Team Member

1-Moatasem Mohamed Abo Taleb

2-Mohamed Mahmoud Elteir

3-Mahmoud Ahmed Elsayed

4-Mohamed Farrag Abdelhady

Moatasem Mohamed Abo Taleb	**Project 8**
Mohamed Mahmoud Elteir	**Project 6**
Mahmoud Ahmed Elsayed	**Project 7**
Mohamed Farrag Abdelhady	**Presentation**

Project 6:

Exploring AWS Identity and Access Management (IAM)

Lab Overview In this lab, you will explore AWS Identity and Access Management (IAM) by managing users, groups, and policies within AWS. The objective is to understand how permissions are assigned and managed through IAM, allowing users to perform specific tasks based on their roles.

Task 1: Explore Users and Groups

- Log in to the AWS Management Console and navigate to IAM.
- List and explore pre-created IAM users and groups.
- Inspect the details and permissions associated with each user

Step 1: List of IAM Users

Step 2: List IAM Groups

```
PS C:\Users\moham> aws iam list-groups
{
    "Groups": [
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Admin",
            "GroupId": "AGPAWBDCU3PD3D3HD5CYH",
            "Arn": "arn:aws:iam::414671231943:group/spl66/EC2-Admin",
            "CreateDate": "2024-10-12T16:24:09+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Support",
            "GroupId": "AGPAWBDCU3PDYEFE2CCYG",
            "Arn": "arn:aws:iam::414671231943:group/spl66/EC2-Support",
            "CreateDate": "2024-10-12T16:24:08+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "S3-Support",
            "GroupId": "AGPAWBDCU3PDW3QINQ4V5",
            "Arn": "arn:aws:iam::414671231943:group/spl66/S3-Support",
            "CreateDate": "2024-10-12T16:24:08+00:00"
        }
    ]
}

PS C:\Users\moham>
```

Step 3: Inspect User Details and Permissions User 1 :

```
PS C:\Users\moham> aws iam get-user --user-name user-1
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDAWBDCU3PD5OIT4ZHZK",
        "Arn": "arn:aws:iam::414671231943:user/spl66/user-1",
        "CreateDate": "2024-10-12T16:24:08+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7580800t1w414671231943"
            }
        ]
    }
}

PS C:\Users\moham>
```

User 2 :

```
                aws iam get-user --user-name user-2
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDAWBDCU3PDZKKEZCAOG",
        "Arn": "arn:aws:iam::414671231943:user/spl66/user-2",
        "CreateDate": "2024-10-12T16:24:08+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7580800t1w414671231943"
            }
        ]
    }
}

PS C:\Users\moham>
```

User 3 :

```
PS C:\Users\moham> aws iam get-user --user-name user-3
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDAWBDCU3PDWL7GTWYAI",
        "Arn": "arn:aws:iam::414671231943:user/spl66/user-3",
        "CreateDate": "2024-10-12T16:24:08+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7580800t1w414671231943"
            }
        ]
    }
}

PS C:\Users\moham>
```

1 – EC2-Support

```
aws iam get-group --group-name EC2-Support

"Users": [],
"Group": {
    "Path": "/spl66/",
    "GroupName": "EC2-Support",
    "GroupId": "AGPAWBDCU3PDYEFE2CCYG",
    "Arn": "arn:aws:iam::414671231943:group/spl66/EC2-Support",
    "CreateDate": "2024-10-12T16:24:08+00:00"
}
```

2 – S3-Support

```
PS C:\Users\moham> aws iam get-group --group-name S3-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPAWBDCU3PDW3QINQ4V5",
        "Arn": "arn:aws:iam::414671231943:group/spl66/S3-Support",
        "CreateDate": "2024-10-12T16:24:08+00:00"
    }
}

PS C:\Users\moham>
```

3 – EC2-admin

```
PS C:\Users\moham> aws iam get-group --group-name EC2-Admin
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPAWBDCU3PD3D3HD5CYH",
        "Arn": "arn:aws:iam::414671231943:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-12T16:24:09+00:00"
    }
}

PS C:\Users\moham>
```

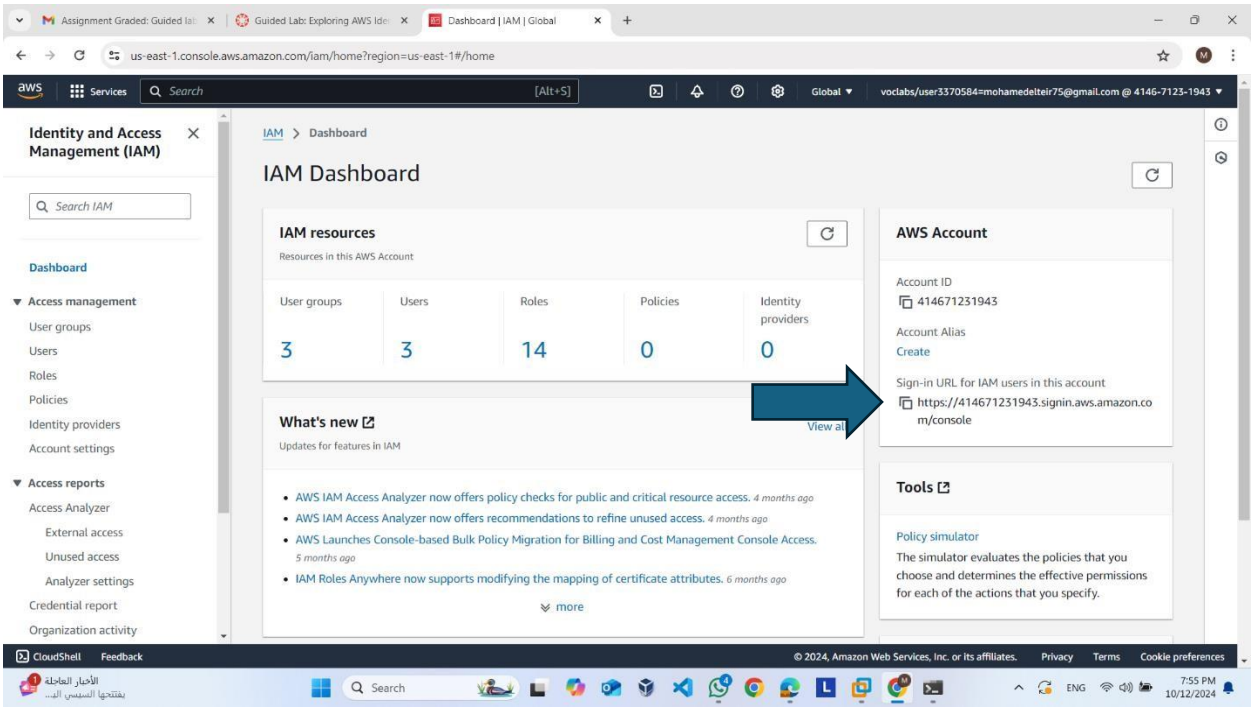
Step 4: Inspect Group Details and Permissions

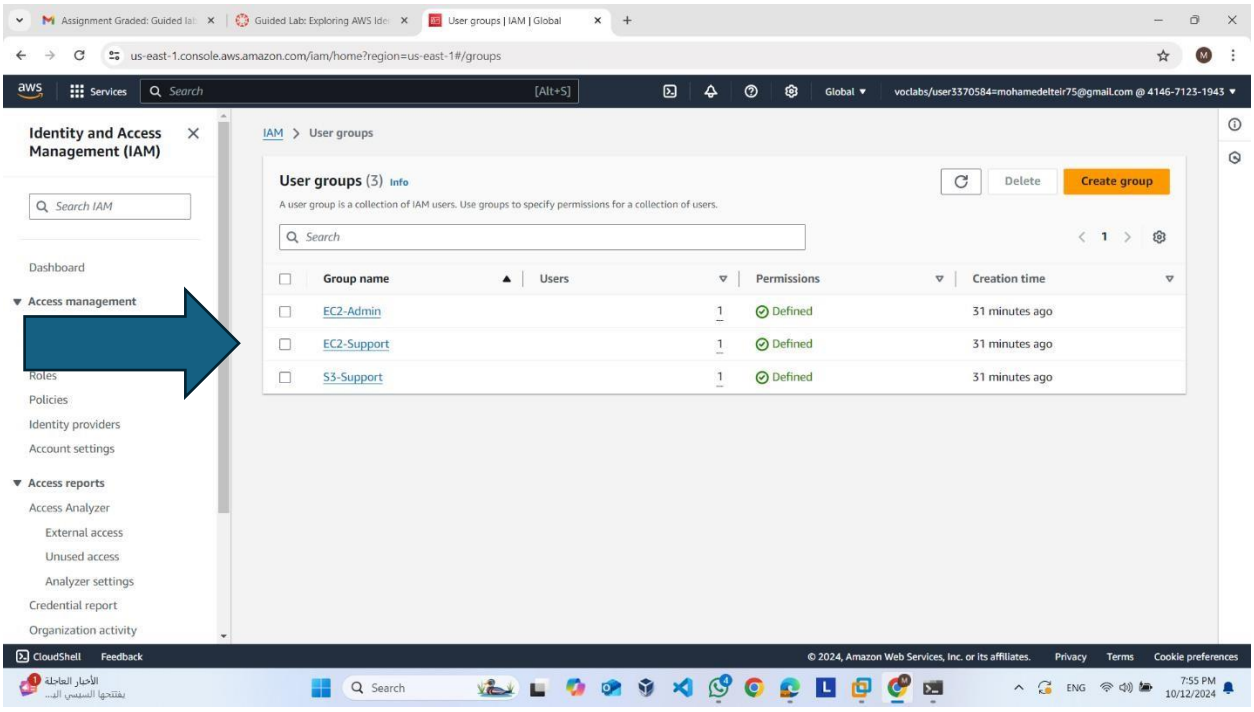
```
PS C:\Users\moham> aws iam list-attached-group-policies --group-name S3-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}

PS C:\Users\moham> aws iam list-attached-group-policies --group-name EC2-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}

PS C:\Users\moham> aws iam list-attached-group-policies --group-name EC2-Admin
{
    "AttachedPolicies": []
}
```

