Project 6

Exploring AWS Identity and Access Management (IAM)

Group 2

BY / Fouad Yasser Fouad & Mohamed Hesham Elsayed

Access and Configure AWS CLI

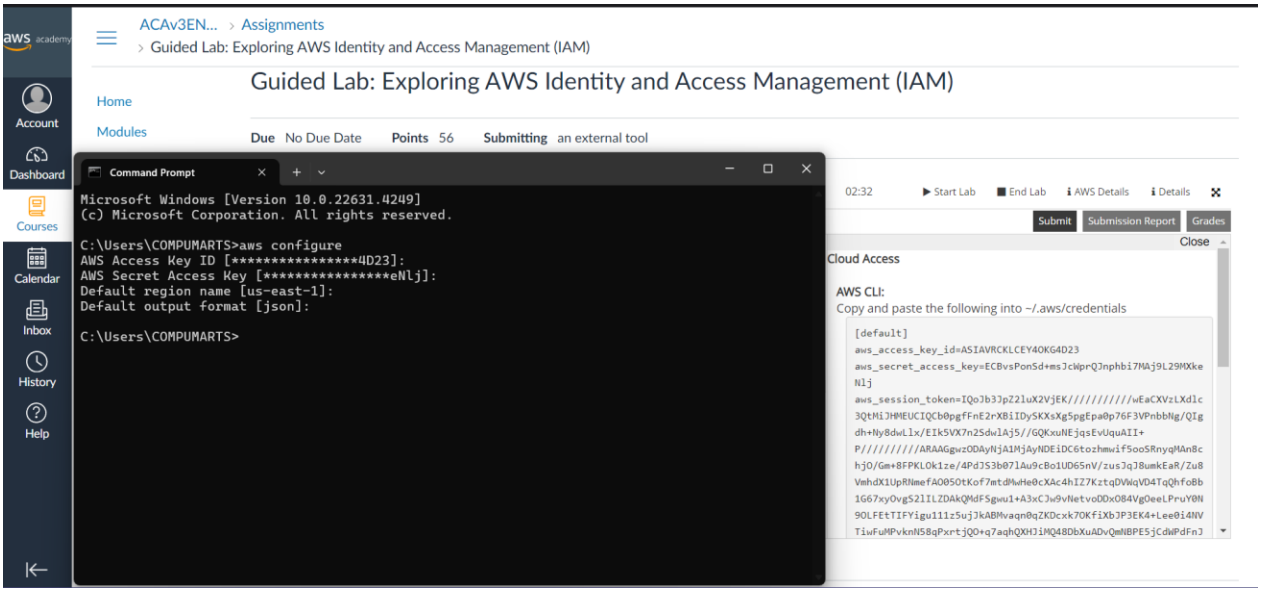
1. **Open the Lab Environment**
   - **Start your lab session as directed.**
2. **Run the Lab**
   - **Initiate the lab session by clicking the "Run Lab" button.**
3. **Access AWS CLI**
   - **Navigate to the AWS Details panel.**
   - **Locate the AWS CLI section and click "Show" to reveal the CLI credentials.**


```
[default]

aws_access_key_id=ASIAVRCKLCEY4OKG4D23

aws_secret_access_key=ECBvsPonSd+msJcWprQJnphbi7MAj9L29MXkeNlj

aws_session_token=IQoJb3JpZ2luX2VjEK//////////wEaCXVzLXdlc3QtMiJHMEUCIQCb0pgfFnE2
rXBiIDySKXsXg5pgEpa0p76F3VPnbbNg/QIgdh+Ny8dwLlx/EIk5VX7n2SdwlAj5//GQKxuNEjqsEvUquA
II+P//////////ARAAGgwzODAyNjA1MjAyNDEiDC6tozhmwif5ooSRnyqMAn8chjO/Gm+8FPKLOk1ze/4P
dJS3b07lAu9cBo1UD65nV/zusJqJ8umkEaR/Zu8VmhdX1UpRNmefAO05OtKof7mtdMwHe0cXAc4hIZ7Kzt
qDVWqVD4TqQhfoBb1G67xyOvgS2lILZDAkQMdFSgwu1+A3xCJw9vNetvoDDxO84VgOeeLPruY0N9OLFEtT
IFYigu111z5ujJkABMvaqn0qZKDcxk7OKfiXbJP3EK4+Lee0i4NVTiwFuMPvknN58qPxrtjQO+q7aqhQXH
JiMQ48DbXuADvQmNBPE5jCdWPdFnJWXYnLAHJrqc+HympW4HTk2CzmcElC9egyQ0kLHNgnfo6KbcCfzh3i
Qg1hTEYw6oiHuAY6nQFVrILOouZ6B0Zv0kaw6LJrxGverQaqEVsCdZLSWkEC4Q85dE/ZFy2CbYQmpCqE/E
dhNv3E2tz2ZmBiLkr3TAqeXkaNB8aUQr6IesHZS6Z1cFz3aOj6eMLhcybsRh+QpwHCcsffnwVULZDuxBOu
lbmLh58YINWBVkG8pn3JVQk+gzAp6BYruEB2iPAfzwgFYXgOsiiIorDQ8iEtT9GY
```


