

CHAPTER 10

VIRTUALIZATION AND CLOUD COMPUTING



CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 10:

Virtualization and Cloud Computing

Exercise 1: Audit Docker Host Security using Docker-Bench-Security Tool	05

Exercise 2: Create IAM Credentials on Google Cloud Platform	21

Exercise 3: Implement AWS Identity and Access Management	42

Exercise 4: Implement Key Management Services in AWS	87

Exercise 5: Secure Amazon Web Services Storage	146

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.

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.

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:

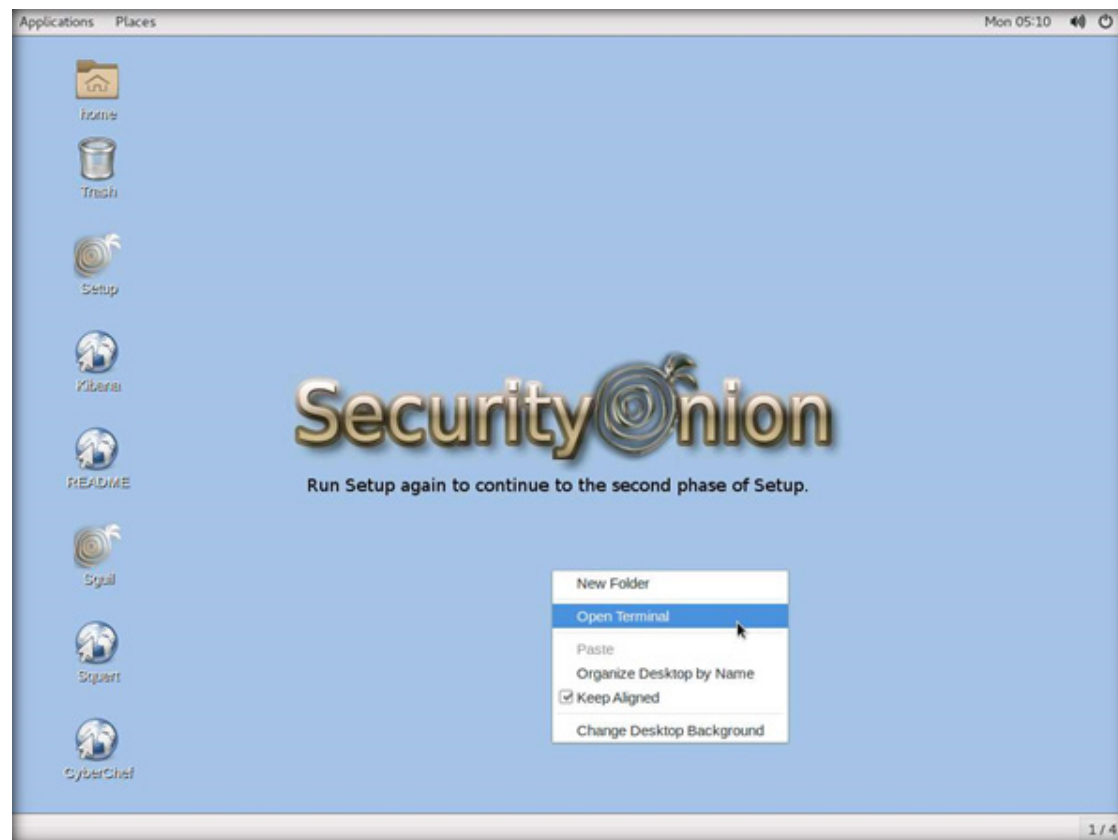
- Install Docker on Ubuntu OS
- Audit Docker Security using Docker-Bench-Security Tool

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.

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.

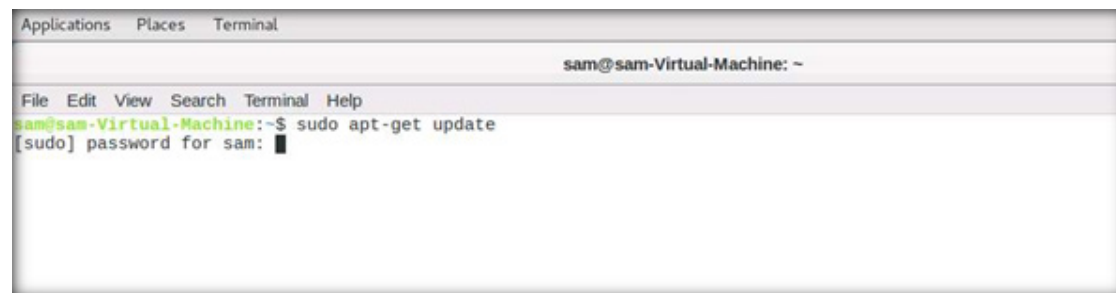


EXERCISE 1: AUDIT DOCKER HOST SECURITY USING DOCKER- BENCH-SECURITY TOOL

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.



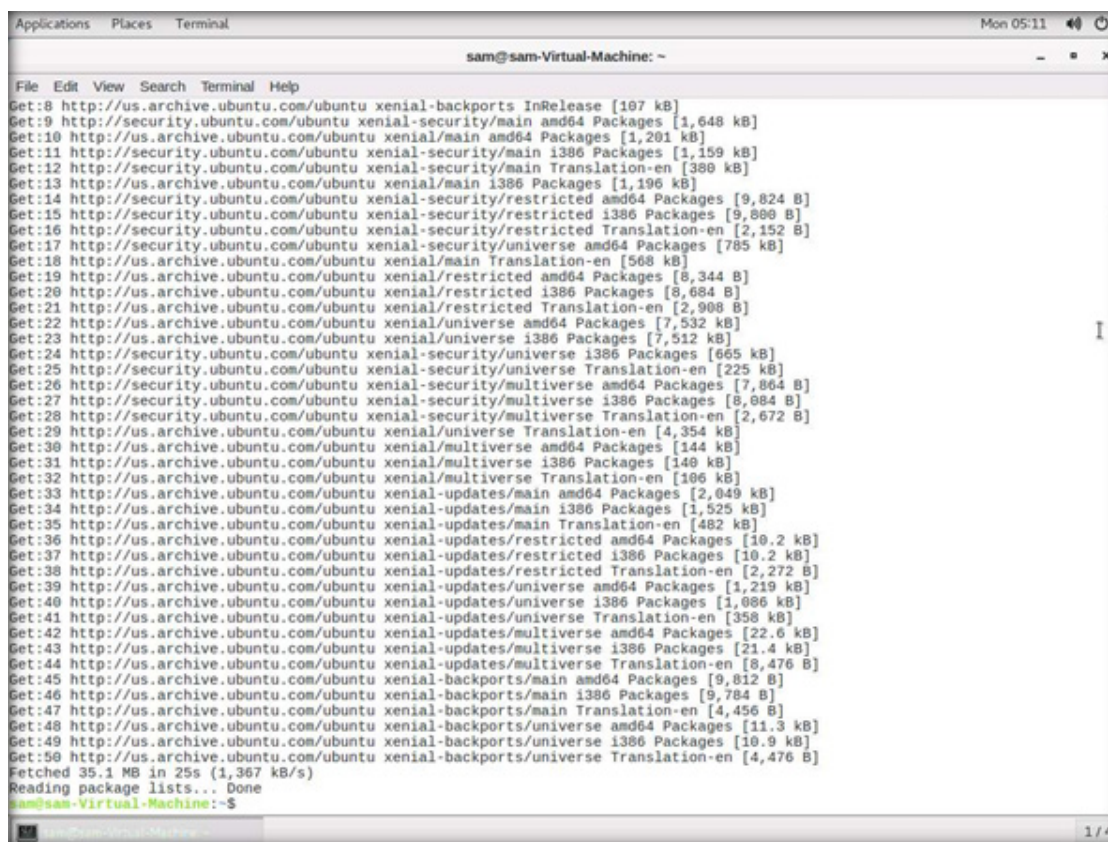
```
Applications  Places  Terminal

sam@sam-Virtual-Machine: ~

File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo apt-get update
[sudo] password for sam: 
```

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

6. System update will be successfully completed.



```
Applications Places Terminal Mon 05:11
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
Get:8 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1,648 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [1,159 kB]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [380 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu xenial/main i386 Packages [1,196 kB]
Get:14 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [9,824 B]
Get:15 http://security.ubuntu.com/ubuntu xenial-security/restricted i386 Packages [9,880 B]
Get:16 http://security.ubuntu.com/ubuntu xenial-security/restricted Translation-en [2,152 B]
Get:17 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [785 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu xenial/main Translation-en [568 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [8,344 B]
Get:20 http://us.archive.ubuntu.com/ubuntu xenial/restricted i386 Packages [8,684 B]
Get:21 http://us.archive.ubuntu.com/ubuntu xenial/restricted Translation-en [2,908 B]
Get:22 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu xenial/universe i386 Packages [7,512 kB]
Get:24 http://security.ubuntu.com/ubuntu xenial-security/universe i386 Packages [665 kB]
Get:25 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [225 kB]
Get:26 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [7,864 B]
Get:27 http://security.ubuntu.com/ubuntu xenial-security/multiverse i386 Packages [8,084 B]
Get:28 http://security.ubuntu.com/ubuntu xenial-security/multiverse Translation-en [2,672 B]
Get:29 http://us.archive.ubuntu.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:30 http://us.archive.ubuntu.com/ubuntu xenial/multiverse amd64 Packages [144 kB]
Get:31 http://us.archive.ubuntu.com/ubuntu xenial/multiverse i386 Packages [140 kB]
Get:32 http://us.archive.ubuntu.com/ubuntu xenial/multiverse Translation-en [106 kB]
Get:33 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [2,049 kB]
Get:34 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [1,525 kB]
Get:35 http://us.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [482 kB]
Get:36 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packages [10.2 kB]
Get:37 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted i386 Packages [10.2 kB]
Get:38 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted Translation-en [2,272 B]
Get:39 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [1,219 kB]
Get:40 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [1,086 kB]
Get:41 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [358 kB]
Get:42 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Packages [22.6 kB]
Get:43 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse i386 Packages [21.4 kB]
Get:44 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translation-en [8,476 B]
Get:45 http://us.archive.ubuntu.com/ubuntu xenial-backports/main amd64 Packages [9,812 B]
Get:46 http://us.archive.ubuntu.com/ubuntu xenial-backports/main i386 Packages [9,784 B]
Get:47 http://us.archive.ubuntu.com/ubuntu xenial-backports/main Translation-en [4,456 B]
Get:48 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Packages [11.3 kB]
Get:49 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe i386 Packages [10.9 kB]
Get:50 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe Translation-en [4,476 B]
Fetched 35.1 MB in 25s (1,367 kB/s)
Reading package lists... Done
sam@sam-Virtual-Machine:~$
```

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

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.



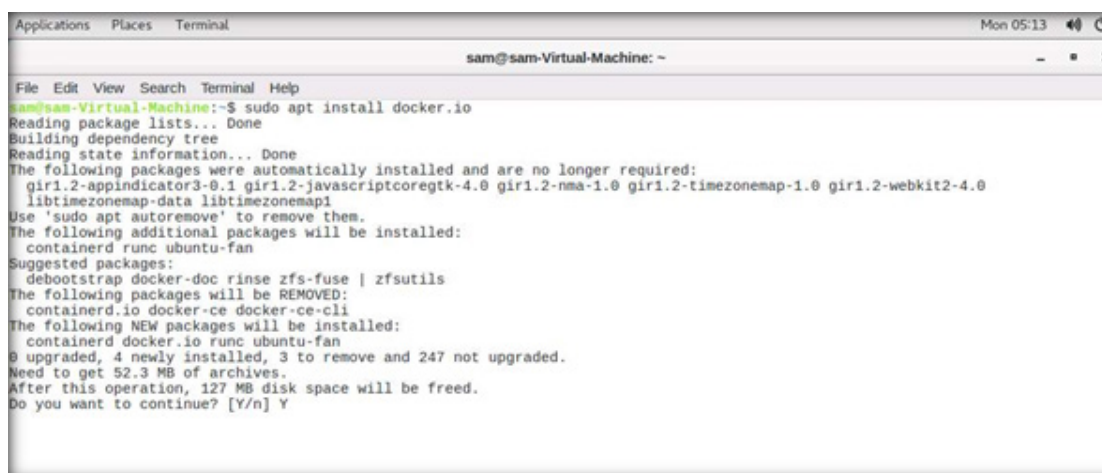
```
Applications  Places  Terminal  Mon
sam@sam-Virtual-Machine: ~

File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo apt-get remove docker docker-engine docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'docker-engine' is not installed, so not removed
Package 'docker' is not installed, so not removed
Package 'docker.io' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timzonemap-1.0 gir1.2-webkit2-4.0
  libtimzonemap-data libtimzonemap1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 247 not upgraded.
sam@sam-Virtual-Machine:~$
```

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

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

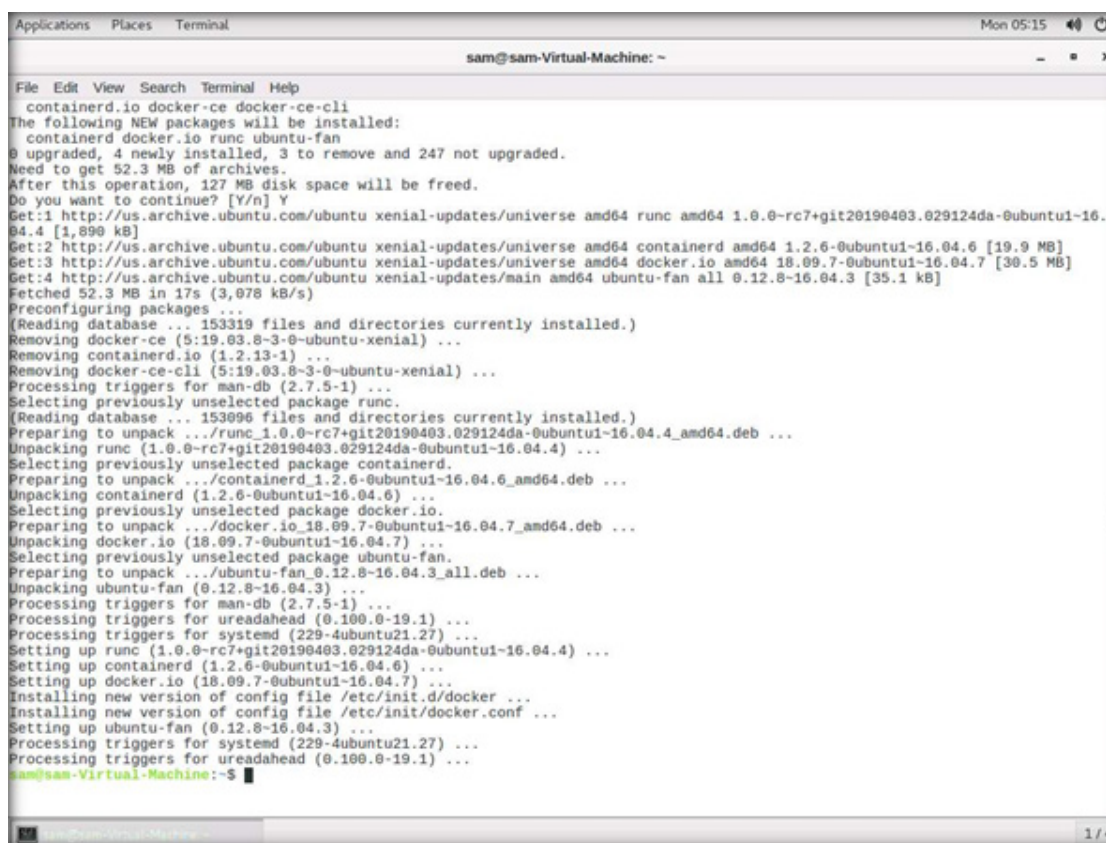
10. If prompted whether to continue, type Y to continue as shown in the screenshot below.



```
Applications  Places  Terminal
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timezonemap-1.0 gir1.2-webkit2-4.0
  libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  containerd runc ubuntu-fan
Suggested packages:
  debootstrap docker-doc rinse zfs-fuse | zfsutils
The following packages will be REMOVED:
  containerd.io docker-ce docker-ce-cli
The following NEW packages will be installed:
  containerd docker.io runc ubuntu-fan
0 upgraded, 4 newly installed, 3 to remove and 247 not upgraded.
Need to get 52.3 MB of archives.
After this operation, 127 MB disk space will be freed.
Do you want to continue? [Y/n] Y
```

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

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



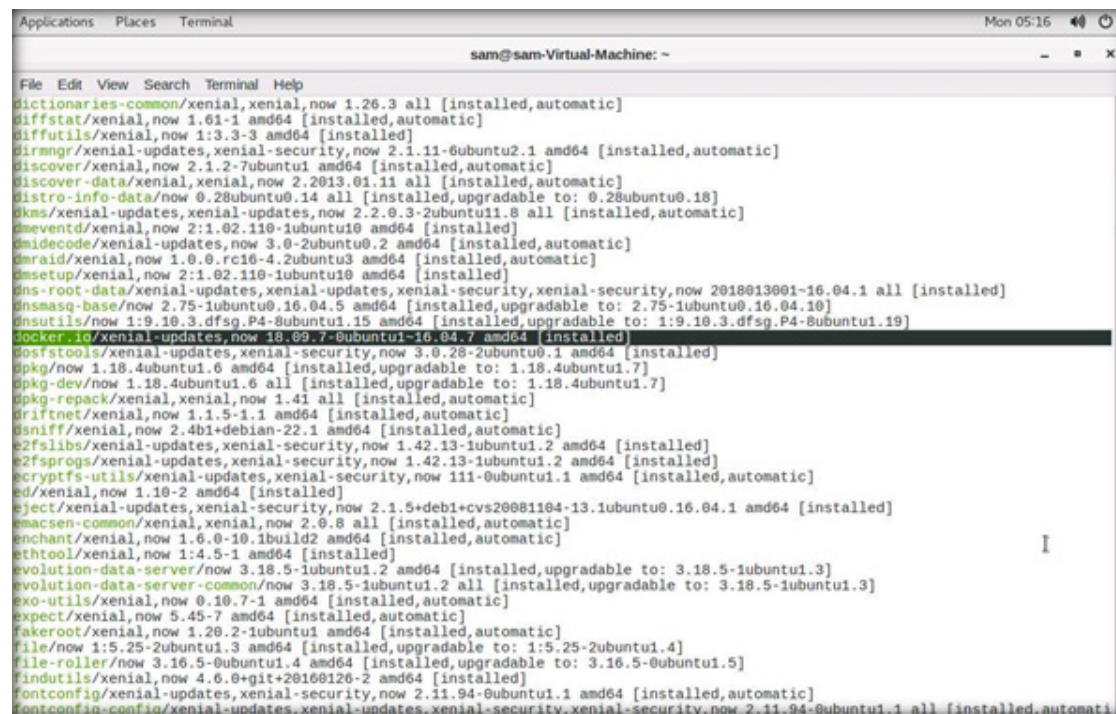
```

Applications  Places  Terminal
sam@sam-Virtual-Machine: ~

File Edit View Search Terminal Help
containerd.io docker-ce docker-ce-cli
The following NEW packages will be installed:
containerd docker.io runc ubuntu-fan
0 upgraded, 4 newly installed, 3 to remove and 247 not upgraded.
Need to get 52.3 MB of archives.
After this operation, 127 MB disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 runc amd64 1.0.0-rc7+git20190403.029124da-0ubuntu1-16.04.4 [1,890 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 containerd amd64 1.2.6-0ubuntu1-16.04.6 [19.9 MB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 docker.io amd64 18.09.7-0ubuntu1-16.04.7 [30.5 MB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 ubuntu-fan all 0.12.8-16.04.3 [35.1 kB]
Fetched 52.3 MB in 17s (3,078 kB/s)
Preconfiguring packages ...
(Reading database ... 153319 files and directories currently installed.)
Removing docker-ce (5:19.03.8-3-0-ubuntu-xenial) ...
Removing containerd.io (1.2.13-1) ...
Removing docker-ce-cli (5:19.03.8-3-0-ubuntu-xenial) ...
Processing triggers for man-db (2.7.5-1) ...
Selecting previously unselected package runc.
(Reading database ... 153096 files and directories currently installed.)
Preparing to unpack .../runc_1.0.0-rc7+git20190403.029124da-0ubuntu1-16.04.4_amd64.deb ...
Unpacking runc (1.0.0-rc7+git20190403.029124da-0ubuntu1-16.04.4) ...
Selecting previously unselected package containerd.
Preparing to unpack .../containerd_1.2.6-0ubuntu1-16.04.6_amd64.deb ...
Unpacking containerd (1.2.6-0ubuntu1-16.04.6) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../docker.io_18.09.7-0ubuntu1-16.04.7_amd64.deb ...
Unpacking docker.io (18.09.7-0ubuntu1-16.04.7) ...
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../ubuntu-fan_0.12.8-16.04.3_all.deb ...
Unpacking ubuntu-fan (0.12.8-16.04.3) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.27) ...
Setting up runc (1.0.0-rc7+git20190403.029124da-0ubuntu1-16.04.4) ...
Setting up containerd (1.2.6-0ubuntu1-16.04.6) ...
Setting up docker.io (18.09.7-0ubuntu1-16.04.7) ...
Installing new version of config file /etc/init.d/docker ...
Installing new version of config file /etc/init.d/docker.conf ...
Setting up ubuntu-fan (0.12.8-16.04.3) ...
Processing triggers for systemd (229-4ubuntu21.27) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
sam@sam-Virtual-Machine:~$
  
```

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.



```

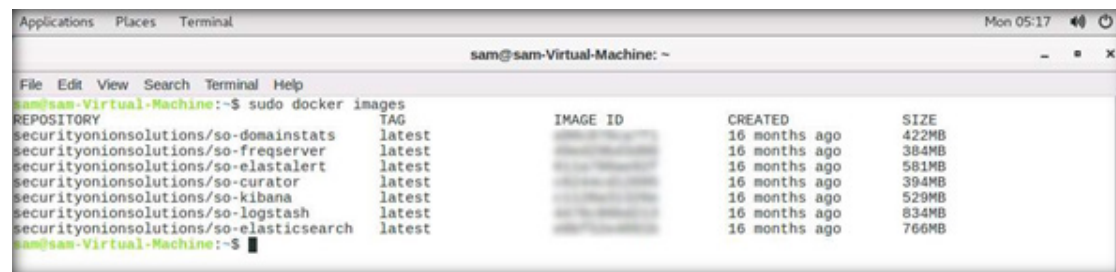
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
dictionaries-common/xenial,xenial,now 1.26.3 all [installed,automatic]
diffstat/xenial,now 1.61-1 amd64 [installed,automatic]
diffutils/xenial,now 1:3.3-3 amd64 [installed]
dirmngr/xenial-updates,xenial-security,now 2.1.11-6ubuntu2.1 amd64 [installed,automatic]
discover/xenial,now 2.1.2-7ubuntu1 amd64 [installed,automatic]
discover-data/xenial,xenial,now 2.2013.01.11 all [installed,automatic]
distro-info-data/now 0.28ubuntu0.14 all [installed,upgradable to: 0.28ubuntu0.18]
dkms/xenial-updates,xenial-updates,now 2.2.0.3-2ubuntu1.8 all [installed,automatic]
dmeventd/xenial,now 2:1.02.110-1ubuntu10 amd64 [installed]
dmidecode/xenial-updates,now 3.0-2ubuntu0.2 amd64 [installed,automatic]
dmraid/xenial,now 1.0.0.rc16-4.2ubuntu3 amd64 [installed,automatic]
dmsetup/xenial,now 2:1.02.110-1ubuntu10 amd64 [installed]
dns-root-data/xenial-updates,xenial-updates,xenial-security,xenial-security,now 2018013001-16.04.1 all [installed]
dnsmasq-base/now 2.75-1ubuntu0.16.04.5 amd64 [installed,upgradable to: 2.75-1ubuntu0.16.04.10]
dnsutils/now 1:9.10.3.dfsg.P4-8ubuntu1.15 amd64 [installed,upgradable to: 1:9.10.3.dfsg.P4-8ubuntu1.19]
docker.io/xenial-updates,now 18.09.7-0ubuntu1-16.04.7 amd64 [installed]
dosfstools/xenial-updates,xenial-security,now 3.0.28-2ubuntu0.1 amd64 [installed]
dpkg/now 1.18.4ubuntu1.6 amd64 [installed,upgradable to: 1.18.4ubuntu1.7]
dpkg-dev/now 1.18.4ubuntu1.6 all [installed,upgradable to: 1.18.4ubuntu1.7]
dpkg-repack/xenial,xenial,now 1.41 all [installed,automatic]
driftnet/xenial,now 1.1.5-1.1 amd64 [installed,automatic]
dsiff/xenial,now 2.4b1+debian-22.1 amd64 [installed,automatic]
e2fslibs/xenial-updates,xenial-security,now 1.42.13-1ubuntu1.2 amd64 [installed]
e2fsprogs/xenial-updates,xenial-security,now 1.42.13-1ubuntu1.2 amd64 [installed]
ecryptfs-utils/xenial-updates,xenial-security,now 1:1.1-0ubuntu1.1 amd64 [installed,automatic]
efs/xenial,now 1.10-2 amd64 [installed]
eject/xenial-updates,xenial-security,now 2.1.5+debian-cvs20081104-13.1ubuntu0.16.04.1 amd64 [installed]
emacsen-common/xenial,xenial,now 2.0.8 all [installed,automatic]
enchant/xenial,now 1.6.0-10.1build2 amd64 [installed,automatic]
ethtool/xenial,now 1:4.5-1 amd64 [installed]
evolution-data-server/now 3.18.5-1ubuntu1.2 amd64 [installed,upgradable to: 3.18.5-1ubuntu1.3]
evolution-data-server-common/now 3.18.5-1ubuntu1.2 all [installed,upgradable to: 3.18.5-1ubuntu1.3]
exo-utils/xenial,now 0.10.7-1 amd64 [installed,automatic]
expect/xenial,now 5.45-7 amd64 [installed,automatic]
fakeroot/xenial,now 1.20.2-1ubuntu1 amd64 [installed,automatic]
file/now 1:5.25-2ubuntu1.3 amd64 [installed,upgradable to: 1:5.25-2ubuntu1.4]
file-roller/now 3.16.5-0ubuntu1.4 amd64 [installed,upgradable to: 3.16.5-0ubuntu1.5]
findutils/xenial,now 4.6.0+git+20160126-2 amd64 [installed]
fontconfig/xenial-updates,xenial-security,now 2.11.94-0ubuntu1.1 amd64 [installed,automatic]
fontconfig-config/xenial-updates,xenial-updates,xenial-security,xenial-security,now 2.11.94-0ubuntu1.1 all [installed,automatic]

```

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

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.



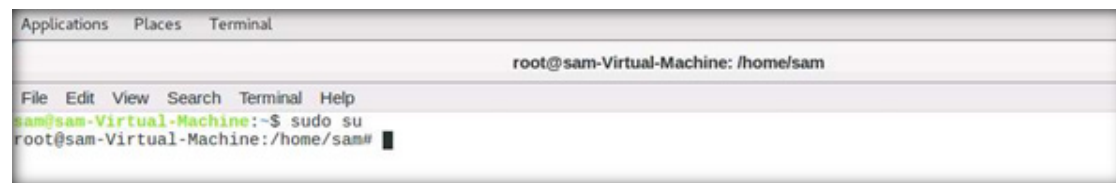
```
sam@sam-Virtual-Machine: ~  
File Edit View Search Terminal Help  
sam@sam-Virtual-Machine:~$ sudo docker images  
REPOSITORY              TAG          IMAGE ID          CREATED           SIZE  
securityonionsolutions/so-domainstats  latest      16 months ago    422MB  
securityonionsolutions/so-freqserver   latest      16 months ago    384MB  
securityonionsolutions/so-elastalert   latest      16 months ago    581MB  
securityonionsolutions/so-curator      latest      16 months ago    394MB  
securityonionsolutions/so-kibana       latest      16 months ago    529MB  
securityonionsolutions/so-logstash     latest      16 months ago    834MB  
securityonionsolutions/so-elasticsearch latest      16 months ago    766MB  
sam@sam-Virtual-Machine:~$
```

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

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`.



```
Applications  Places  Terminal  
root@sam-Virtual-Machine: /home/sam  
File Edit View Search Terminal Help  
sam@sam-Virtual-Machine:~$ sudo su  
root@sam-Virtual-Machine:/home/sam#
```

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.



```
Applications  Places  Terminal

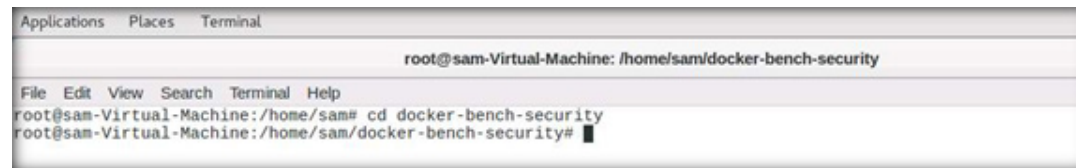
root@sam-Virtual-Machine: /home/sam

File Edit View Search Terminal Help
root@sam-Virtual-Machine:/home/sam# sudo su
root@sam-Virtual-Machine:/home/sam# git clone https://github.com/docker/docker-bench-security.git
Cloning into 'docker-bench-security'...
remote: Enumerating objects: 2411, done.
remote: Counting objects: 100% (310/310), done.
remote: Compressing objects: 100% (108/108), done.
remote: Total 2411 (delta 212), reused 272 (delta 199), pack-reused 2101
Receiving objects: 100% (2411/2411), 3.92 MiB | 423.00 KiB/s, done.
Resolving deltas: 100% (1684/1684), done.
Checking connectivity... done.
root@sam-Virtual-Machine:/home/sam#
```

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

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

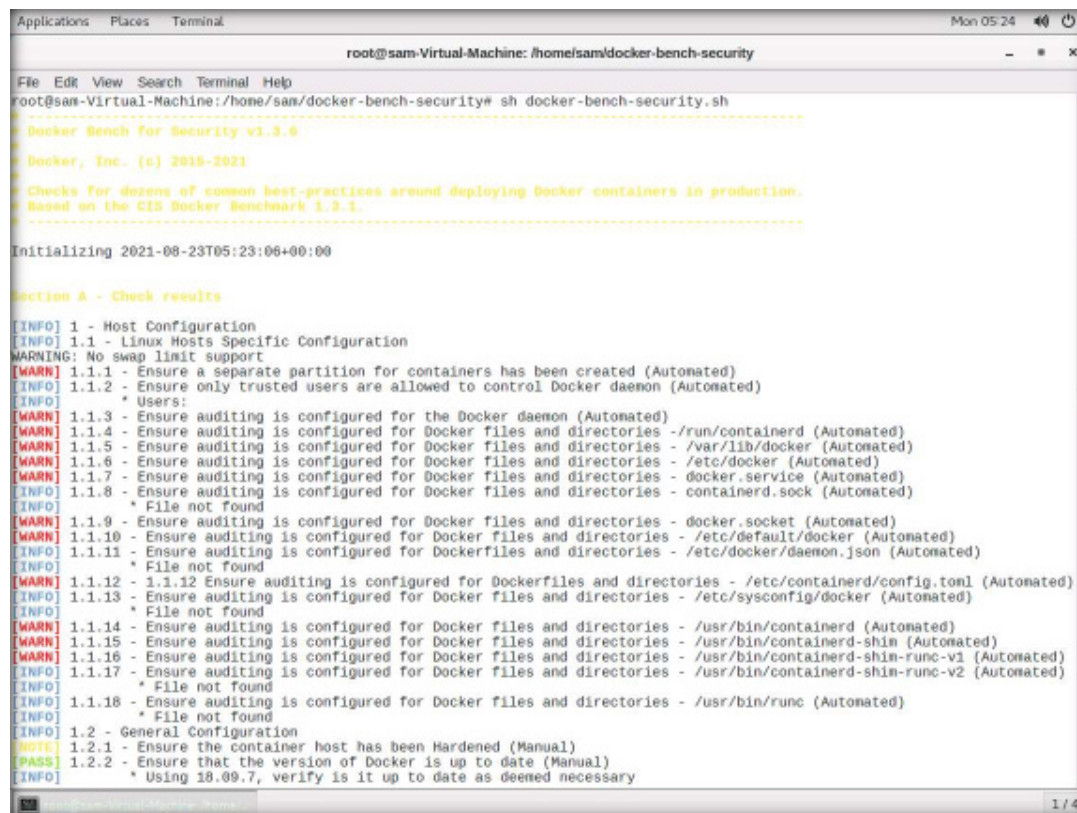
20. Next, to change directory to the docker-bench-security folder, type `cd docker-bench-security` and press Enter.



```
Applications  Places  Terminal  
root@sam-Virtual-Machine: /home/sam/docker-bench-security  
File Edit View Search Terminal Help  
root@sam-Virtual-Machine:/home/sam# cd docker-bench-security  
root@sam-Virtual-Machine:/home/sam/docker-bench-security#
```

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.



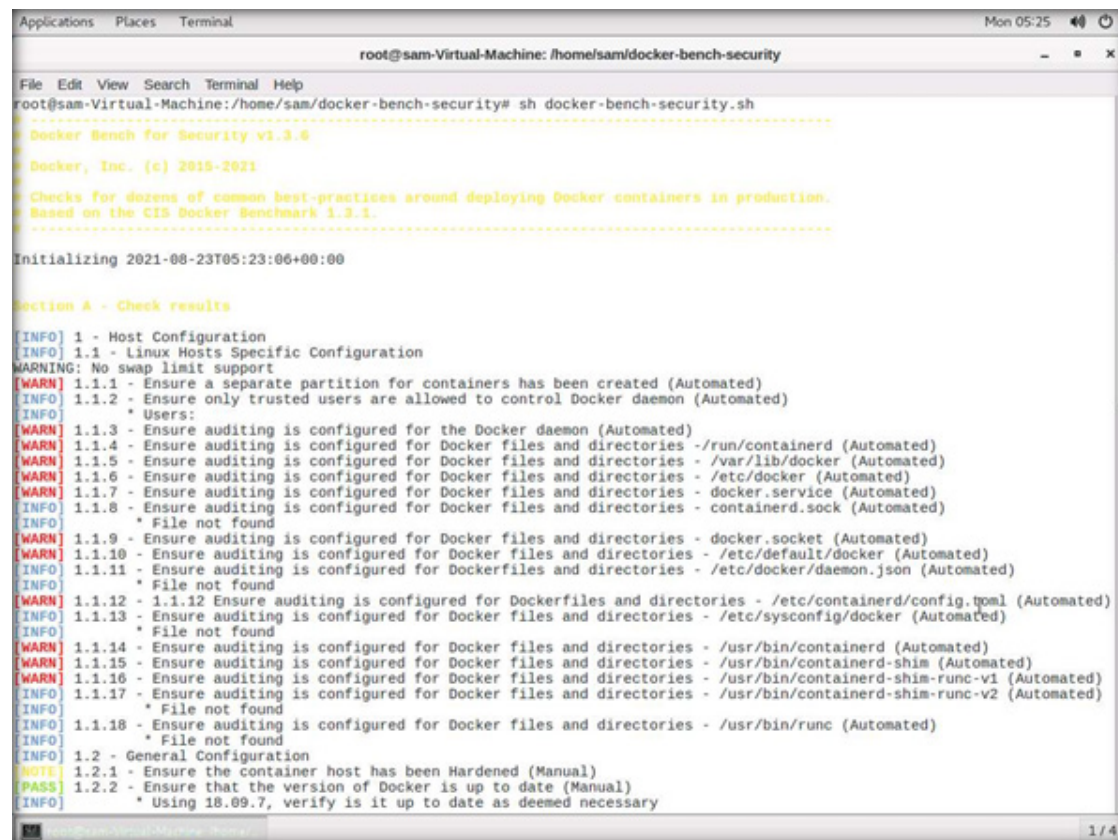
```
Applications  Places  Terminal
root@sam-Virtual-Machine: /home/sam/docker-bench-security
File Edit View Search Terminal Help
root@sam-Virtual-Machine: /home/sam/docker-bench-security# sh docker-bench-security.sh
Docker Bench for Security v1.3.0
Docker, Inc. (c) 2015-2021
Checks for dozens of common best-practices around deploying Docker containers in production.
Based on the CIS Docker Benchmark 1.2.1.

Initializing 2021-08-23T05:23:06+00:00

Section A - Check results
[INFO] 1 - Host Configuration
[INFO] 1.1 - Linux Hosts Specific Configuration
[WARN] No swap limit support
[WARN] 1.1.1 - Ensure a separate partition for containers has been created (Automated)
[INFO] 1.1.2 - Ensure only trusted users are allowed to control Docker daemon (Automated)
[INFO] * Users:
[WARN] 1.1.3 - Ensure auditing is configured for the Docker daemon (Automated)
[WARN] 1.1.4 - Ensure auditing is configured for Docker files and directories - /run/containerd (Automated)
[WARN] 1.1.5 - Ensure auditing is configured for Docker files and directories - /var/lib/docker (Automated)
[WARN] 1.1.6 - Ensure auditing is configured for Docker files and directories - /etc/docker (Automated)
[WARN] 1.1.7 - Ensure auditing is configured for Docker files and directories - docker.service (Automated)
[INFO] 1.1.8 - Ensure auditing is configured for Docker files and directories - containerd.sock (Automated)
[INFO] * File not found
[WARN] 1.1.9 - Ensure auditing is configured for Docker files and directories - docker.socket (Automated)
[WARN] 1.1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker (Automated)
[INFO] 1.1.11 - Ensure auditing is configured for Dockerfiles and directories - /etc/docker/daemon.json (Automated)
[INFO] * File not found
[WARN] 1.1.12 - 1.1.12 Ensure auditing is configured for Dockerfiles and directories - /etc/containerd/config.toml (Automated)
[INFO] 1.1.13 - Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker (Automated)
[INFO] * File not found
[WARN] 1.1.14 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd (Automated)
[WARN] 1.1.15 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim (Automated)
[WARN] 1.1.16 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v1 (Automated)
[INFO] 1.1.17 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v2 (Automated)
[INFO] * File not found
[INFO] 1.1.18 - Ensure auditing is configured for Docker files and directories - /usr/bin/runc (Automated)
[INFO] * File not found
[INFO] 1.2 - General Configuration
[NOTE] 1.2.1 - Ensure the container host has been Hardened (Manual)
[PASS] 1.2.2 - Ensure that the version of Docker is up to date (Manual)
[INFO] * Using 18.09.7, verify it is up to date as deemed necessary
```

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

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.

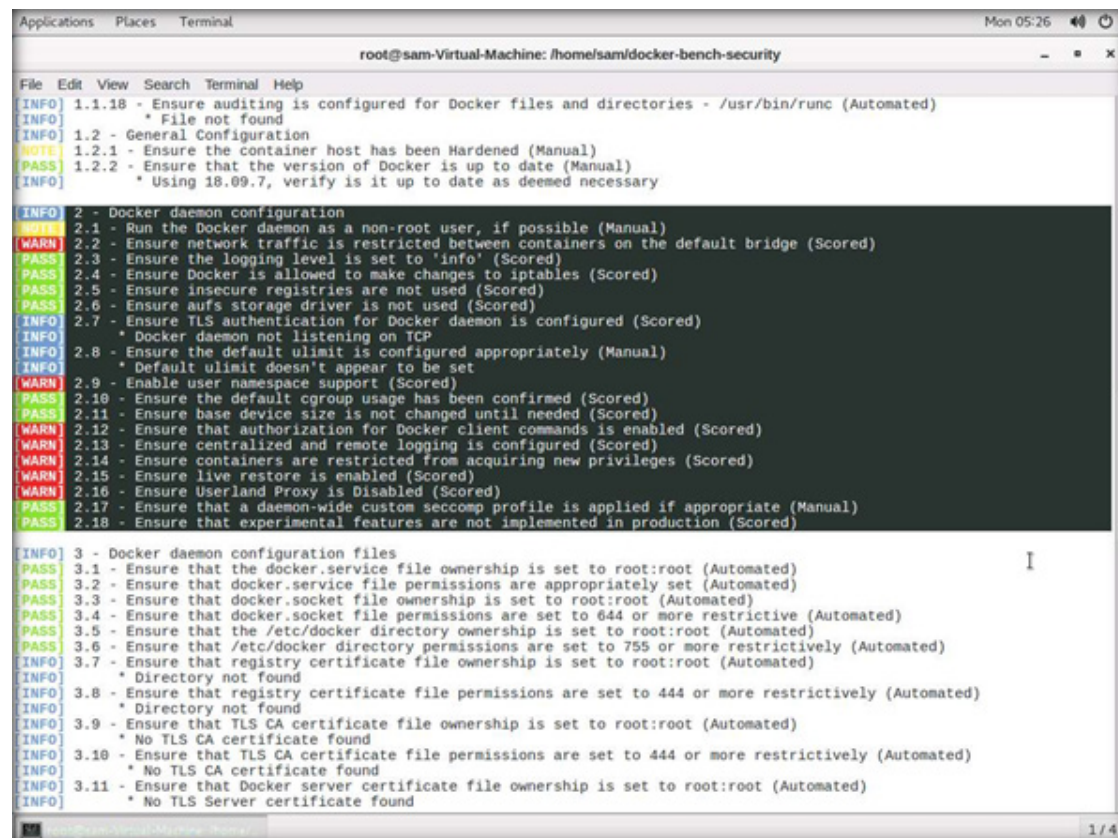


```
root@sam-Virtual-Machine: /home/sam/docker-bench-security
File Edit View Search Terminal Help
root@sam-Virtual-Machine:/home/sam/docker-bench-security# sh docker-bench-security.sh
-----
* Docker Bench for Security v1.3.6
*
* Docker, Inc. (c) 2015-2021
*
* Checks for dozens of common best-practices around deploying Docker containers in production.
* Based on the CIS Docker Benchmark 1.3.1.
*
-----
Initializing 2021-08-23T05:23:06+00:00

Section A - Check results
[INFO] 1 - Host Configuration
[INFO] 1.1 - Linux Hosts Specific Configuration
WARNING: No swap limit support
[WARN] 1.1.1 - Ensure a separate partition for containers has been created (Automated)
[INFO] 1.1.2 - Ensure only trusted users are allowed to control Docker daemon (Automated)
[INFO] * Users:
[WARN] 1.1.3 - Ensure auditing is configured for the Docker daemon (Automated)
[WARN] 1.1.4 - Ensure auditing is configured for Docker files and directories - /run/containerd (Automated)
[WARN] 1.1.5 - Ensure auditing is configured for Docker files and directories - /var/lib/docker (Automated)
[WARN] 1.1.6 - Ensure auditing is configured for Docker files and directories - /etc/docker (Automated)
[WARN] 1.1.7 - Ensure auditing is configured for Docker files and directories - docker.service (Automated)
[INFO] 1.1.8 - Ensure auditing is configured for Docker files and directories - containerd.sock (Automated)
[INFO] * File not found
[WARN] 1.1.9 - Ensure auditing is configured for Docker files and directories - docker.socket (Automated)
[WARN] 1.1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker (Automated)
[INFO] 1.1.11 - Ensure auditing is configured for Dockerfiles and directories - /etc/docker/daemon.json (Automated)
[INFO] * File not found
[WARN] 1.1.12 - Ensure auditing is configured for Dockerfiles and directories - /etc/containerd/config.toml (Automated)
[INFO] 1.1.13 - Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker (Automated)
[INFO] * File not found
[WARN] 1.1.14 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd (Automated)
[WARN] 1.1.15 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim (Automated)
[WARN] 1.1.16 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v1 (Automated)
[INFO] 1.1.17 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v2 (Automated)
[INFO] * File not found
[INFO] 1.1.18 - Ensure auditing is configured for Docker files and directories - /usr/bin/runc (Automated)
[INFO] * File not found
[INFO] 1.2 - General Configuration
[NOTE] 1.2.1 - Ensure the container host has been Hardened (Manual)
[PASS] 1.2.2 - Ensure that the version of Docker is up to date (Manual)
[INFO] * Using 18.09.7, verify if it up to date as deemed necessary
```

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

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.



```

root@sam-Virtual-Machine: /home/sam/docker-bench-security

File Edit View Search Terminal Help

[INFO] 1.1.18 - Ensure auditing is configured for Docker files and directories - /usr/bin/runc (Automated)
[INFO] * File not found
[INFO] 1.2 - General Configuration
[NOTE] 1.2.1 - Ensure the container host has been Hardened (Manual)
[PASS] 1.2.2 - Ensure that the version of Docker is up to date (Manual)
[INFO] * Using 18.09.7, verify is it up to date as deemed necessary

[INFO] 2 - Docker daemon configuration
[NOTE] 2.1 - Run the Docker daemon as a non-root user, if possible (Manual)
[WARN] 2.2 - Ensure network traffic is restricted between containers on the default bridge (Scored)
[PASS] 2.3 - Ensure the logging level is set to 'info' (Scored)
[PASS] 2.4 - Ensure Docker is allowed to make changes to iptables (Scored)
[PASS] 2.5 - Ensure insecure registries are not used (Scored)
[PASS] 2.6 - Ensure aufs storage driver is not used (Scored)
[INFO] 2.7 - Ensure TLS authentication for Docker daemon is configured (Scored)
[INFO] * Docker daemon not listening on TCP
[INFO] 2.8 - Ensure the default ulimit is configured appropriately (Manual)
[INFO] * Default ulimit doesn't appear to be set
[WARN] 2.9 - Enable user namespace support (Scored)
[PASS] 2.10 - Ensure the default cgroup usage has been confirmed (Scored)
[PASS] 2.11 - Ensure base device size is not changed until needed (Scored)
[WARN] 2.12 - Ensure that authorization for Docker client commands is enabled (Scored)
[WARN] 2.13 - Ensure centralized and remote logging is configured (Scored)
[WARN] 2.14 - Ensure containers are restricted from acquiring new privileges (Scored)
[WARN] 2.15 - Ensure live restore is enabled (Scored)
[WARN] 2.16 - Ensure Userland Proxy is Disabled (Scored)
[PASS] 2.17 - Ensure that a daemon-wide custom seccomp profile is applied if appropriate (Manual)
[PASS] 2.18 - Ensure that experimental features are not implemented in production (Scored)

[INFO] 3 - Docker daemon configuration files
[PASS] 3.1 - Ensure that the docker.service file ownership is set to root:root (Automated)
[PASS] 3.2 - Ensure that docker.service file permissions are appropriately set (Automated)
[PASS] 3.3 - Ensure that docker.socket file ownership is set to root:root (Automated)
[PASS] 3.4 - Ensure that docker.socket file permissions are set to 644 or more restrictive (Automated)
[PASS] 3.5 - Ensure that the /etc/docker directory ownership is set to root:root (Automated)
[PASS] 3.6 - Ensure that /etc/docker directory permissions are set to 755 or more restrictively (Automated)
[INFO] 3.7 - Ensure that registry certificate file ownership is set to root:root (Automated)
[INFO] * Directory not found
[INFO] 3.8 - Ensure that registry certificate file permissions are set to 444 or more restrictively (Automated)
[INFO] * Directory not found
[INFO] 3.9 - Ensure that TLS CA certificate file ownership is set to root:root (Automated)
[INFO] * No TLS CA certificate found
[INFO] 3.10 - Ensure that TLS CA certificate file permissions are set to 444 or more restrictively (Automated)
[INFO] * No TLS CA certificate found
[INFO] 3.11 - Ensure that Docker server certificate file ownership is set to root:root (Automated)
[INFO] * No TLS Server certificate found
  
```

EXERCISE 1:

AUDIT DOCKER HOST SECURITY USING DOCKER- BENCH-SECURITY TOOL

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.

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

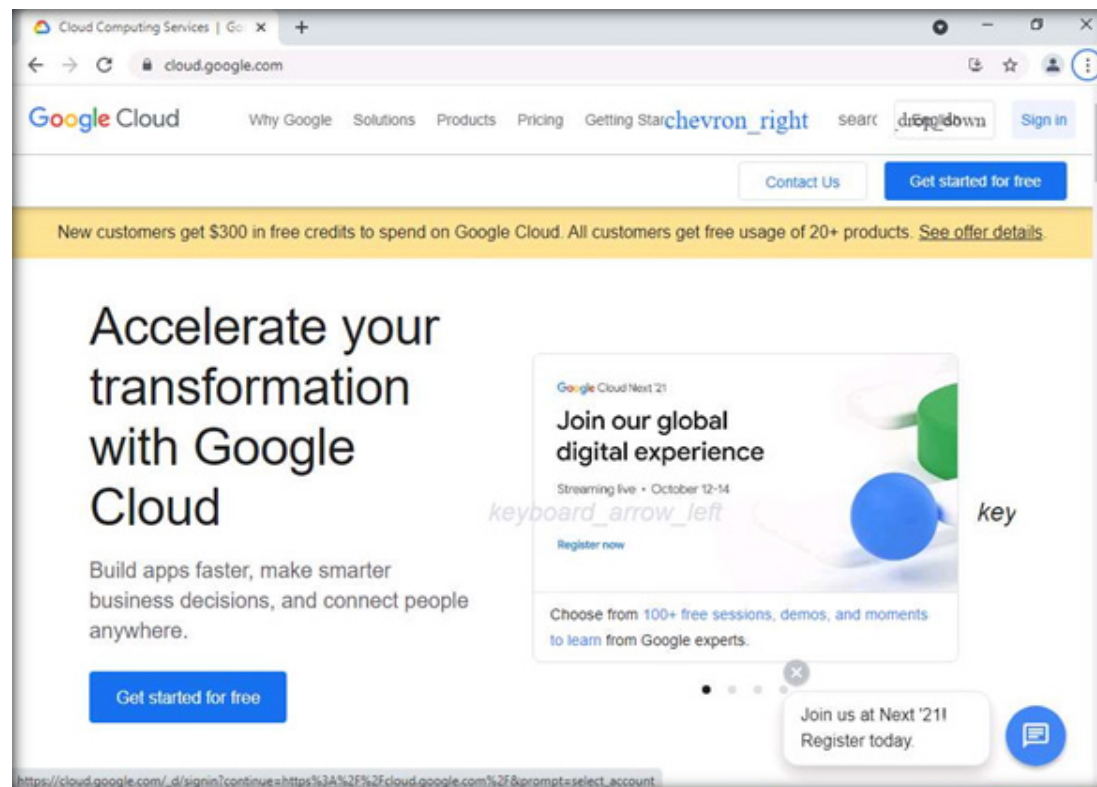
The services offered by the Google Cloud Platform (GCP) include computing, data storage and analytics, machine learning, networking, bigdata, cloud AI, management tools, identity and security, IoT, and API platforms.

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.

