

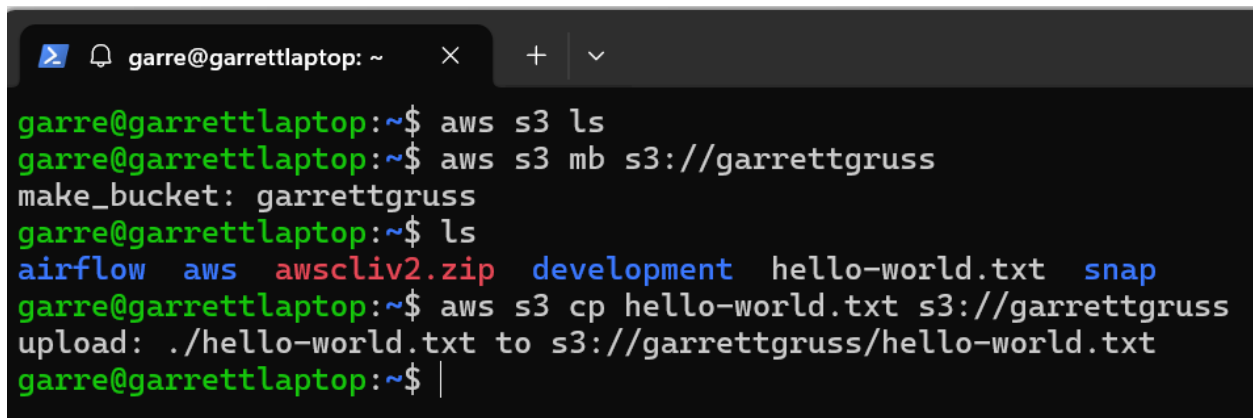
# Lab 1

Garrett Gruss 4976-3695

January 30, 2026

## 1 Summary

This exercise covered the creation of a user root account and several IAM user accounts. Access keys were created and inactivated through the AWS CLI. User groups were created and configured through the console and S3 Access was tested to verify the account permissions were configured.

A terminal window with a dark background and light-colored text. The window title bar shows 'garre@garrettlaptop: ~' and standard window controls. The terminal content shows a series of commands and their outputs: 'aws s3 ls' returns an empty list; 'aws s3 mb s3://garrettgruss' creates a bucket; 'ls' shows the current directory contents including 'airflow', 'aws', 'awscliv2.zip', 'development', 'hello-world.txt', and 'snap'; 'aws s3 cp hello-world.txt s3://garrettgruss' uploads the file; and the final command 'upload: ./hello-world.txt to s3://garrettgruss/hello-world.txt' shows the upload path.

```
garre@garrettlaptop:~$ aws s3 ls
garre@garrettlaptop:~$ aws s3 mb s3://garrettgruss
make_bucket: garrettgruss
garre@garrettlaptop:~$ ls
airflow  aws  awscliv2.zip  development  hello-world.txt  snap
garre@garrettlaptop:~$ aws s3 cp hello-world.txt s3://garrettgruss
upload: ./hello-world.txt to s3://garrettgruss/hello-world.txt
garre@garrettlaptop:~$ |
```

Figure 1: Exercise 1.1

My security credentials

Root user

Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference

Account details

Actions

Account name

Garrett-Gruss

Account ID

349577273469

Email address

garrett.g.gruss+1@gmail.com

Canonical user ID

1ce99383dff16b44166404ccf7bd866cb905f12797bcd3bbb2bc12508cb1156

Multi-factor authentication (MFA) (1)

Remove

Resync

Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
<input type="radio"/> Virtual	arn:aws:iam::349577273469:mfa/phone	Not Applicable	Wed Sep 03 2025

Figure 2: Exercise 6.1

garrett-gruss-admin

Info

Delete

Summary

ARN

arn:aws:iam::349577273469:user/garrett-gruss-admin

Created

January 30, 2026, 10:50 (UTC-06:00)

Console access

Enabled without MFA

Last console sign-in

Never

Access key 1

Create access key

Permissions

Groups (1)

Tags

Security credentials

Last Accessed

Permissions policies (3)

Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type

All types

< 1 >

Policy name	Type	Attached via
<input type="checkbox"/> admin	Customer managed	Group Admin
<input type="checkbox"/> AmazonS3FullAccess	AWS managed	Group Admin
<input type="checkbox"/> IAMUserChangePassword	AWS managed	Directly

Figure 3: Exercise 6.2 (1)