4. **Configure AWS CLI**
   - **Open Command Prompt (cmd) on your Windows machine.**
   - **Enter the following command to start the configuration process:**

```bash
aws configure
```

- **When prompted, input the AWS credentials provided:**
  - **AWS Access Key ID: [Enter your aws_access_key_id]**
  - **AWS Secret Access Key: [Enter your aws_secret_access_key]**
  - **Default region name: [Enter the desired AWS region, e.g., us-west-2]**
  - **Default output format: [Enter your preferred output format, e.g., json]**



Task 1: Explore Users and Groups

1. **List All IAM Users**

   - **Use the following CLI command to list all IAM users:**

```bash
aws iam list-users
```

```
Command Prompt

Microsoft Windows [Version 10.0.22631.4249]
(c) Microsoft Corporation. All rights reserved.

C:\Users\COMPUMARTS>aws configure
AWS Access Key ID [****************4D23]:
AWS Secret Access Key [****************eNlj]:
Default region name [us-east-1]:
Default output format [json]:

C:\Users\COMPUMARTS>aws iam list-users
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDAVRCKLCEY5AO7VVCI7",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-1",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDAVRCKLCEYR6ZO5TH5Z",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-2",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDAVRCKLCEY6AGQANYPE",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-3",
            "CreateDate": "2024-10-05T22:57:50+00:00"
        }
    ]
}


C:\Users\COMPUMARTS>
```

2. **List IAM Groups**

   - **Use the following CLI command to list all IAM groups:**

```bash
aws iam list-groups
```

```
C:\Users\COMPUMARTS>aws iam list-groups
{
    "Groups": [
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Admin",
            "GroupId": "AGPAVRCKLCEYQGERRWBGP",
            "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Admin",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Support",
            "GroupId": "AGPAVRCKLCEYRV3ZTL2FF",
            "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Support",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "S3-Support",
            "GroupId": "AGPAVRCKLCEY34Z2QFRIH",
            "Arn": "arn:aws:iam::380260520241:group/spl66/S3-Support",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        }
    ]
}


C:\Users\COMPUMARTS>
```

3. **Inspect User Details**

   - **Replace [username] with the actual username to inspect details of a specific IAM user:**

```bash
aws iam get-user --user-name <user_name>
```

1. **User-1**

```
C:\Users\COMPUMARTS>aws iam get-user --user-name user-1
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDAVRCKLCEY5AO7VVCI7",
        "Arn": "arn:aws:iam::380260520241:user/spl66/user-1",
        "CreateDate": "2024-10-05T22:57:49+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7852140t1w380260520241"
            }
        ]
    }
}


C:\Users\COMPUMARTS>
```

2. **User-2**

```
C:\Users\COMPUMARTS>aws iam get-user --user-name user-2
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDAVRCKLCEYR6ZO5TH5Z",
        "Arn": "arn:aws:iam::380260520241:user/spl66/user-2",
        "CreateDate": "2024-10-05T22:57:49+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7852140t1w380260520241"
            }
        ]
    }
}


C:\Users\COMPUMARTS>
```

3. **User-3**

```
C:\Users\COMPUMARTS>aws iam get-user --user-name user-3
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDAVRCKLCEY6AGQANYPE",
        "Arn": "arn:aws:iam::380260520241:user/spl66/user-3",
        "CreateDate": "2024-10-05T22:57:50+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7852140t1w380260520241"
            }
        ]
    }
}


C:\Users\COMPUMARTS>
```

4. **Inspect Group Details**

   - **Replace [groupname] with the actual group name to inspect details of a specific IAM group:**

```bash
aws iam get-group --group-name <group_name>
```

1. **S3-Support**

```
C:\Users\COMPUMARTS>aws iam get-group --group-name S3-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPAVRCKLCEY34Z2QFRIH",
        "Arn": "arn:aws:iam::380260520241:group/spl66/S3-Support",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

2. **EC2-Support**

```
C:\Users\COMPUMARTS>aws iam get-group --group-name EC2-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPAVRCKLCEYRV3ZTL2FF",
        "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Support",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

3. **EC2-Admin**

```
C:\Users\COMPUMARTS>aws iam get-group --group-name EC2-Admin
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPAVRCKLCEYQGERRWBGP",
        "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

Task 2: Inspect IAM Policies

1. **List Policies Attached to a Group**
   - **To list the policies attached to a specific IAM group, use the following CLI command:**
   - **Replace [group name] with the actual name of the IAM group.**