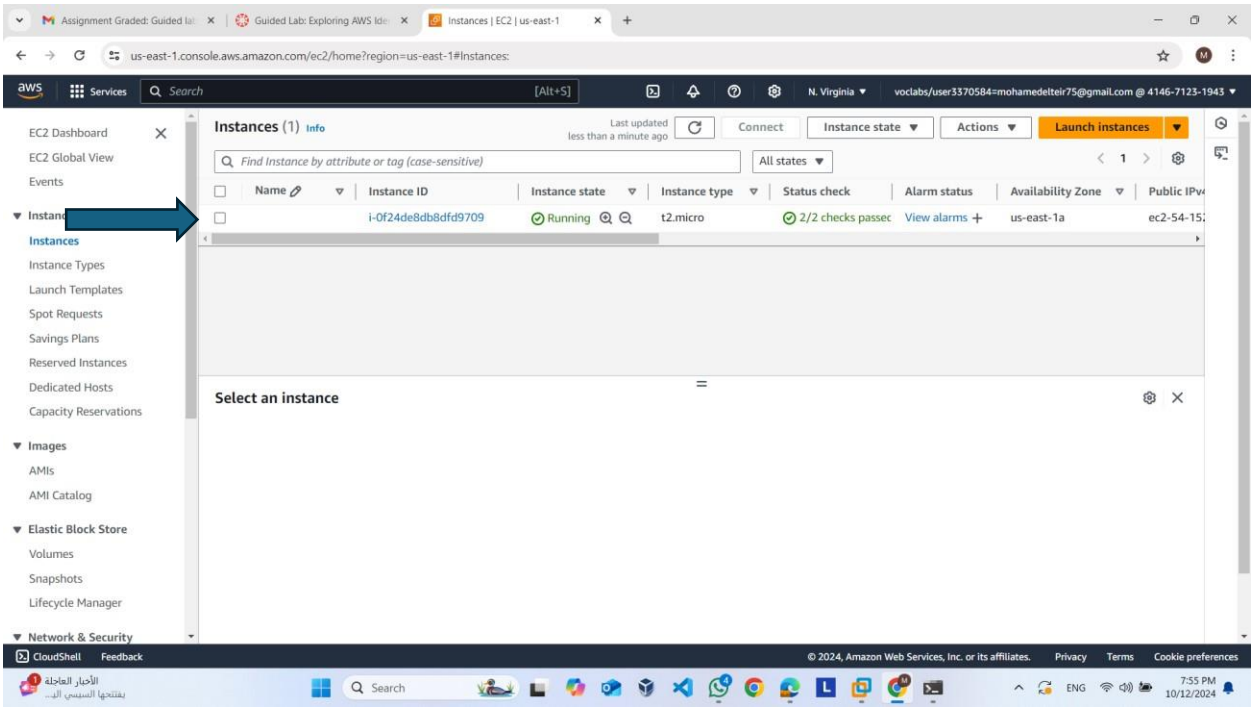
Step 5 : Get Policy Details

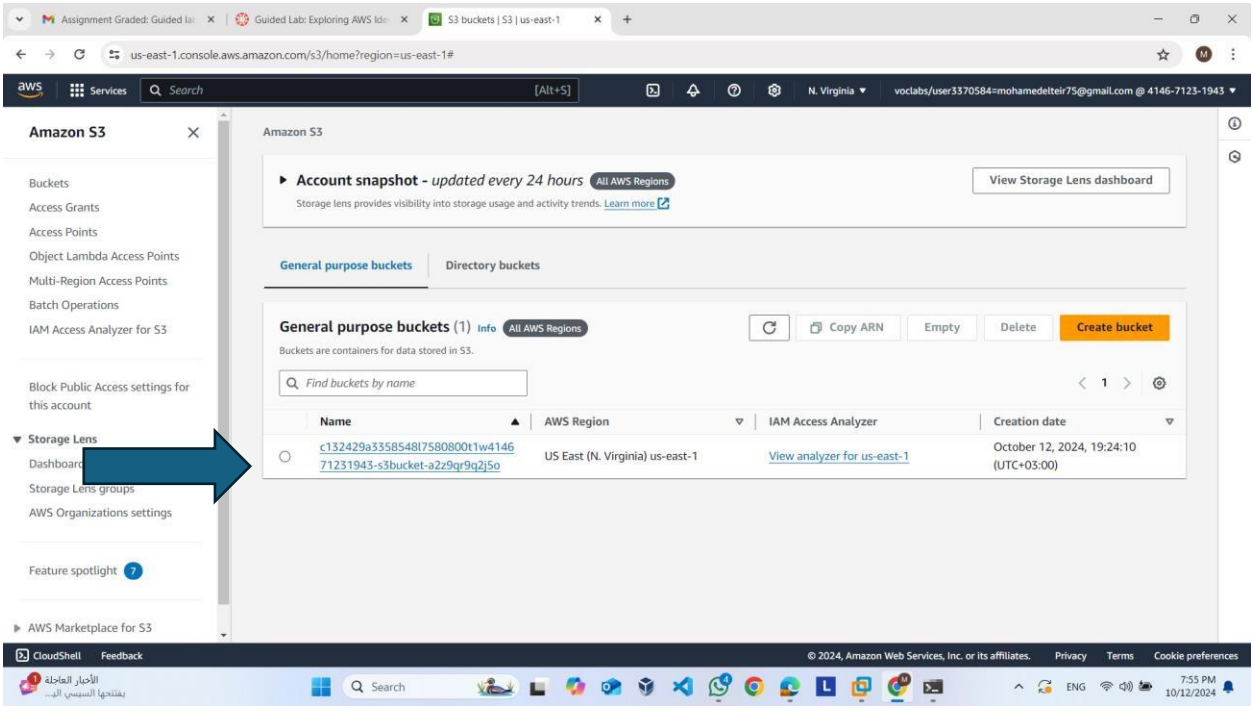
```
PS C:\Users\moham> aws iam get-policy --policy-arn arn:aws:ec2:us-east-1:414671231943:instance/i-0f24de8db8dfd9709

An error occurred (ValidationError) when calling the GetPolicy operation: Invalid serviceaws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2Re
adOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}

PS C:\Users\moham> aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}
```

