Cloud Computing Lab 2

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

Q – Lab 2

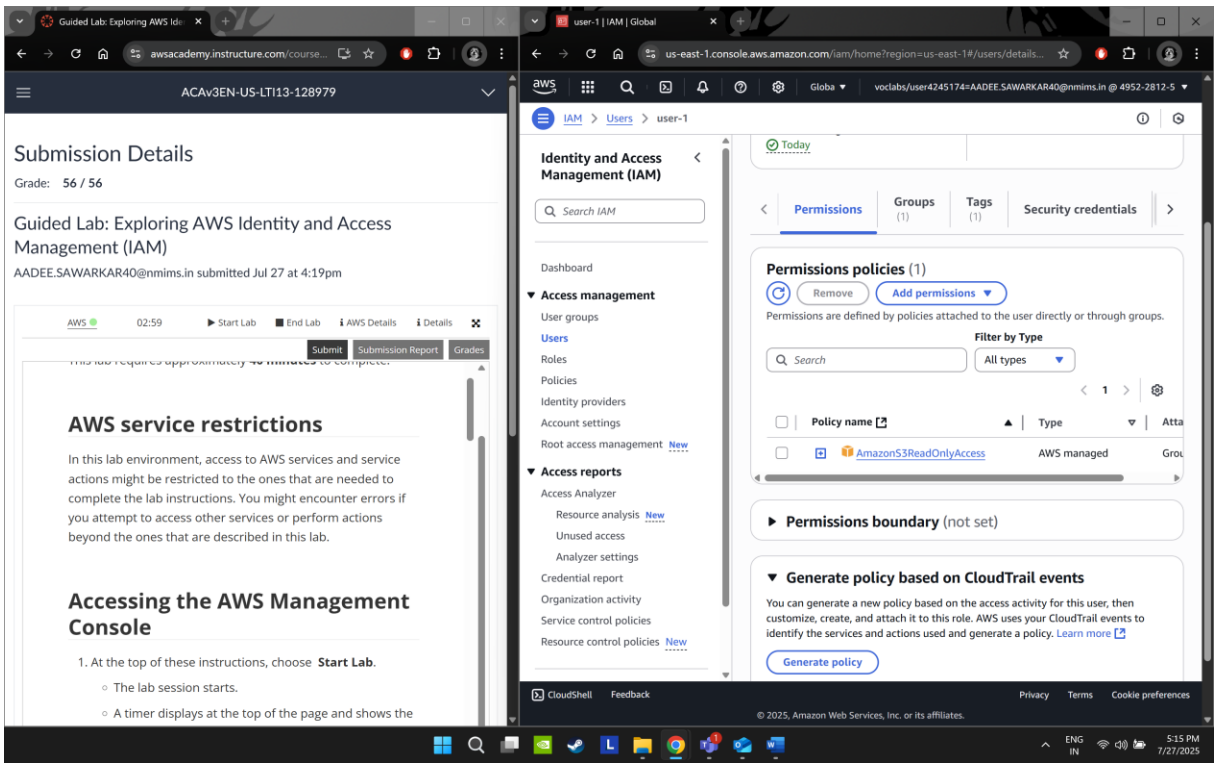
(Module 3 on AWS academy)