```bash
aws iam list-attached-group-policies --group-name <Group-Name>
```

1. **S3-Support**

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

C:\Users\COMPUMARTS>
```

2. **EC2-Support**

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

C:\Users\COMPUMARTS>
```

3. **EC2-Admin**

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

C:\Users\COMPUMARTS>
```

2- Retrieve the Policy Document

- **Once you have the Policy ARN from the previous command, retrieve the policy document using:**
- **Replace [policy-arn] with the ARN of the policy, and [version-id] with the version ID of the policy document.**
- **This command will show the policy document in JSON format, which includes statements like "Effect", "Action", and "Resource".**

bash Copy code

```bash
aws iam get-policy --policy-arn <Policy-ARN>
```

1. **S3-Support**

```
C:\Users\COMPUMARTS>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": []
    }
}


C:\Users\COMPUMARTS>
```

2. **EC2-Support**

```
C:\Users\COMPUMARTS>aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess
{
    "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": []
    }
}


C:\Users\COMPUMARTS>
```

Task 3: Add Users to Groups

1. **Add User-1 to S3-Support Group**
2. **Add User-2 to EC2-Support Group**
3. **Add User-3 to EC2-Admin Group**

```
C:\Users\COMPUMARTS>aws iam add-user-to-group --user-name User-1 --group-name S3-Support

C:\Users\COMPUMARTS>aws iam add-user-to-group --user-name User-2 --group-name EC2-Support

C:\Users\COMPUMARTS>aws iam add-user-to-group --user-name User-3 --group-name EC2-Admin

C:\Users\COMPUMARTS>
```

4. **Verify users are in the specified groups, list the users in each group using:**

1. **S3-Support**

```
C:\Users\COMPUMARTS>aws iam get-group --group-name S3-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDAVRCKLCEY5AO7VVCI7",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-1",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPAVRCKLCEY34Z2QFRIH",
        "Arn": "arn:aws:iam::380260520241:group/spl66/S3-Support",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

2. **EC2-Support**

```
C:\Users\COMPUMARTS>aws iam get-group --group-name EC2-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDAVRCKLCEYR6ZO5TH5Z",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-2",
            "CreateDate": "2024-10-05T22:57:49+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPAVRCKLCEYRV3ZTL2FF",
        "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Support",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

3. **EC2-Admin**

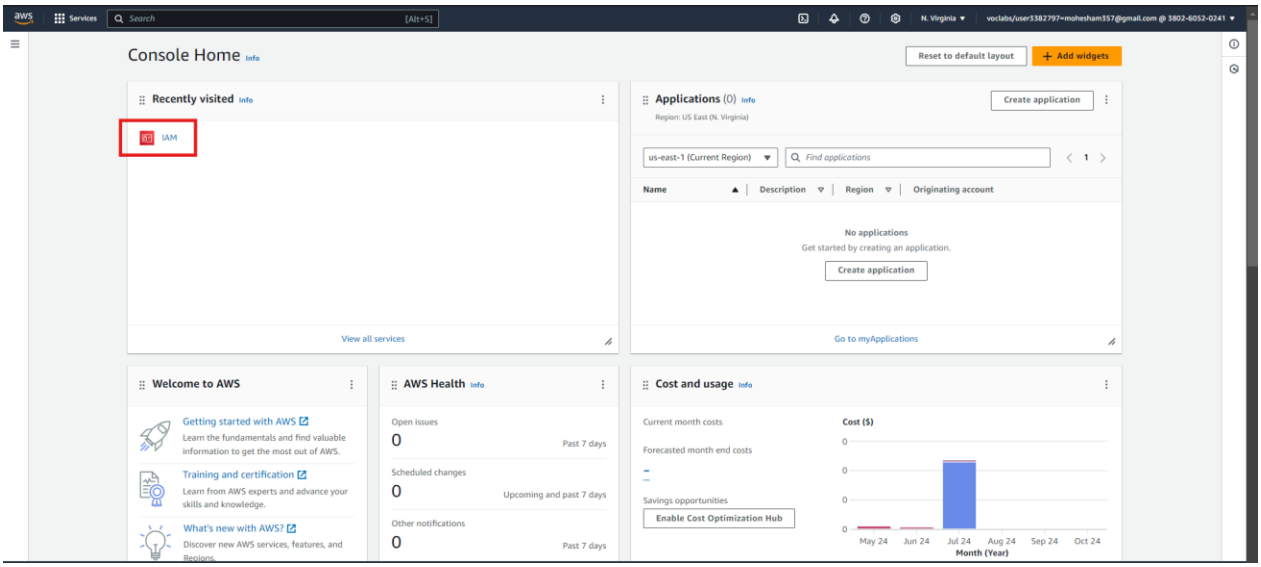
```
C:\Users\COMPUMARTS>aws iam get-group --group-name EC2-Admin
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDAVRCKLCEY6AGQANYPE",
            "Arn": "arn:aws:iam::380260520241:user/spl66/user-3",
            "CreateDate": "2024-10-05T22:57:50+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPAVRCKLCEYQGERRWBGP",
        "Arn": "arn:aws:iam::380260520241:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-05T22:57:49+00:00"
    }
}


C:\Users\COMPUMARTS>
```