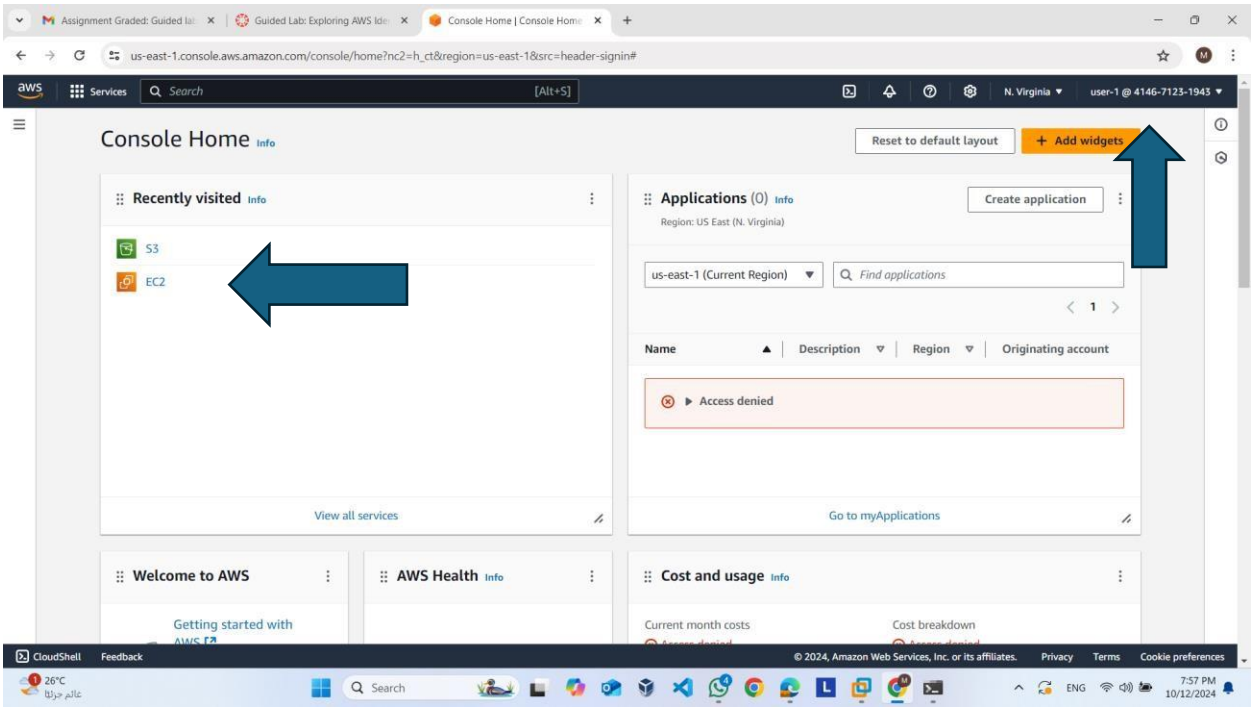

```
PS C:\Users\moham> aws iam get-policy --policy-arn arn:aws:ec2:us-east-1:414671231943:instance/i-0f24de8db8dfd9709

An error occurred (ValidationError) when calling the GetPolicy operation: Invalid serviceaws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2Re
adOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}

PS C:\Users\moham> aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}
```

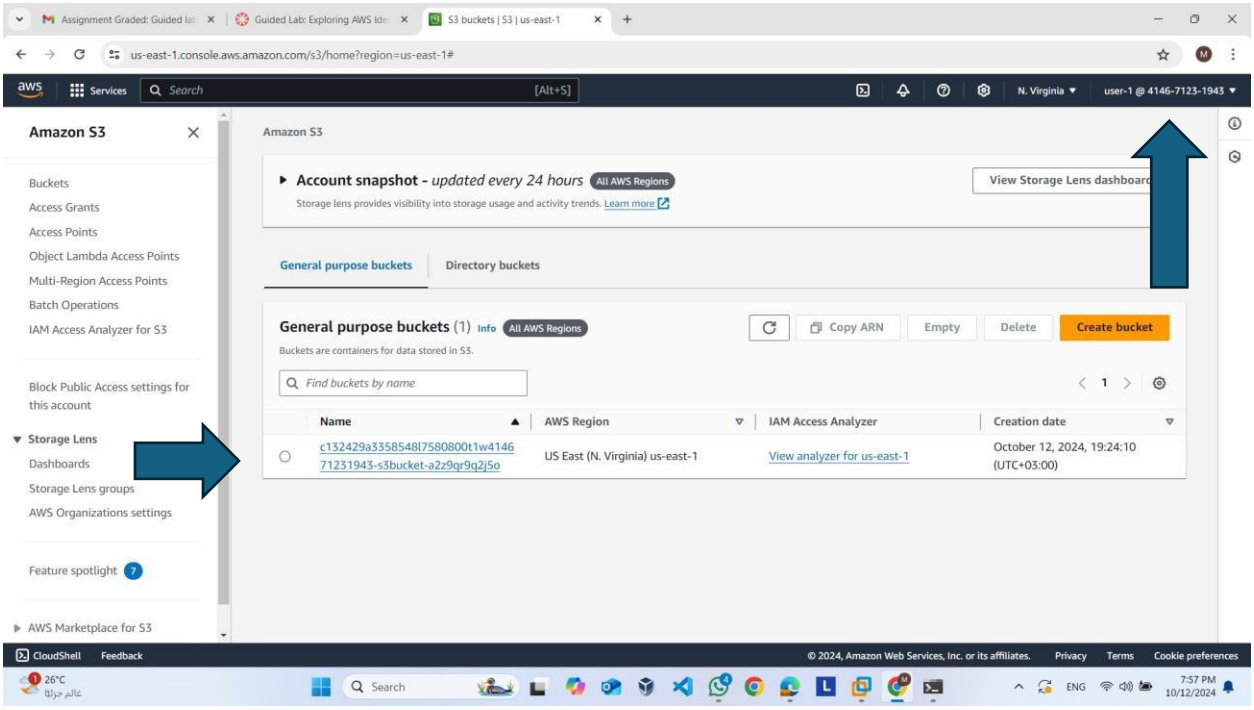

Assignment Graded: Guided lab
Guided Lab: Exploring AWS Ide
Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
Services
Search
[Alt+S]
Global
voclabs/user3370584=mohamedelteir75@gmail.com @ 4146-7123-1943
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Dashboard
IAM Dashboard
IAM resources
Resources in this AWS Account
User groups
Users
Roles
Policies
Identity providers
3
3
14
0
0
What's new
Updates for features in IAM
View all
AWS IAM Access Analyzer now offers policy checks for public and critical resource access. 4 months ago
AWS IAM Access Analyzer now offers recommendations to refine unused access. 4 months ago
AWS Launches Console-based Bulk Policy Migration for Billing and Cost Management Console Access. 5 months ago
IAM Roles Anywhere now supports modifying the mapping of certificate attributes. 6 months ago
more
AWS Account
Account ID
414671231943
Account Alias
Create
Sign-in URL for IAM users in this account
https://414671231943.signin.aws.amazon.com/console
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
7:55 PM
10/12/2024

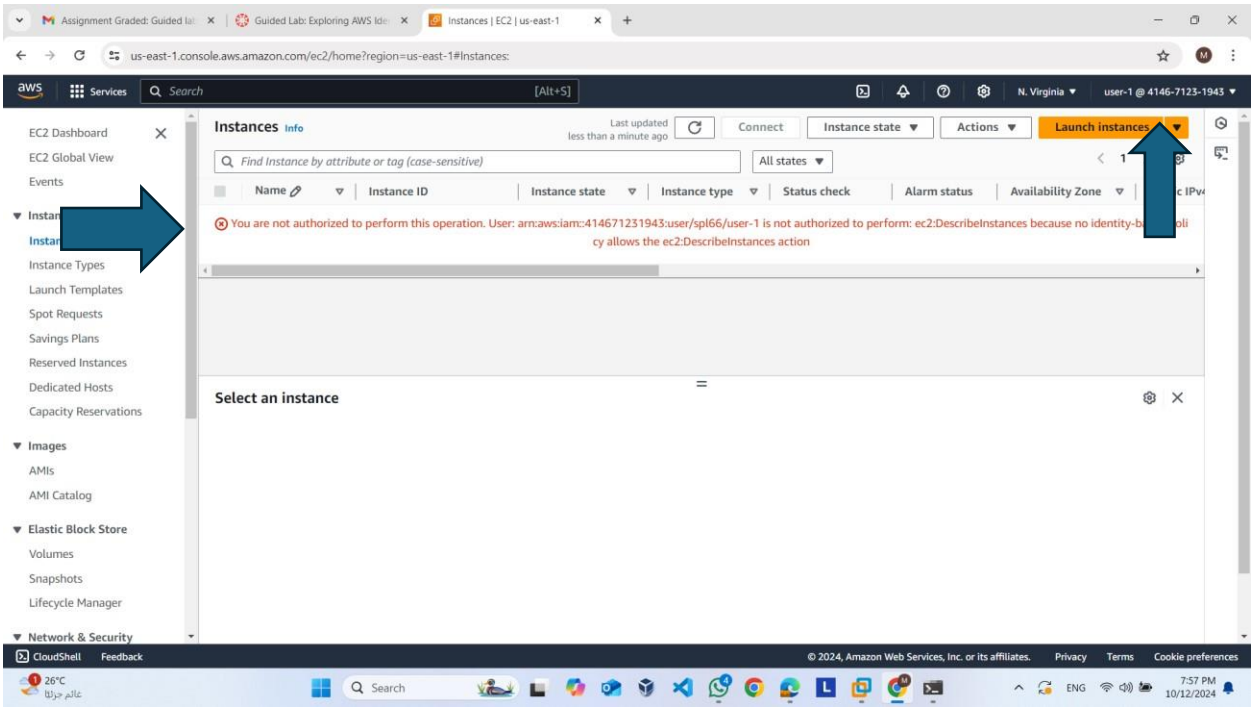

Assignment Graded: Guided lab
Guided Lab: Exploring AWS Ide
User groups | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups
Services
Search
[Alt+S]
Global
voclabs/user3370584=mohamedelteir75@gmail.com @ 4146-7123-1943
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > User groups
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
EC2-Admin
1
Defined
31 minutes ago
EC2-Support
1
Defined
31 minutes ago
S3-Support
1
Defined
31 minutes ago
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
7:55 PM
10/12/2024