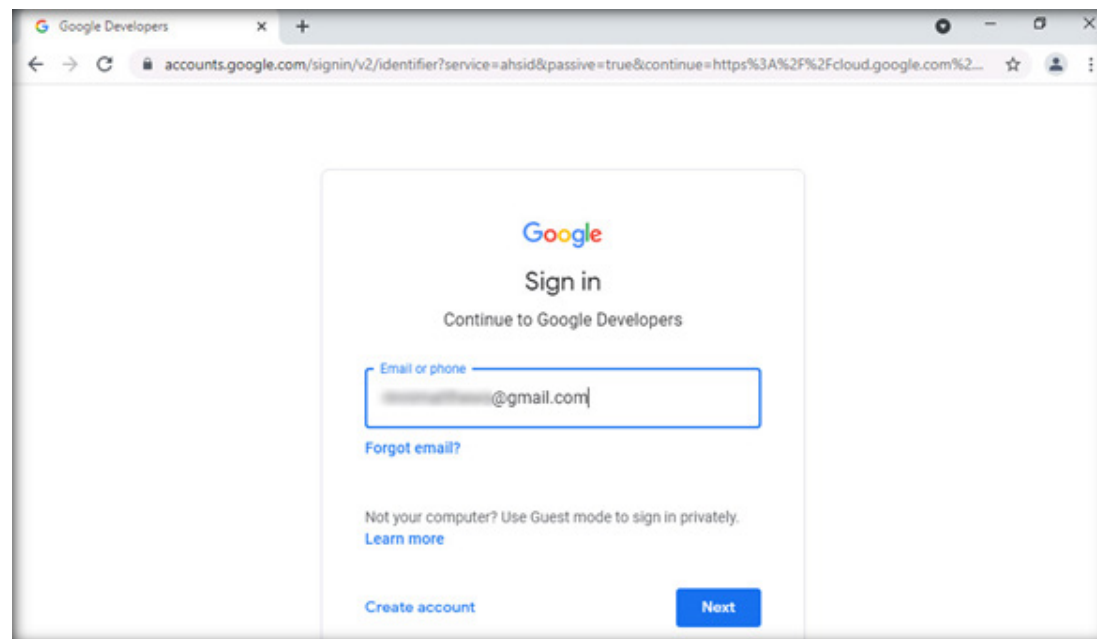
EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

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



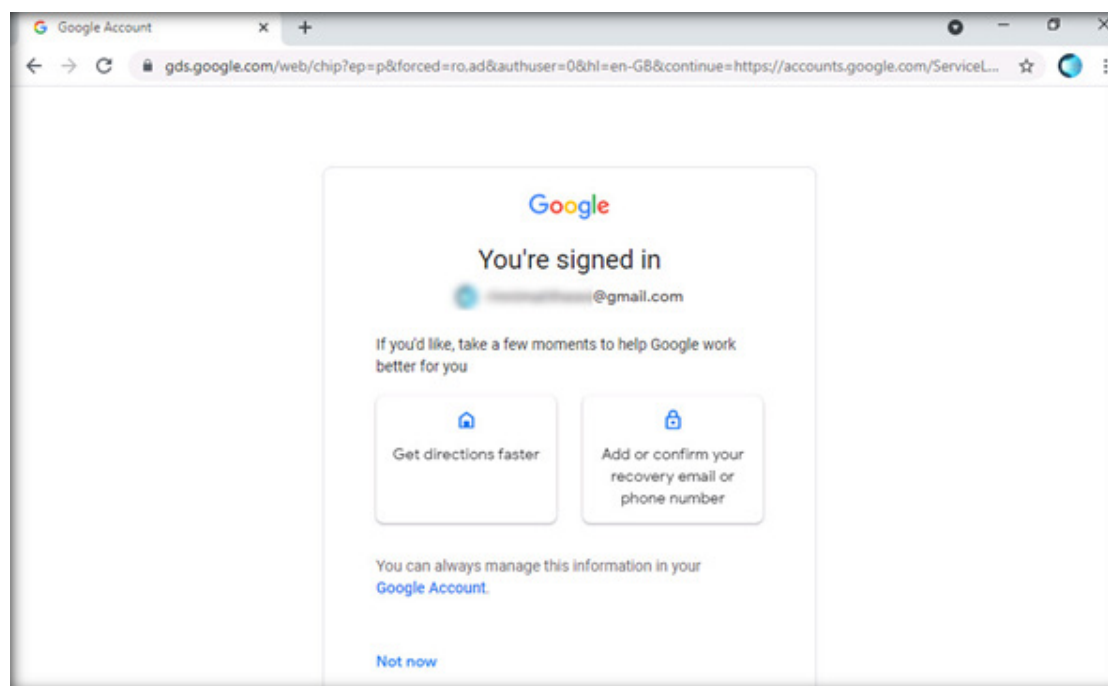
EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

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



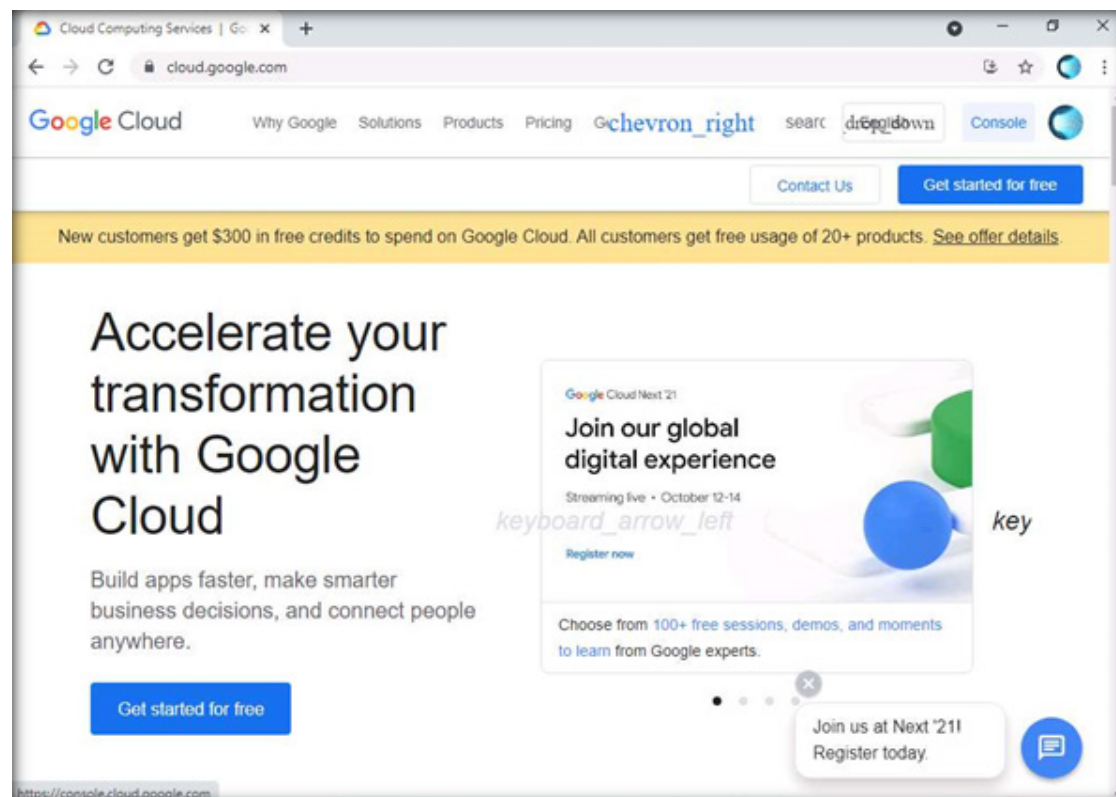
EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

7. In the next page, enter your password and click Next.
8. You're signed in page appears, click Not now to continue.



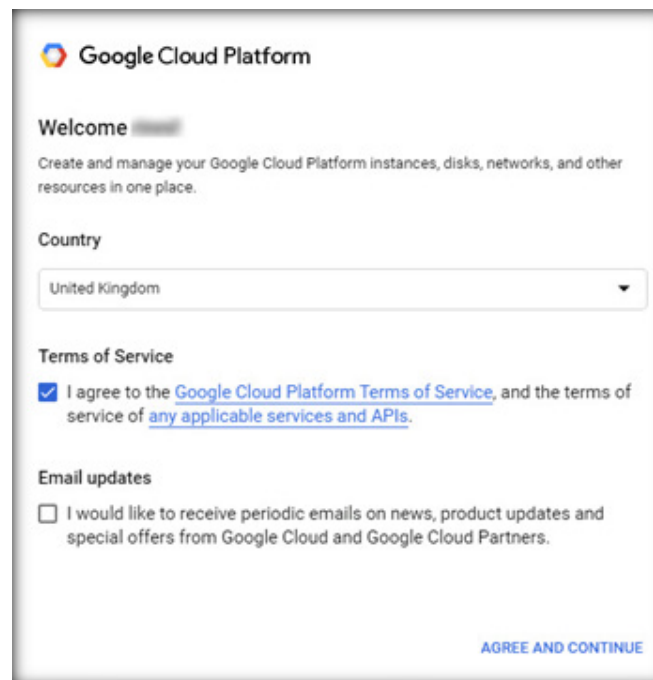
EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

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

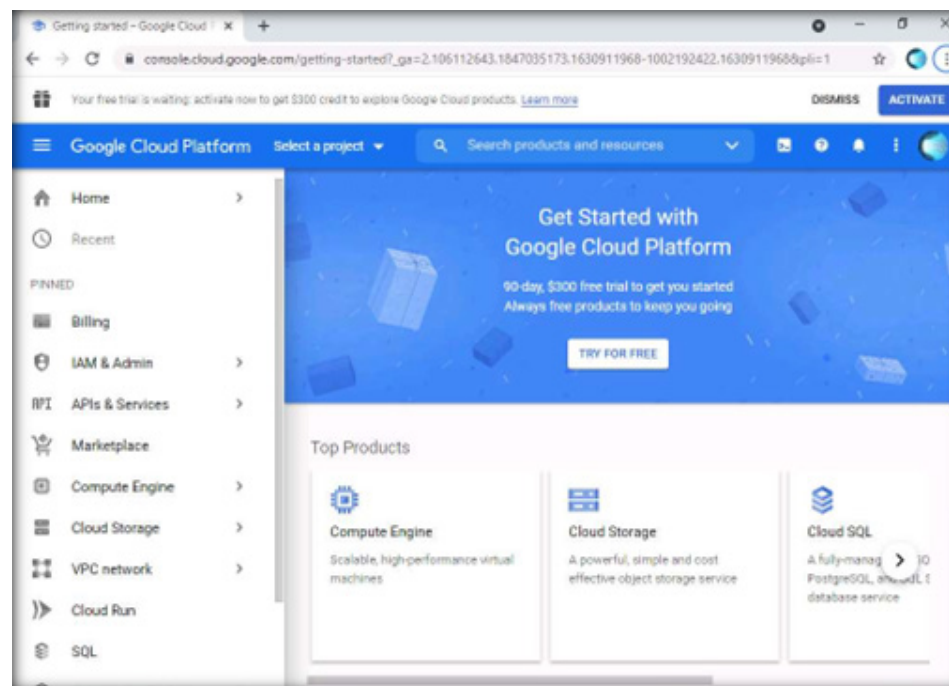
10. A welcome page appears. Under the Terms of Service section, select I agree checkbox and click AGREE AND CONTINUE.
Note: The options in the screenshot might differ in your lab environment.



The screenshot shows the Google Cloud Platform welcome page. At the top is the Google Cloud Platform logo. Below it is a 'Welcome' message followed by a description: 'Create and manage your Google Cloud Platform instances, disks, networks, and other resources in one place.' There is a 'Country' dropdown menu currently set to 'United Kingdom'. Under the 'Terms of Service' section, there is a checked checkbox for 'I agree to the Google Cloud Platform Terms of Service, and the terms of service of any applicable services and APIs.' Below that, under 'Email updates', there is an unchecked checkbox for 'I would like to receive periodic emails on news, product updates and special offers from Google Cloud and Google Cloud Partners.' At the bottom right is a blue link that says 'AGREE AND CONTINUE'.

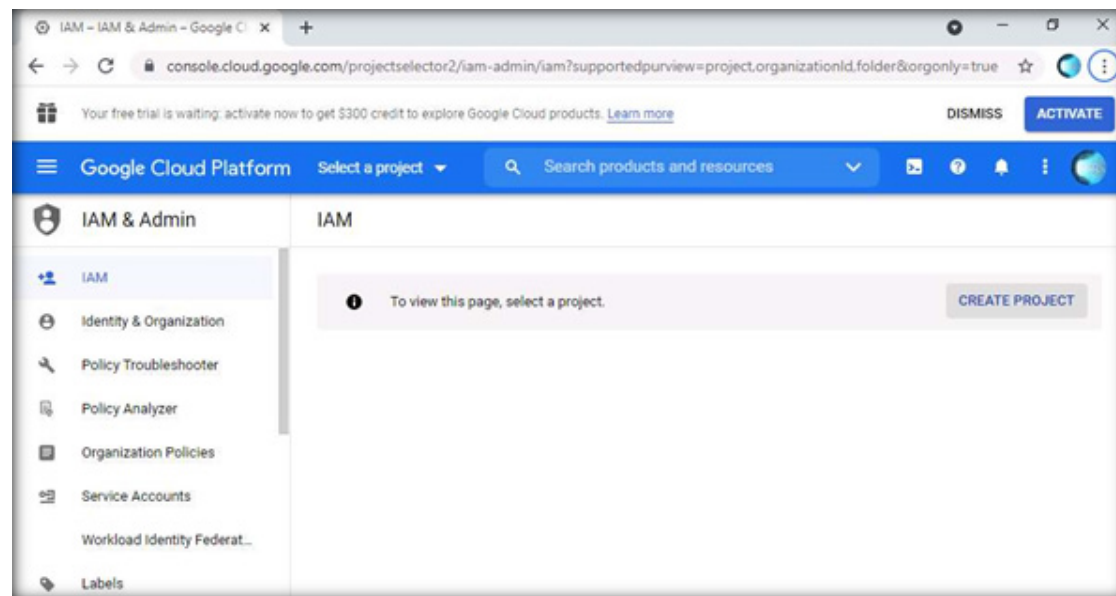
EXERCISE 2: CREATE IAM CREDENTIALS ON GOOGLE CLOUD PLATFORM

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.



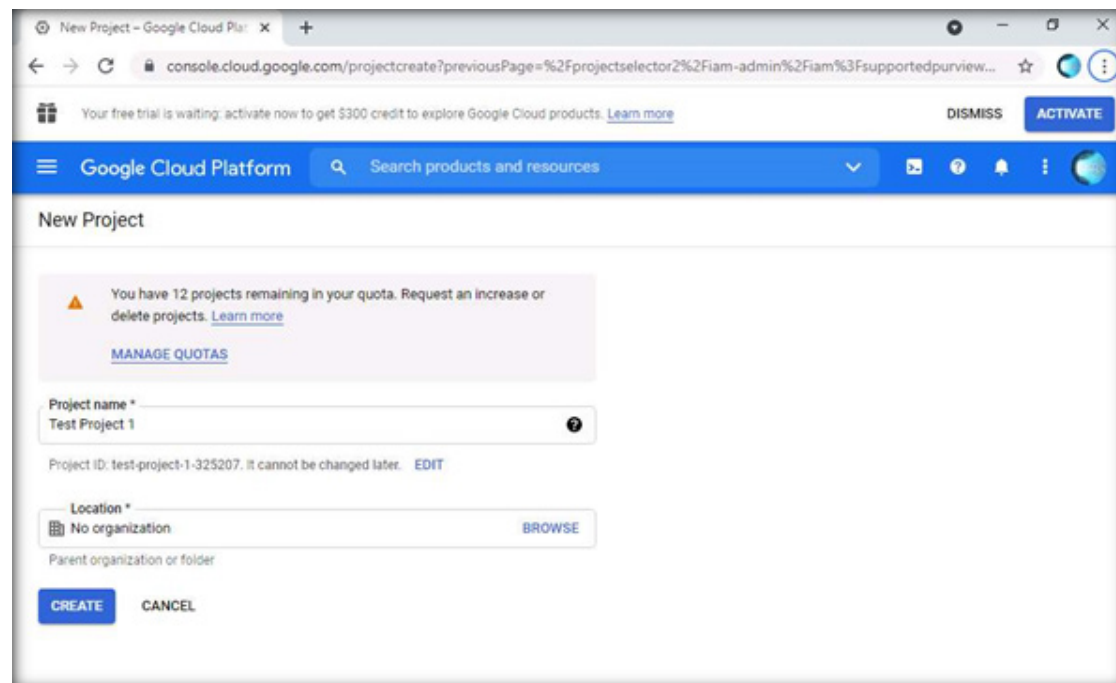
EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

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.



New Project - Google Cloud Pla: x +

console.cloud.google.com/projectcreate?previousPage=%2Fprojectselector%2Fiam-admin%2Fiam%3Fsupportedpurview... ☆ ⓘ

Your free trial is waiting: activate now to get \$300 credit to explore Google Cloud products. [Learn more](#) DISMISS ACTIVATE

Google Cloud Platform Search products and resources

New Project

⚠ You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)
[MANAGE QUOTAS](#)

Project name *
Test Project 1 ⓘ

Project ID: test-project-1-325207. It cannot be changed later. [EDIT](#)

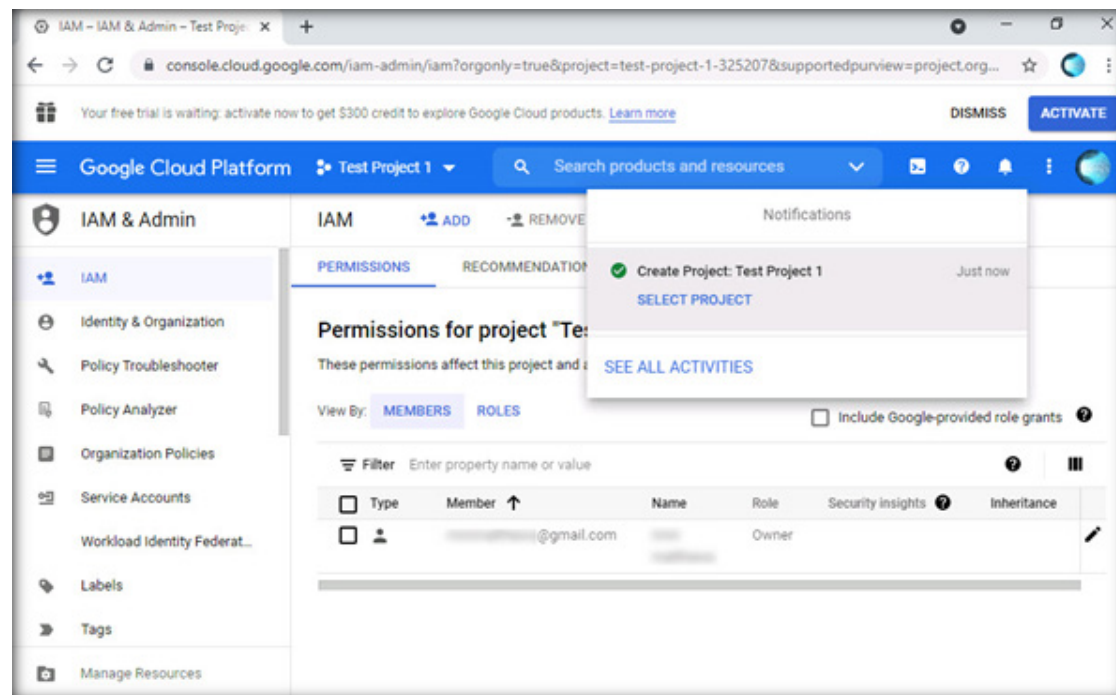
Location *
No organization [BROWSE](#)

Parent organization or folder

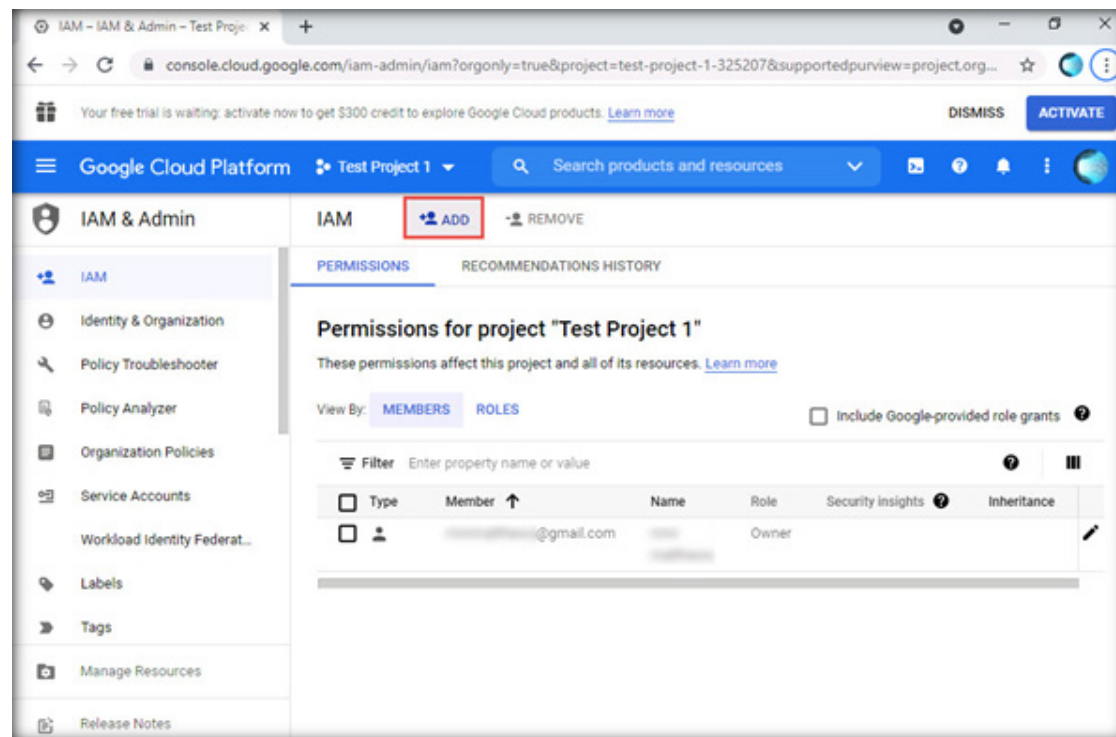
CREATE CANCEL

EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

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



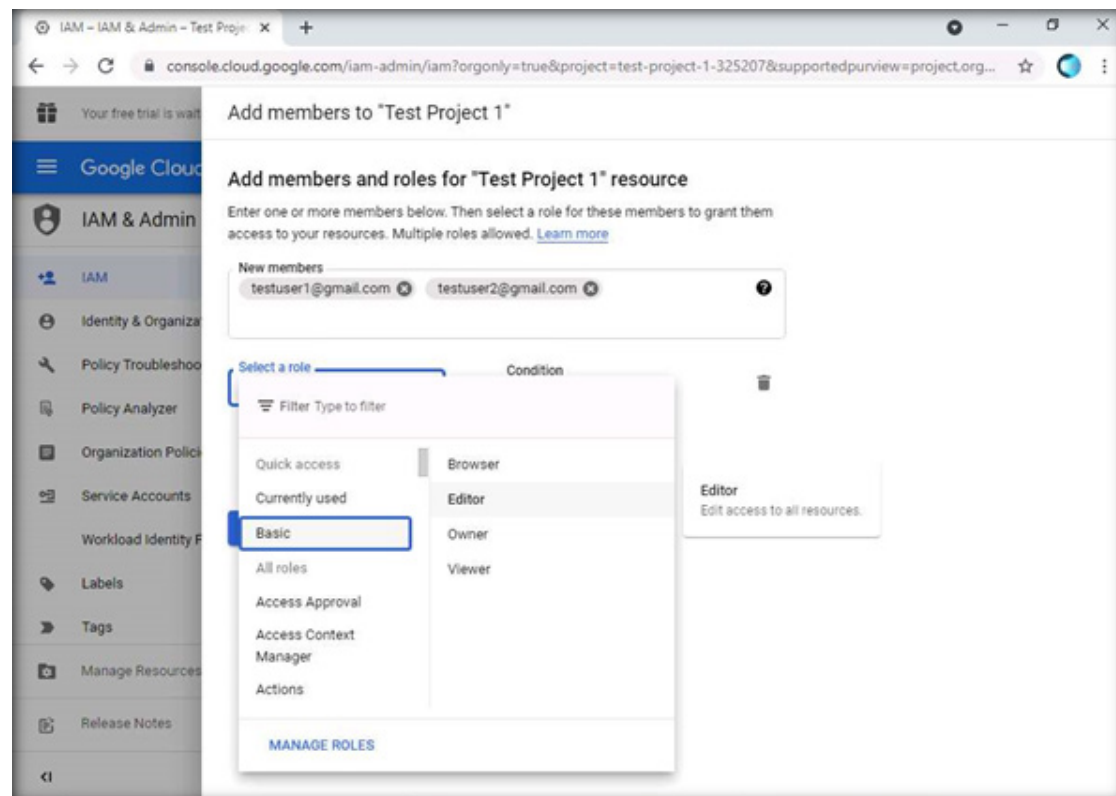
16. Now, click ADD button present at the top of the page.



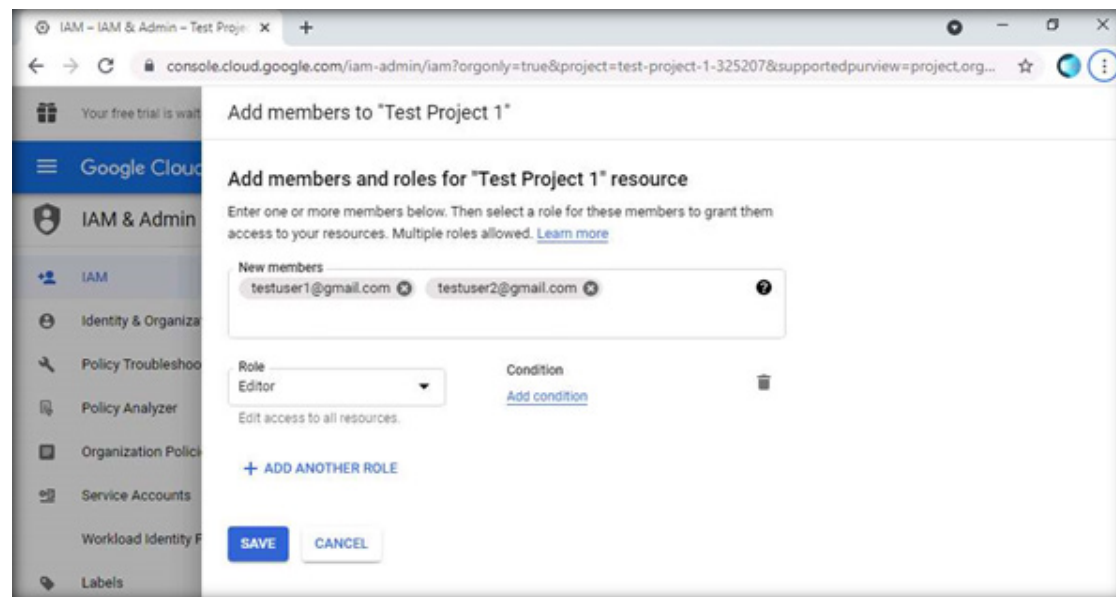
EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

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.

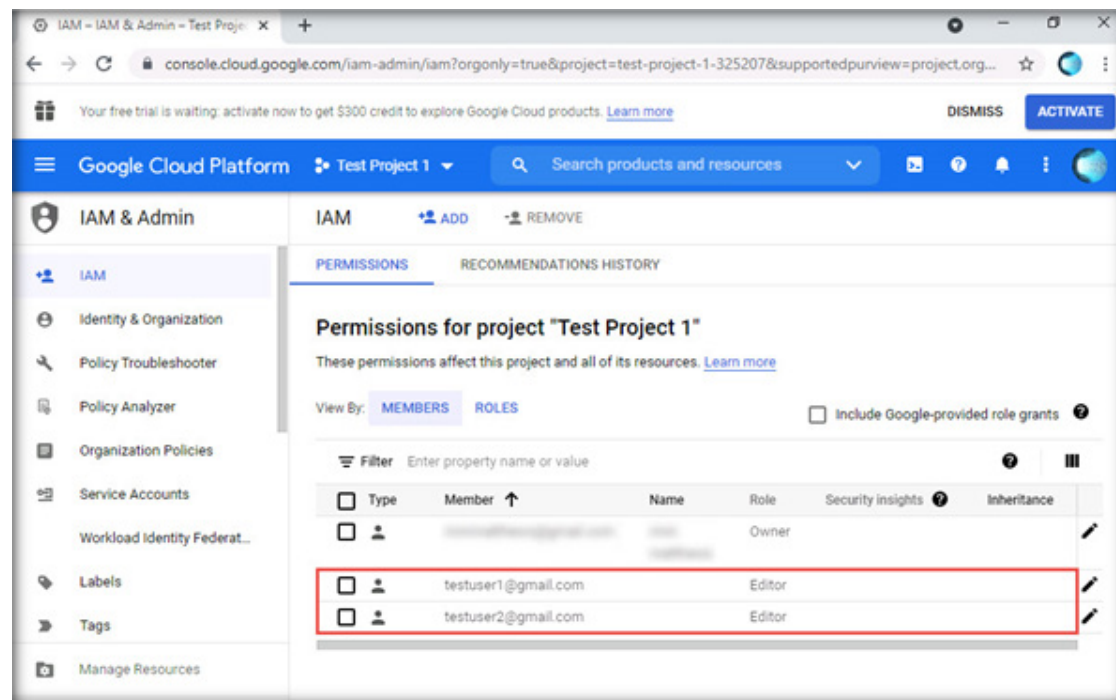


19. Click SAVE to save the settings.



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.

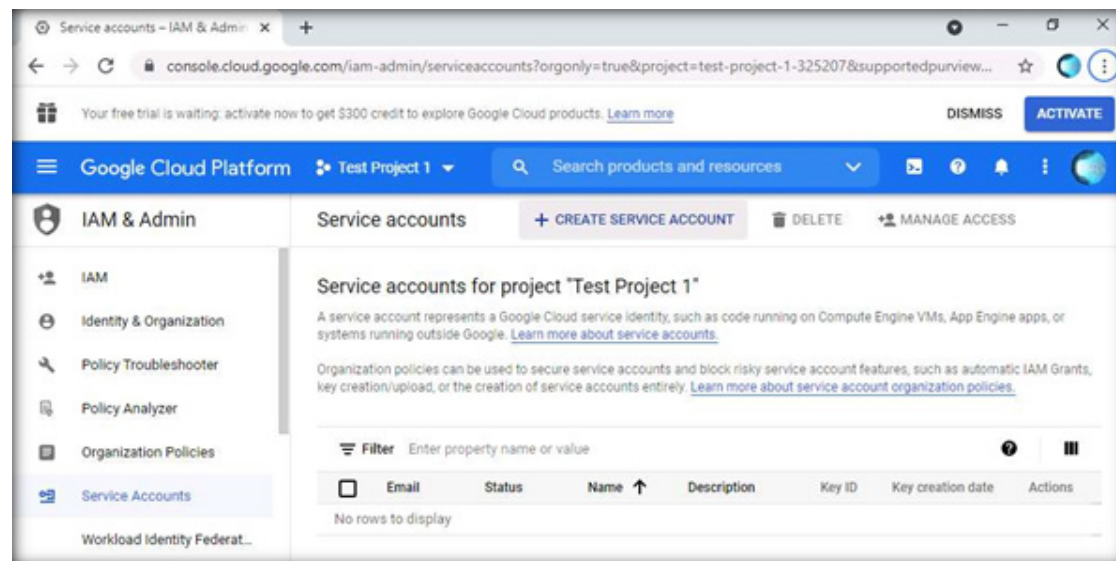


21. Now, we will create a service account. To do so, click Service Accounts option from the left-pane.

Note: A service account is a type of Google account that grants permissions to the virtual machines instead of end users.

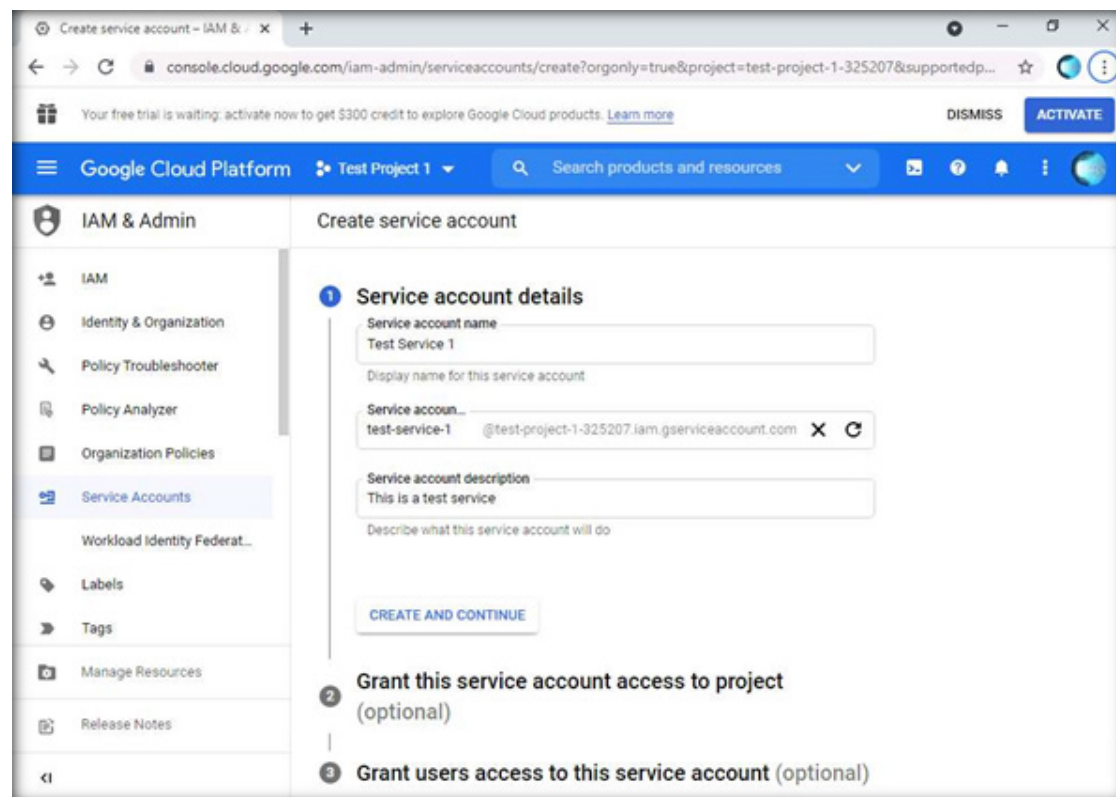
22. The Service accounts page appears; click on CREATE SERVICE ACCOUNT from the top-section of the page, as shown in the screenshot below.

Note: If Google tutorial pop-up appears, click GOT IT to close it.



EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

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.



Google Cloud Platform | Test Project 1 | Search products and resources

IAM & Admin

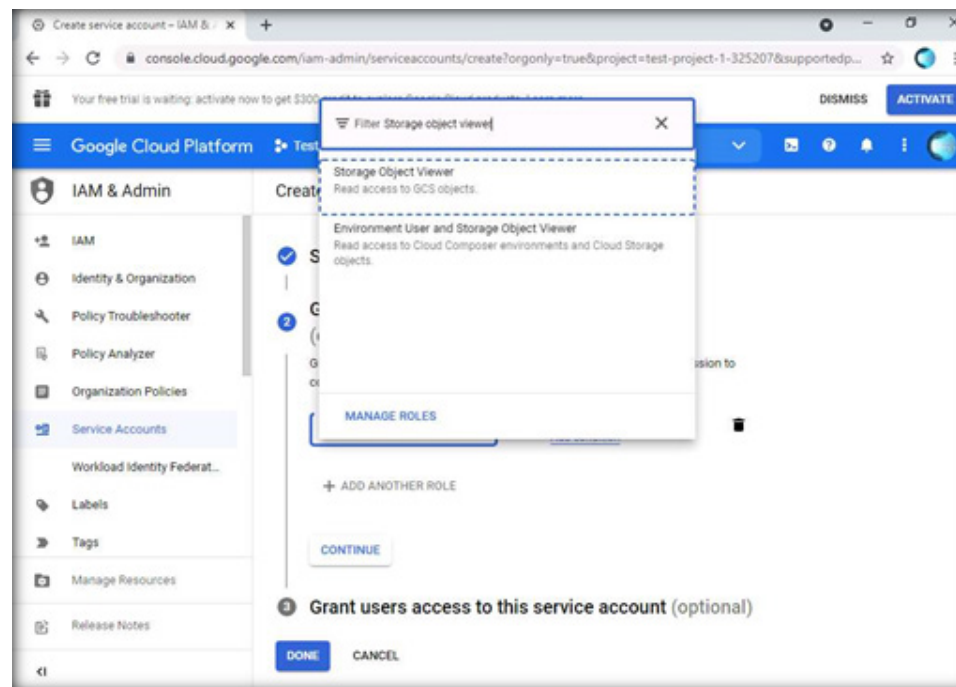
- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federat...
- Labels
- Tags
- Manage Resources
- Release Notes

Create service account

- Service account details**
 - Service account name: Test Service 1
 - Display name for this service account:
 - Service account email: test-service-1@test-project-1-325207.iam.gserviceaccount.com
 - Service account description: This is a test service
 - Describe what this service account will do:
 - CREATE AND CONTINUE**
- Grant this service account access to project (optional)**
- Grant users access to this service account (optional)**

EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

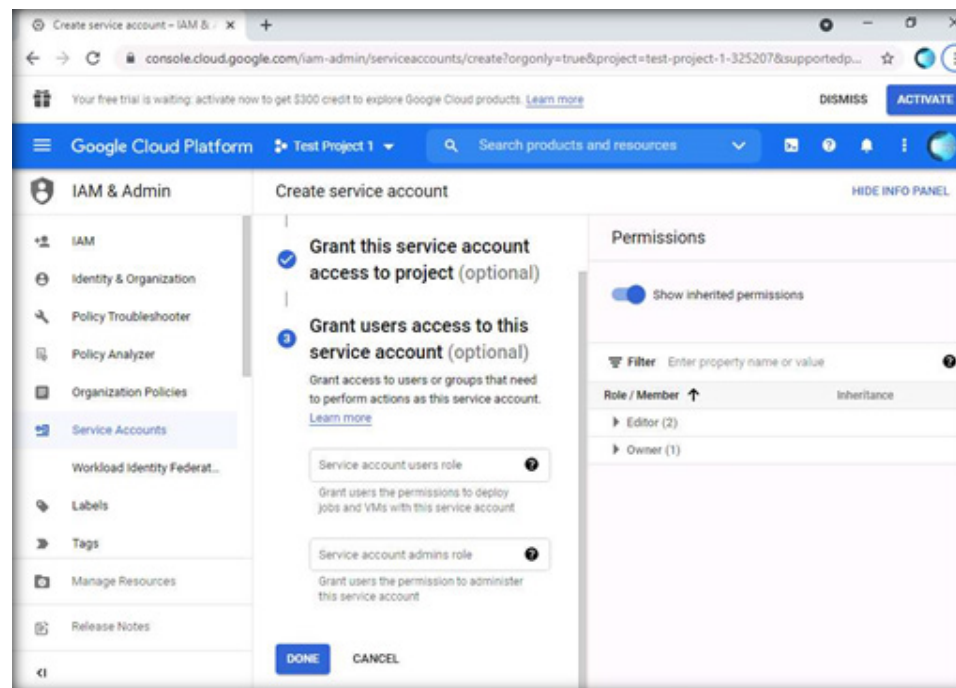
24. The Grant this service account access to project section appears, click Select a role field. A drop-down with options appears, in the Type to filter field, enter Storage object viewer. Select Storage object viewer from the options.



EXERCISE 2:
CREATE IAM
CREDENTIALS ON
GOOGLE CLOUD
PLATFORM

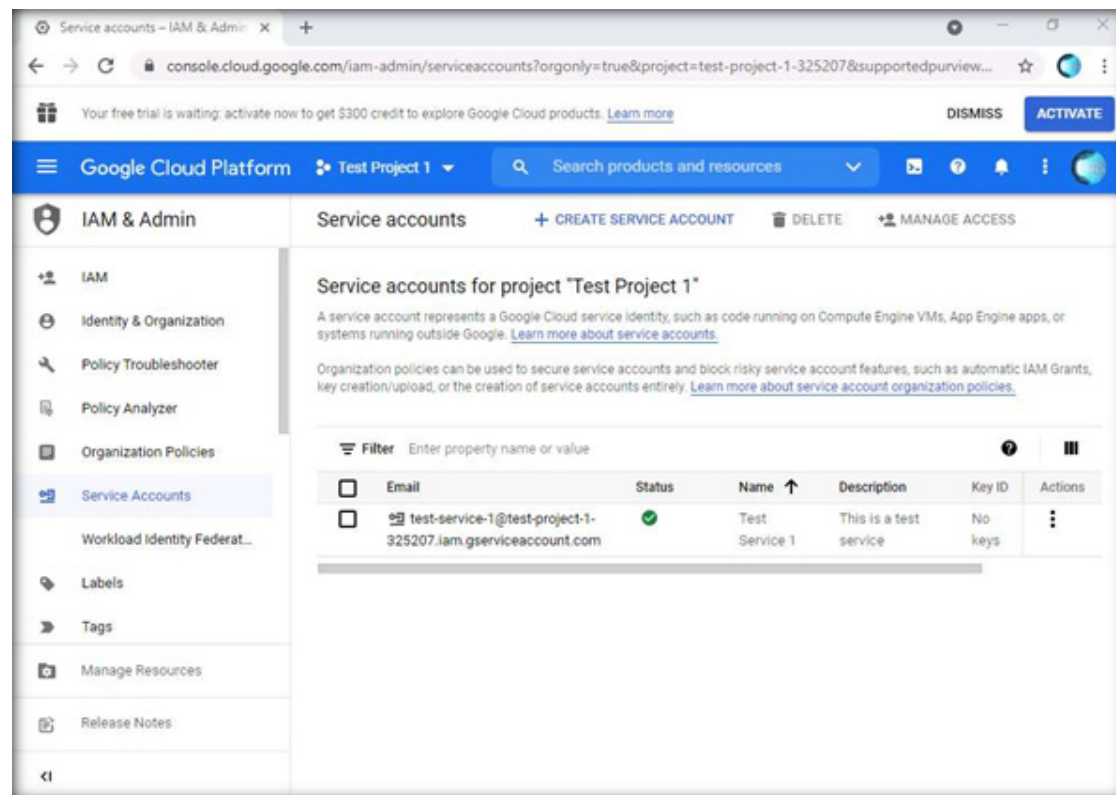
25. Click CONTINUE.

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.



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.

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.

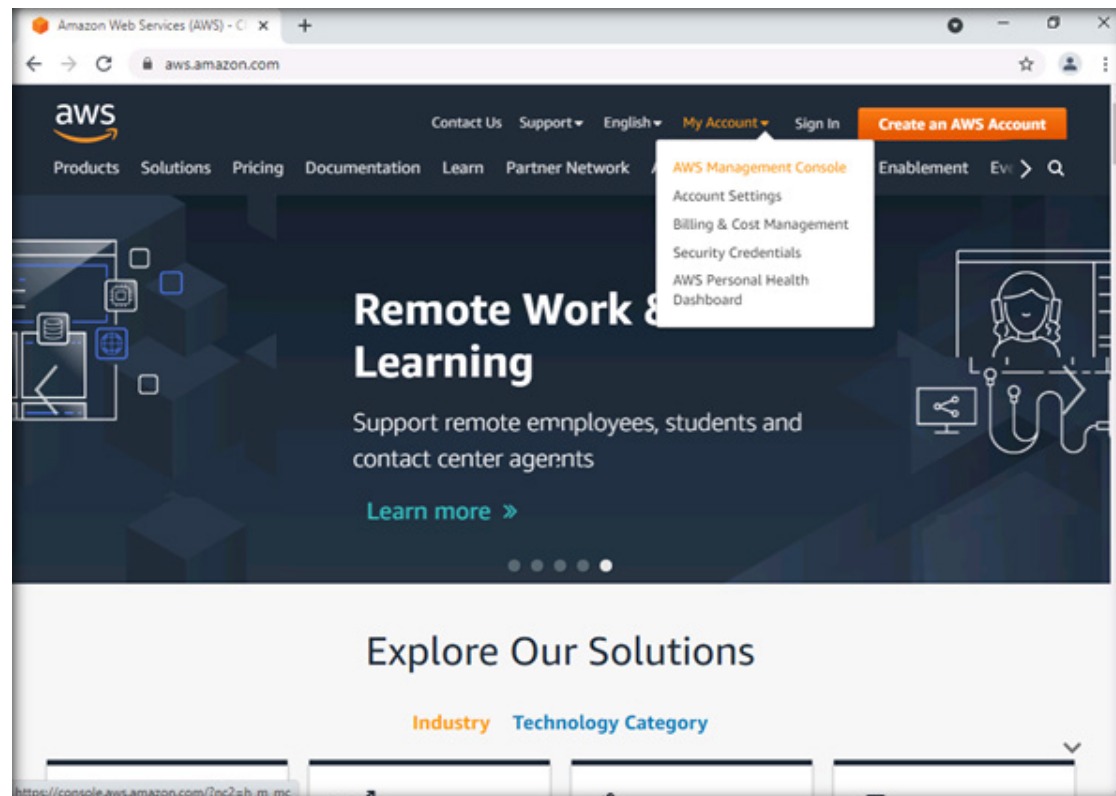
Note: Before starting this lab, you should create an AWS account using the following: <https://portal.aws.amazon.com/billing/signup>. Once the registration is completed, perform the following tasks.

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.

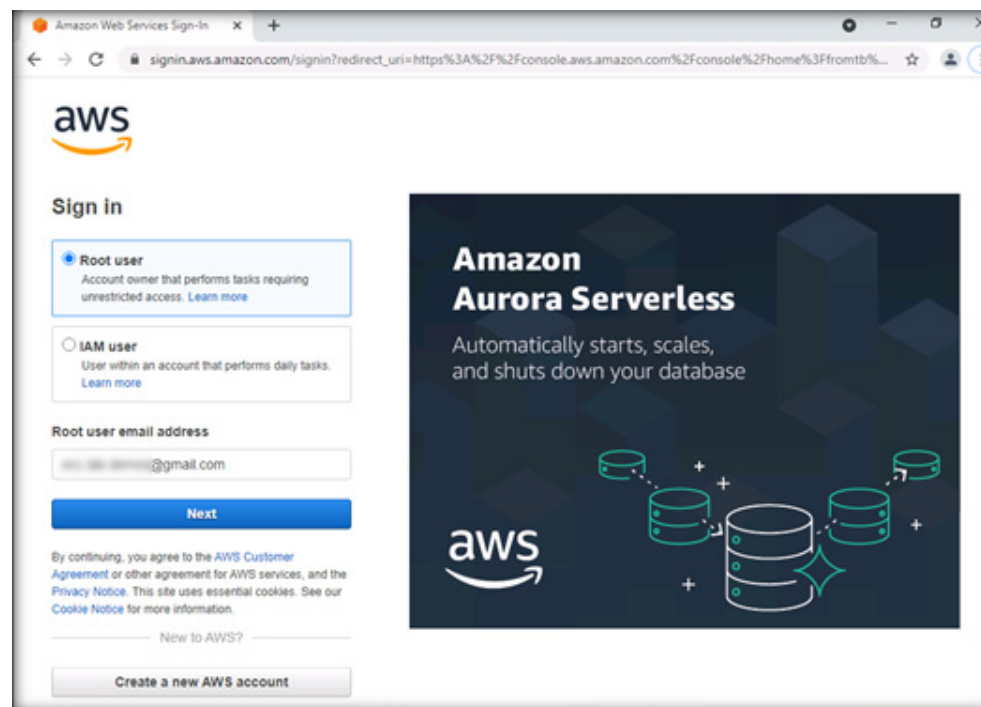
2. The Google Chrome browser opens. Go to the address bar, type <https://aws.amazon.com/>, and press Enter.

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.



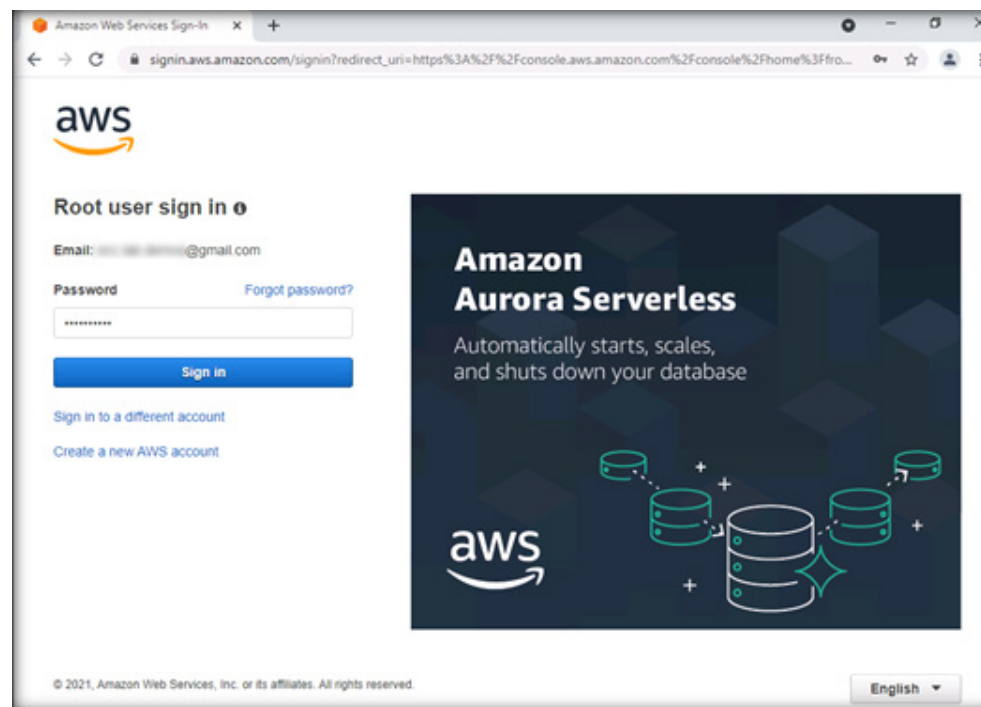
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

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.



