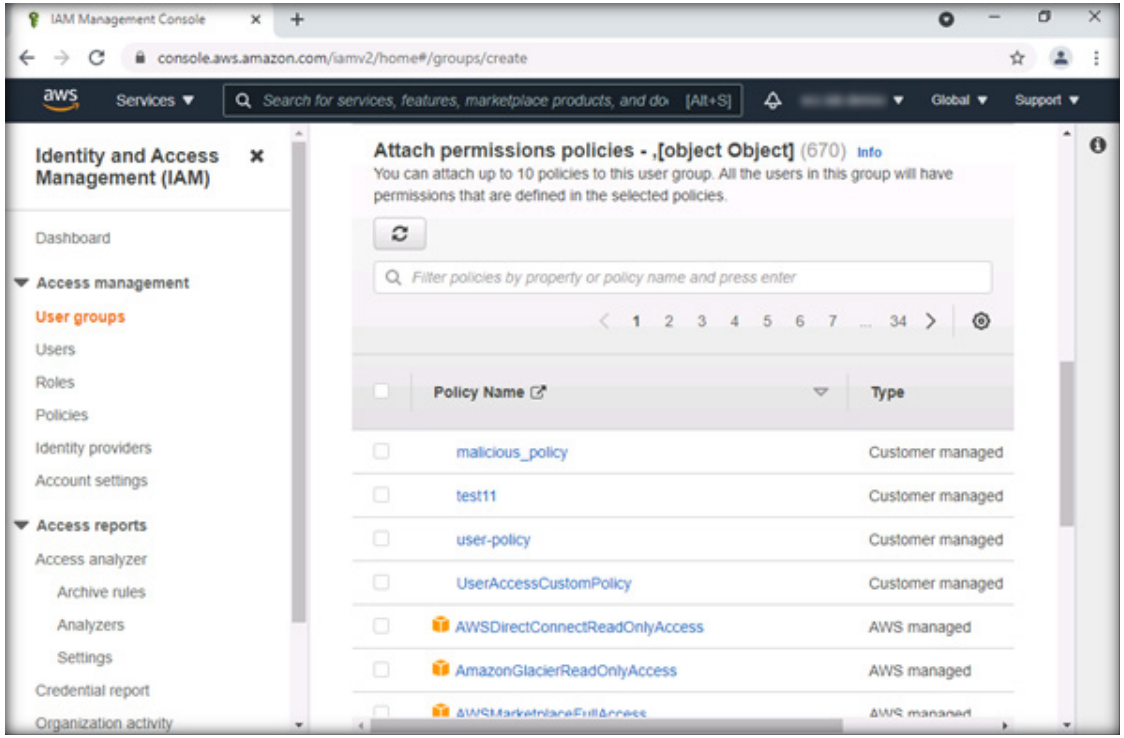
9. In the Create user group section, type the group name in the User group name field (here, the group name is Testing_Group).



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

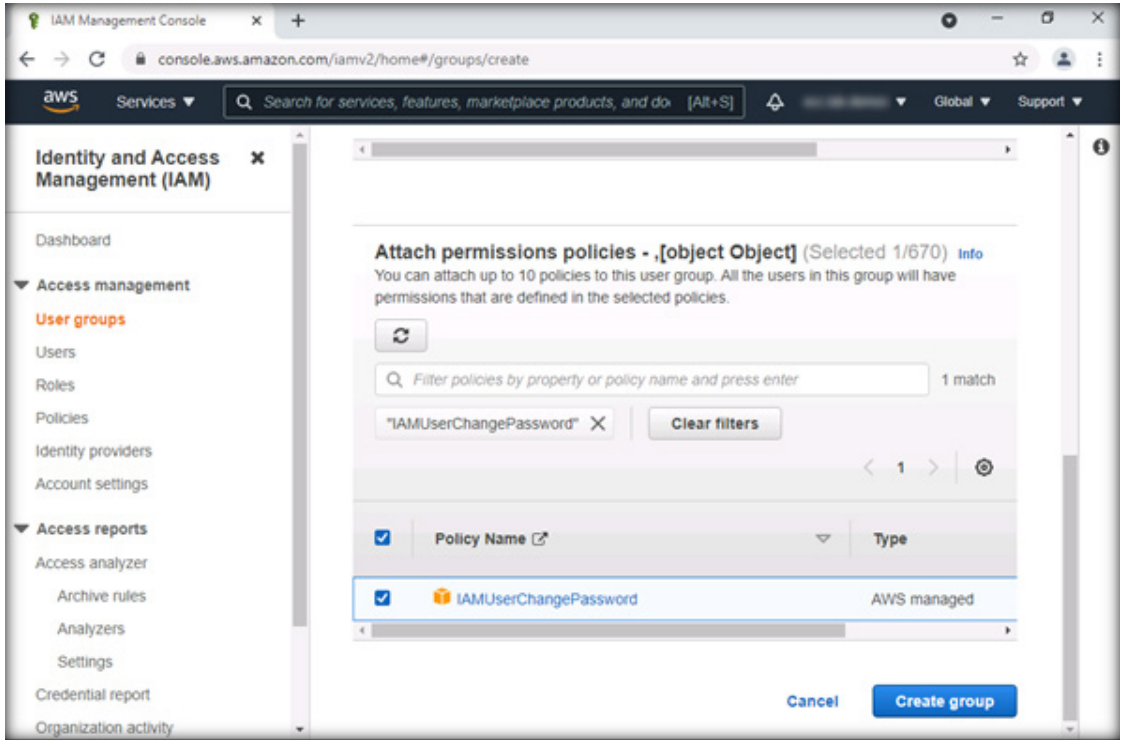
Copyrights @ 2022 EC-Council International Ltd.

10. Scroll down to Attach permissions policies. In the Attach permissions policies section, search for IAMUserChangePassword. The match record gets filtered. Check IAMUserChangePassword.



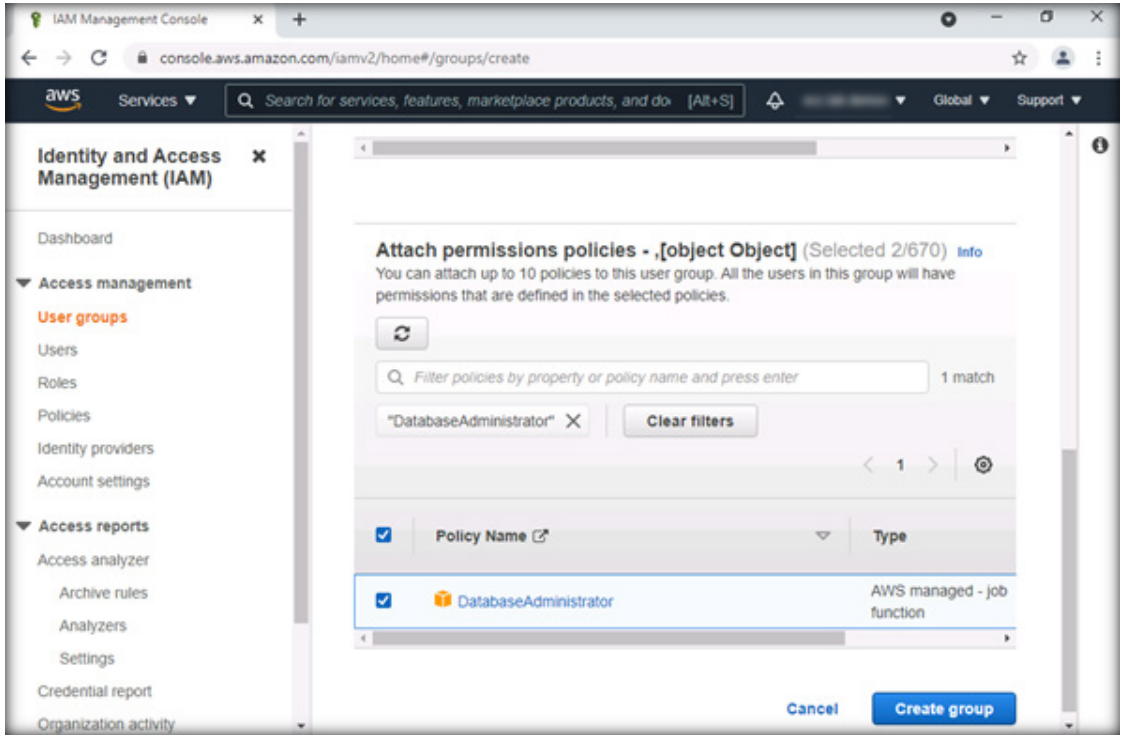
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



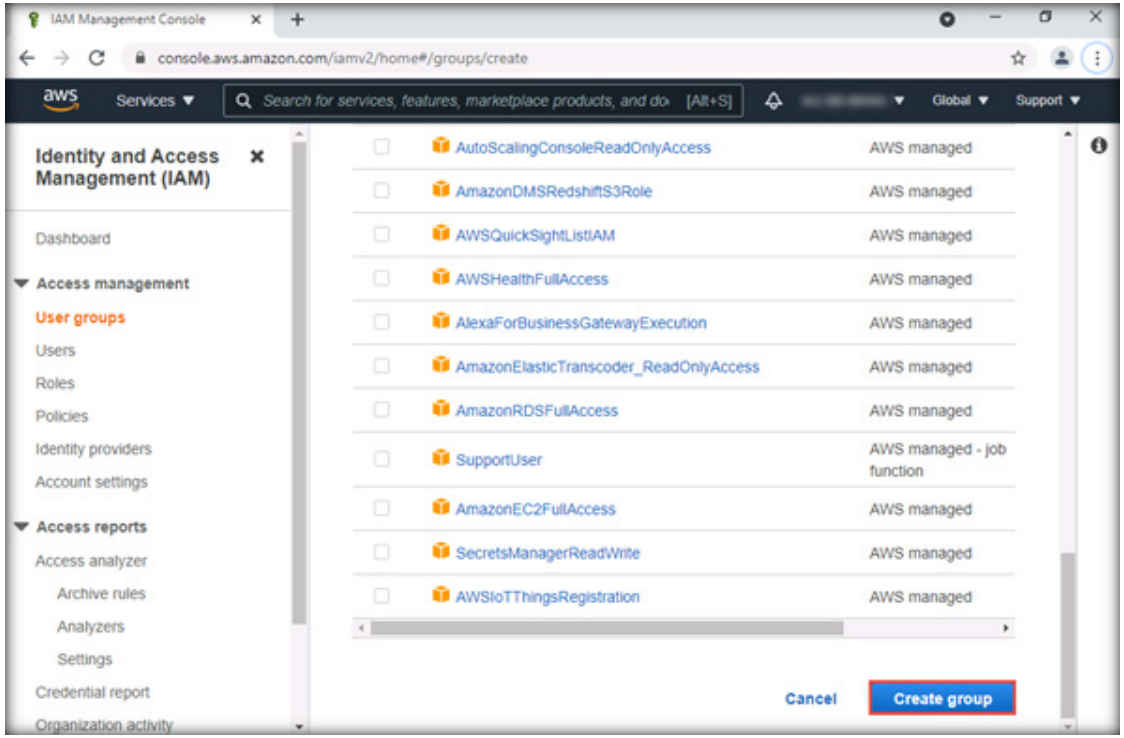
Copyrights @ 2022 EC-Council International Ltd.

11. Next, clear the filter and search for DatabaseAdministrator. The match record gets filtered. Check DatabaseAdministrator.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

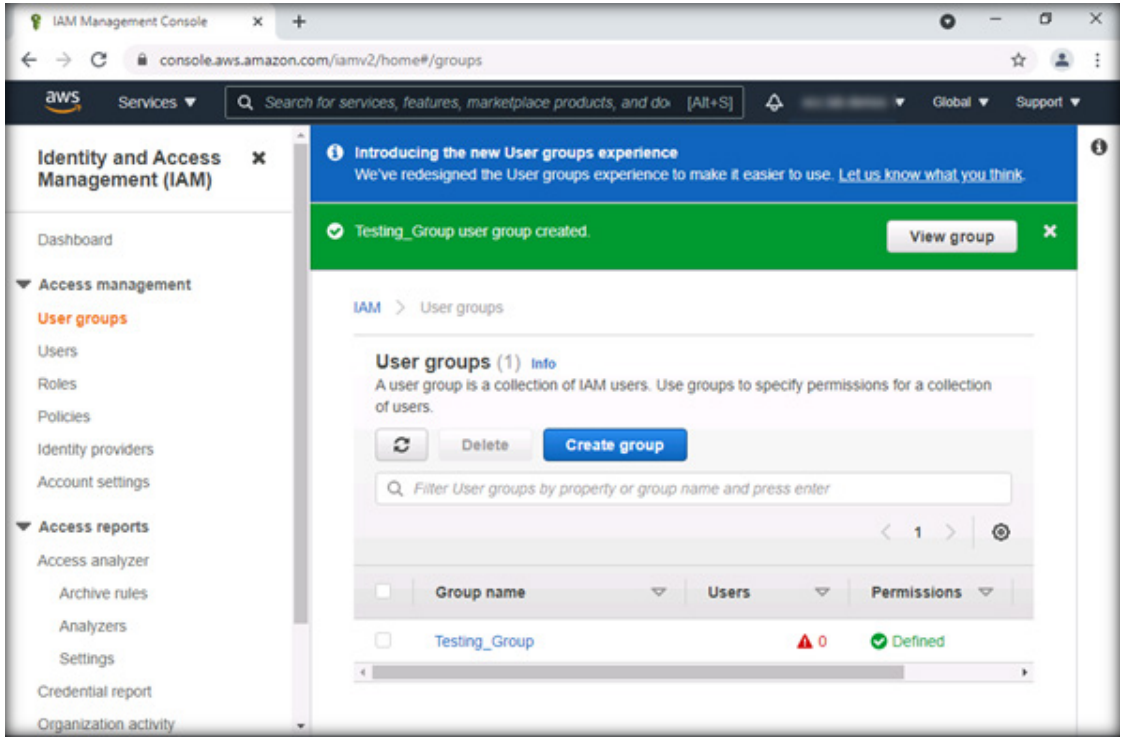
12. Scroll down the page and click on Create group.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

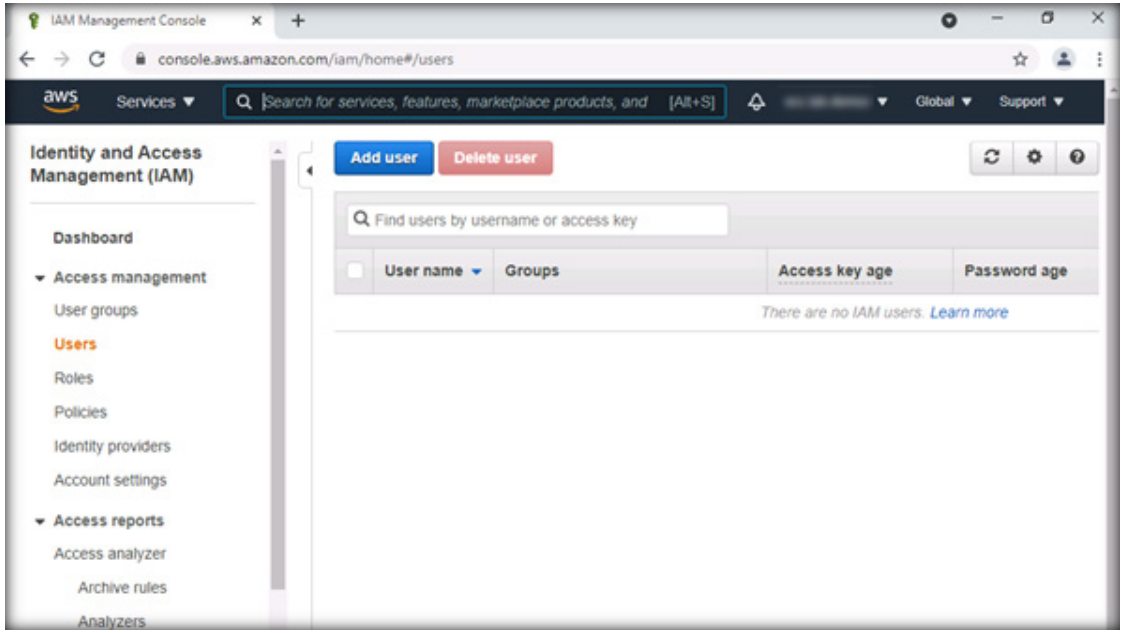
Copyrights @ 2022 EC-Council International Ltd.

13. Testing_Group will be created under Groups as shown in the screenshot below.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

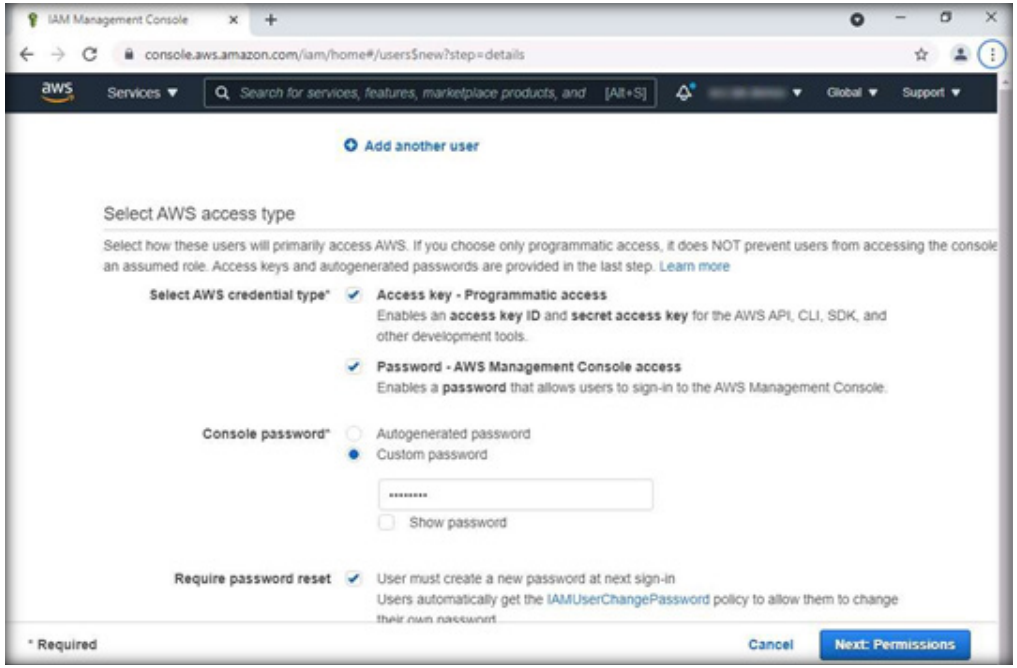
14. Select Users from the Identity and Access Management (IAM) section, and click on Add user to create a new user.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

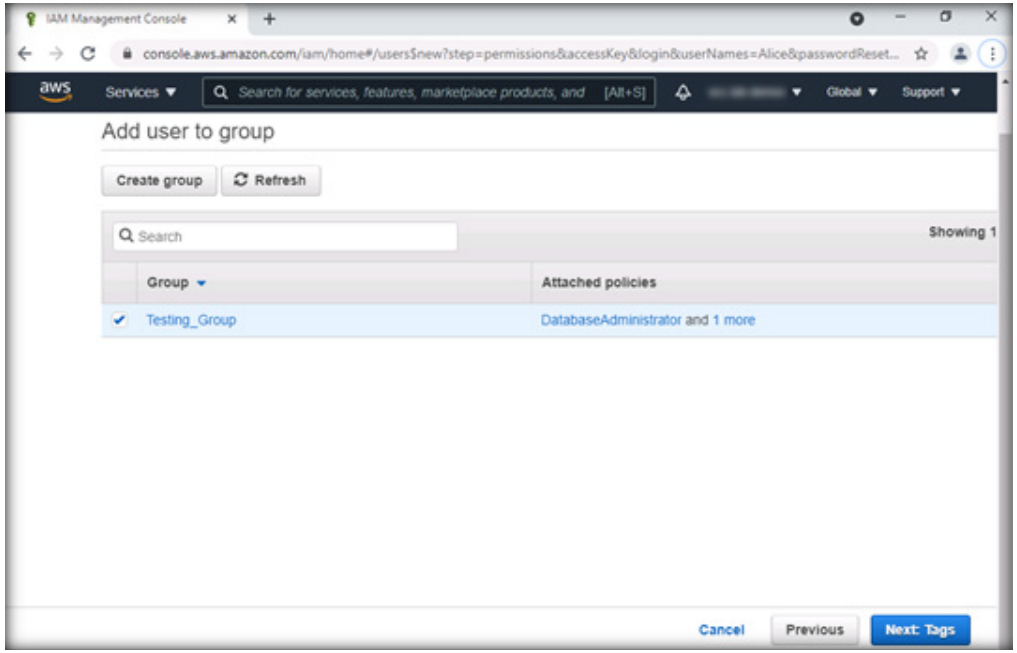
15. The Add user page appears. In the User name field, provide any name (here, the username is Alice).

16. Under Select AWS access type, check Access key - Programmatic access and Password - AWS Management Console access. Choose the Custom password radio button and type the password in the password field (here, we use User@123). Require password reset is optional; however, check this setting. Next, click on Next: Permissions.



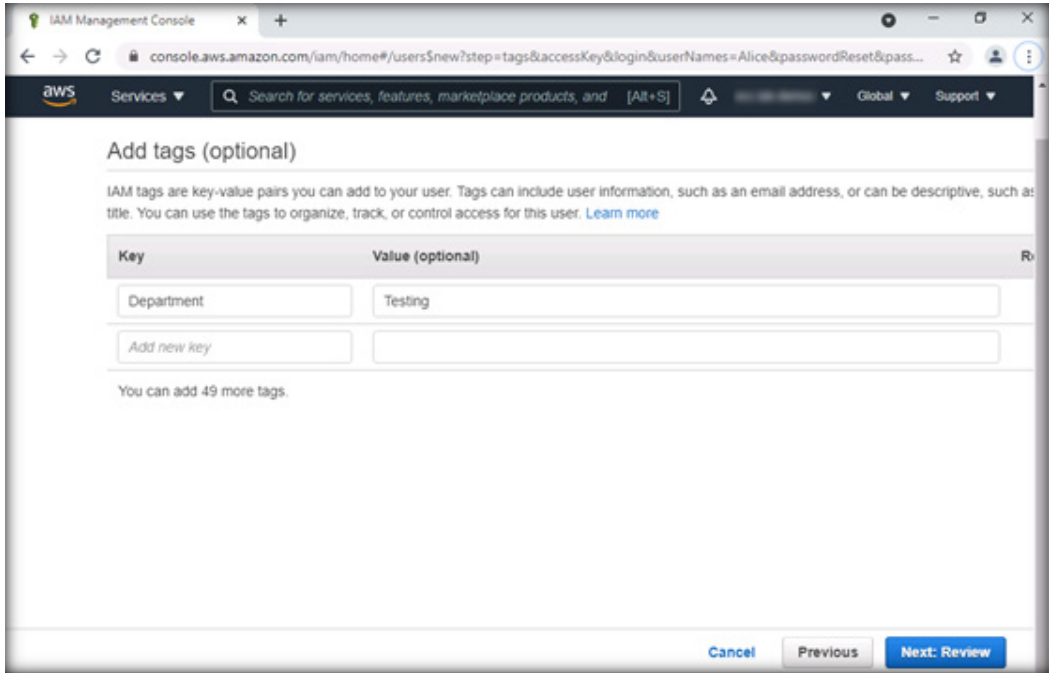
EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

17. In the Set permissions section, the Add user to group is selected, by default. Check the newly created group (here, the group is Testing_ Group). We have now added the user to the group. Click on Next: Tags.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

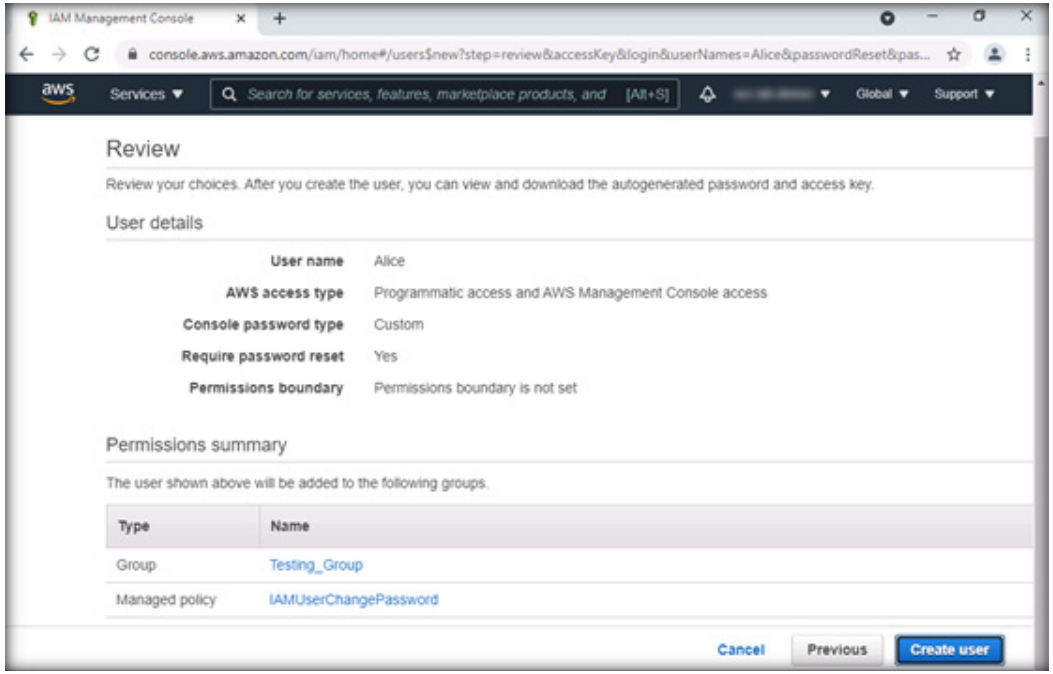
18. Tags are optional; however, tagging will help us search for Tag keys easily later. Type Department in the field under Key and Testing under Value (optional). Click on Next: Review to proceed to reviewing IAM User creation.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

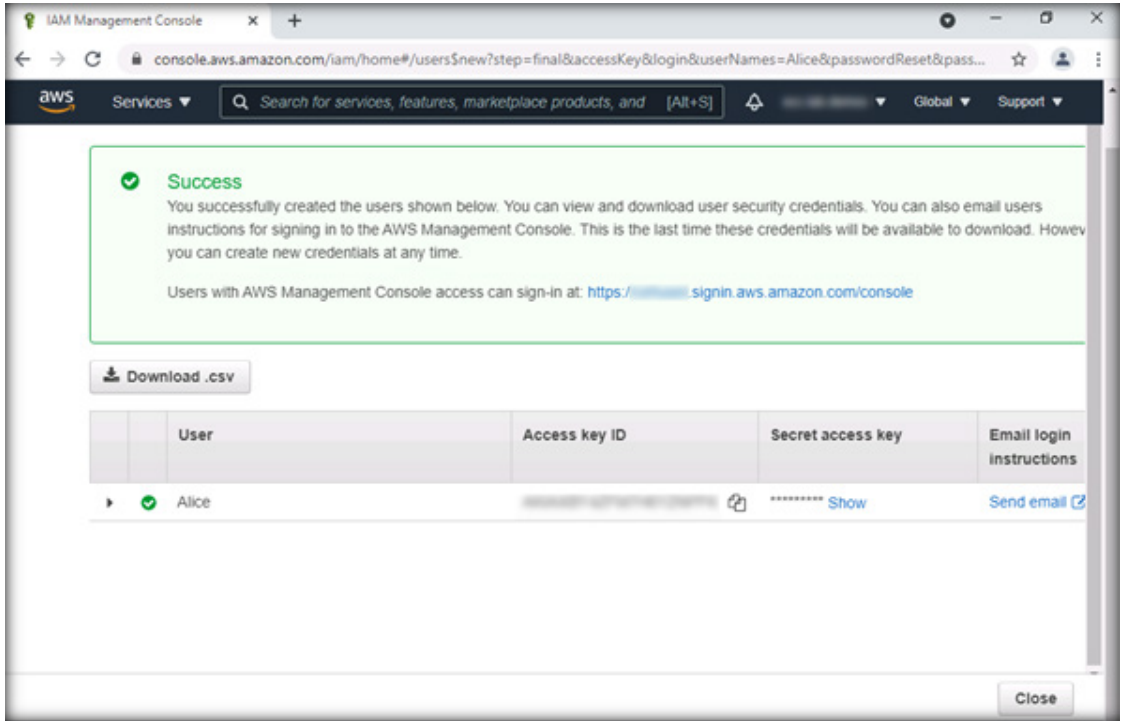
19. On the Review page, we will be able to view the settings and IAM User properties before creating the user. Once you have verified the settings, click on Create user.



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

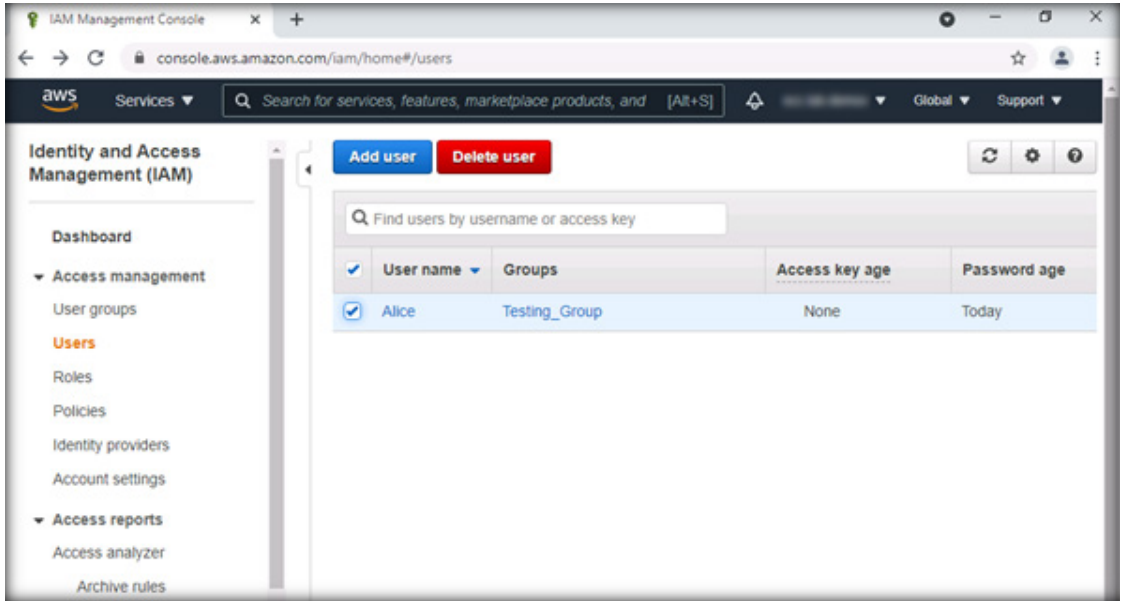
Copyrights @ 2022 EC-Council International Ltd.

20. After you click on Create user, a Success message is displayed. You have an option to Send Email to get the login instructions for the newly created IAM User. Click on Close (lower right corner of the page) to return to the IAM page. It will redirect you to the Users page.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

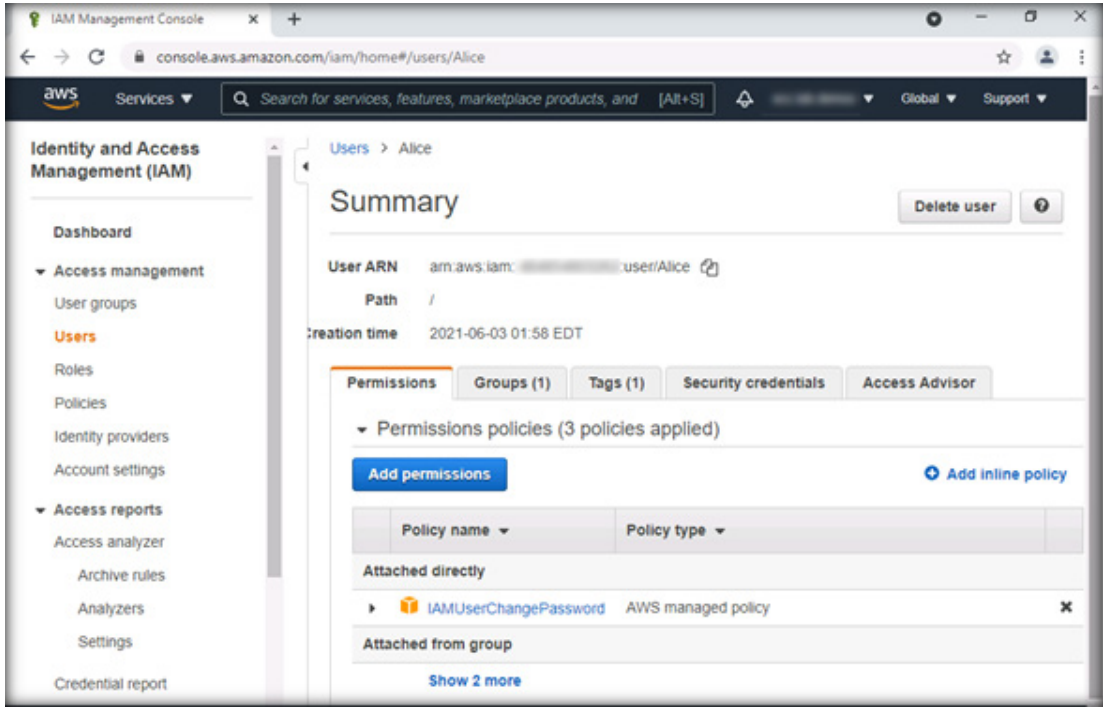
21. Next, let us attach a policy to the user. Select the user for whom you want to add a policy and click the user name. In this instance, let us select Alice as shown in the screenshot below.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

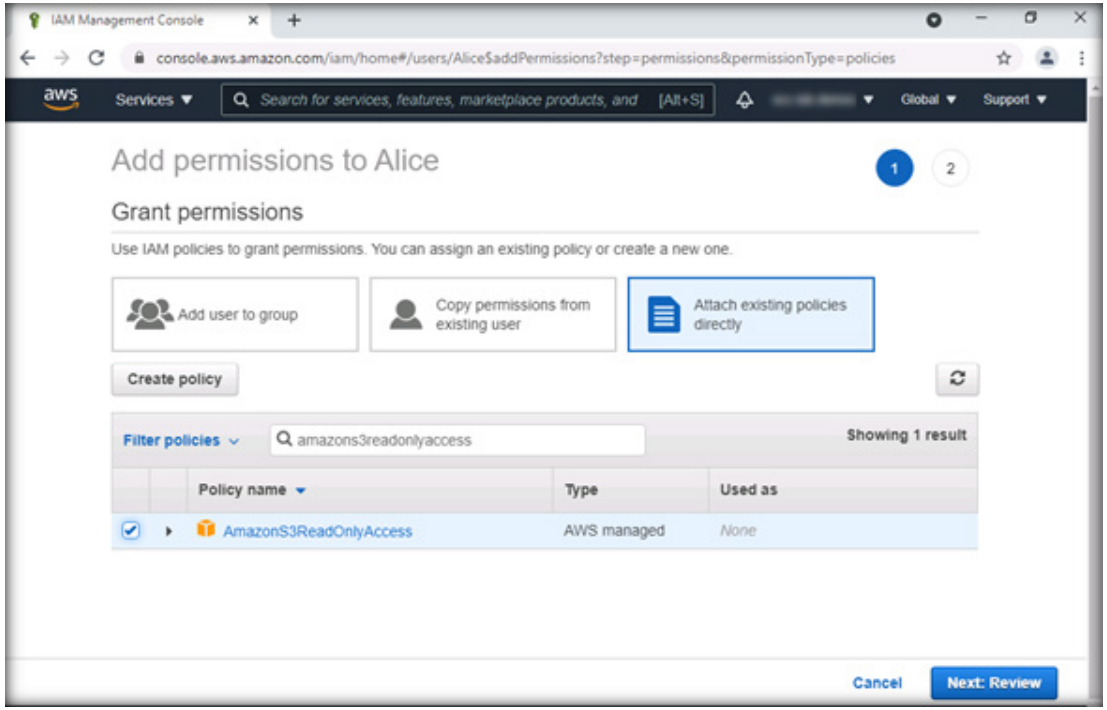
22. The Summary page appears (here, it appears for Alice). Click on Add permissions.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

23. In the Grant permissions page, click on Attach existing policies directly.

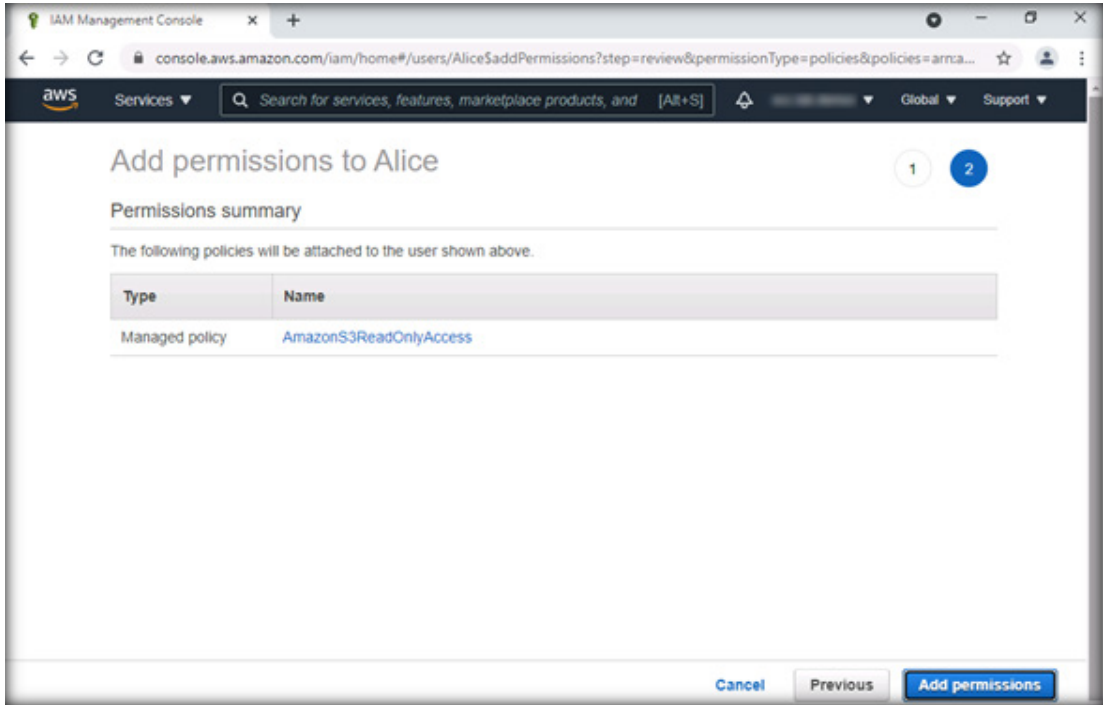
24. In the Filter policies field, search for amazons3readonlyaccess. This will display all pre-configured policies for S3. Select AmazonS3ReadOnlyAccess, and click on Next: Review.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