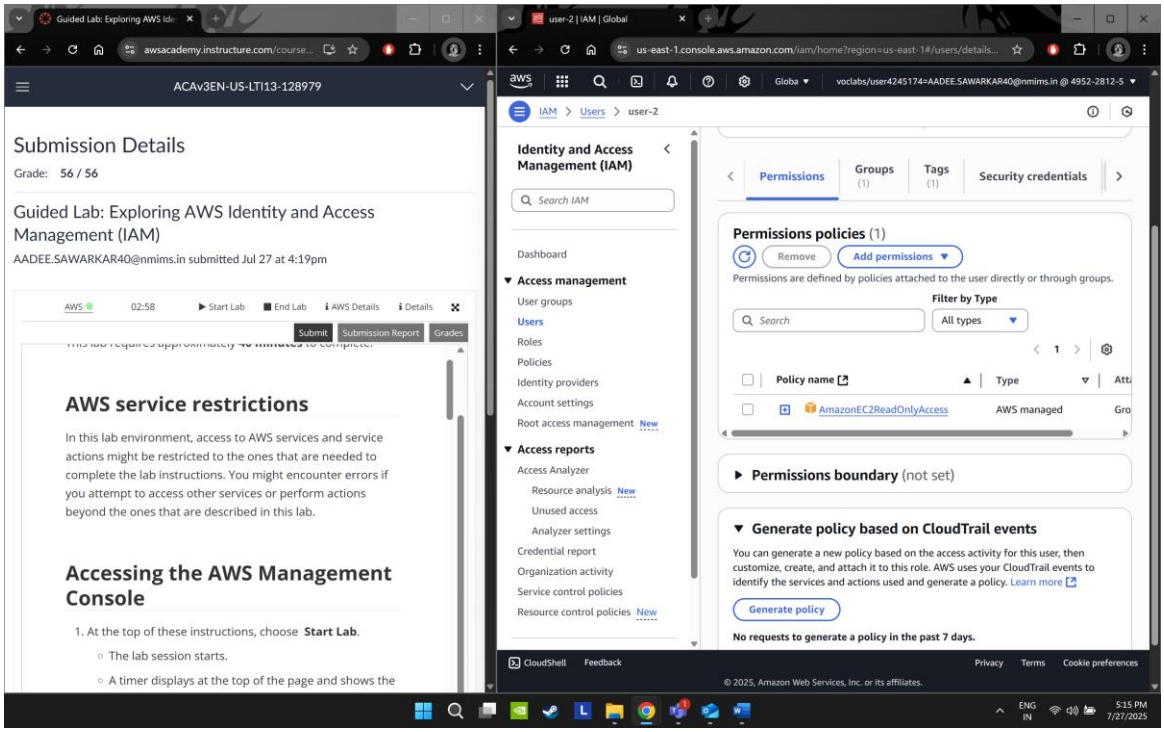
Guided Lab: Exploring AWS Identity and Access Management (IAM)

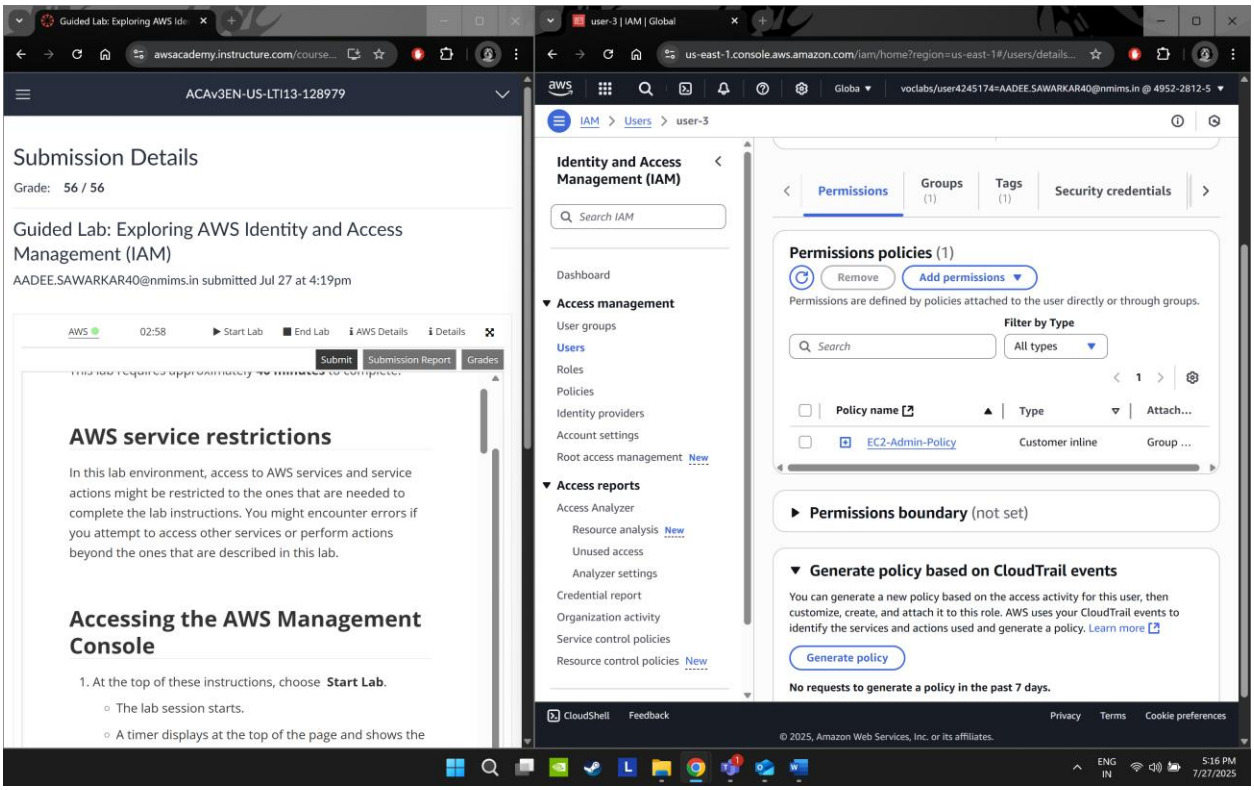
Results:

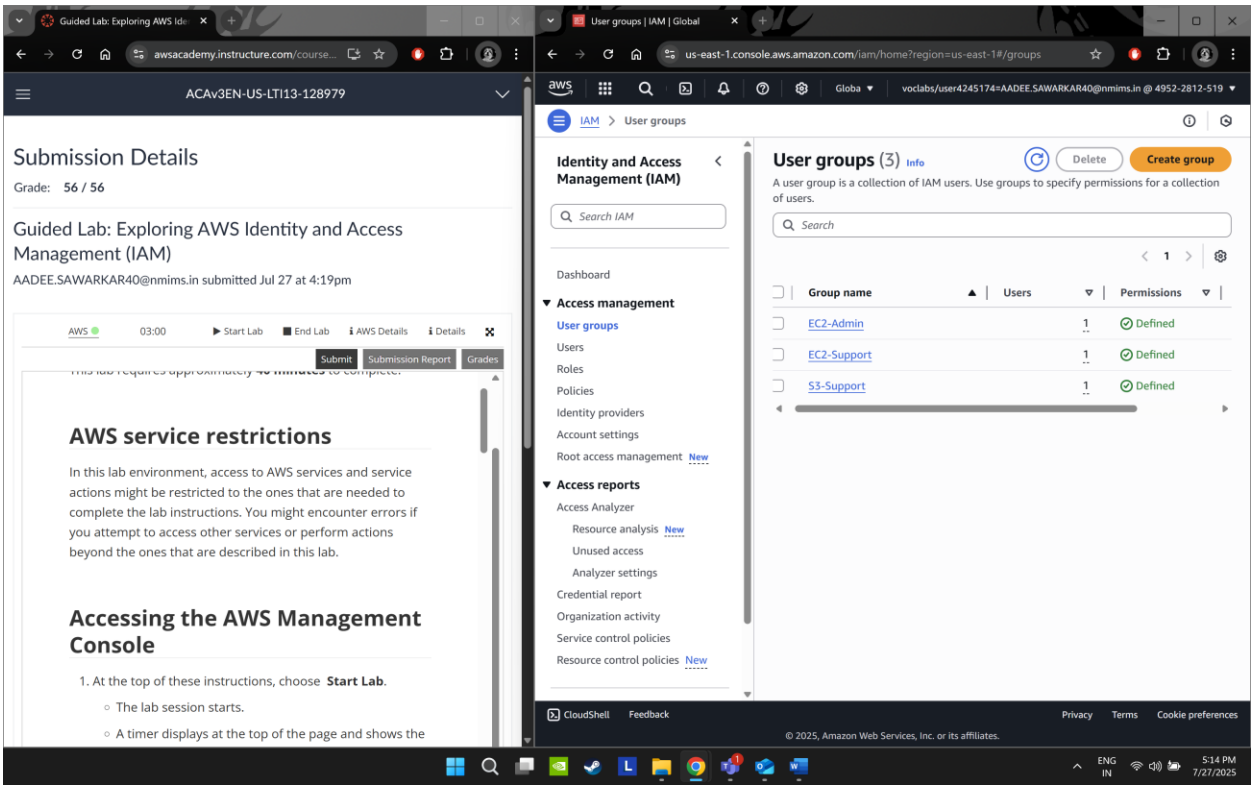
Module 3 Knowledge Check Assignments	Jul 27 at 4:34pm	100 / 100
Guided Lab: Exploring AWS Identity and Access Management (IAM) Lab Assignments	Jul 27 at 4:19pm	56 / 56