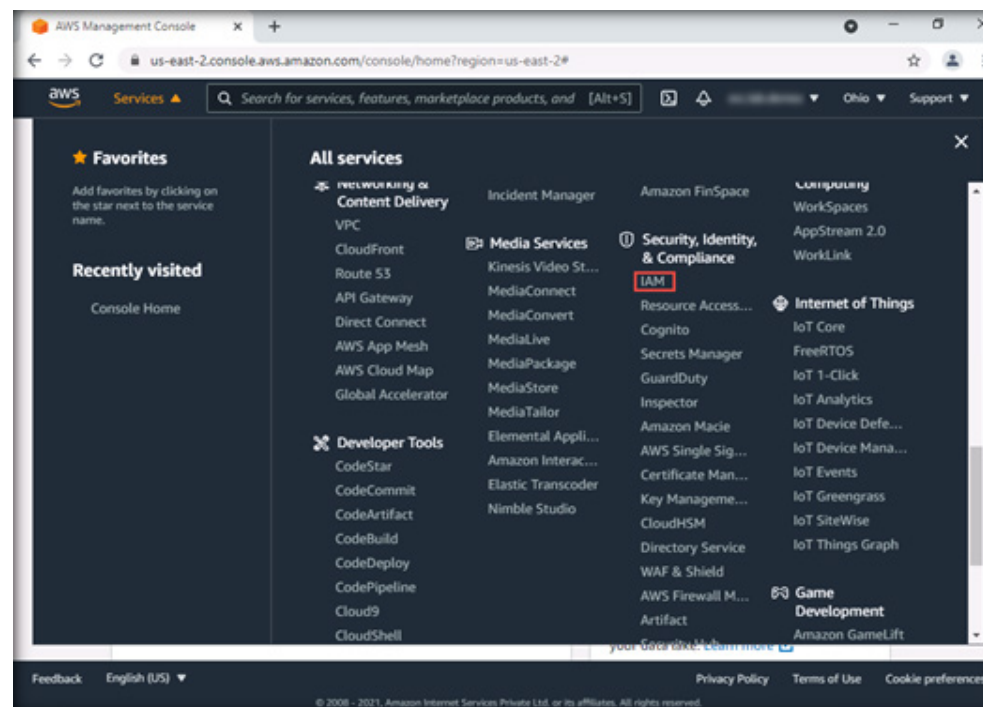
EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

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



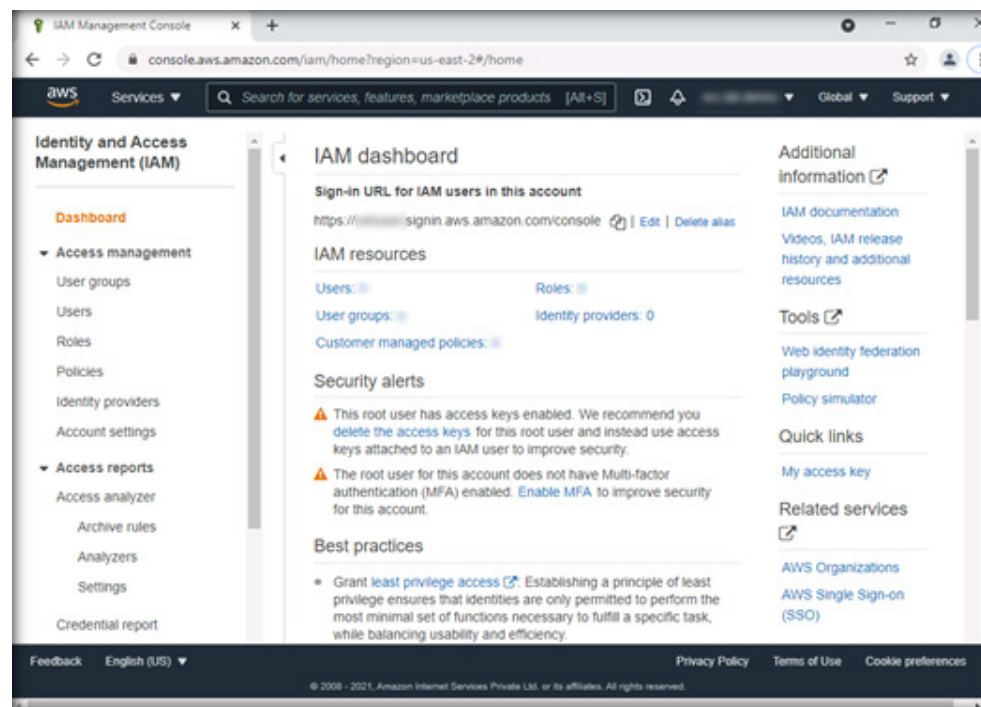
EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

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

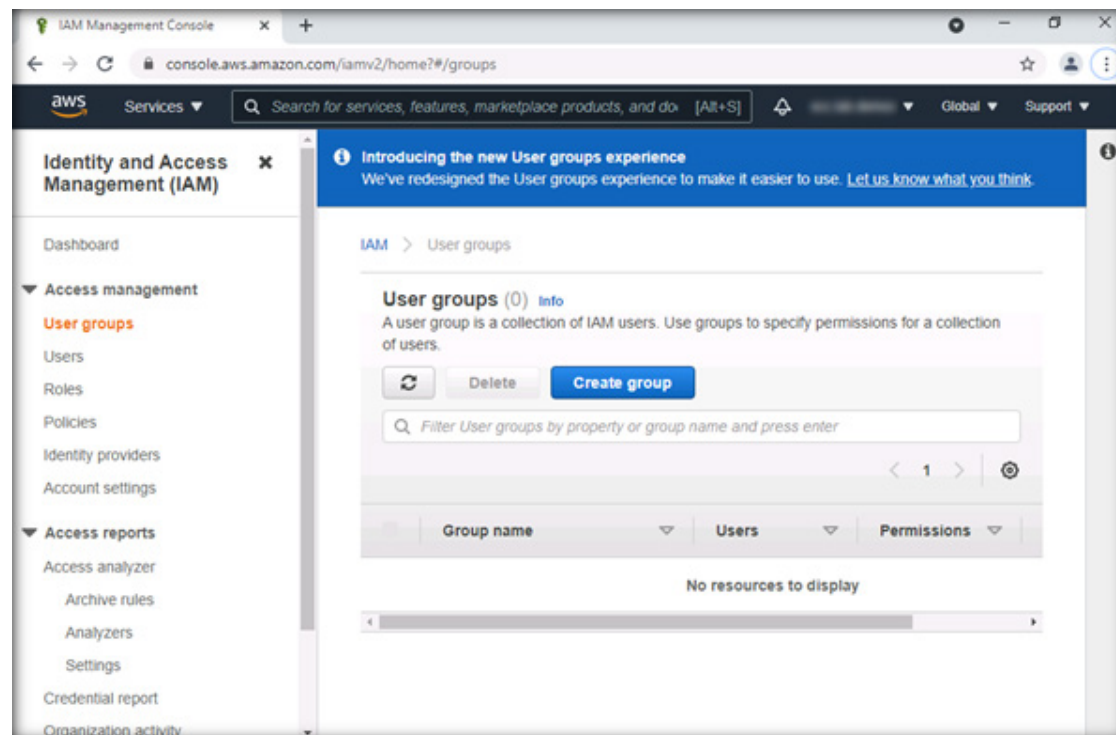


EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

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

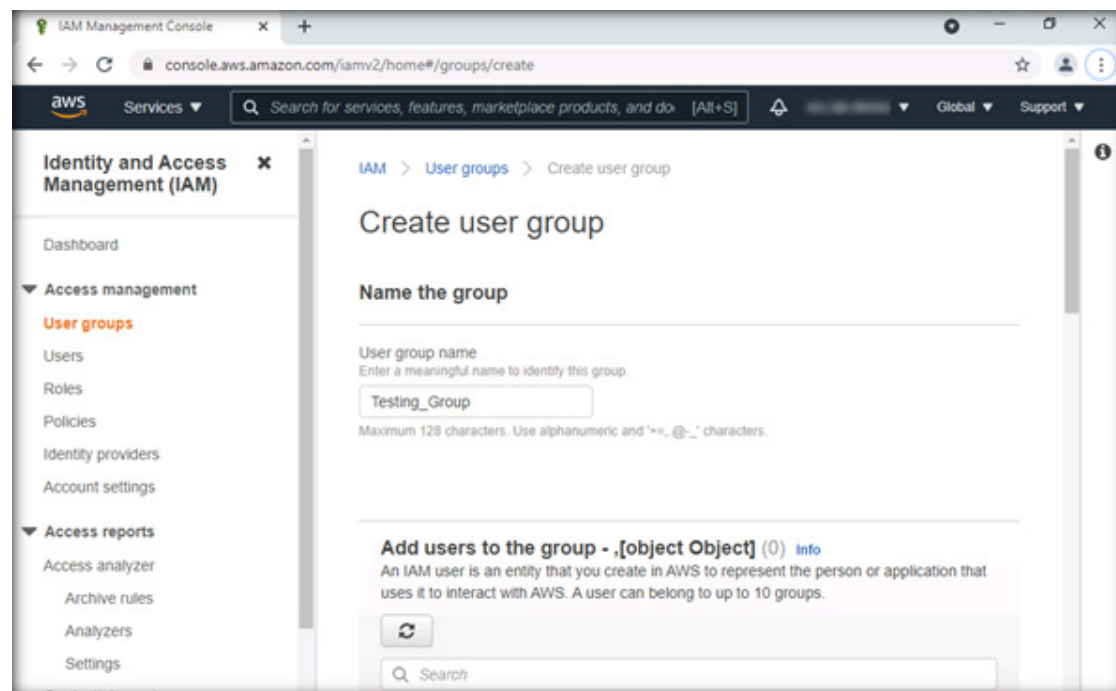


8. Now, click on Create group.

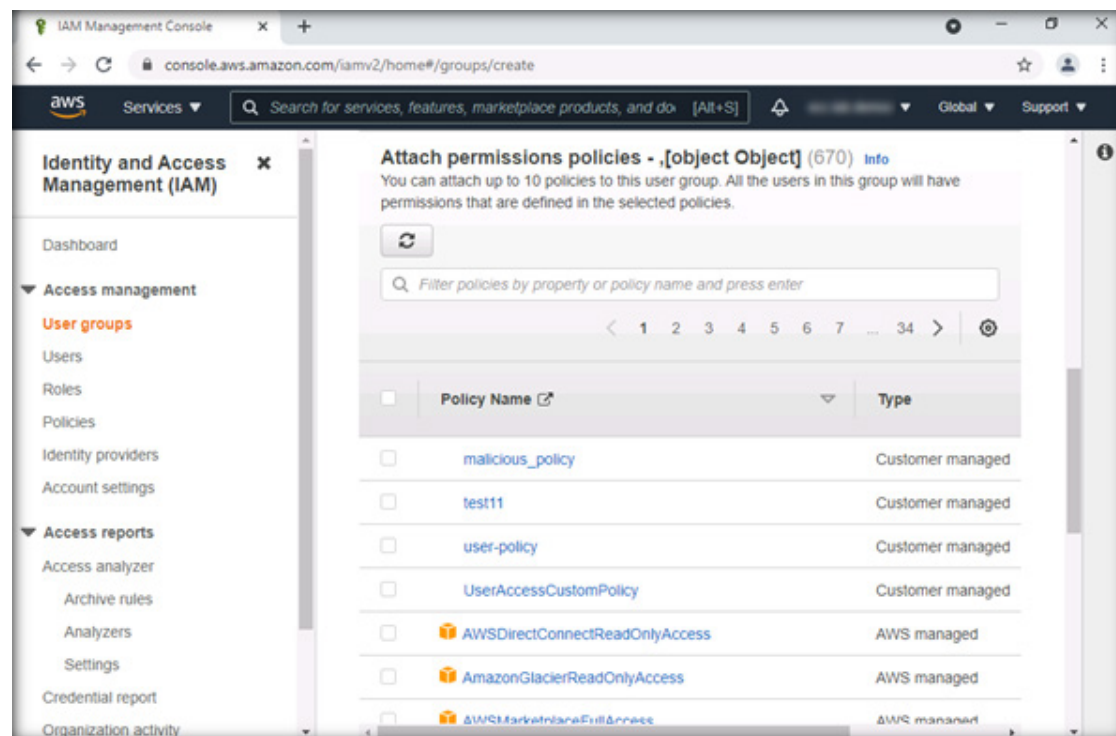


EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

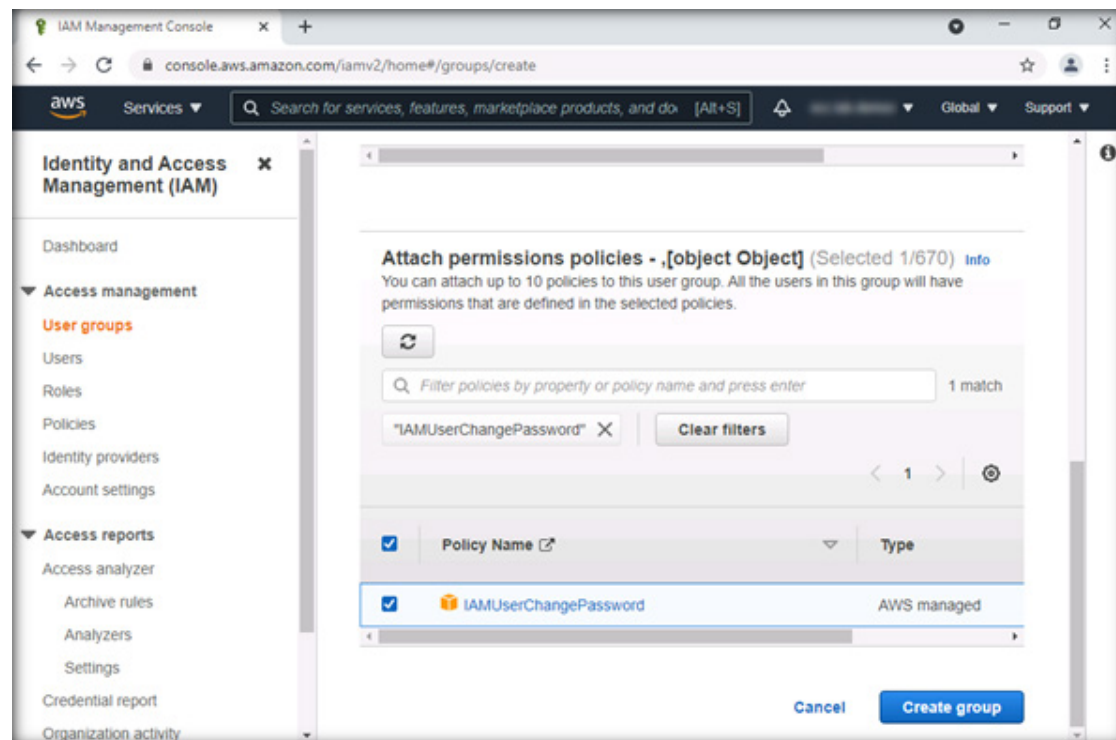
9. In the Create user group section, type the group name in the User group name field (here, the group name is Testing_Group).



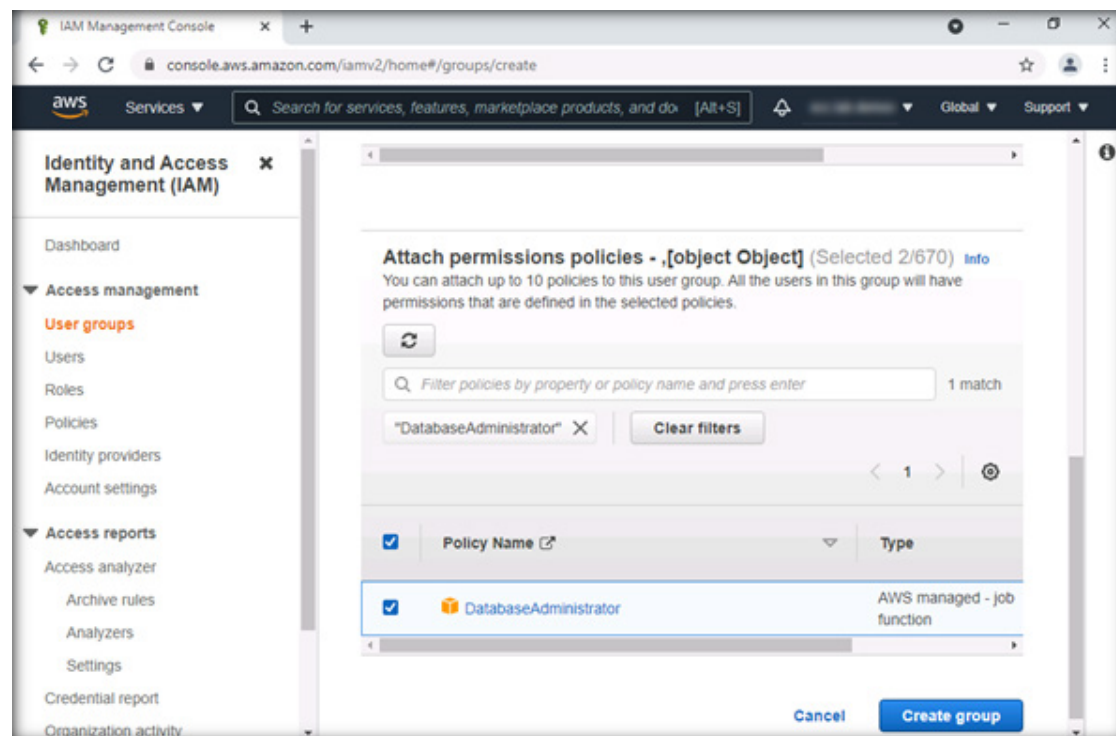
10. Scroll down to Attach permissions policies. In the Attach permissions policies section, search for IAMUserChangePassword. The match record gets filtered. Check IAMUserChangePassword.



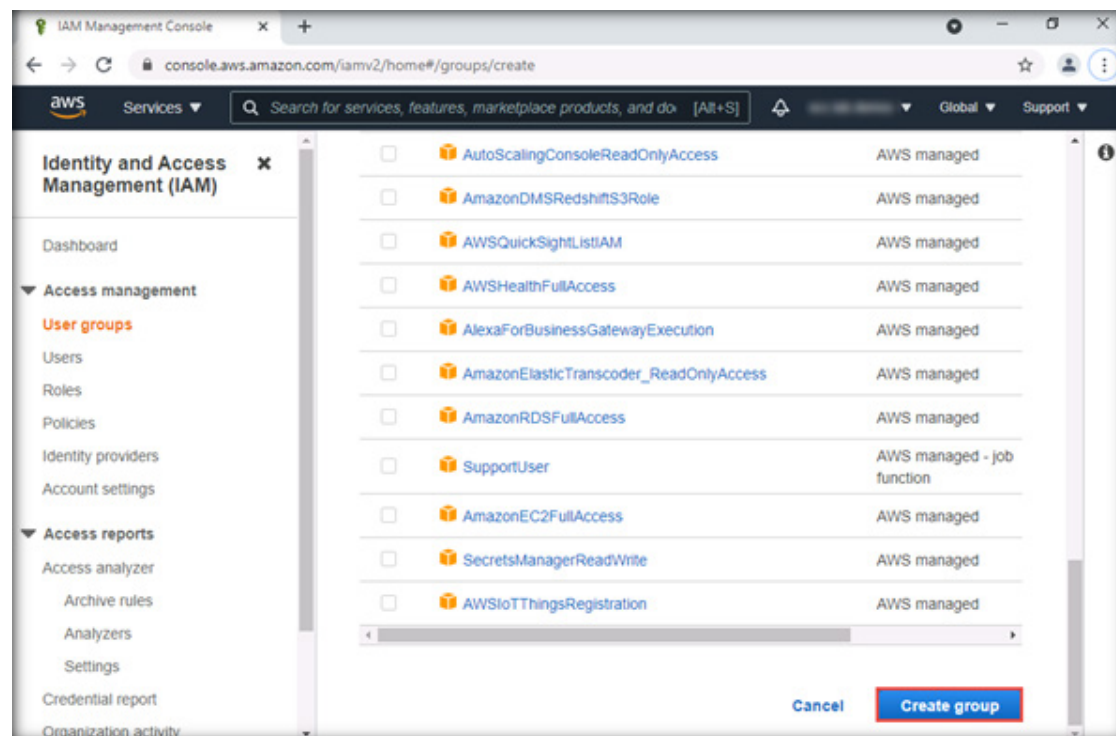
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



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

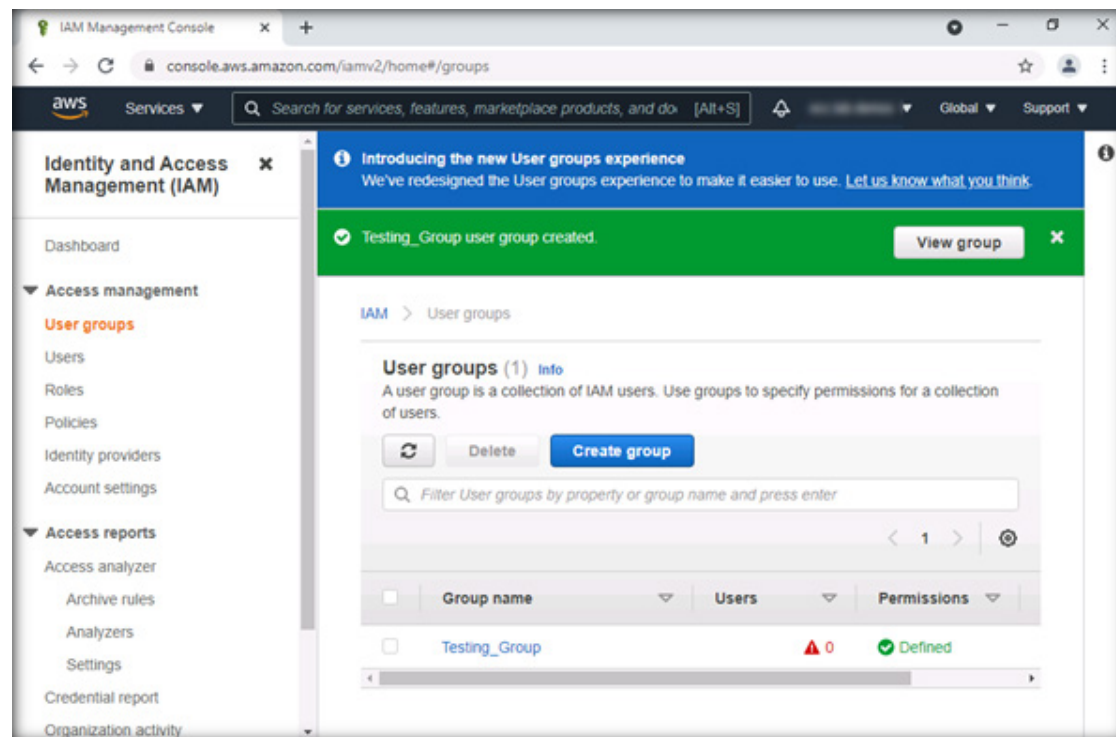


12. Scroll down the page and click on Create group.

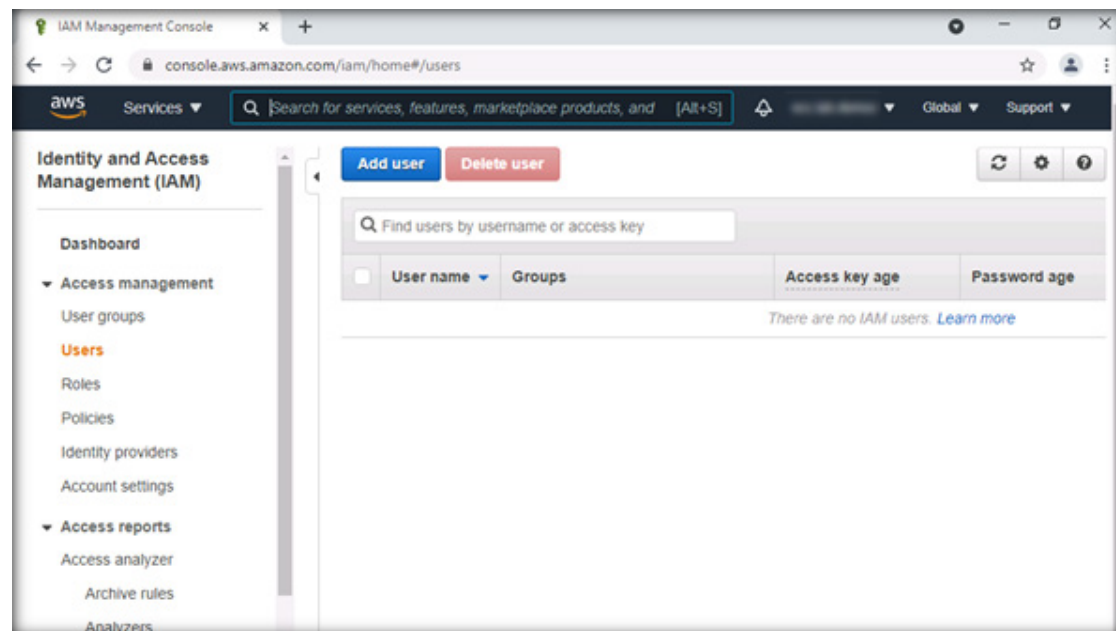


EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

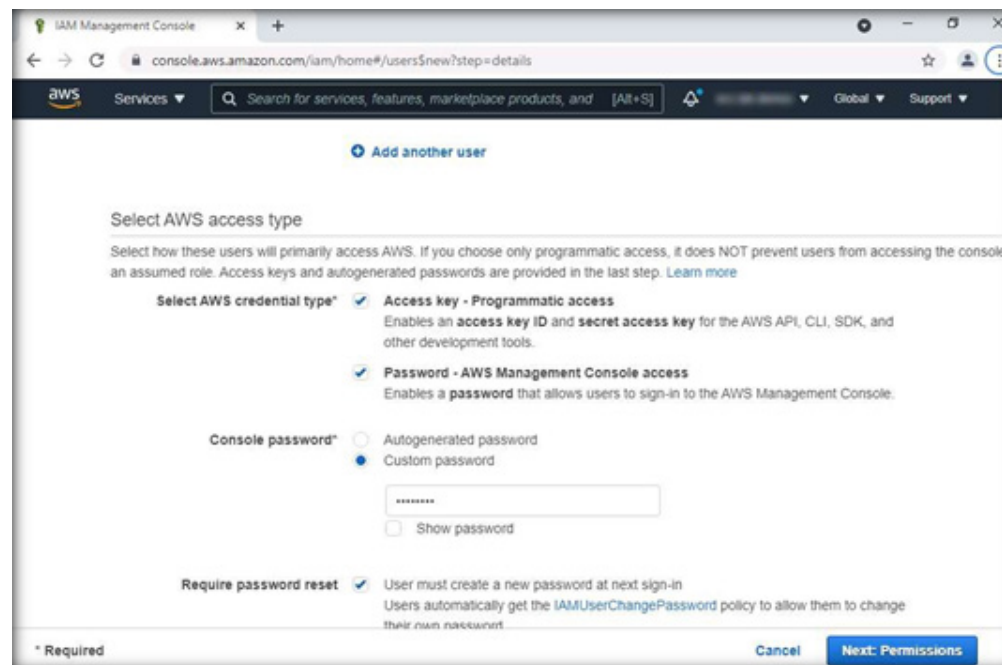
13. Testing_Group will be created under Groups as shown in the screenshot below.



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



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.



add AWS IAM Management Console

console.aws.amazon.com/iam/home#/users\$new?step=details

Services Search for services, features, marketplace products, and [Alt+S]

Global Support

+ Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console as an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

- ☒ Access key - Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ Password - AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

- ☐ Autogenerated password
- ☒ Custom password

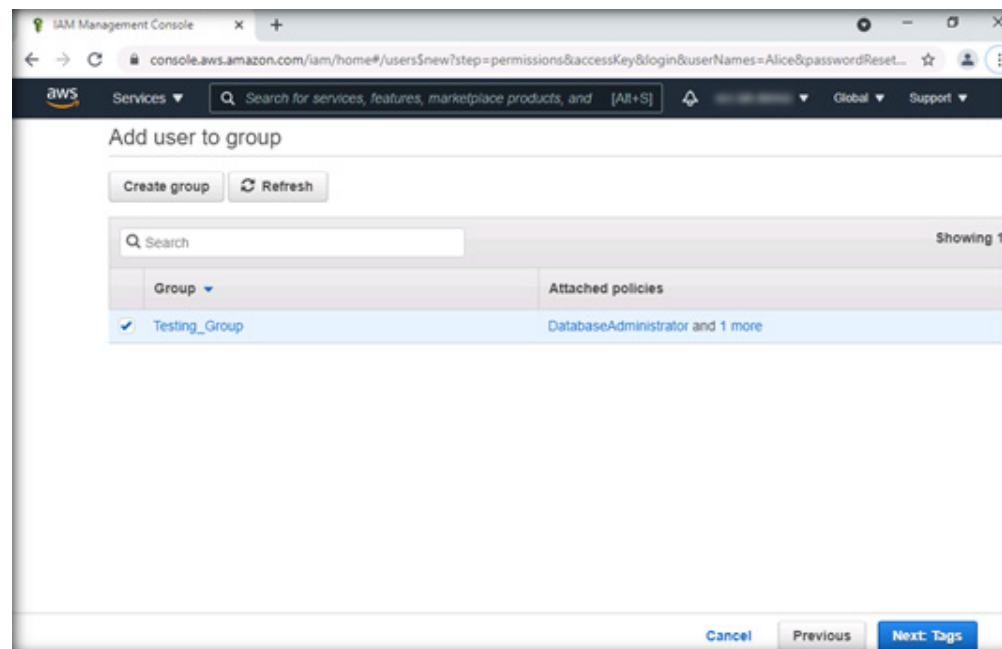
☐ Show password

Require password reset ☒ User must create a new password at next sign-in
Users automatically get the `iam:UserChangePassword` policy to allow them to change their own password.

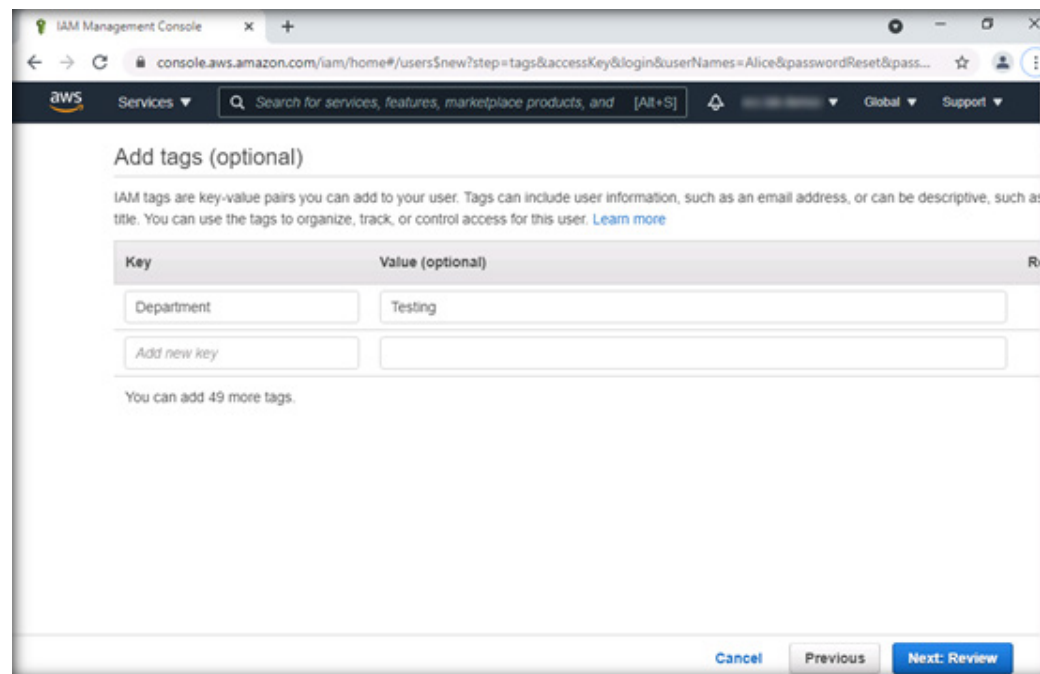
* Required

Cancel Next: Permissions

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.



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.



Add tags (optional)

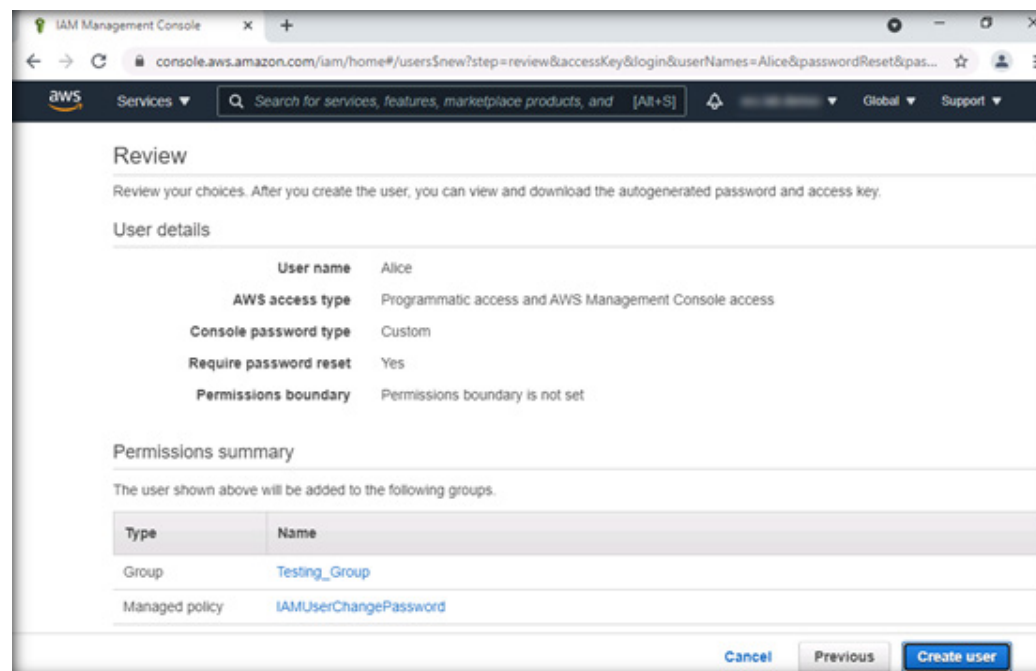
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)
Department	Testing
Add new key	

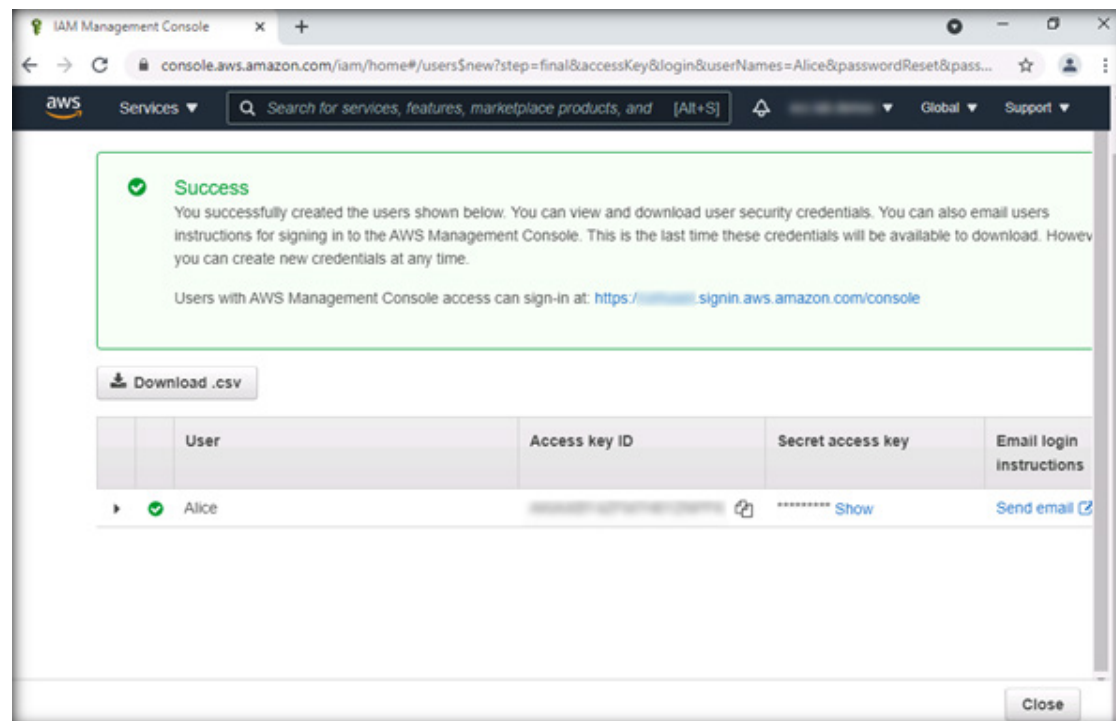
You can add 49 more tags.

[Cancel](#) [Previous](#) [Next: Review](#)

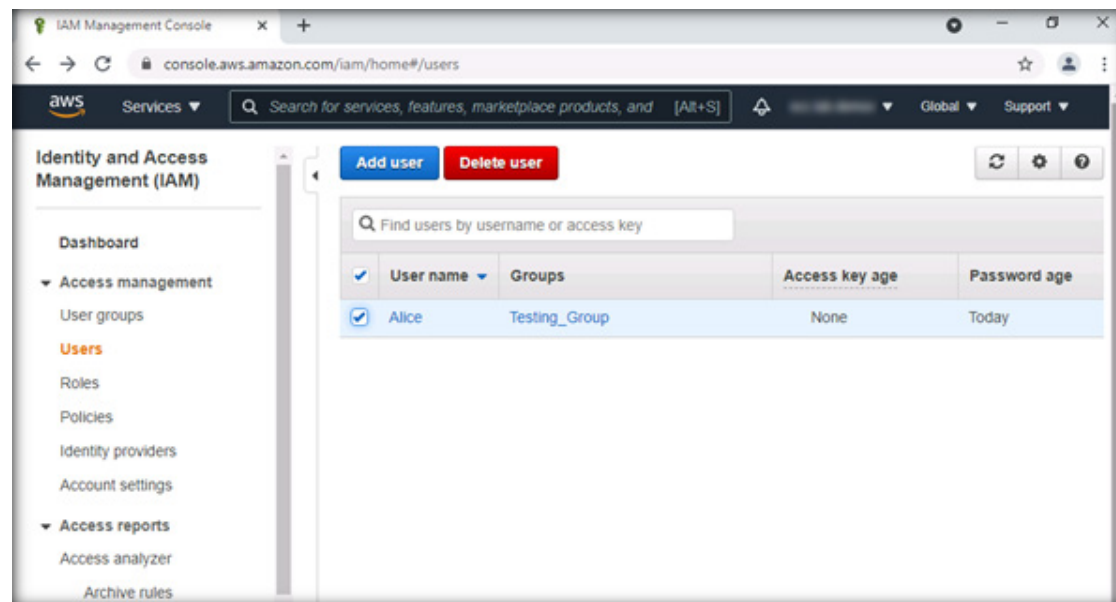
19. On the Review page, we will be able to view the settings and IAM User properties before creating the user. Once you have verified the settings, click on Create user.



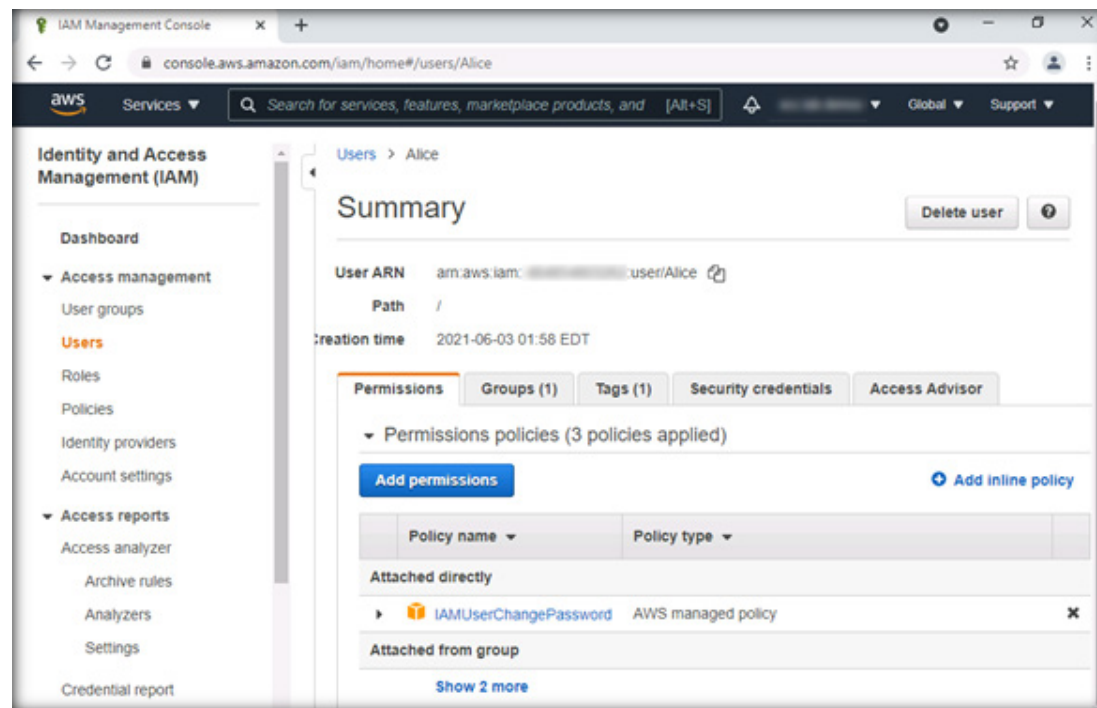
20. After you click on Create user, a Success message is displayed. You have an option to Send Email to get the login instructions for the newly created IAM User. Click on Close (lower right corner of the page) to return to the IAM page. It will redirect you to the Users page.



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.

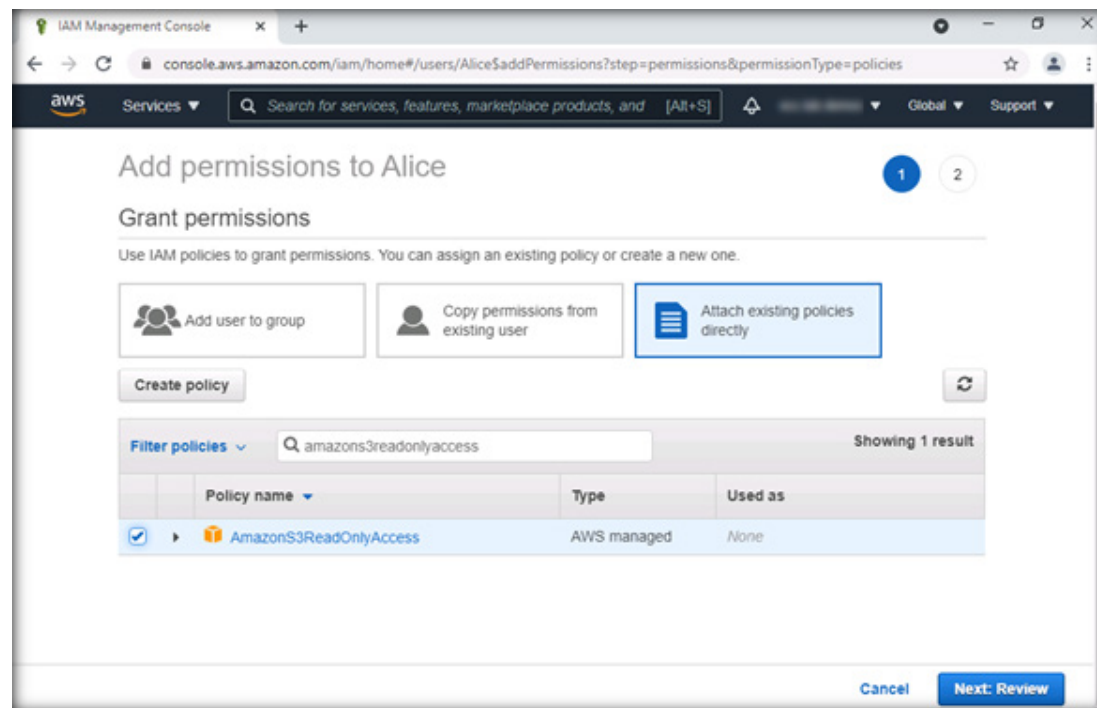


22. The Summary page appears (here, it appears for Alice). Click on Add permissions.

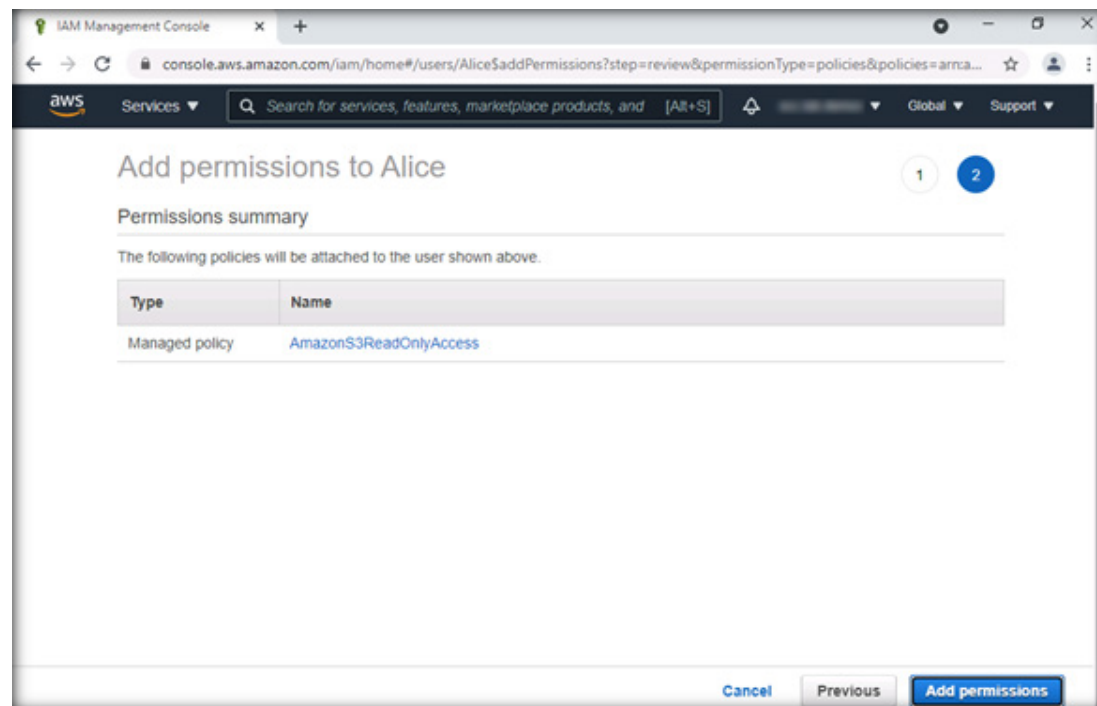


23. In the Grant permissions page, click on Attach existing policies directly.

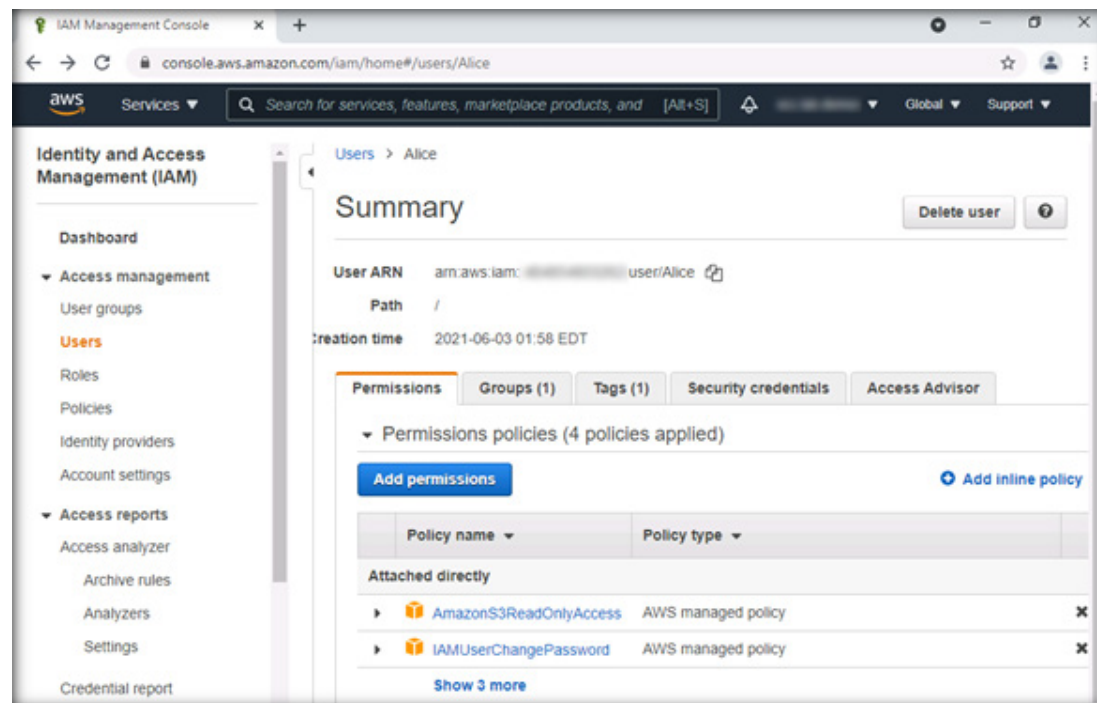
24. In the Filter policies field, search for amazons3readonlyaccess. This will display all pre-configured policies for S3. Select AmazonS3ReadOnlyAccess, and click on Next: Review.



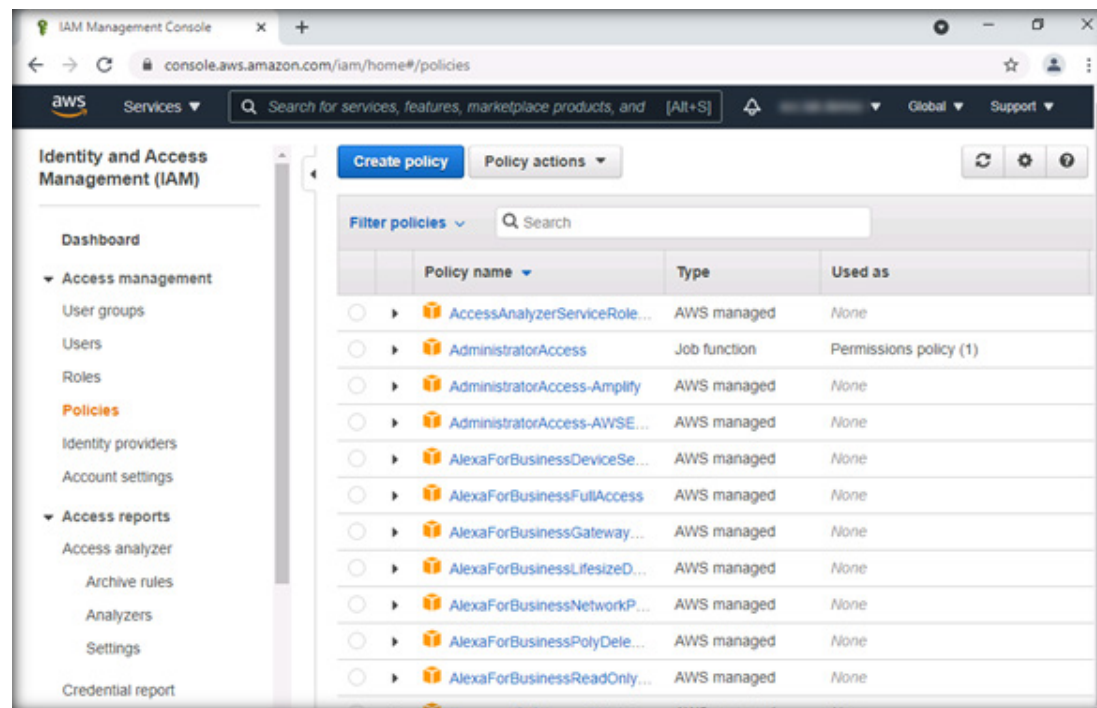
25. In the Permissions summary page, review the assigned policies to the IAM User. After you have reviewed the policies, click on Add permissions.