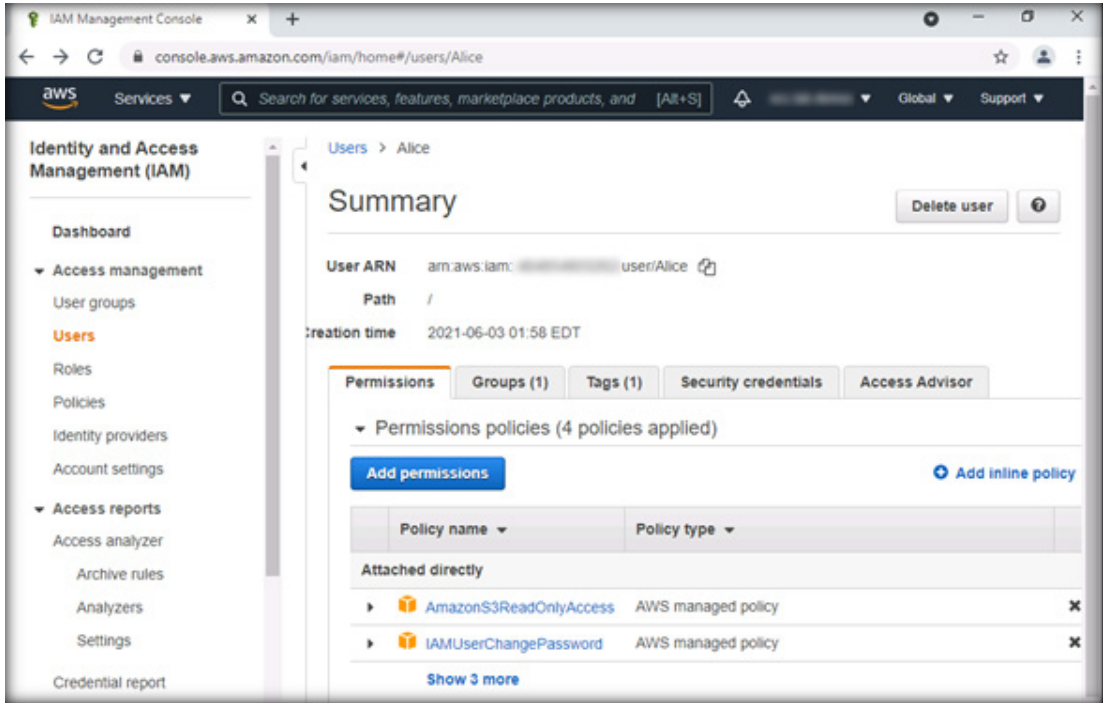
25. In the Permissions summary page, review the assigned policies to the IAM User. After you have reviewed the policies, click on Add permissions.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

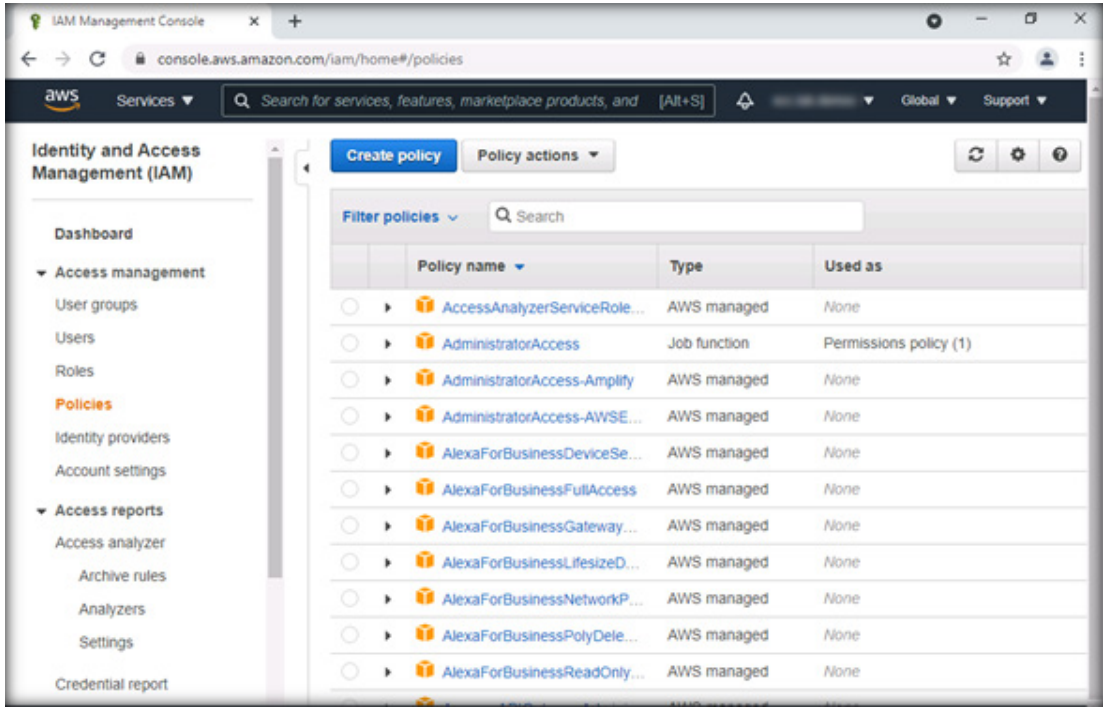
Copyrights @ 2022 EC-Council International Ltd.

26. The policy that was assigned will be displayed once you view the IAM User (here, Alice). The policy is displayed under Attached directly.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

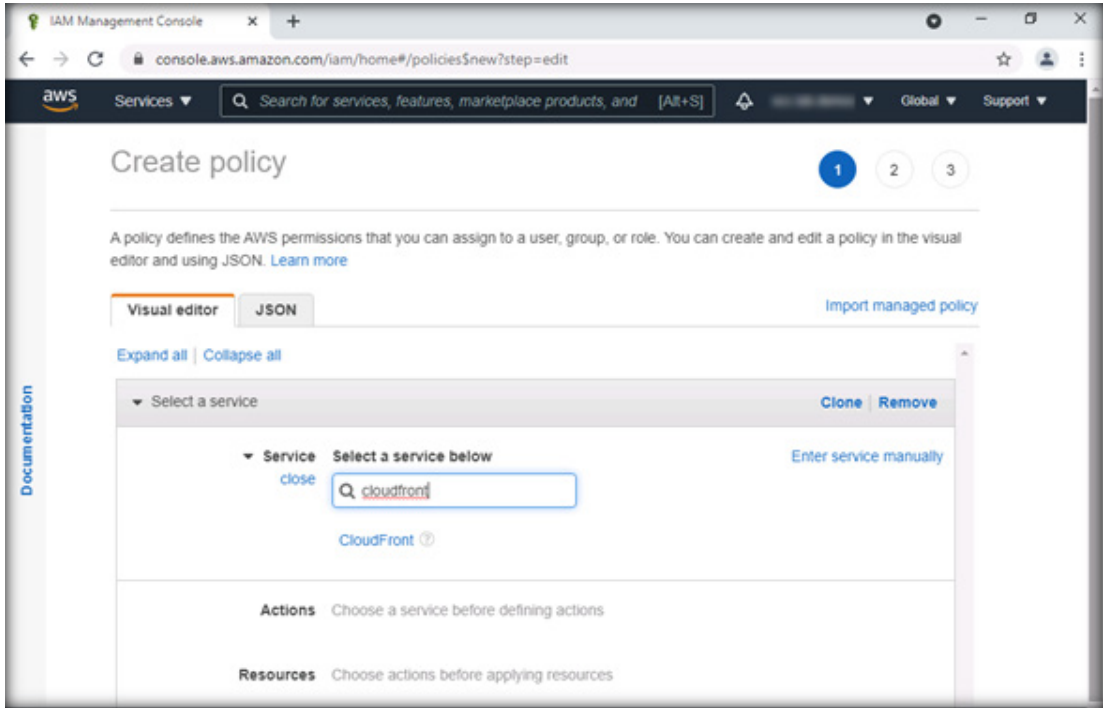
27. Next, we will create a custom IAM policy. Click on Policies under the Identity and Access Management (IAM) console. Click on Create policy.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

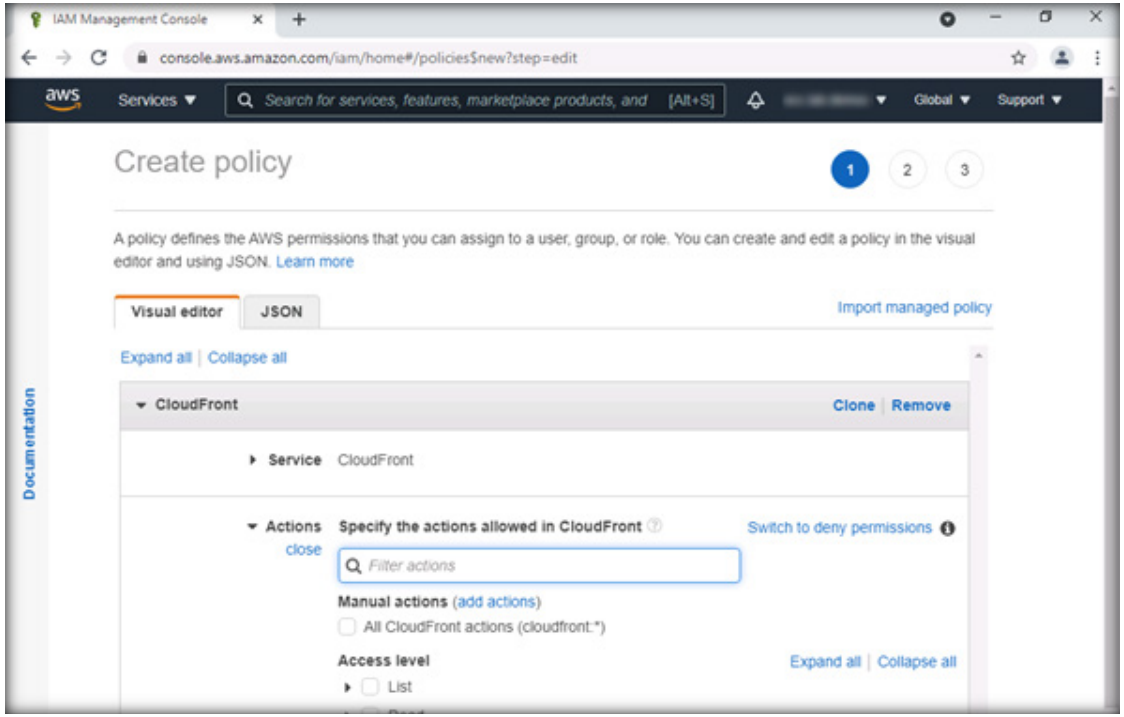
Copyrights @ 2022 EC-Council International Ltd.

28. Click the link Choose a service, specify the service that you wish to use and edit the permissions. In this example, let us use CloudFront on Service.



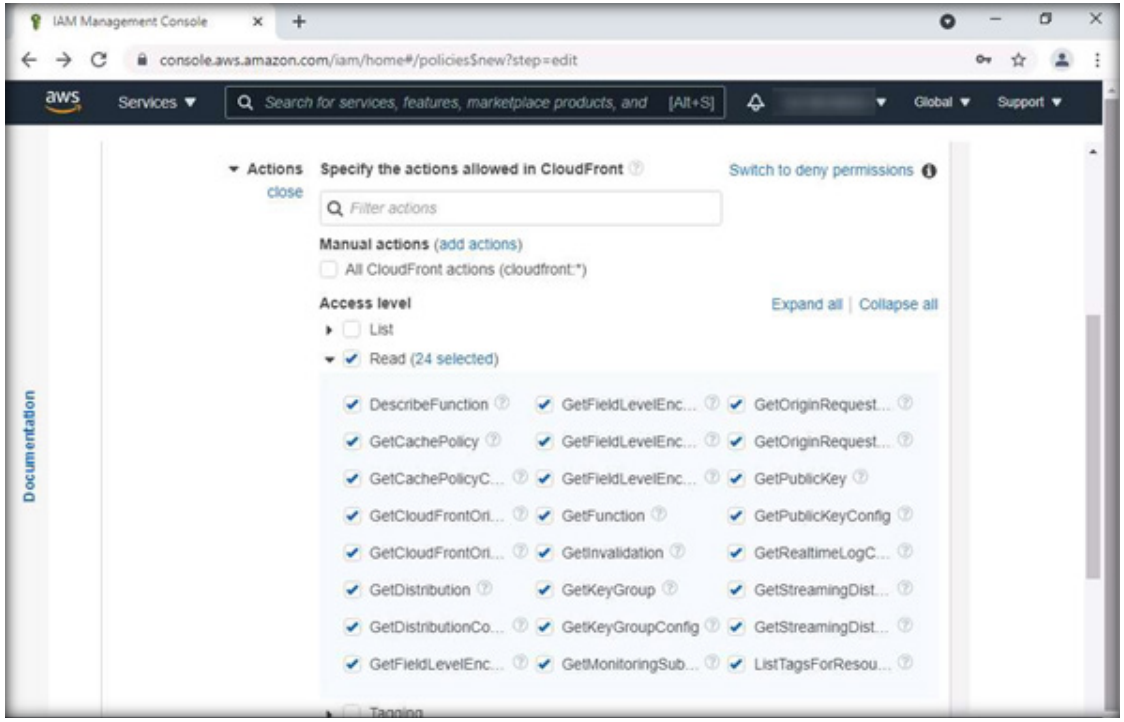
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



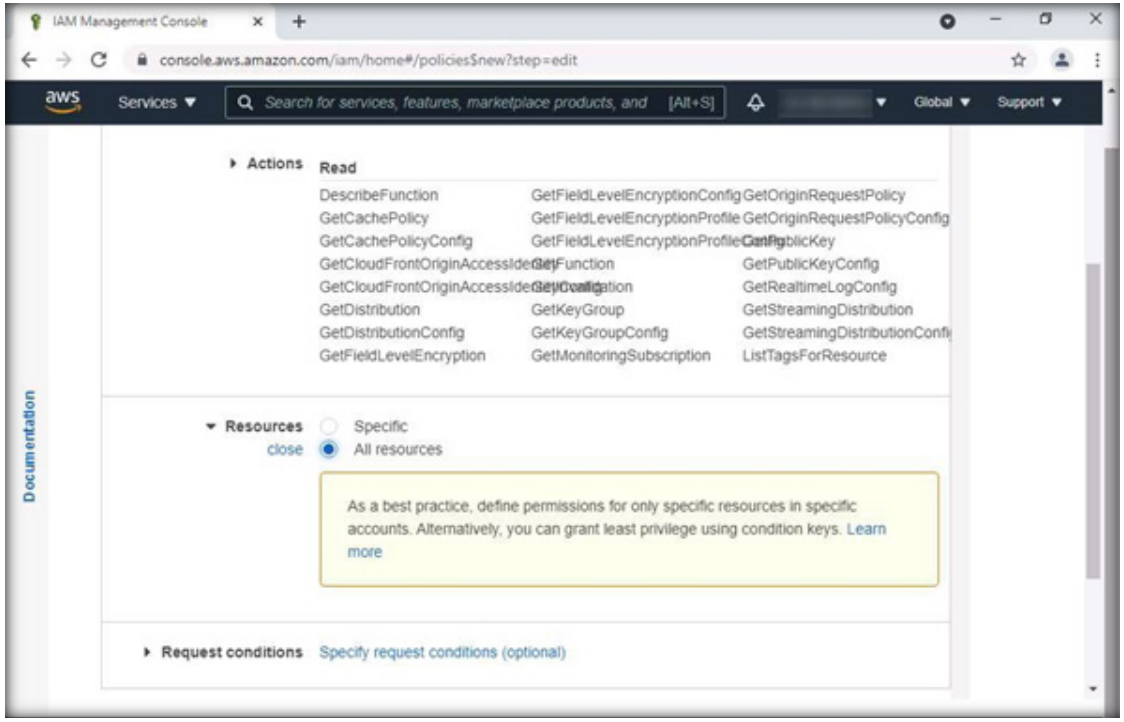
Copyrights @ 2022 EC-Council International Ltd.

29. Expand the Actions menu to select the Access level for CloudFront service. In this example, let us enable only Read access for CloudFront.
Note: The number of Read access policies might vary in your lab environment.



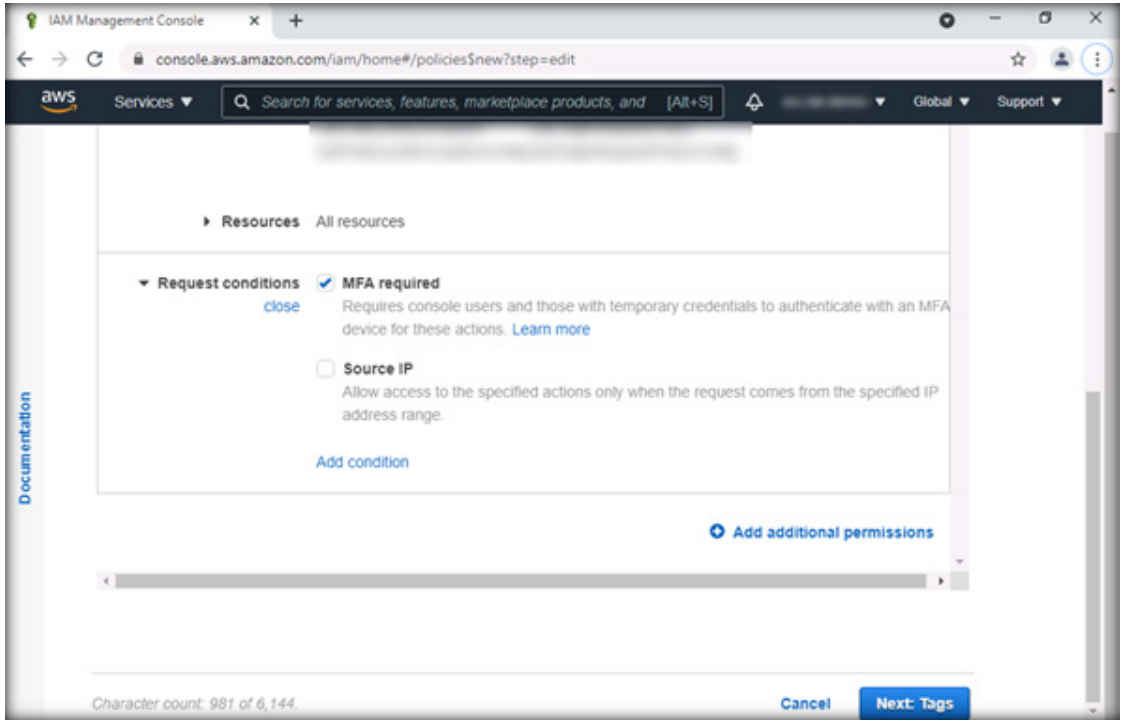
EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

30. Scroll down and expand the Resources section. Select All resources radio button.



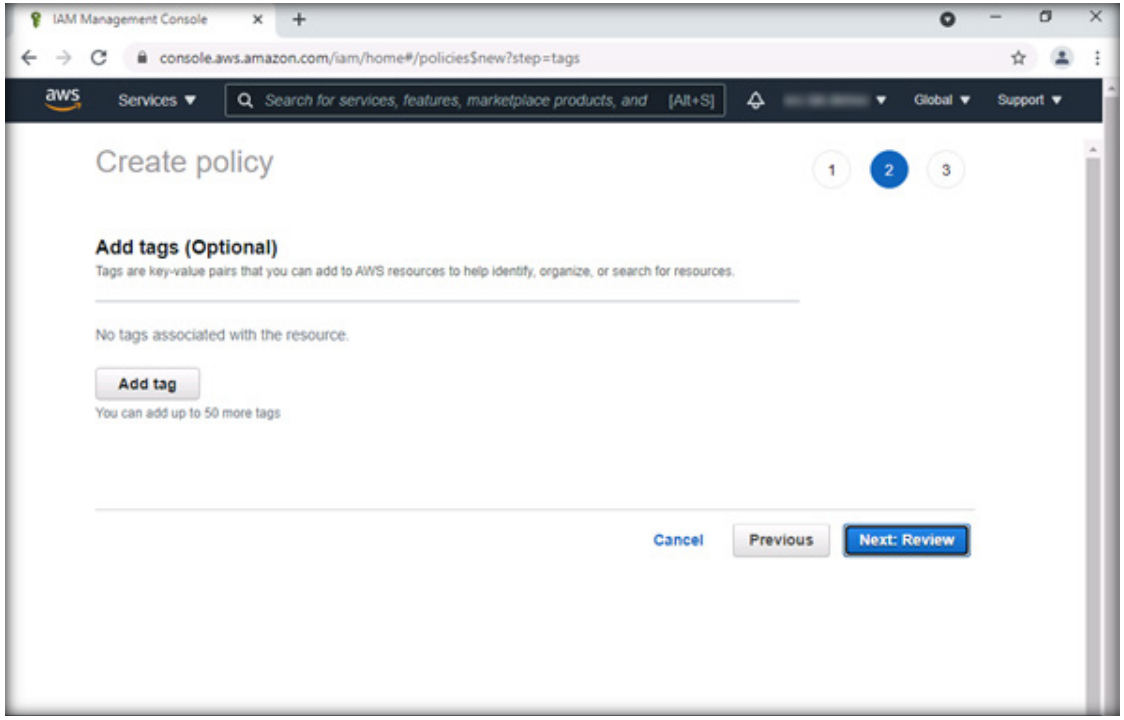
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

31. Expand Request conditions. Check MFA required, and click on Next: Tags.



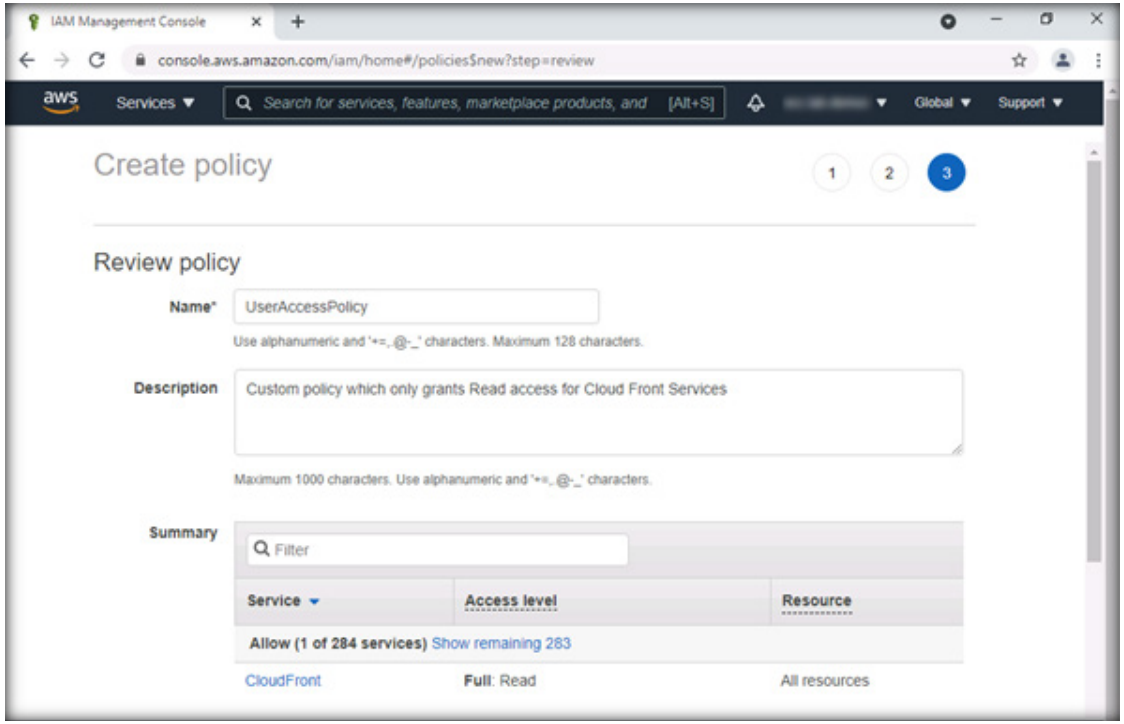
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

32. In the Add tags section click on Next: Review.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

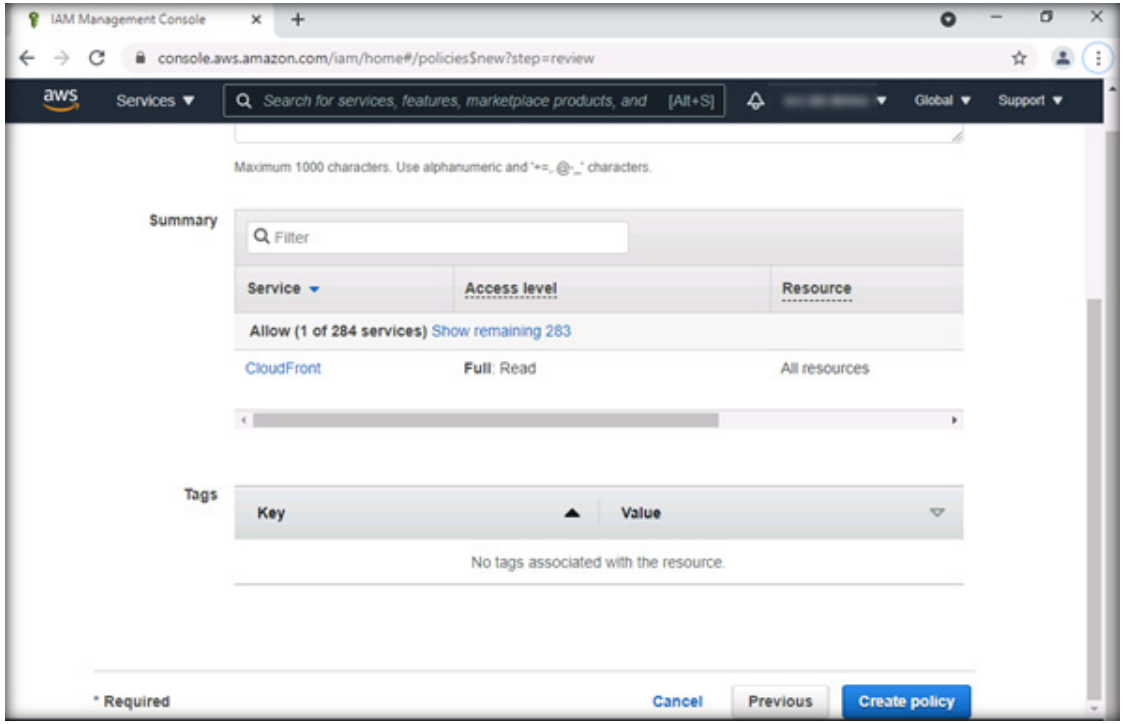
33. In the Review policy section, provide a name for the policy in the Name field and add a description in the Description field.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

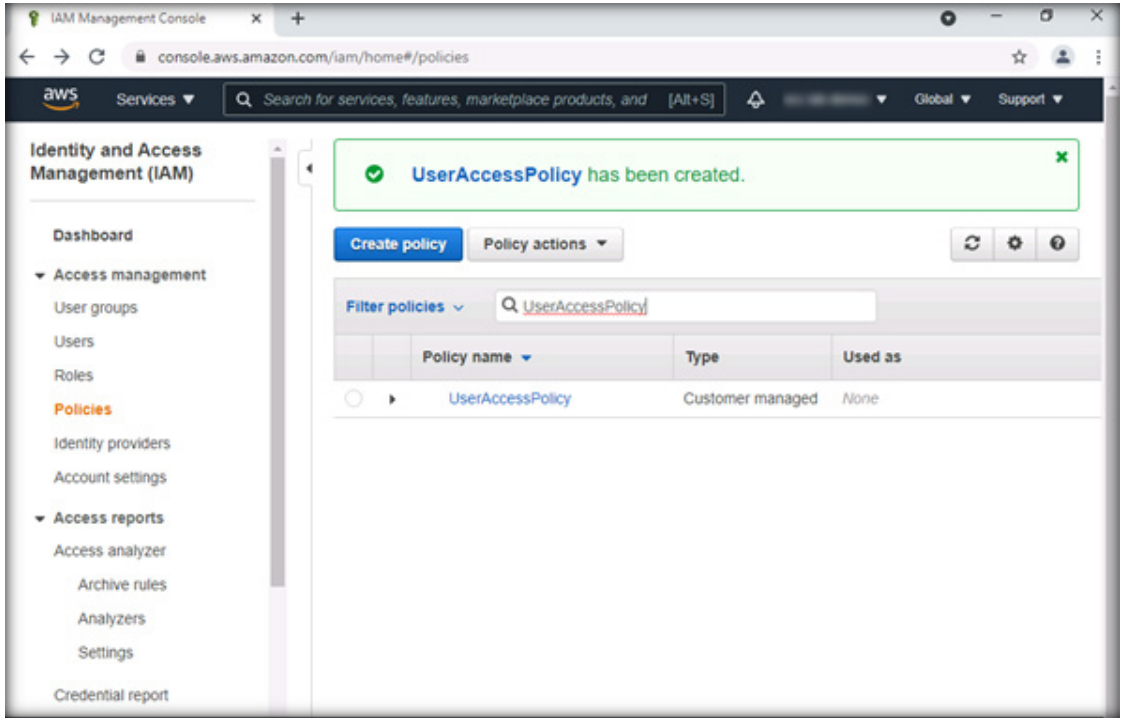
34. Scroll down and click on Create policy.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

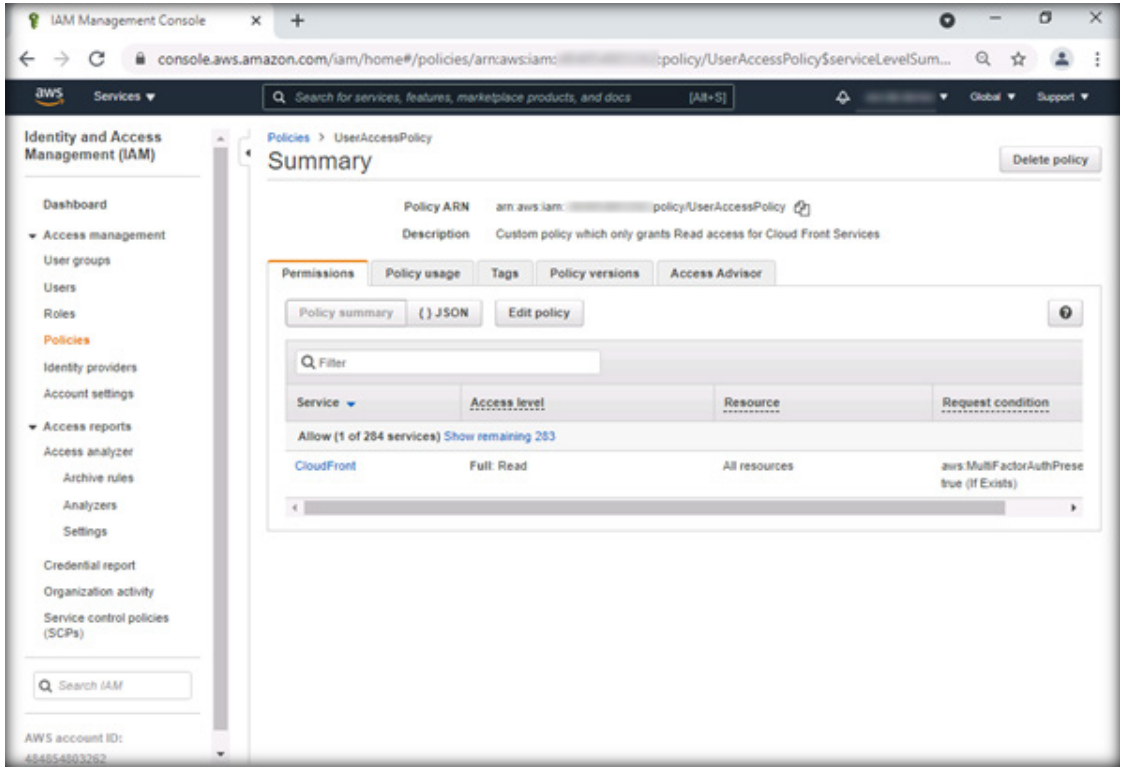
35. The new policy will be successfully created. To check the created policy, click on Policies, type the name of the policy in the search box of Filter policies, then click on the selected policy.



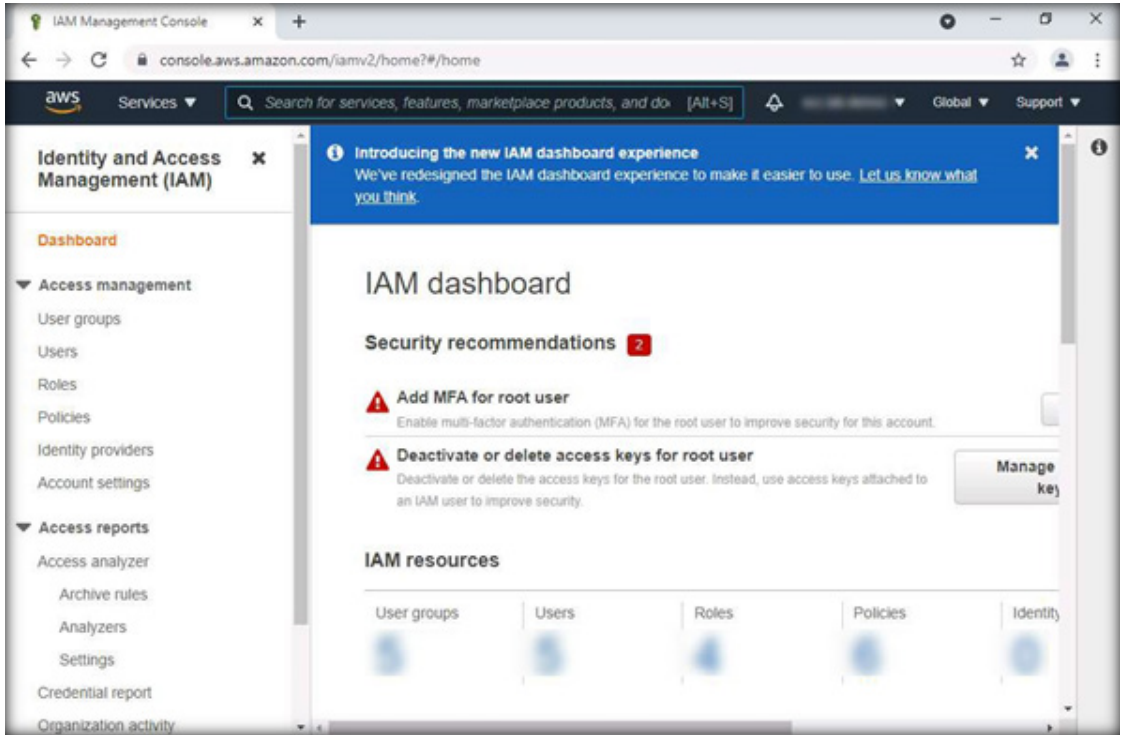
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

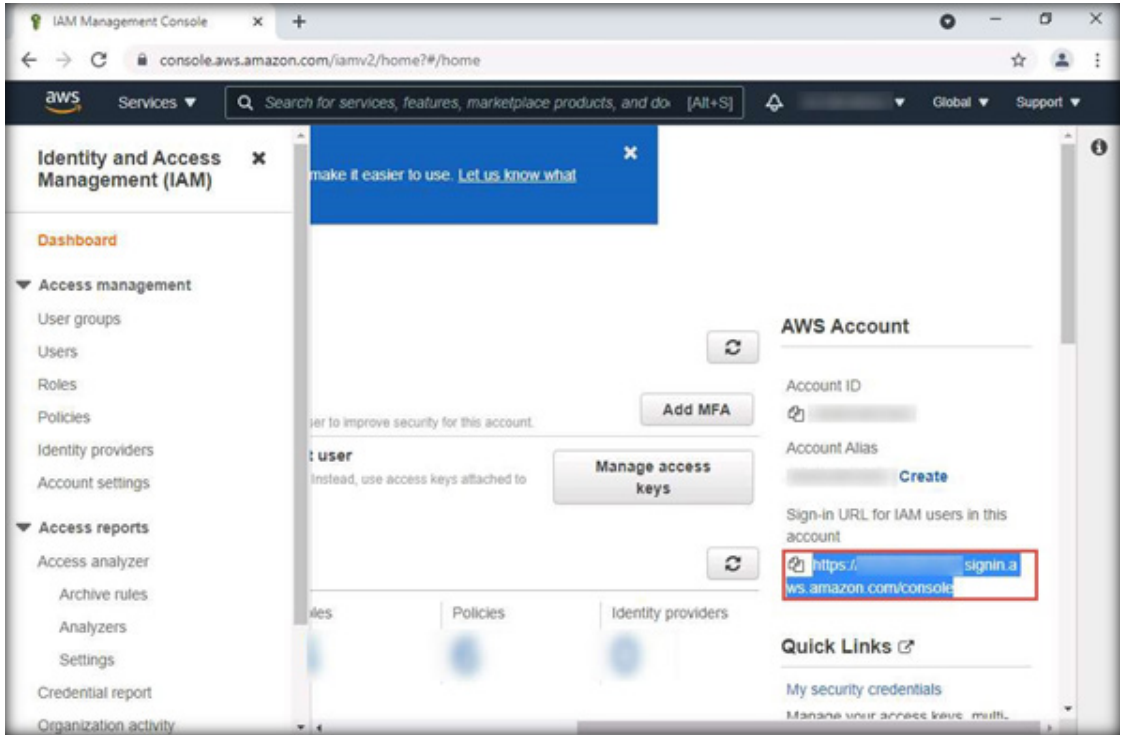


36. Click on the Dashboard under the Identity and Access Management (IAM) section.



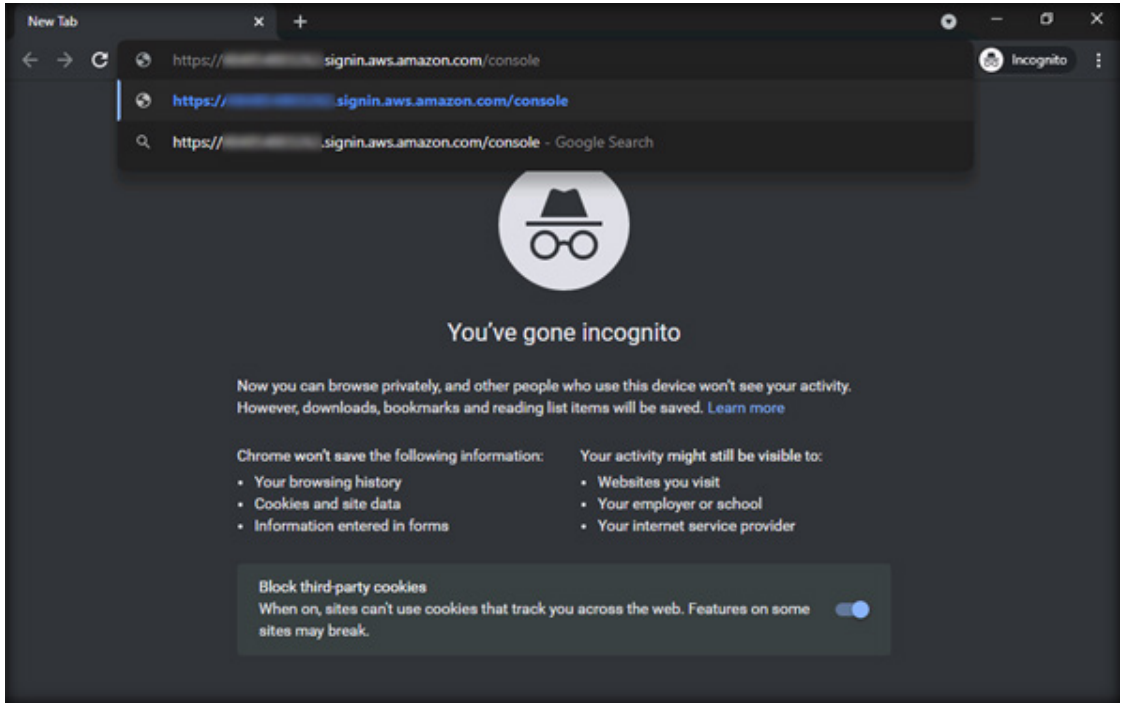
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

37. You can see the IAM users sign-in link under AWS Account, copy the link.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

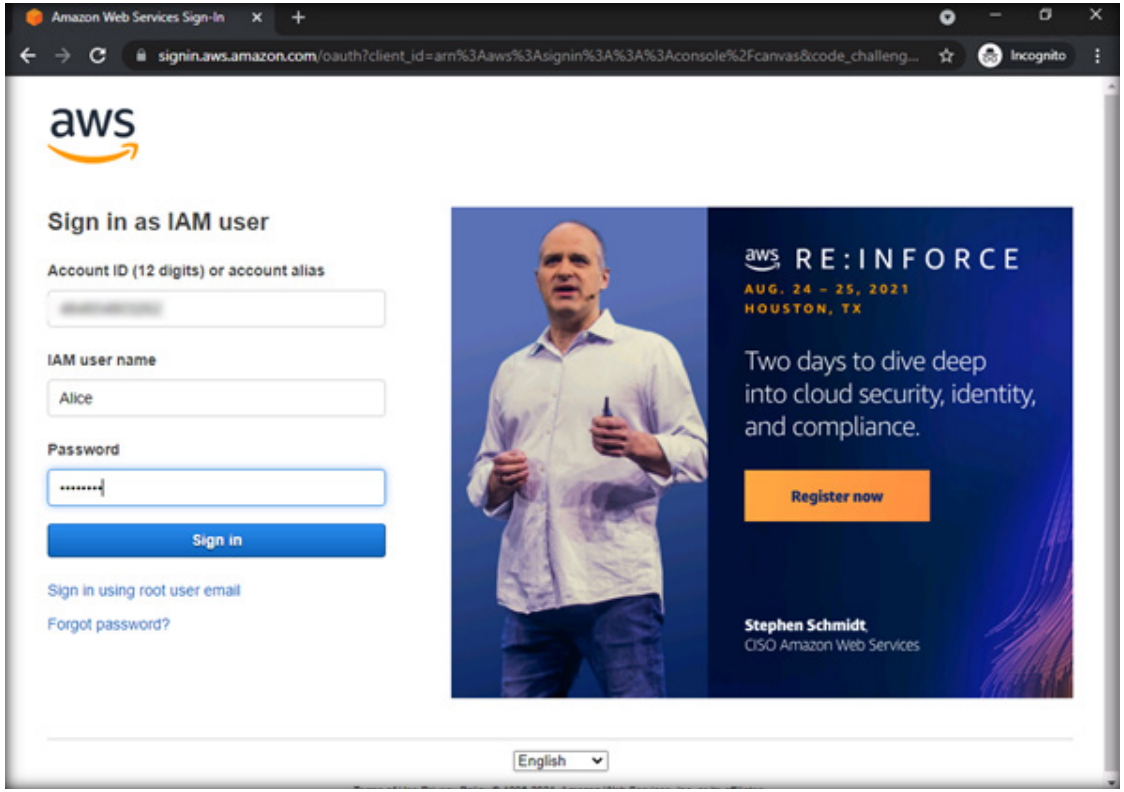
38. Open the Google Chrome browser in incognito mode, paste the copied URL, and press the Enter button.



