

Cloud Computing Lab 2

BTI – CE	Aadee Sawarkar
Year 6 / Semester 11	26/07/2025
C2 / C117	27/07/2025

Q – Lab 2

(Module 3 on AWS academy)

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Results:

Module 3 Knowledge Check
Assignments

Jul 27 at
4:34pm

100 / 100



Guided Lab: Exploring AWS Identity and Access
Management (IAM)
Lab Assignments

Jul 27 at
4:19pm

56 / 56



Permissions given to users:

The image shows two side-by-side screenshots. The left screenshot is from a web browser displaying the 'Submission Details' page for a guided lab titled 'Guided Lab: Exploring AWS Identity and Access Management (IAM)'. The page shows a grade of 56 / 56 and a submission time of Jul 27 at 4:19pm. Below the submission details, there is a section titled 'AWS service restrictions' and another titled 'Accessing the AWS Management Console' with a list of instructions. The right screenshot is from the AWS IAM console, showing the 'Permissions' tab for a user named 'user-1'. It displays a list of 'Permissions policies (1)' with a table showing policy names and types. The table has columns for 'Policy name', 'Type', and 'Attached to'. The first policy listed is 'AmazonS3ReadOnlyAccess' with a type of 'AWS managed'. Below the table, there is a section for 'Permissions boundary (not set)' and a 'Generate policy based on CloudTrail events' section.

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Grade: 56 / 56

Submitted Jul 27 at 4:19pm

Start Lab

End Lab

AWS Details

Details

Submit

Submission Report

Grades

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

- At the top of these instructions, choose **Start Lab**.
 - The lab session starts.
 - A timer displays at the top of the page and shows the

user-2 | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details...

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

Permissions

Groups (1)

Tags (1)

Security credentials

Permissions policies (1)

Remove

Add permissions

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

Search

Filter by Type

All types

Policy name	Type	Att...
AmazonEC2ReadOnlyAccess	AWS managed	Gro...

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Generate policy

No requests to generate a policy in the past 7 days.

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Grade: 56 / 56

Submitted Jul 27 at 4:19pm

Start Lab

End Lab

AWS Details

Details

Submit

Submission Report

Grades

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

- At the top of these instructions, choose **Start Lab**.
 - The lab session starts.
 - A timer displays at the top of the page and shows the

user-3 | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details...

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

Permissions

Groups (1)

Tags (1)

Security credentials

Permissions policies (1)

Remove

Add permissions

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

Search

Filter by Type

All types

Policy name	Type	Attach...
EC2-Admin-Policy	Customer inline	Group ...

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Generate policy

No requests to generate a policy in the past 7 days.

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Grade: 56 / 56

AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm

AWS

03:00

Start Lab

End Lab

AWS Details

Details

Submit

Submission Report

Grades

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

- At the top of these instructions, choose **Start Lab**.
 - The lab session starts.
 - A timer displays at the top of the page and shows the

User groups | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

User groups (3)

Info

Delete

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

Group name	Users	Permissions
EC2-Admin	1	Defined
EC2-Support	1	Defined
S3-Support	1	Defined

more

AWS Account

Account ID

495228125192

Account Alias

Sign-in URL copied

Sign-in URL for IAM users in this account

https://495228125192.signin.aws.amazon.com/console

Tools

Relay simulator

Logged In with User 1

The screenshot shows two browser windows. The left window displays the 'Submission Details' page for a guided lab titled 'Exploring AWS Identity and Access Management (IAM)'. It shows the user 'user-1' with password 'Lab-Password1' and a list of instructions. The right window shows the AWS IAM console 'Buckets' page for the user 'user-1'. It displays a list of buckets, including 'c171385a4446362111028301t1w495228125192-s3bucket-xuif4aw2j20k', and a table of objects (currently empty).

Submission Details
Grade: 56 / 56
Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm

Instructions:

37. Sign in with the following credentials:
 - IAM user name: user-1
 - Password: Lab-Password1
38. Choose the **Services** menu, and choose **S3**. You can also use the search bar to find and choose **S3**.
39. Choose the name of one of your buckets, and browse the contents.
Because this user is part of the **S3-Support** group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.
Now, test whether the user has access to Amazon EC2.
40. Choose the **Services** menu, and choose **EC2**. You can also use the search bar to find and choose **EC2**.
41. In the left navigation pane, choose **Instances**.
You cannot see any instances. Instead, an error message says you are not authorized to perform this operation. This

Amazon S3 Buckets
c171385a4446362111028301t1w495228125192-s3bucket-xuif4aw2j20k
Objects (0)
No objects
You don't have any objects in this bucket.

The screenshot shows two browser windows. The left window displays the 'Submission Details' page for a guided lab titled 'Exploring AWS Identity and Access Management (IAM)'. It shows the user 'user-1' with password 'Lab-Password1' and a list of instructions. The right window shows the AWS IAM console 'Instances' page for the user 'user-1'. It displays a list of instances (currently empty) and a table of instances (currently empty). A red box highlights an error message: 'You are not authorized to perform this operation. User: arn:aws:iam::495228125192:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action'.