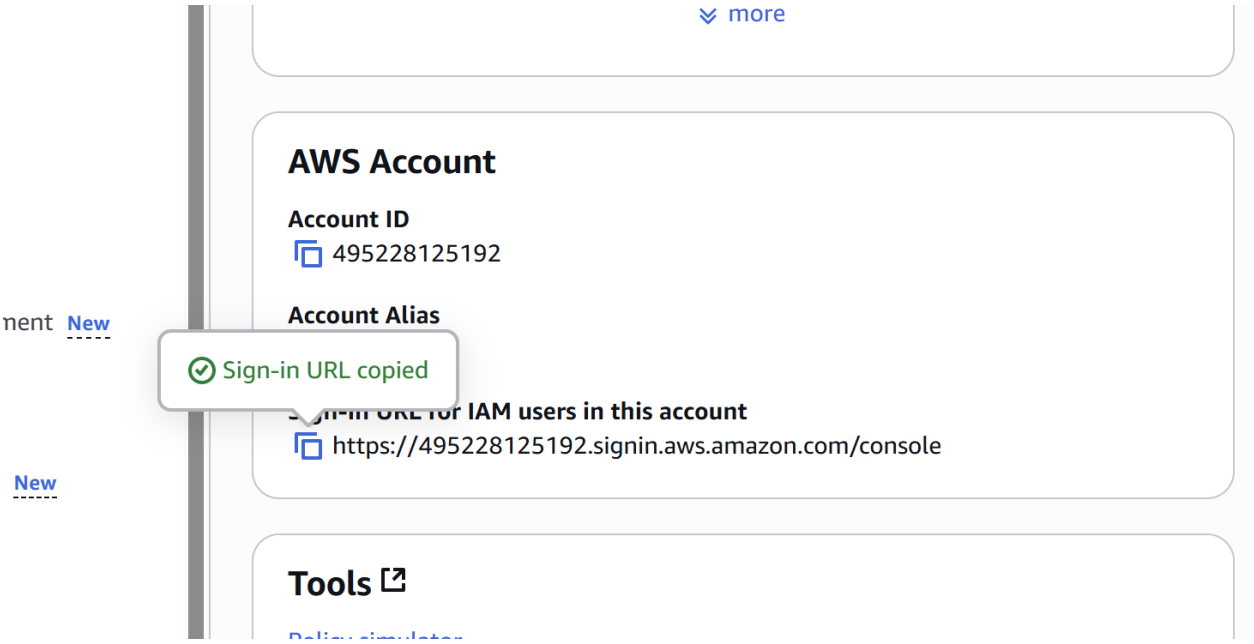
Permissions given to users:



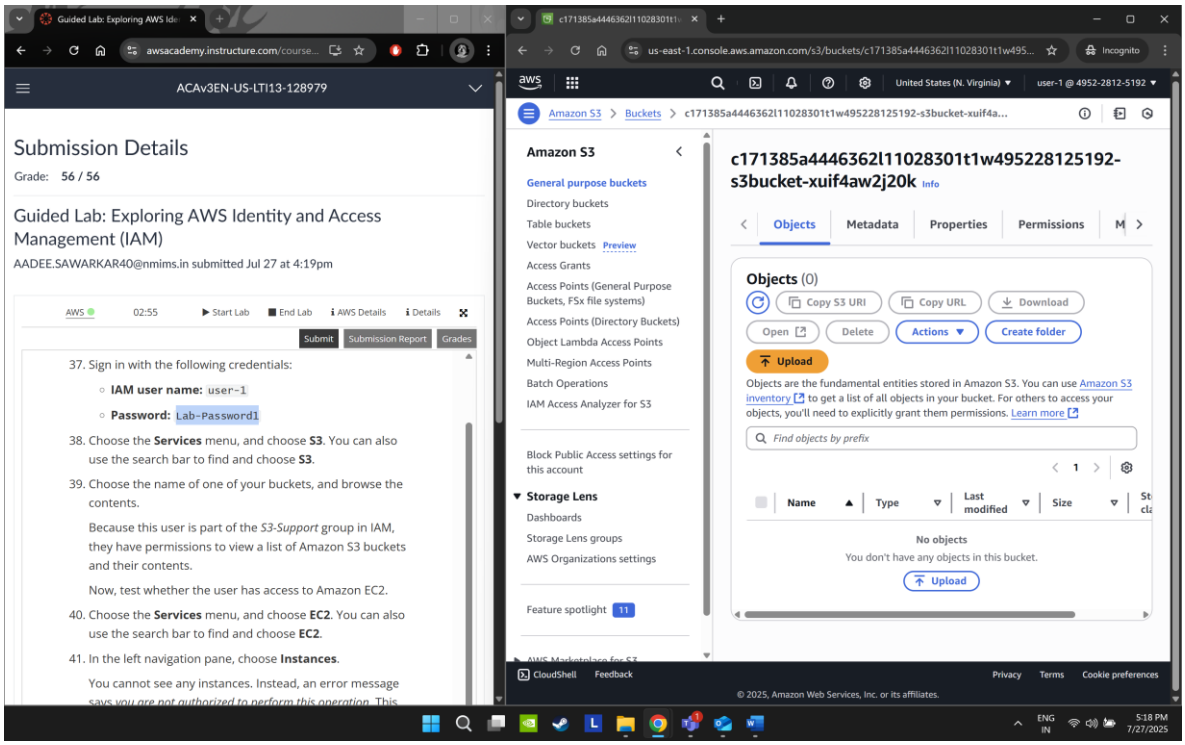

ACAv3EN-US-LTI13-128979
Submission Details
Grade: 56 / 56
Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm
AWS 02:58 Start Lab End Lab AWS Details Details
Submit Submission Report Grades
AWS service restrictions
In this lab environment, 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
1. 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
IAM > Users > user-2
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
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.
Filter by Type
Search
All types
Policy name
Type
AmazonEC2ReadOnlyAccess
AWS managed
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.
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
5:15 PM
7/27/2025