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

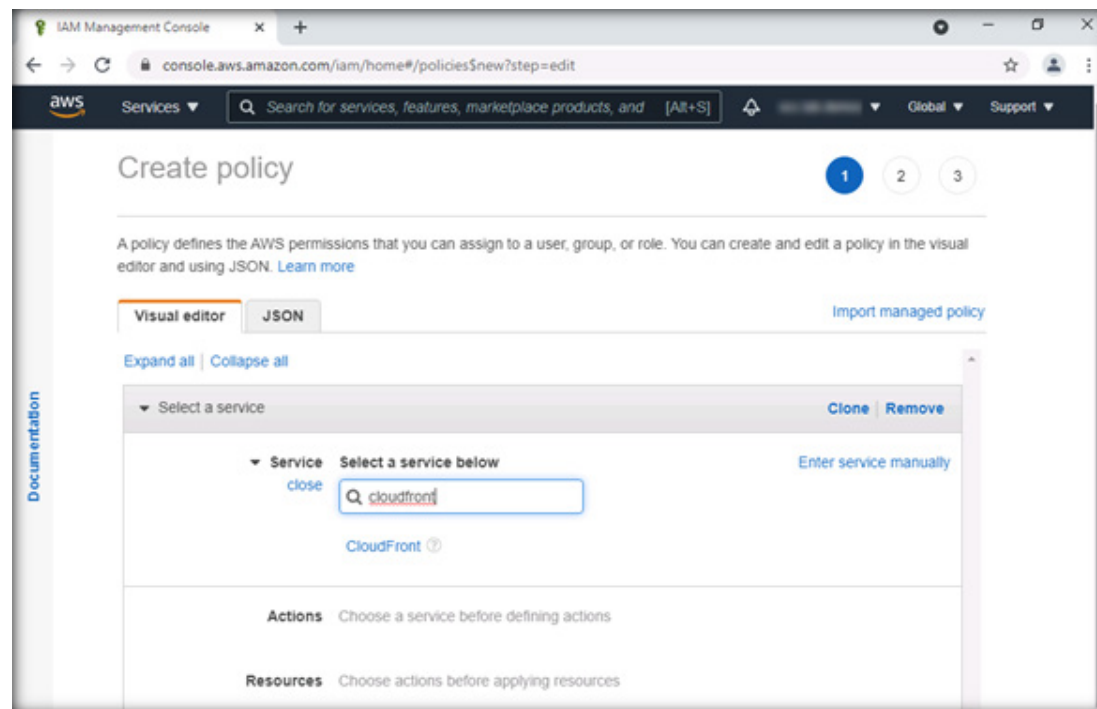


27. Next, we will create a custom IAM policy. Click on Policies under the Identity and Access Management (IAM) console. Click on Create policy.

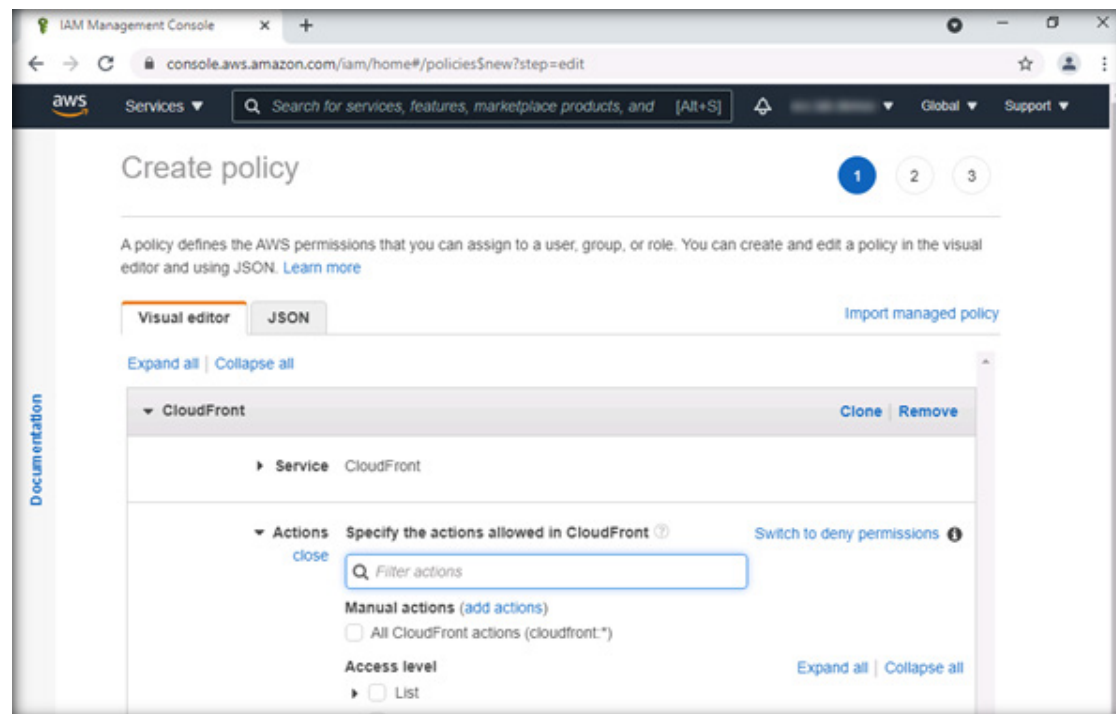


EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

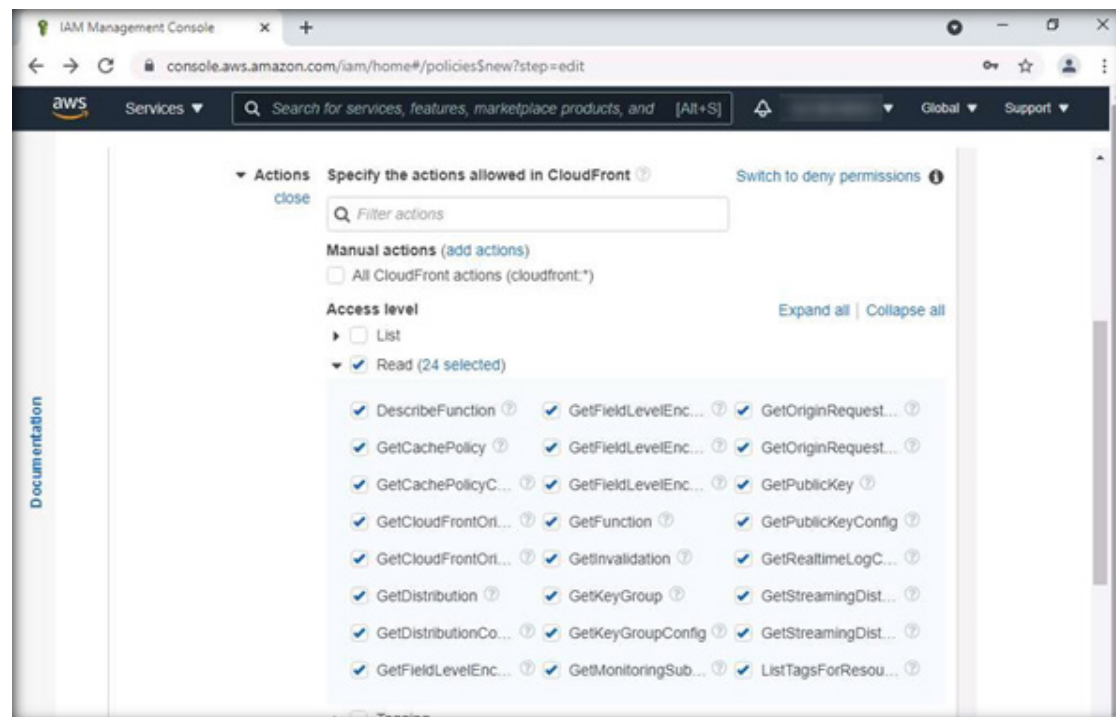
28. Click the link Choose a service, specify the service that you wish to use and edit the permissions. In this example, let us use CloudFront on Service.



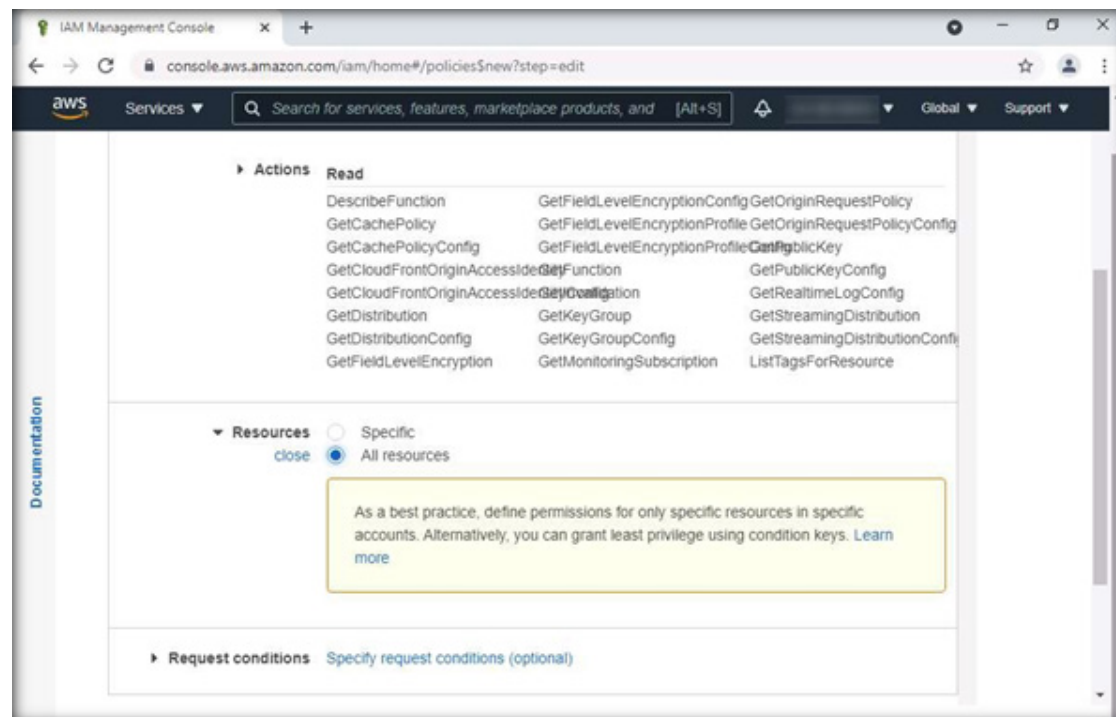
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



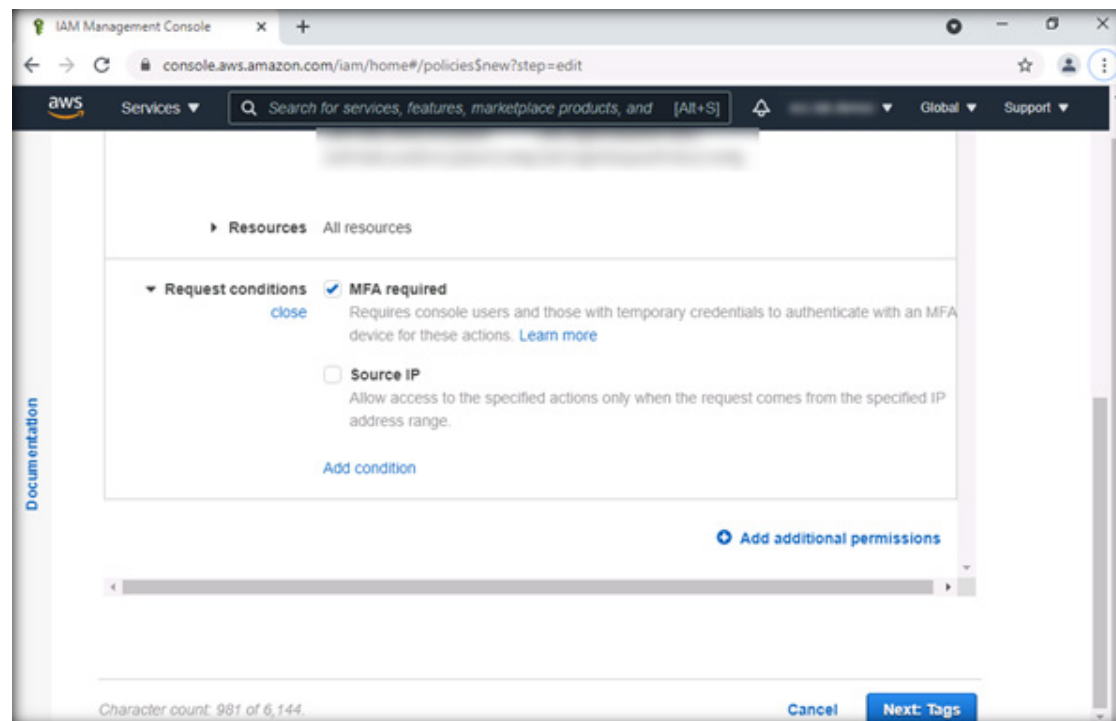
29. Expand the Actions menu to select the Access level for CloudFront service. In this example, let us enable only Read access for CloudFront. Note: The number of Read access policies might vary in your lab environment.



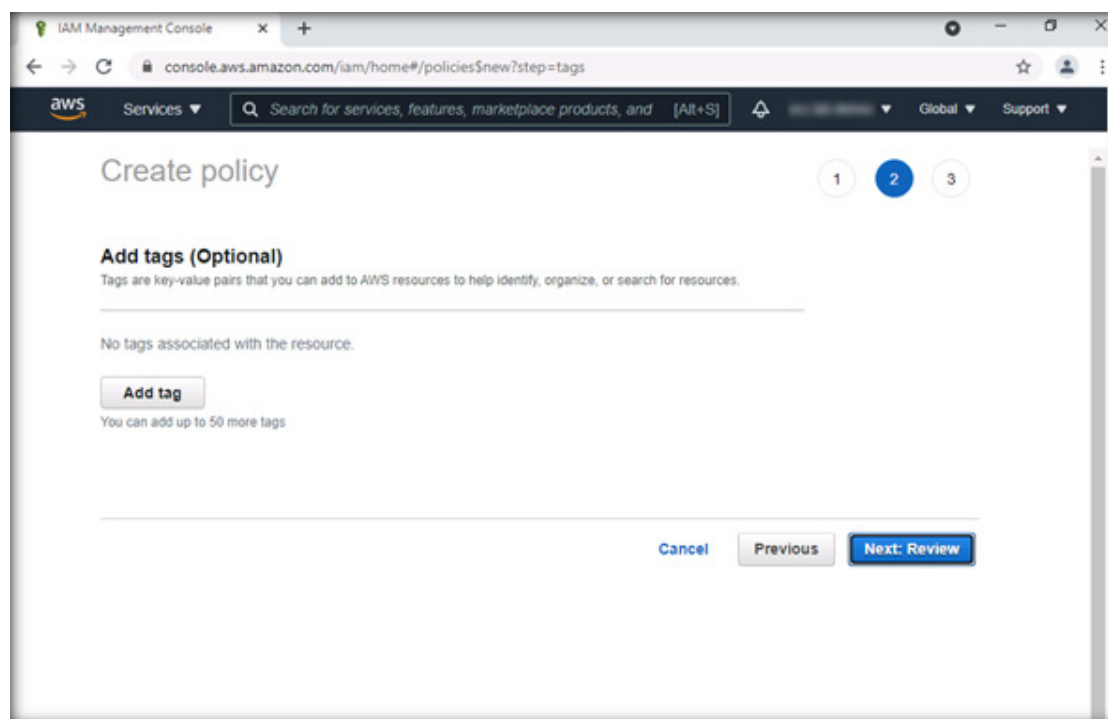
30. Scroll down and expand the Resources section. Select All resources radio button.



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

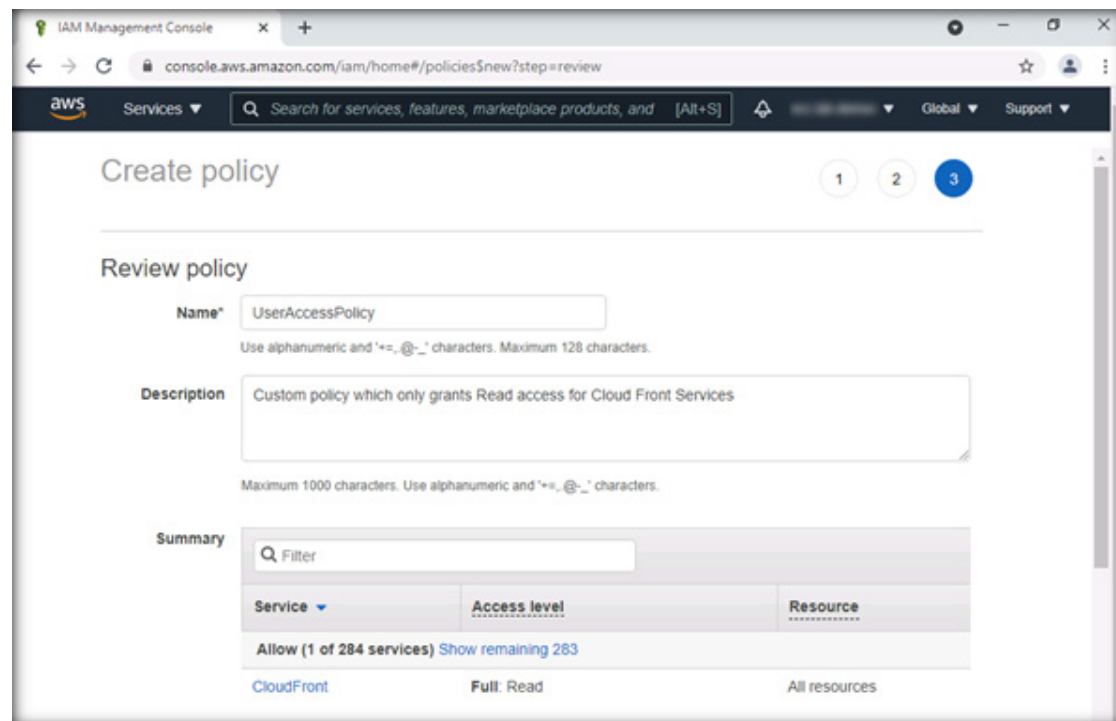


32. In the Add tags section click on Next: Review.



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

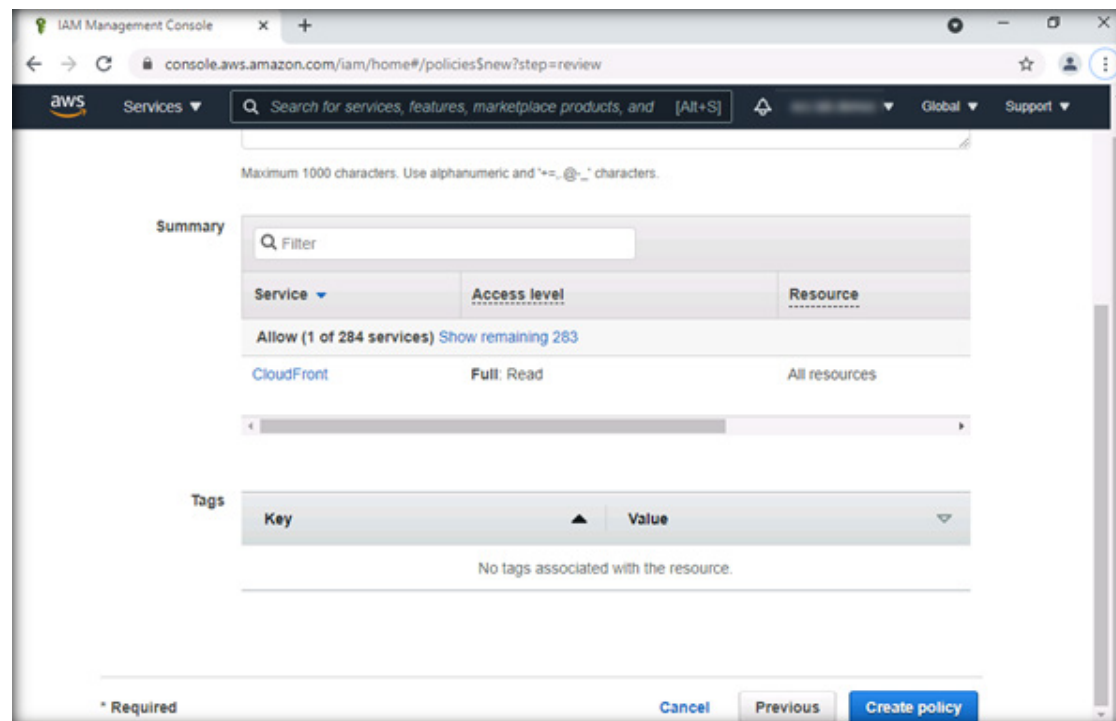
33. In the Review policy section, provide a name for the policy in the Name field and add a description in the Description field.



The screenshot shows the AWS IAM Management Console 'Create policy' page, specifically the 'Review policy' step (step 3 of 3). The 'Name' field is filled with 'UserAccessPolicy' and the 'Description' field contains 'Custom policy which only grants Read access for Cloud Front Services'. Below the description is a 'Summary' section with a search filter and a table of permissions.

Service	Access level	Resource
Allow (1 of 284 services) Show remaining 283		
CloudFront	Full: Read	All resources

34. Scroll down and click on Create policy.



The screenshot shows the 'Create policy' review step in the AWS IAM Management Console. The browser address bar shows the URL: `console.aws.amazon.com/iam/home#/policies$new?step=review`. The page has a dark header with the AWS logo and navigation links. Below the header, there is a search bar and a note: 'Maximum 1000 characters. Use alphanumeric and '+=, @, _' characters.'

The main content area is divided into two sections: 'Summary' and 'Tags'.

Summary

There is a search filter input field. Below it is a table with three columns: 'Service', 'Access level', and 'Resource'.

Service	Access level	Resource
CloudFront	Full: Read	All resources

Below the table, it says 'Allow (1 of 284 services) Show remaining 283'.

Tags

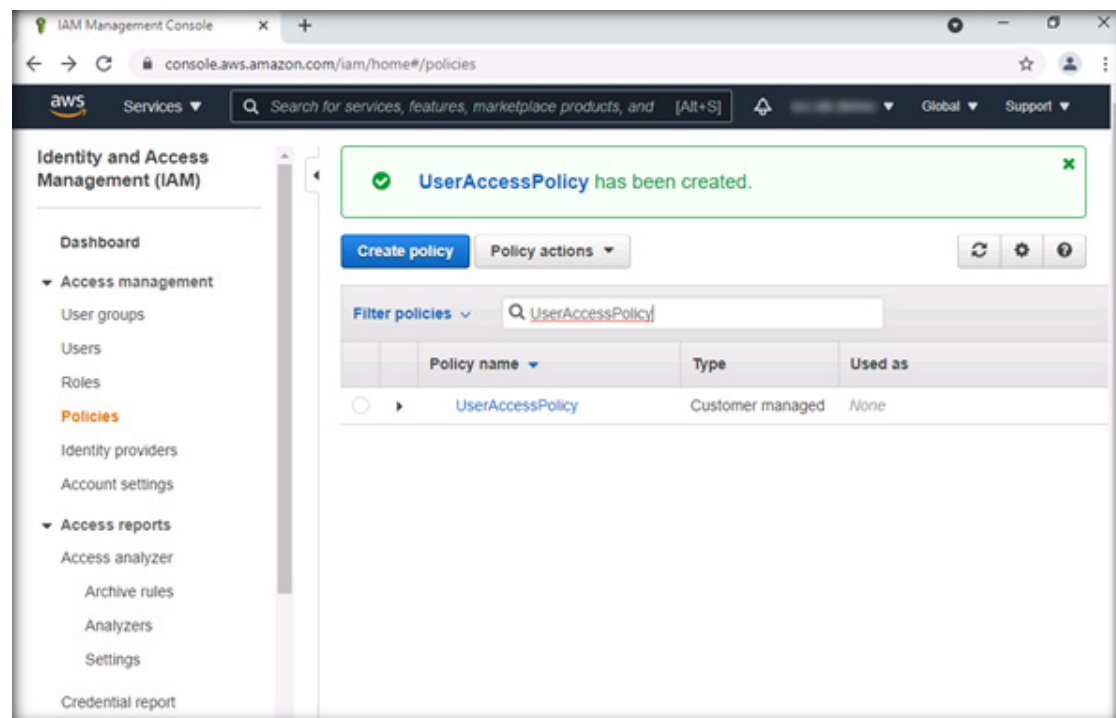
There is a table with two columns: 'Key' and 'Value'.

Key	Value
No tags associated with the resource.	

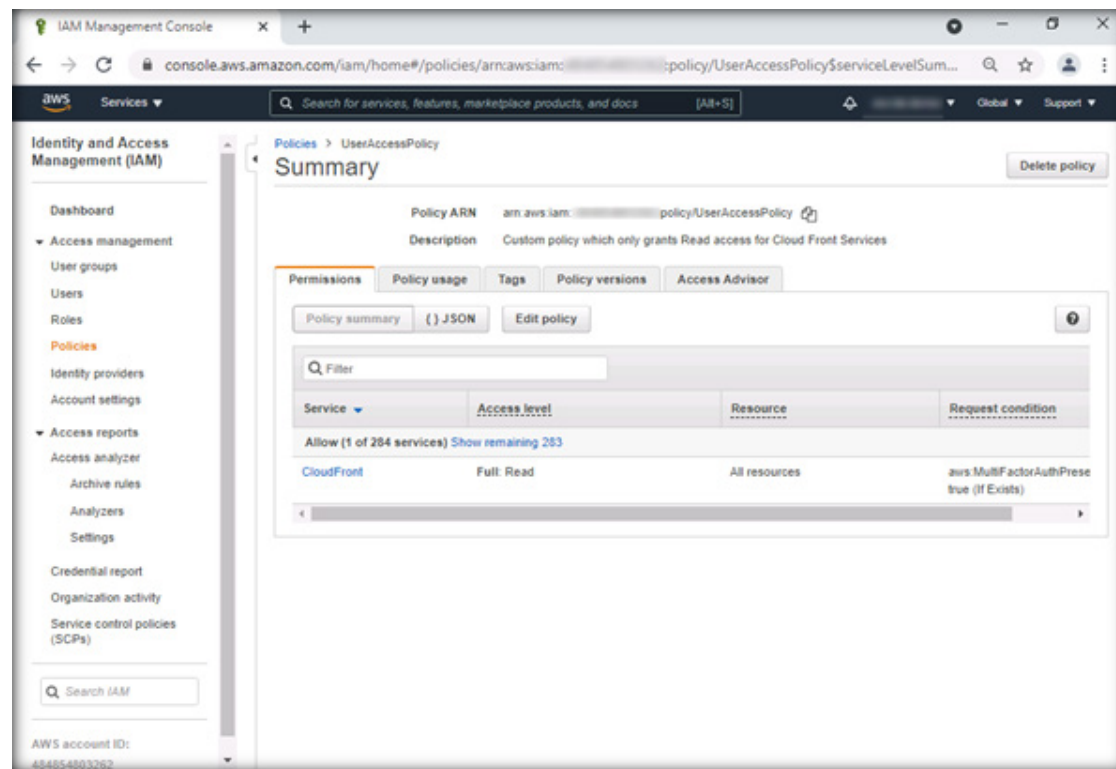
At the bottom of the page, there are three buttons: 'Cancel', 'Previous', and 'Create policy'.

EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

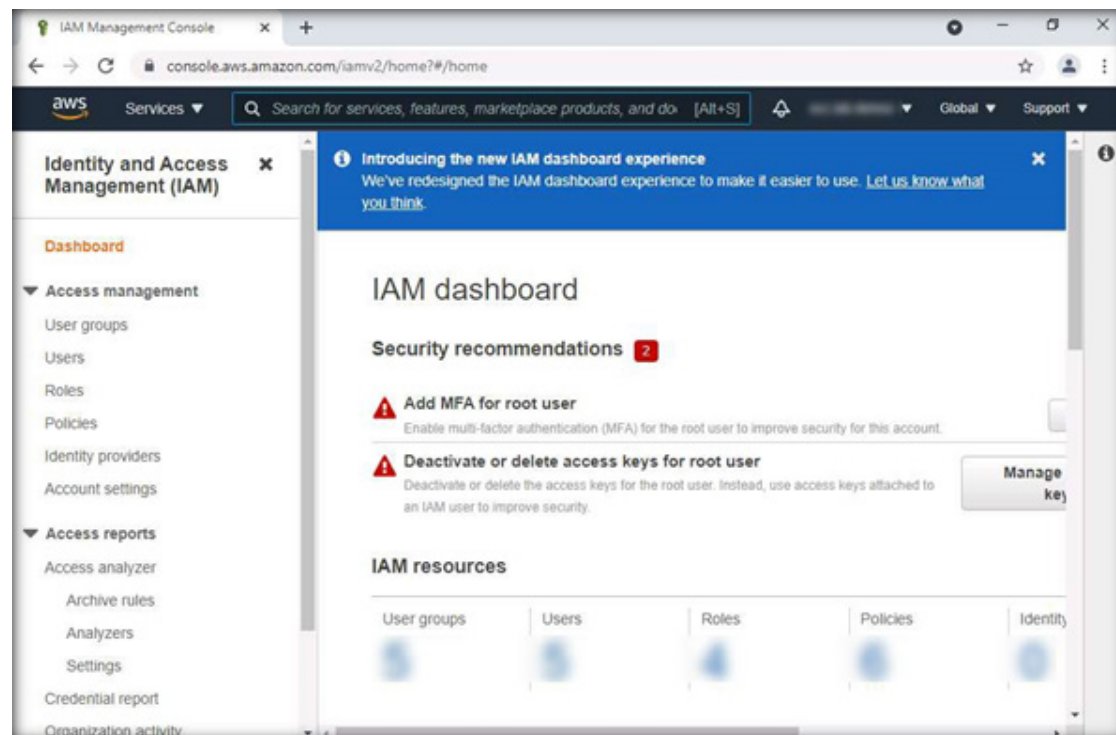
35. The new policy will be successfully created. To check the created policy, click on Policies, type the name of the policy in the search box of Filter policies, then click on the selected policy.



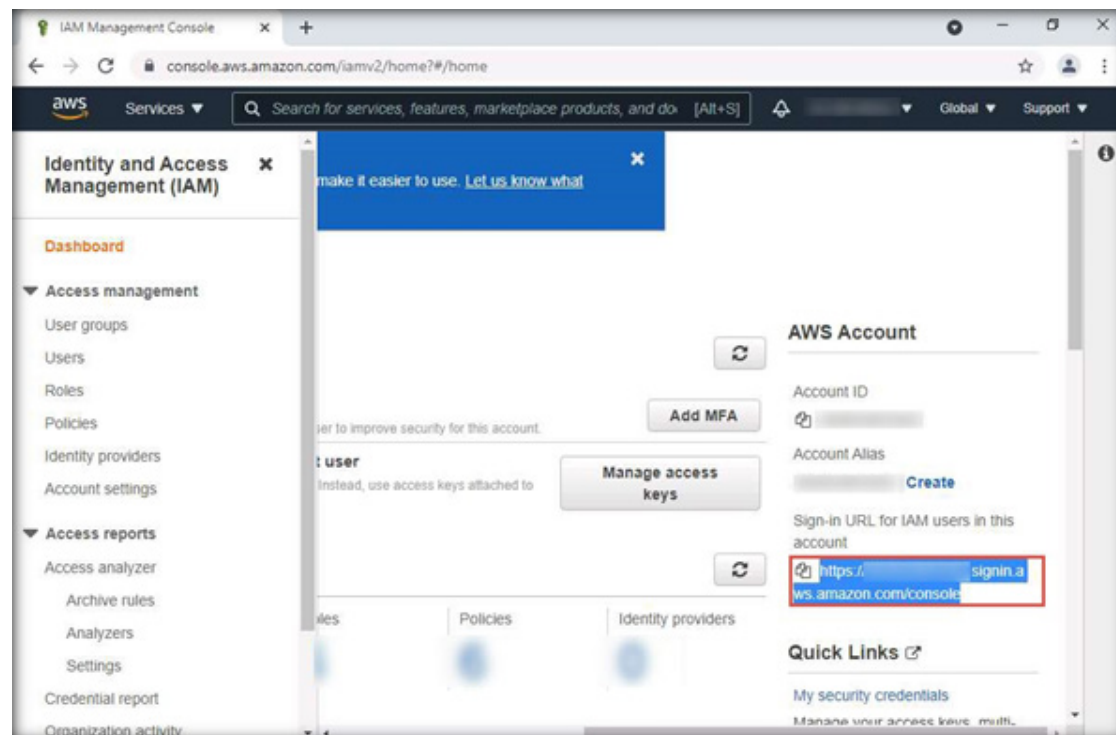
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT



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

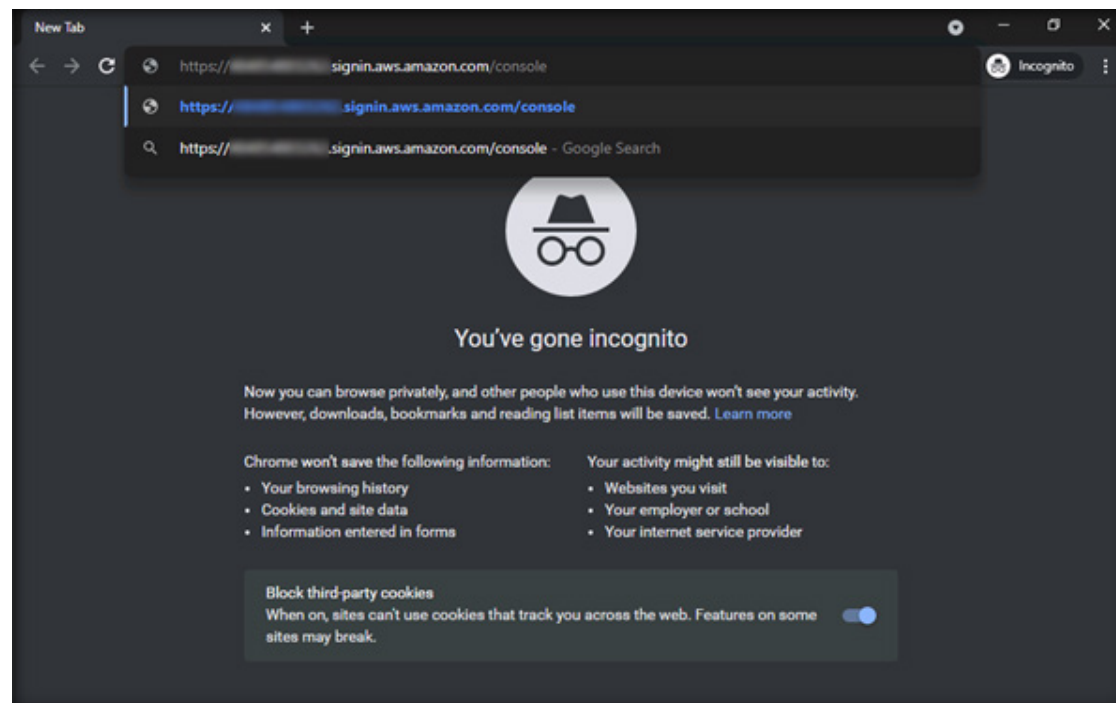


37. You can see the IAM users sign-in link under AWS Account, copy the link.

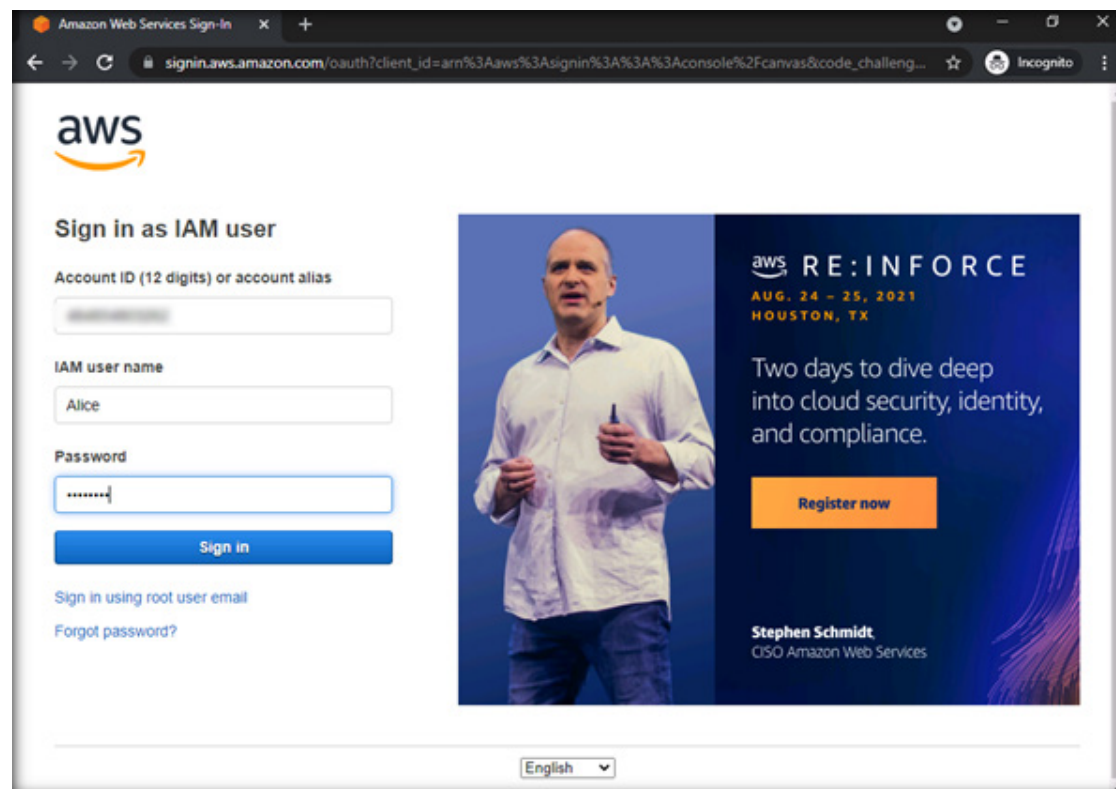


EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

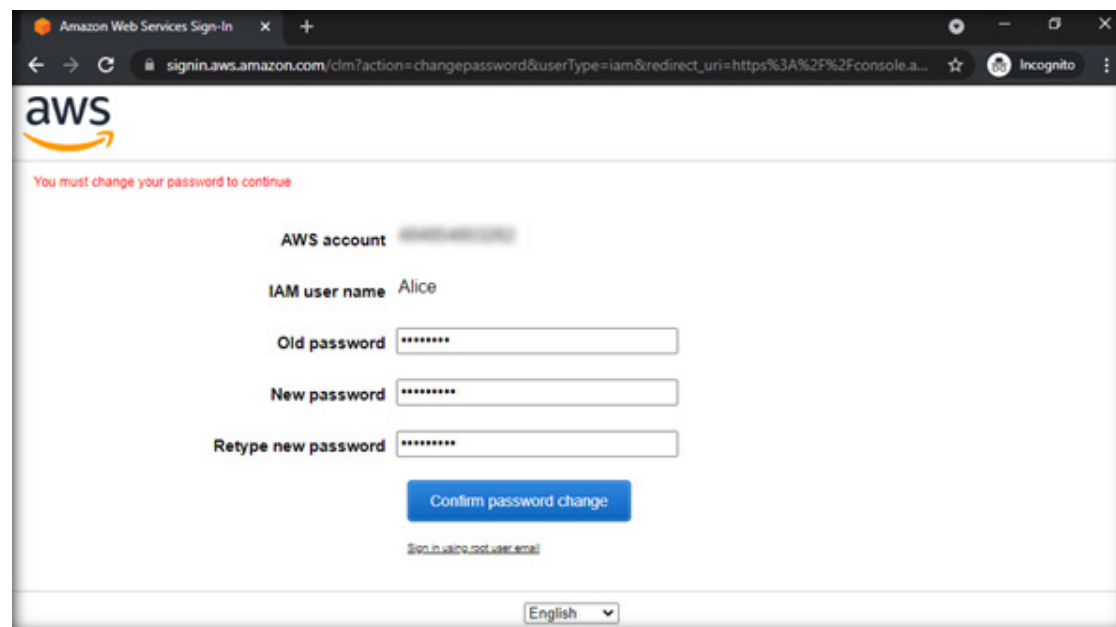
38. Open the Google Chrome browser in incognito mode, paste the copied URL, and press the Enter button.



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.



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



Amazon Web Services Sign-In x +

sign-in.aws.amazon.com/clm?action=change-password&userType=iam&redirect_uri=https%3A%2F%2Fconsole.a...

aws

You must change your password to continue

AWS account [REDACTED]

IAM user name Alice

Old password [REDACTED]

New password [REDACTED]

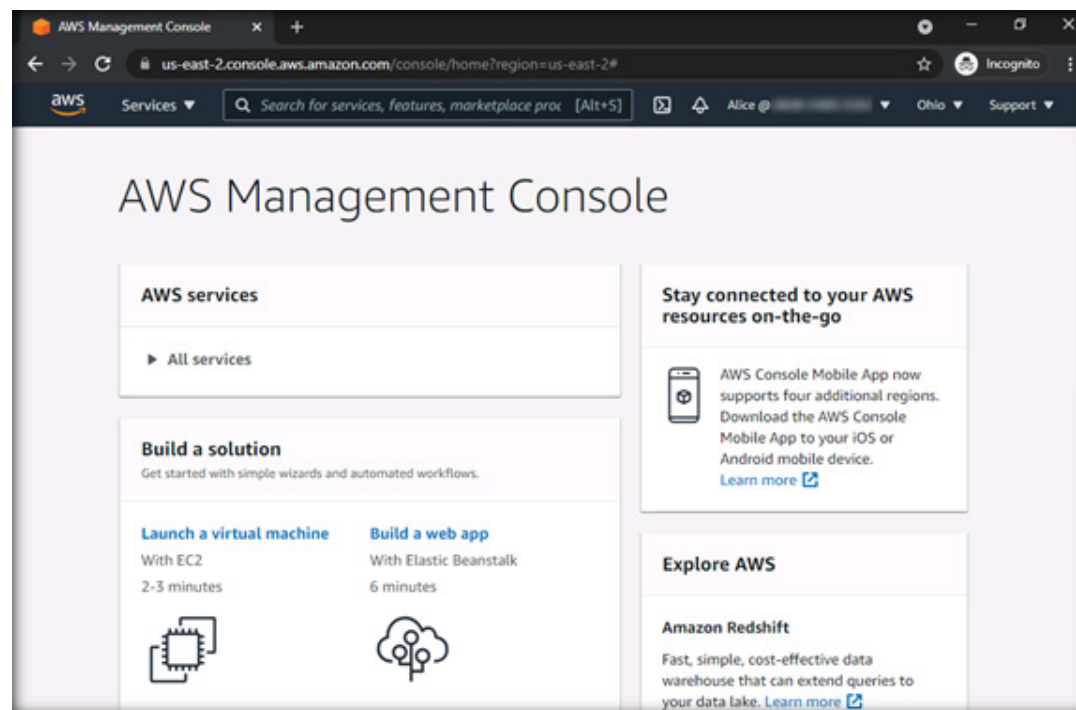
Retype new password [REDACTED]

Confirm password change

[Sign in using your user email](#)

English

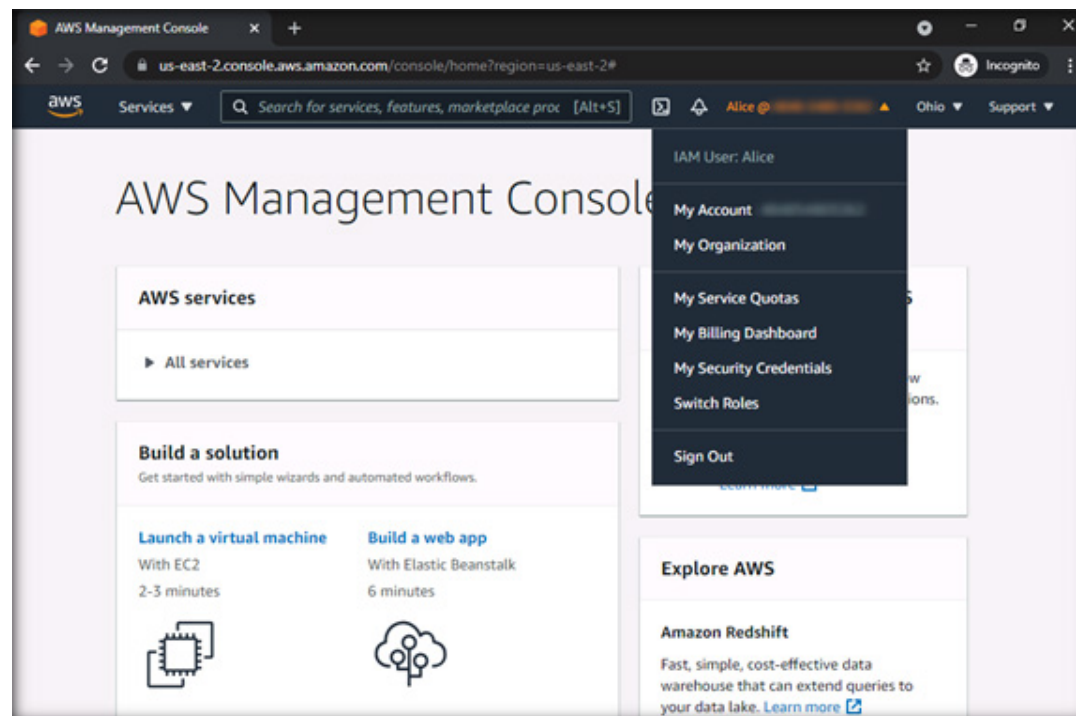
41. User Alice is now logged in as an IAM user.



EXERCISE 3:
IMPLEMENT
AWS IDENTITY
AND ACCESS
MANAGEMENT

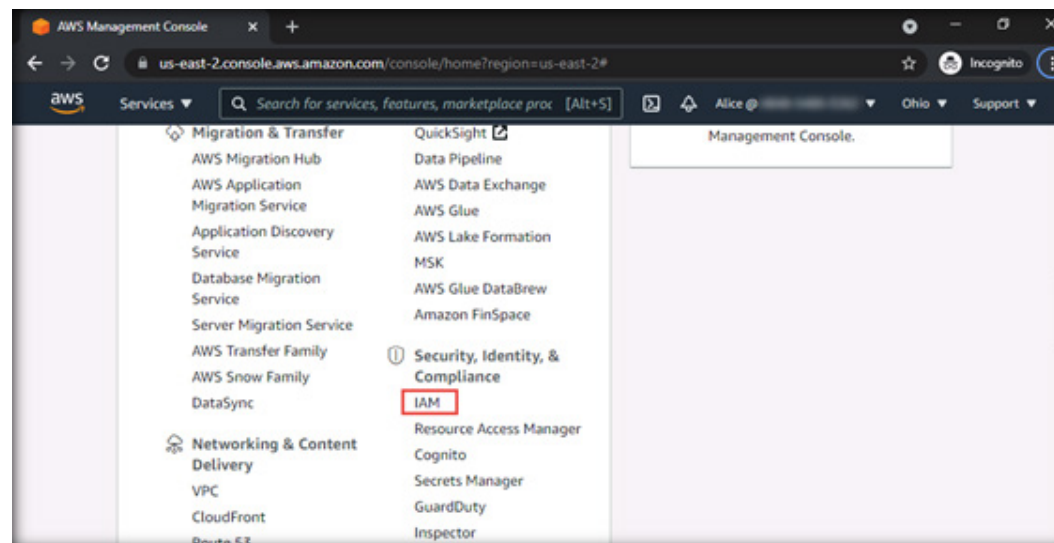
42. We have given only Read permission to Alice who can access only limited resources.

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.



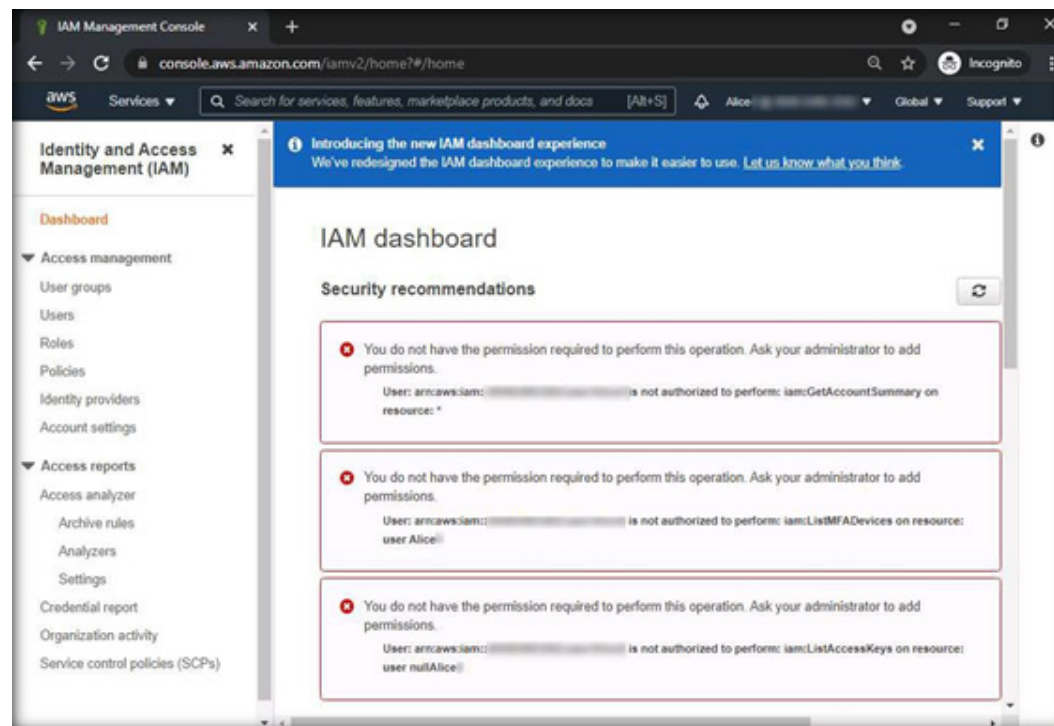
EXERCISE 3: IMPLEMENT AWS IDENTITY AND ACCESS MANAGEMENT

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

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



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.

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.

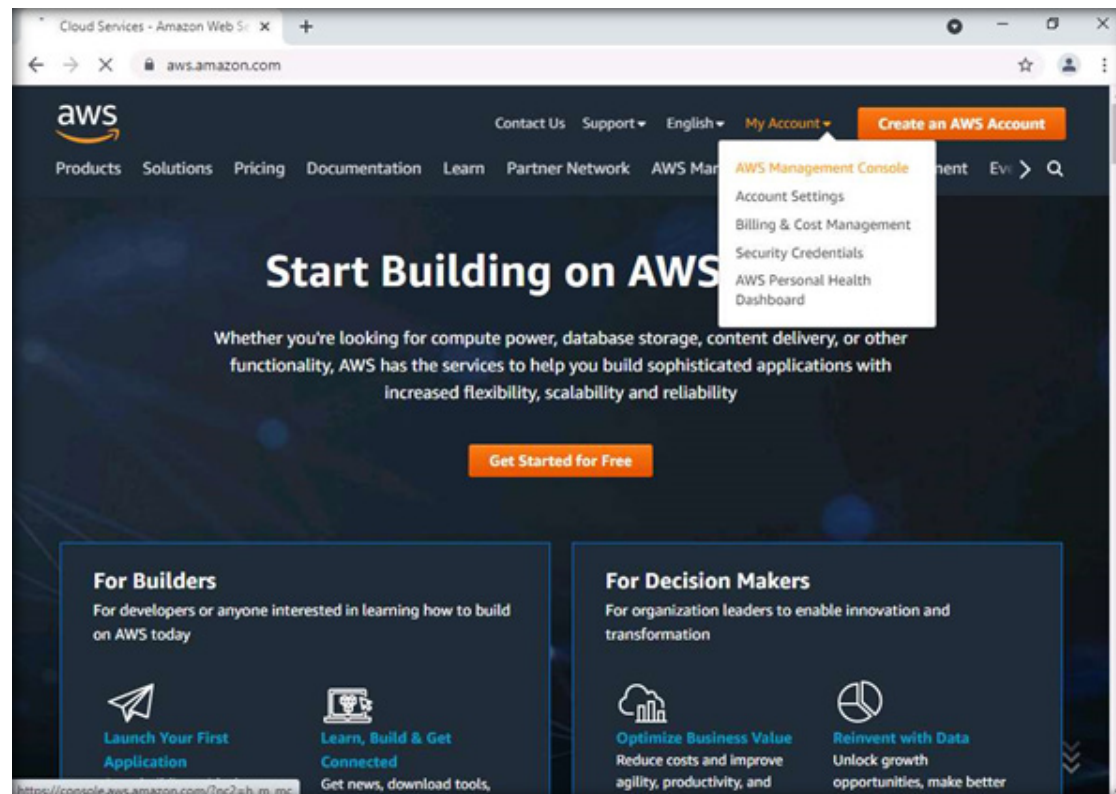
Note: You need to execute Exercise 3 of this module before executing this lab as the user and group created in the previous lab are used in this lab.