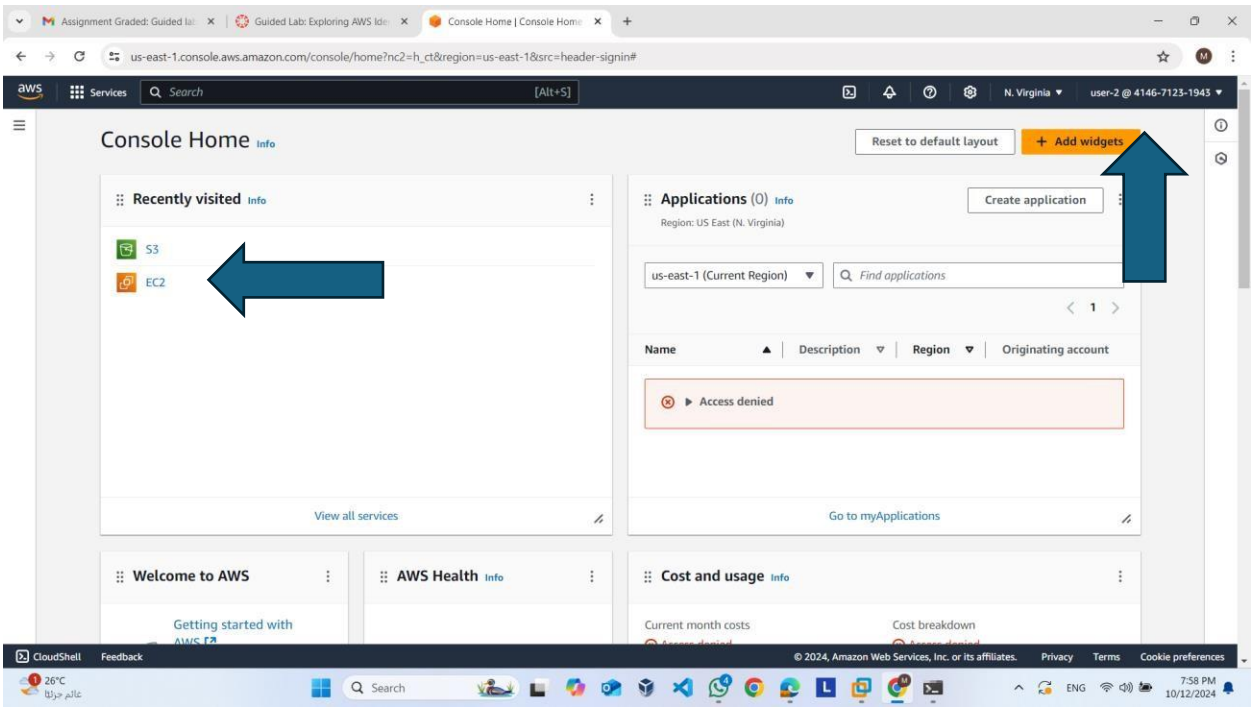

Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
voclabs/user3370584=mohamedelteir75@gmail.com @ 4146-7123-1943
EC2 Dashboard
EC2 Global View
Events
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
i-0f24de8db8dfd9709
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
7:55 PM
10/12/2024

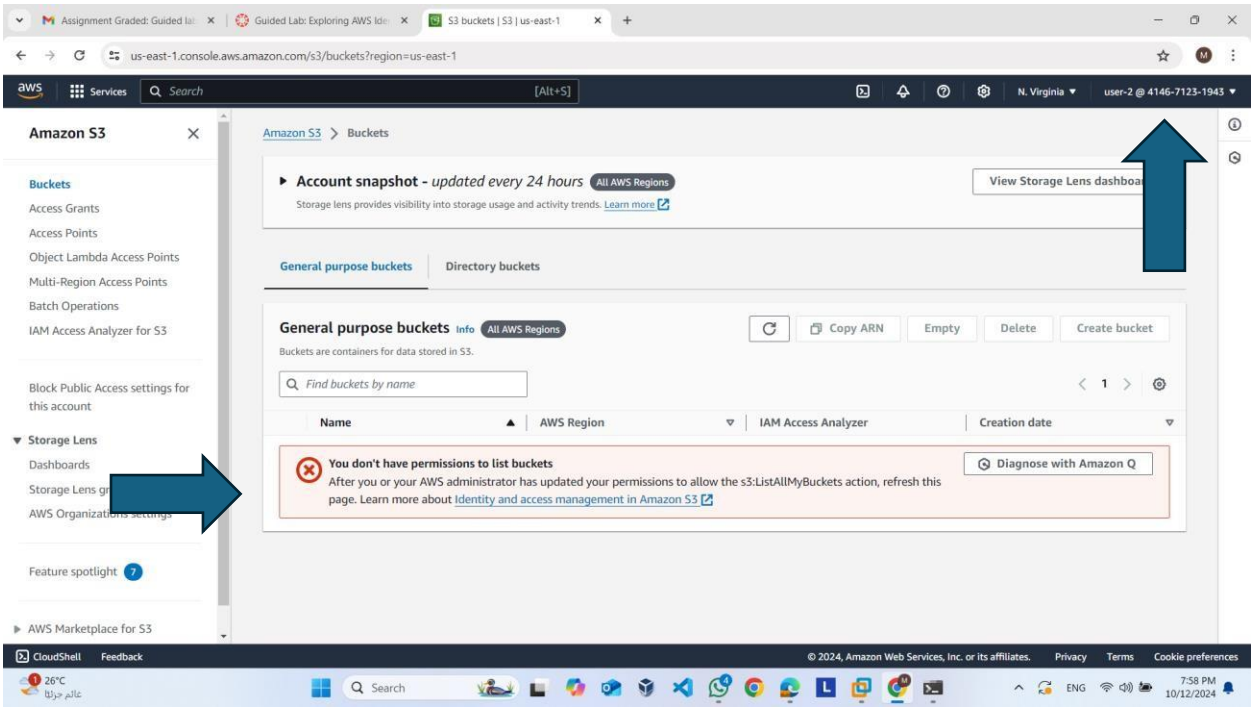

S3 buckets | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/home?region=us-east-1#
Services
Search
[Alt+S]
N. Virginia
voclabs/user3370584=mohamedelteir75@gmail.com @ 4146-7123-1943
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7580800t1w414671231943-s3bucket-a2z9qr9q2j5o
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 12, 2024, 19:24:10 (UTC+03:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
7:55 PM
10/12/2024