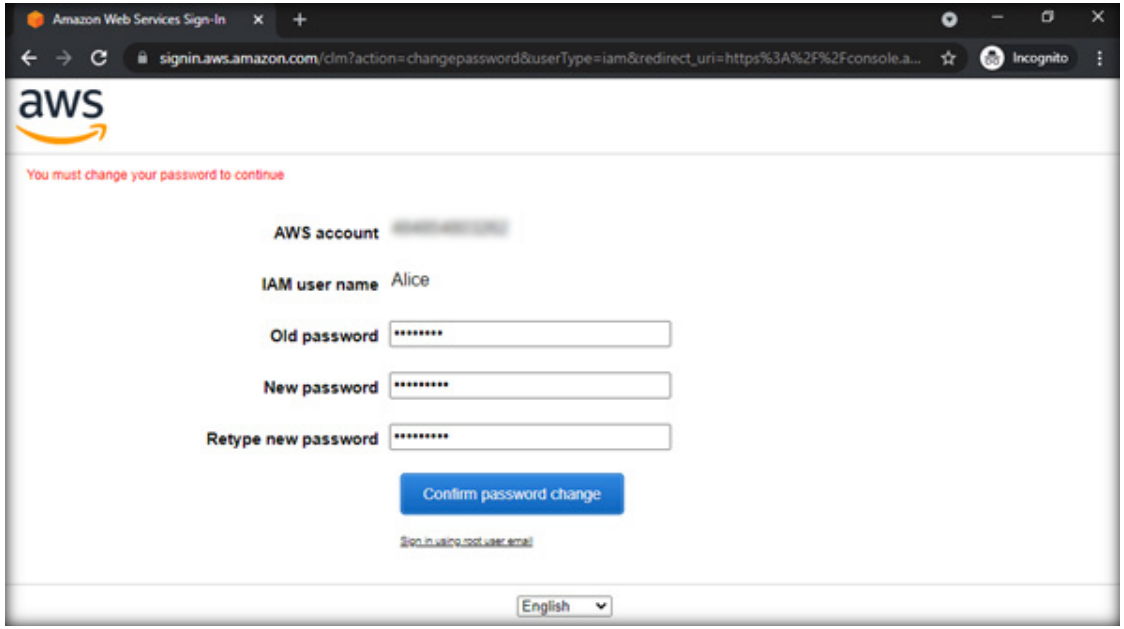
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

39. The new sign-in page appears. Type the IAM user name and Password that we created in the previous step (IAM user name: Alice and Password: User@123). Click on Sign in button.

EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

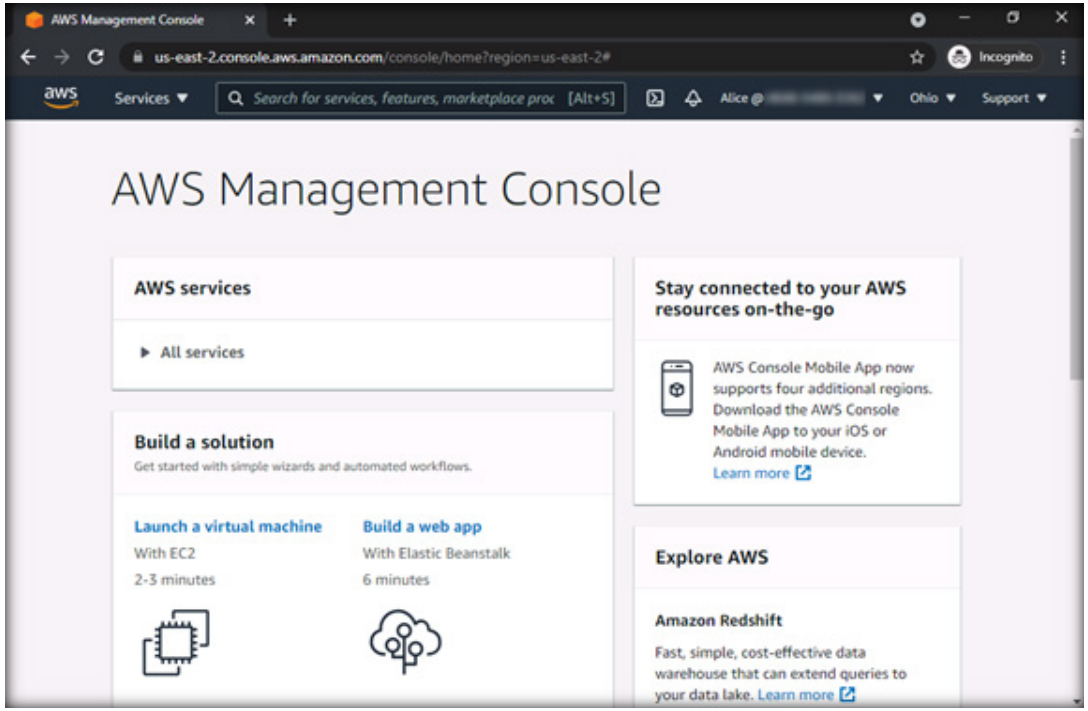


40. A new page will open wherein you can reset the password. Change the password and click on Confirm password change button.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

41. User Alice is now logged in as an IAM user.

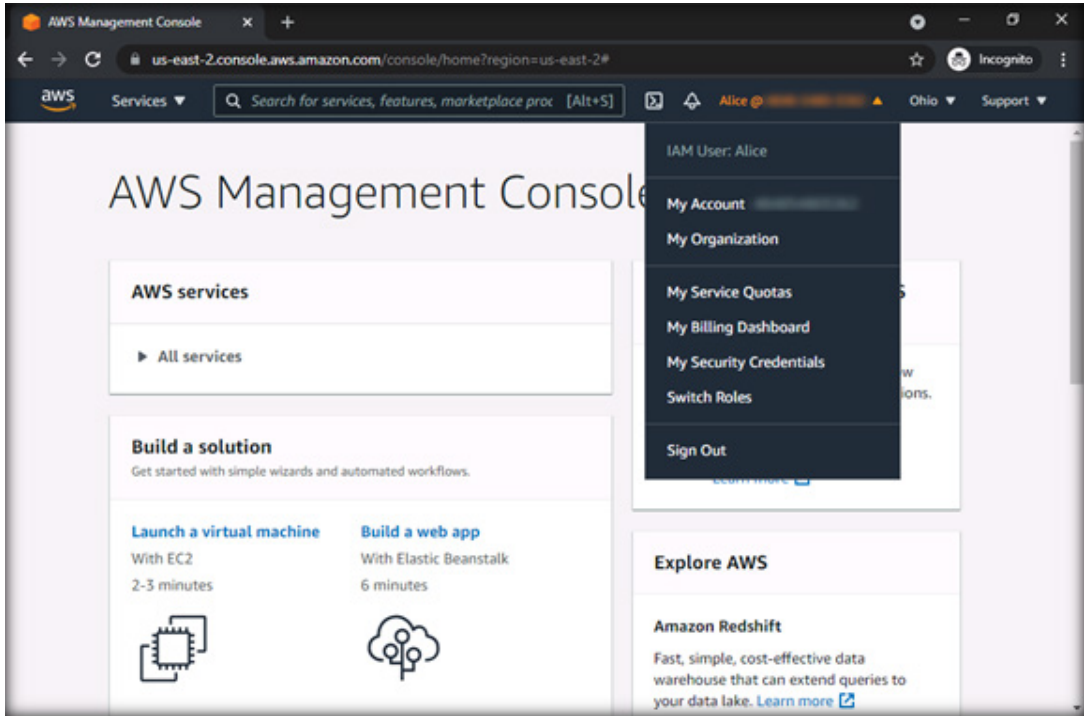


EXERCISE 3:
IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

42. We have given only Read permission to Alice who can access only limited resources.

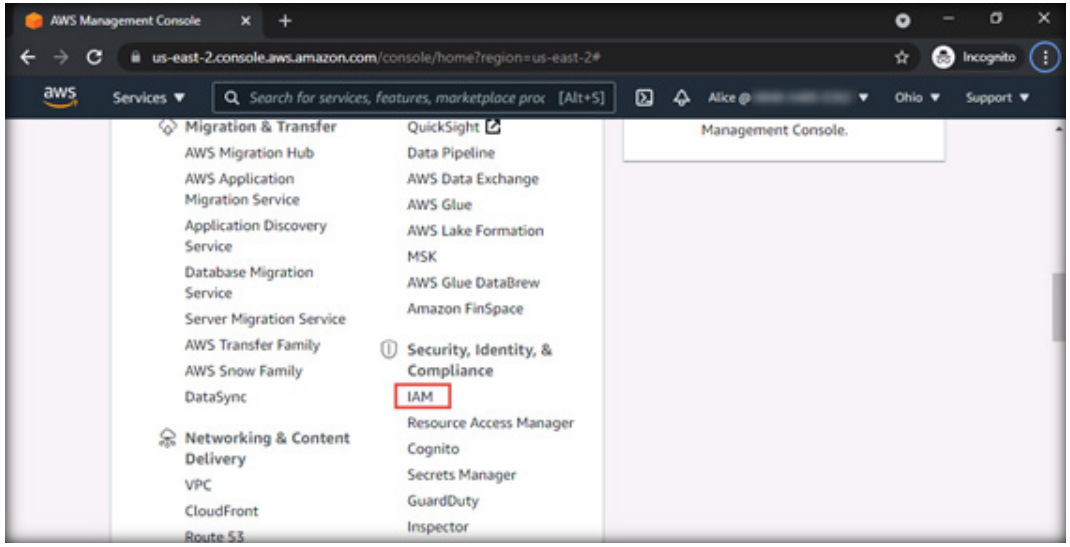
43. Click “Alice” from the upper section of the page and the drop-down menu appears. You can see that the user has been added as an IAM User.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

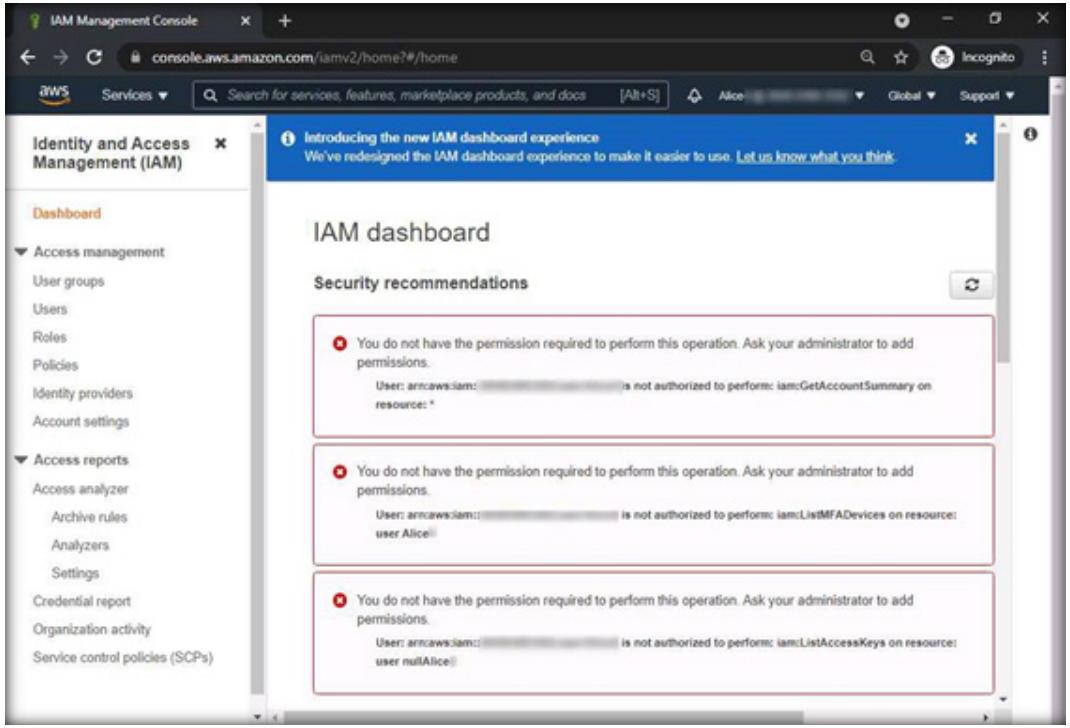
44. Next, try to access the IAM service. Expand All services under AWS services field and then select IAM under Security, Identity, & Compliance.



EXERCISE 3:
IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

Copyrights @ 2022 EC-Council International Ltd.

45. Errors appear as shown in the screenshot below. The IAM User Alice does not have permission to access IAM services.



EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

46. As described above, a security professional can create an IAM Group, Users, and custom policies in AWS.

47. Log out from the AWS platform and close all open windows.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 4: **IMPLEMENT KEY MANAGEMENT SERVICES IN AWS**

Key management involves generating, using, protecting, storing, backing up, and deleting encryption keys.

LAB SCENARIO

Security professionals follow different data security methods to protect data stored on the cloud. Generally, data are encrypted to protect its confidentiality and integrity. Securing the encryption keys from unauthorized access is a major concern for security professionals. Amazon Web Services (AWS) Key Management Service (KMS) provides a key management service for secured storing and rotating of encryption keys with strict access control. It is important for a security professional to understand AWS KMS and learn how to create and manage cryptographic keys and as well as implement the keys in AWS services and applications.

OBJECTIVE

In this lab, you will learn to do the following:

- Create KMS Master Key
- Encrypt AWS S3 using AWS KMS Master Key
- Encrypt EBS Volume using AWS KMS Mater Key
- Encrypt Amazon Redshift Using KMS Master Key

OVERVIEW OF KEY MANAGEMENT

Cloud Key management is linked with Cloud Identity and Access Management and Cloud Audit Logs for controlling and monitoring access to individual keys and their use.

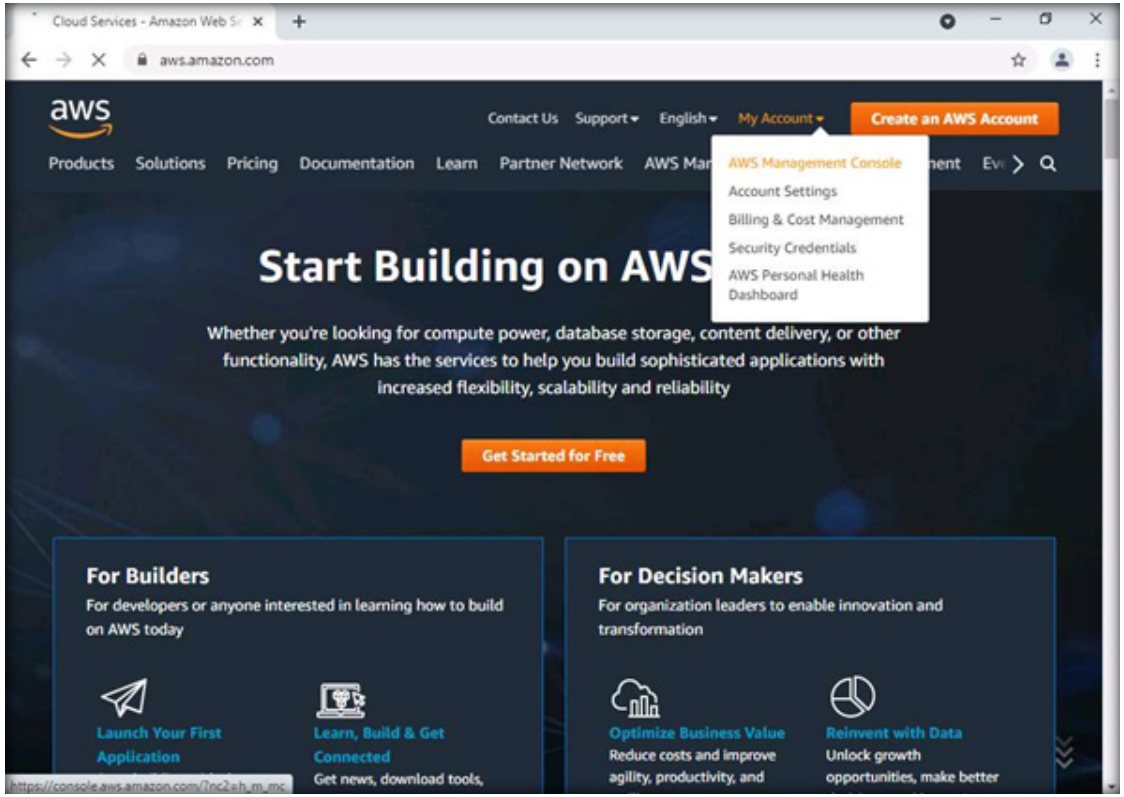
Copyrights @ 2022 EC-Council International Ltd.

Note: You need to execute Exercise 3 of this module before executing this lab as the user and group created in the previous lab are used in this lab.
Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.
1. In the Admin Machine-1 virtual machine, double-click on the Google Chrome icon on the Desktop to open the browser.

2. The Google Chrome browser opens. Go to the address bar, type https://aws.amazon.com/, and press Enter.

3. The AWS Web Services - Cloud Computing Services page appears. Click on AWS Management Console from the My Account drop-down menu as shown in the screenshot below.

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

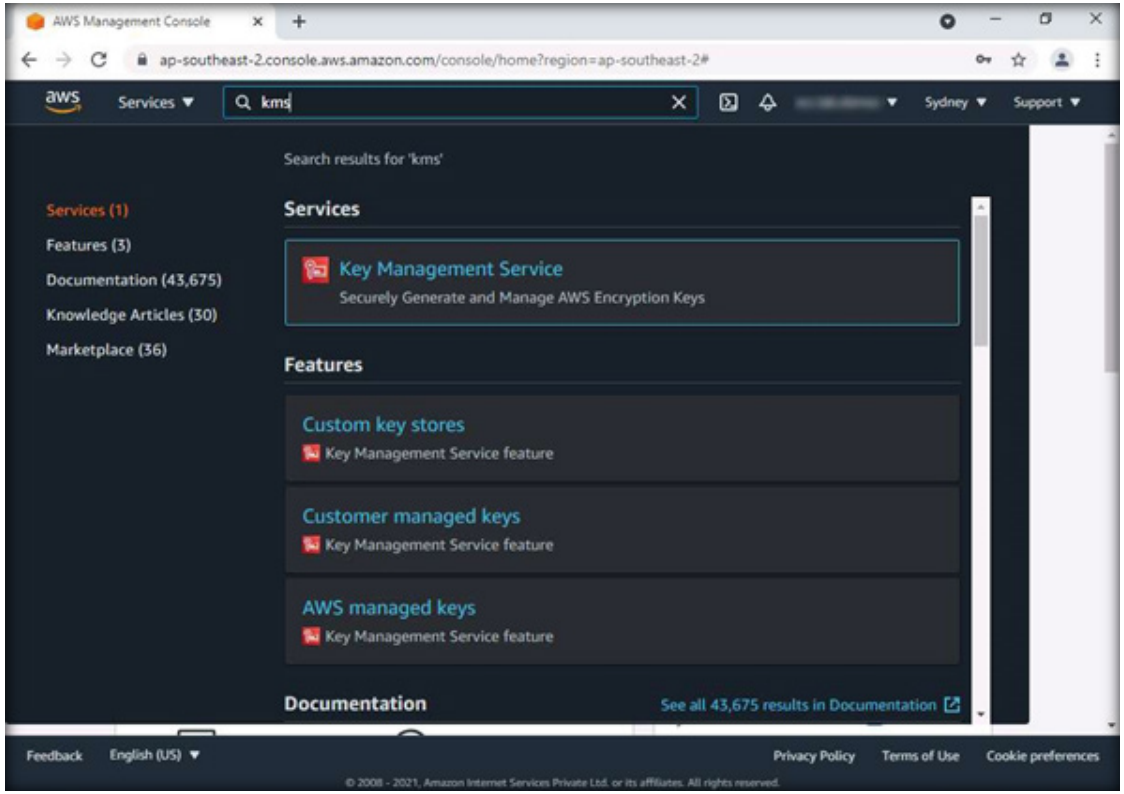


4. The AWS Web Services Sign-in page appears. Type the AWS administrator account ID, and click on Next.

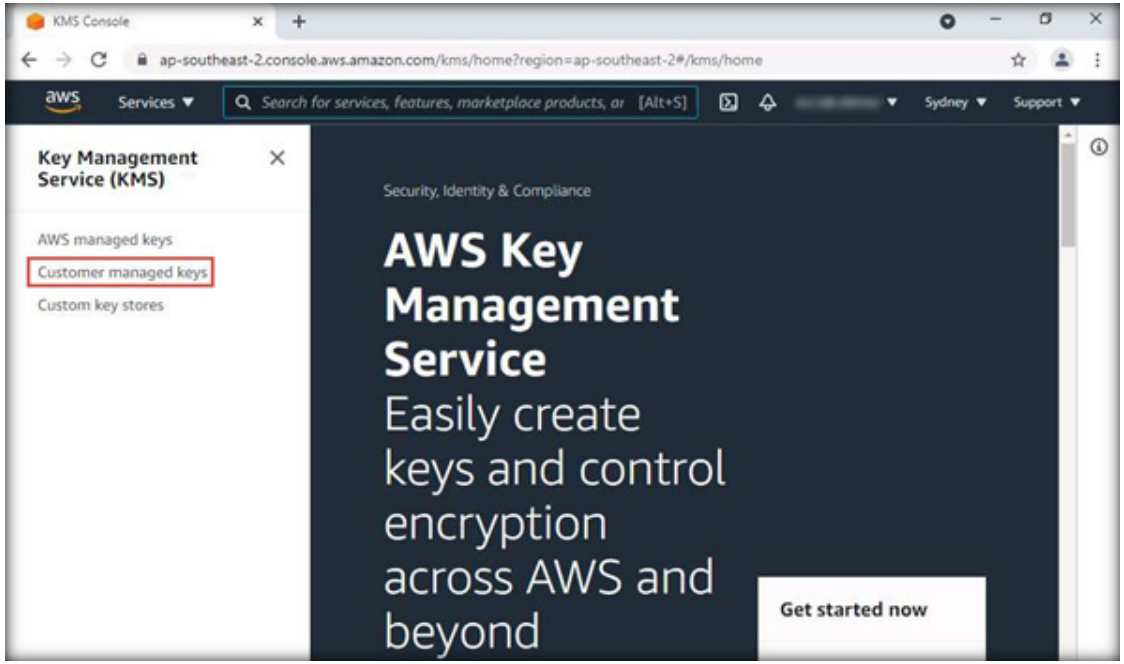
5. In the Password field, type the password, and click on Sign-in.

6. Type KMS in the Search field, and then select Key Management Service from the search result.

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

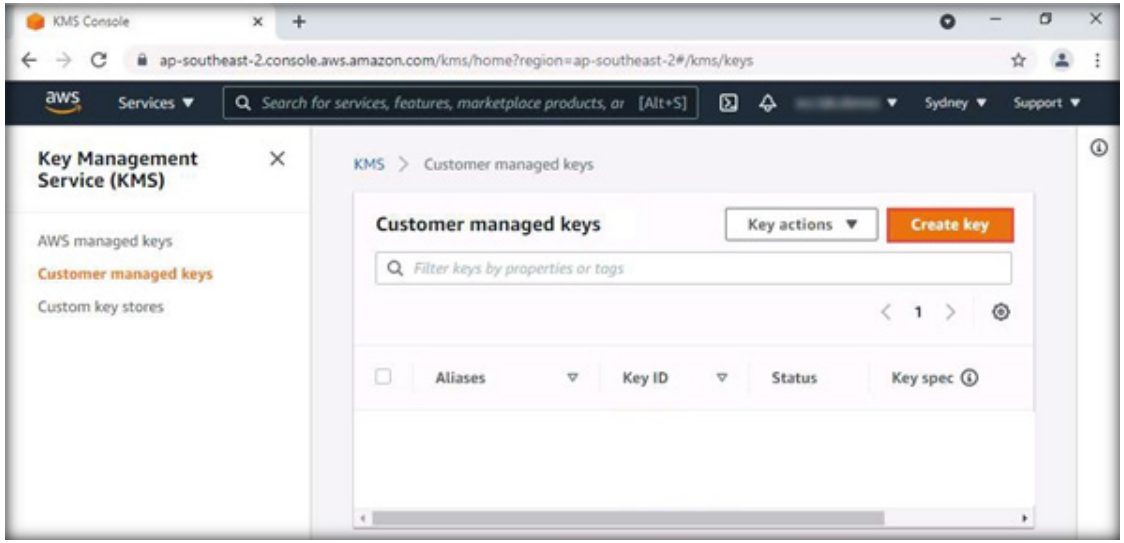


7. The KMS Console page appears. Click on Customer managed keys in the left pane.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

8. The Customer managed keys section appears. Click on Create key.



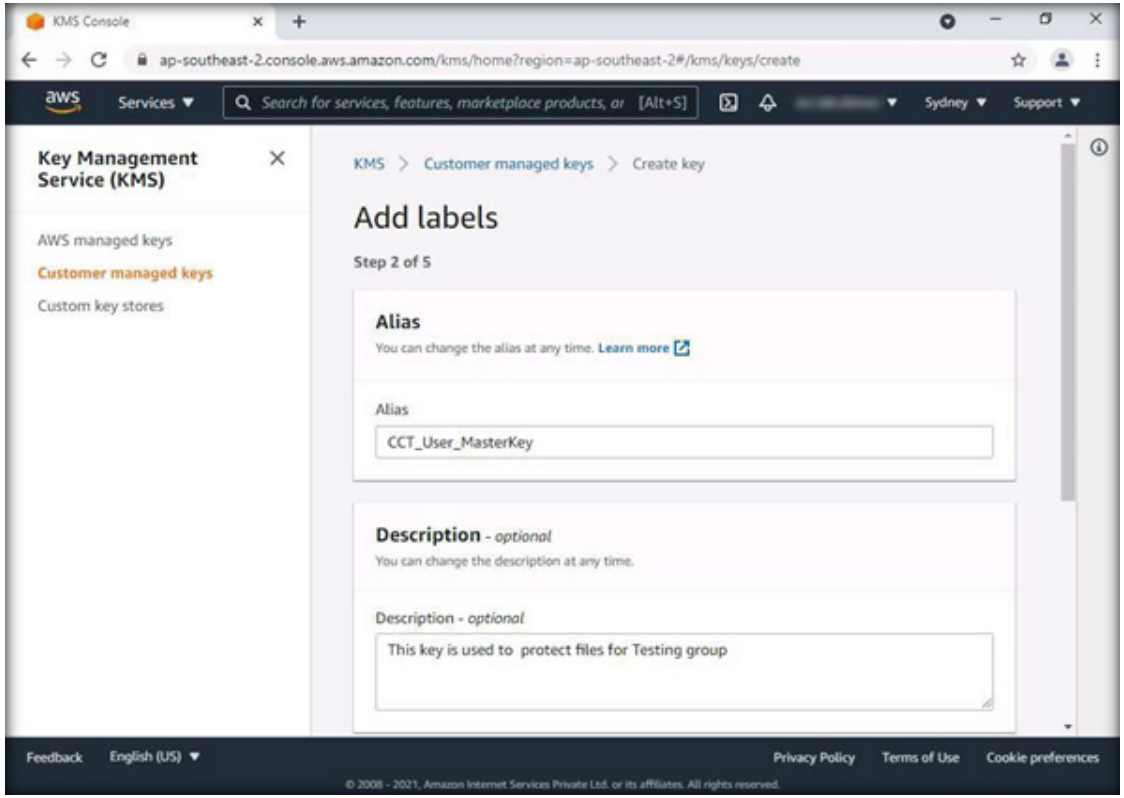
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

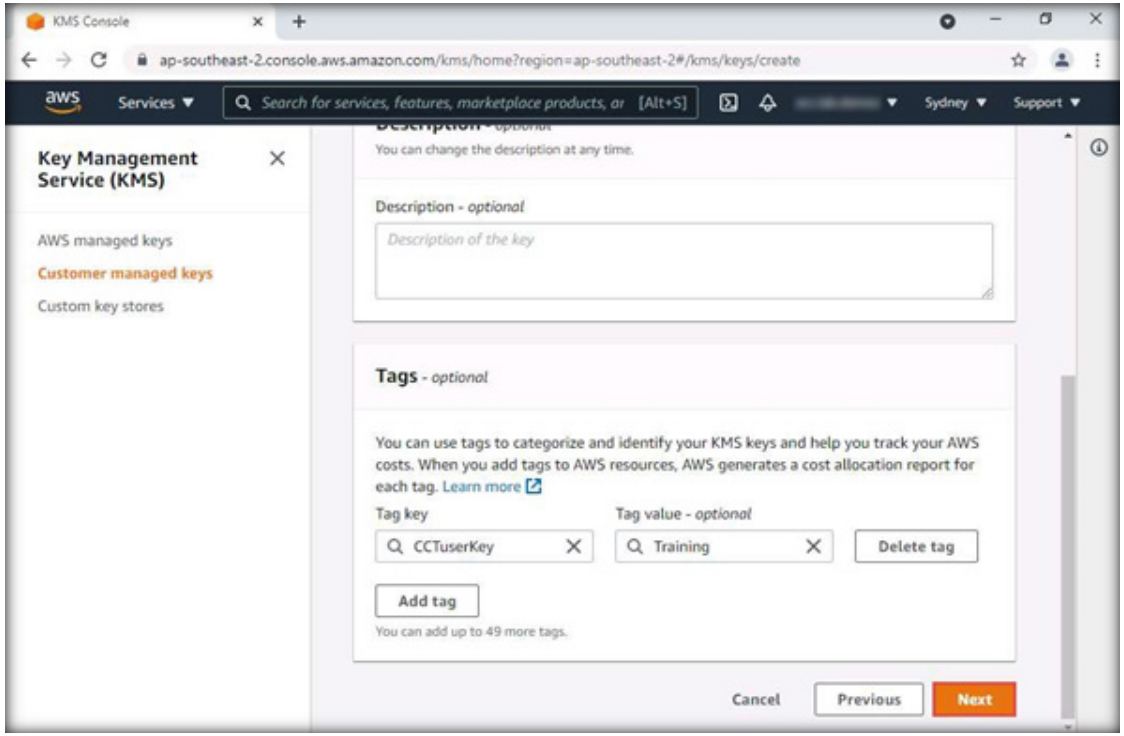
9. By default, the Symmetric key is selected. Click on Next to continue.

10. Type CCT_User_MasterKey in the Alias field, which will serve as the name of your Master Key. The Description is optional; however, entering a brief description of what the key does is recommended. Under the Tags section, you can Add Tags that can help identify the Master Key using Tag key and Tag value. Click on Next.

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

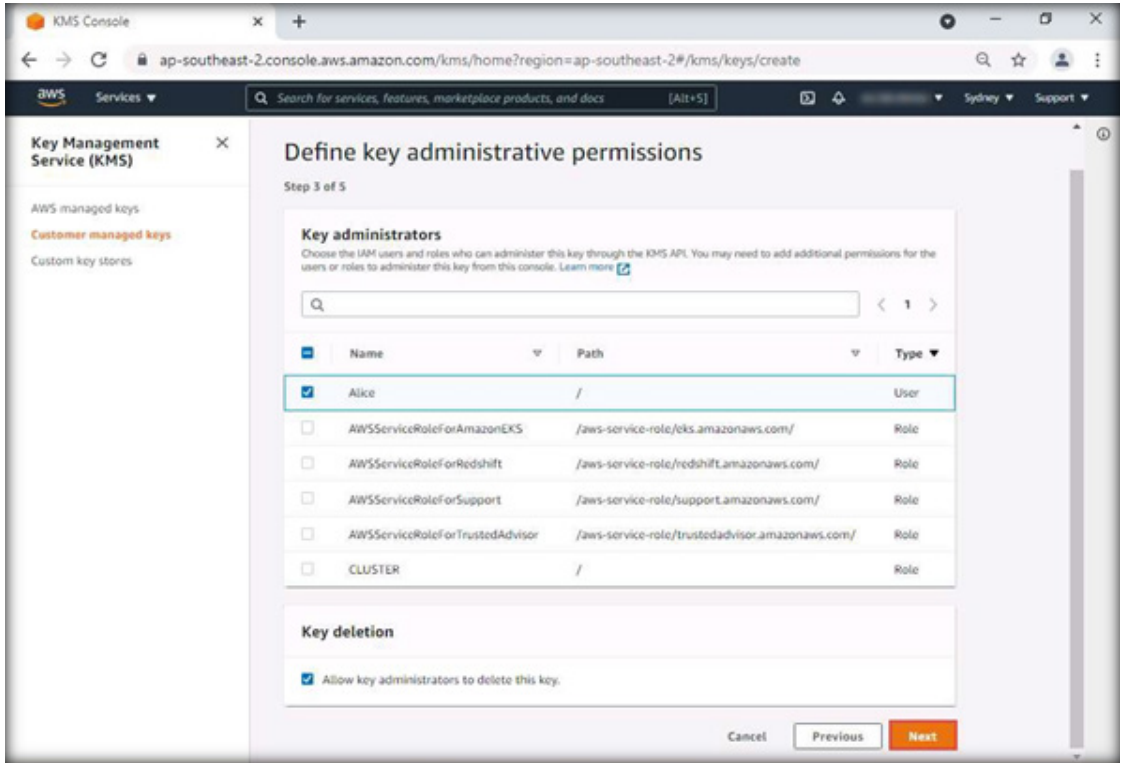


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



Copyrights @ 2022 EC-Council International Ltd.