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.

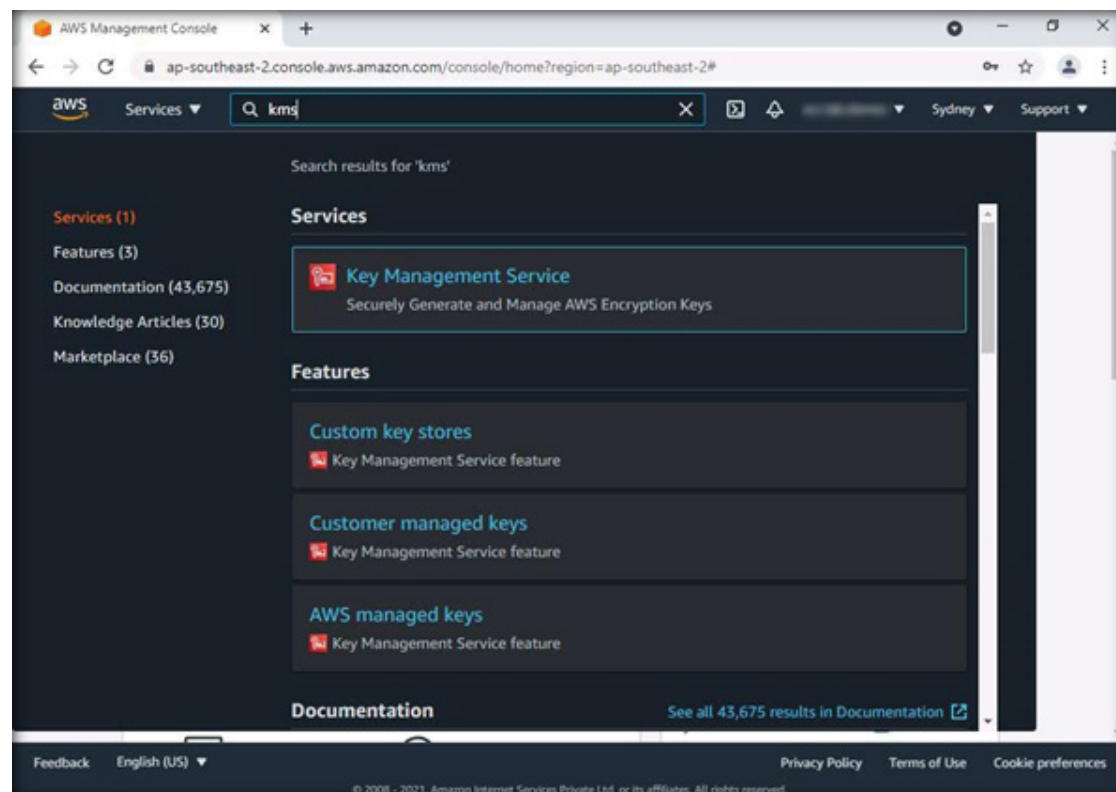
2. The Google Chrome browser opens. Go to the address bar, type `https://aws.amazon.com/`, and press Enter.

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.



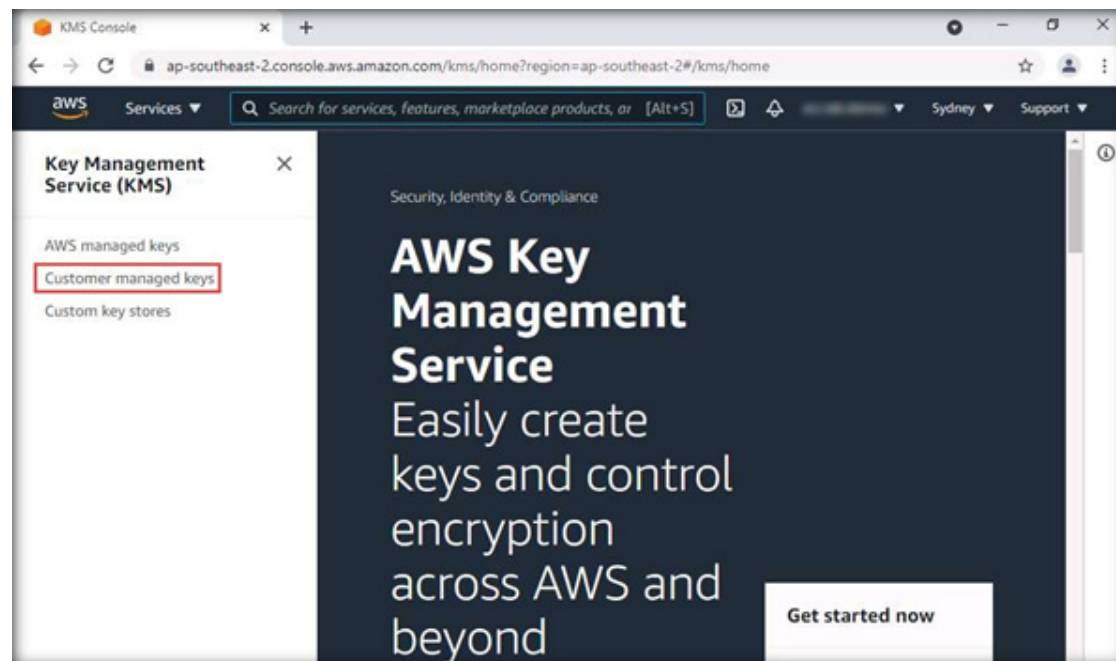
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

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.



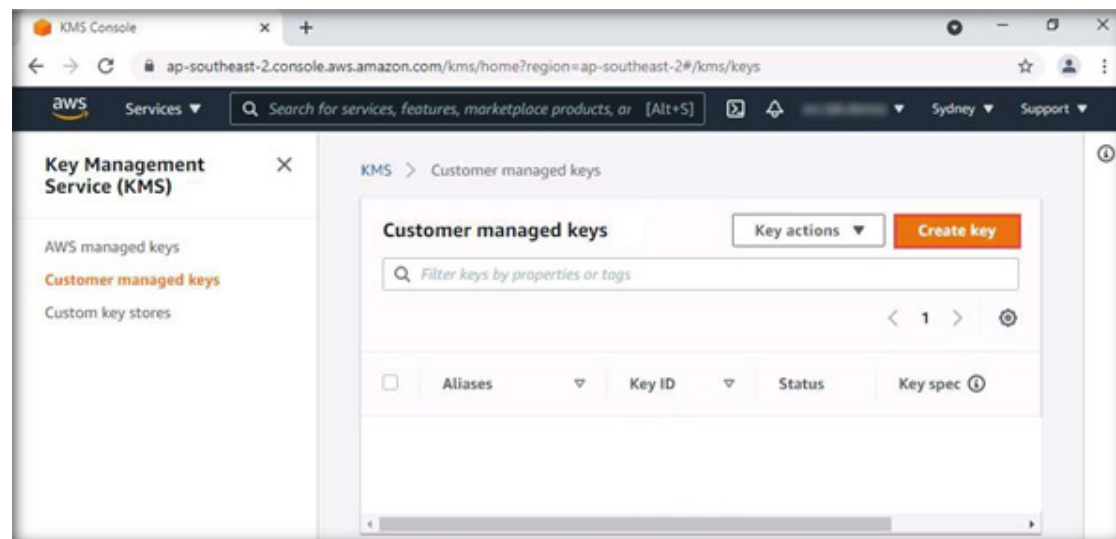
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

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



EXERCISE 4:
IMPLEMENT KEY
MANAGEMENT
SERVICES IN
AWS

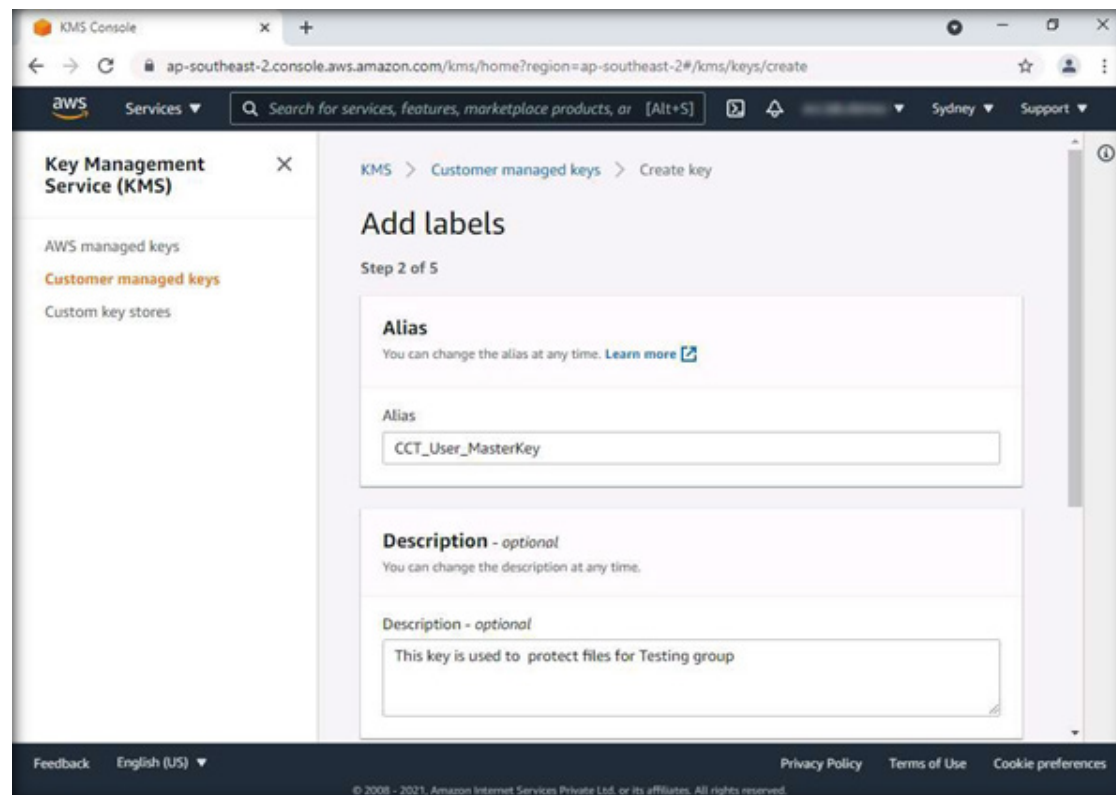
8. The Customer managed keys section appears. Click on Create key.



EXERCISE 4:
IMPLEMENT KEY
MANAGEMENT
SERVICES IN
AWS

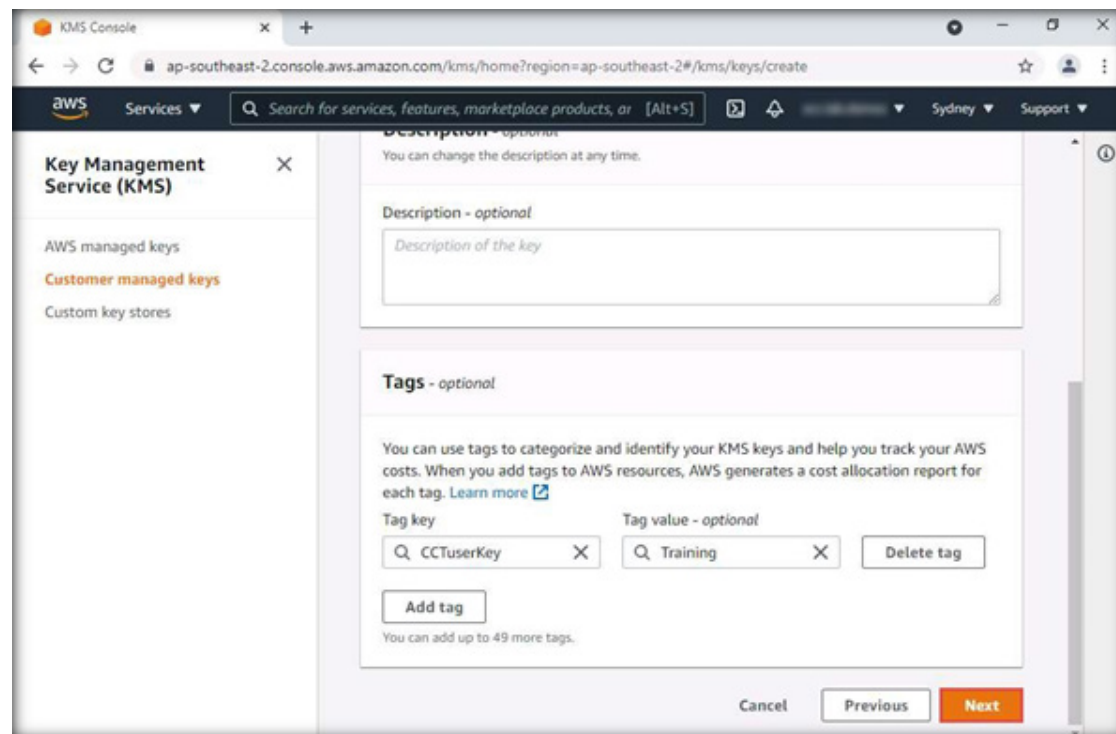
9. By default, the Symmetric key is selected. Click on Next to continue.

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.



The screenshot shows the AWS KMS Console interface for creating a new key. The browser address bar indicates the URL: `ap-southeast-2.console.aws.amazon.com/kms/home?region=ap-southeast-2#/kms/keys/create`. The left sidebar shows the navigation menu with 'Key Management Service (KMS)' selected. The main content area is titled 'Add labels' and is 'Step 2 of 5'. It contains two sections: 'Alias' and 'Description - optional'. The 'Alias' section has a text input field containing 'CCT_User_MasterKey'. The 'Description - optional' section has a text area containing 'This key is used to protect files for Testing group'. The bottom of the page includes a footer with 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



The screenshot shows the AWS KMS Console 'Create Key' page. The left sidebar contains the 'Key Management Service (KMS)' menu with options for 'AWS managed keys', 'Customer managed keys' (highlighted), and 'Custom key stores'. The main content area is titled 'Create Key' and includes a 'Description - optional' section with a text input field containing 'Description of the key'. Below this is a 'Tags - optional' section with a description of tags and a table for adding tags. The table has columns for 'Tag key' and 'Tag value - optional'. One tag is added with the key 'CCTUserKey' and the value 'Training'. There is a 'Delete tag' button next to the tag. At the bottom of the tag section is an 'Add tag' button. The bottom of the page has 'Cancel', 'Previous', and 'Next' buttons.

Key Management Service (KMS)

- AWS managed keys
- Customer managed keys**
- Custom key stores

Create Key

Description - optional
You can change the description at any time.

Description - optional
Description of the key

Tags - optional
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. [Learn more](#)

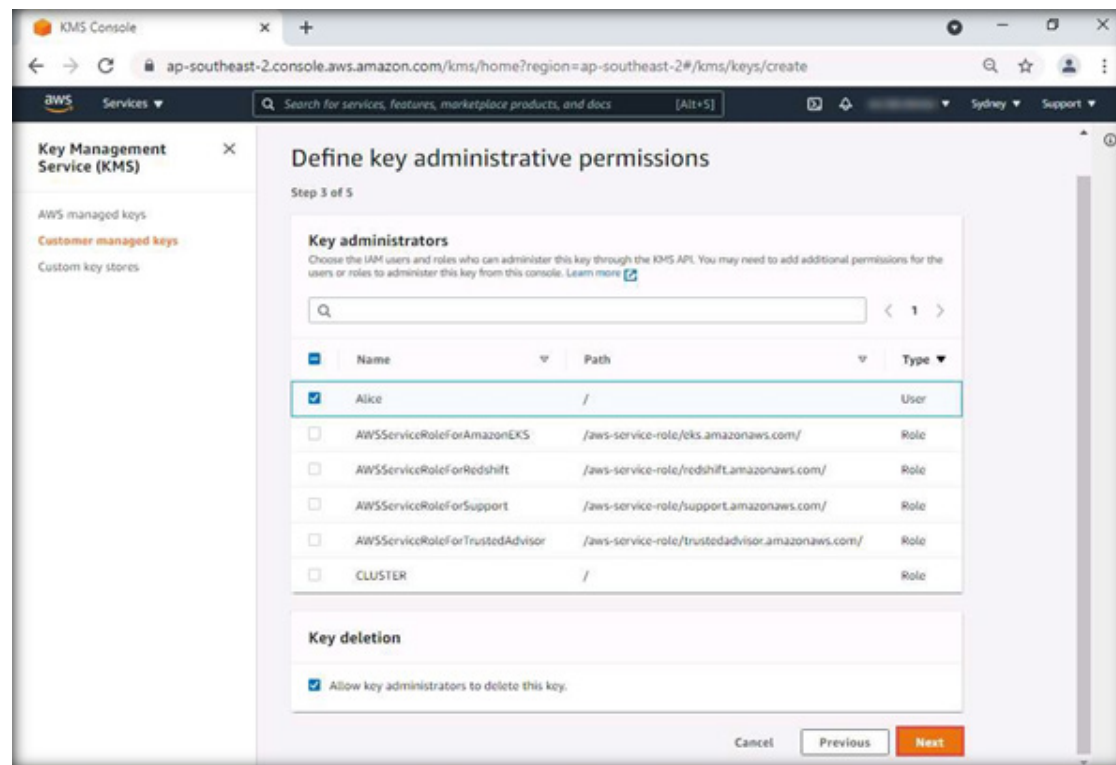
Tag key	Tag value - optional	
CCTUserKey	Training	Delete tag

Add tag

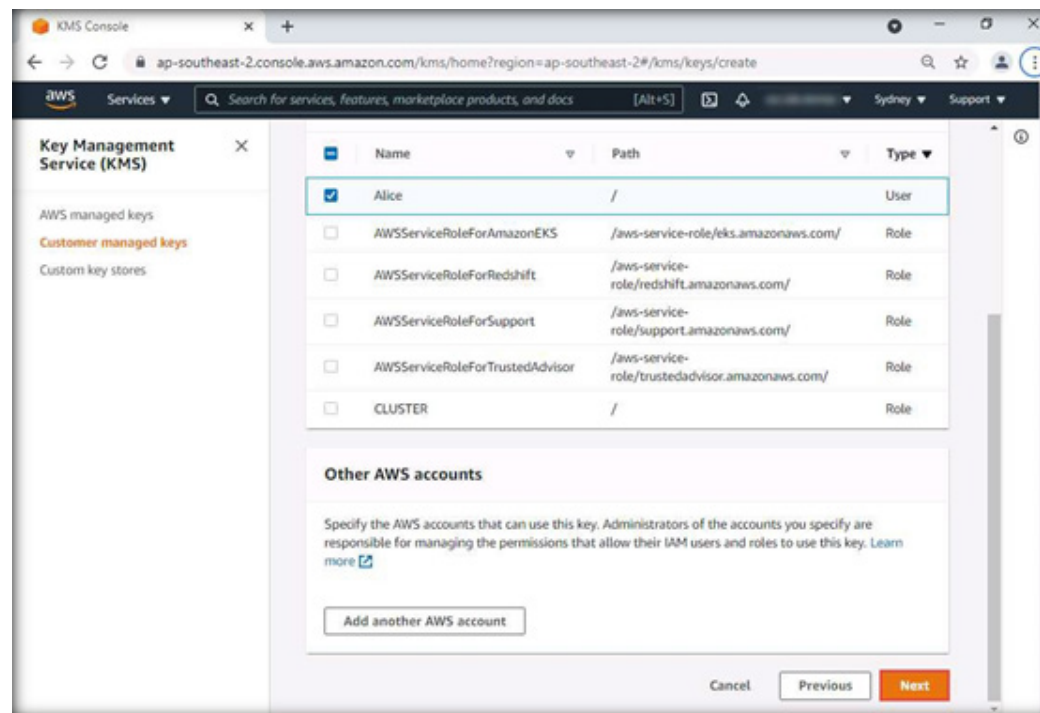
You can add up to 49 more tags.

Cancel Previous Next

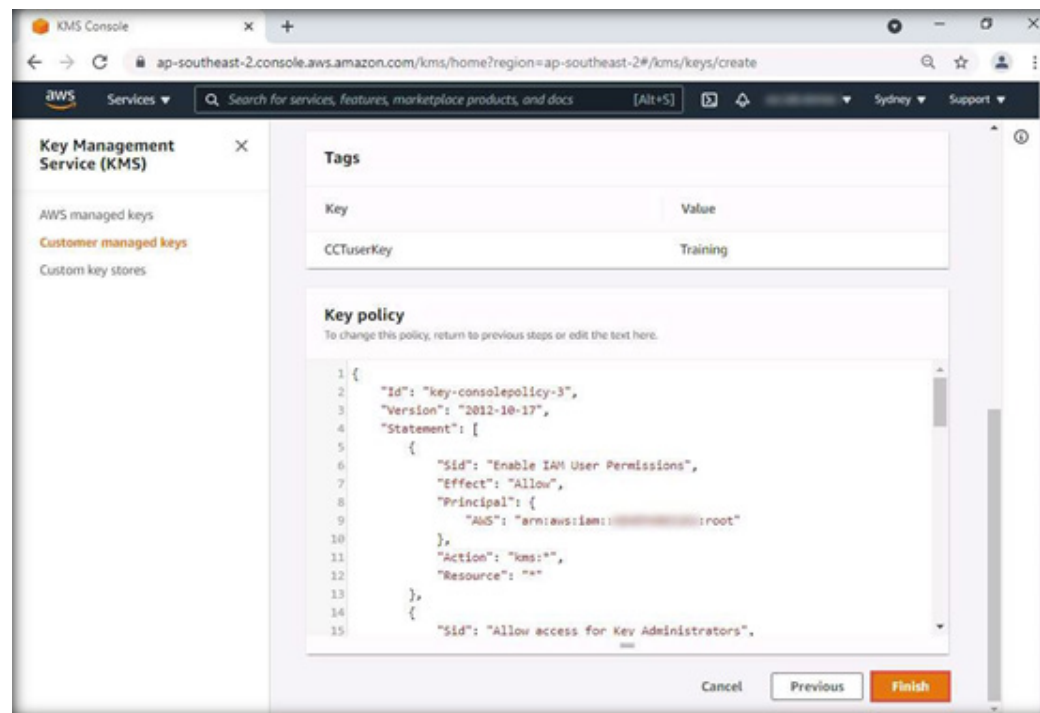
11. To allow users to perform encryption and decryption, we must assign key permissions for the users. In this example, we will permit Alice to use the Master Key and click Next.



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.

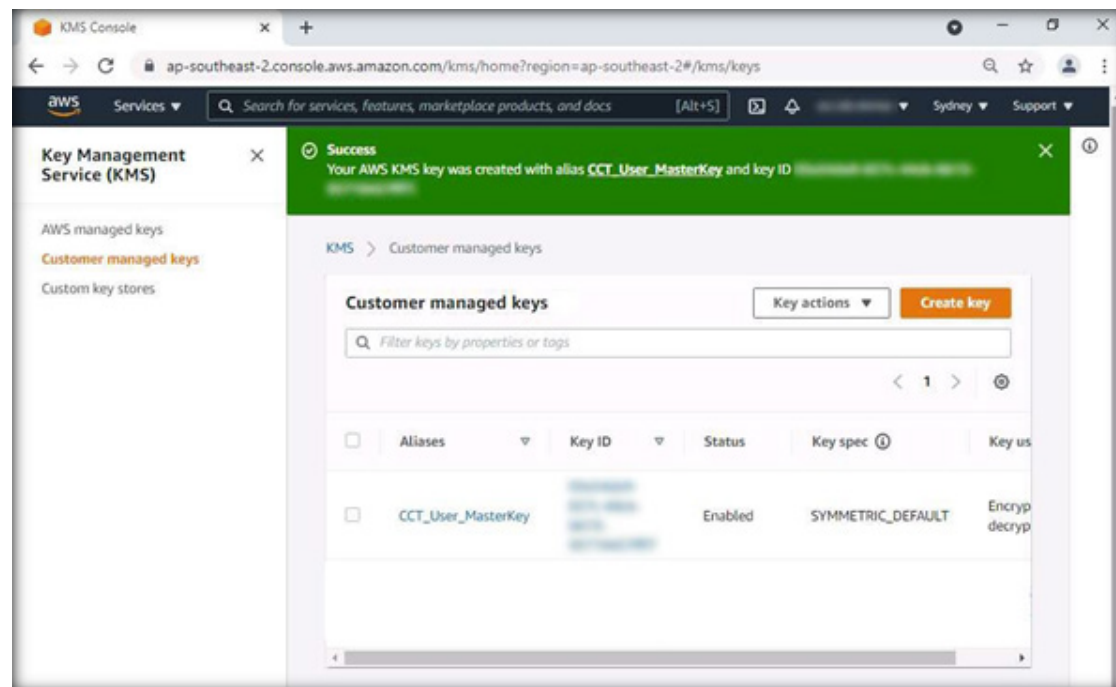


13. You can Review and edit key policy, which is in JSON format. Click on Finish to create the Master Key.

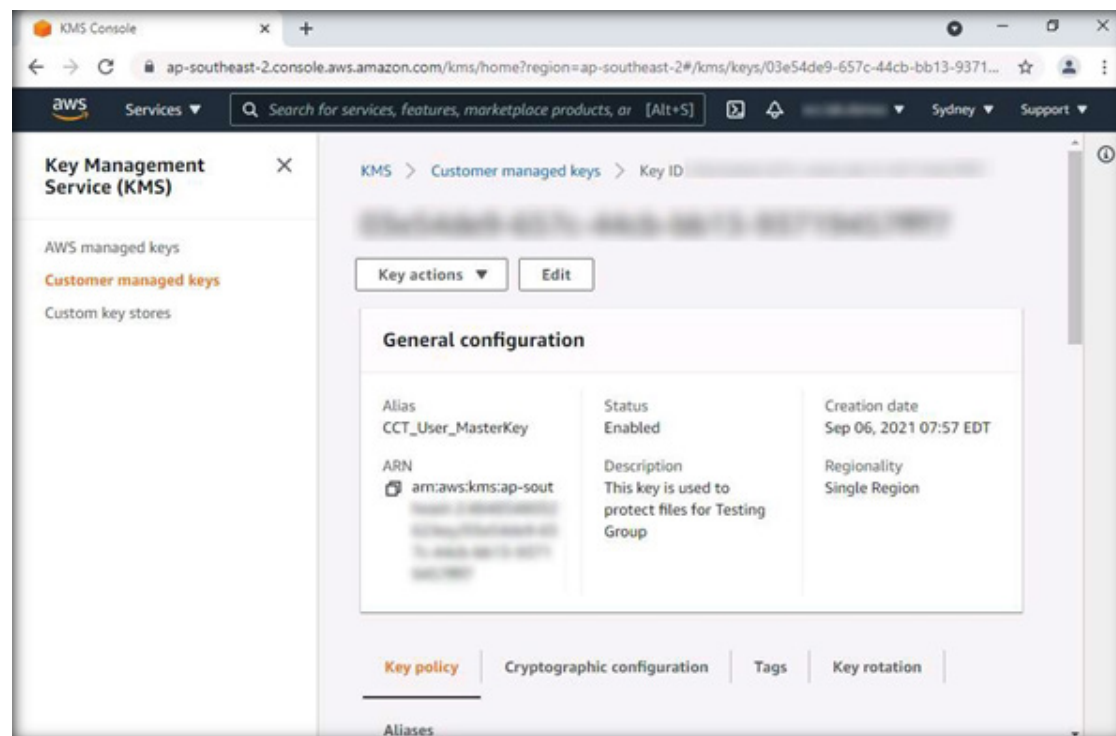


EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS

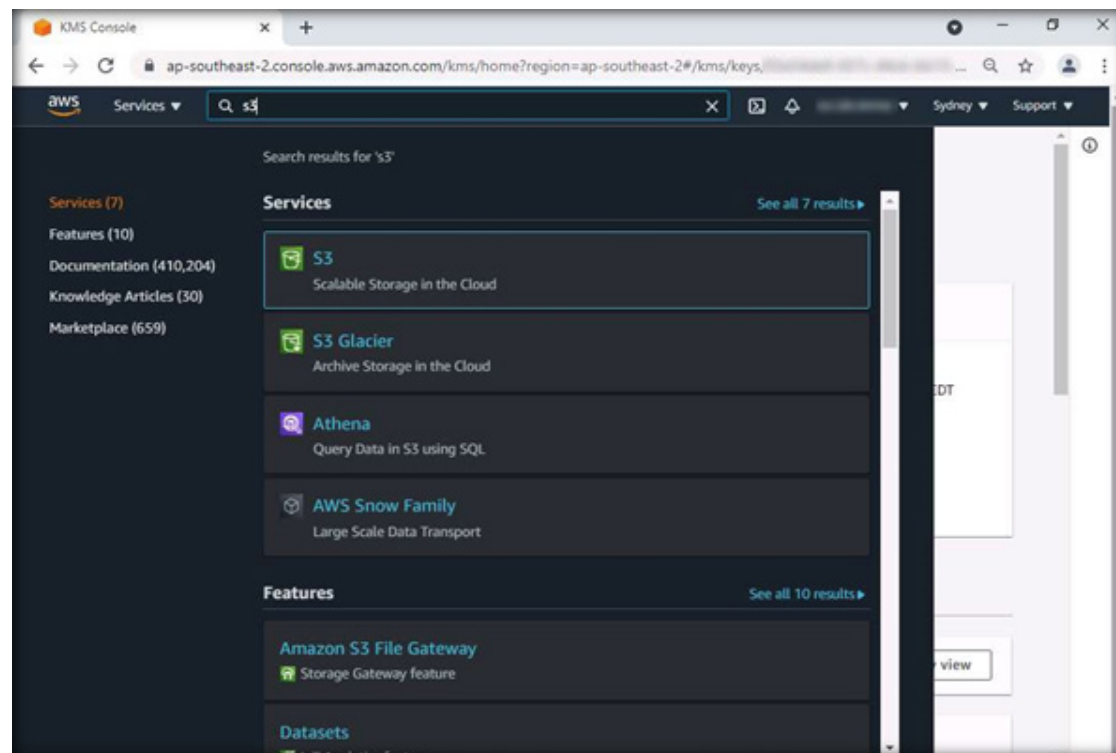
14. The key has been created successfully, and it now appears in the Customer managed keys section.



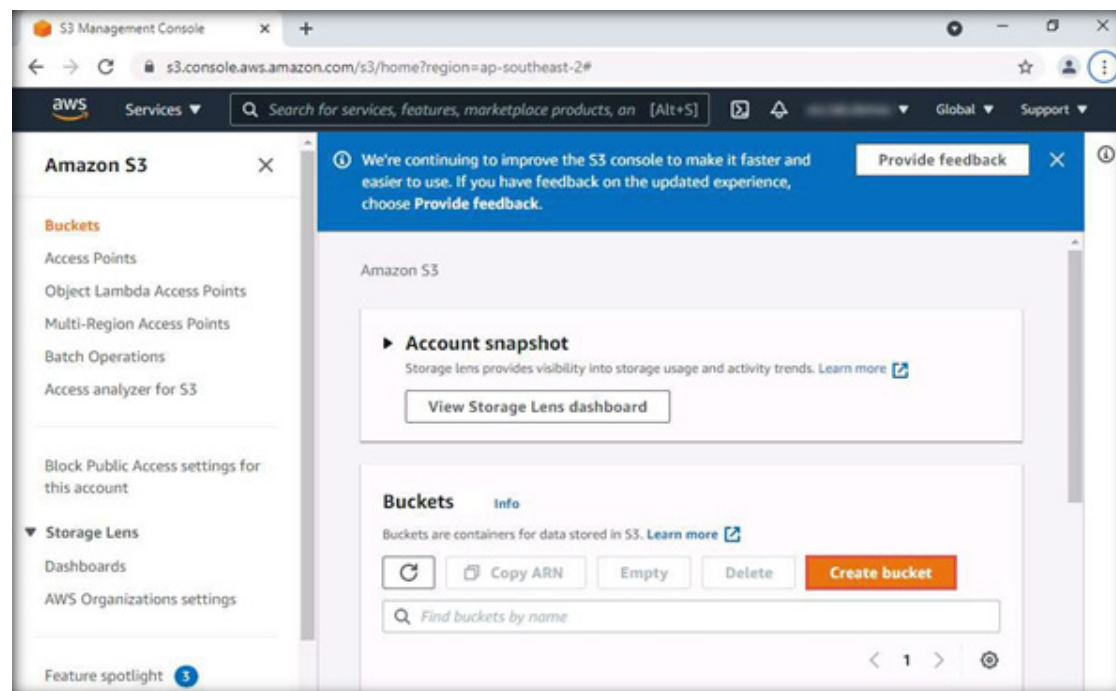
15. After creating the key, you can go to Customer managed keys and click on the key (here, it is CCT_User_Masterkey) in the Alias column to view the Master Key properties.



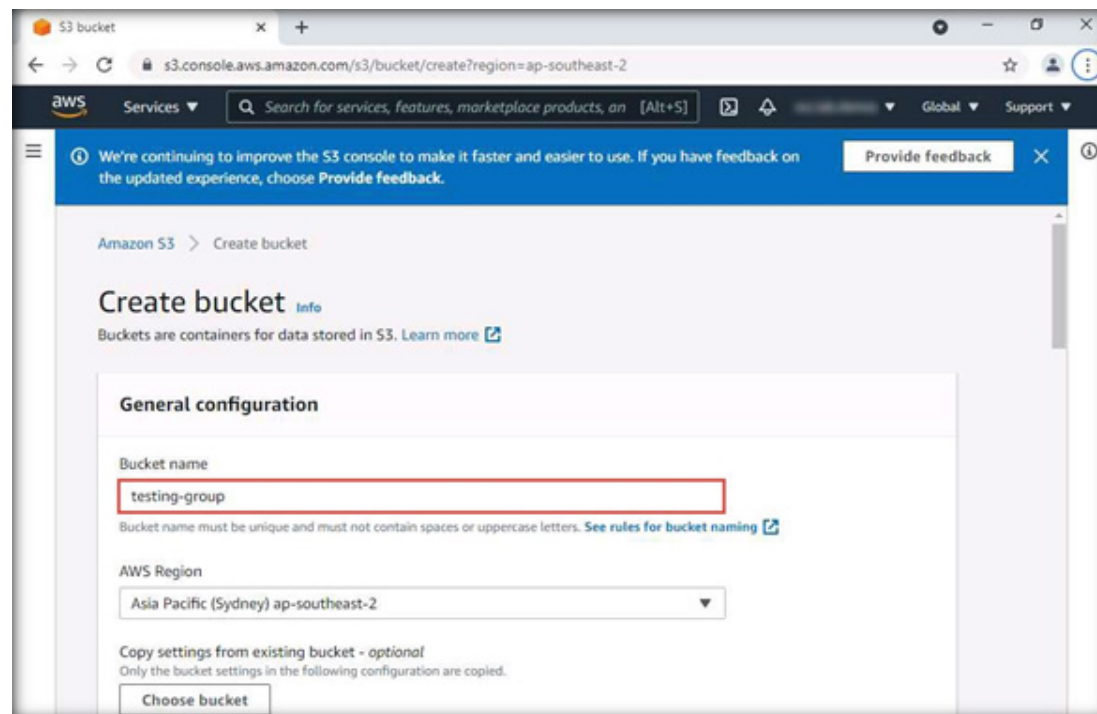
16. In the AWS Management Console, click on Services from the menu bar and enter S3 in the search field. Click on S3 Scalable Storage in the Cloud from the search results.



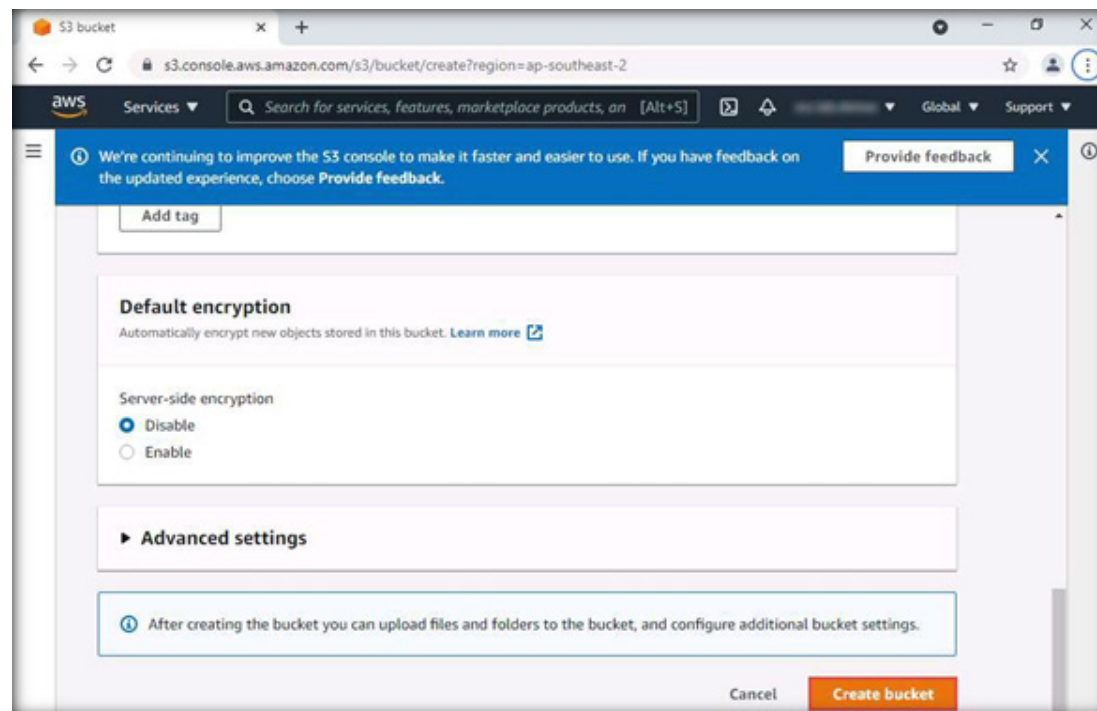
17. The S3 buckets page appears. Click on Create bucket.



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.

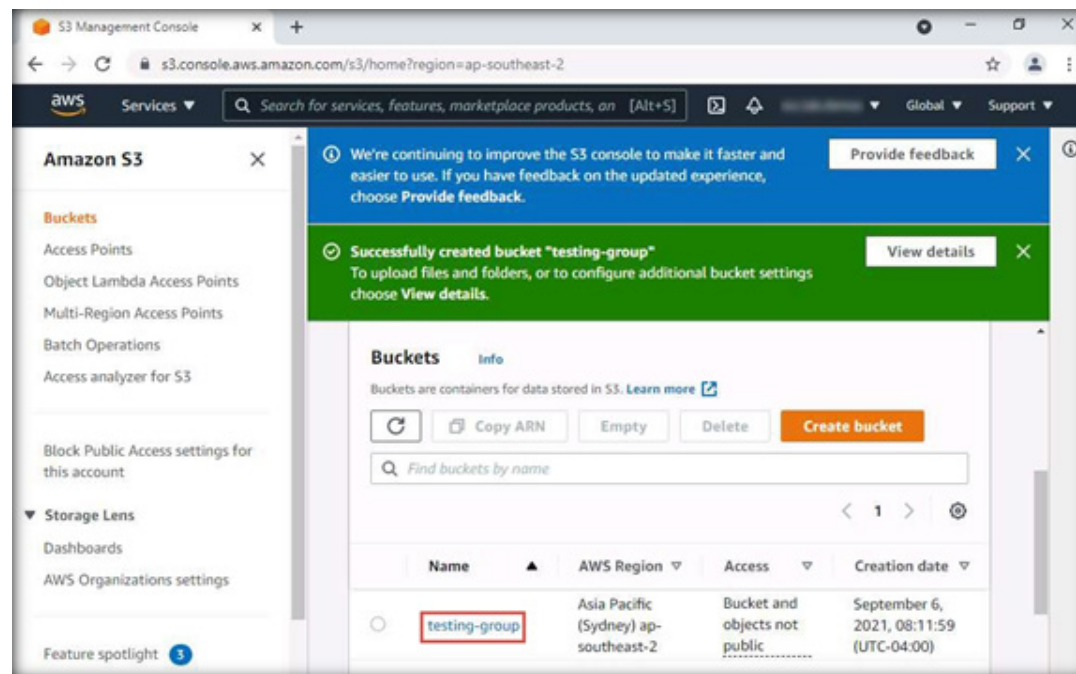


19. Retain default settings for all other sections, scroll down and click on Create bucket.

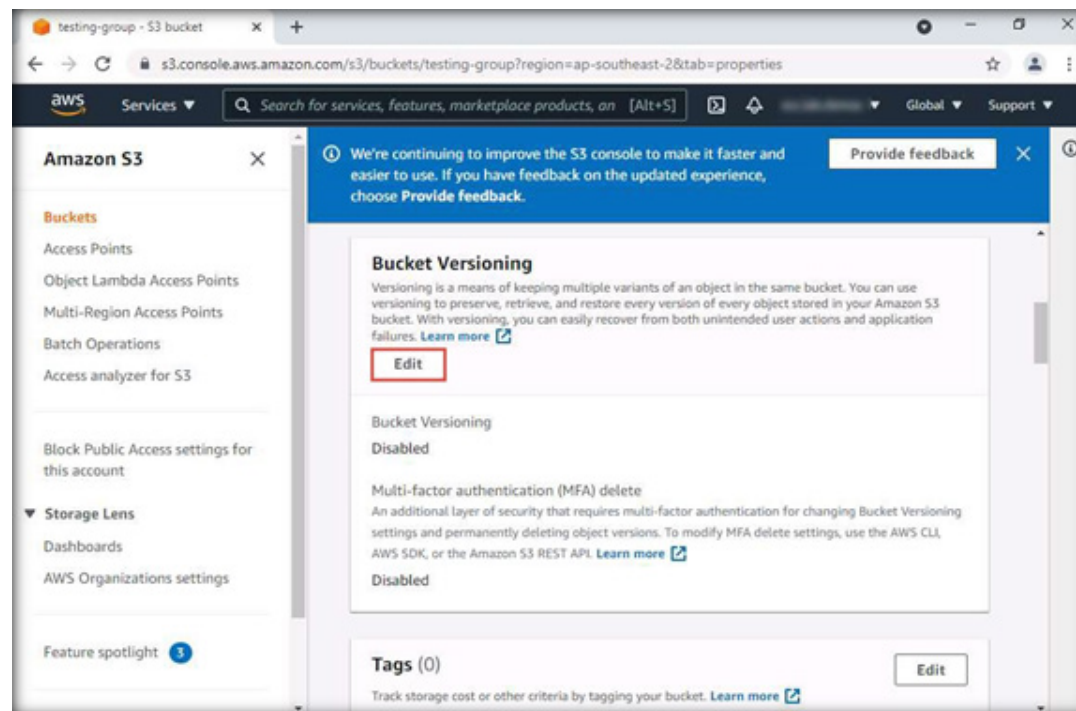


20. The S3 buckets page appears.

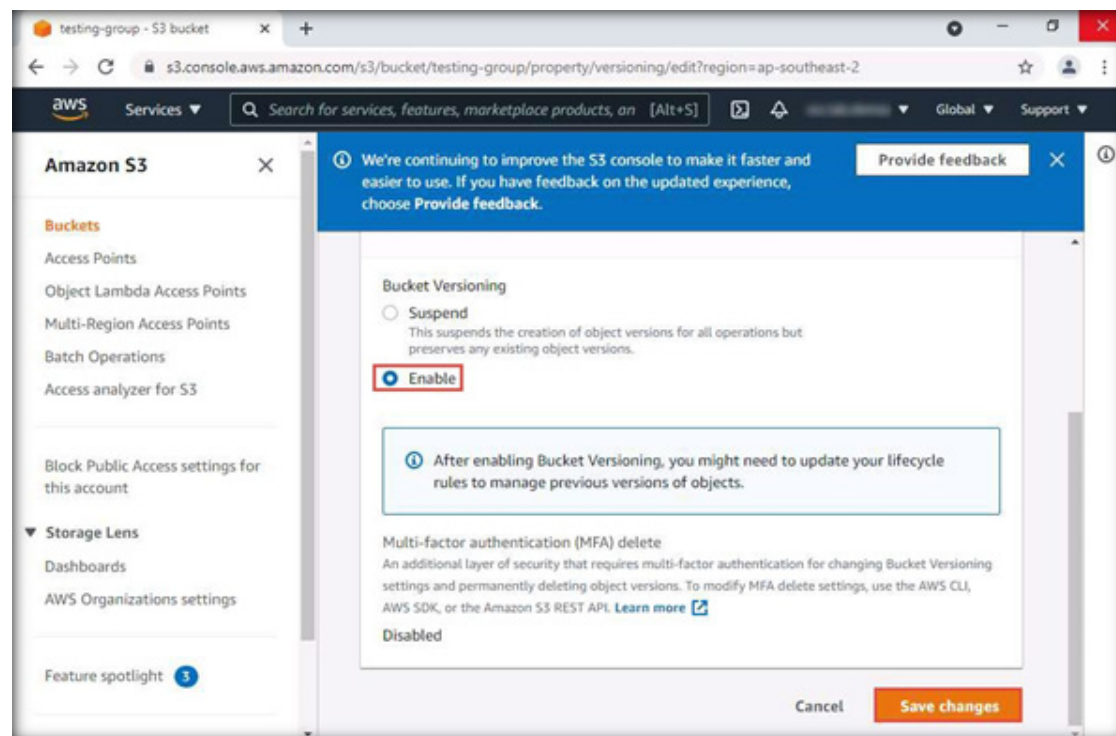
21. Click on the bucket for which you want to configure the encryption settings (here, click on testing-group).



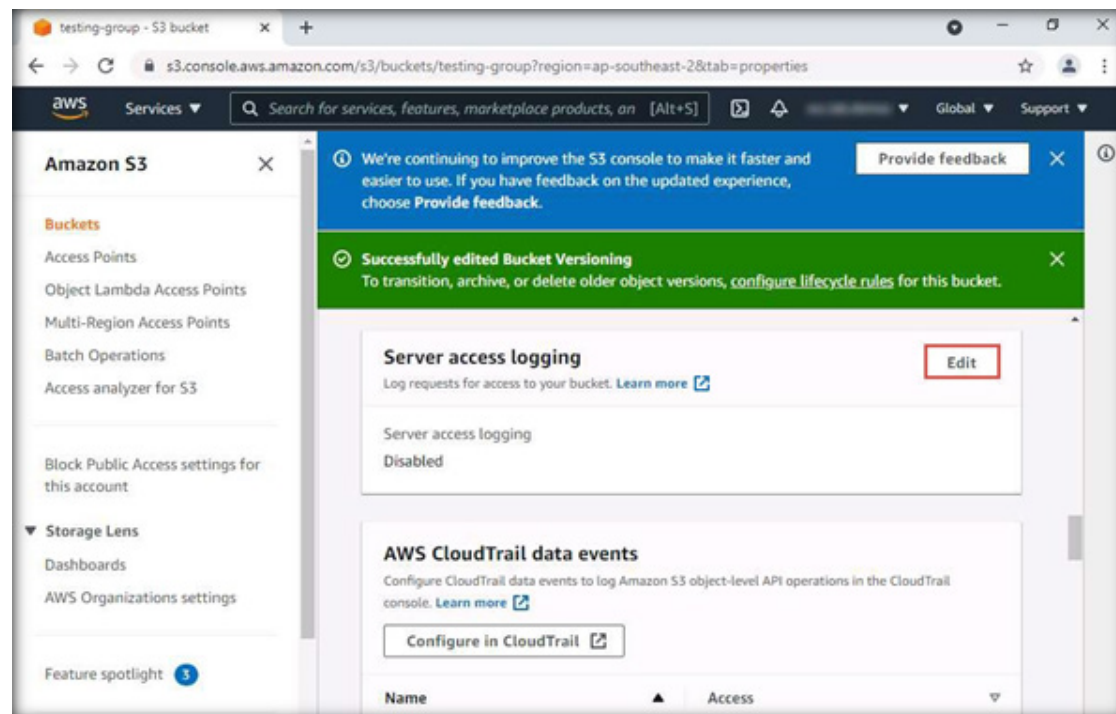
22. The testing-group bucket page appears. Click on Properties, and then click on the Edit button under the Bucket Versioning section.



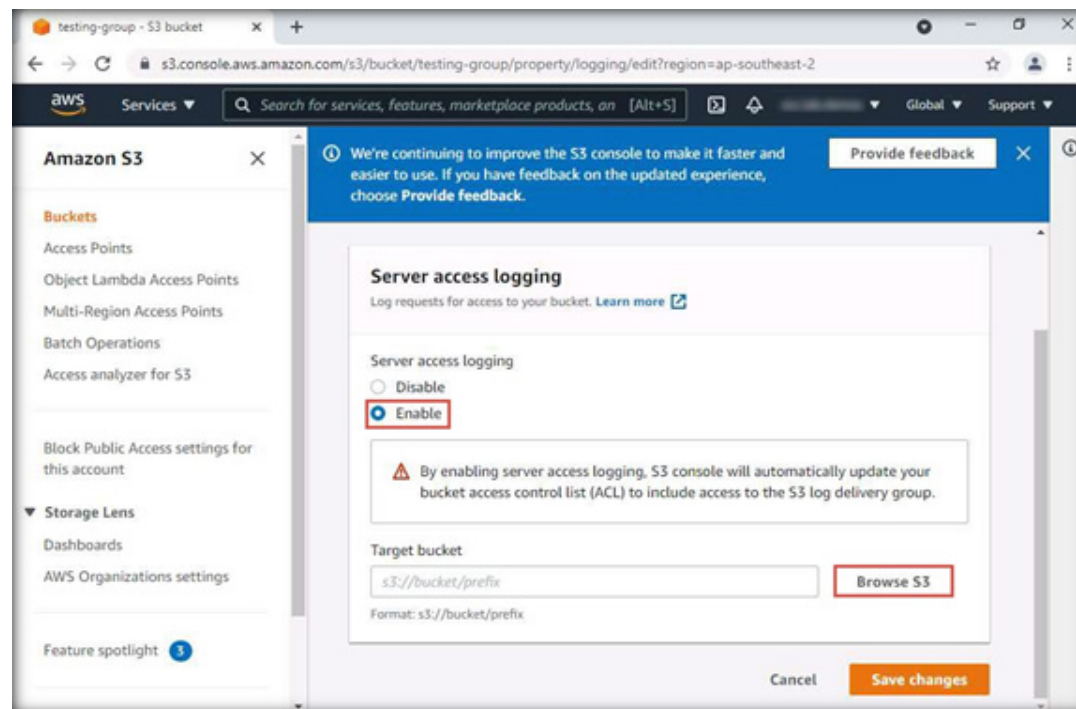
23. Click on the Enable radio button under Bucket Versioning to enable it, and then scroll down and select Save changes.