Submission Details
Grade: 56 / 56
Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm

Instructions:

37. Sign in with the following credentials:
 - IAM user name: user-1
 - Password: Lab-Password1
38. Choose the **Services** menu, and choose **S3**. You can also use the search bar to find and choose **S3**.
39. Choose the name of one of your buckets, and browse the contents.
Because this user is part of the **S3-Support** group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.
Now, test whether the user has access to Amazon EC2.
40. Choose the **Services** menu, and choose **EC2**. You can also use the search bar to find and choose **EC2**.
41. In the left navigation pane, choose **Instances**.
You cannot see any instances. Instead, an error message says you are not authorized to perform this operation. This

Amazon EC2 Instances
You are not authorized to perform this operation. User: arn:aws:iam::495228125192:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action
Retry Diagnose with Amazon Q
Select an instance

Logged In with User 2

The screenshot shows two browser windows. The left window is the AWS Academy lab 'Exploring AWS Identity and Access Management (IAM)' with a submission grade of 56/56. The right window is the AWS console 'Instance details' for EC2 instance i-09baec15abcfe8f66 in us-east-1. The instance is in a 'Running' state. The console shows various details including Instance ID, Private IP4 addresses, Instance state, Hostname type, Instance type, Auto-assigned IP address, and AWS Compute Optimizer finding. The IAM Role is also visible.

Submission Details
Grade: 56 / 56

Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm

02:52 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Details ✕

Submit Submission Report Grades

◦ If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, **N. Virginia**).

47. Select the EC2 instance.

48. Choose the **Instance state** menu, and then choose **Stop instance**.

49. To confirm that you want to stop the instance, choose **Stop**.

An error message appears and says that *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information without making changes.

Next, check whether *user-2* can access Amazon S3.

50. Choose the **Services** menu, and choose **S3**. You can also use the search bar to find and choose **S3**.

Instance details | EC2 | us-east-1

EC2 Dashboard EC2 Global View Events

Instances
Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations

Images
AMIs AMI Catalog

Elastic Block Store
Volumes Snapshots Lifecycle Manager

Network & Security
Security Groups Elastic IPs

Instance summary for i-09baec15abcfe8f66
Updated less than a minute ago

Instance ID
i-09baec15abcfe8f66

Private IP4 addresses
10.1.11.173

Instance state
Running

Hostname type
IP name: ip-10-1-11-173.ec2.internal

Instance type
t2.micro

Auto-assigned IP address
3.234.141.126 [Public IP]

AWS Compute Optimizer finding
User: arnaws:iam:495228125192:user/spl66/user-2 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on r

Public IP4 address
3.234.141.126 | open address

IPv6 address
-

Public DNS
ec2-3-234-141-126.compute-1.amazonaws.com | open address

Private IP DNS name (IPv4 only)
ip-10-1-11-173.ec2.internal

Answer private resource DNS name
-

Elastic IP addresses
-

VPC ID
vpc-02cf1b232fb5d58f2 (Lab VPC) | open address

IAM Role
-

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows two browser windows. The left window is the AWS Academy lab 'Exploring AWS Identity and Access Management (IAM)' with a submission grade of 56/56. The right window is the AWS console 'S3 buckets' in eu-north-1. It shows a list of buckets with an 'Error Access Denied' message highlighted. The console also displays 'Account snapshot' and 'External access summary' sections.

Submission Details
Grade: 56 / 56

Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm

02:51 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Details ✕

Submit Submission Report Grades

Next, check whether *user-2* can access Amazon S3.

50. Choose the **Services** menu, and choose **S3**. You can also use the search bar to find and choose **S3**.

An error message says *You don't have permissions to list buckets* because *user-2* does not have permissions to use Amazon S3.

You will now sign-in as *user-3*, who was hired as your Amazon EC2 administrator.

51. First, sign out *user-2* from the console:

- In the upper-right corner of the page, choose **user-2**.
- Choose **Sign Out**.

Task 3.4: Test user-3 permissions

52. Paste the sign-in link into the private browser again, and press ENTER.

53. Sign in with the following credentials:

S3 buckets | S3 | eu-north-1

Amazon S3 Buckets

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (0) Info Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

1

Error Access Denied Diagnose with Amazon Q

Account snapshot Info View dashboard
Updated daily
Storage Lens provides visibility into storage usage and activity trends.

External access summary - new Info
Updated daily
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Logged In with User 3

The screenshot shows two side-by-side browser windows. The left window displays the 'Submission Details' for a lab titled 'Guided Lab: Exploring AWS Identity and Access Management (IAM)'. The lab instructions include steps 52 through 56, with step 56 being 'Select the EC2 instance.' The right window shows the AWS Management Console for the 'us-east-1' region, specifically the 'Instances' page. An EC2 instance with ID 'i-09baec15abcfe8f66' is selected. The instance is in the 'Running' state. A context menu is open over the 'Instance state' button, showing options: 'Start instance', 'Reboot instance', 'Hibernate instance', and 'Terminate (delete) instance'. The instance details on the right include: Instance ID 'i-09baec15abcfe8f66', Private IPv4 address '10.1.11.173', Instance state 'Running', Hostname type 'IP name: ip-10-1-11-173.ec2.internal', Instance type 't2.micro', Auto-assigned IP address '3.234.141.126 [Public IP]', AWS Compute Optimizer finding (warning icon), Public DNS 'ec2-3-234-141-126.compute-1.amazonaws.com', Private IP DNS name 'ip-10-1-11-173.ec2.internal', VPC ID 'vpc-02cf1b232fb5d58f2 (Lab VPC)', and IAM Role.

The screenshot shows the same two browser windows as the previous image, but with updated content. In the left window, the lab instructions now include steps 56 through 59. Step 57 is 'Choose the Instance state menu, and then choose Stop instance.' Step 58 is 'To confirm that you want to stop the instance, choose Stop.' Step 59 is 'Close your private browser window.' The right window shows the AWS Management Console with a green banner at the top stating 'Successfully initiated stopping of i-09baec15abcfe8f66'. The instance details for 'i-09baec15abcfe8f66' now show the 'Instance state' as 'Stopping'. The other details remain the same as in the previous image.