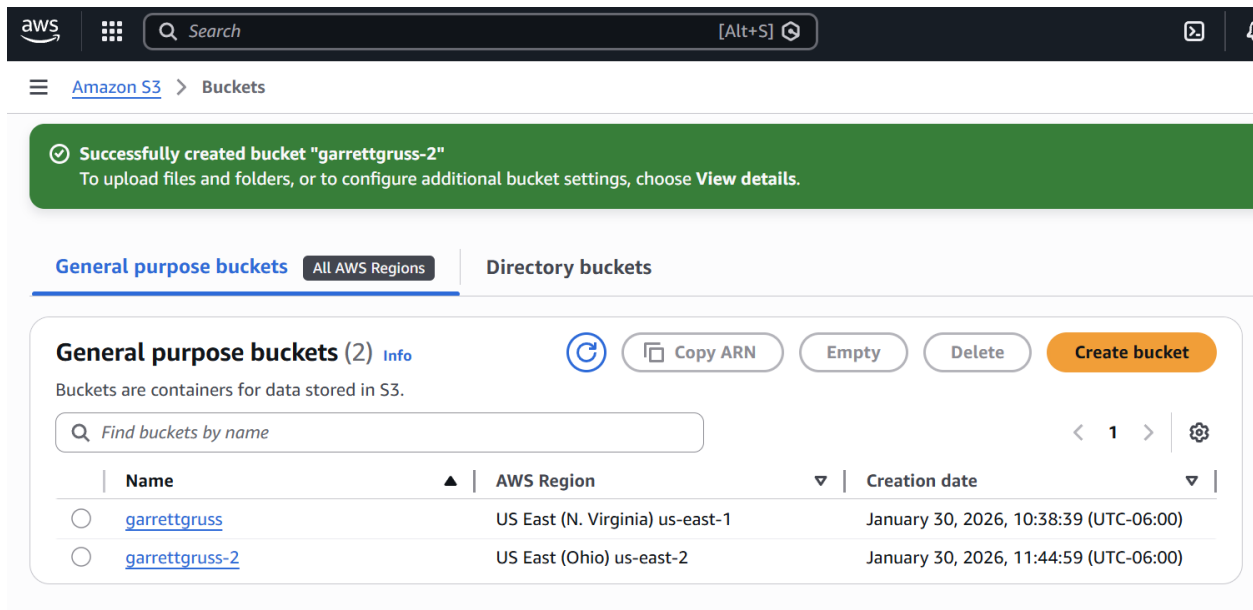


Figure 4: Exercise 6.2 (2)

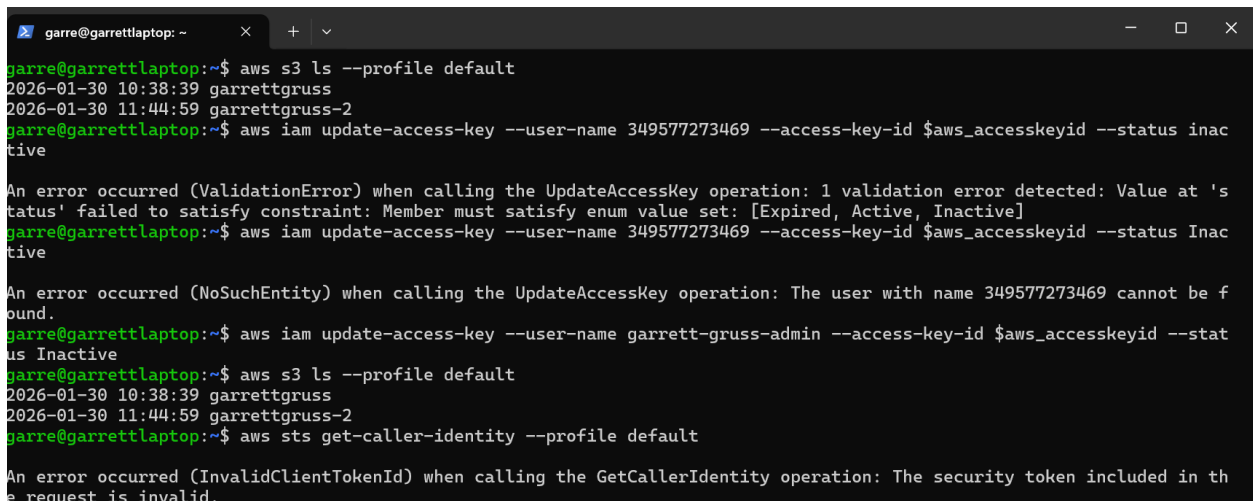


Figure 5: Exercise 6.3

exercise-6.4

Info

Delete

Summary

Edit


User group name

exercise-6.4

Creation time

January 30, 2026, 12:11 (UTC-06:00)

ARN


 arn:aws:iam::349577273469:group/exercise-6.4

Users (2)

Permissions


Access Advisor

Users in this group (2)

 Remove Add users

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Q Search

< 1 > 





<input type="checkbox"/>	User name 	 Groups	Last activity 	Creation time 
<input type="checkbox"/>	<a href="#">test1</a>	1	None	Now
<input type="checkbox"/>	<a href="#">test2</a>		None	Now

Figure 6: Exercise 6.4