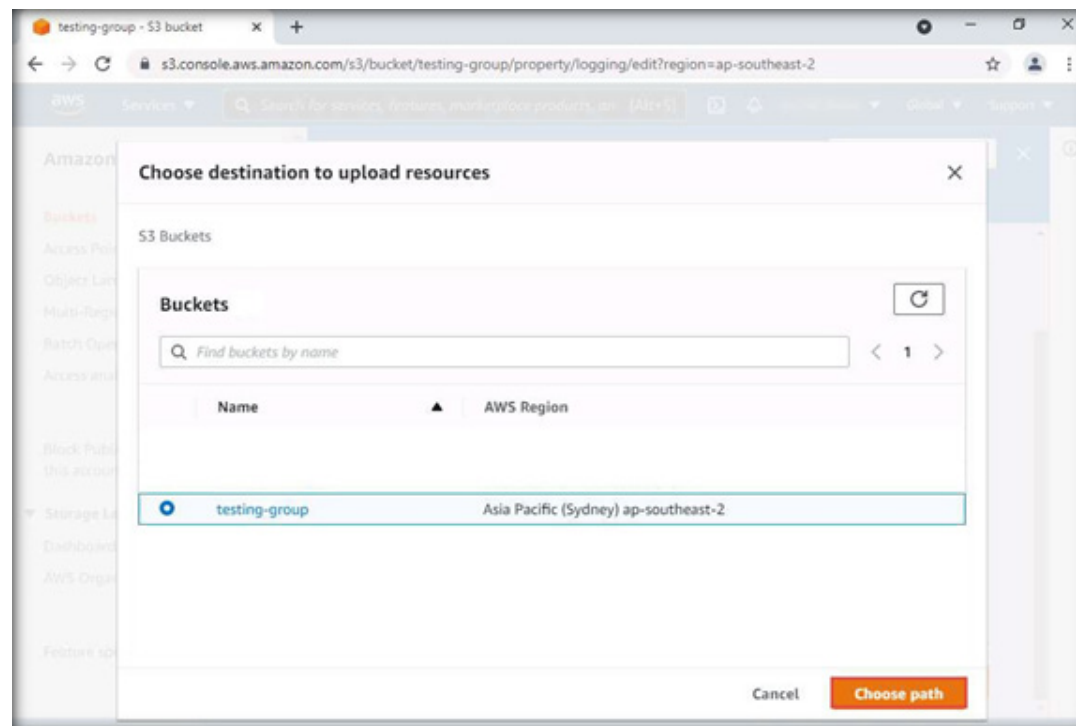
24. In the testing-group bucket page scroll down to Server access logging and click on Edit.



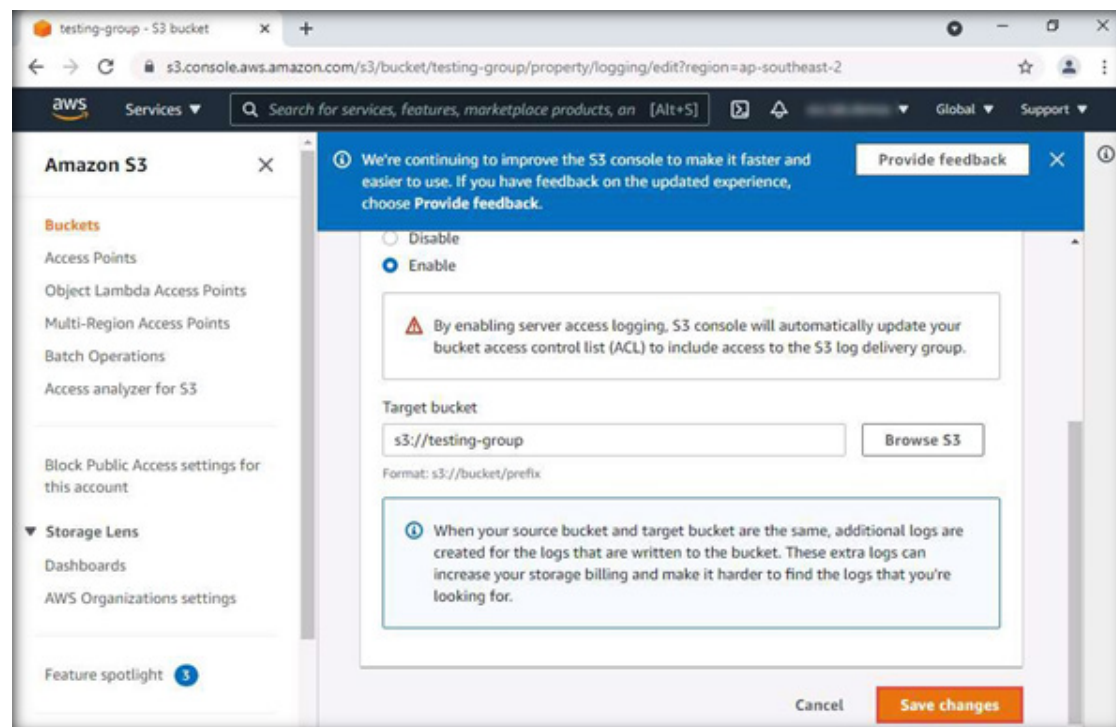
25. Click on the Enable radio button under Server access logging Similarly and click on Browse S3 to select the target bucket.



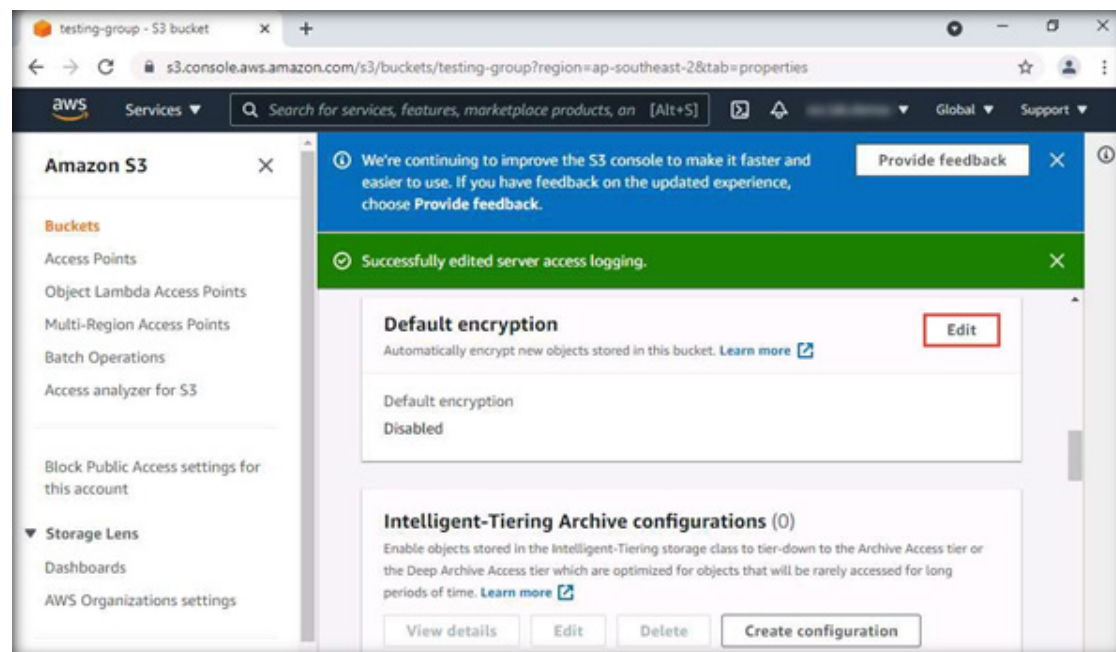
26. In the Choose destination to upload resources window select testing-group s3 bucket and click on Choose path.



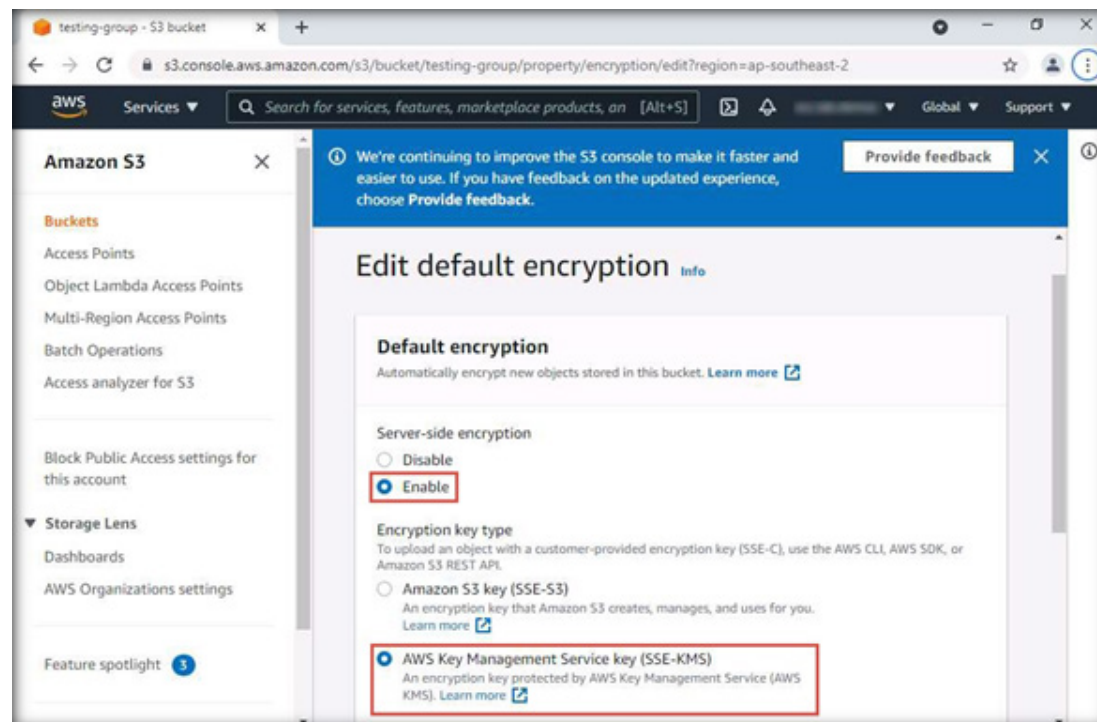
27. The testing-group appears in Target bucket, scroll down and click on Save changes.



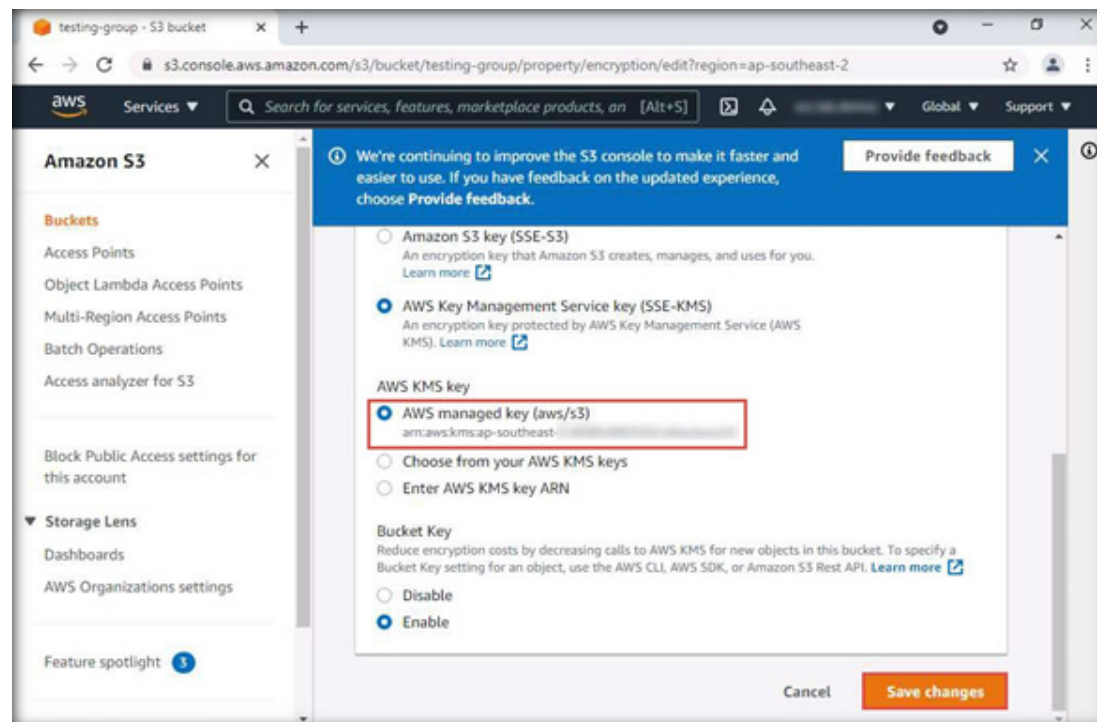
28. Next, in the testing-group bucket page, scroll down and click on Edit button under Default encryption.



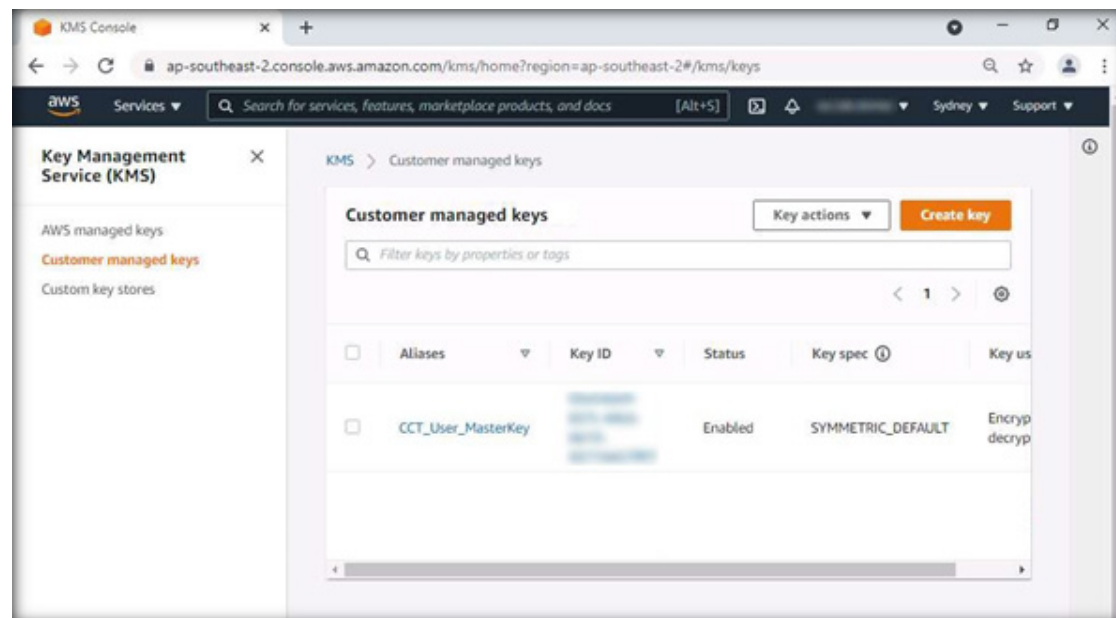
29. In the Edit default encryption window select Enable radio button and choose the AWS Key Management Service key (SSE-KMS) radio button from the list of encryption key types, and select AWS managed key aws/s3 under AWS KMS key section, which will use the default AWS Managed Keys. Click on Save changes.



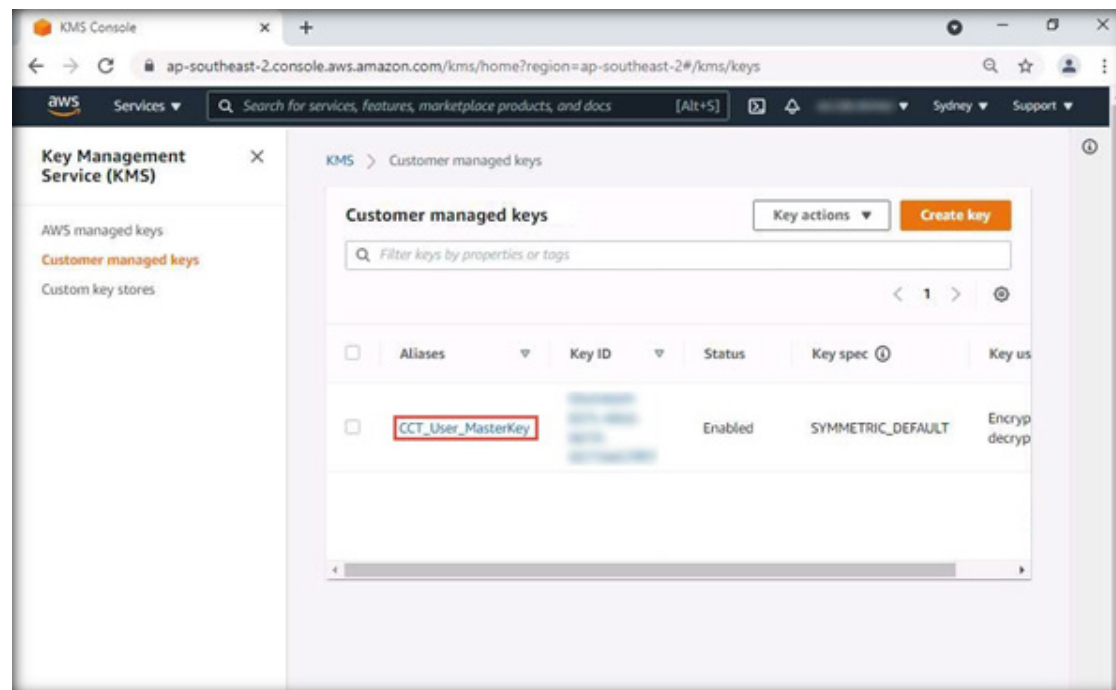
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



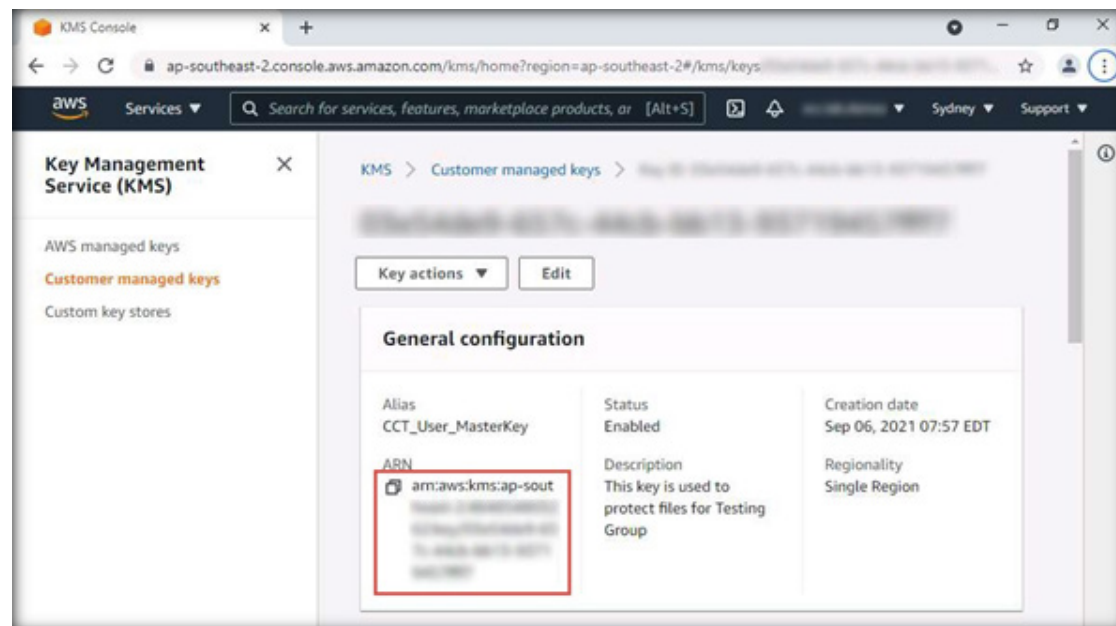
30. We have created the testing-group bucket for encrypting data. The user can push data into this bucket.
31. The user can also use a customer managed key for this bucket. Let us see how to use the customer managed key for the testing-group bucket to encrypt the data.
32. Go to Key Management Services (KMS), and select Customer managed keys.



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

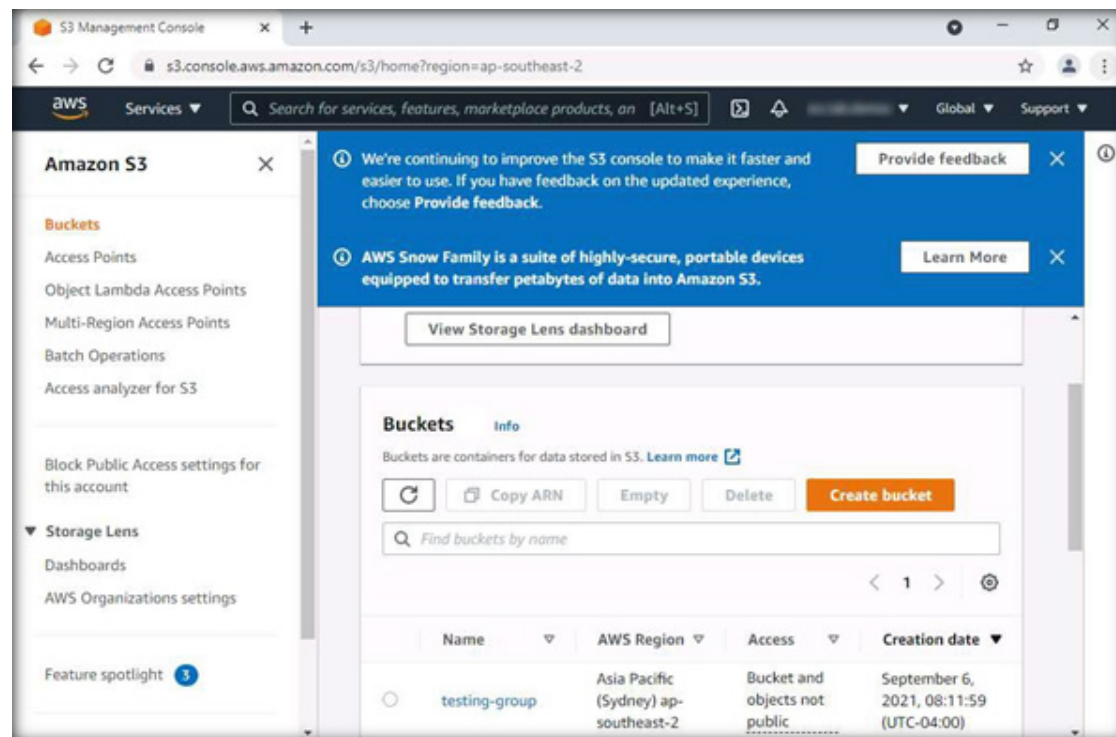


34. Under the CCT_user_MasterKey's General configuration, select the Amazon Resource Names (ARN) key which uniquely identify AWS resources key under the ARN field and copy it.

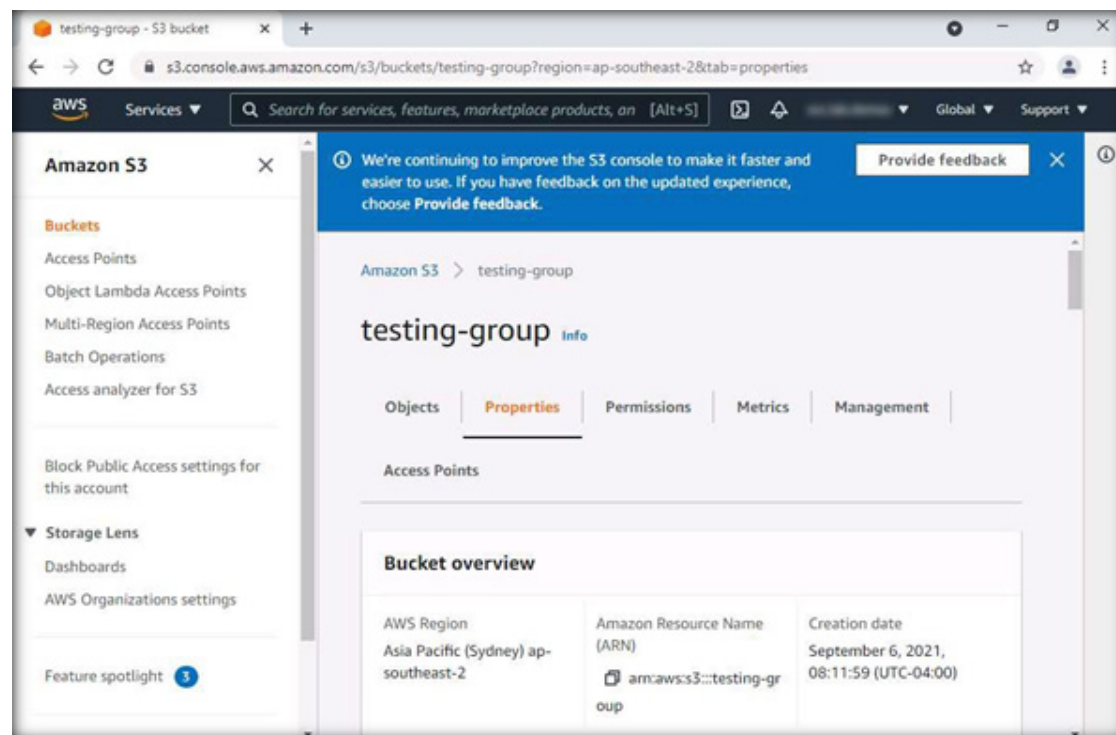


35. Open Notepad and paste the copied link.

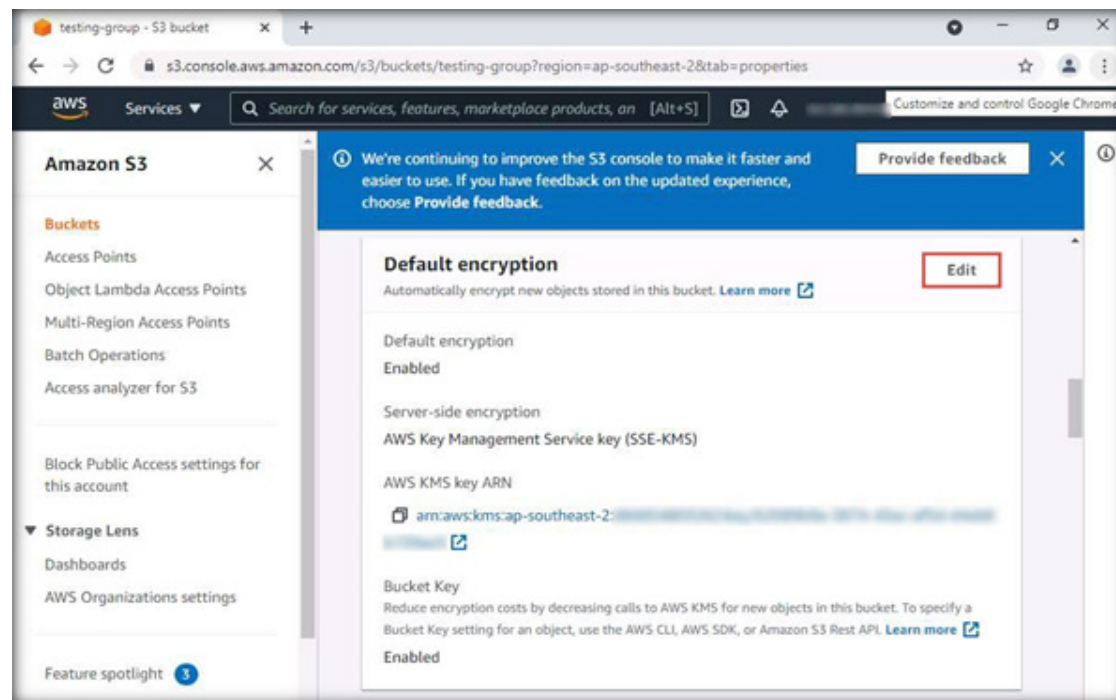
36. Switch to the browser. Navigate to S3 Management Console and select testing-group under Bucket name.



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

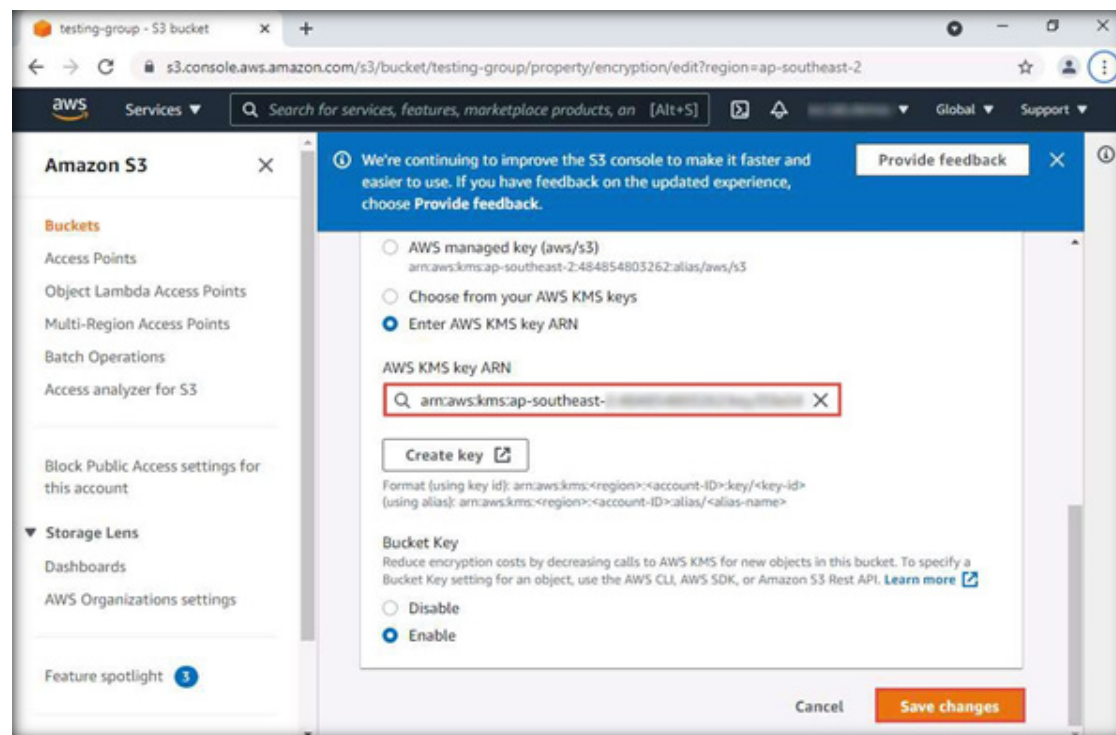


38. Scroll down and click on Edit button under Default encryption.

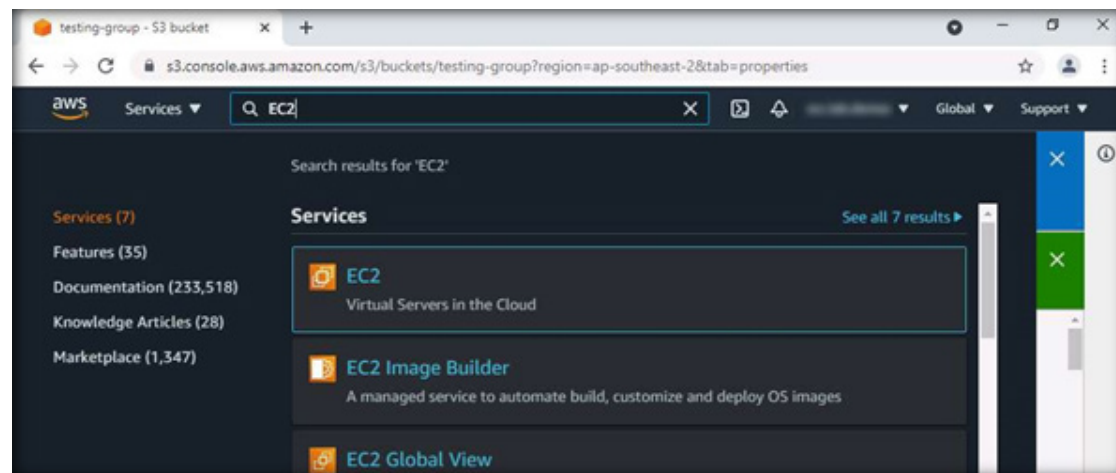


39. Switch to Notepad and copy the key that we had pasted in Step 35.

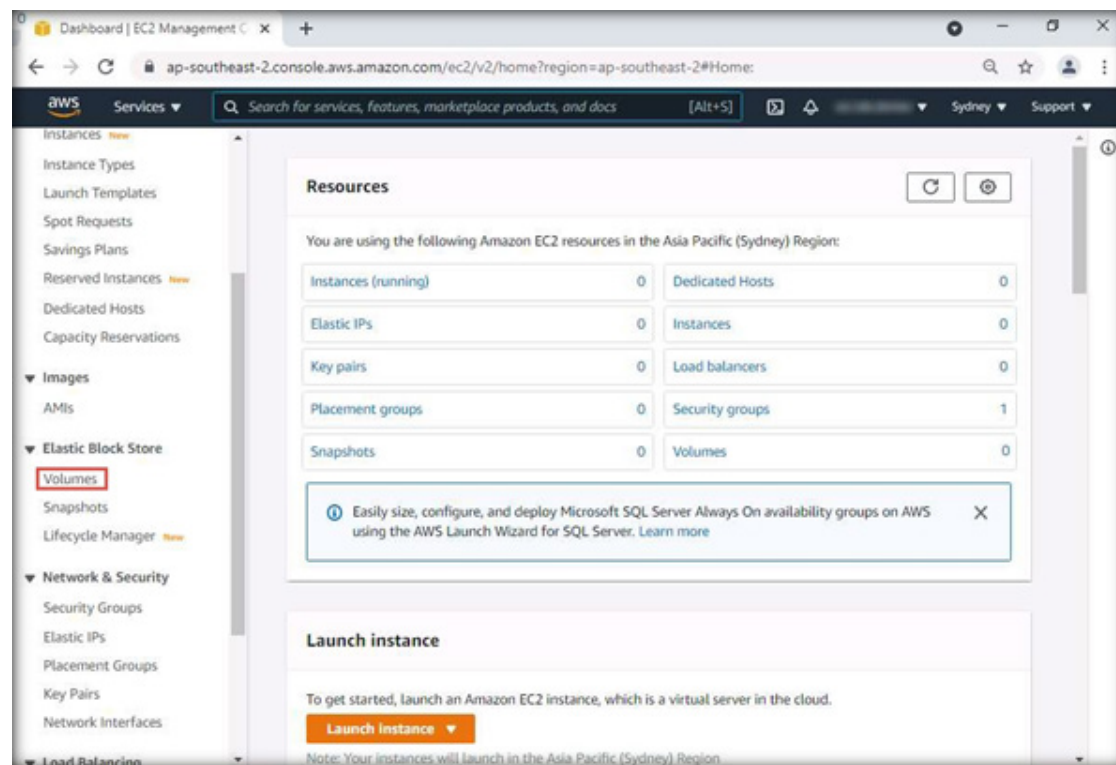
40. Again, switch back to the Default Encryption and select the Enter AWS KMS key ARN radio button and paste the key that was copied in Step 35 in the AWS KMS key ARN. Click on Save changes.



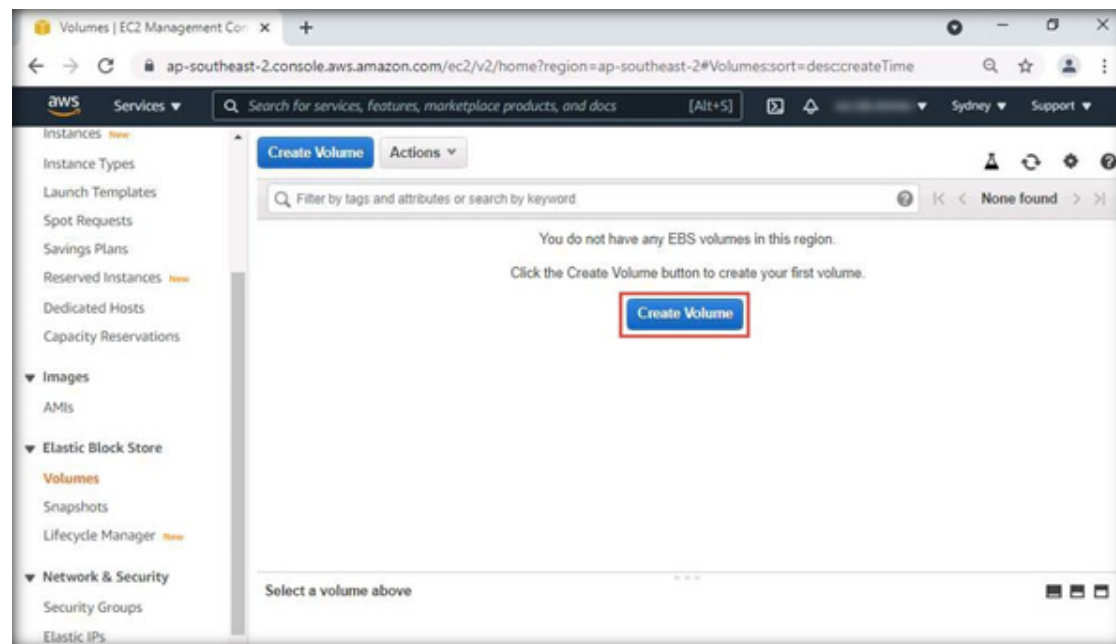
41. In this way, with the help of Customer Managed Keys, the user can encrypt and protect storage data.
42. Amazon EBS supports KMS. Its encryption provides security to data at rest by encrypting data volumes, boot volumes, and snapshots using Amazon-managed keys or keys created and managed using the 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.



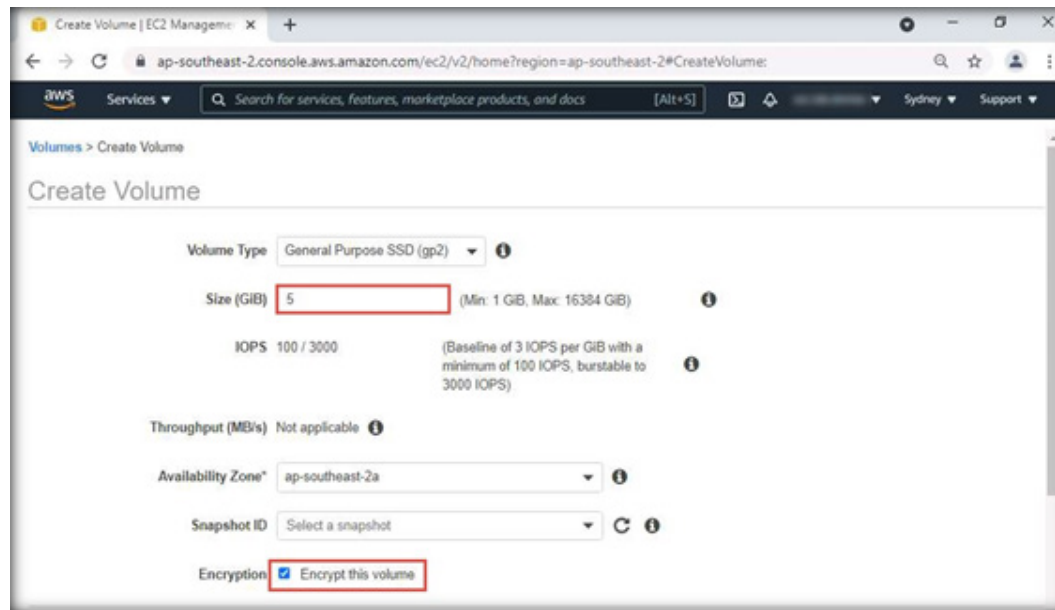
44. Once the EC2 Service Console page opens, click on Volumes in the left pane under Elastic Block Store.



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



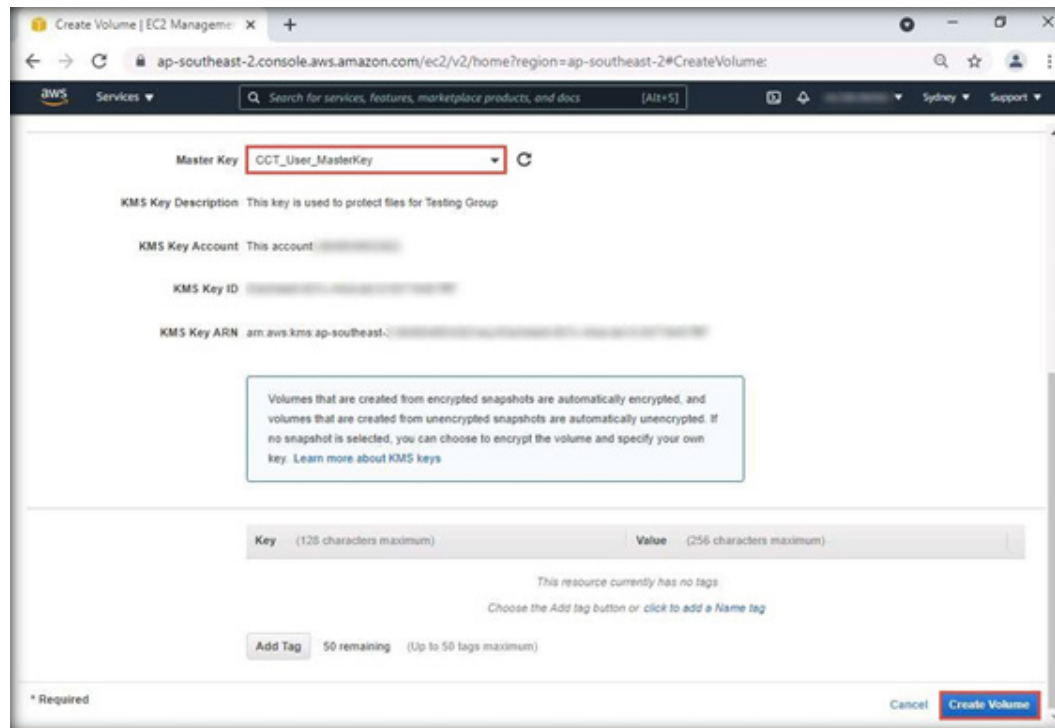
46. In the Create Volume page, select the Volume Type and specify the size of the volume in the Size (GiB) field. If you need the disk to restore existing data, you can select a Snapshot ID, in which you have saved another volume's Snapshot. Check Encryption: Encrypt this volume.



The screenshot displays the AWS Management Console 'Create Volume' page. The browser address bar shows the URL: `ap-southeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-2#CreateVolume:`. The page title is 'Create Volume'. The form includes the following fields and options:

- Volume Type:** General Purpose SSD (gp2) (with an information icon)
- Size (GiB):** 5 (with a red border around the input field and a range of (Min: 1 GiB, Max: 16384 GiB) and an information icon)
- IOPS:** 100 / 3000 (with a note: (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) and an information icon)
- Throughput (MB/s):** Not applicable (with an information icon)
- Availability Zone:** ap-southeast-2a (with an information icon)
- Snapshot ID:** Select a snapshot (with a refresh icon and an information icon)
- Encryption:** ☒ Encrypt this volume (with a red border around the checkbox)

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.



Create Volume | EC2 Management Console

ap-southeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-2#CreateVolume:

Master Key: CCT_User_MasterKey

KMS Key Description: This key is used to protect files for Testing Group

KMS Key Account: This account

KMS Key ID:

KMS Key ARN: arn:aws:kms:ap-southeast-2:::key/

Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume and specify your own key. [Learn more about KMS keys](#)

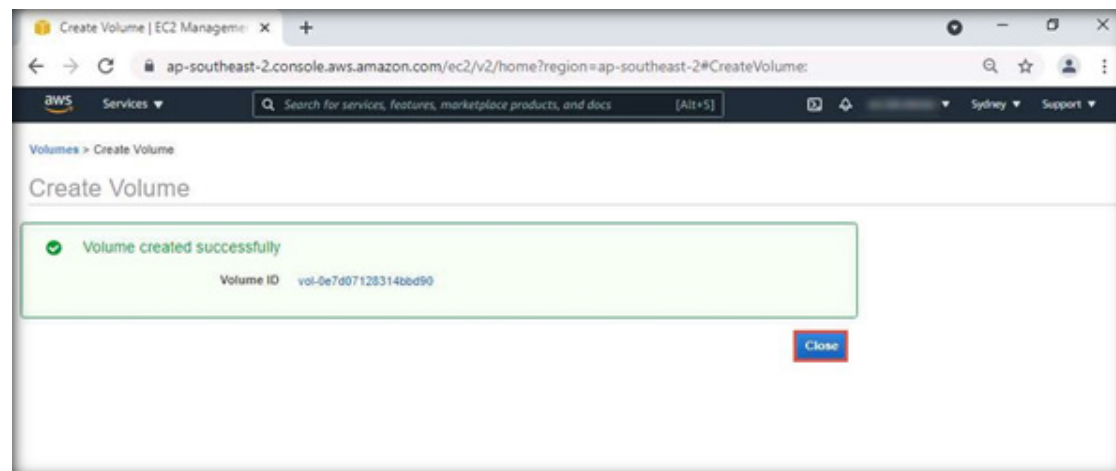
Key (128 characters maximum) Value (256 characters maximum)

This resource currently has no tags. Choose the Add tag button or click to add a Name tag.

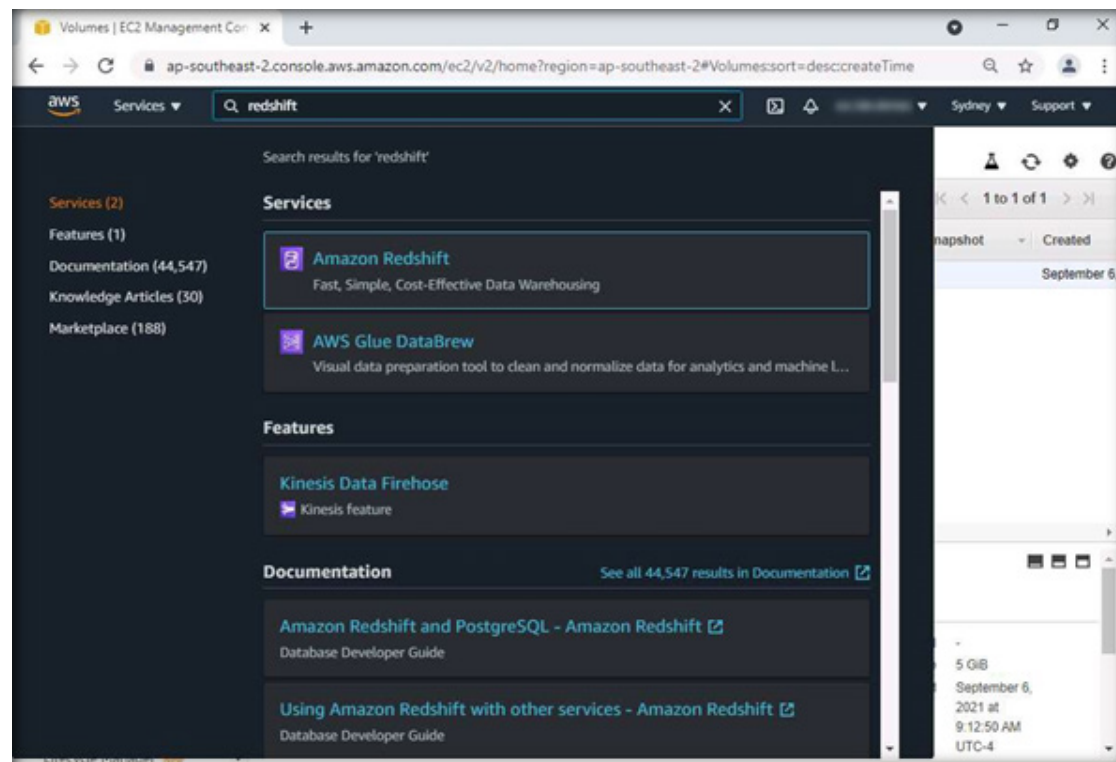
Add Tag 50 remaining (Up to 50 tags maximum)

* Required Cancel Create Volume

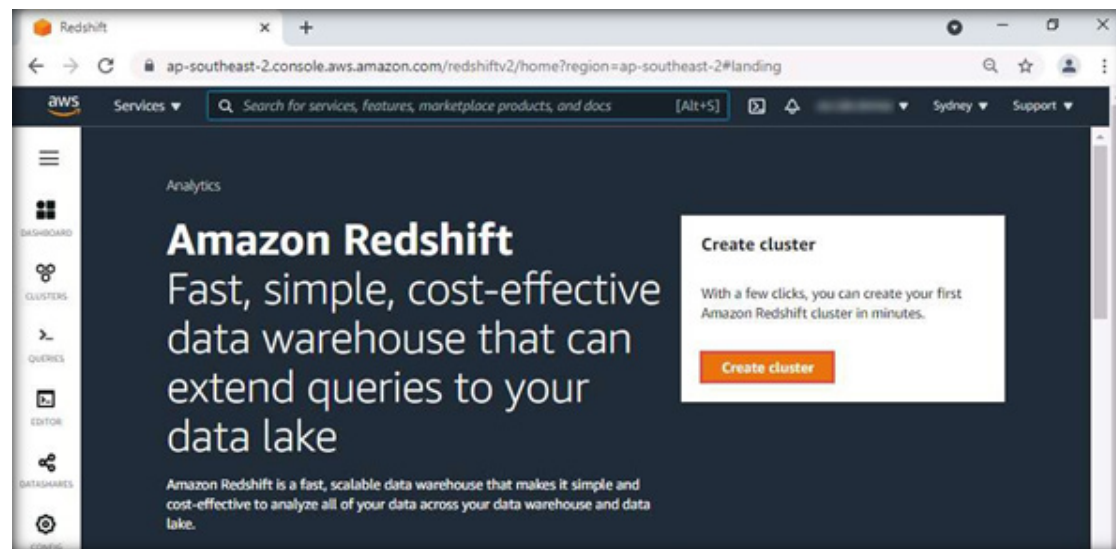
48. The Volume created successfully dialog message will appear once the disk is created. Click on Close.



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.