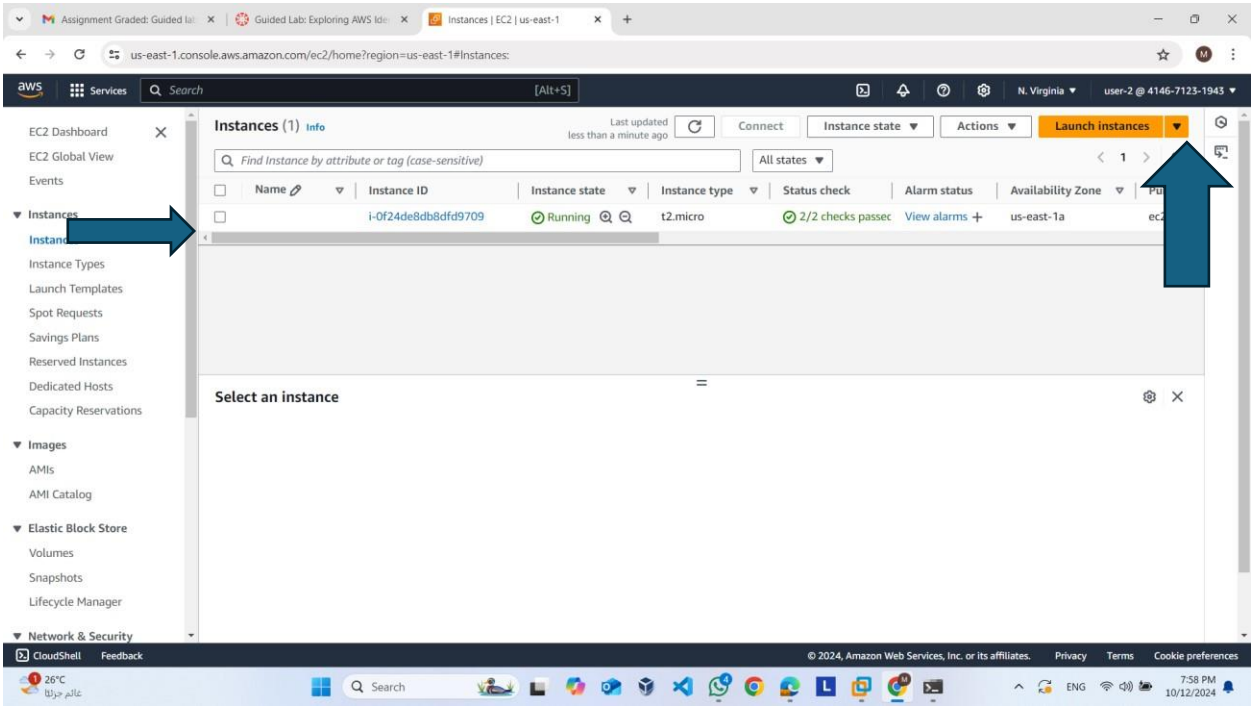

Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
S3
EC2
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
View all services
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
Current month costs
Cost breakdown
Getting started with AWS
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

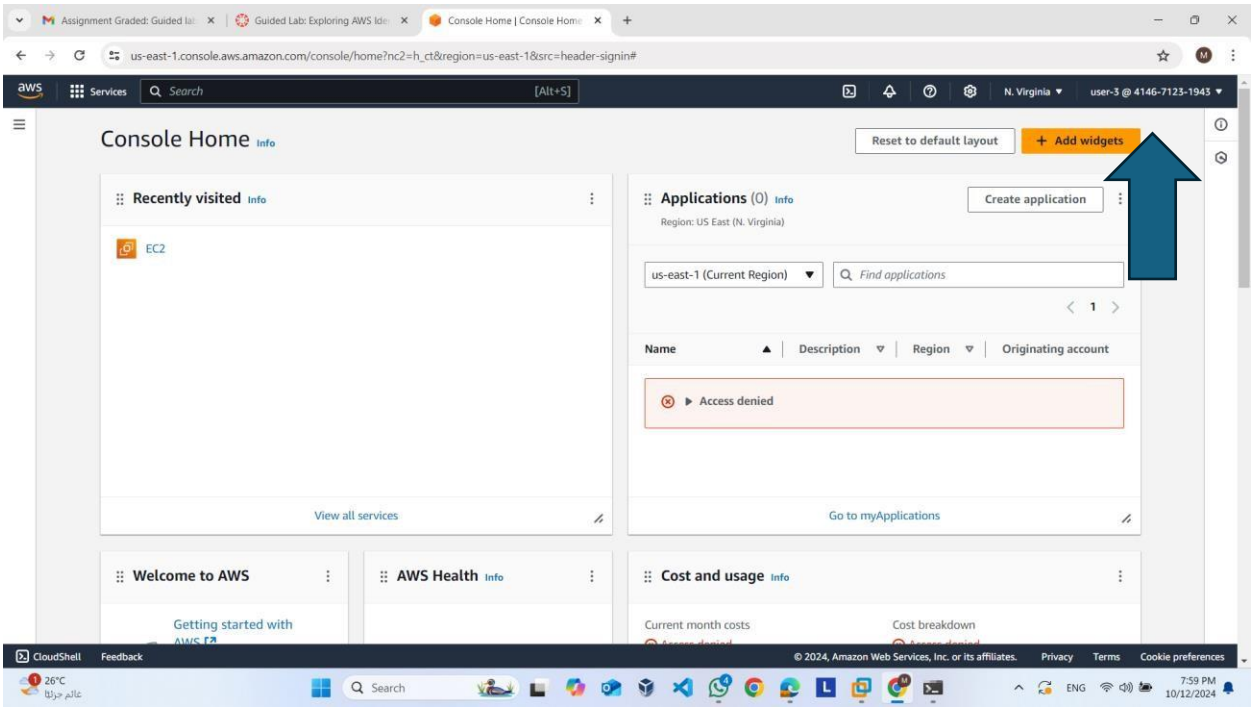

Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7580800t1w414671231943-s3bucket-a2z9qr9q2j5o
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 12, 2024, 19:24:10 (UTC+03:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

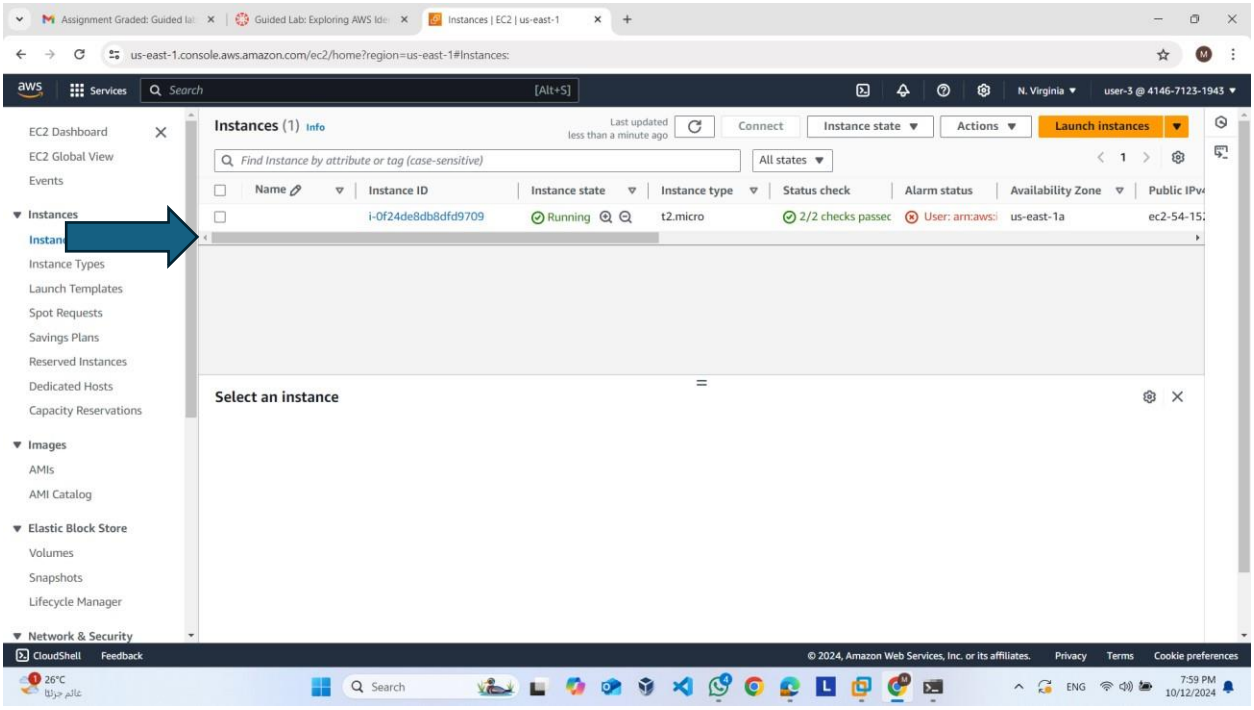

Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
user-1 @ 4146-7123-1943
EC2 Dashboard
EC2 Global View
Events
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instances Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
You are not authorized to perform this operation. User: arn:aws:iam::414671231943:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Search
ENG
7:57 PM
10/12/2024