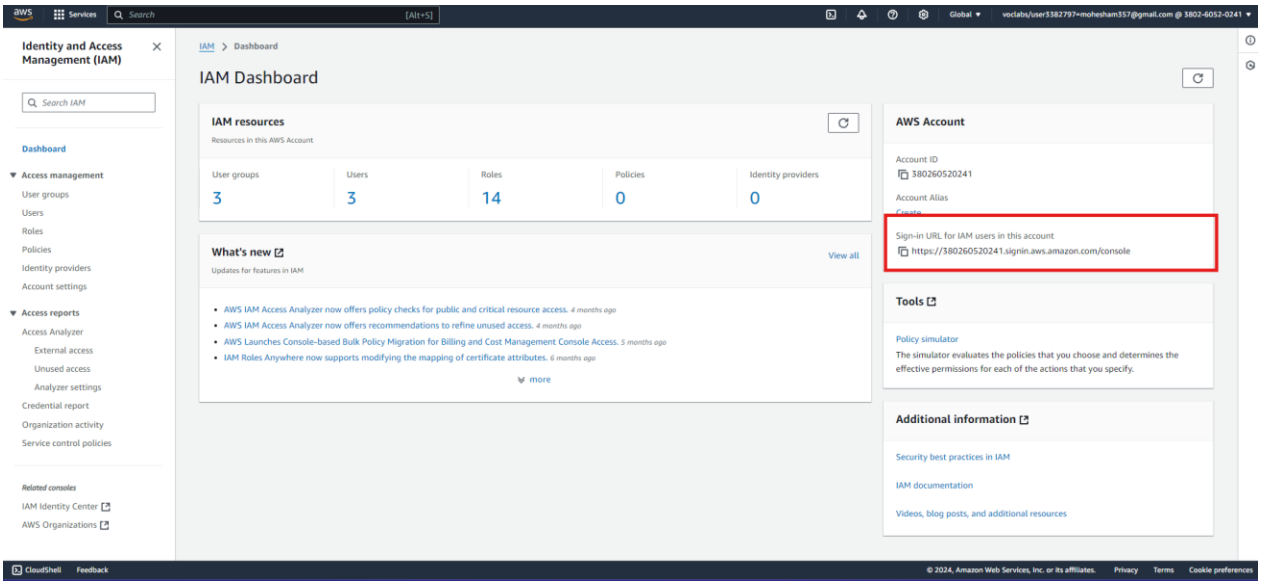
Task 4: Test Permissions

To verify the access of each user, you need to simulate their login using the AWS Management Console. Since testing involves logging in via the browser, here's how to proceed for each user:

Task 4.1: Get the console sign-in URL

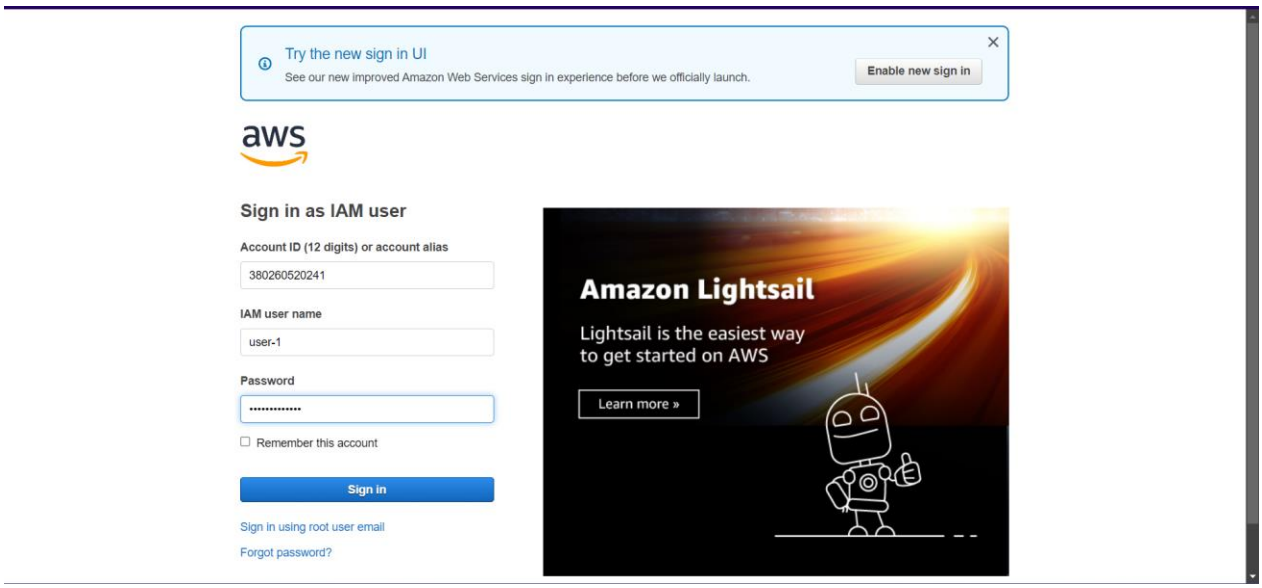
- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.