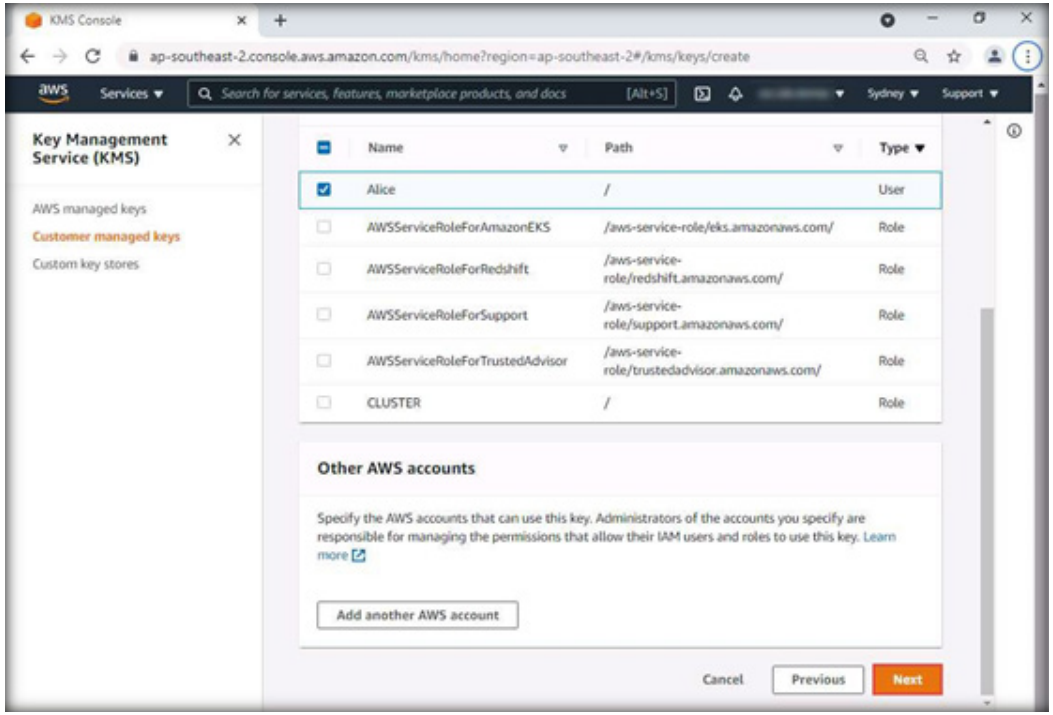
11. To allow users to perform encryption and decryption, we must assign key permissions for the users. In this example, we will permit Alice to use the Master Key and click Next.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

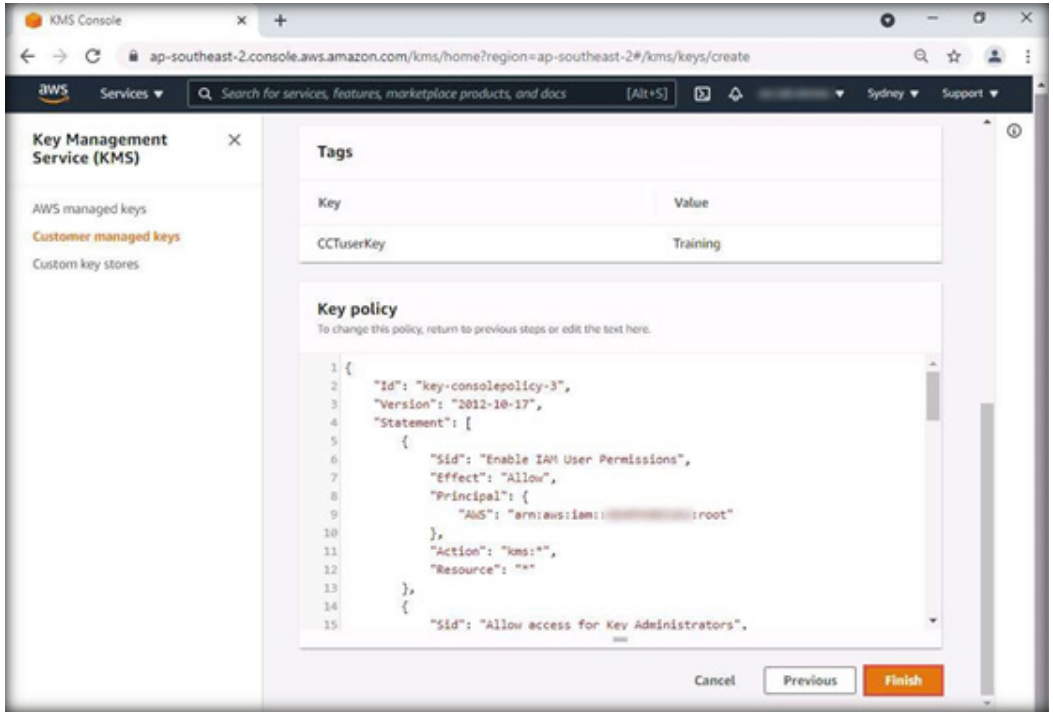
12. At this step, there is an option to Add another AWS account. However, we have already added the user Alice. Therefore, click on Next to continue.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

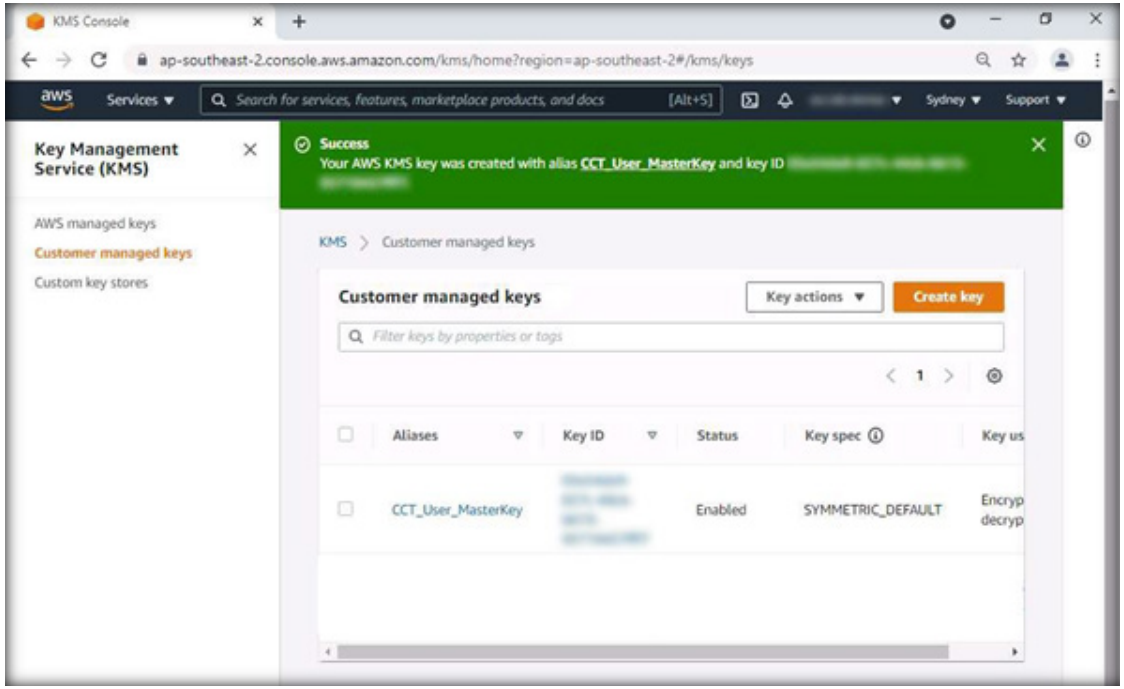
Copyrights @ 2022 EC-Council International Ltd.

13. You can Review and edit key policy, which is in JSON format. Click on Finish to create the Master Key.



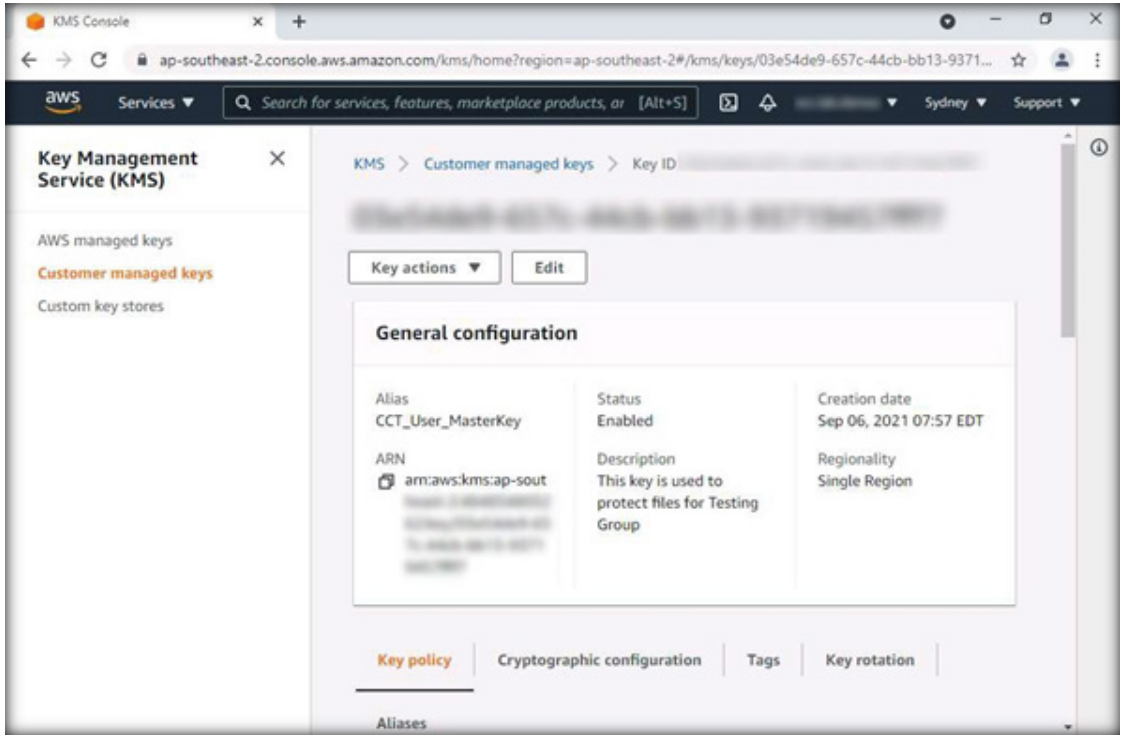
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

14. The key has been created successfully, and it now appears in the Customer managed keys section.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

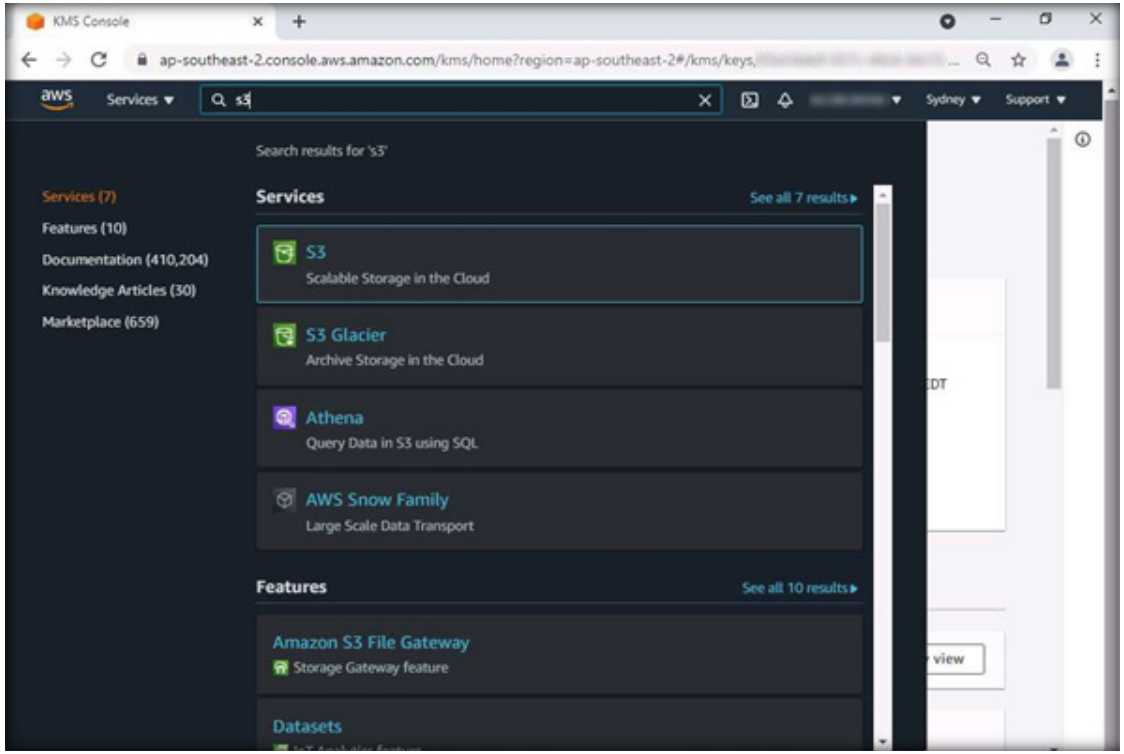
15. After creating the key, you can go to Customer managed keys and click on the key (here, it is CCT_User_Masterkey) in the Alias column to view the Master Key properties.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

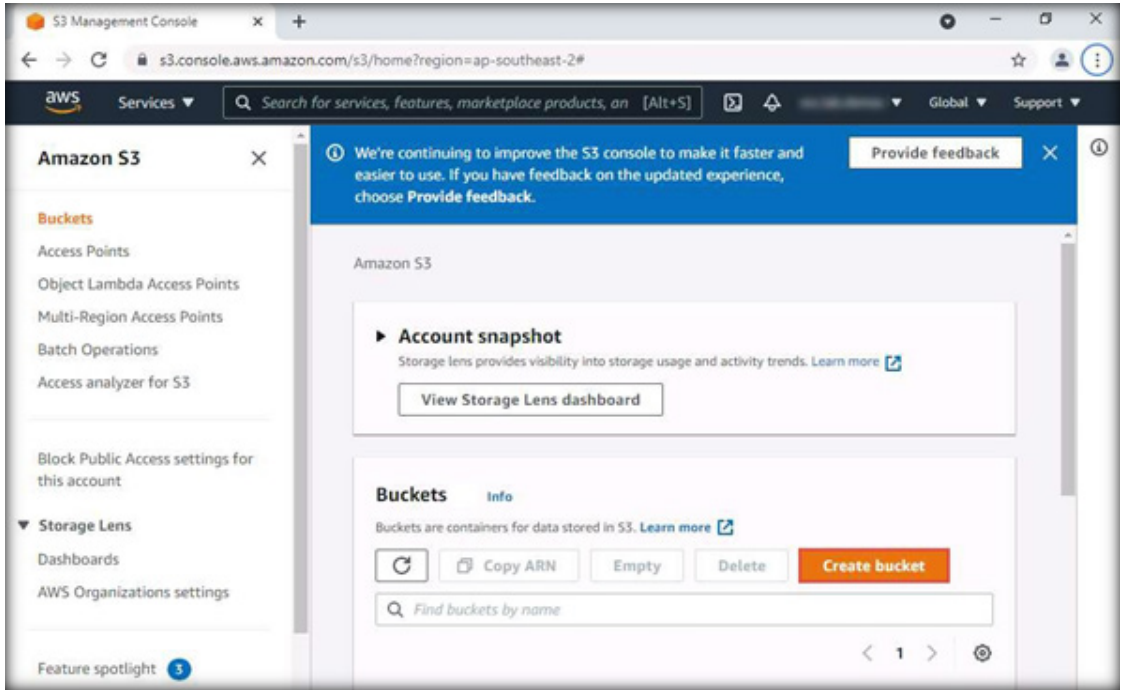
16. In the AWS Management Console, click on Services from the menu bar and enter S3 in the search field. Click on S3 Scalable Storage in the Cloud from the search results.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

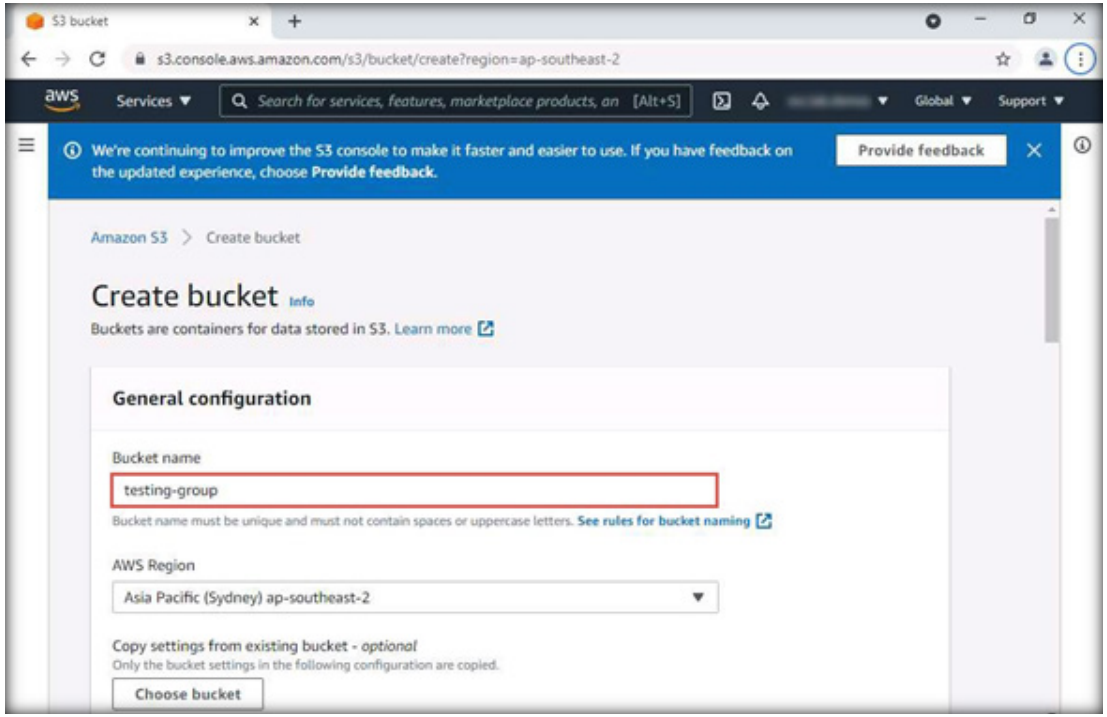
17. The S3 buckets page appears. Click on Create bucket.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

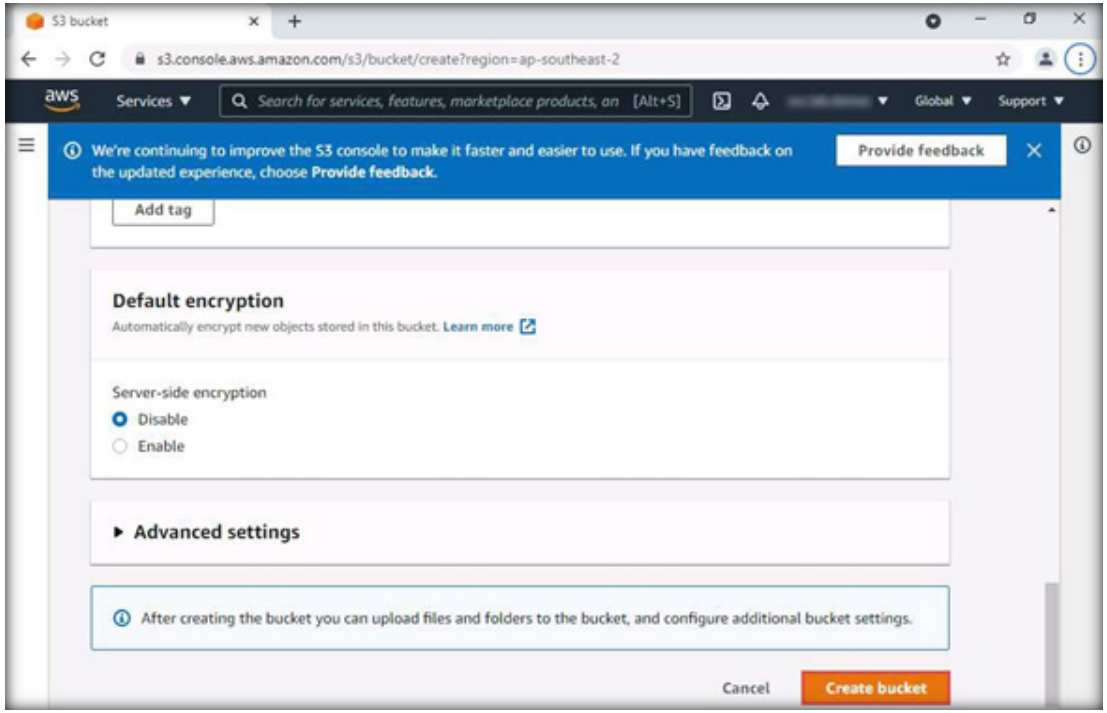
18. The Create bucket pop-up appears. Under General configuration, type the name of the bucket in the Bucket name field (here, the bucket name is testing-group), and retain the other default settings.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

19. Retain default settings for all other sections, scroll down and click on Create bucket.

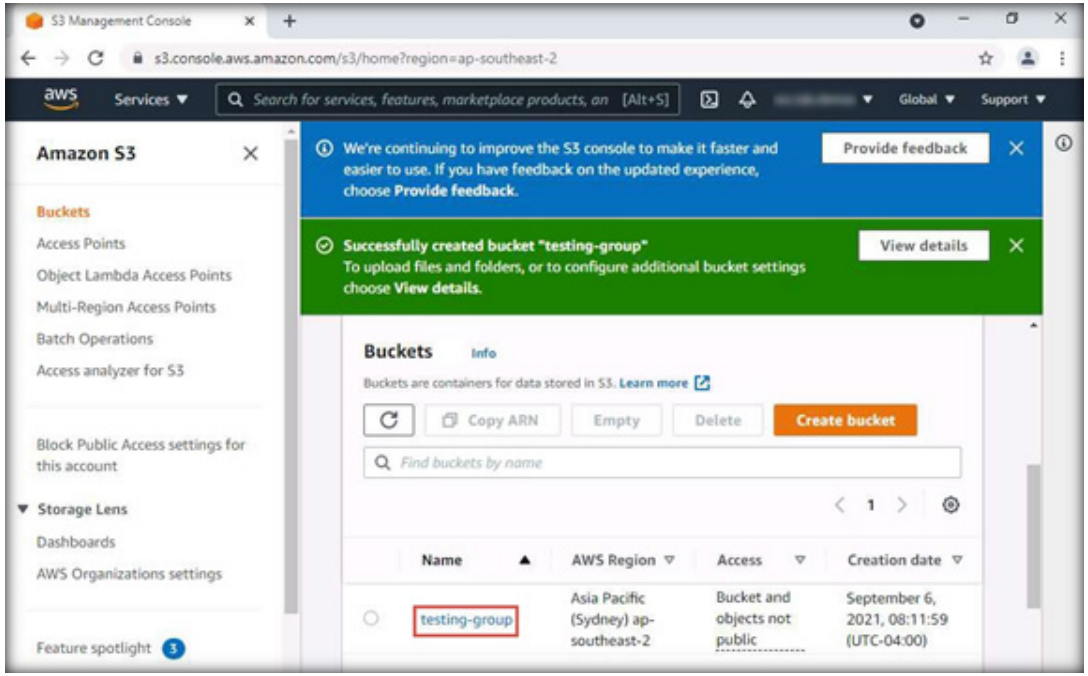


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

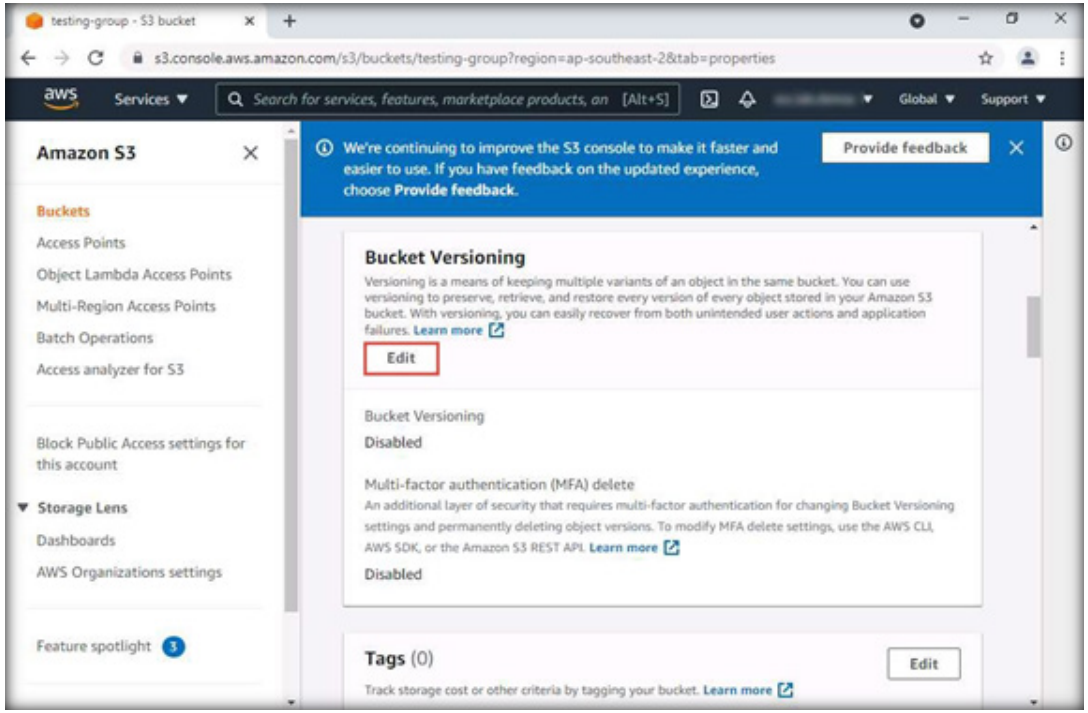
20. The S3 buckets page appears.

21. Click on the bucket for which you want to configure the encryption settings (here, click on testing-group).



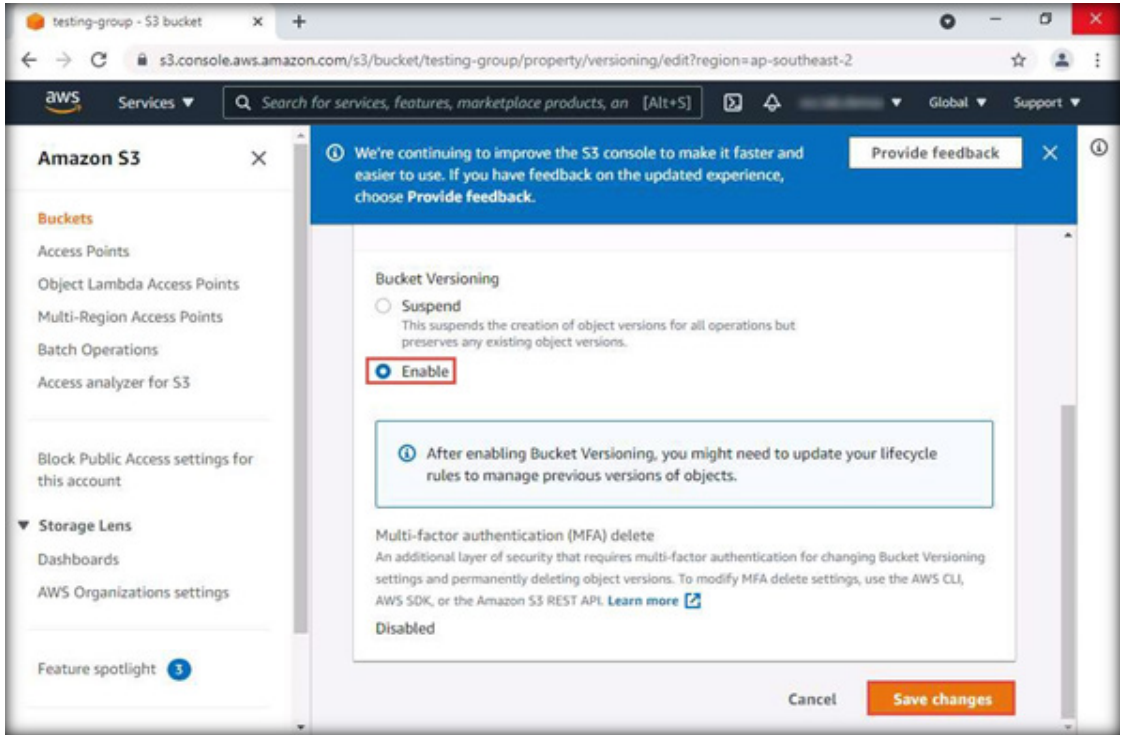
Copyrights @ 2022 EC-Council International Ltd.

22. The testing-group bucket page appears. Click on Properties, and then click on the Edit button under the Bucket Versioning section.



Copyrights @ 2022 EC-Council International Ltd.

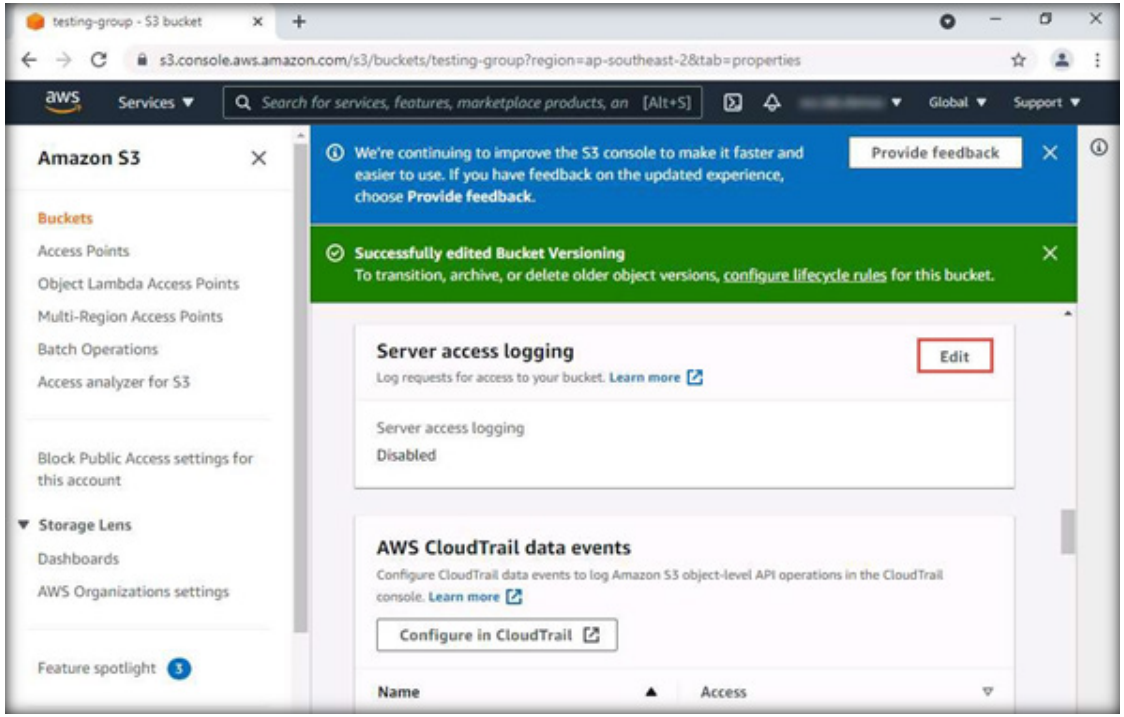
23. Click on the Enable radio button under Bucket Versioning to enable it, and then scroll down and select Save changes.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

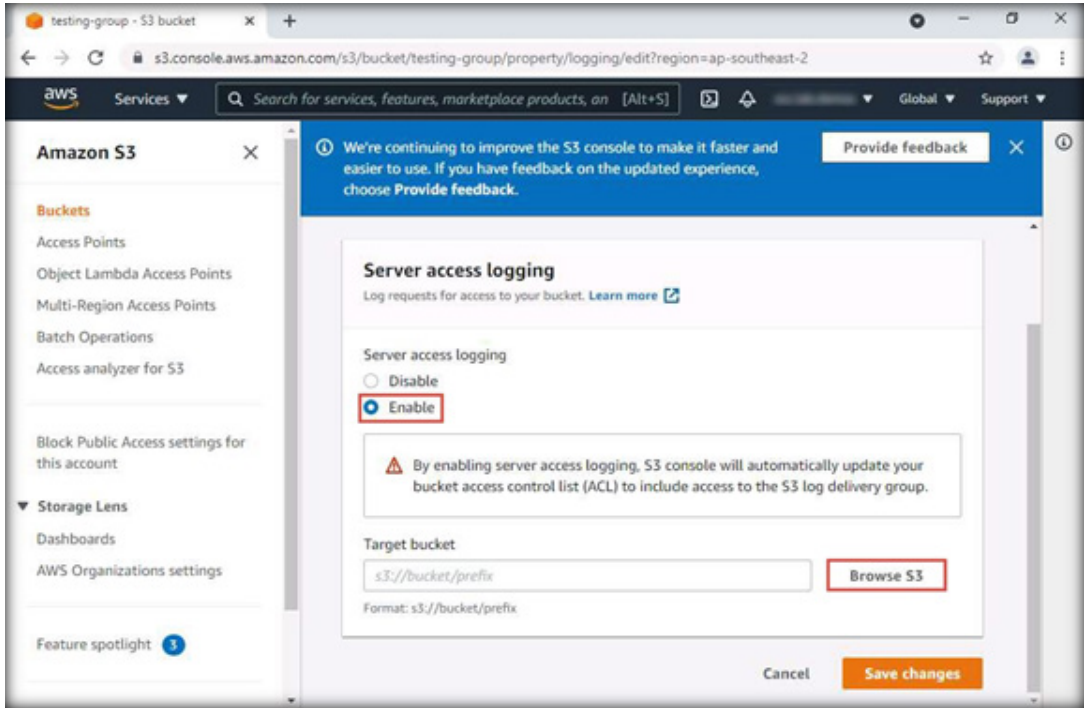
24. In the testing-group bucket page scroll down to Server access logging and click on Edit.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

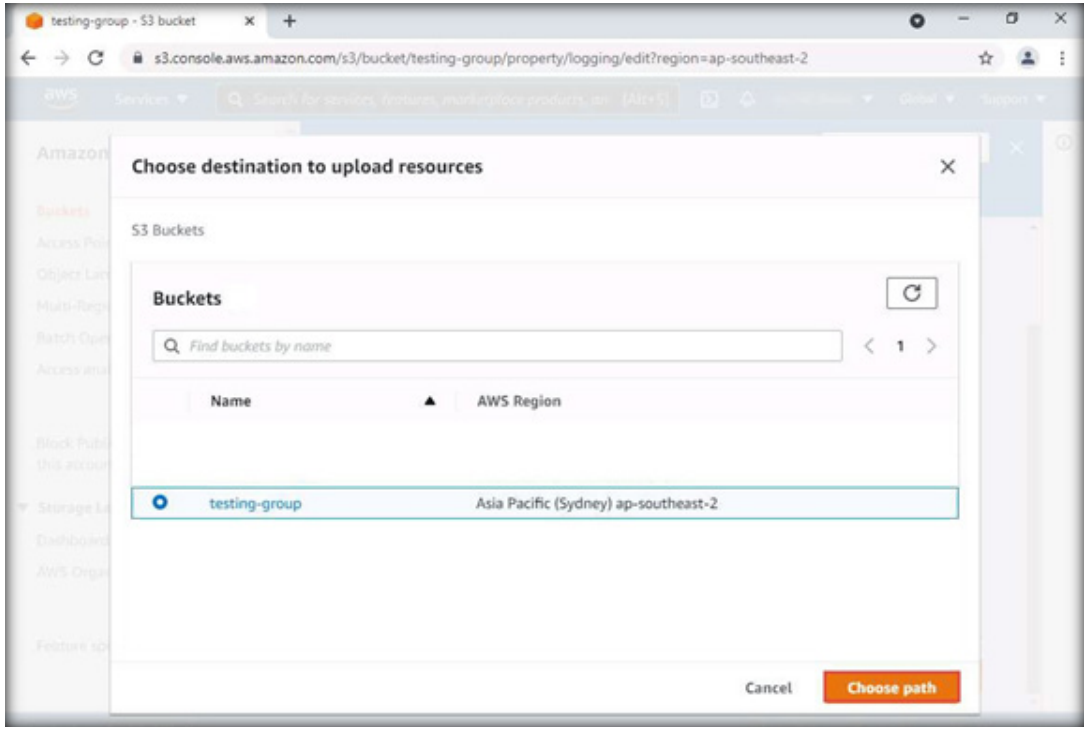
Copyrights @ 2022 EC-Council International Ltd.

25. Click on the Enable radio button under Server access logging Similarly and click on Browse S3 to select the target bucket.