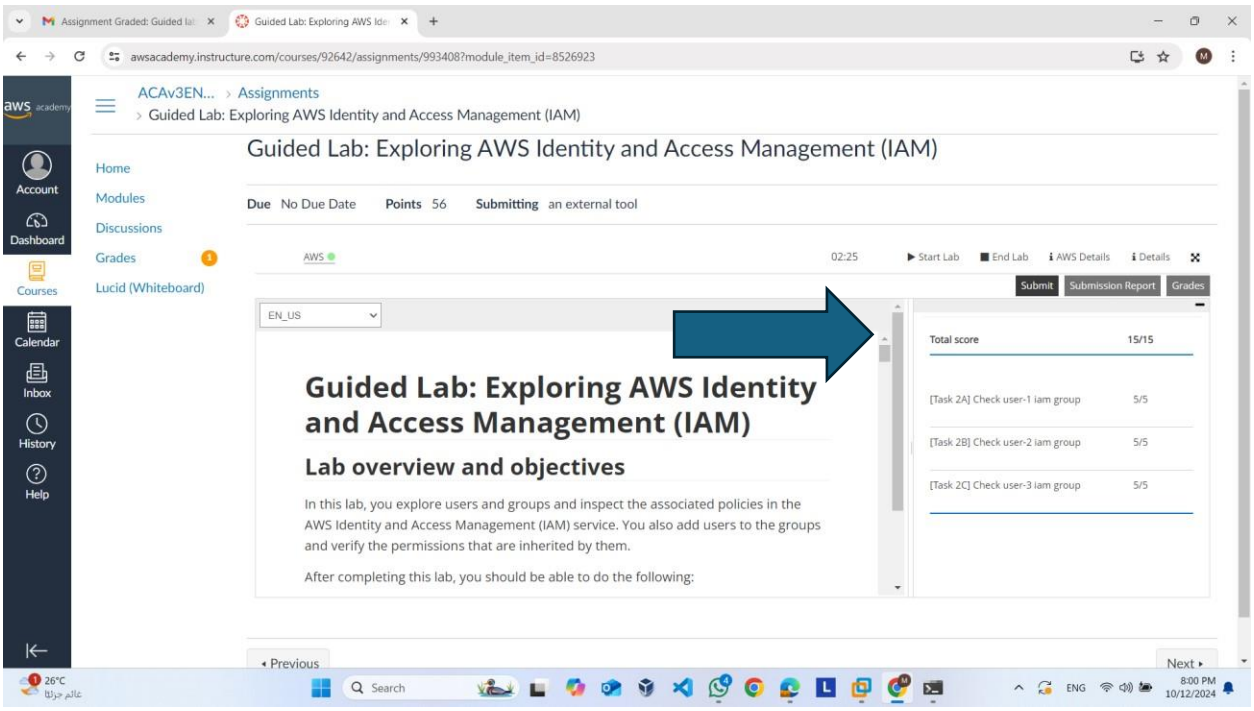

Console Home | Console Home
us-east-1.console.aws.amazon.com/console/home?nc2=h_ct&region=us-east-1&src=header-signin#
Services
Search
[Alt+S]
N. Virginia
user-2 @ 4146-7123-1943
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
S3
EC2
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
Getting started with AWS
AWS Health Info
Cost and usage Info
Current month costs
Cost breakdown
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Search
ENG
7:58 PM
10/12/2024


Assignment Graded: Guided la
Guided Lab: Exploring AWS Ide
S3 buckets | S3 | us-east-1
us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1
Services
Search
[Alt+S]
N. Virginia
user-2 @ 4146-7123-1943
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
You don't have permissions to list buckets
After you or your AWS administrator has updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3
Diagnose with Amazon Q
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Search
ENG
7:58 PM
10/12/2024


Assignment Graded: Guided la
Guided Lab: Exploring AWS Ide
Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
user-2 @ 4146-7123-1943
EC2 Dashboard
EC2 Global View
Events
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
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
i-0f24de8db8dfd9709
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Search
ENG
7:58 PM
10/12/2024


Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
EC2
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
View all services
Go to myApplications
Welcome to AWS
Getting started with AWS
AWS Health Info
Cost and usage Info
Current month costs
Cost breakdown
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
i-0f24de8db8dfd9709
Running
t2.micro
2/2 checks passed
us-east-1a
Select an instance
EC2 Dashboard
EC2 Global View
Events
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


awsacademy.instructure.com/courses/92642/assignments/993408?module_item_id=8526923
ACAv3EN... › Assignments
› Guided Lab: Exploring AWS Identity and Access Management (IAM)
Guided Lab: Exploring AWS Identity and Access Management (IAM)
Home
Modules
Discussions
Grades
Lucid (Whiteboard)
Due No Due Date Points 56 Submitting an external tool
02:25
Start Lab
End Lab
AWS Details
Details
Submit
Submission Report
Grades
EN_US
Total score 15/15
[Task 2A] Check user-1 iam group 5/5
[Task 2B] Check user-2 iam group 5/5
[Task 2C] Check user-3 iam group 5/5
Guided Lab: Exploring AWS Identity and Access Management (IAM)
Lab overview and objectives
In this lab, you explore users and groups and inspect the associated policies in the AWS Identity and Access Management (IAM) service. You also add users to the groups and verify the permissions that are inherited by them.
After completing this lab, you should be able to do the following:
Previous
Next
Account
Dashboard
Courses
Calendar
Inbox
History
Help
Search
ENG
8:00 PM
10/12/2024

Project 9:

Creating an Amazon Virtual Private Cloud (VPC)

Access and Configure AWS CLI

1. **Open the Lab Environment**
    - **Start your lab session as directed.**
2. **Run the Lab**
    - **Initiate the lab session by clicking the "Run Lab" button.**
3. **Access AWS CLI**
    - **Navigate to the AWS Details panel.**
    - **Locate the AWS CLI section and click "Show" to reveal the CLI credentials.**

AWS CLI:

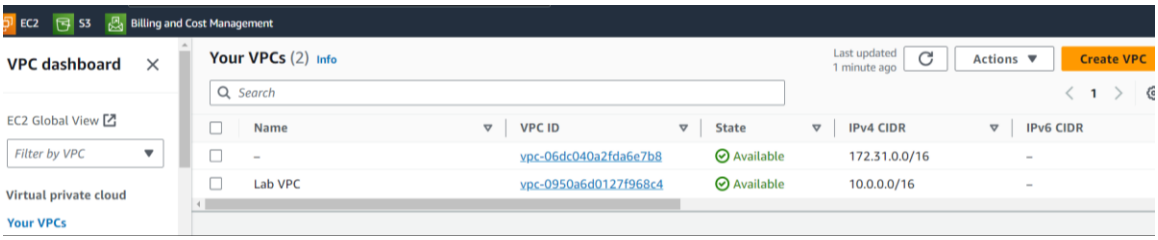
Copy and paste the following into ~/.aws/credentials

```
[default]

aws_access_key_id=ASIAXHLQ2PRMZWM3WZS3

aws_secret_access_key=Iaj9aC5nAOFeFVrvgt4buNgXfnZq+Wv4hrKGeZMU

aws_session_token=IQoJb3JpZ2luX2VjEOn//////////wEaCXVzLXdlc3QtMiJHMEUCIA0v0C4g8len
xl5tttYNvJblb2oPfZu5zDDTvfc1/ADjAiEA8a3RK22iK0iRtcu+zpa175zCEHkSitszx5K9d5rwGB4qsQ
IIQhABGgw0OTY4NDIyMTAzOTMiDEZykTA1VTlICoFG/CqOAld6wrFxxTXU9DcAnwutpaUUa6RuzB1fiKQo
GLaV30ULSAyGDwRtljPwwe1VdEMfZos6ueX11UqkFI4Pq3KpcyAXTpfQaVqFlDdCfnQCigAg2LdNrlW+/E
2ifCDmfbMUZsG7uGGosvJpo8PEb0wVJ+fM7WsIj3xTvf4WmDjXLRZgqiX7sVagNqOHdgOshjCvX679Rsrv
EMF7JdlrR5yYJuwtEqaFgZe4cQNFJz87O9Rgt56NFFxmuXPEpRIuTz7hcrHF27nPqTUy0JEY8uDWkUHrwn
ieXVy3VAa1lVWg3cHCAbCuYhY7TKxLDOXN7ugCD0qVh6m6fHbqUG9W6WQqfpKEQ4IwjVZYbTz2hKkx+zDI
3JO4BjqdAS80PL1MVq58/569ysrjaoWZfYZzXoGob9H5GIwVUff2LQhx8flekyiJAD40B7hOBQ7TSr6Vhd
SCDDPd5SJTF2+jJ2mik0AQpZq4R/AKxjsdeIwa/vjjmX7Gy5gE/d0mDctkmTl5yDcYvWnuxddVx5qHEhuj
n5+xEPP9rScnPgYy/HirsyFEEOI42cnyeiaGeBMtj7thFgXT48zFm1w=
```

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Compumart>aws configure
AWS Access Key ID [****************G37W]: ASIAXHLQ2PRMZWM3WZS3
AWS Secret Access Key [****************7/2G]: Iaj9aC5nAOFeFVrvgt4buNgXfnZq+Wv4hrKGeZMU
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