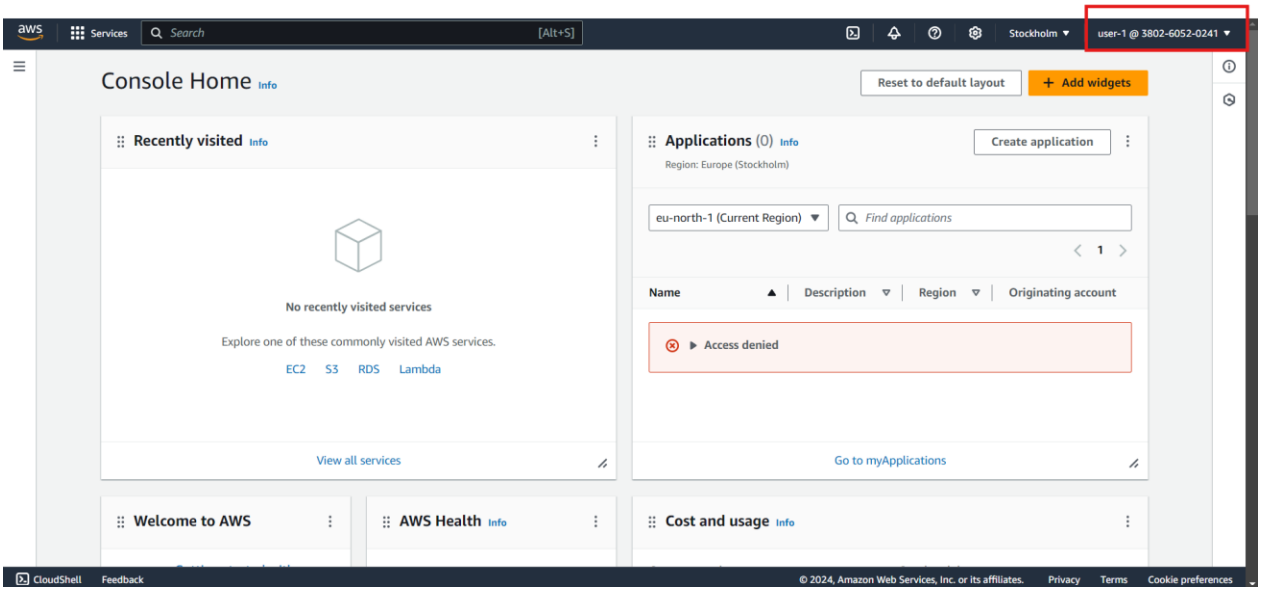




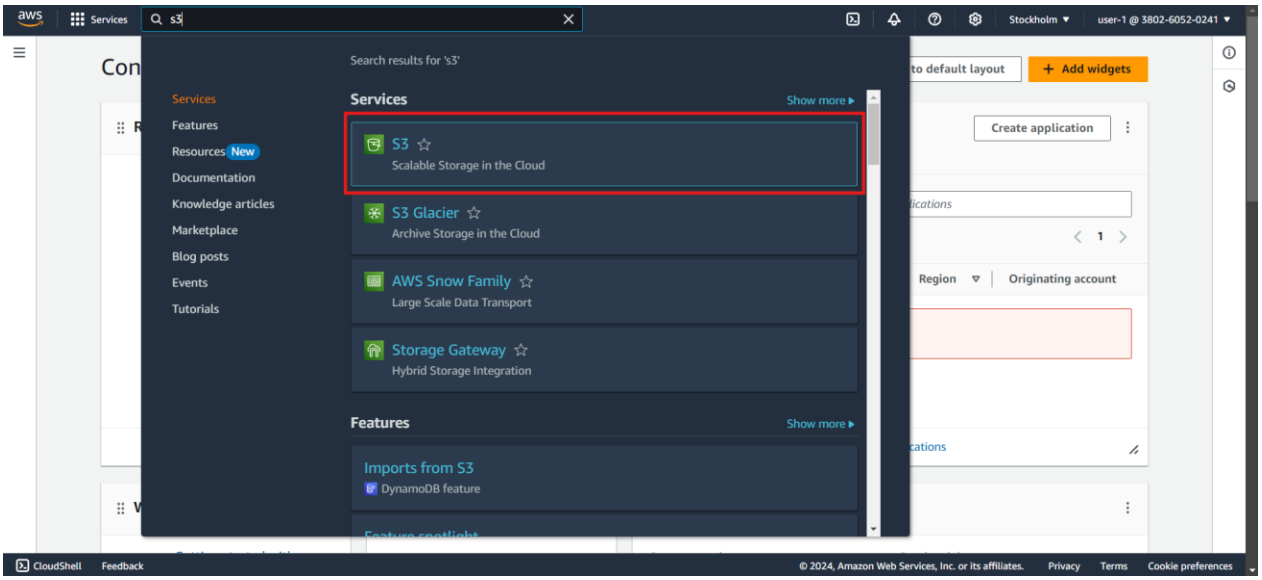
Task 4.2: Test user-1 permissions

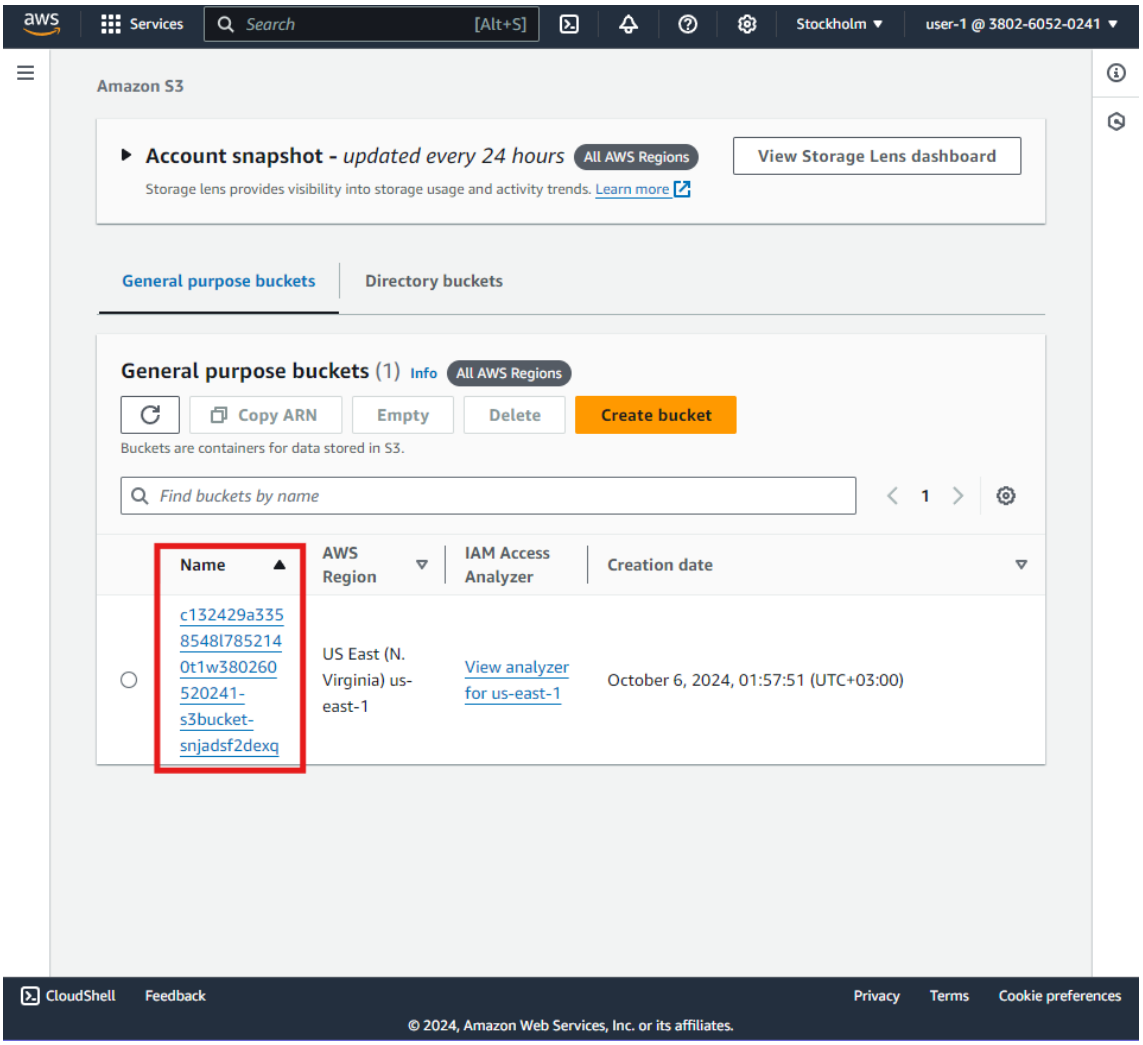
2. Open a private or incognito window in your browser.
3. Paste the sign-in link into the private browser, and press ENTER.
4. Sign in with the following credentials:
    - **IAM user name:** user-1
    - **Password:** Lab-Password1