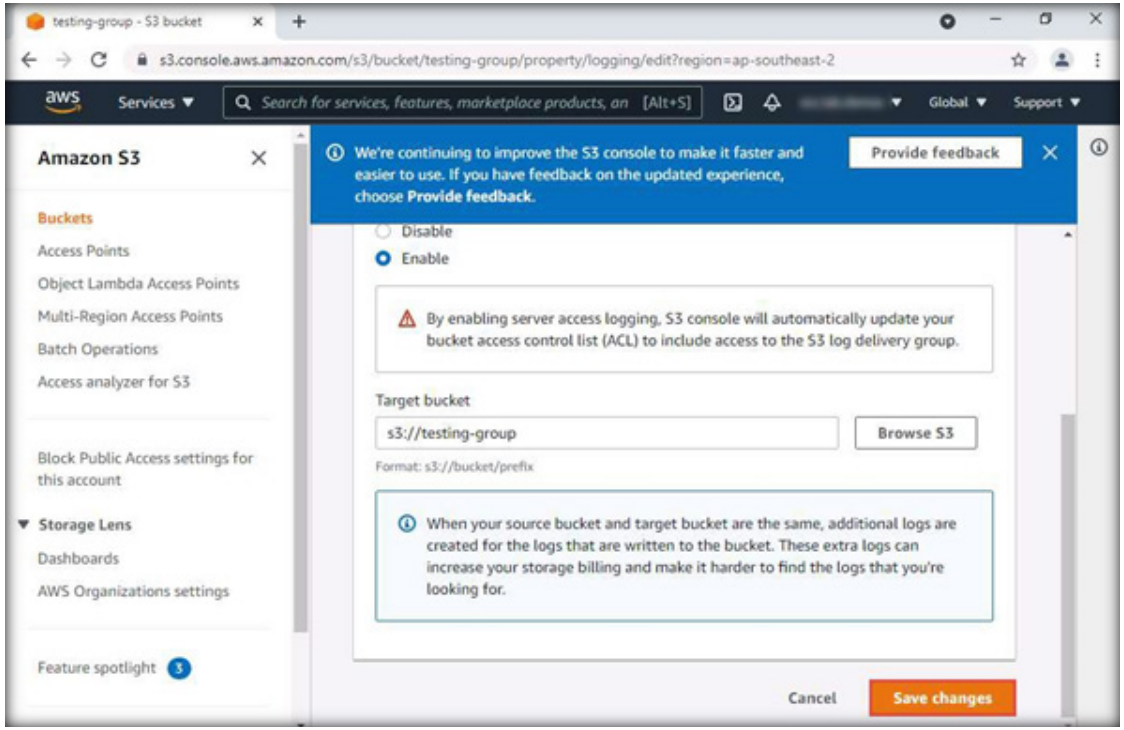
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

26. In the Choose destination to upload resources window select testing-group s3 bucket and click on Choose path.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

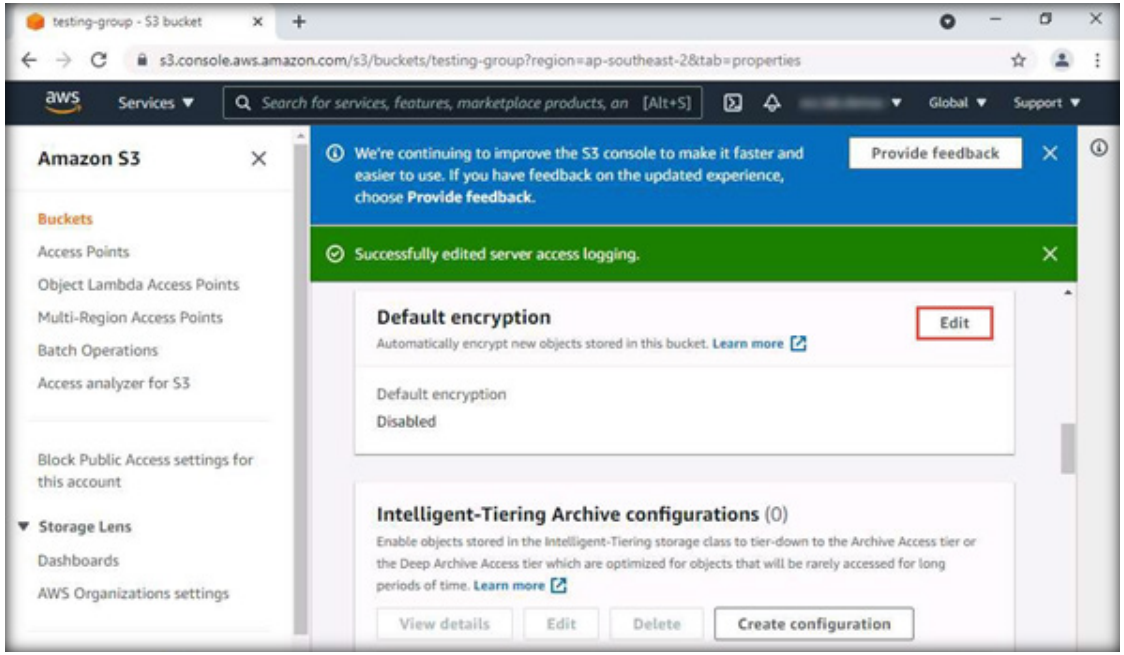
27. The testing-group appears in Target bucket, scroll down and click on Save changes.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

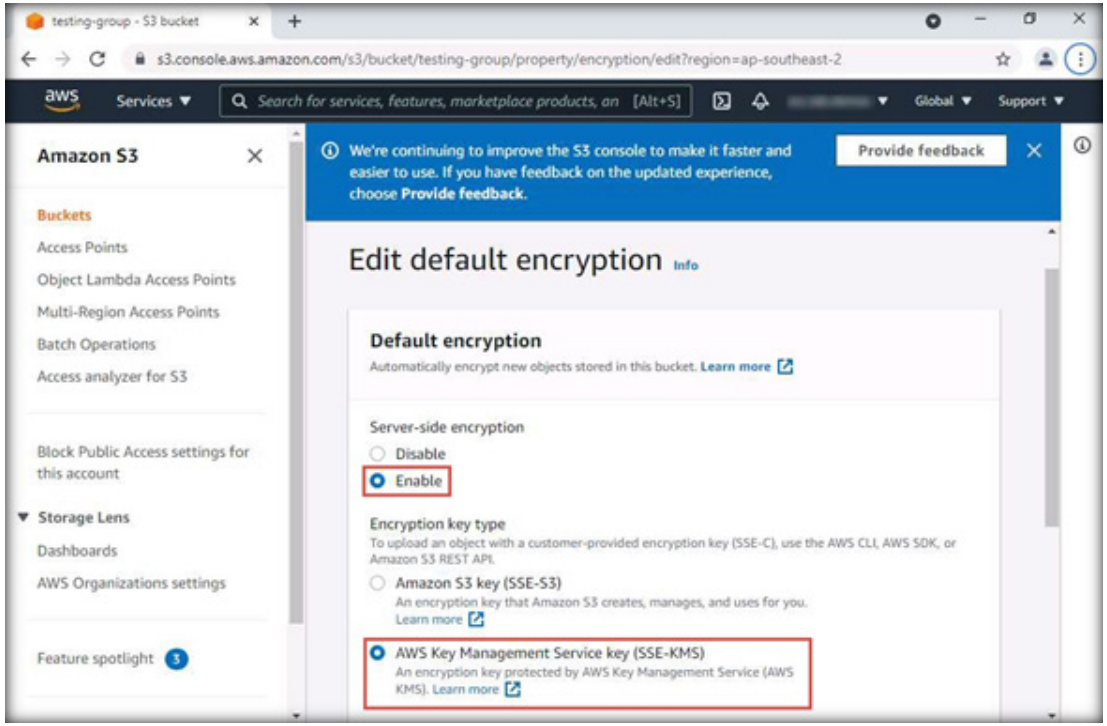
28. Next, in the testing-group bucket page, scroll down and click on Edit button under Default encryption.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

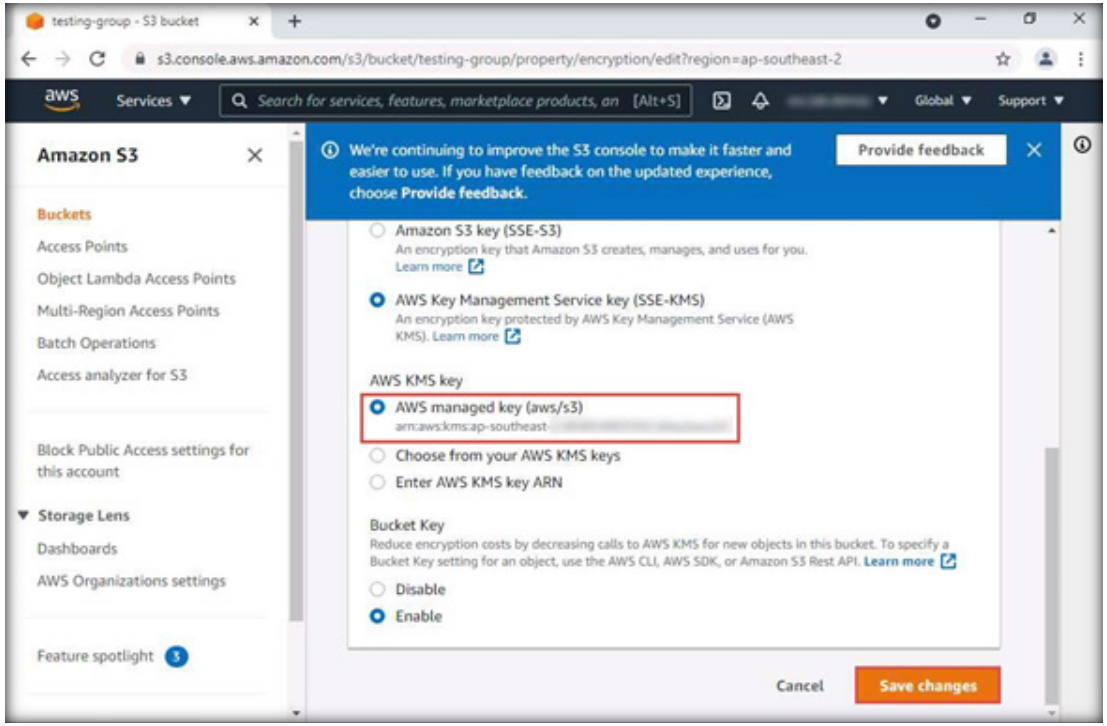
29. In the Edit default encryption window select Enable radio button and choose the AWS Key Management Service key (SSE-KMS) radio button from the list of encryption key types, and select AWS managed key aws/s3 under AWS KMS key section, which will use the default AWS Managed Keys. Click on Save changes.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

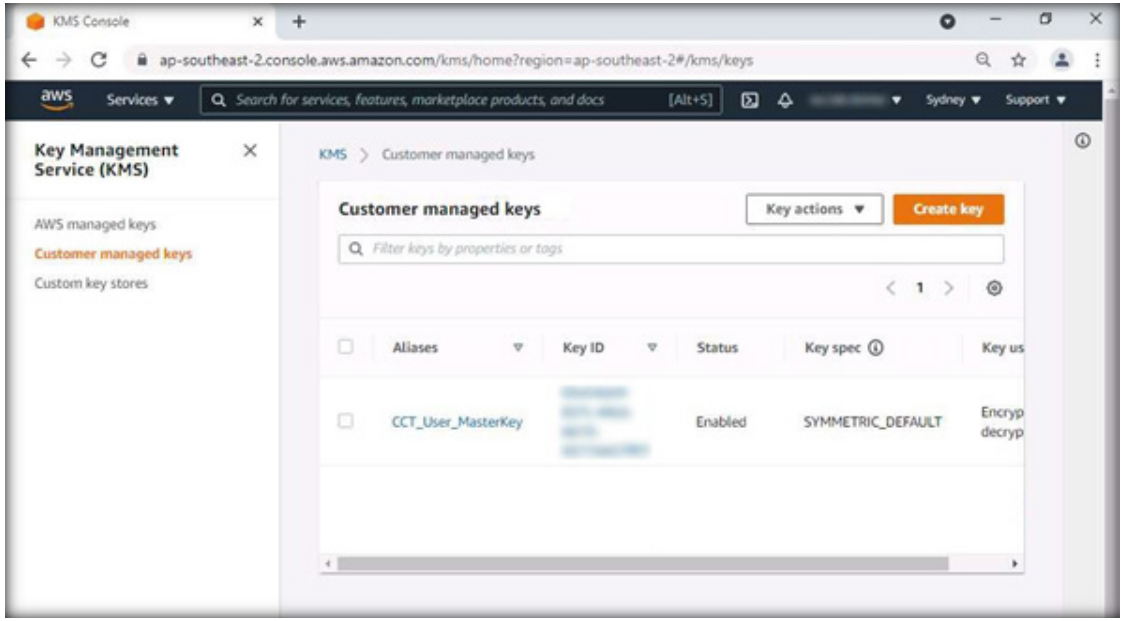


Copyrights @ 2022 EC-Council International Ltd.

30. We have created the testing-group bucket for encrypting data. The user can push data into this bucket.

31. The user can also use a customer managed key for this bucket. Let us see how to use the customer managed key for the testing-group bucket to encrypt the data.

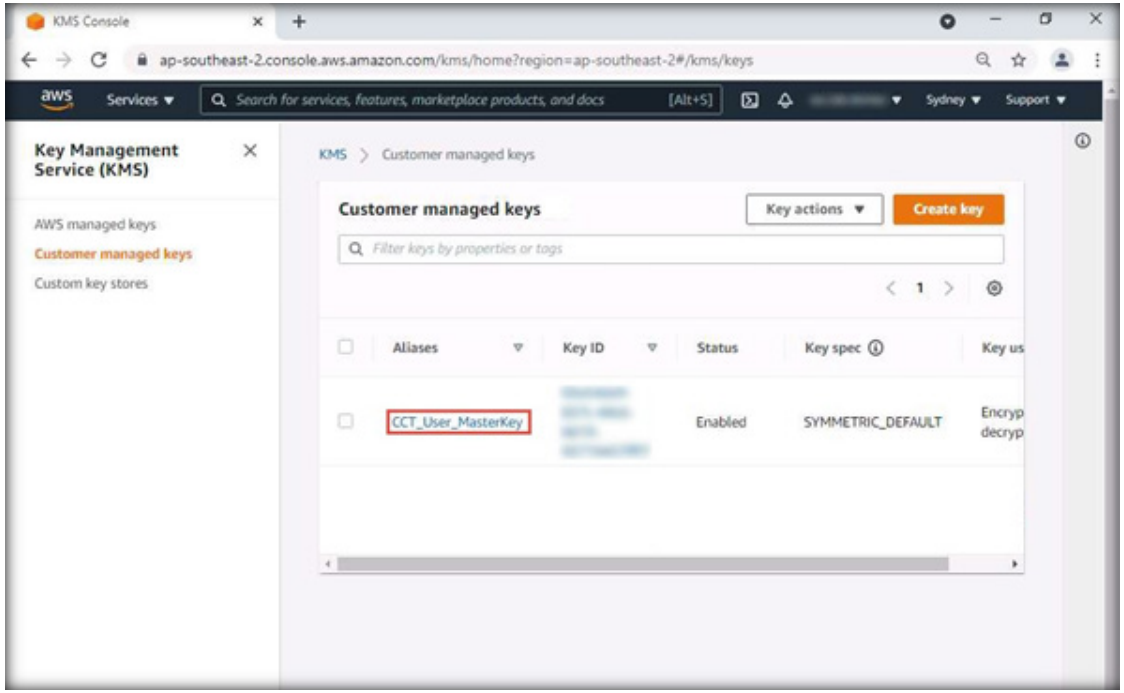
32. Go to Key Management Services (KMS), and select Customer managed keys.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

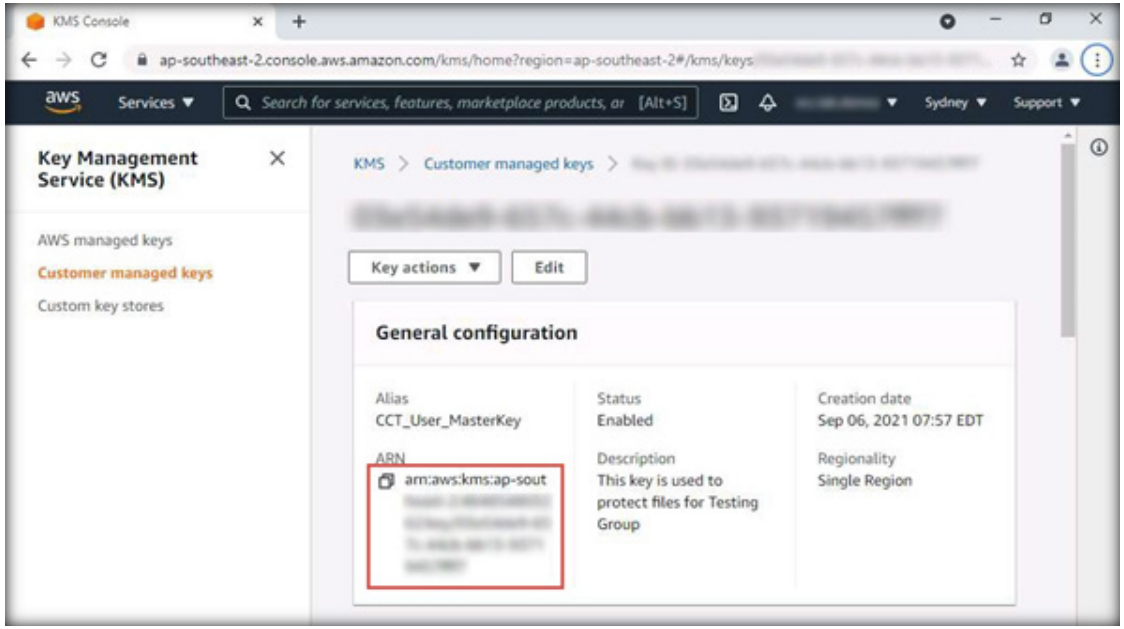
Copyrights @ 2022 EC-Council International Ltd.

33. Under the Customer managed keys pane, click on CCT_User_MasterKey Alias.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

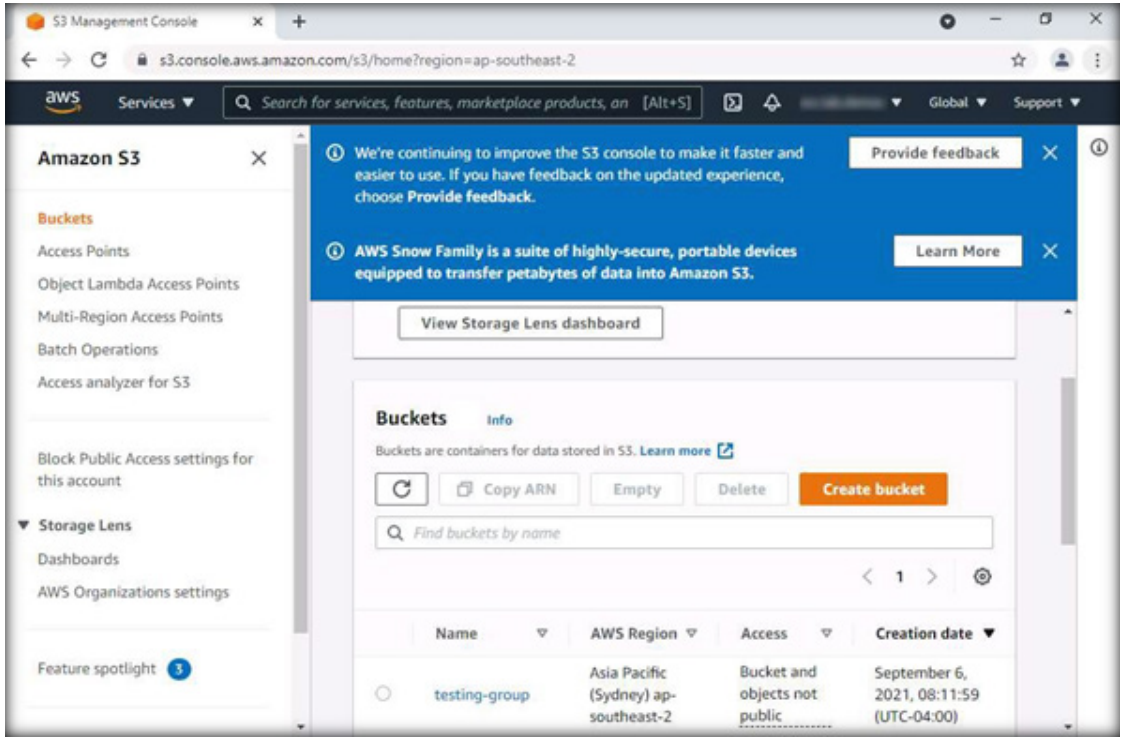
34. Under the CCT_user_MasterKey's General configuration, select the Amazon Resource Names (ARN) key which uniquely identify AWS resourceskey under the ARN field and copy it.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

35. Open Notepad and paste the copied link.

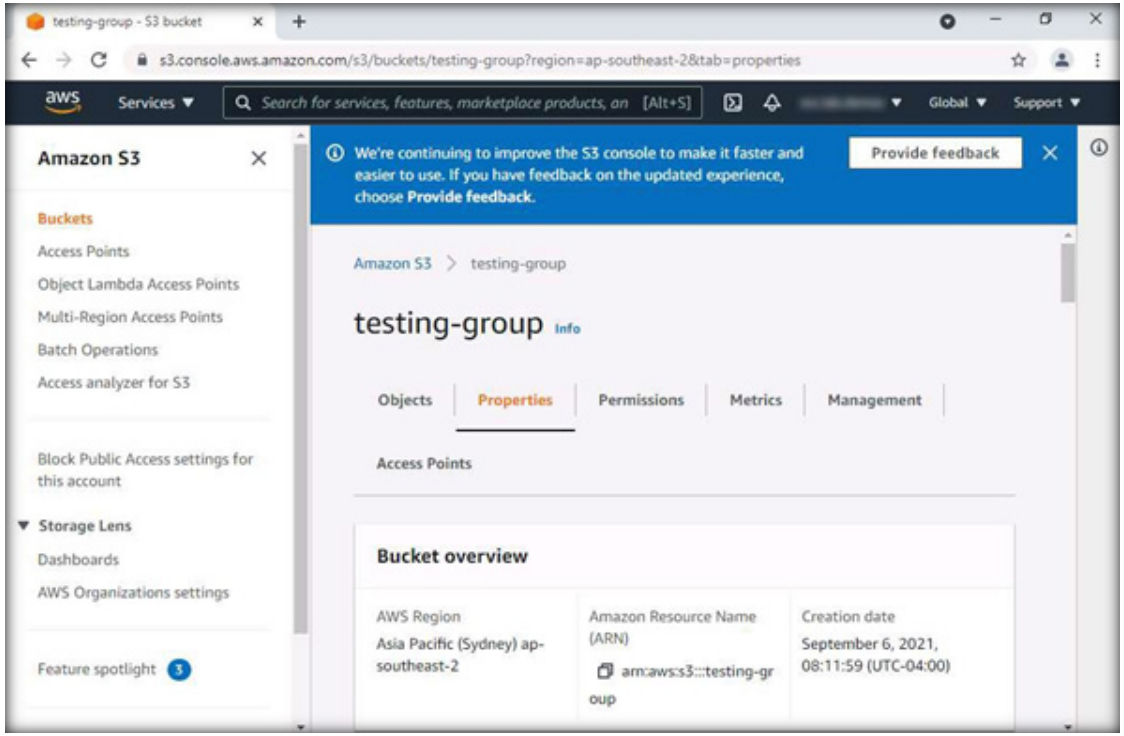
36. Switch to the browser. Navigate to S3 Management Console and select testing-group under Bucket name.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

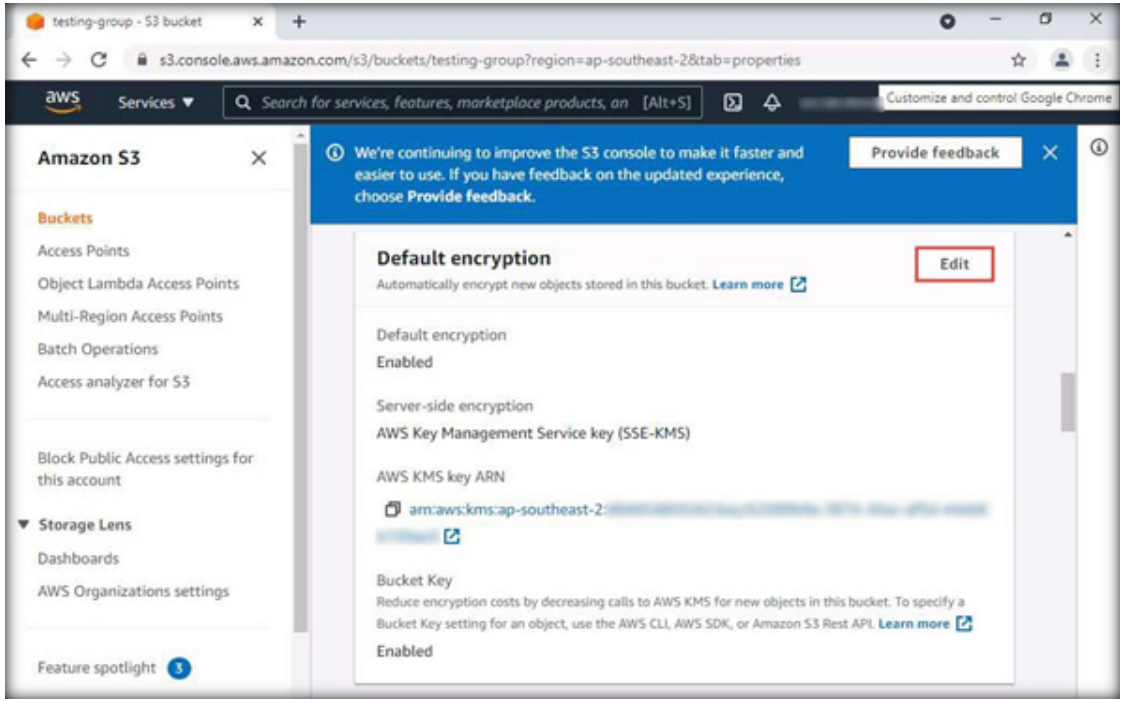
Copyrights @ 2022 EC-Council International Ltd.

37. The testing-group pane opens. Select the Properties tab.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

38. Scroll down and click on Edit button under Default encryption.

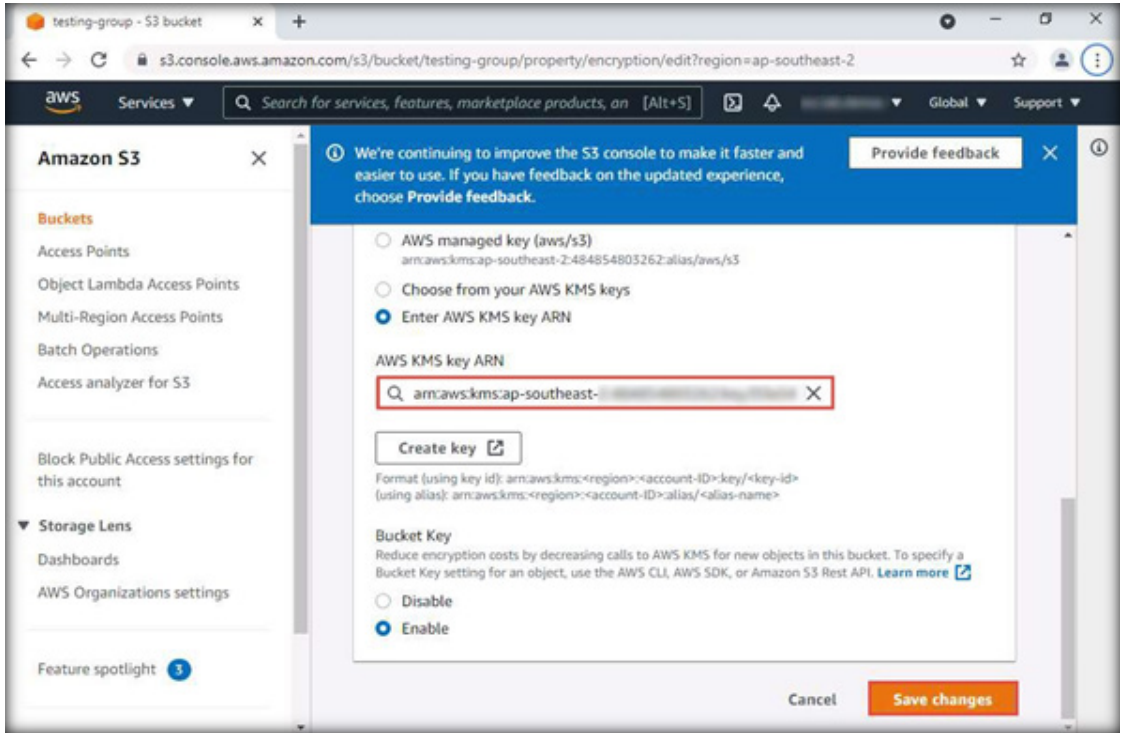


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

39. Switch to Notepad and copy the key that we had pasted in Step 35.

40. Again, switch back to the Default Encryption and select the Enter AWS KMS key ARN radio button and paste the key that was copied in Step 35 in the AWS KMS key ARN. Click on Save changes.



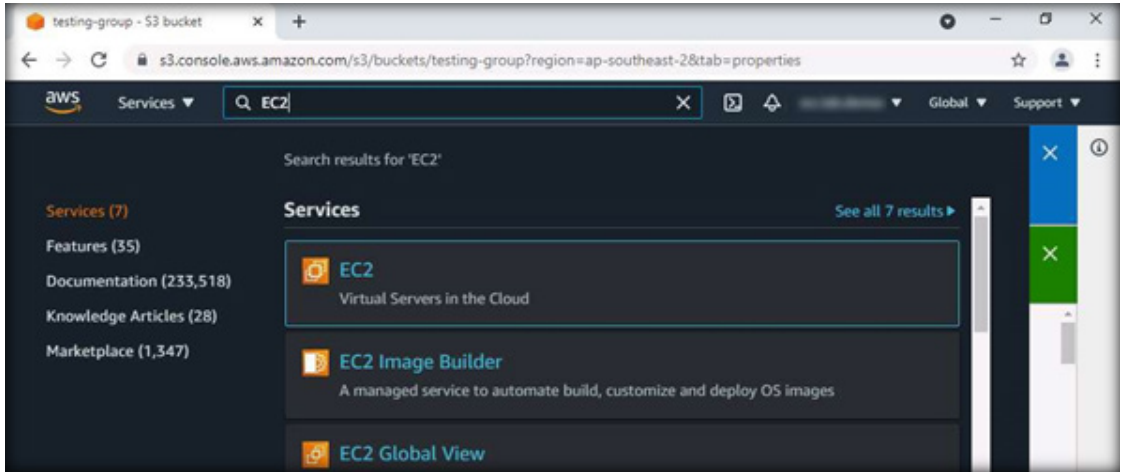
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

41. In this way, with the help of Customer Managed Keys, the user can encrypt and protect storage data.

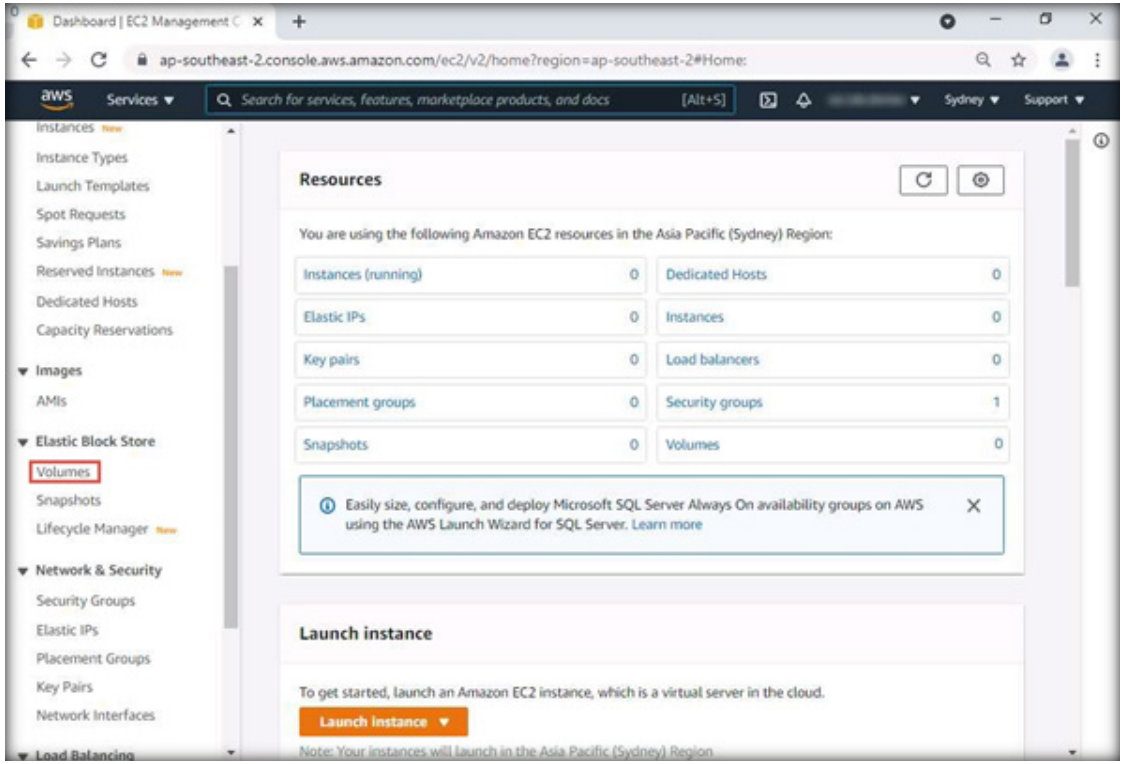
42. Amazon EBS supports KMS. Its encryption provides security to data at rest by encrypting data volumes, boot volumes, and snapshots using Amazon-managed keys or keys created and managed using the AWS KMS.

43. Click on Services from the menu bar, and search for EC2. From the search results, click on EC2 Virtual Servers in the Cloud as shown in the screenshot below.