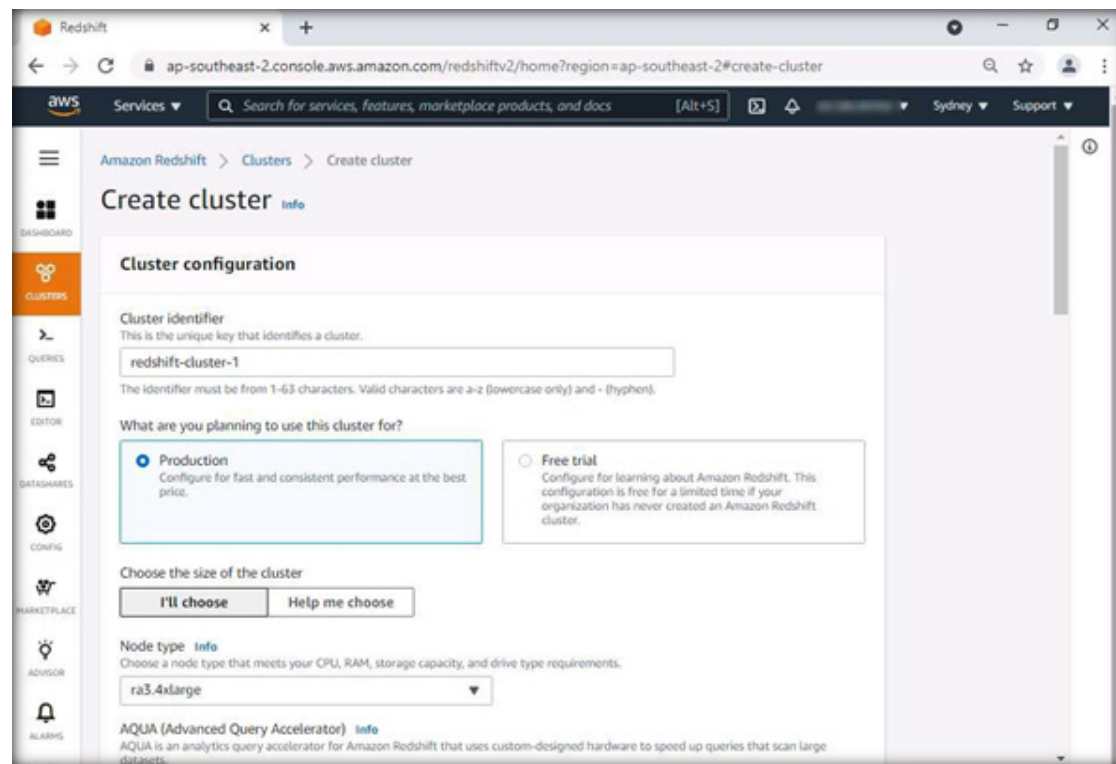


52. Close the welcome popup that appears. Click on Create cluster in the Redshift dashboard.

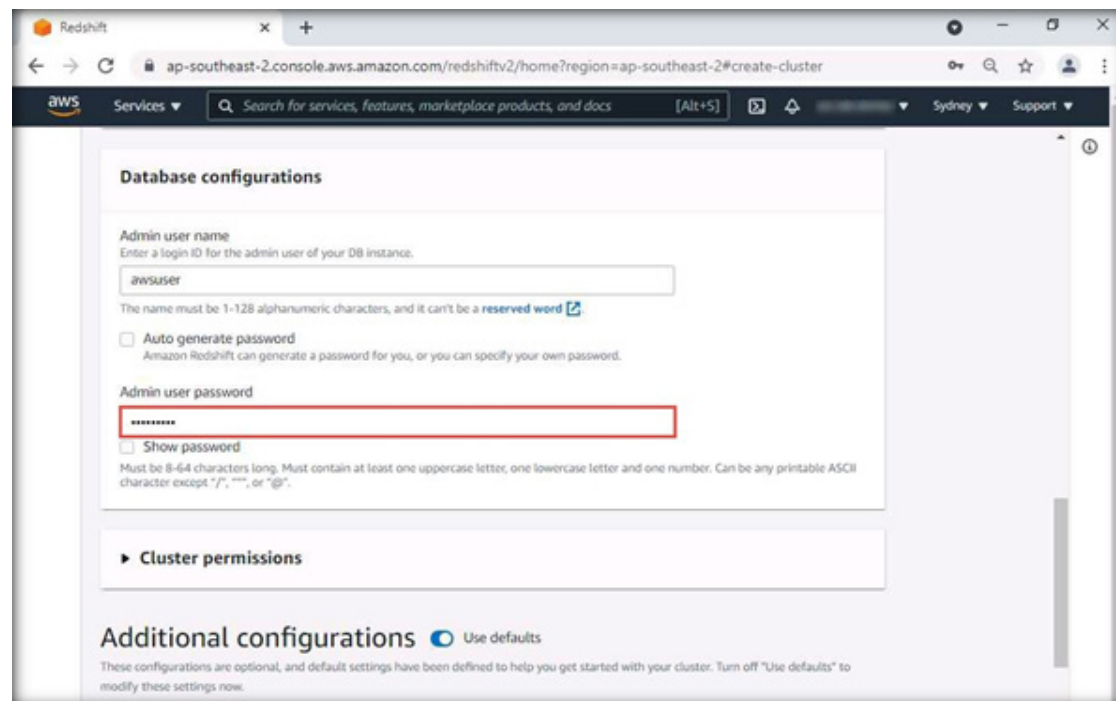


EXERCISE 4:
IMPLEMENT KEY
MANAGEMENT
SERVICES IN
AWS

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.



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



Redshift

ap-southeast-2.console.aws.amazon.com/redshiftv2/home?region=ap-southeast-2#create-cluster

Services Search for services, features, marketplace products, and docs [Alt+S] Sydney Support

Database configurations

Admin user name
Enter a login ID for the admin user of your DB instance.

awsuser

The name must be 1-128 alphanumeric characters, and it can't be a [reserved word](#).

☐ Auto generate password
Amazon Redshift can generate a password for you, or you can specify your own password.

Admin user password

Dbuser123

☐ Show password
Must be 8-64 characters long. Must contain at least one uppercase letter, one lowercase letter and one number. Can be any printable ASCII character except "/", "", or "@".

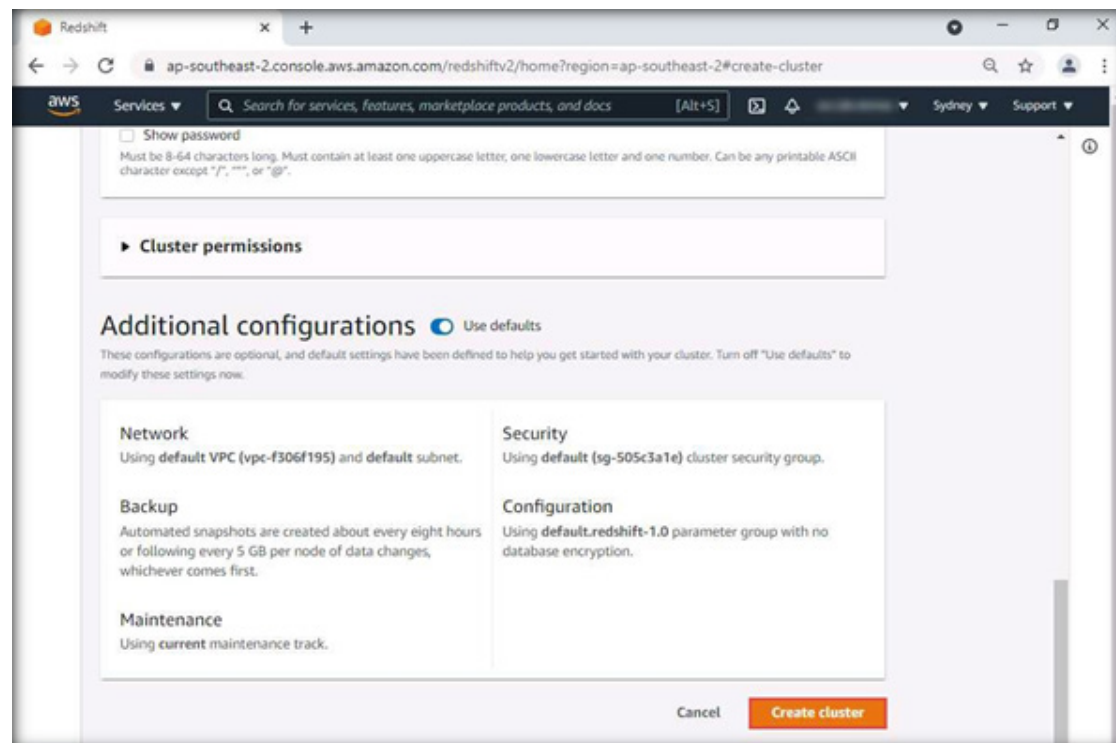
► Cluster permissions

Additional configurations

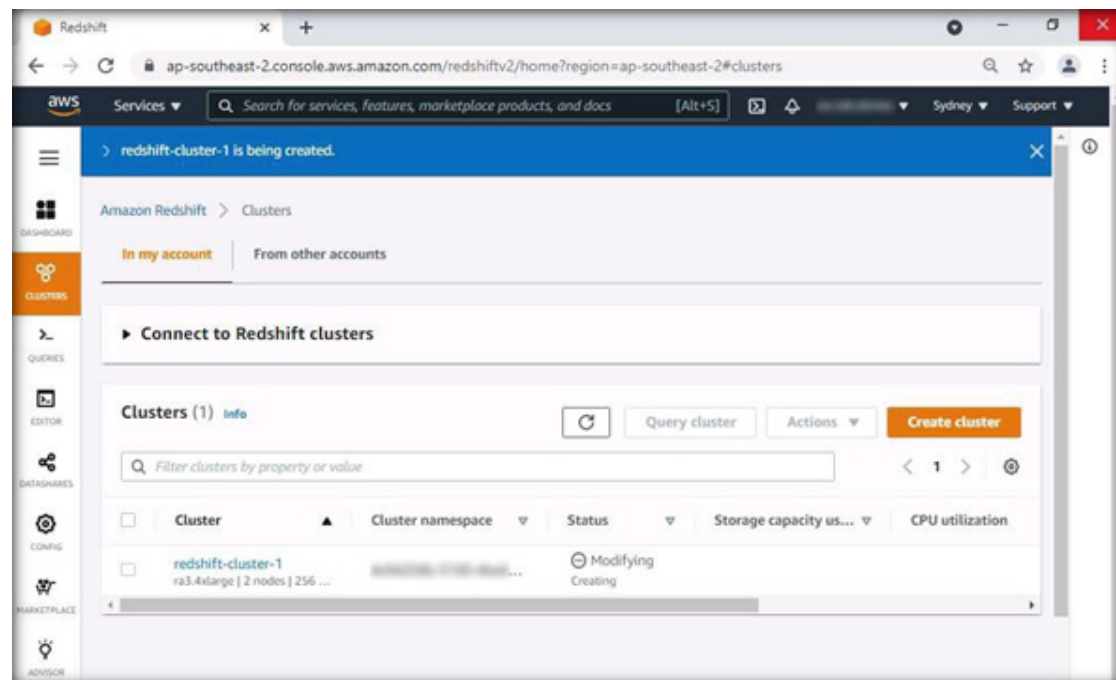
☒ Use defaults

These configurations are optional, and default settings have been defined to help you get started with your cluster. Turn off "Use defaults" to modify these settings now.

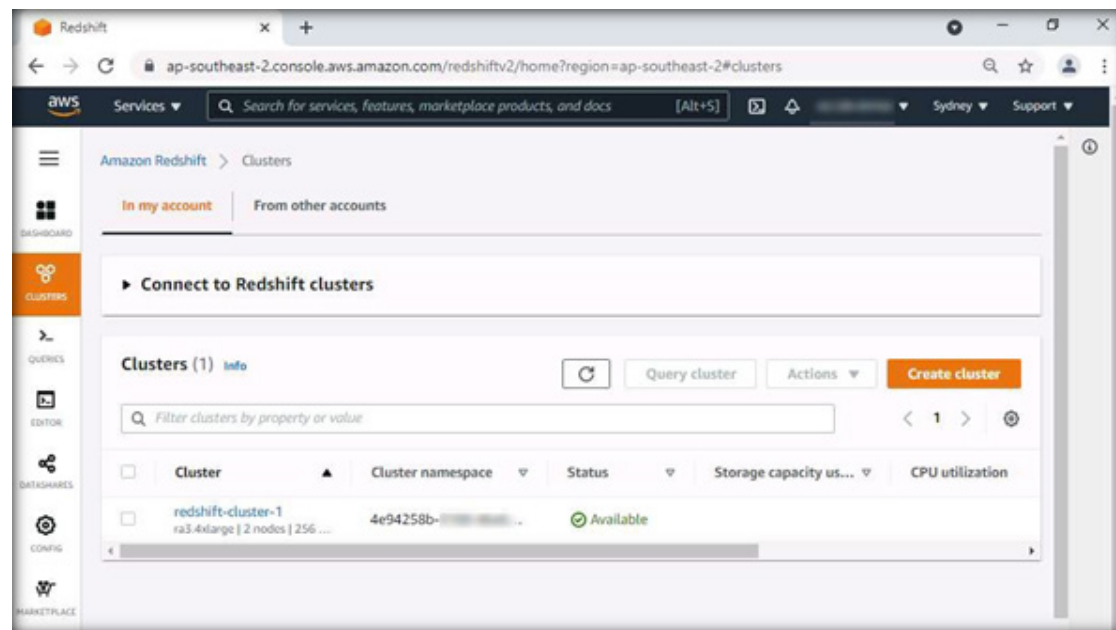
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



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.

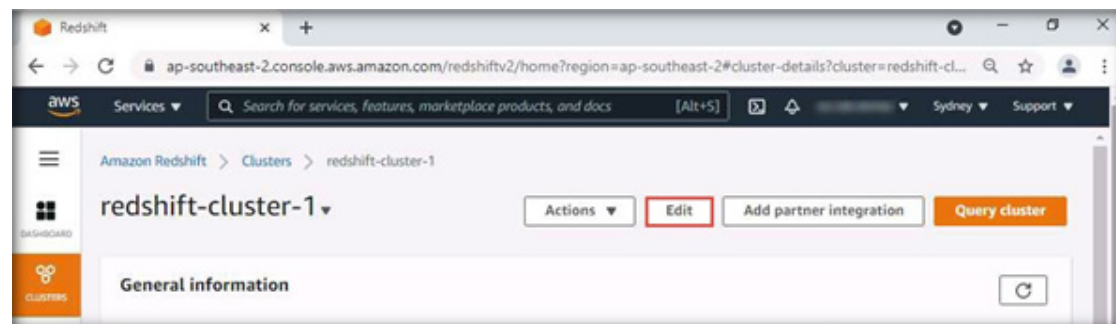


56. Once the cluster is fully created, you can see that the cluster's Status is Available.

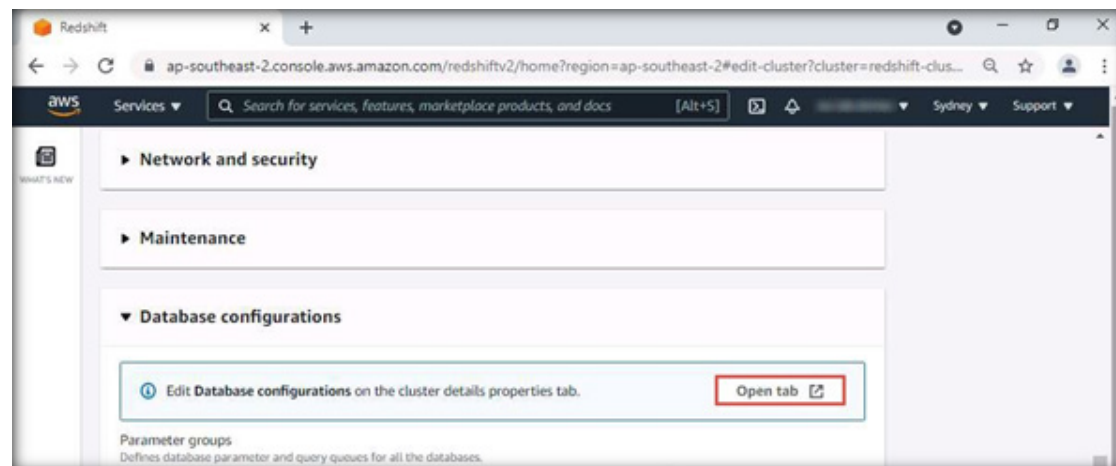


57. Click on the newly created cluster link (here, the cluster link is redshift-cluster-1) to modify the cluster setting.

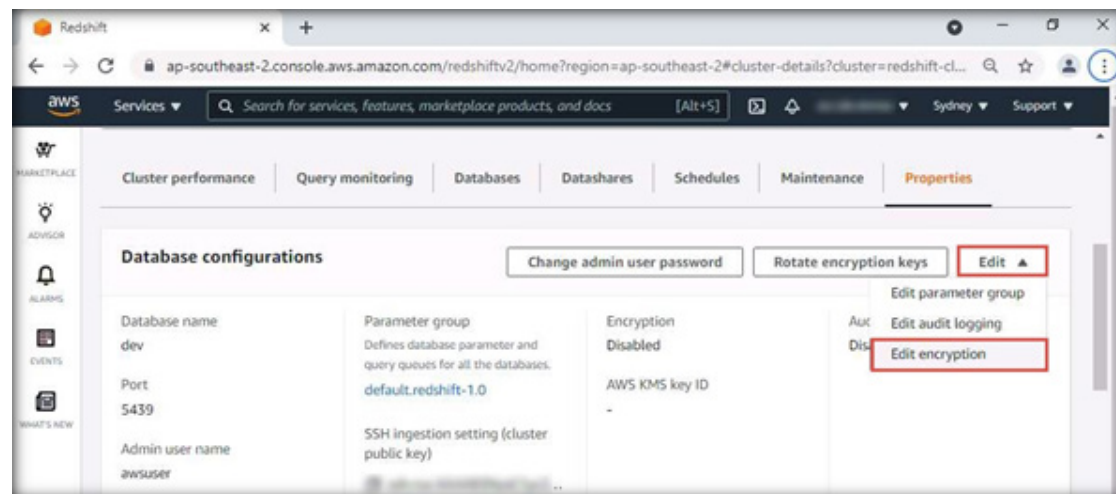
58. The newly created cluster redshift-cluster-1 page appears. Click on Edit button.



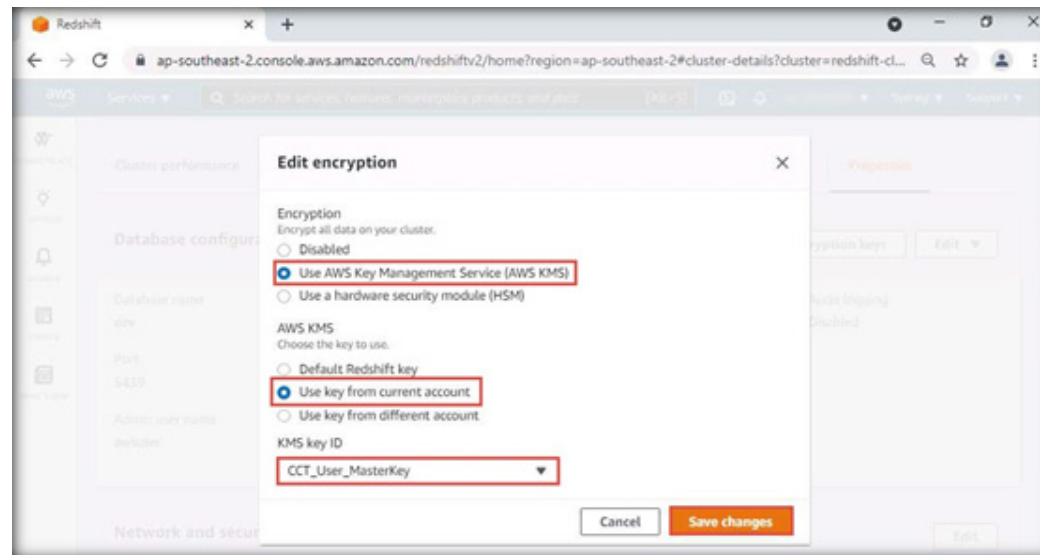
59. The Edit cluster redshift-cluster-1 page appears, scroll down to Database configurations. Click on Open tab.



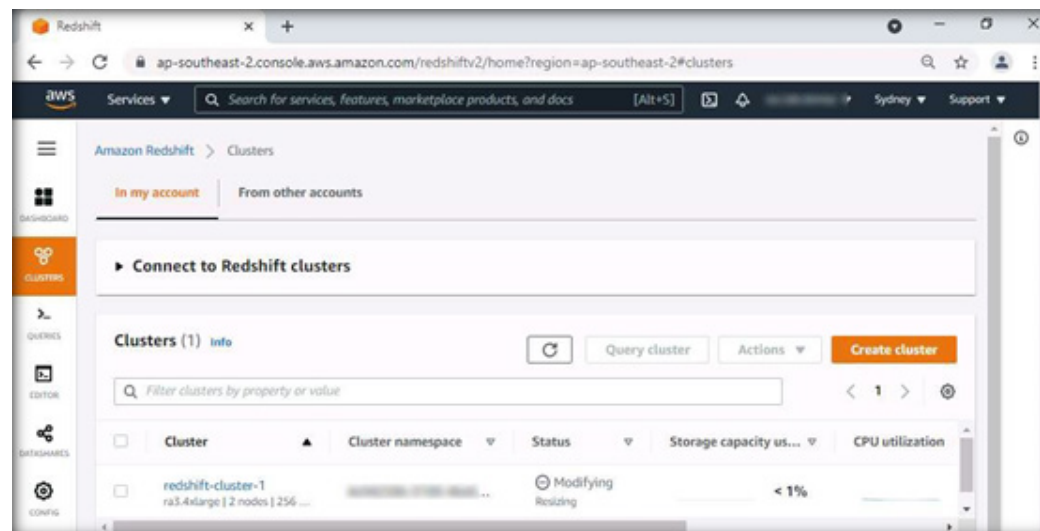
60. You will be redirected to Properties section. In the Properties section click on Edit drop down and select Edit encryption. In Edit encryption window, choose the Use AWS Key Management Service (AWS KMS) radio button, then choose Use key from current account, and finally choose CCT_User_Masterkey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



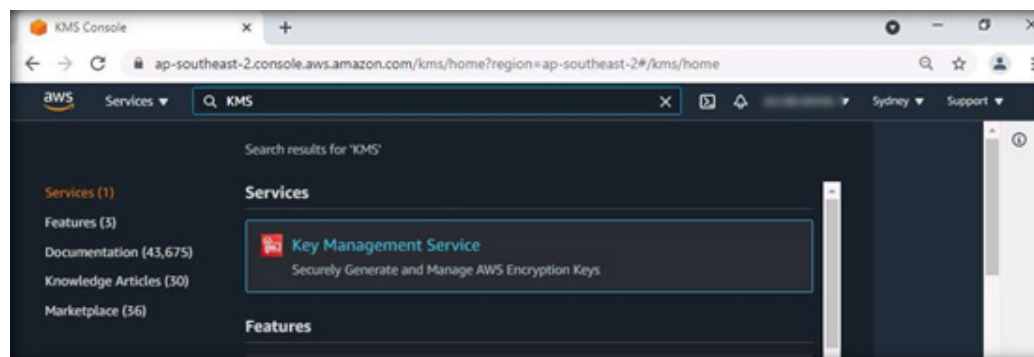
EXERCISE 4: IMPLEMENT KEY MANAGEMENT SERVICES IN AWS



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

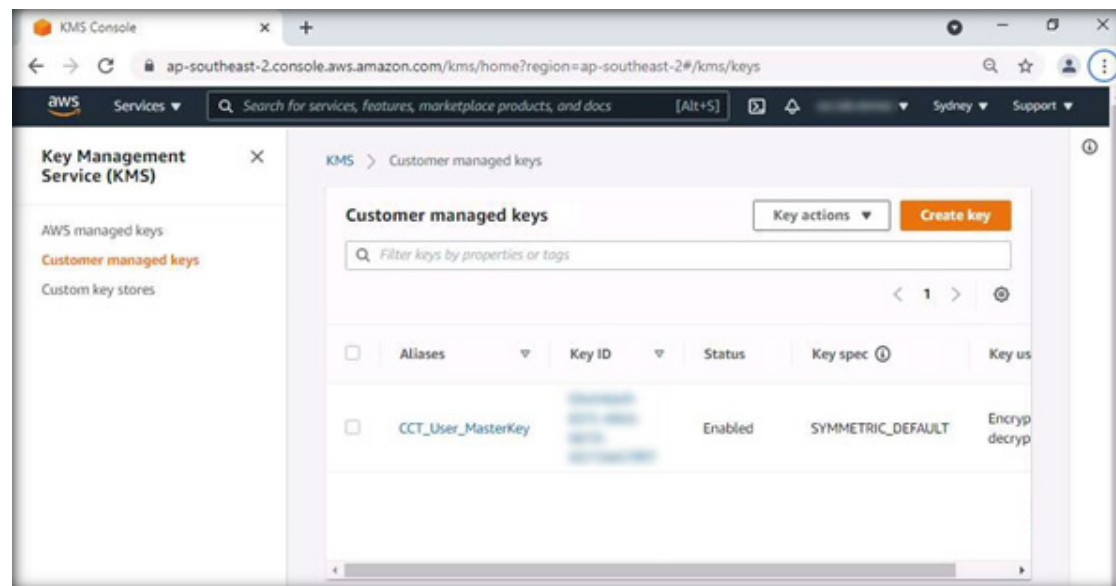


62. On the AWS Web Console, click on Services and search for KMS. Select Key Management Service.

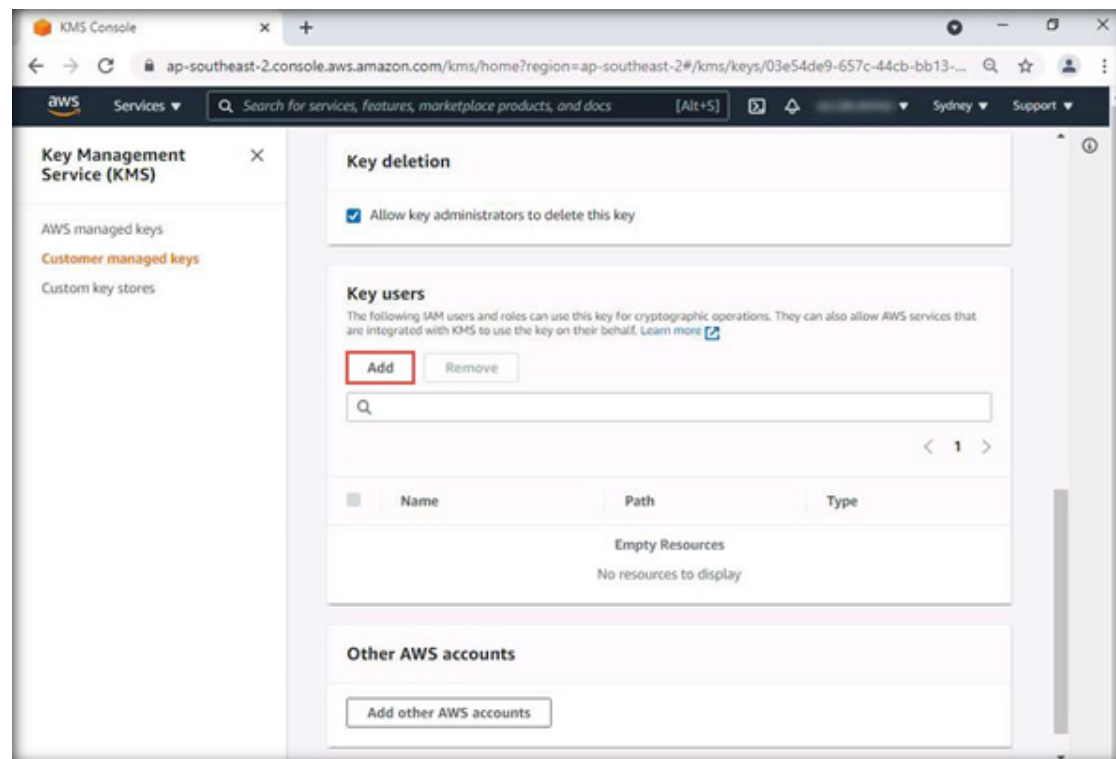


EXERCISE 4:
IMPLEMENT KEY
MANAGEMENT
SERVICES IN
AWS

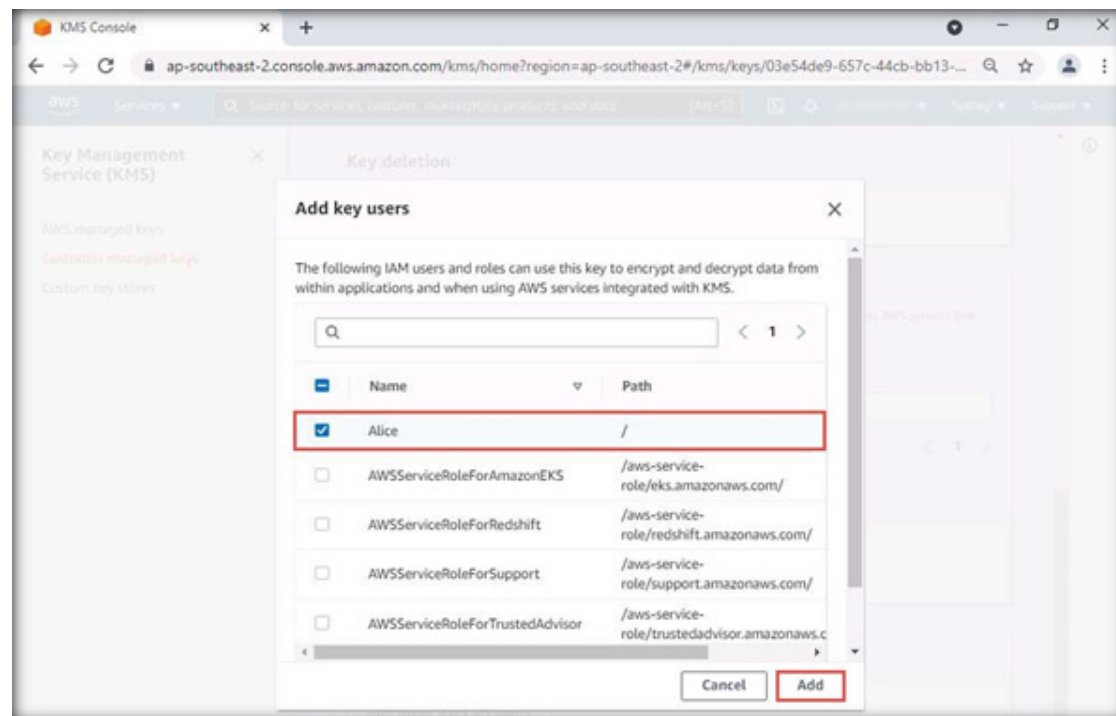
63. Once the KMS Console page appears, click on Customer managed keys (here CCT_User_MasterKey).



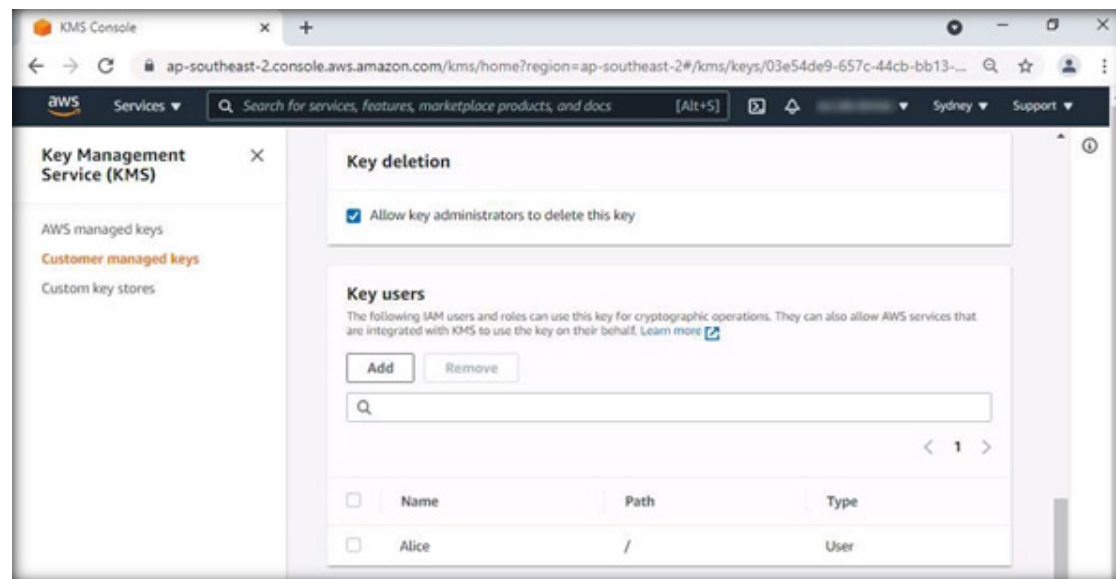
64. Scroll down until the Key users section. Click on Add.



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.



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

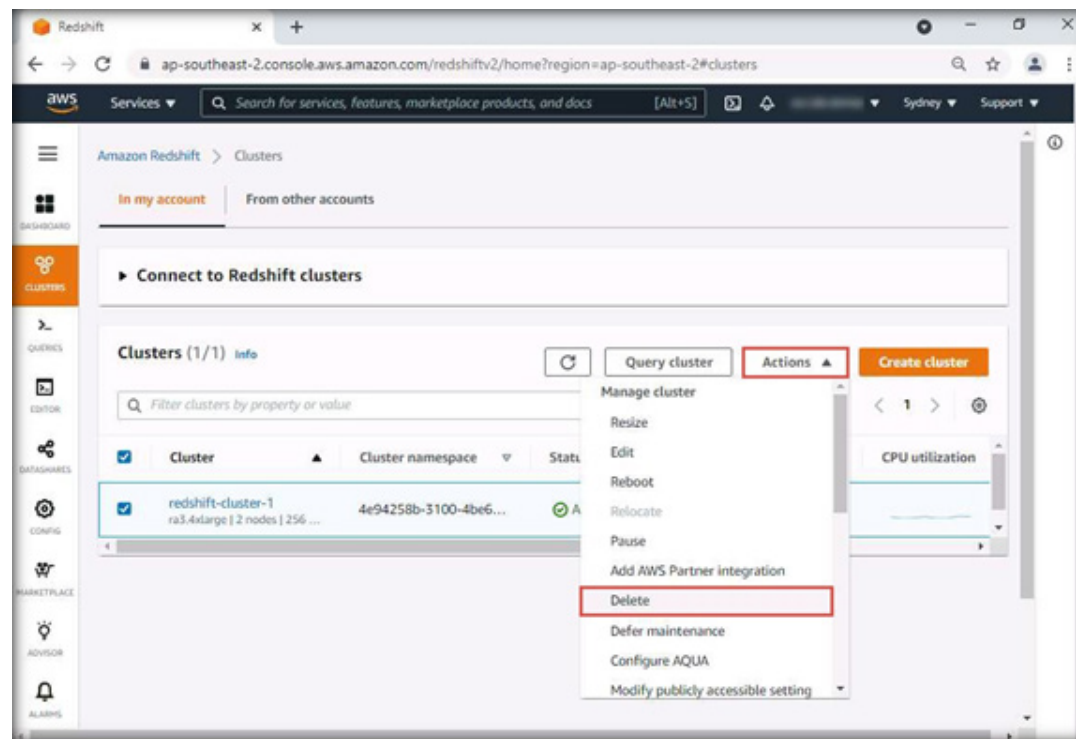


67. Thus, a security professional can implement AWS KMS.

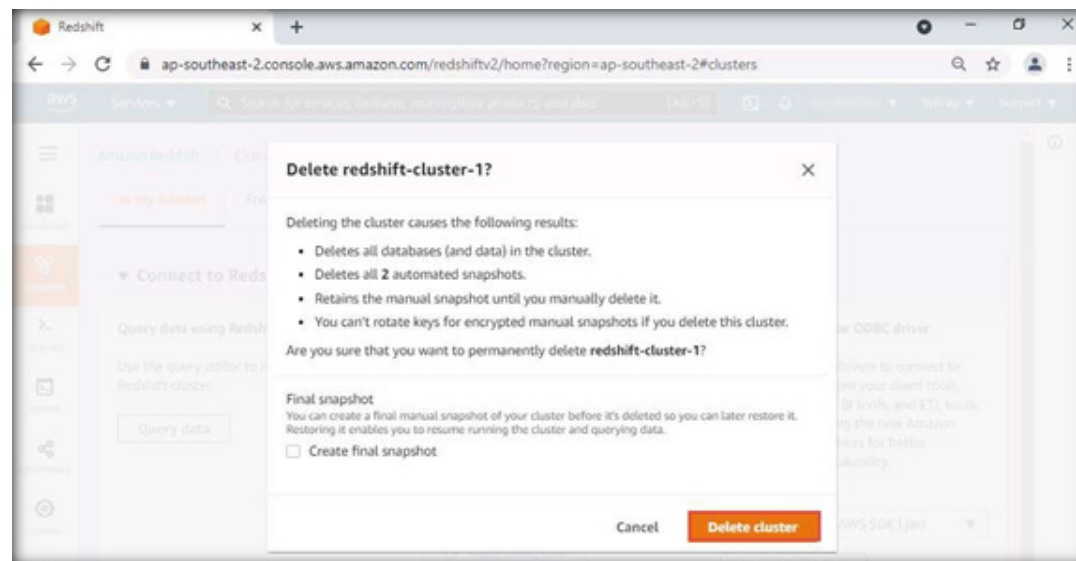
68. Now ensure that you delete the created cluster. To do this, type redshift in the main search bar and select Amazon Redshift.

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.



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



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

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 policies to give access to the right entities.

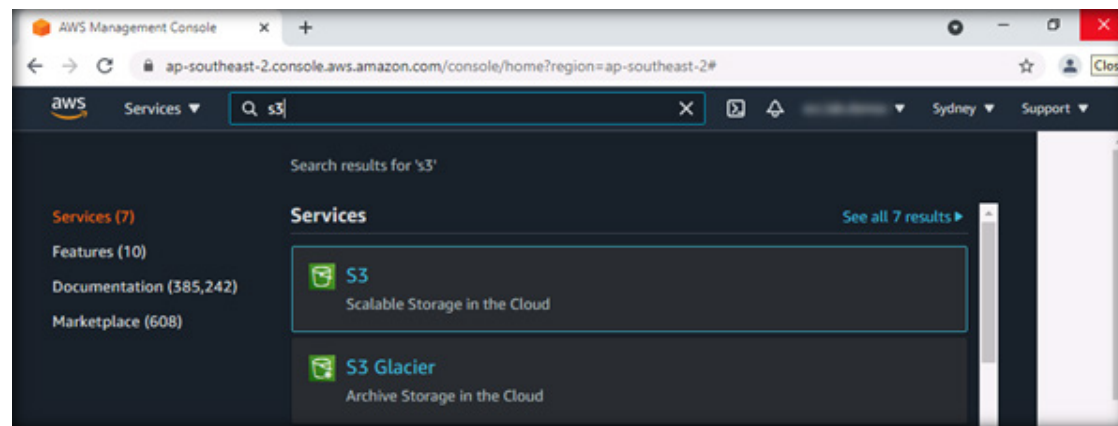
Note: Before starting this lab, you should create an AWS account using the following: <https://portal.aws.amazon.com/billing/signup>. Once the registration is completed, perform the following tasks.

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.

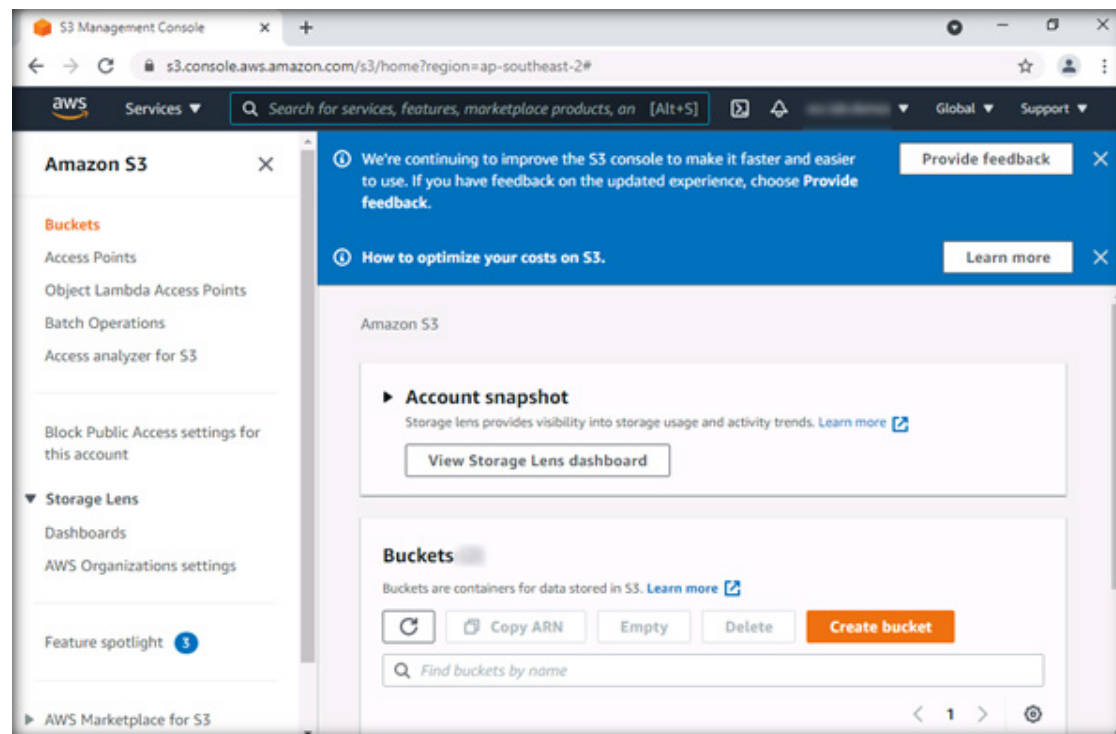
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

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.

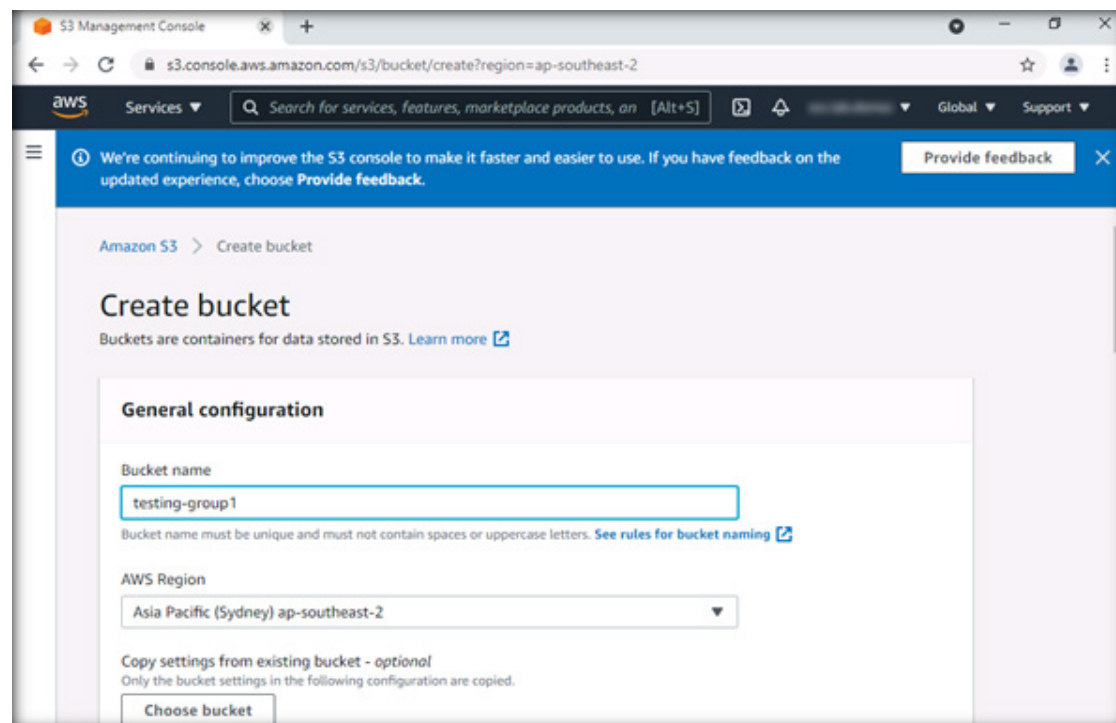


EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

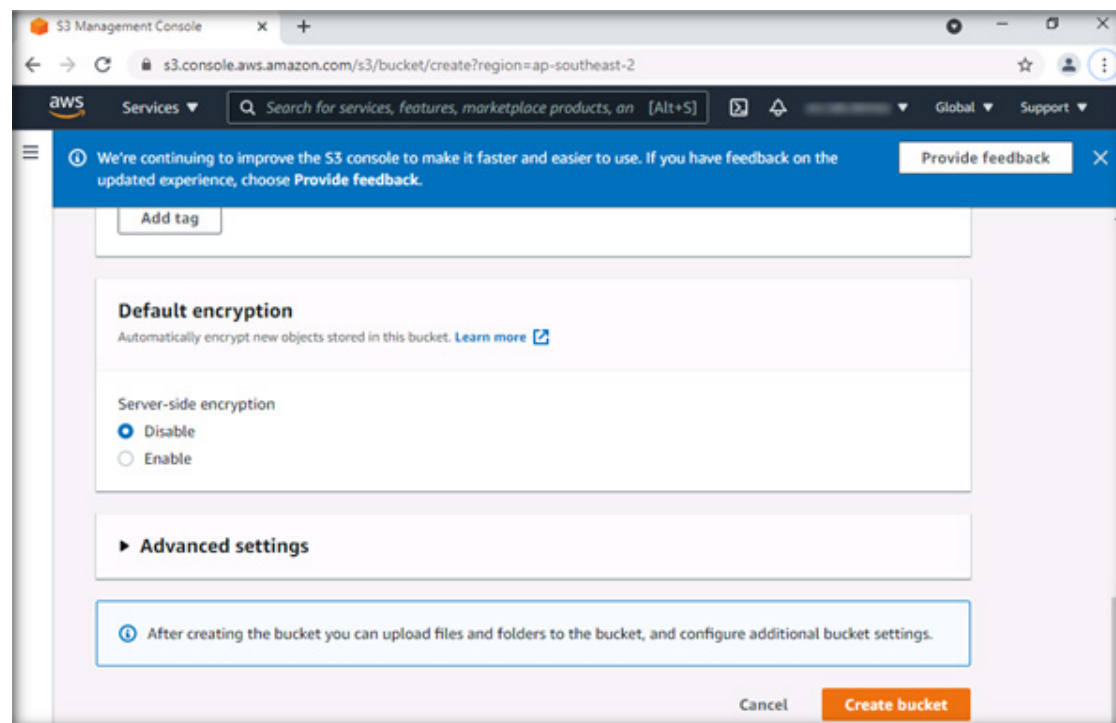
7. The S3 buckets page appears. Click on Create bucket.



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.

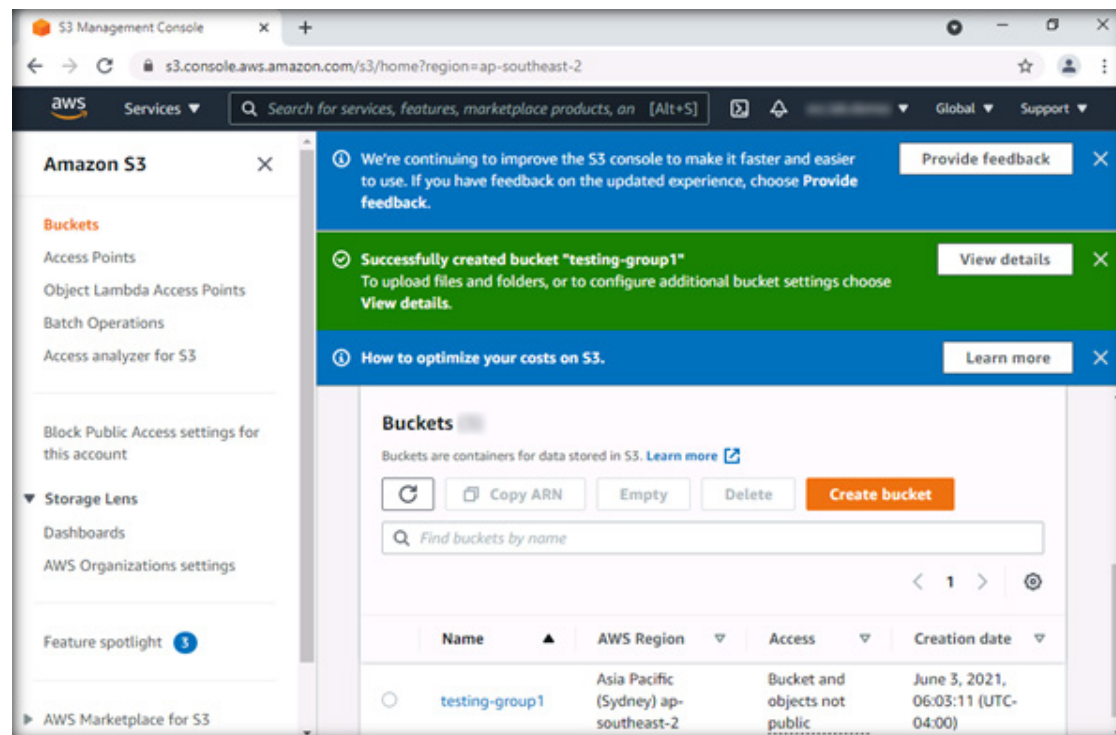


9. Retain default settings for all other sections, scroll down and click on Create bucket.

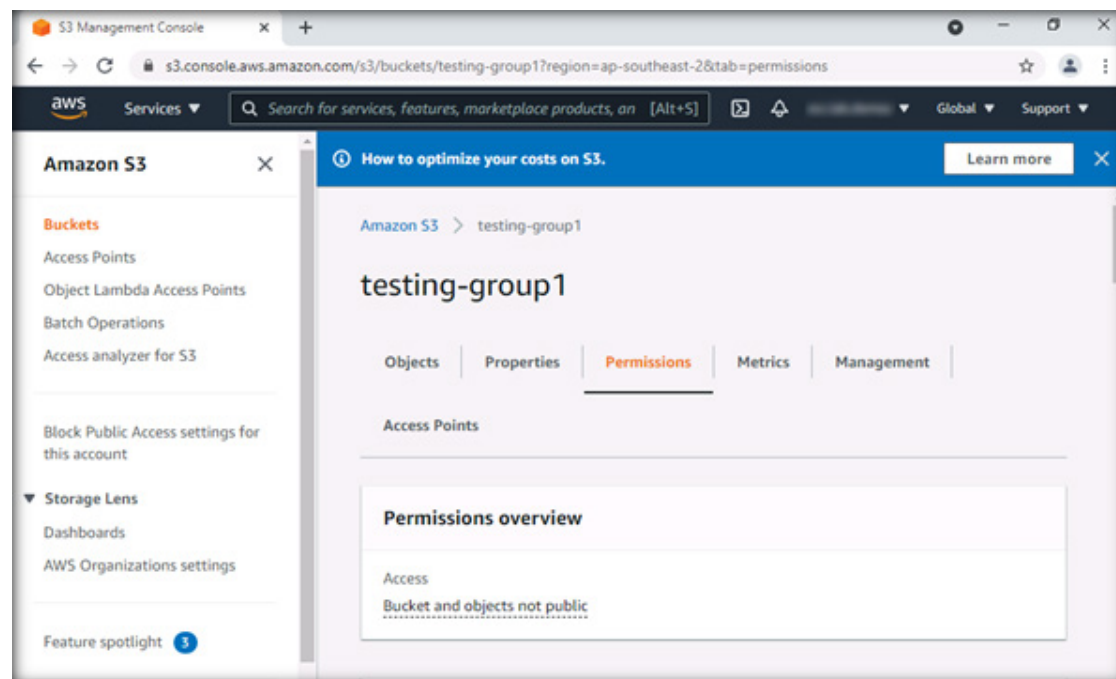


10. The new bucket is created.

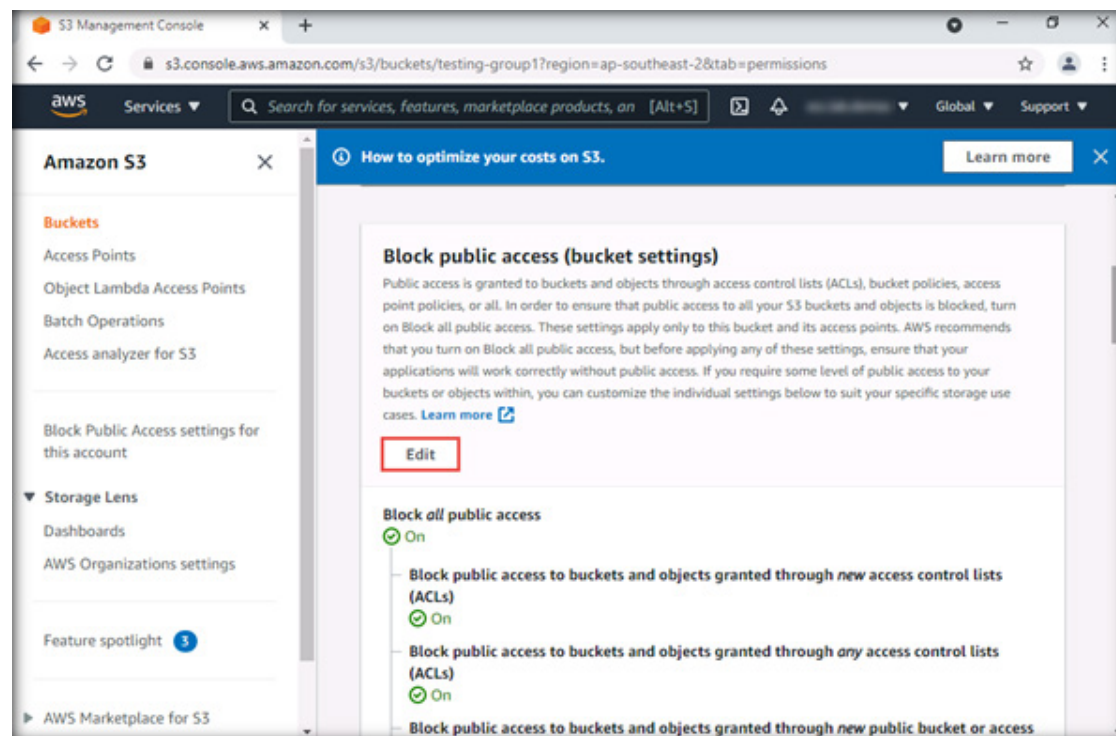
11. Select the testing-group1 S3 bucket.