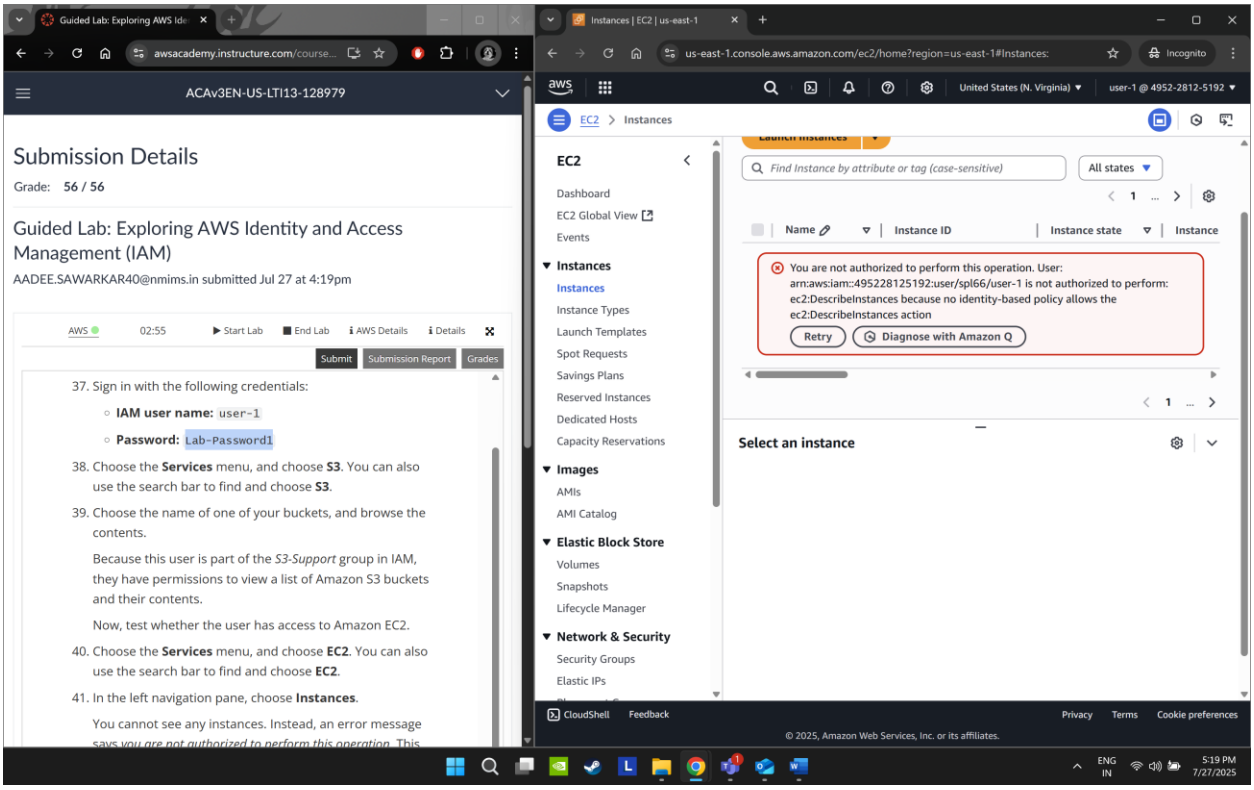

ACAv3EN-US-LTI13-128979
Submission Details
Grade: 56 / 56
Guided Lab: Exploring AWS Identity and Access Management (IAM)
AADEE.SAWARKAR40@nmims.in submitted Jul 27 at 4:19pm
AWS 02:58 Start Lab End Lab AWS Details Details
Submit Submission Report Grades
AWS service restrictions
In this lab environment, 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
1. 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
IAM > Users > user-3
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
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.
Filter by Type
Search
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.
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
5:16 PM
7/27/2025


ACAv3EN-US-LTI13-128979
Submission Details
Grade: 56 / 56
Guided Lab: Exploring AWS Identity and Access Management (IAM)
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
1. 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
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