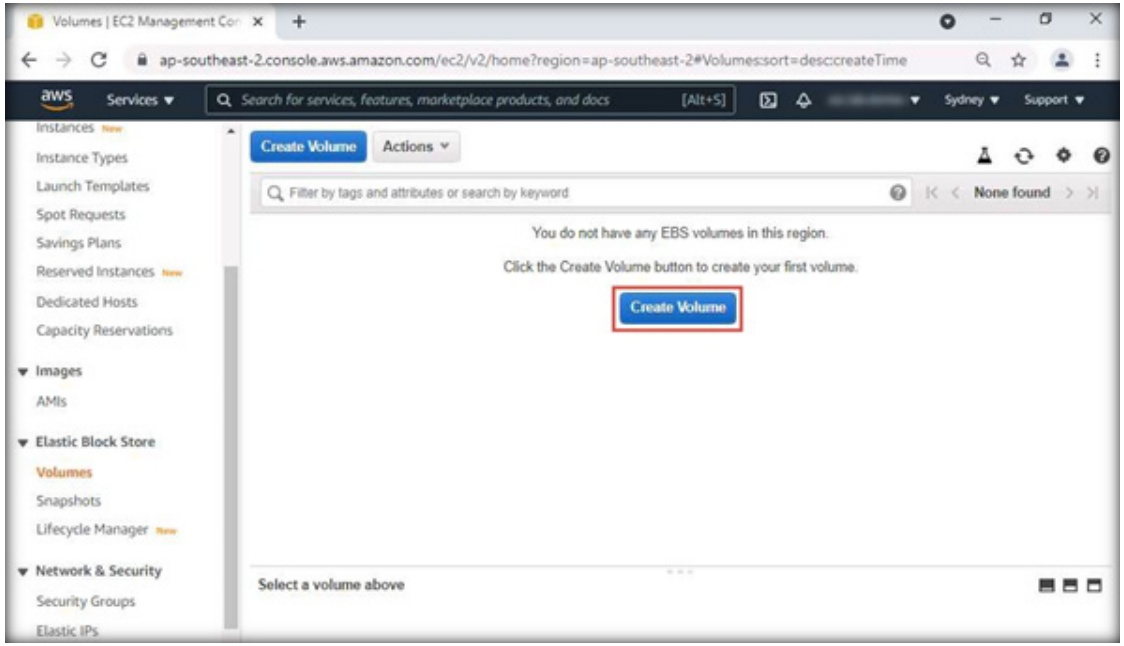
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

44. Once the EC2 Service Console page opens, click on Volumes in the left pane under Elastic Block Store.



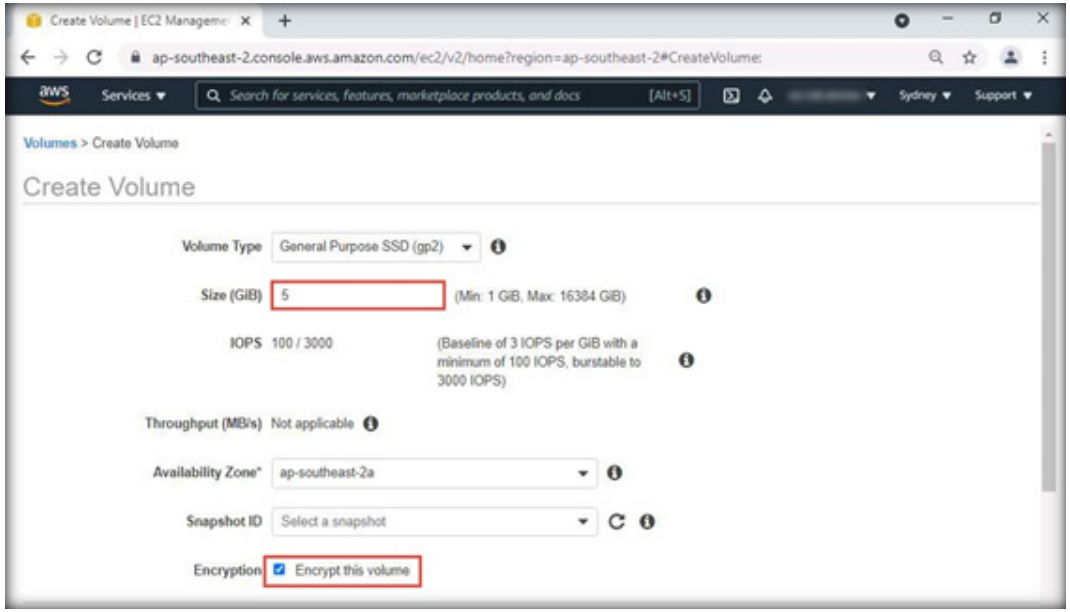
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

45. To create a new volume, click on Create Volume.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

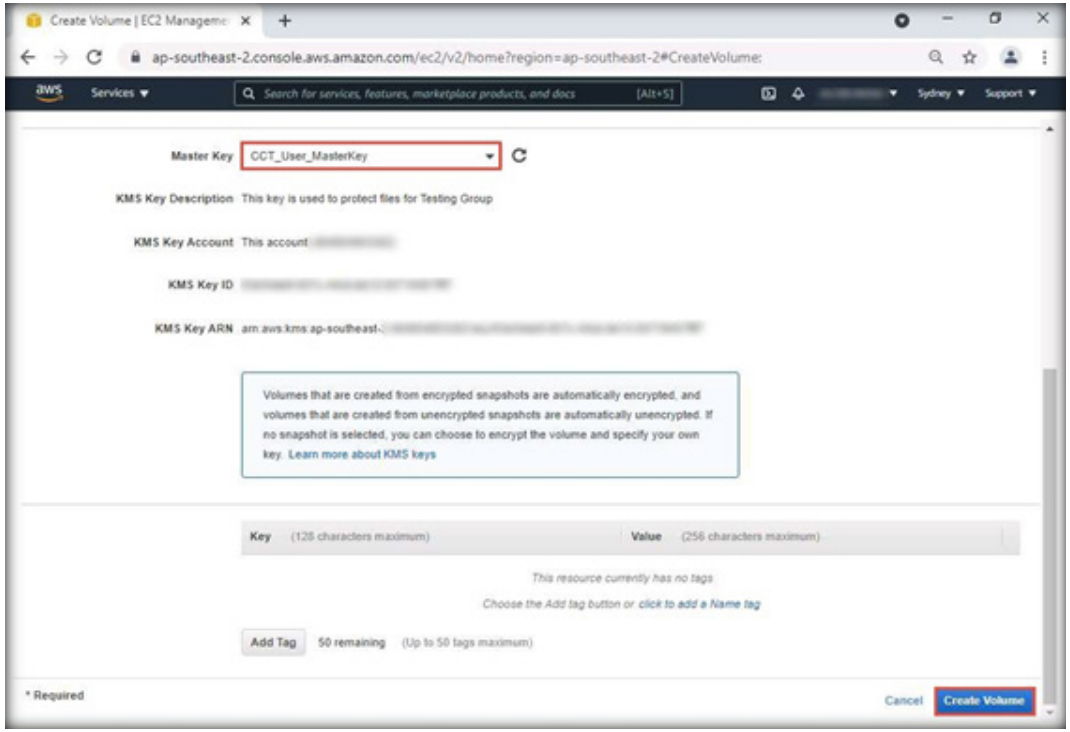
46. In the Create Volume page, select the Volume Type and specify the size of the volume in the Size (GiB) field. If you need the disk to restore existing data, you can select a Snapshot ID, in which you have saved another volume's Snapshot. Check Encryption: Encrypt this volume.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

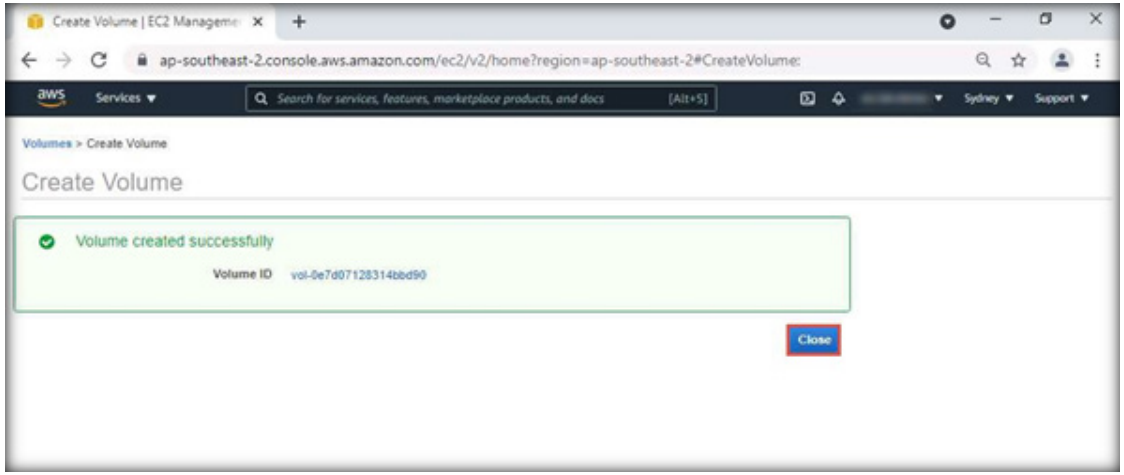
47. In the Master Key field, select the Customer Managed Key we created: CCT_User_MasterKey. After entering the required details, scroll down and click on Create Volume.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

48. The Volume created successfully dialog message will appear once the disk is created. Click on Close.

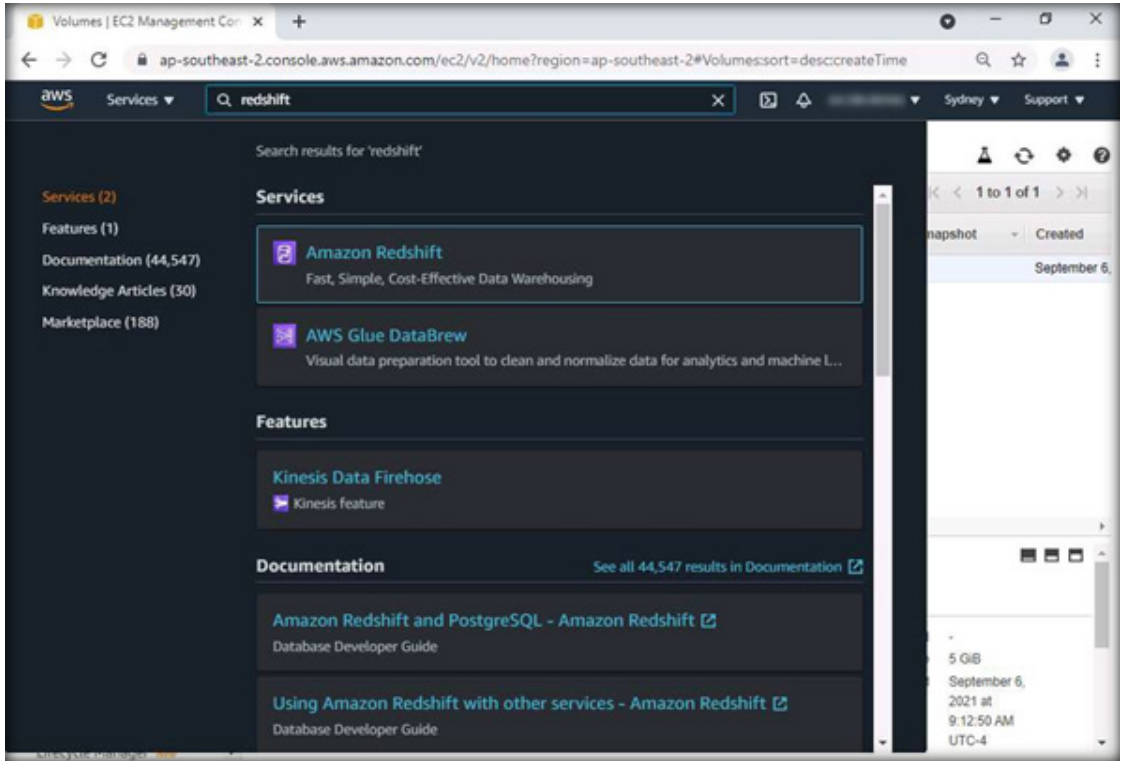


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

49. In this way, the KMS Master Key is used to encrypt the EBS volume.

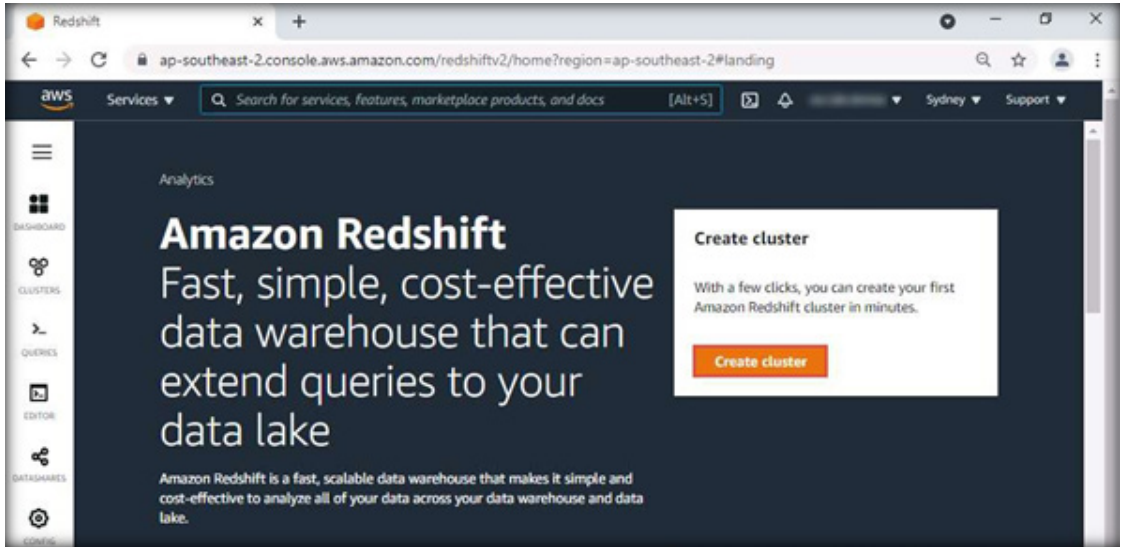
50. As we have encrypted EBS Volume, we will now encrypt Amazon Redshift using KMS Master Key.

51. Go to main search bar and search for redshift and select Amazon Redshift.



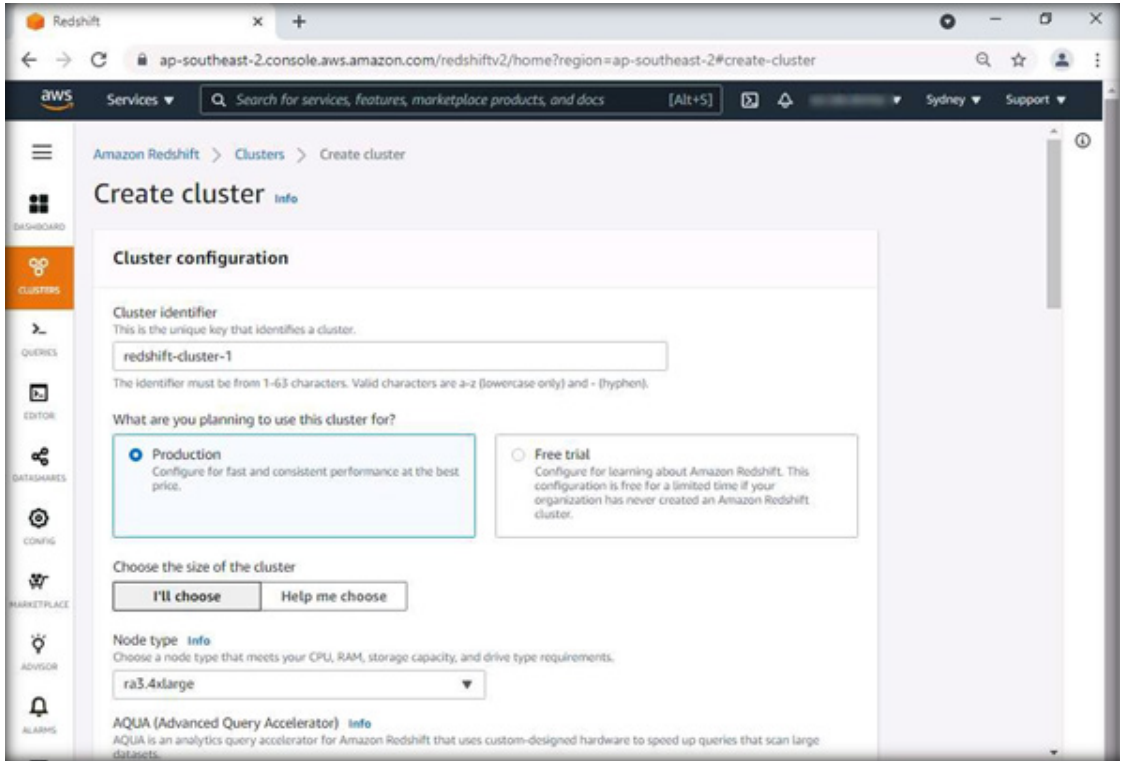
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

52. Close the welcome popup that appears. Click on Create cluster in the Redshift dashboard.



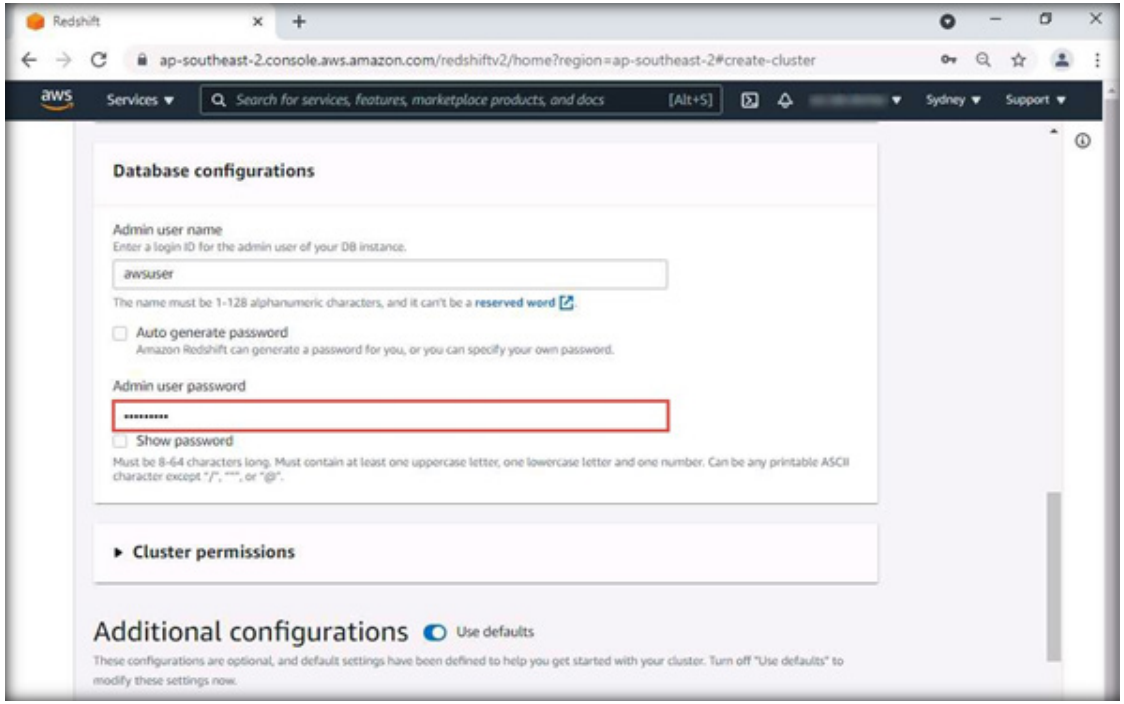
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

53. The Cluster configuration page appears. (Here, we are selecting the Production option to create a new Redshift cluster. If you are in free trial, select a Free trial option, and proceed. Please note that if you select the Production option, your account will be charged as per the AWS pricing model so make sure that you delete the Redshift cluster service after performing the lab.) Scroll down the page to view the detailed configuration of the cluster.



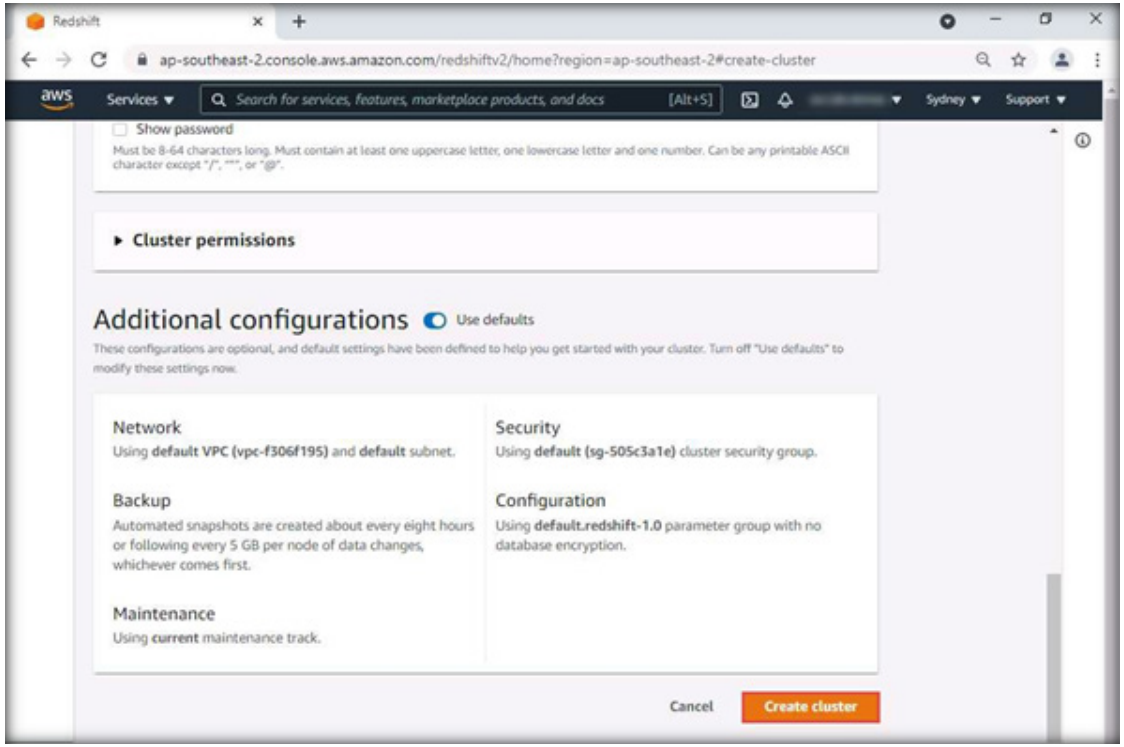
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

54. Type the password Dbuser123 in the Admin user password field. Keep the remaining default settings as it is and click on Create cluster.

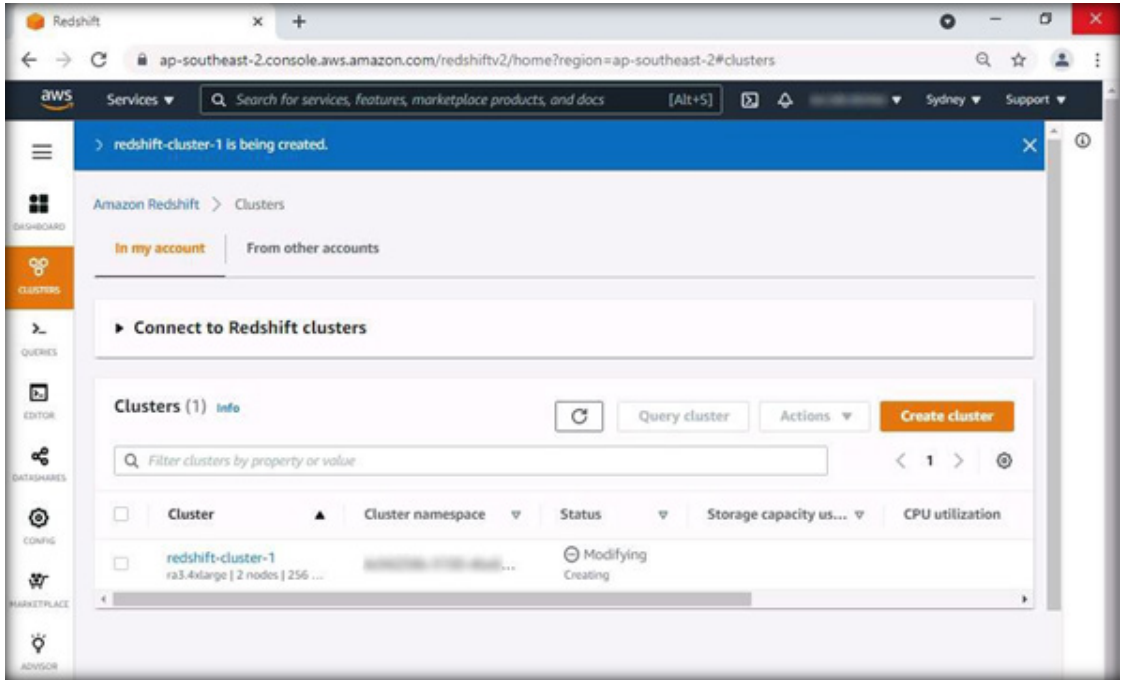


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



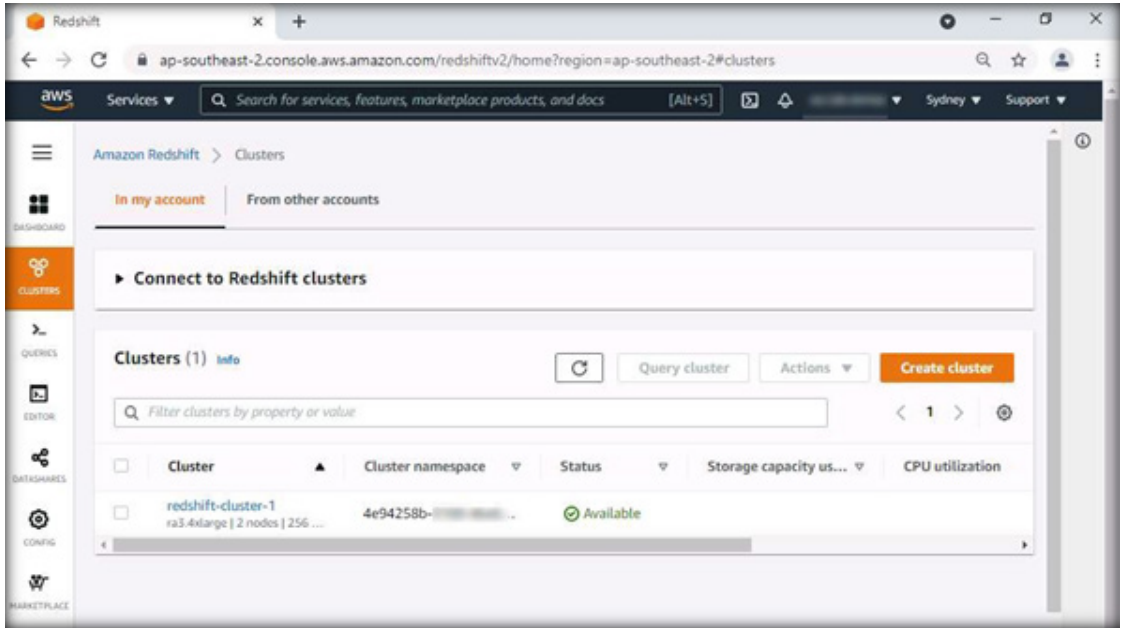
55. The redshift-cluster-1 is now being created. Observe, that it is showed under the Status column as Modifying and Creating. Wait until the cluster is fully created.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

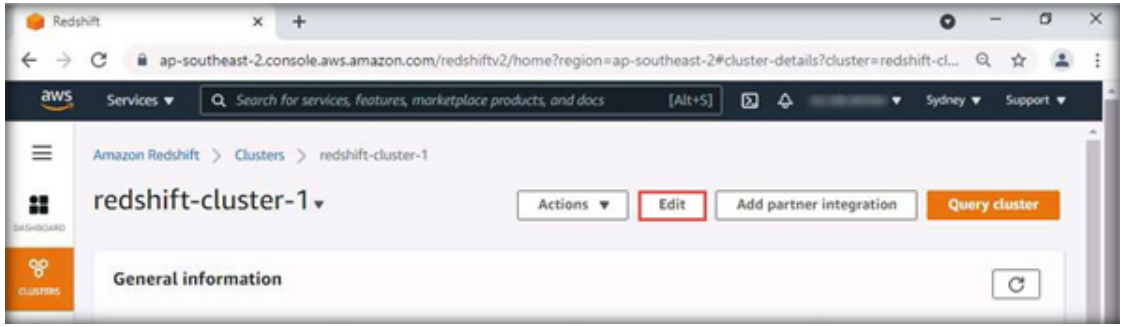
56. Once the cluster is fully created, you can see that the cluster's Status is Available.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

57. Click on the newly created cluster link (here, the cluster link is redshift-cluster-1) to modify the cluster setting.

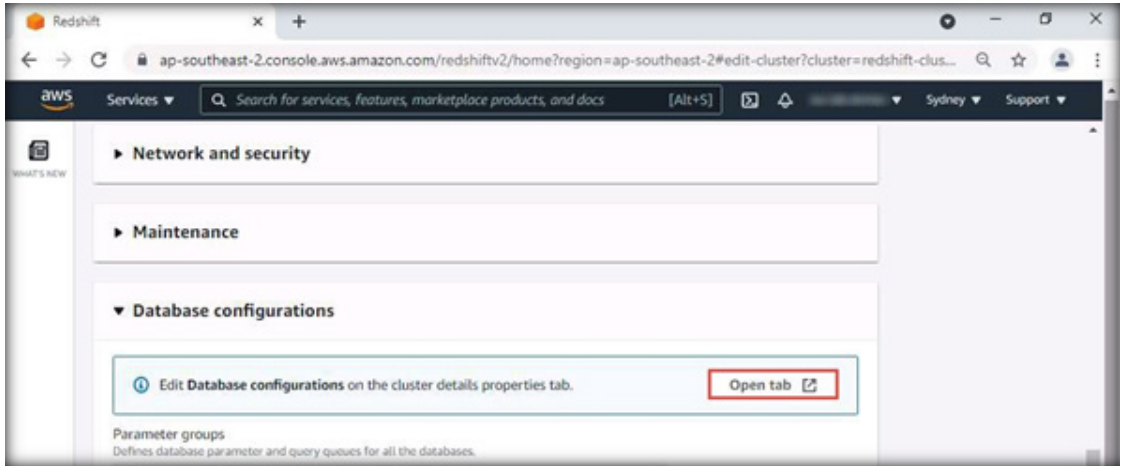
58. The newly created cluster redshift-cluster-1 page appears. Click on Edit button.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

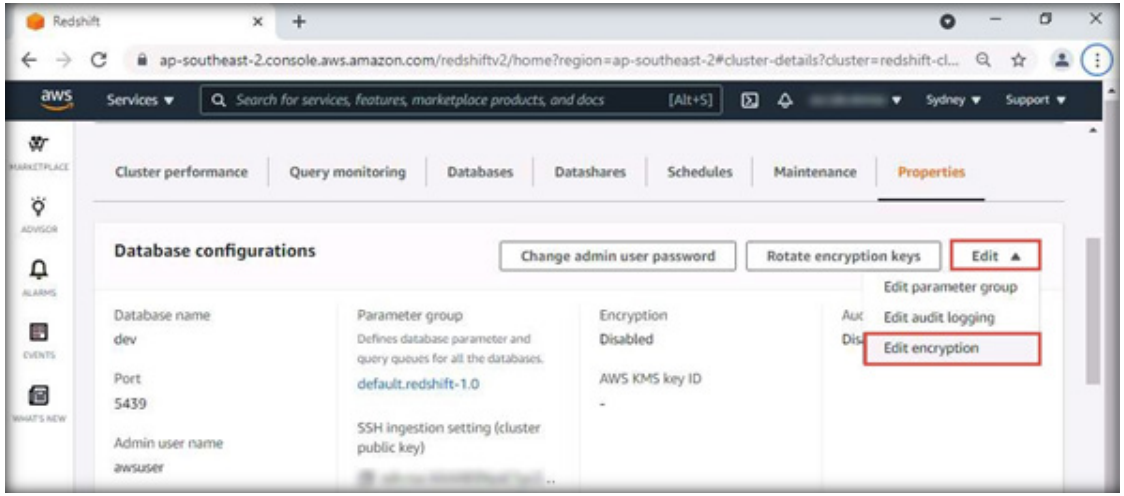
Copyrights @ 2022 EC-Council International Ltd.

59. The Edit cluster redshift-cluster-1 page appears, scroll down to Database configurations. Click on Open tab.



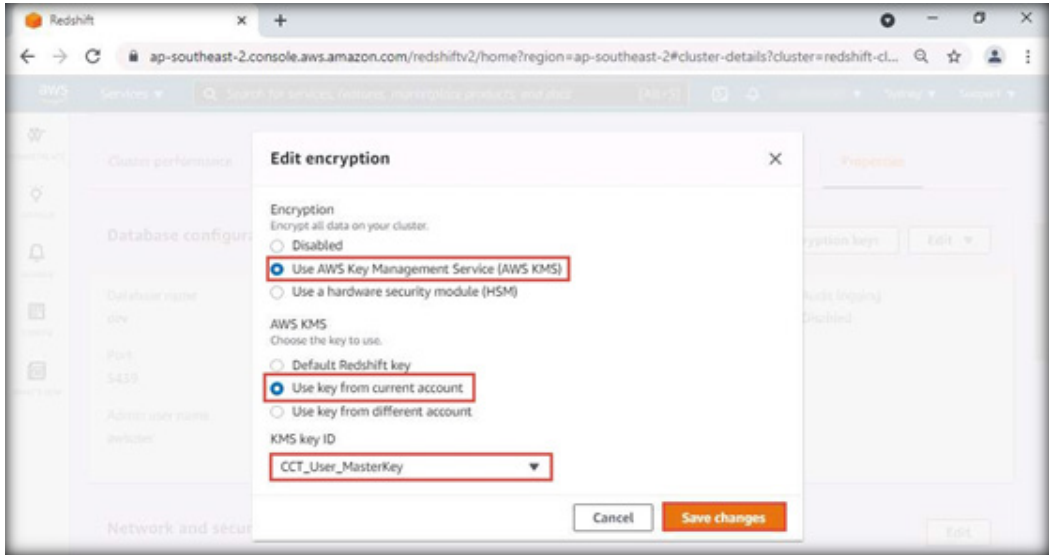
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

60. You will be redirected to Properties section. In the Properties section click on Edit drop down and select Edit encryption. In Edit encryption window, choose the Use AWS Key Management Service (AWS KMS) radio button, then choose Use key from current account, and finally choose CCT_User_Masterkey in KMS key ID drop-down. Click Save changes.

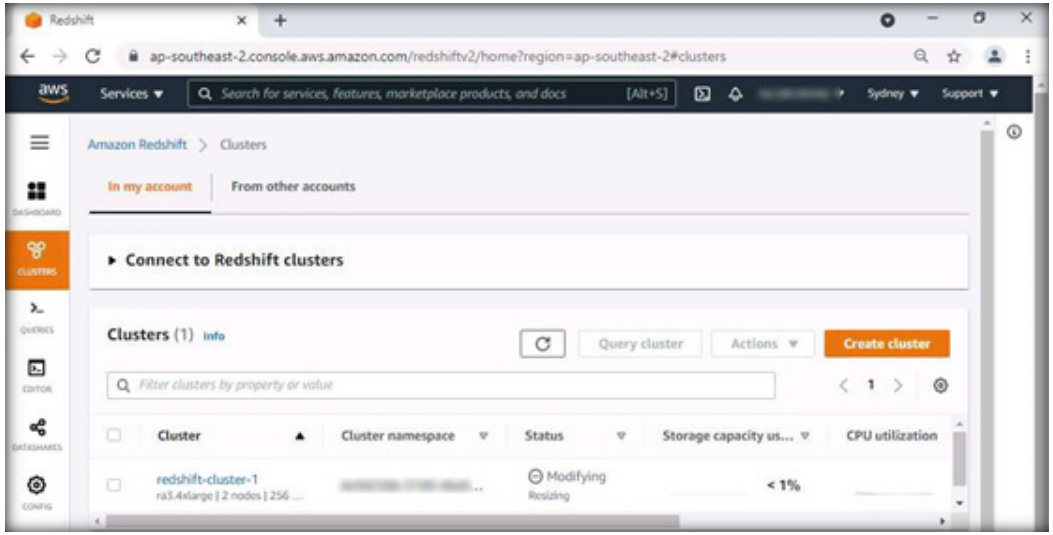


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

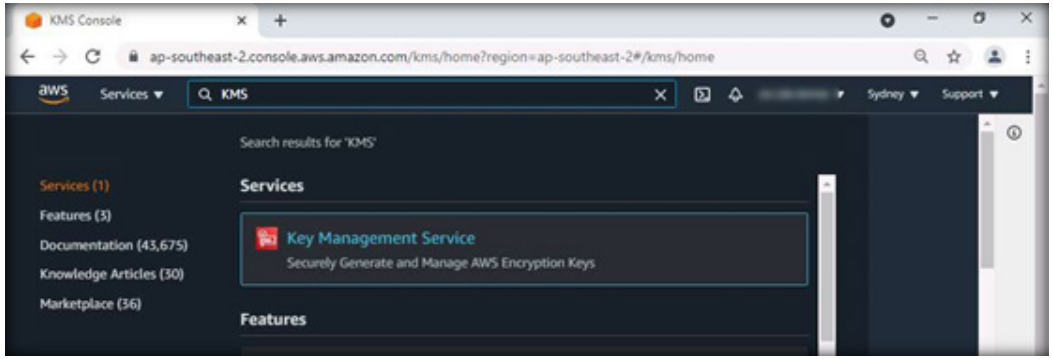


61. See the cluster's status in Status column. It shows Modifying and Resizing.



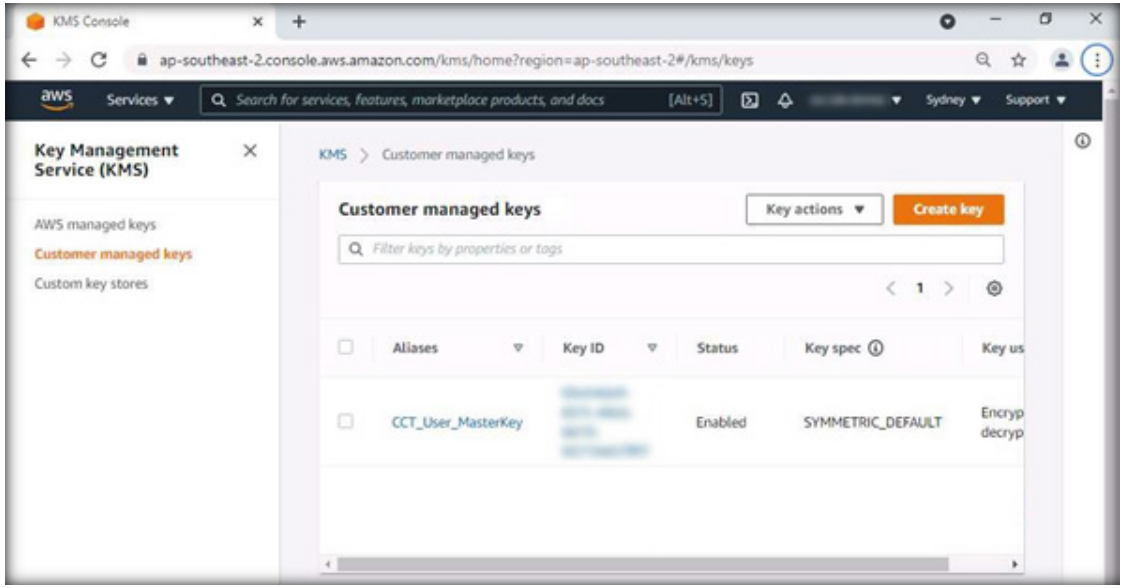
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

62. On the AWS Web Console, click on Services and search for KMS. Select Key Management Service.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

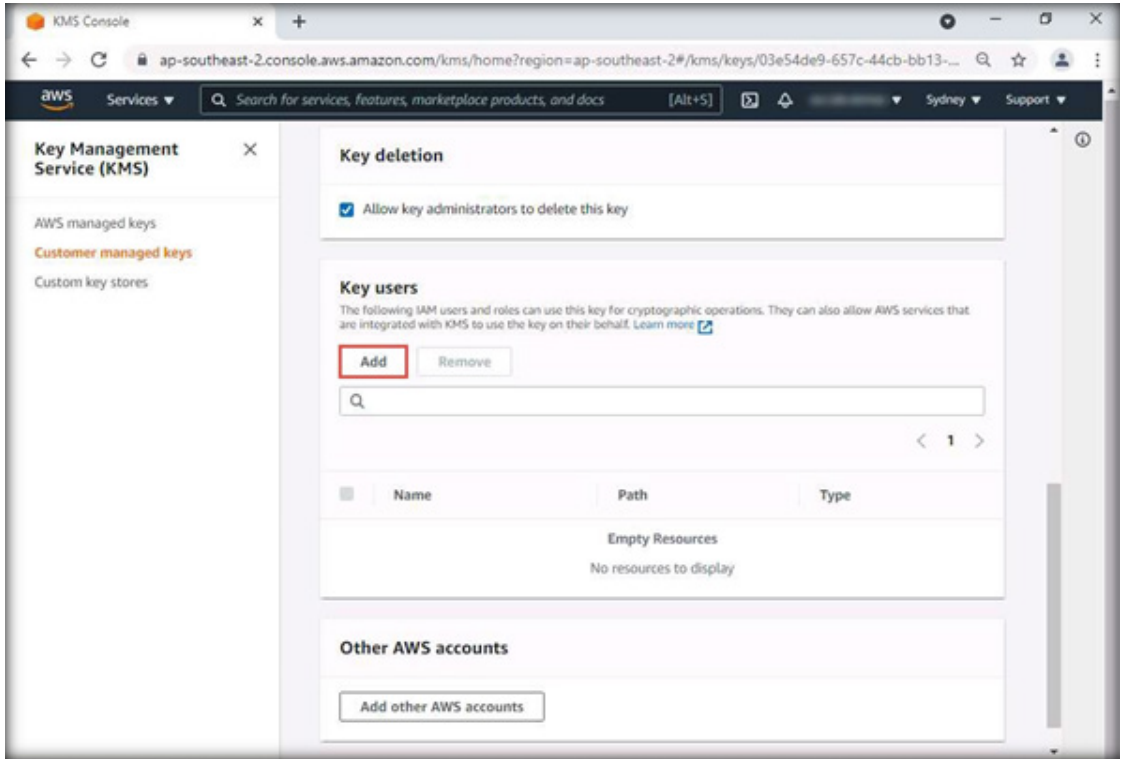
63. Once the KMS Console page appears, click on Customer managed keys (here CCT_User_MasterKey).