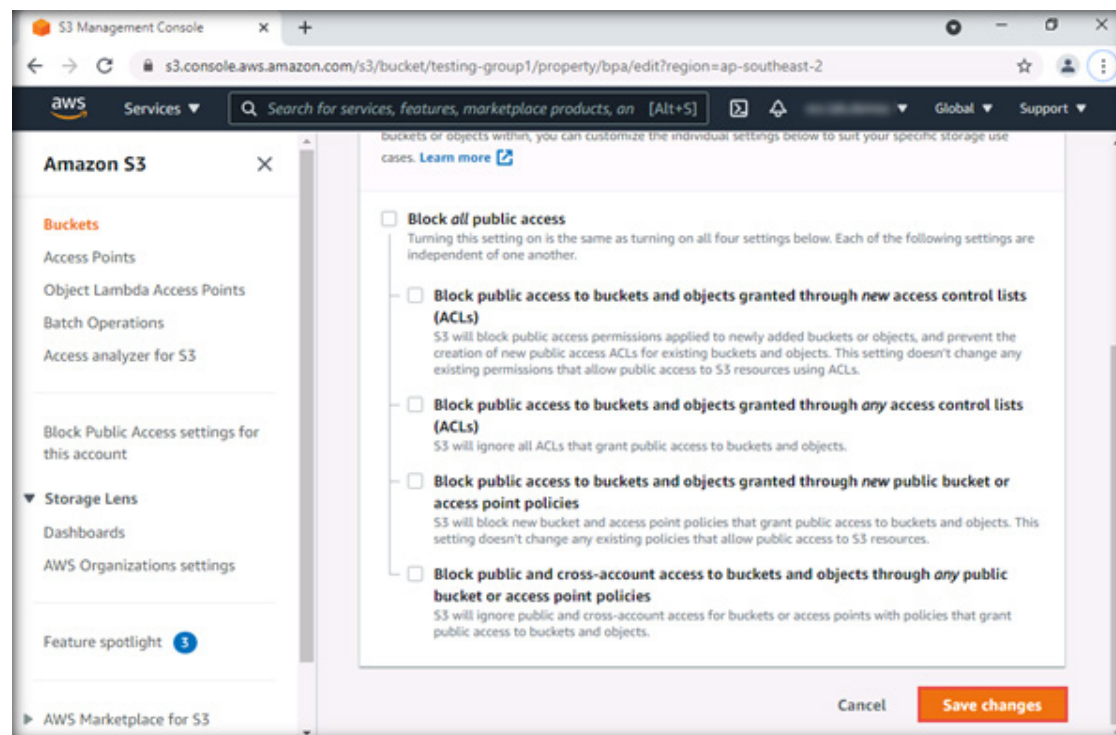
12. The Amazon S3 > testing-group1 page appears. Click on the Permissions tab.



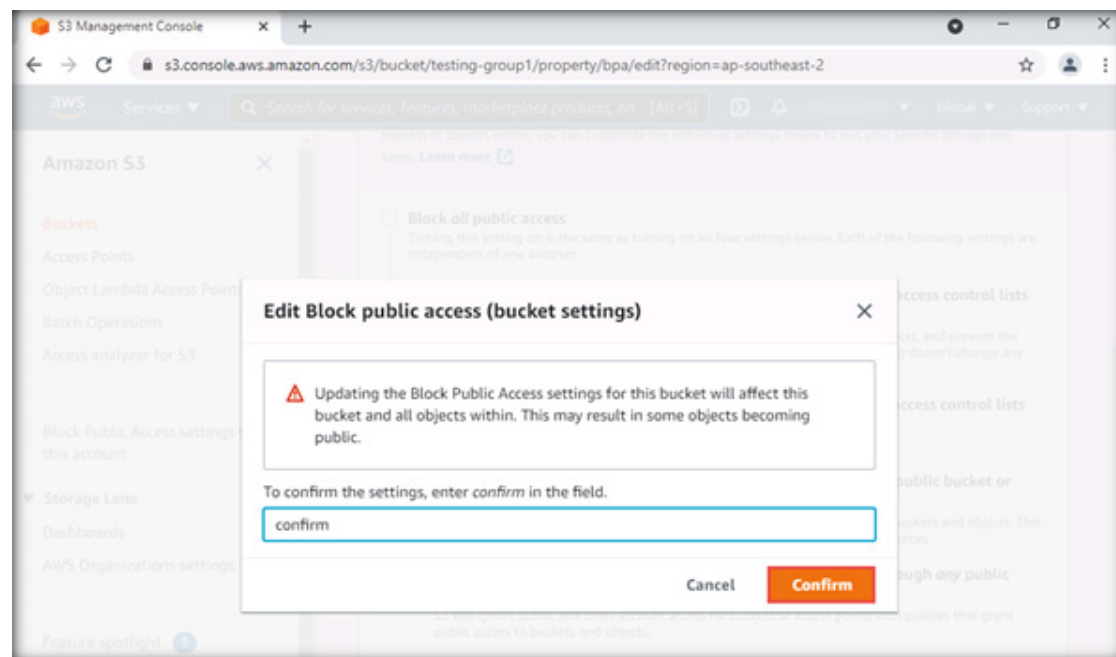
13. By default, the Block all public access tab is selected; click on Edit.



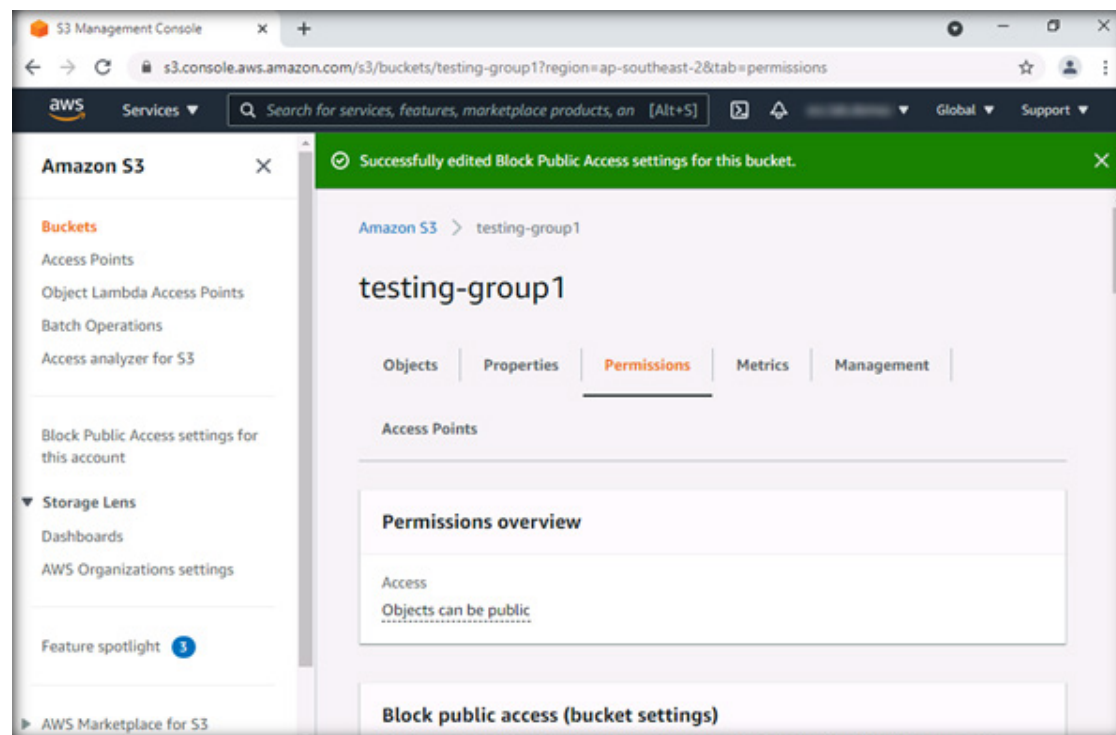
14. Uncheck Block all public access and click on Save changes.



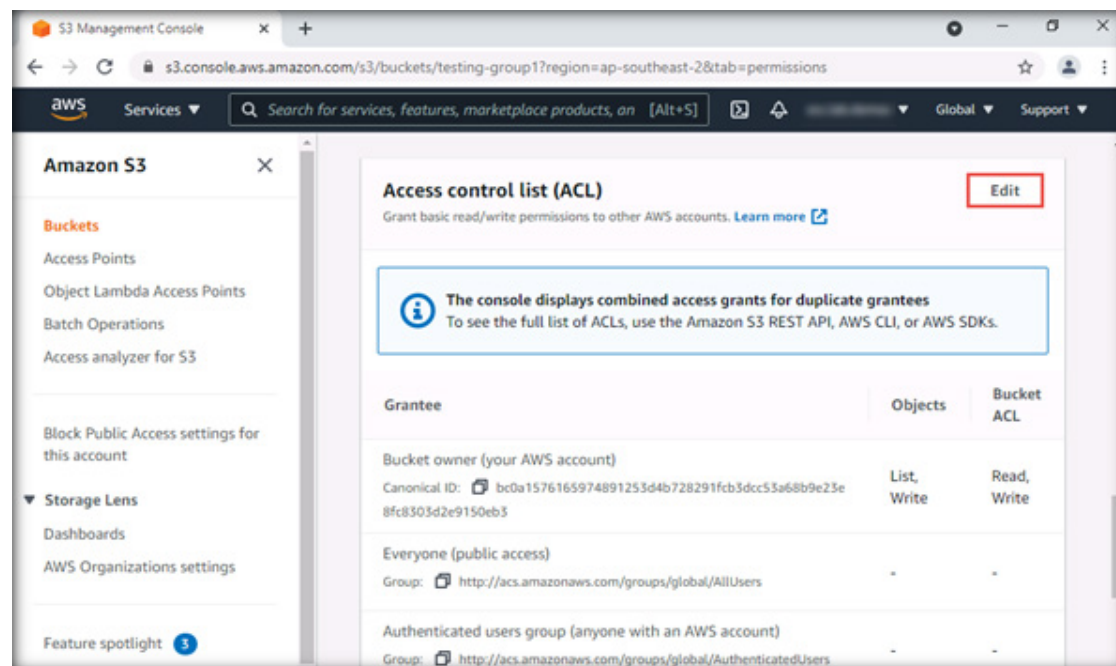
15. The confirmation dialog appears. Type confirm and click on Confirm.



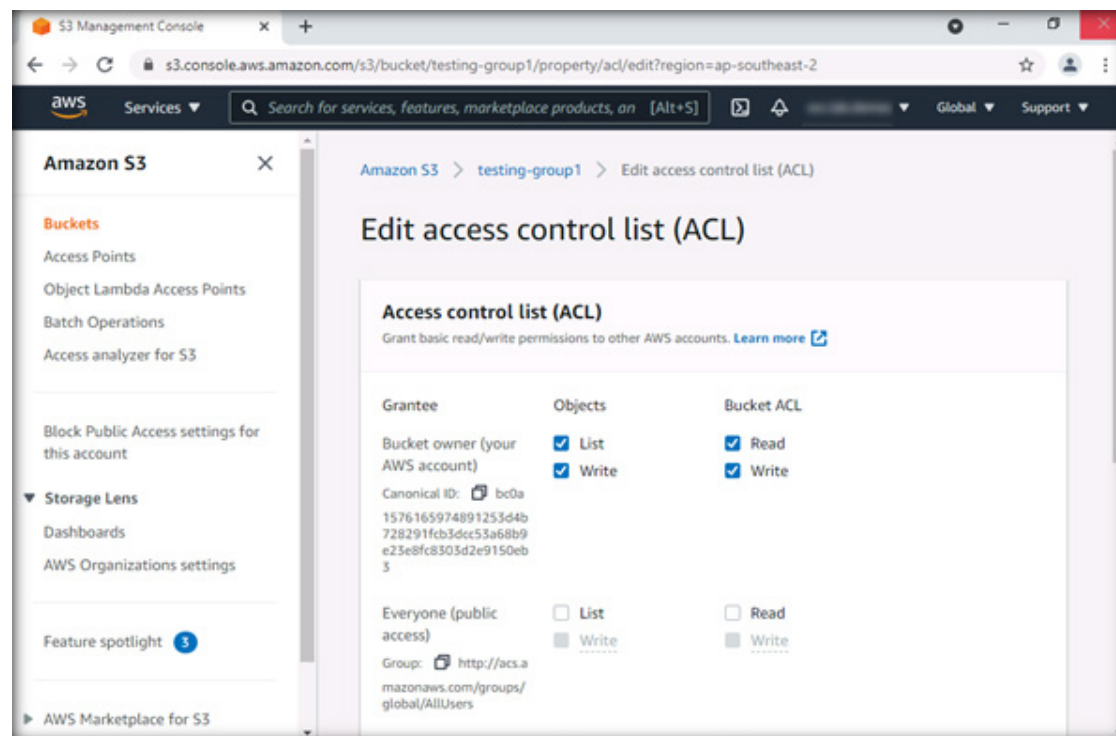
16. The Successfully edited Block Public Access settings for this bucket message appears.



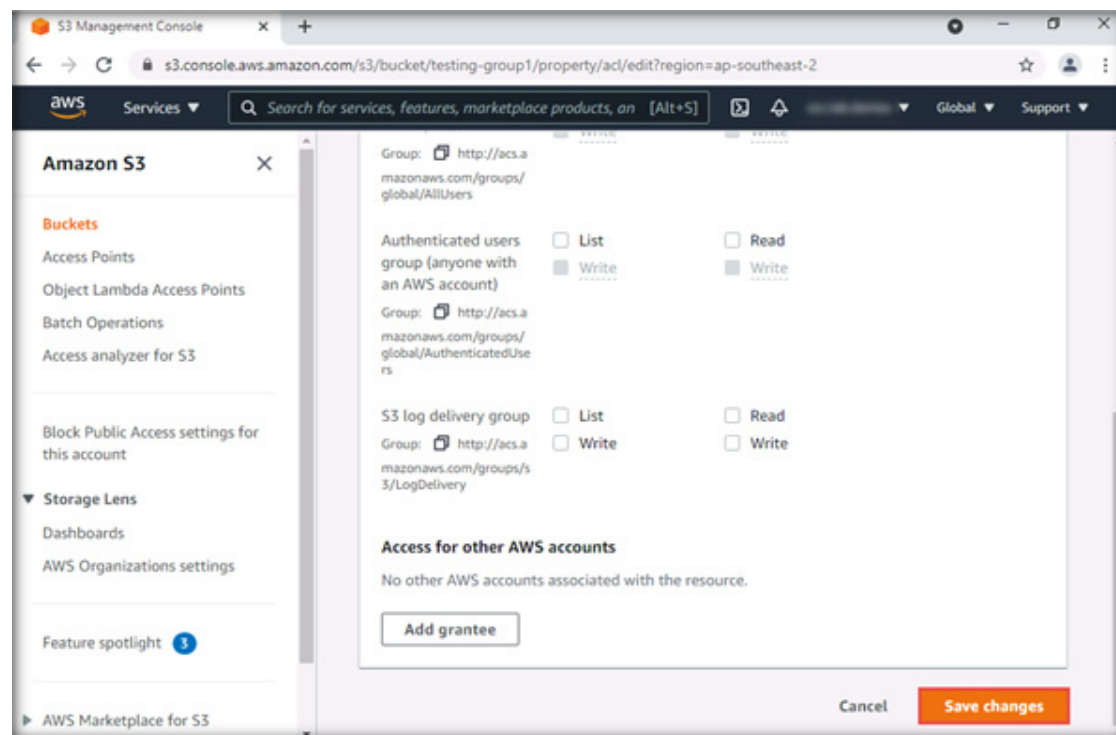
17. Next, scroll down to Access control List under the Permissions tab and click on Edit.



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.

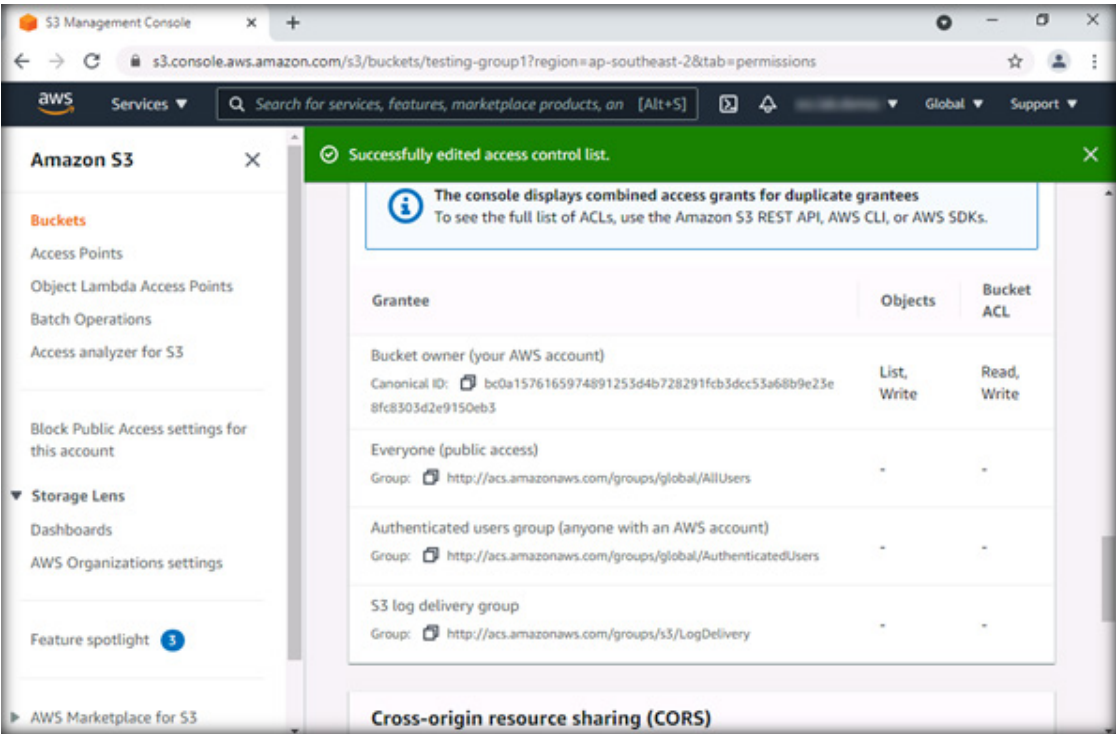


19. Scroll down and click on Save changes to apply the permissions on the AWS account.

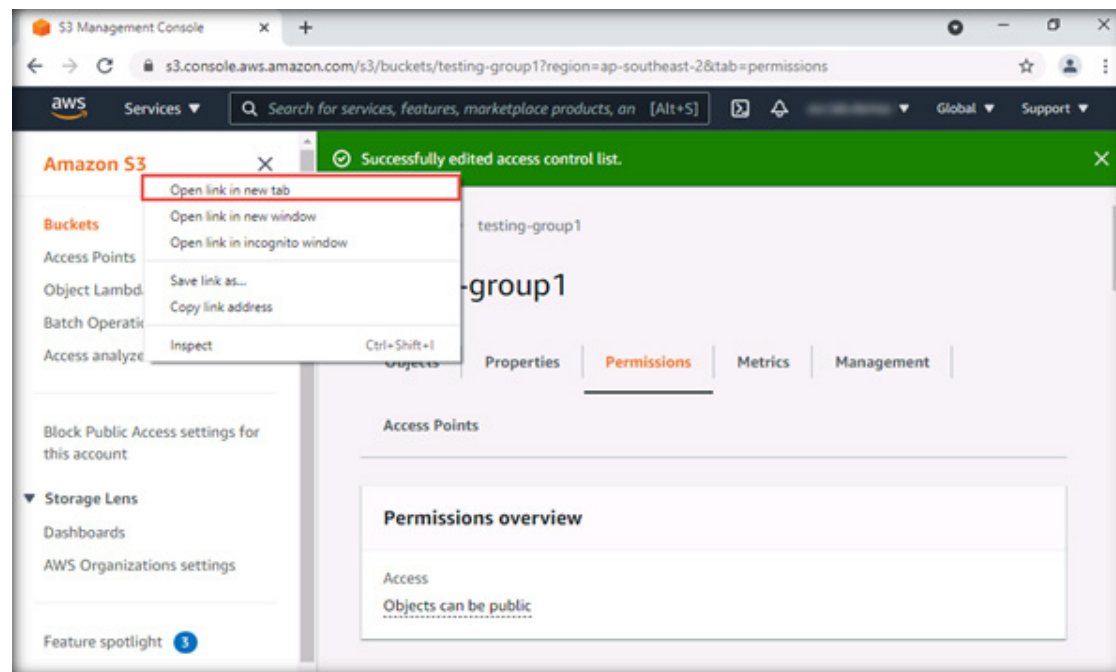


20. Public access settings have been updated successfully.

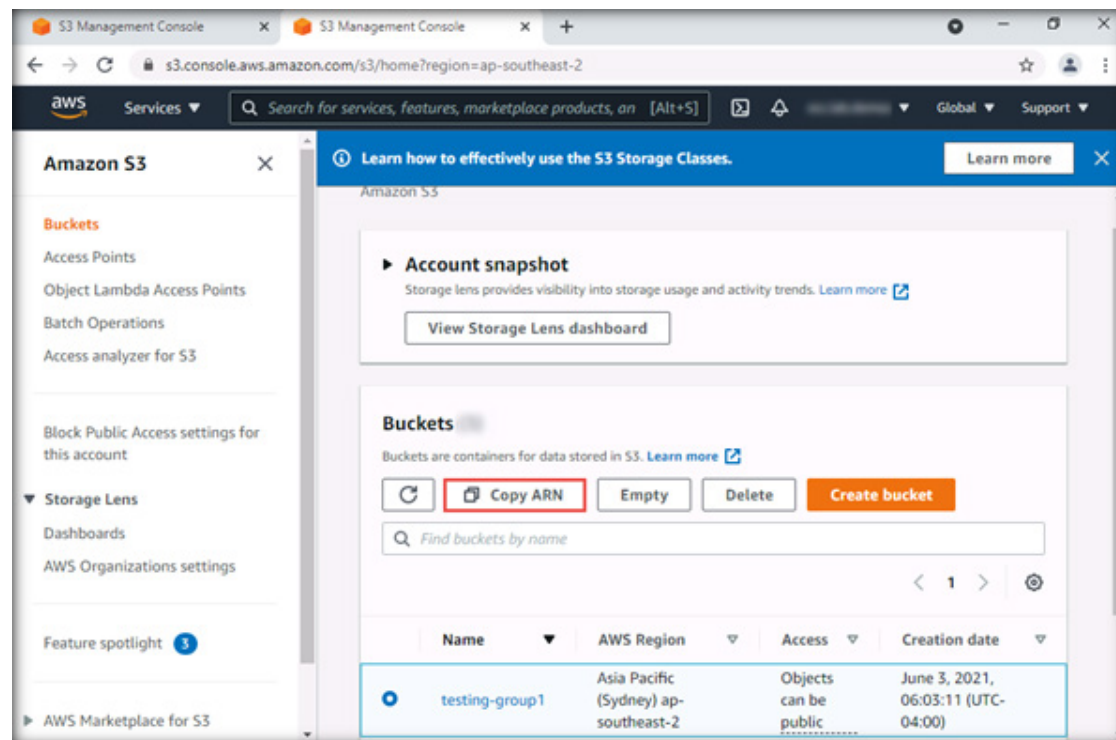
EXERCISE 5:
SECURE AMAZON
WEB SERVICES
STORAGE



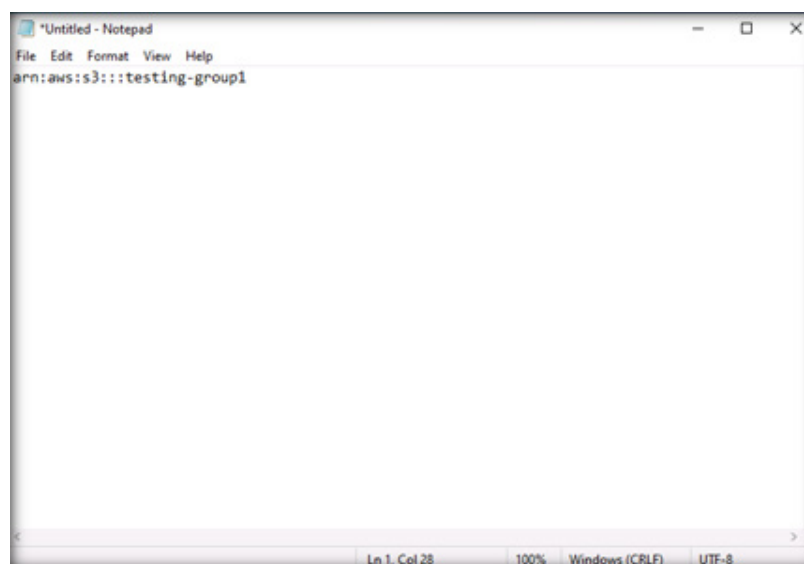
21. We have created a bucket policy with the name testing-group1. We need the ARN of the bucket policy. Right-click on Amazon S3 in the left corner and click on Open link in new tab.



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.



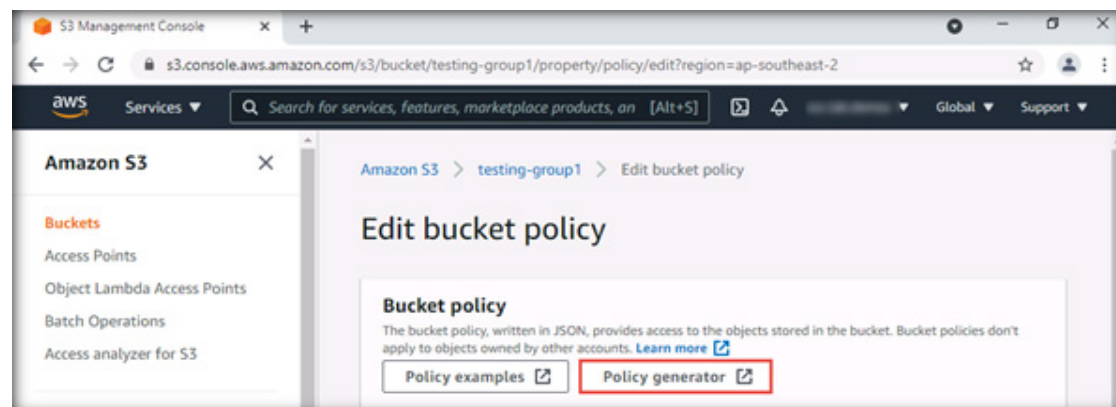
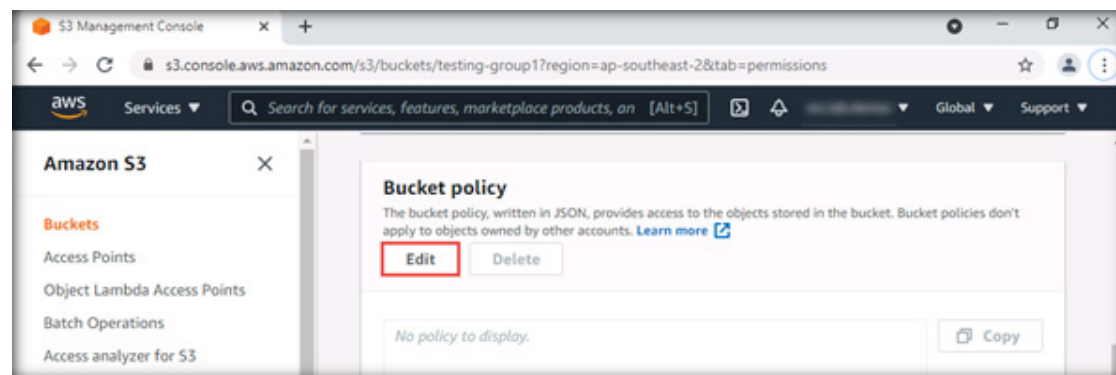
23. Open Notepad and paste the copied ARN into it.



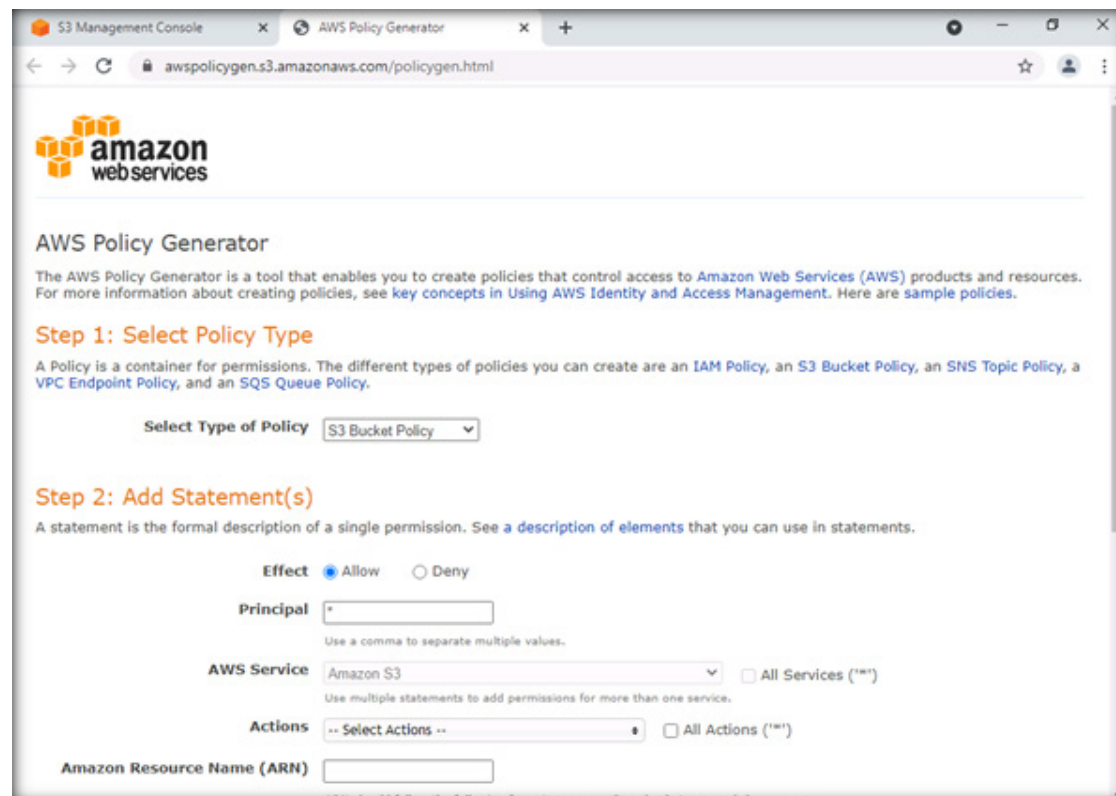
EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE

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.



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. Set AWS Service to Amazon S3.



amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services ("*")

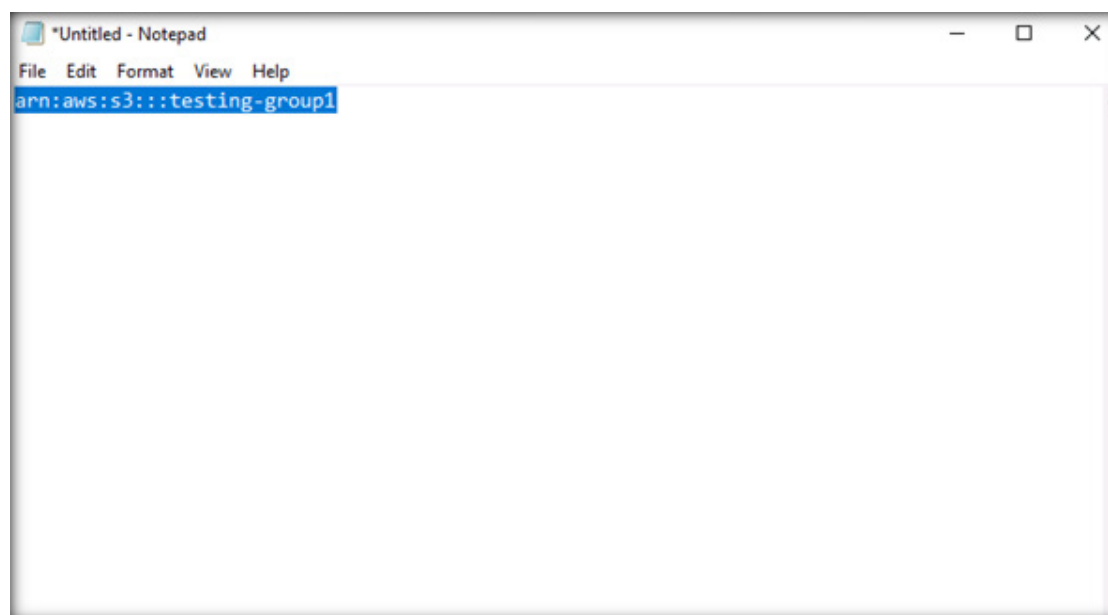
Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- ☐ All Actions ("*")

Amazon Resource Name (ARN)

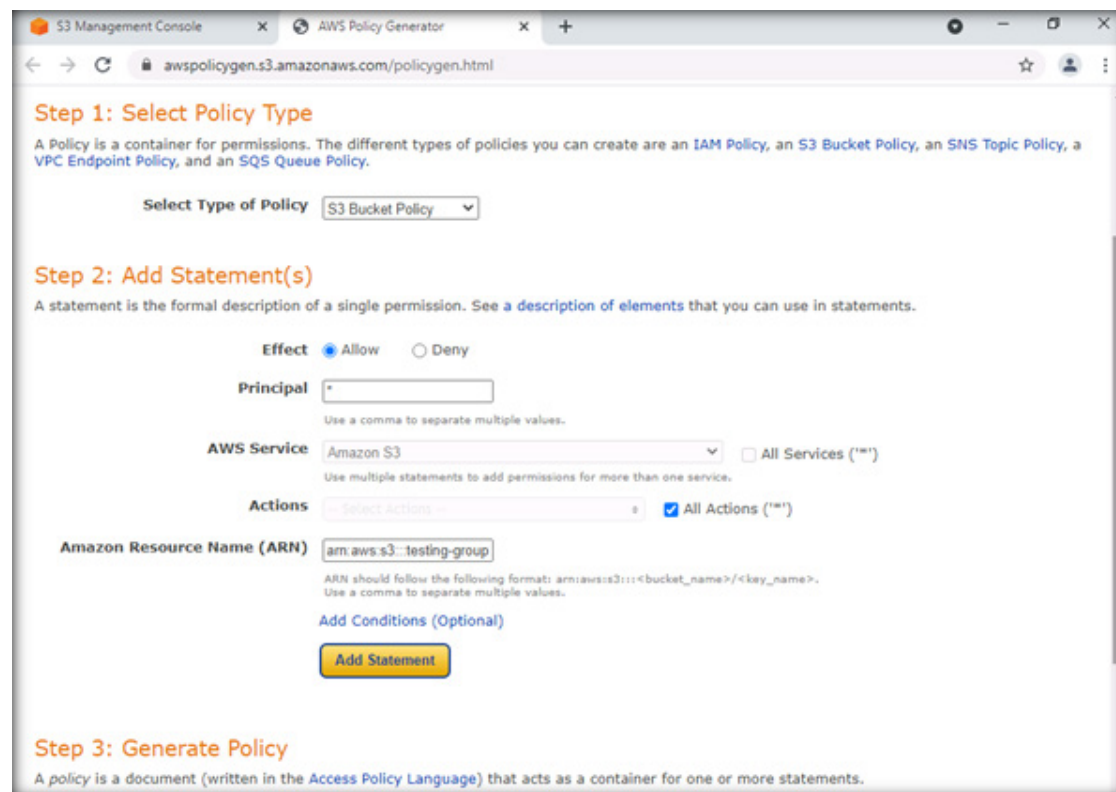
ARNs should follow the following format: `arn:aws:s3:::bucket-name/key-name`

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.



Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect: ☒ Allow ☐ Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon S3 ☐ All Services ("*")

Use multiple statements to add permissions for more than one service.

Actions: Select Actions ☒ All Actions ("*")

Amazon Resource Name (ARN): arn:aws:s3::testing-group

ARN should follow the following format: `arn:aws:s3:::<bucket_name>/<key_name>`.
Use a comma to separate multiple values.

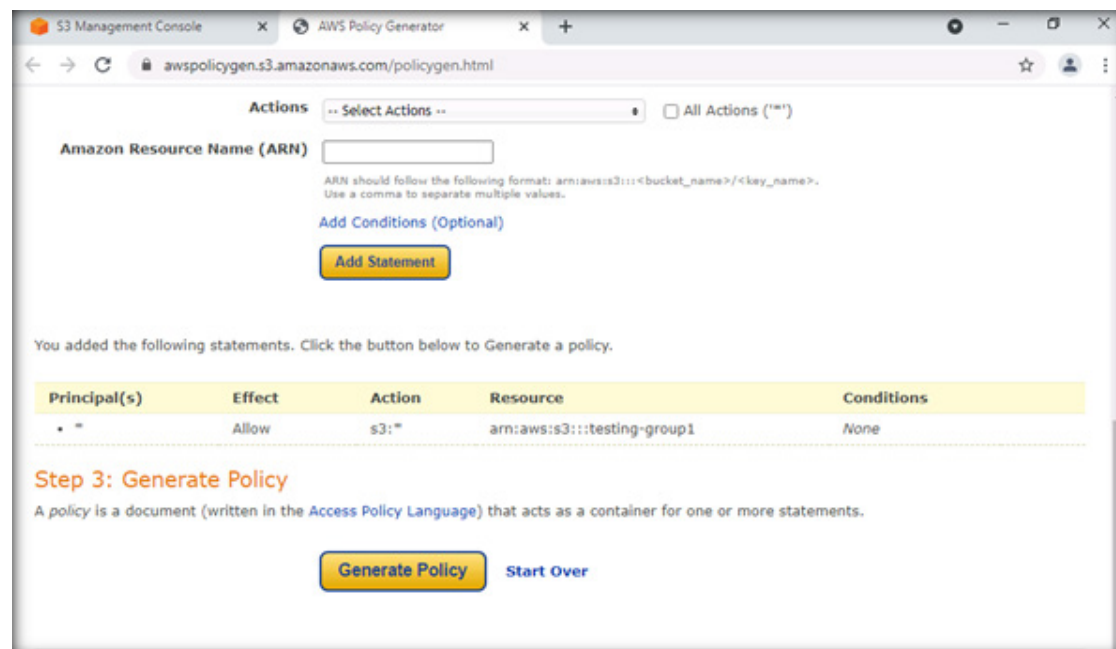
[Add Conditions \(Optional\)](#)

Add Statement

Step 3: Generate Policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

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

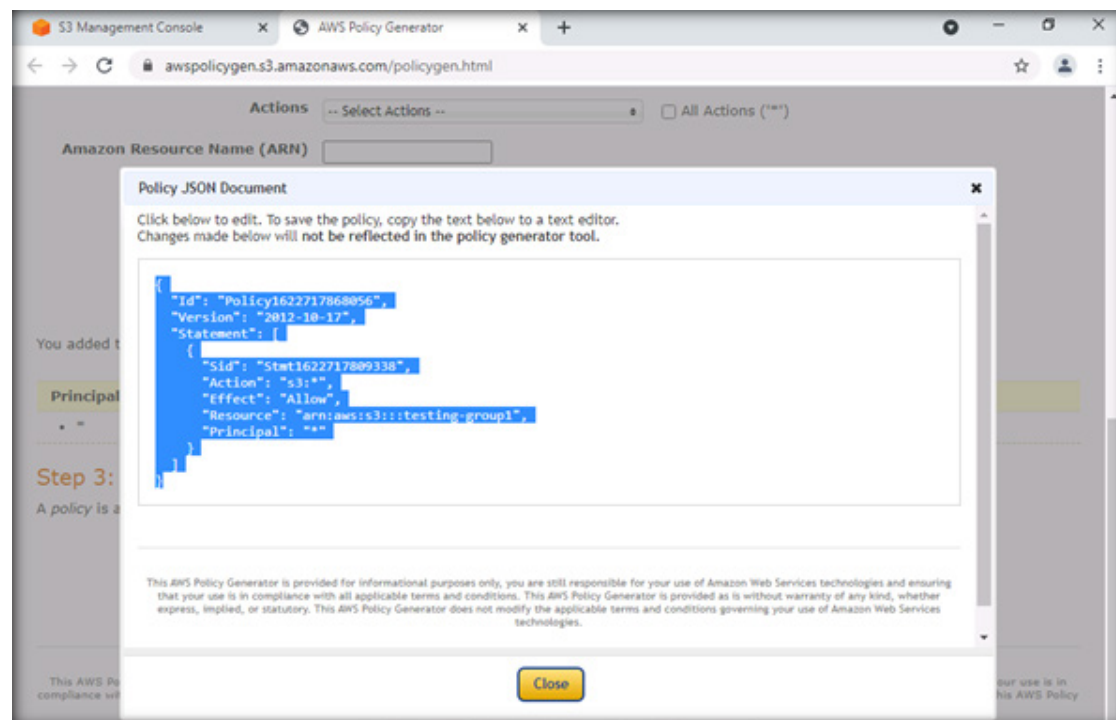


The screenshot shows the AWS Policy Generator interface in a web browser. The browser tabs include 'S3 Management Console' and 'AWS Policy Generator'. The address bar shows 'awspolicygen.s3.amazonaws.com/policygen.html'. The 'Actions' dropdown is set to '-- Select Actions --' with a checkbox for 'All Actions ("*")'. The 'Amazon Resource Name (ARN)' field is empty, with a note: 'ARN should follow the following format: arn:aws:s3:::bucket_name/<key_name>. Use a comma to separate multiple values.' Below this is a link 'Add Conditions (Optional)' and a yellow 'Add Statement' button. A message states: 'You added the following statements. Click the button below to Generate a policy.' Below this is a table with one row of data:

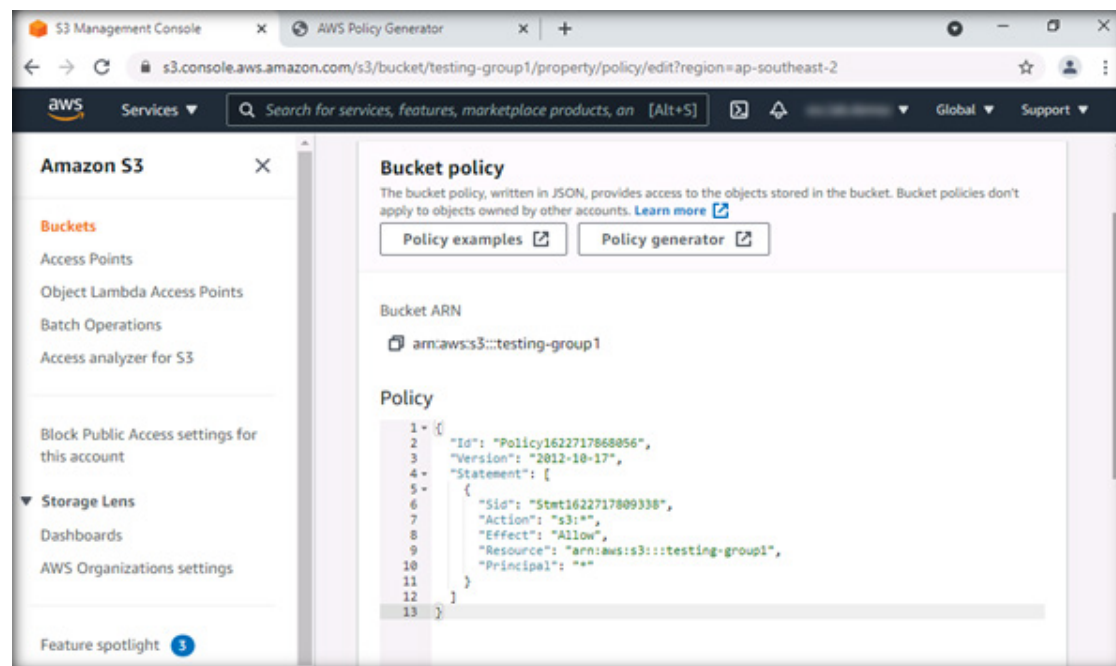
Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:*	arn:aws:s3:::testing-group1	None

Below the table is the section 'Step 3: Generate Policy' with the text: 'A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.' At the bottom are two buttons: 'Generate Policy' (yellow) and 'Start Over' (blue).

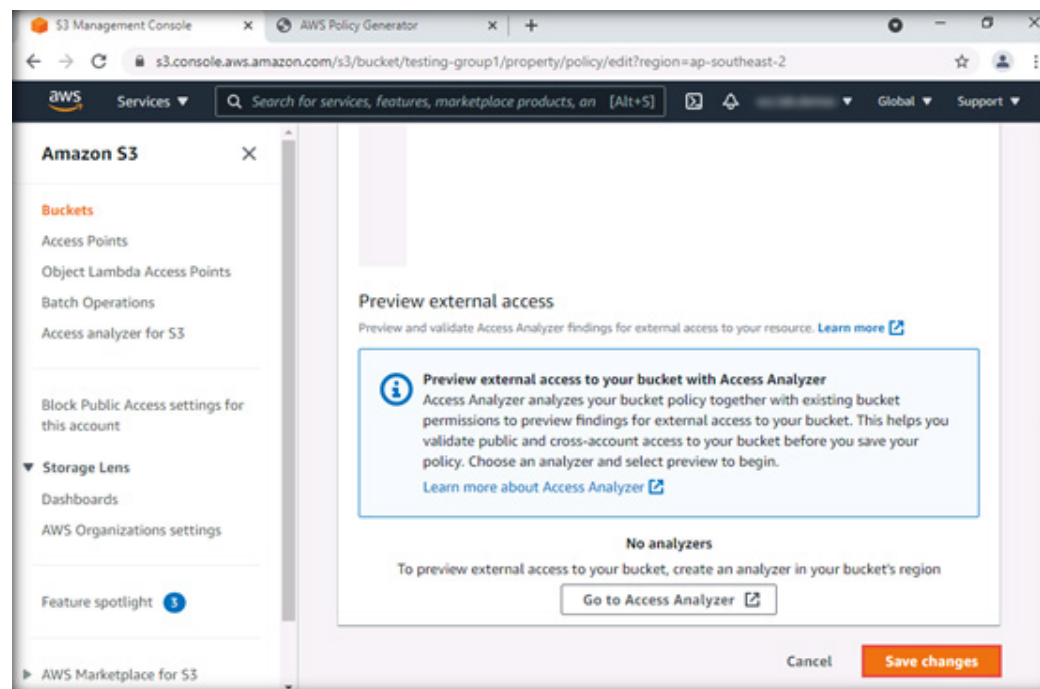
30. The Policy JSON Document pop-up appears, along with the generated JSON code. Copy the code as shown in the screenshot below and click on Close.



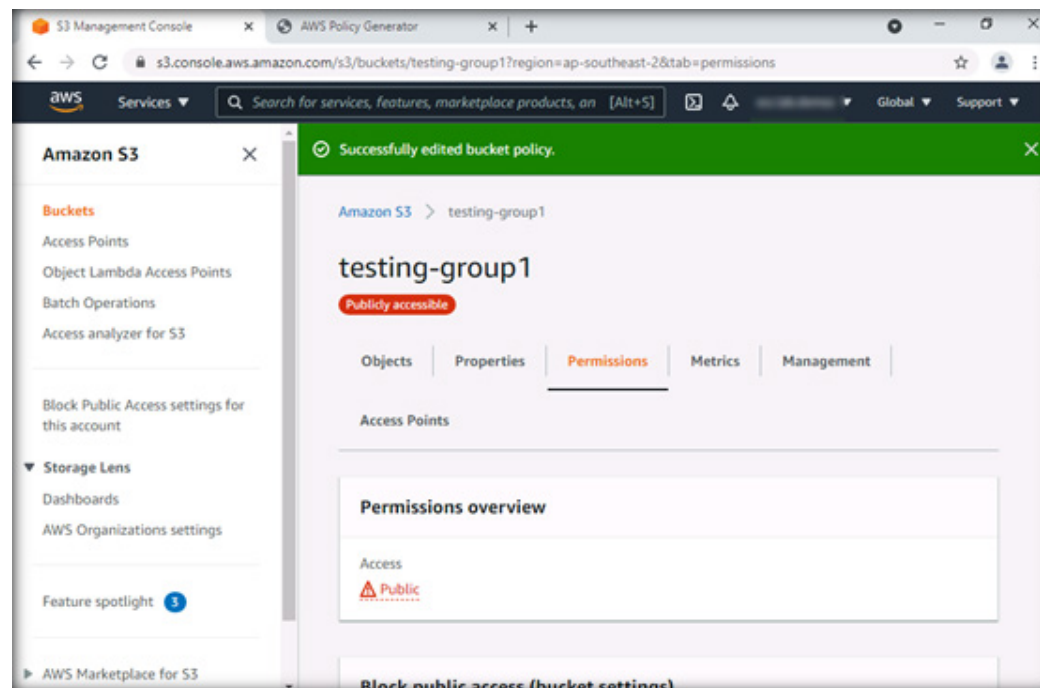
31. Switch to the first tab of the web browser S3 Management Console to configure Bucket Policy. Paste the copied JSON code from the Bucket policy editor, scroll down and click on Save changes.



EXERCISE 5: SECURE AMAZON WEB SERVICES STORAGE



32. Now the bucket has public access.



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.

EC-Council