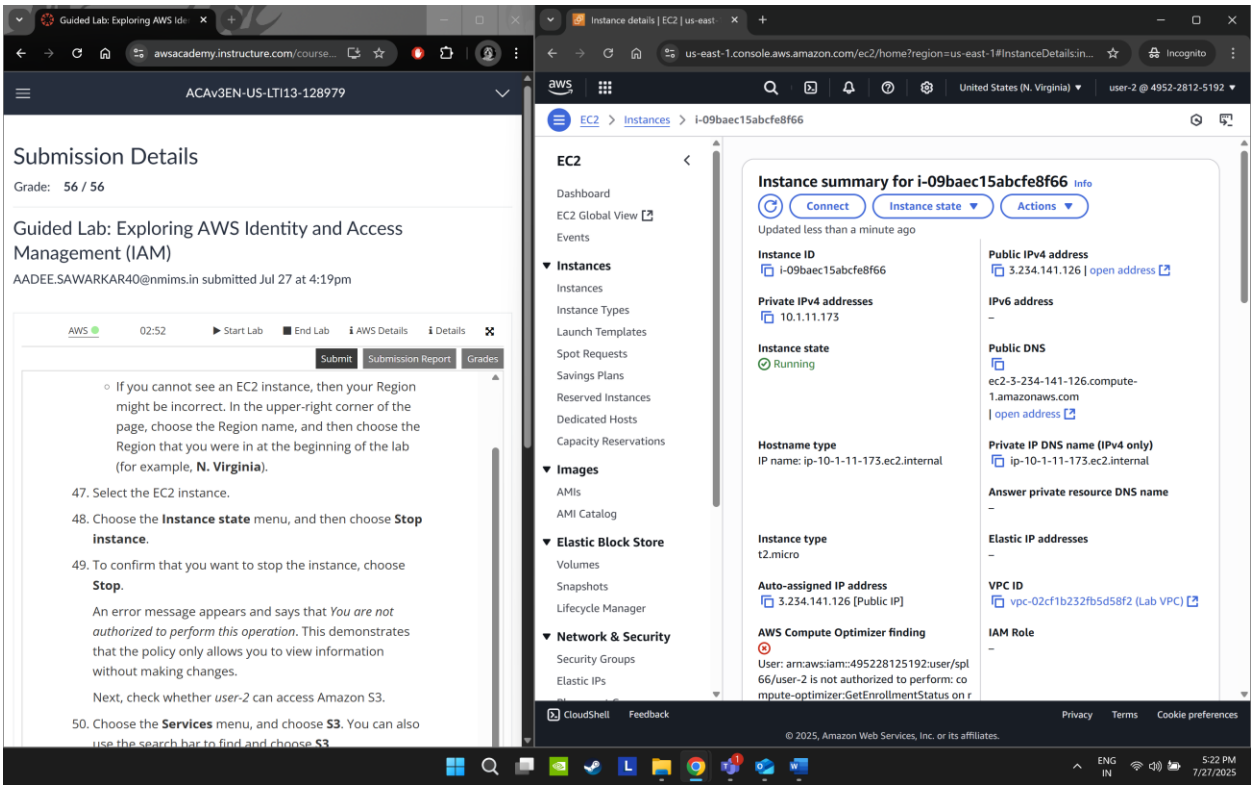

more
AWS Account
Account ID
495228125192
Account Alias
nent New
Sign-in URL copied
https://495228125192.signin.aws.amazon.com/console
New
Tools

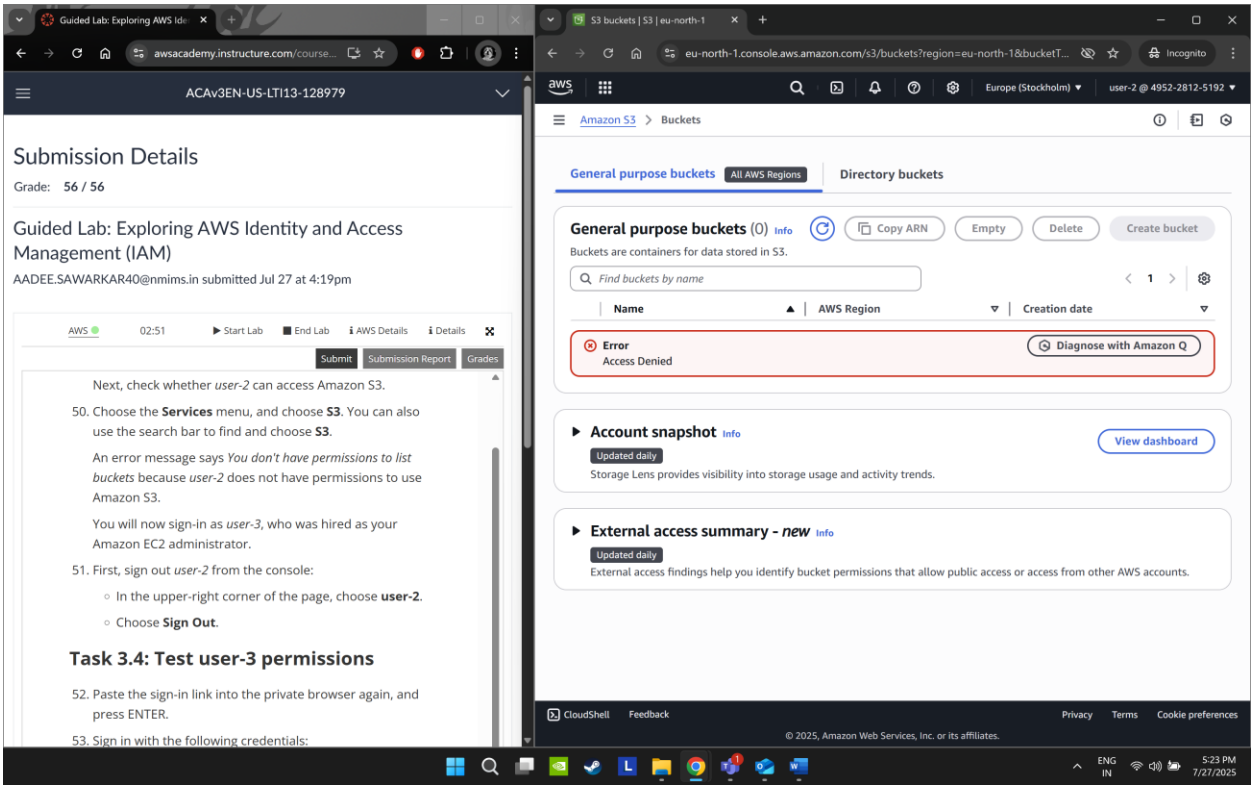
Logged In with User 1





Logged In with User 2





Logged In with User 3