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

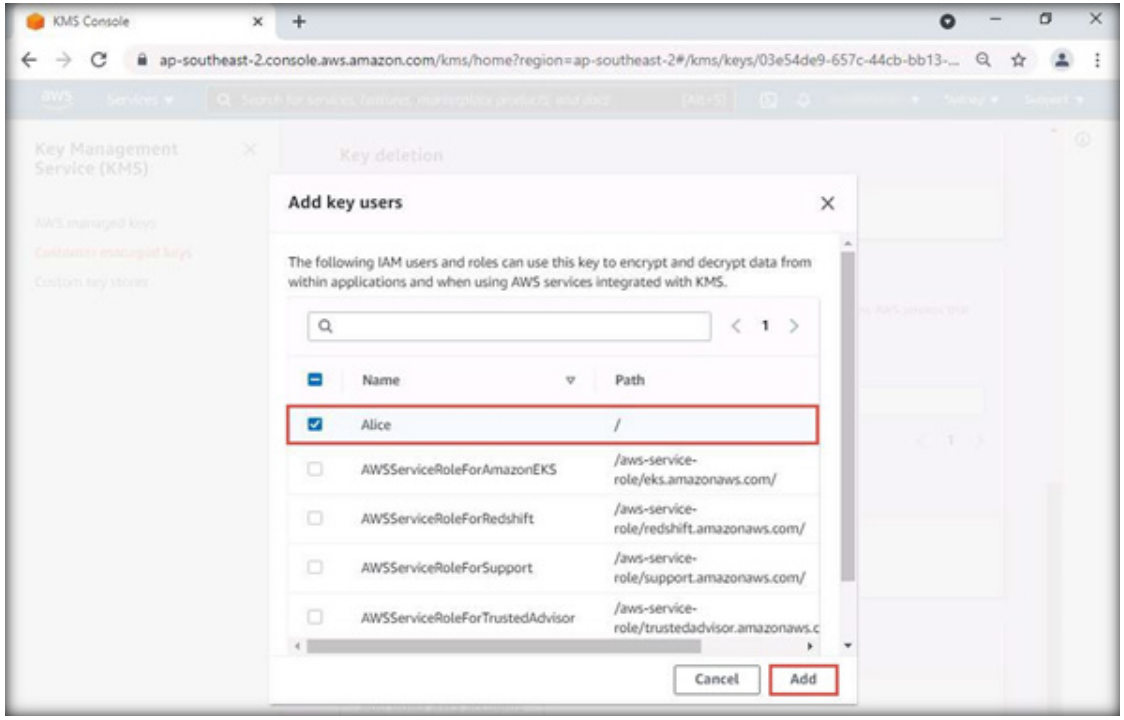
Copyrights @ 2022 EC-Council International Ltd.

64. Scroll down until the Key users section. Click on Add.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

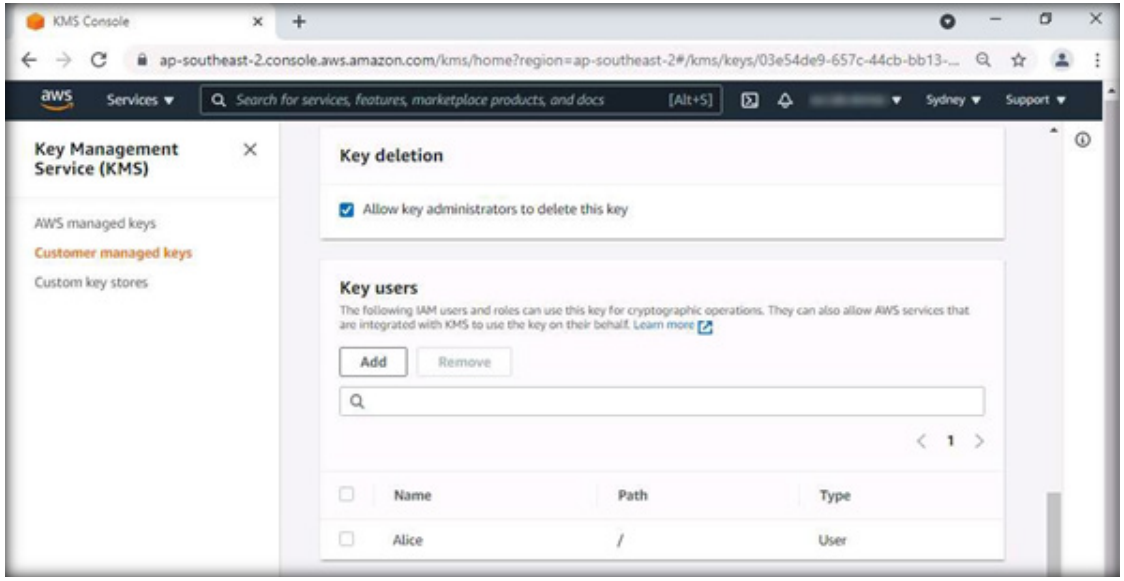
65. Use the search box to filter the IAM users. Type Alice as shown in the screenshot below and check Alice. We will add the IAM User Alice so that the user can access the Master Key. Click on Add.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

66. After you have added the user, it will appear as added in the Key users section.

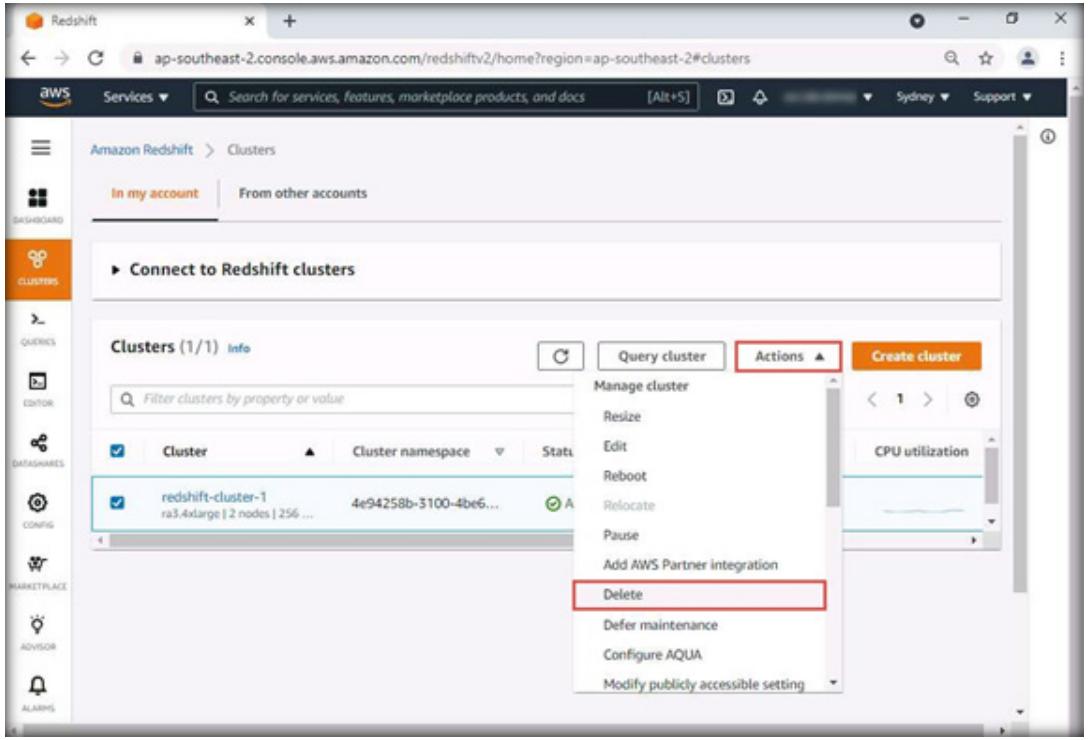


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

67. Thus, a security professional can implement AWS KMS.

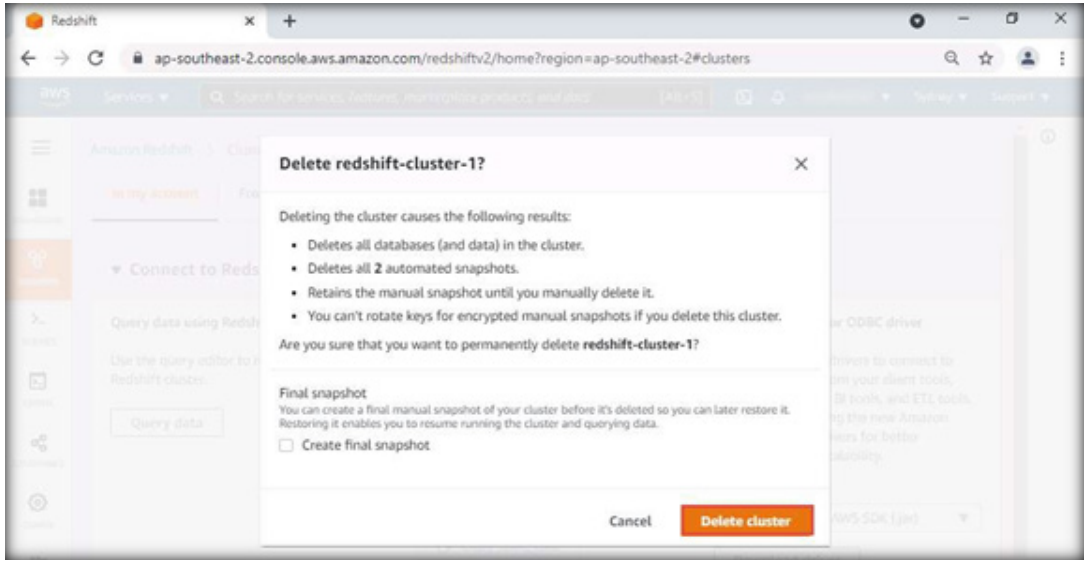
68. Now ensure that you delete the created cluster. To do this, type redshift in the main search bar and select Amazon Redshift.

69. Select the Clusters icon from AWS icon bar on the left. Select the created cluster from the list and click Actions from the drop-down menu. Click Delete.
Note: If the status of the cluster is still Modifying and Resizing wait for it to change to Available, then delete the Cluster.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

70. The Delete redshift-cluster-1 popup appears. Uncheck the Create Final Snapshot and click Delete cluster to delete the created cluster.



EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

Copyrights @ 2022 EC-Council International Ltd.

71. Log out from the AWS platform and close all open windows.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 5: **SECURE AMAZON WEB SERVICES STORAGE**

S3 buckets are used by customers and end-users to store text documents, PDFs, videos, images, etc.

LAB SCENARIO

In the cloud, data is stored on Internet-connected servers in data centres. It is important that security professionals understand and implement the data storage security features for data encryption and access management tools provided by service providers to secure the data stored in the data centres.

OBJECTIVE

This lab will demonstrate how to restrict access to S3 resources by creating bucket policies, Access Control Lists (ACLs), and IAM policies to provide access to selected entities.

In this lab, you will learn to do the following:

- Assign Permissions to Amazon S3 Using ACL
- Assign Permissions to Amazon S3 Using Bucket Policy

OVERVIEW OF AWS STORAGE

Amazon S3 allows upload and retrieval data at any time and from anywhere on the Internet. It stores data as objects (text file/photo/video) within buckets. In the default state, all the Amazon S3 buckets are accessed by authorized users. Restrict access to S3 resources by combining bucket policies, ACLs and IAM polices to give access to the right entities.

Copyrights @ 2022 EC-Council International Ltd.

Note: Before starting this lab, you should create an AWS account using the following: https://portal.aws.amazon.com/billing/signup. Once the registration is completed, perform the following tasks.
Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, double-click on the Google Chrome icon on the Desktop to open the browser.

2. The Google Chrome browser opens. Go to the address bar, type https://aws.amazon.com/, and press Enter.
Note: If you are already logged in, skip the login steps.

3. The AWS Web Services - Cloud Computing Services page appears. Click on AWS Management Console from the My Account drop-down menu as shown in the screenshot below.

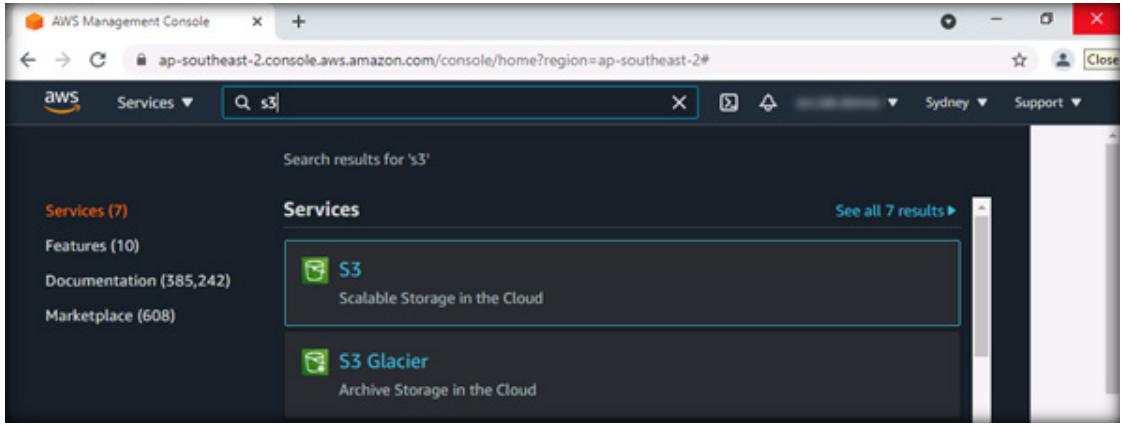
4. The AWS Web Services Sign-in page appears. Type the AWS administrator account ID, and click on Next.
Note: In the next window, type the characters seen in the image and click on submit.

EXERCISE 5:
SECURE AMAZON WEB SERVICES STORAGE

Copyrights @ 2022 EC-Council International Ltd.

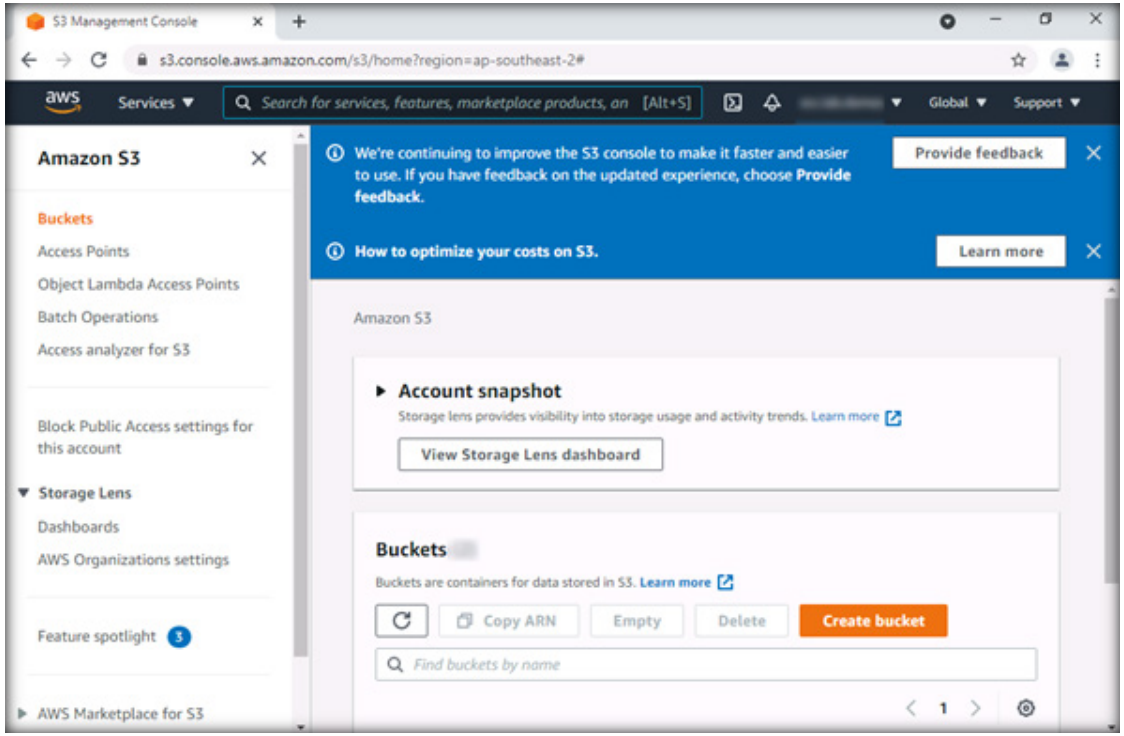
5. In the Password field, type the password, and click on Sign-in.

6. Click on Services. In the search field, type S3, and then click on S3 Scalable Storage in the Cloud from the search results.



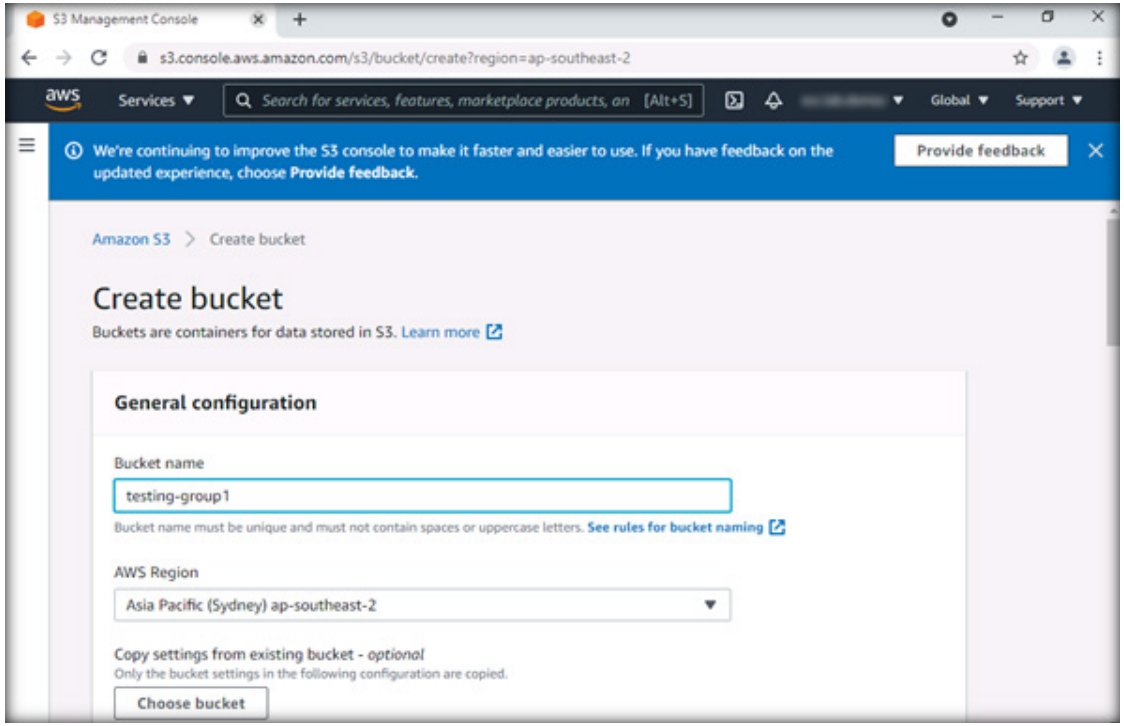
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

7. The S3 buckets page appears. Click on Create bucket.



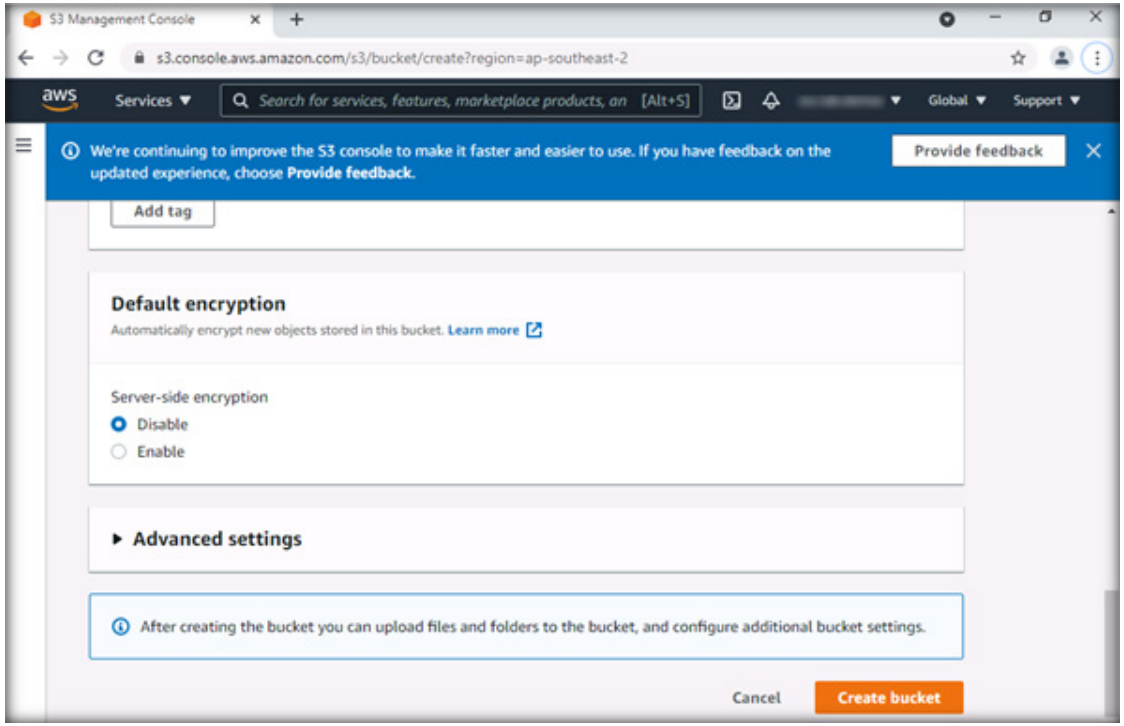
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

8. The Create bucket pop-up appears. Under General configuration, type the name of the bucket in the Bucket name field (here, the bucket name is testing-group1), and retain the other default settings.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

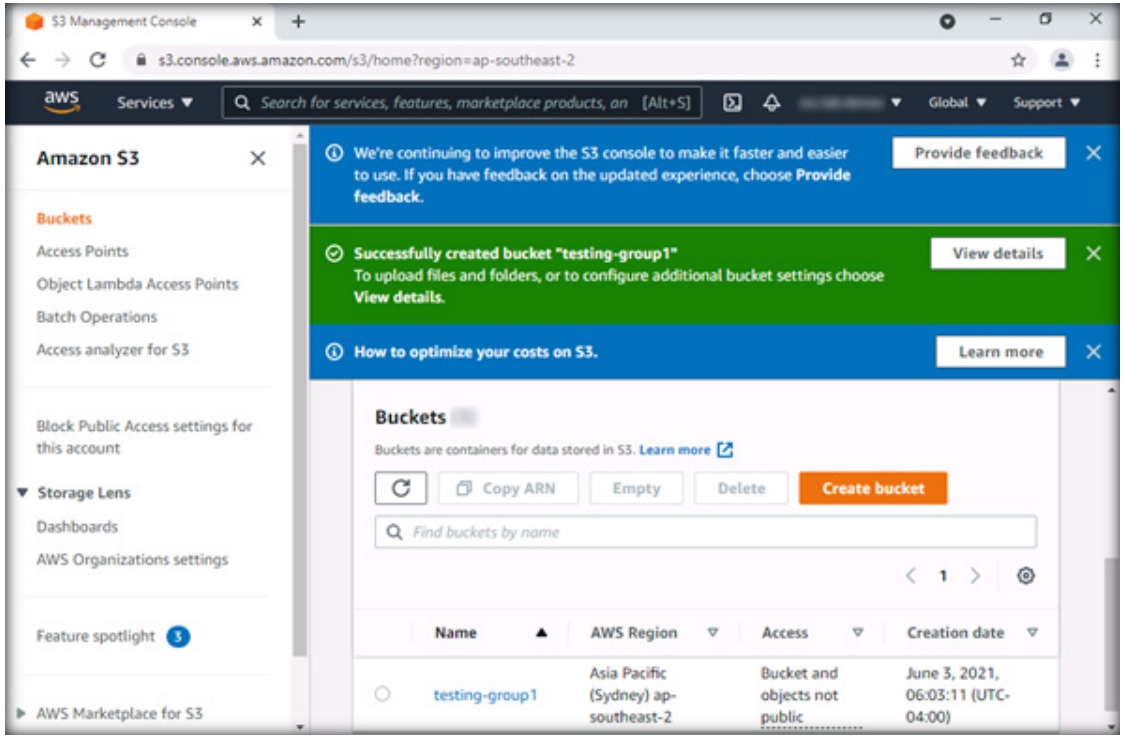
9. Retain default settings for all other sections, scroll down and click on Create bucket.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

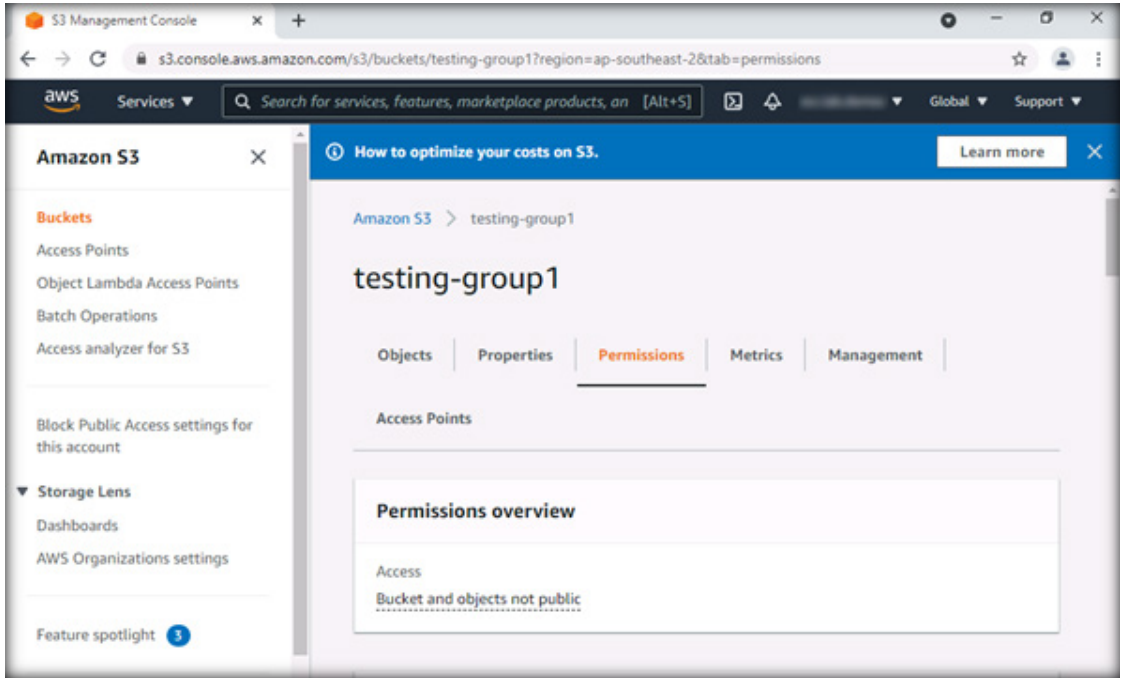
10. The new bucket is created.

11. Select the testing-group1 S3 bucket.



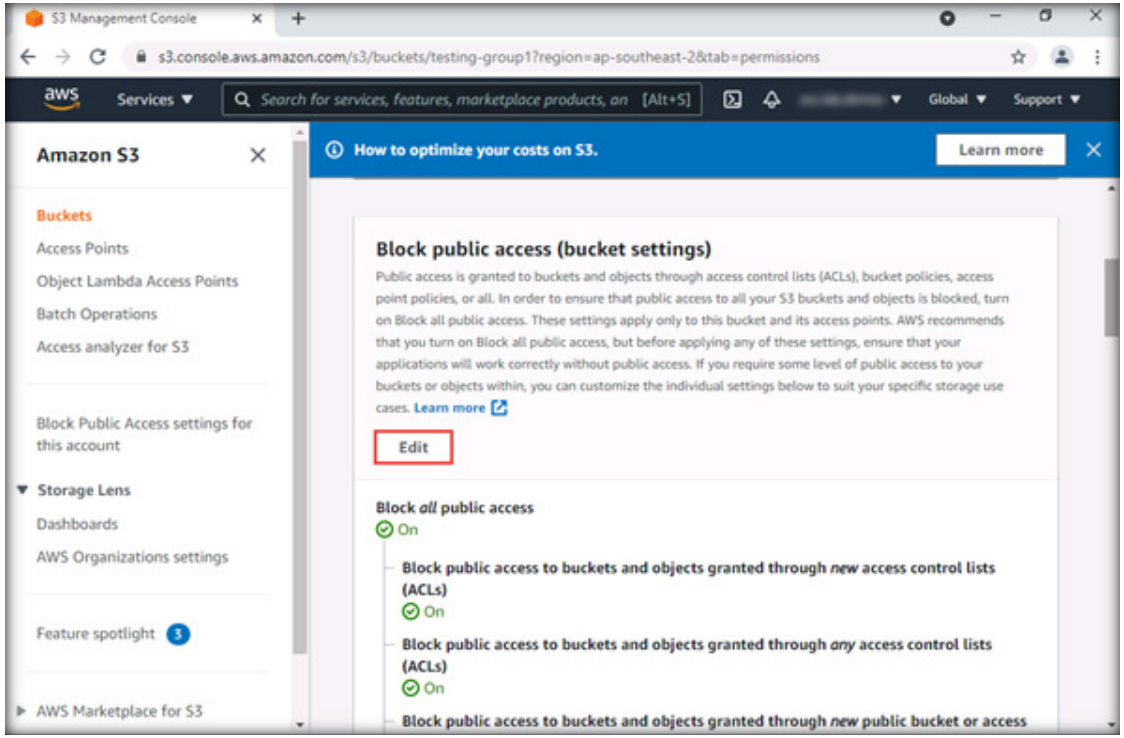
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

12. The Amazon S3 > testing-group1 page appears. Click on the Permissions tab.



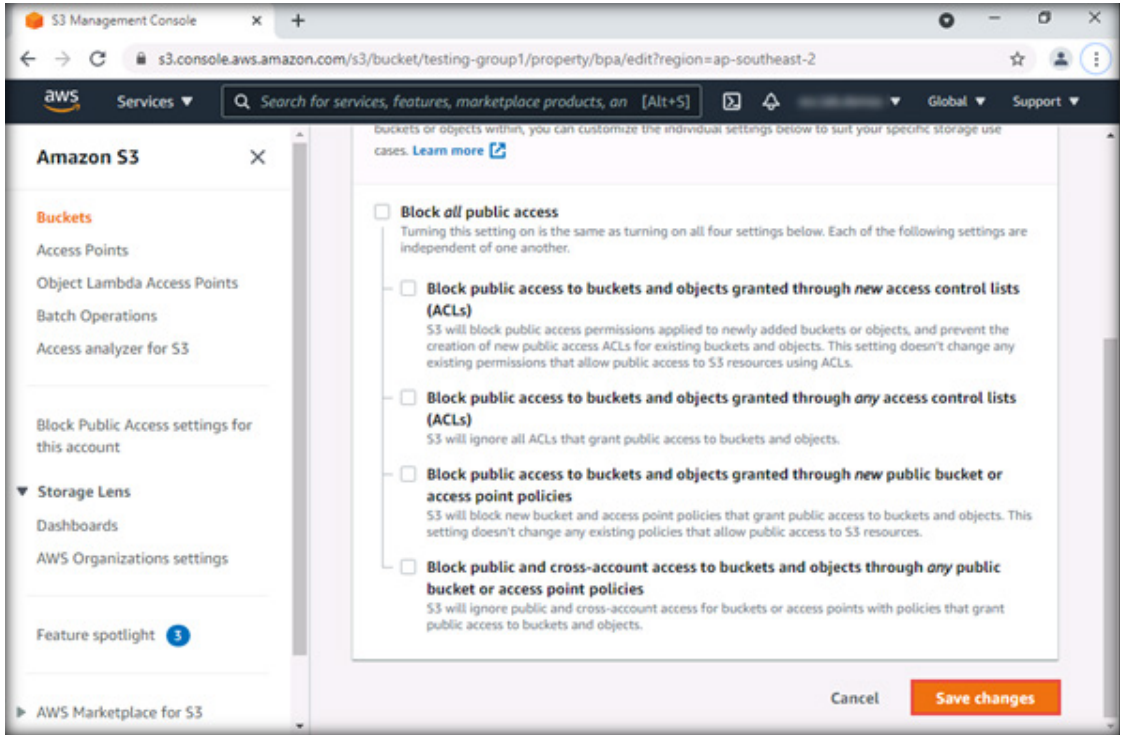
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

13. By default, the Block all public access tab is selected; click on Edit.



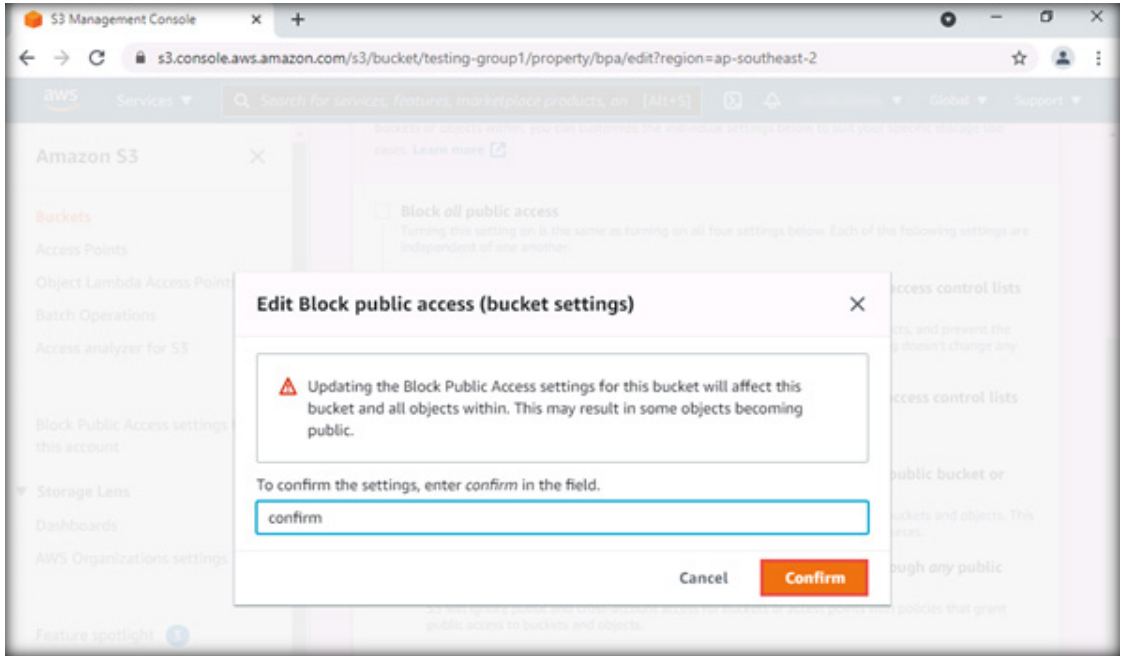
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

14. Uncheck Block all public access and click on Save changes.



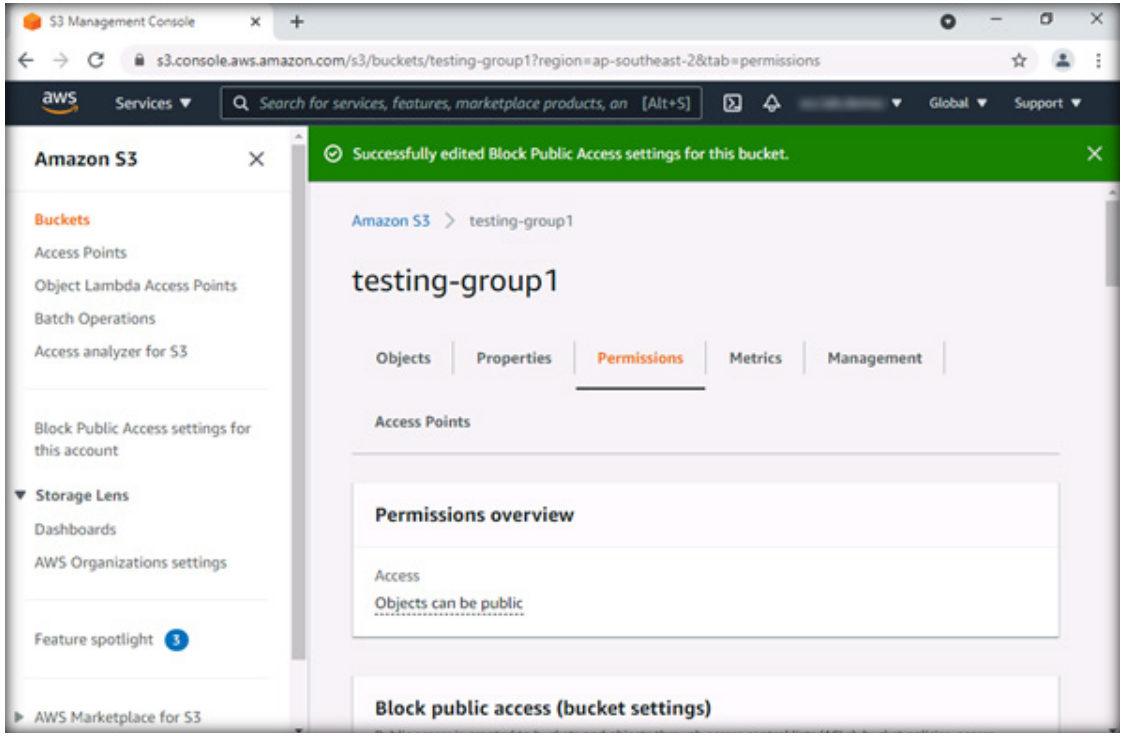
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

15. The confirmation dialog appears. Type confirm and click on Confirm.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

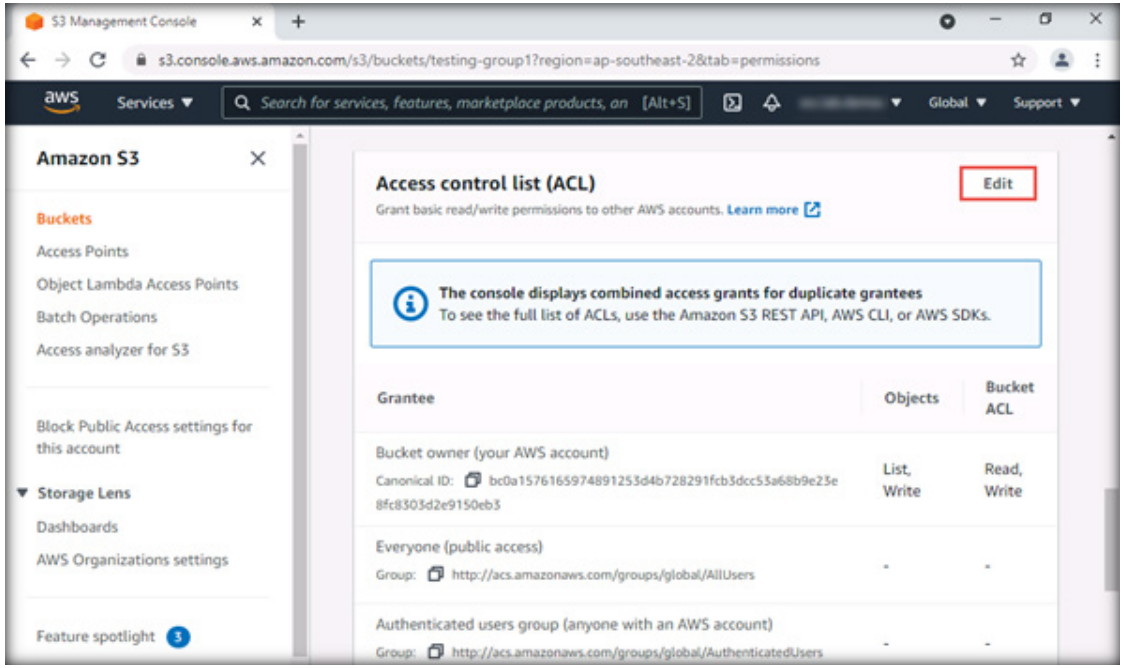
16. The Successfully edited Block Public Access settings for this bucket message appears.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

Copyrights @ 2022 EC-Council International Ltd.