Task 1: Creating a VPC

```
C:\Users\Compumart>aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications "ResourceType=vpc,Tags=[{Key=Name,Value=Lab VPC}]"
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-0fabfee6c769769ad",
        "State": "pending",
        "VpcId": "vpc-0950a6d0127f968c4",
        "OwnerId": "496842210393",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-026eba95ea96a43aa",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "Lab VPC"
            }
        ]
    }
}
```



Task 2: Creating Subnets

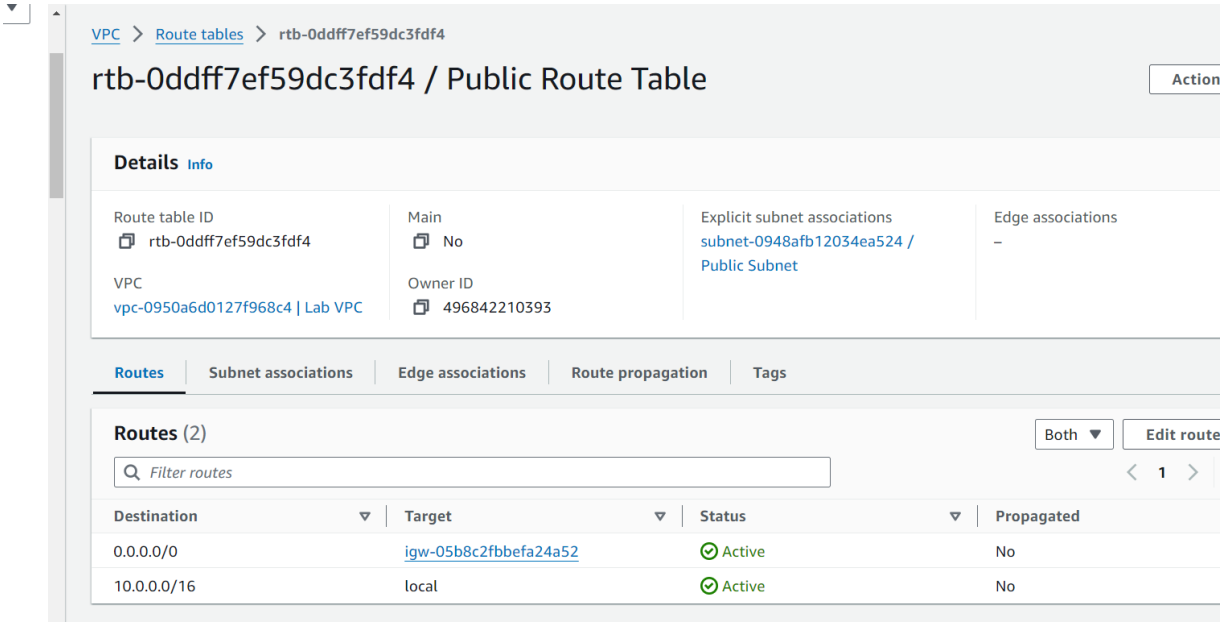
• Task 2.1: Creating a Public Subnet

```
C:\Users\Compumart>aws ec2 modify-vpc-attribute --vpc-id vpc-0950a6d0127f968c4 --enable-dns-support

C:\Users\Compumart>aws ec2 modify-vpc-attribute --vpc-id vpc-0950a6d0127f968c4 --enable-dns-hostnames

C:\Users\Compumart>
C:\Users\Compumart>aws ec2 create-subnet --vpc-id vpc-0950a6d0127f968c4 --cidr-block 10.0.0.0/24 --availability-zone us-east-1a --tag-specifications "ResourceType=subnet,Ta
gs=[{Key=Name,Value=Public Subnet}]"
{
    "Subnet": {
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az2",
        "AvailableIpAddressCount": 251,
        "CidrBlock": "10.0.0.0/24",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-0948afb12034ea524",
        "VpcId": "vpc-0950a6d0127f968c4",
        "OwnerId": "496842210393",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Public Subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:496842210393:subnet/subnet-0948afb12034ea524",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        }
    }
}
```

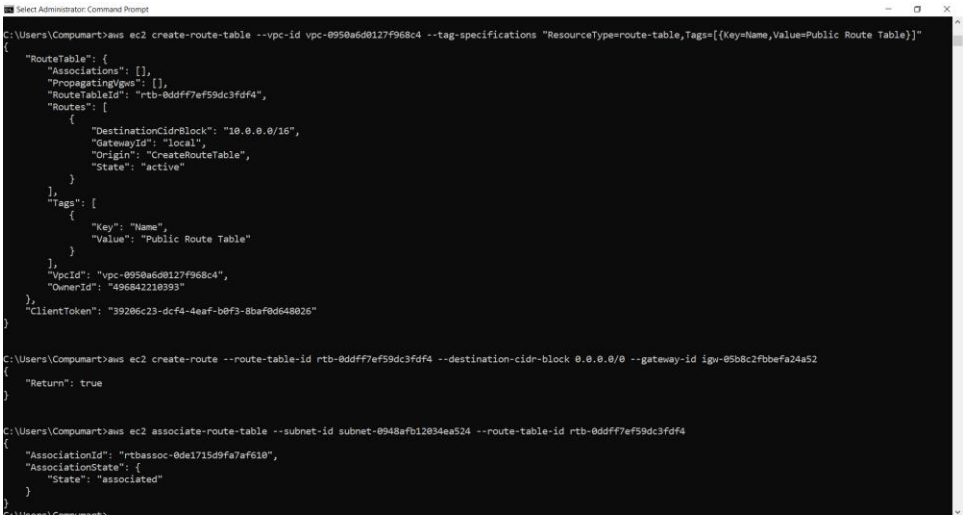
• Task 2.2: Creating a Private Subnet

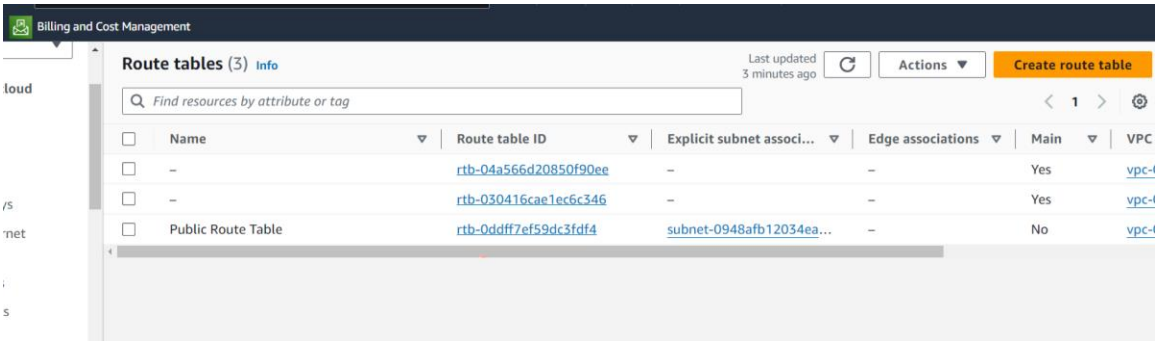
```
Select Administrator: Command Prompt

C:\Users\Compumart>aws ec2 create-subnet --vpc-id vpc-0950a6d0127f968c4 --cidr-block 10.0.2.0/23 --availability-zone us-east-1a --tag-specifications "ResourceType=subn
gs=[{Key=Name,Value=Private Subnet}]"
{
    "Subnet": {
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az2",
        "AvailableIpAddressCount": 507,
        "CidrBlock": "10.0.2.0/23",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-0b99dc58766a80667",
        "VpcId": "vpc-0950a6d0127f968c4",
        "OwnerId": "496842210393",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Private Subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:496842210393:subnet/subnet-0b99dc58766a80667",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        }
    }
}
```