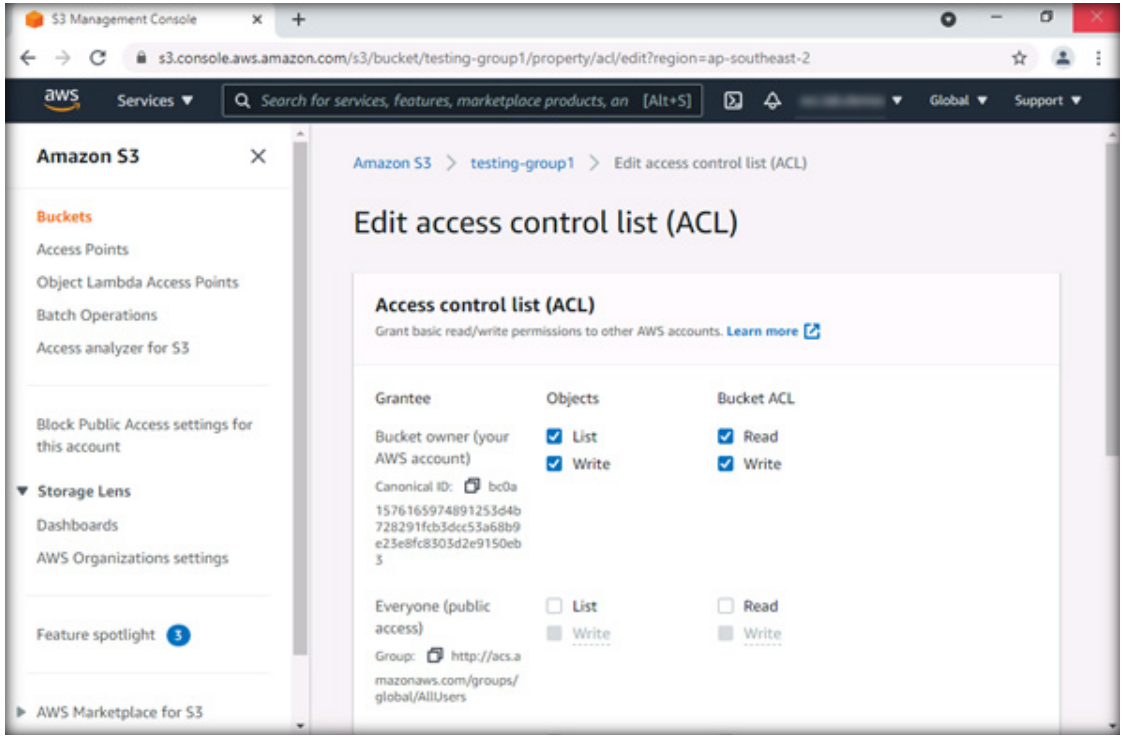
17. Next, scroll down to Access control List under the Permissions tab and click on Edit.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

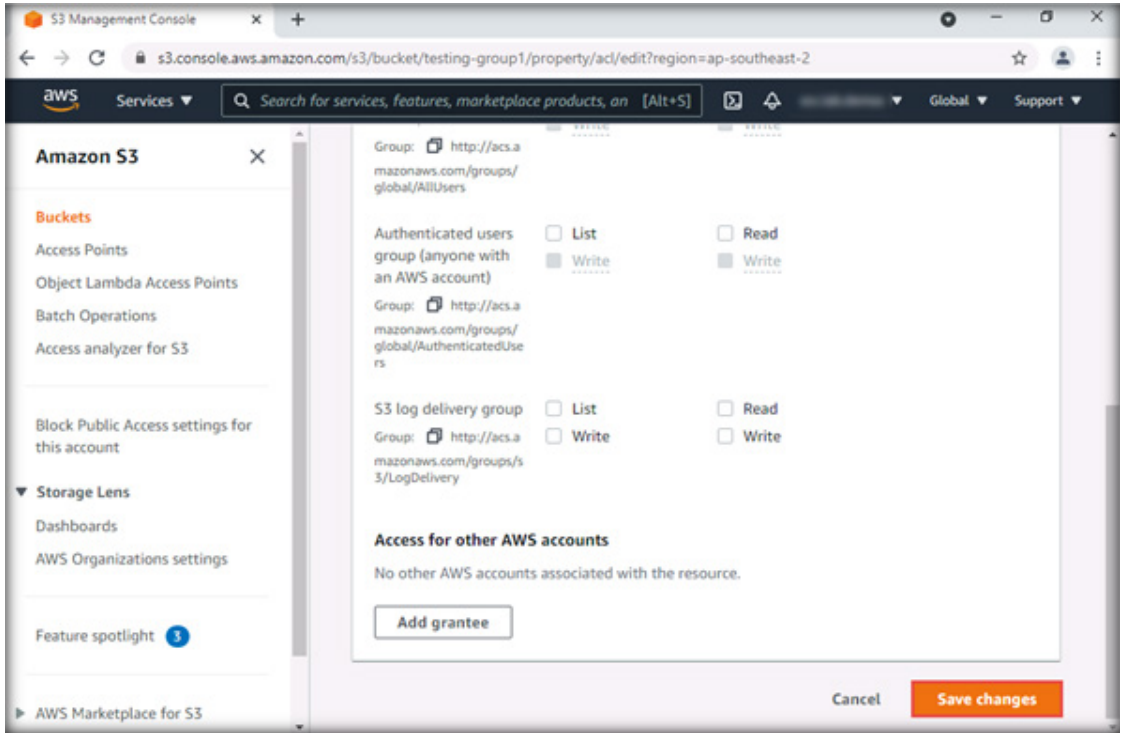
Copyrights @ 2022 EC-Council International Ltd.

18. In the Edit access control list (ACL) window, we will set all permissions to our ACL on our AWS account, under the Bucket owner section ensure that all the permissions are checked under Objects and Bucket ACL.



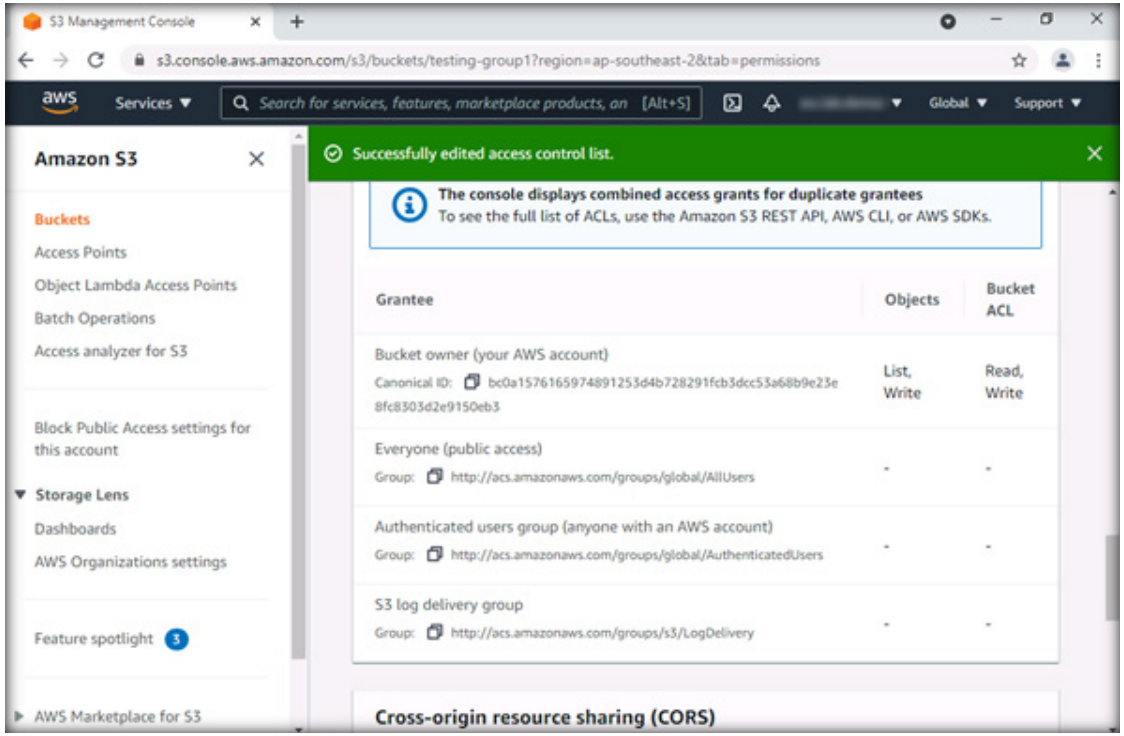
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

19. Scroll down and click on Save changes to apply the permissions on the AWS account.



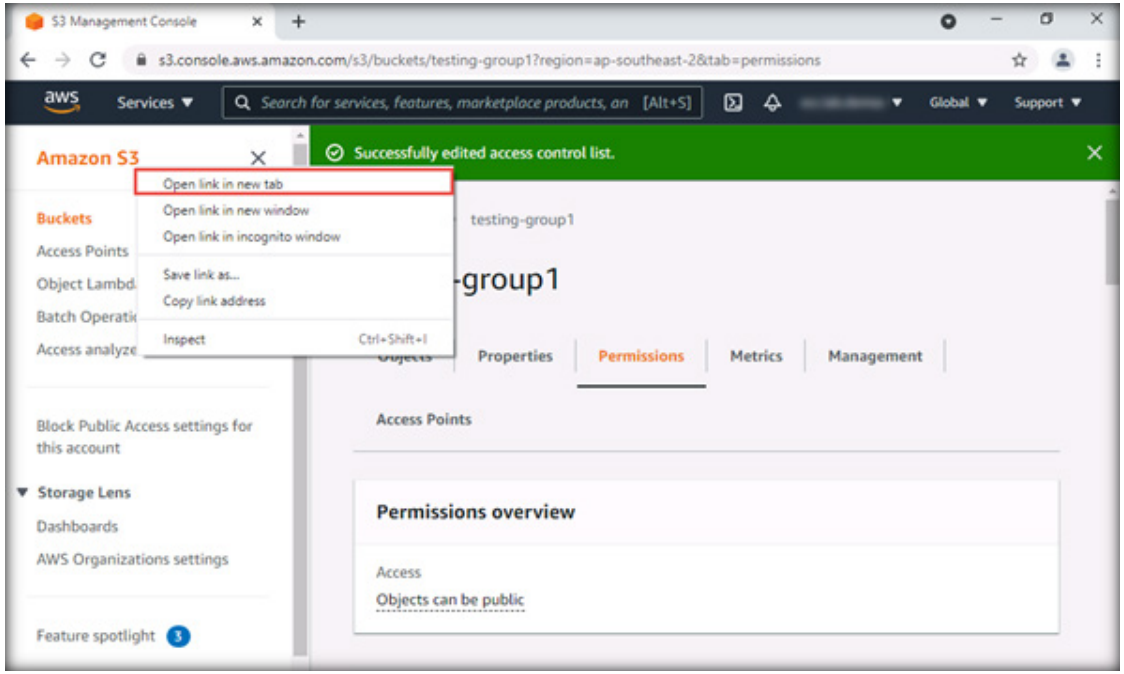
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

20. Public access settings have been updated successfully.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

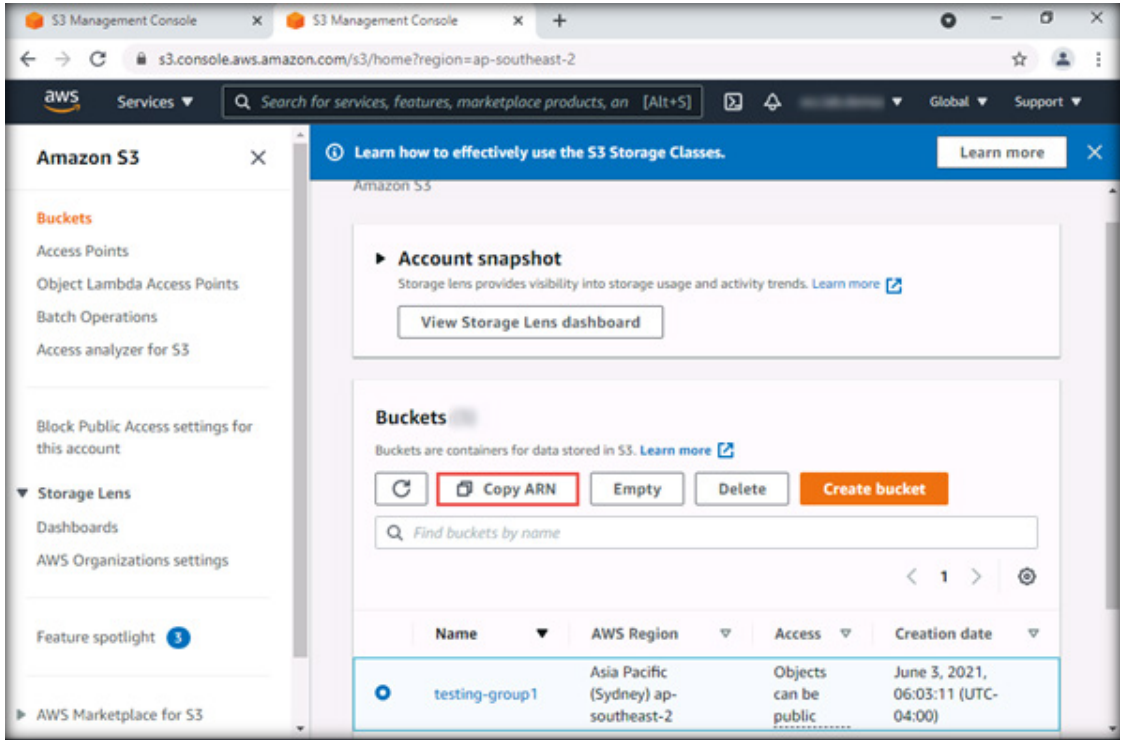
21. We have created a bucket policy with the name testing-group1. We need the ARN of the bucket policy. Right-click on Amazon S3 in the left corner and click on Open link in new tab.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

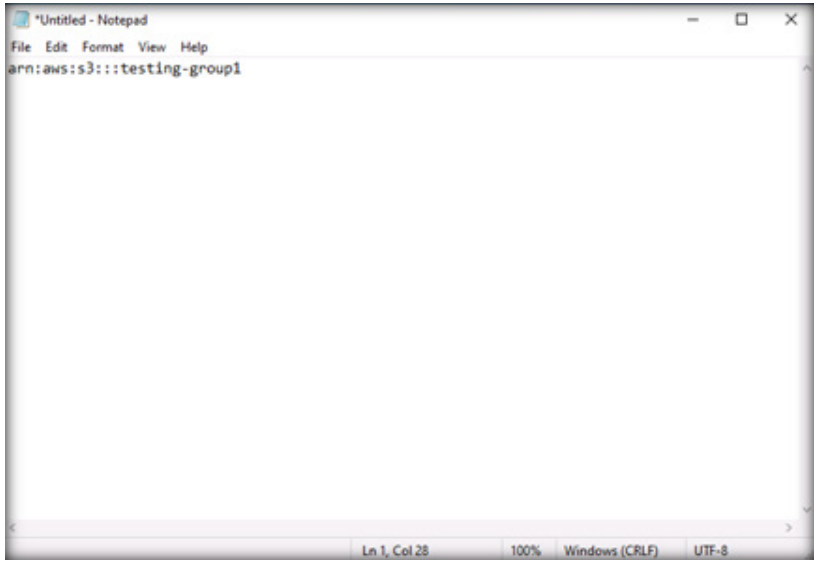
Copyrights @ 2022 EC-Council International Ltd.

22. Check the bucket for which you want to know the ARN number (here, testing-group1). The details of testing-group1 appear. Click on Copy ARN.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

23. Open Notepad and paste the copied ARN into it.

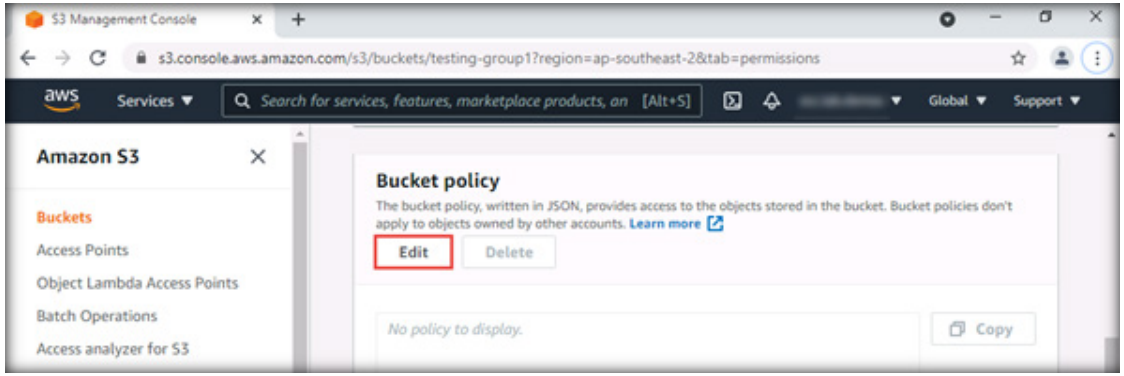


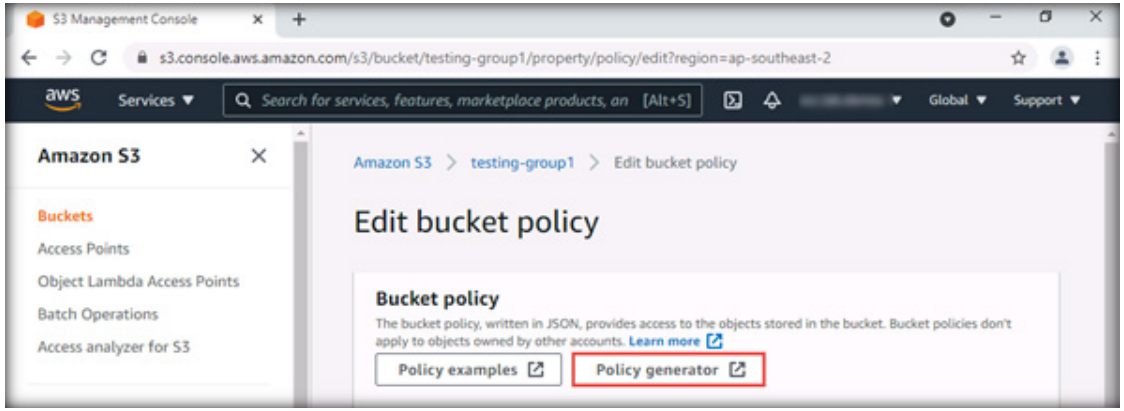
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

24. Switch to the browser and close the second browser tab. You will return to the first browser tab.

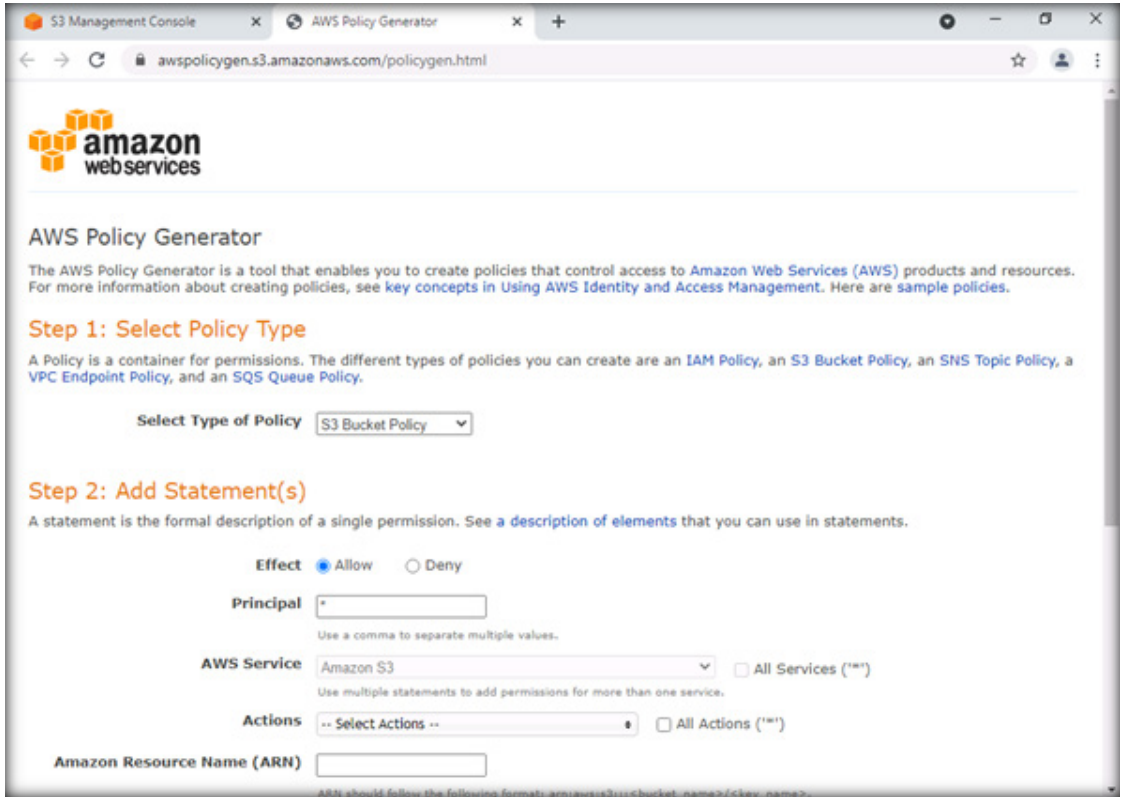
25. Scroll down to Bucket Policy under the Permissions tab and click on Edit and click on Policy generator link. A new tab of the browser opens switch to a new tab.

EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE





26. The AWS Policy Generator page appears, as shown in the screenshot below. Set Select Type of Policy to S3 Bucket Policy. Set Effect to Allow. In the Principal field, let us specify a wildcard ("*") to allow all principals for now. Set AWS Service to Amazon S3.

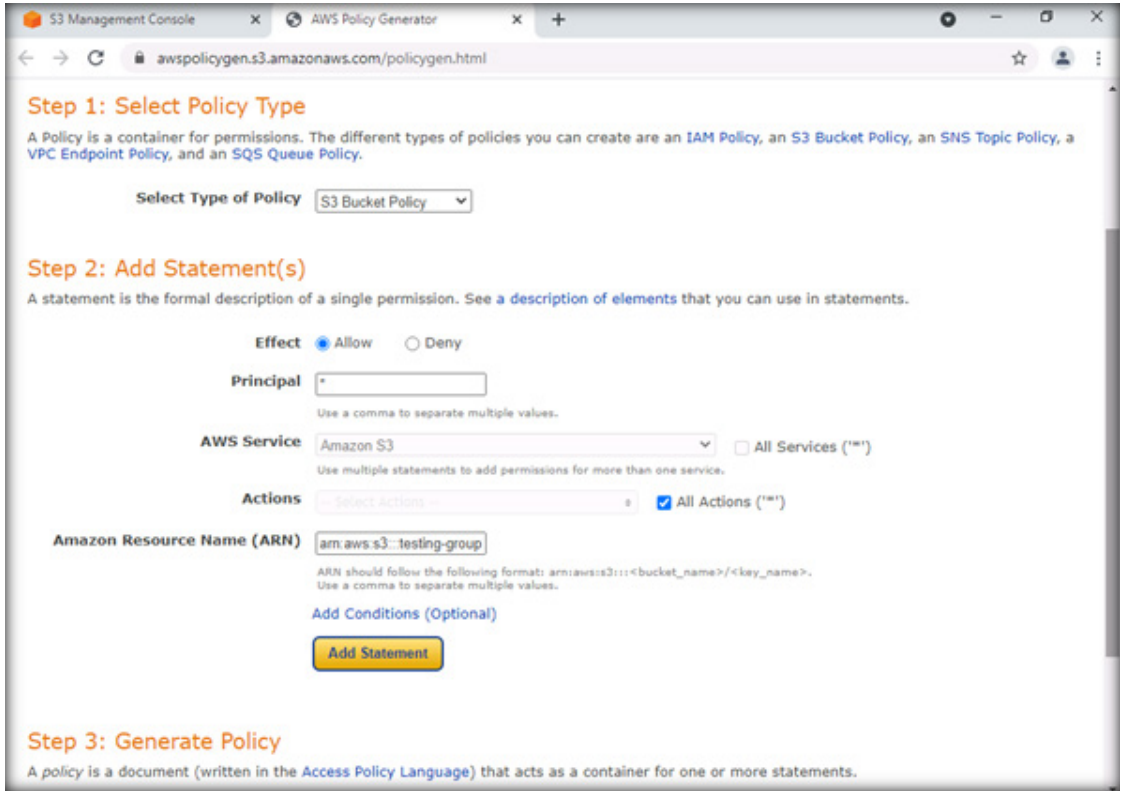


EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

27. Switch to Notepad and copy the ARN that we have pasted.

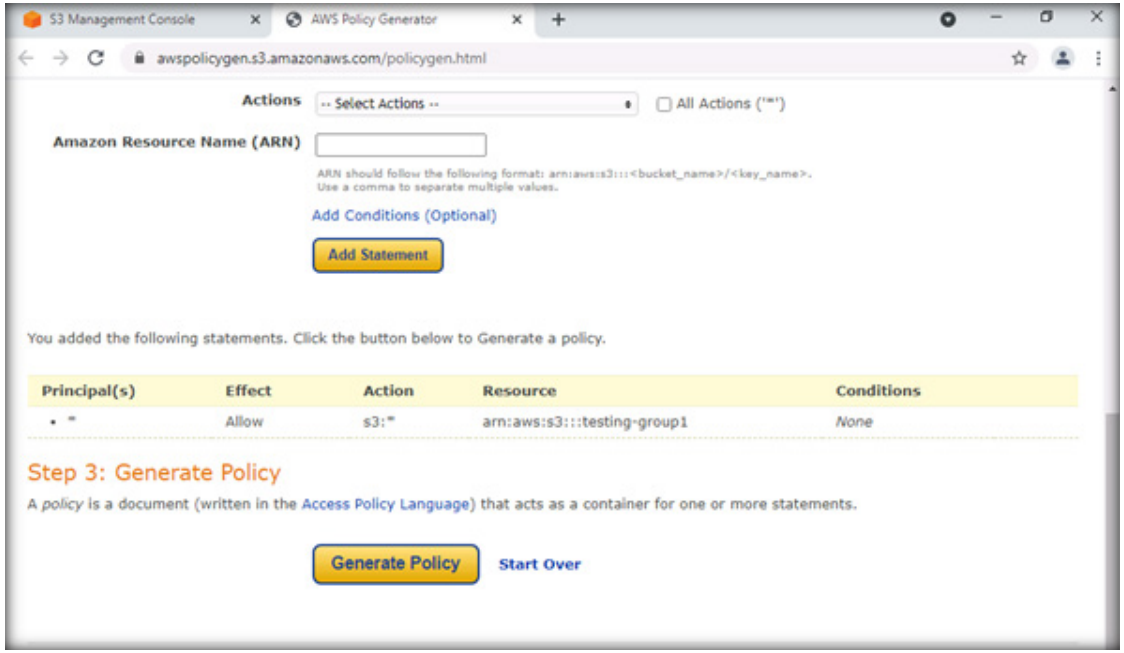
EXERCISE 5:
SECURE AMAZON
WEB SERVICES
STORAGE

28. Go to the browser and check the All Actions checkbox, paste the copied ARN value in the Amazon Resource Name (ARN) field, and click on Add Statement.



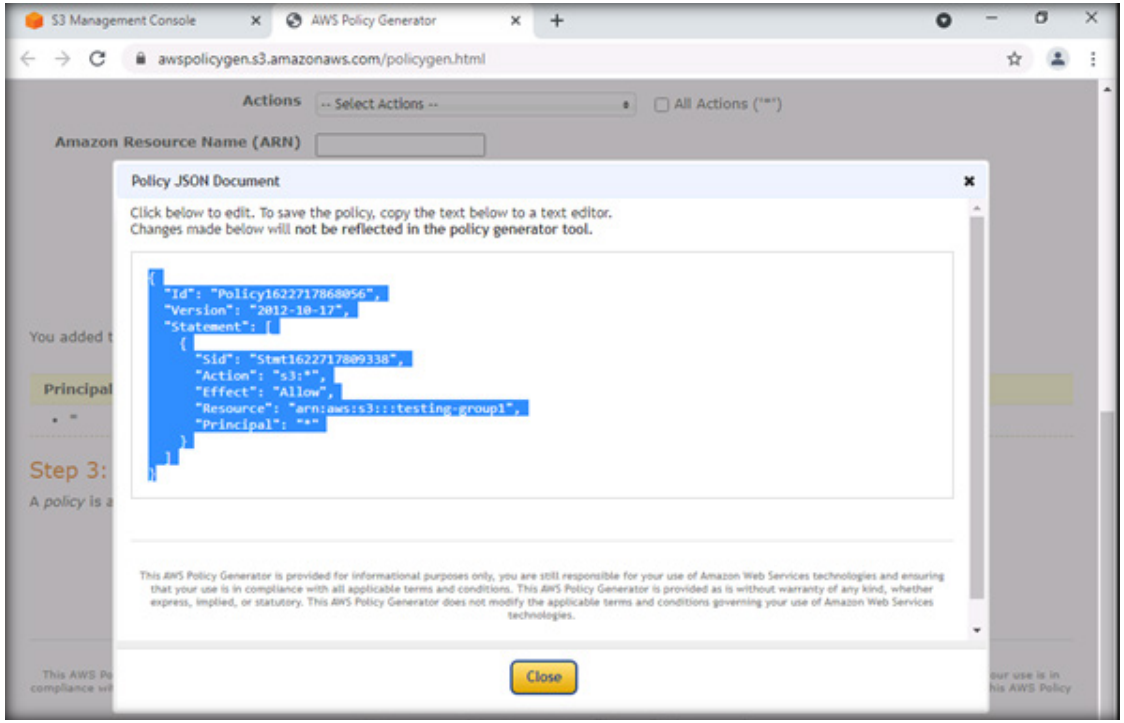
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

29. Once the statement is added, click on Generate Policy in the Step 3: Generate Policy section.



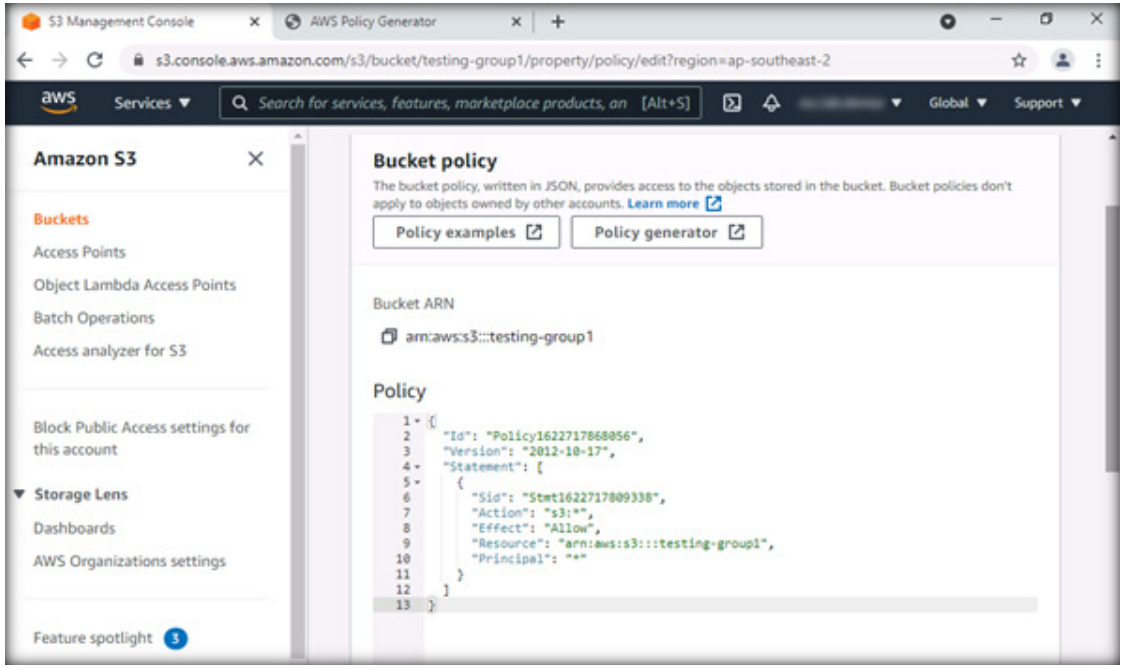
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

30. The Policy JSON Document pop-up appears, along with the generated JSON code. Copy the code as shown in the screenshot below and click on Close.



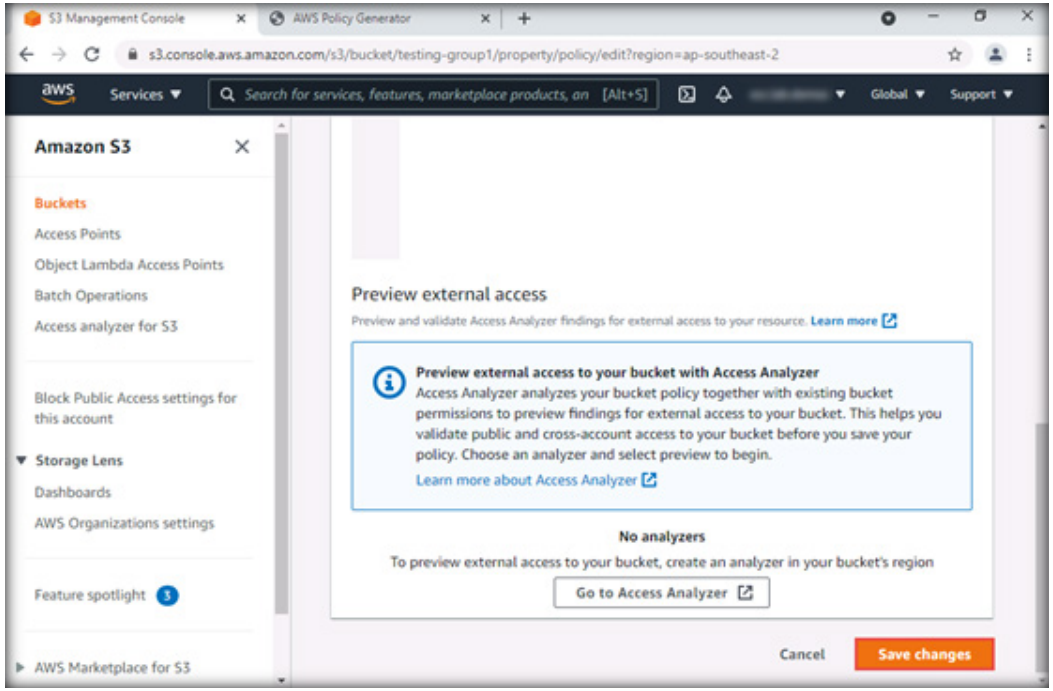
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

31. Switch to the first tab of the web browser S3 Management Console to configure Bucket Policy. Paste the copied JSON code from the Bucket policy editor, scroll down and click on Save changes.



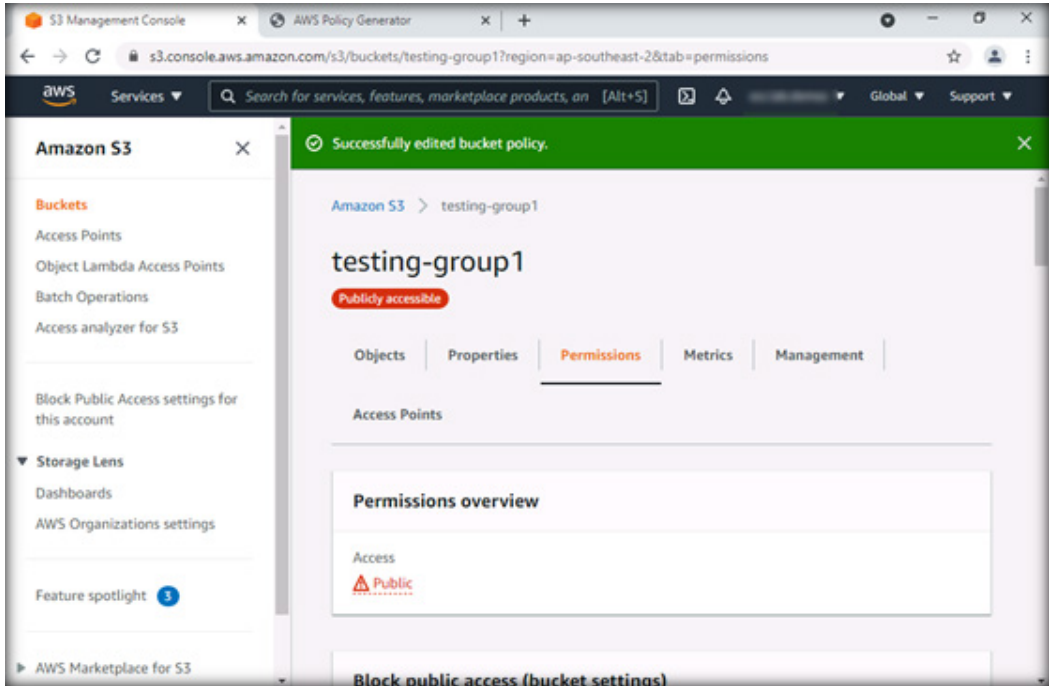
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE



Copyrights @ 2022 EC-Council International Ltd.

32. Now the bucket has public access.



EXERCISE 5:
SECURE AMAZON
WEB SERVICES
STORAGE

33. As described above, the security professional can assign permissions to S3 using bucket policy.

34. Log out from the AWS platform and close all open windows.

35. Turn off Admin Machine-1 and PfSense Firewall virtual machines.

Copyrights @ 2022 EC-Council International Ltd.


EC-Council