Task 3: Creating an Internet Gateway

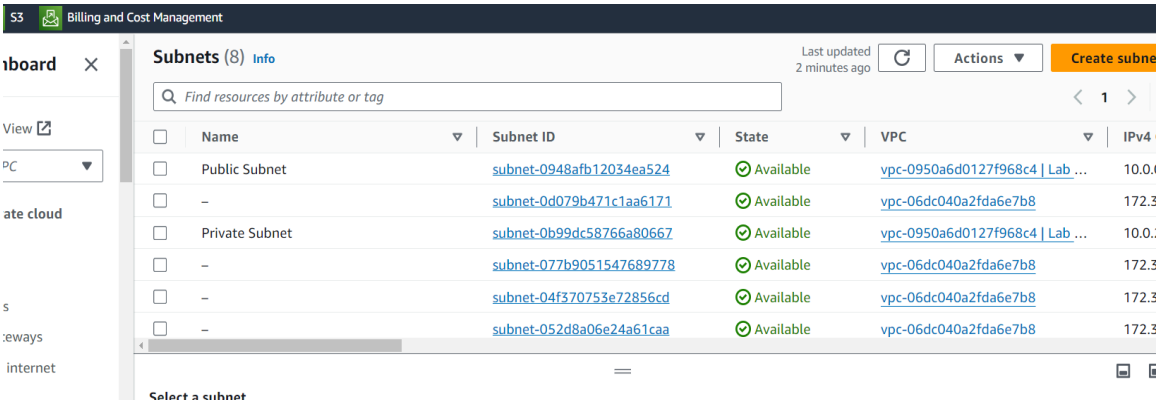


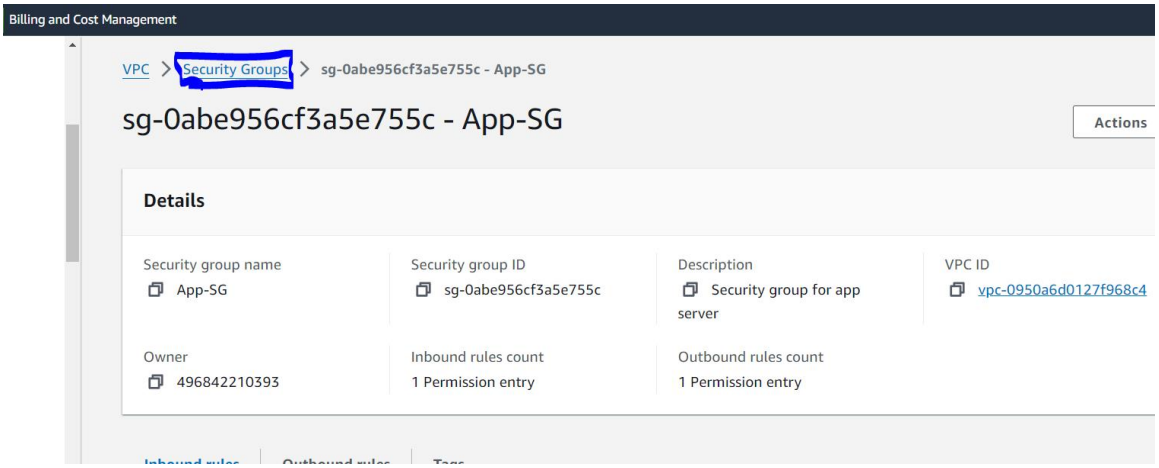
Task 4: Configuring Route Table



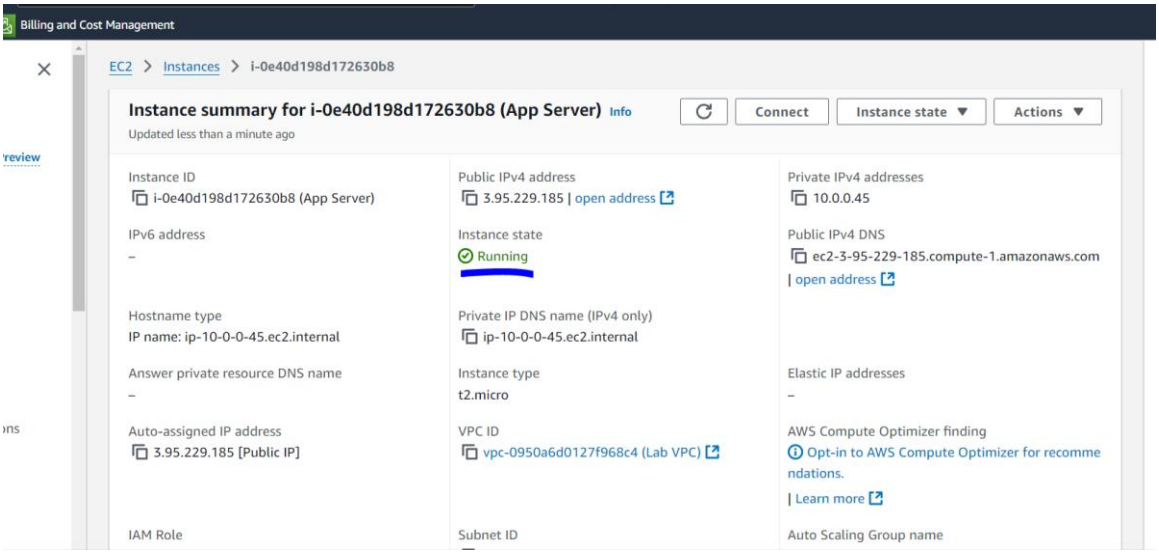


Task 5: Creating a Security Group for the Application Server





Task 6: Launching an Application Server in the Public Subnet



Project 8

Database Management Project Using Amazon RDS

In this project, a database was set up on Amazon RDS to facilitate secure and efficient data management and storage. We used MySQL as the database engine with specific configurations for secure connectivity and access control.

Image 1: Database Details on Amazon RDS

This image shows the Amazon RDS interface for the database named 'inventory-db'. The overall status of the database is 'Available', indicating it is ready for use. The database is created on a db.t3.micro instance, suitable for small applications. You can see the connectivity details, including the Endpoint, which can be used to connect to the database from outside AWS.

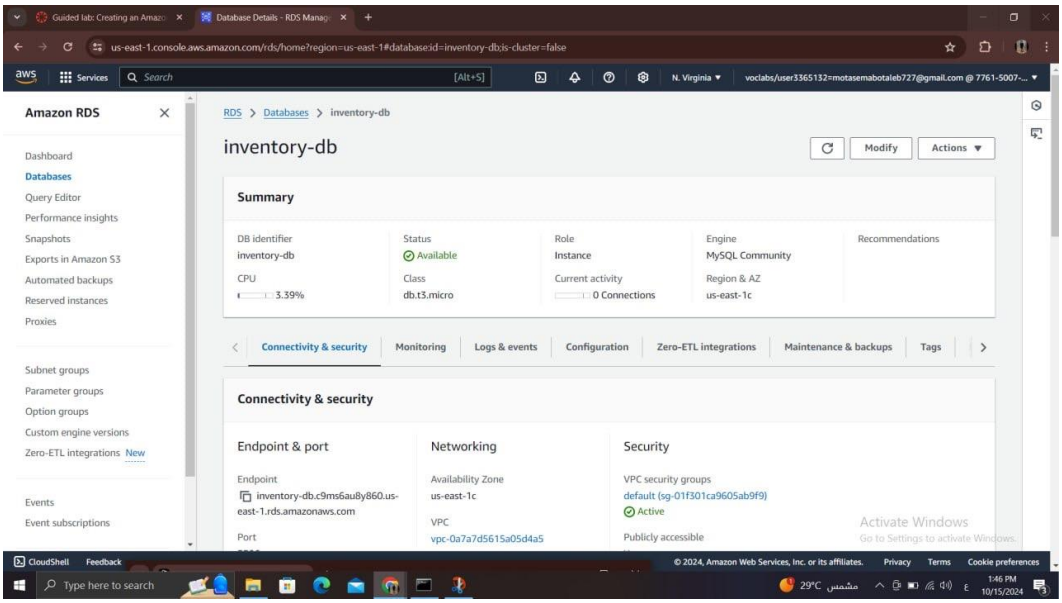


Image 2: Using AWS CLI Command to Retrieve Database Endpoint

In this image, the AWS CLI command 'describe-db-instances' is used, which retrieves specific information about the database. Here, the command queries the 'Endpoint.Address' of the database 'inventory-db'. The displayed address can be used for direct connections to the database from applications or other systems.

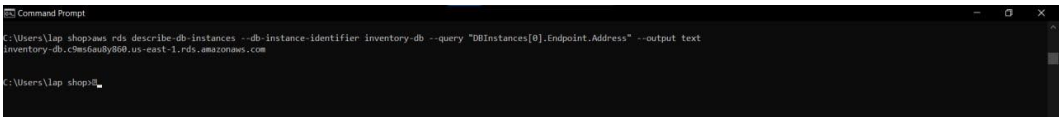


Image 3: Creating a Database Using AWS CLI

This image demonstrates the use of the 'create-db-instance' command in AWS CLI to create the 'inventory-db' database. A storage allocation of 20 GB is specified, along with defining a master username and password for secure access. The command also assigns the VPC
security group to ensure the database is protected and accessible only from specified networks.