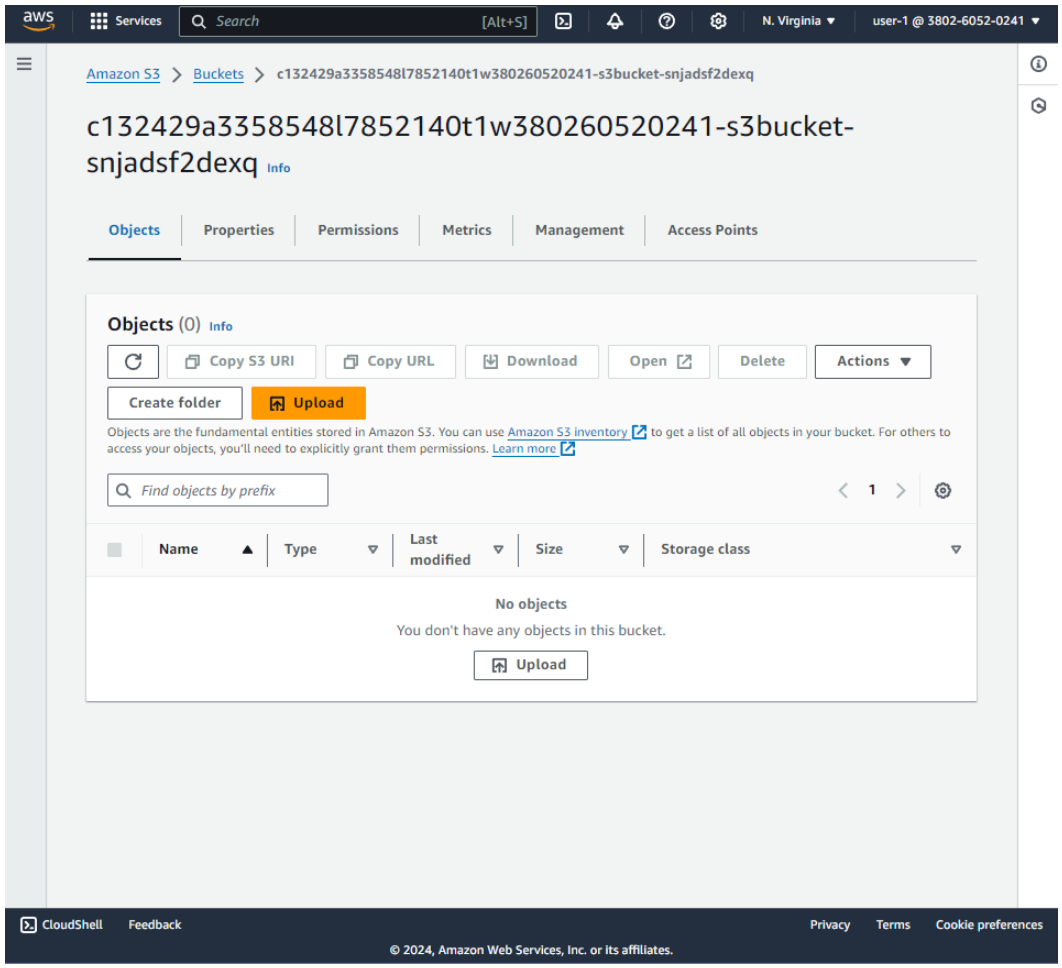




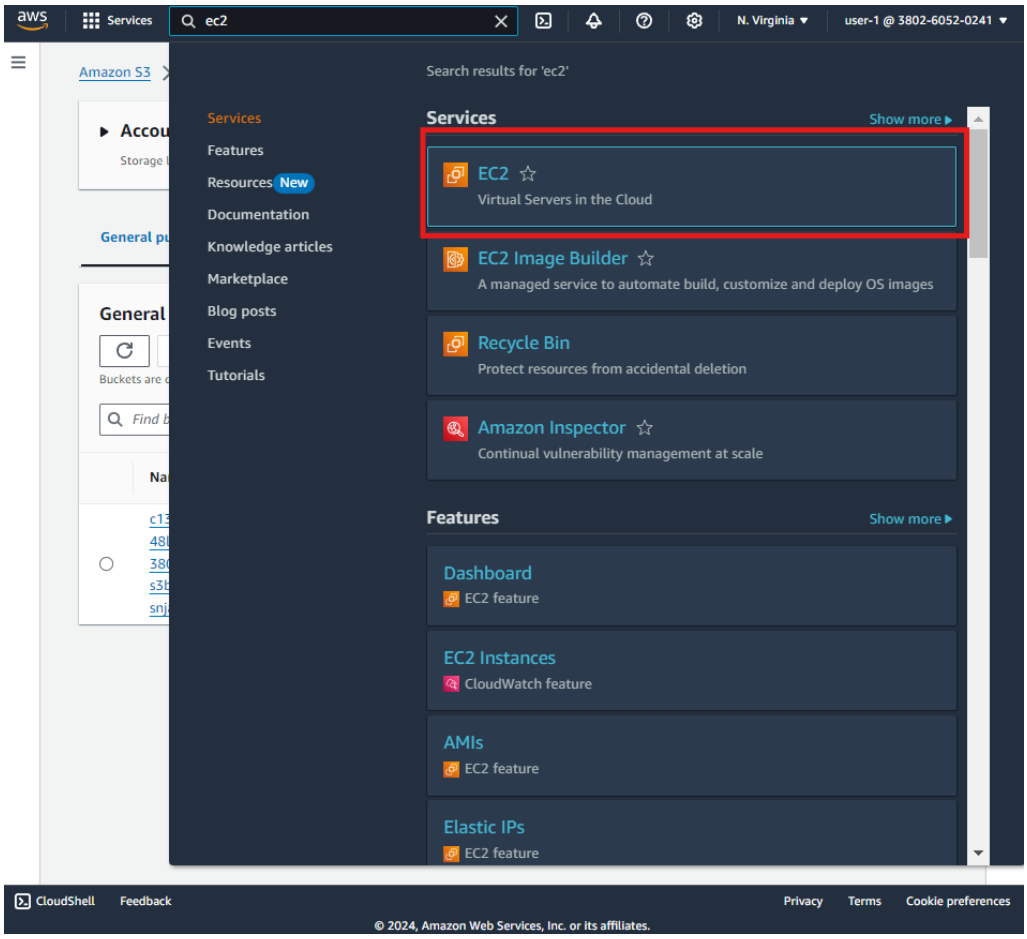
5. Navigate to the S3 service and try to list buckets.

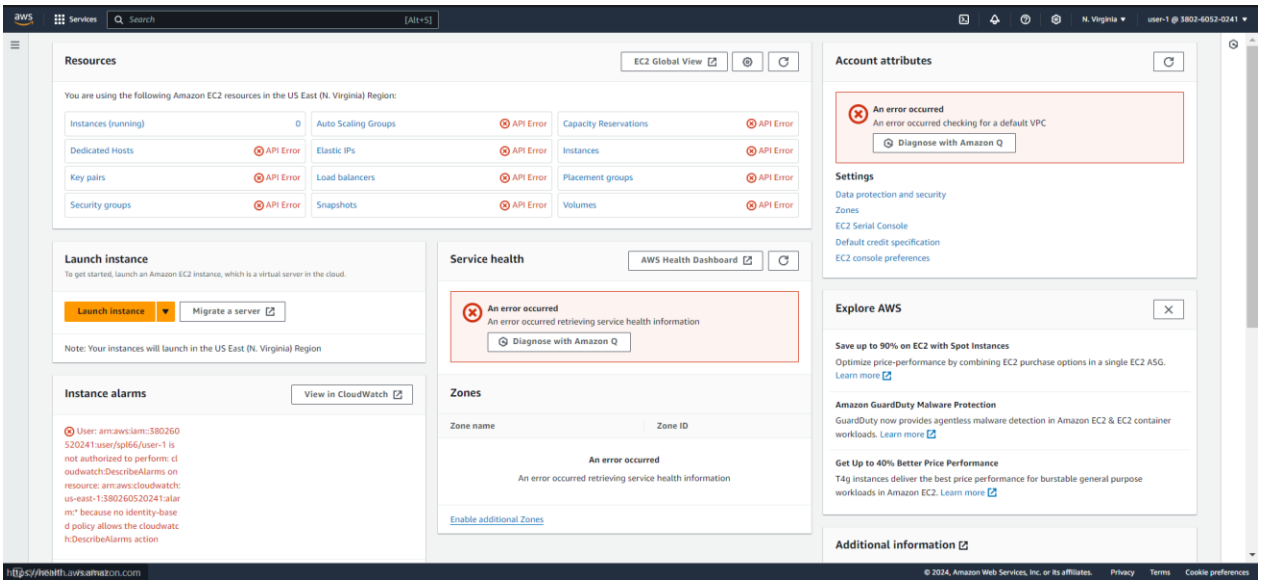

aws
Services
s3
Stockholm
user-1 @ 3802-6052-0241
Search results for 's3'
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Services
Show more
S3
Scalable Storage in the Cloud
S3 Glacier
Archive Storage in the Cloud
AWS Snow Family
Large Scale Data Transport
Storage Gateway
Hybrid Storage Integration
Features
Show more
Imports from S3
DynamoDB feature
to default layout
+ Add widgets
Create application
Region
Originating account
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

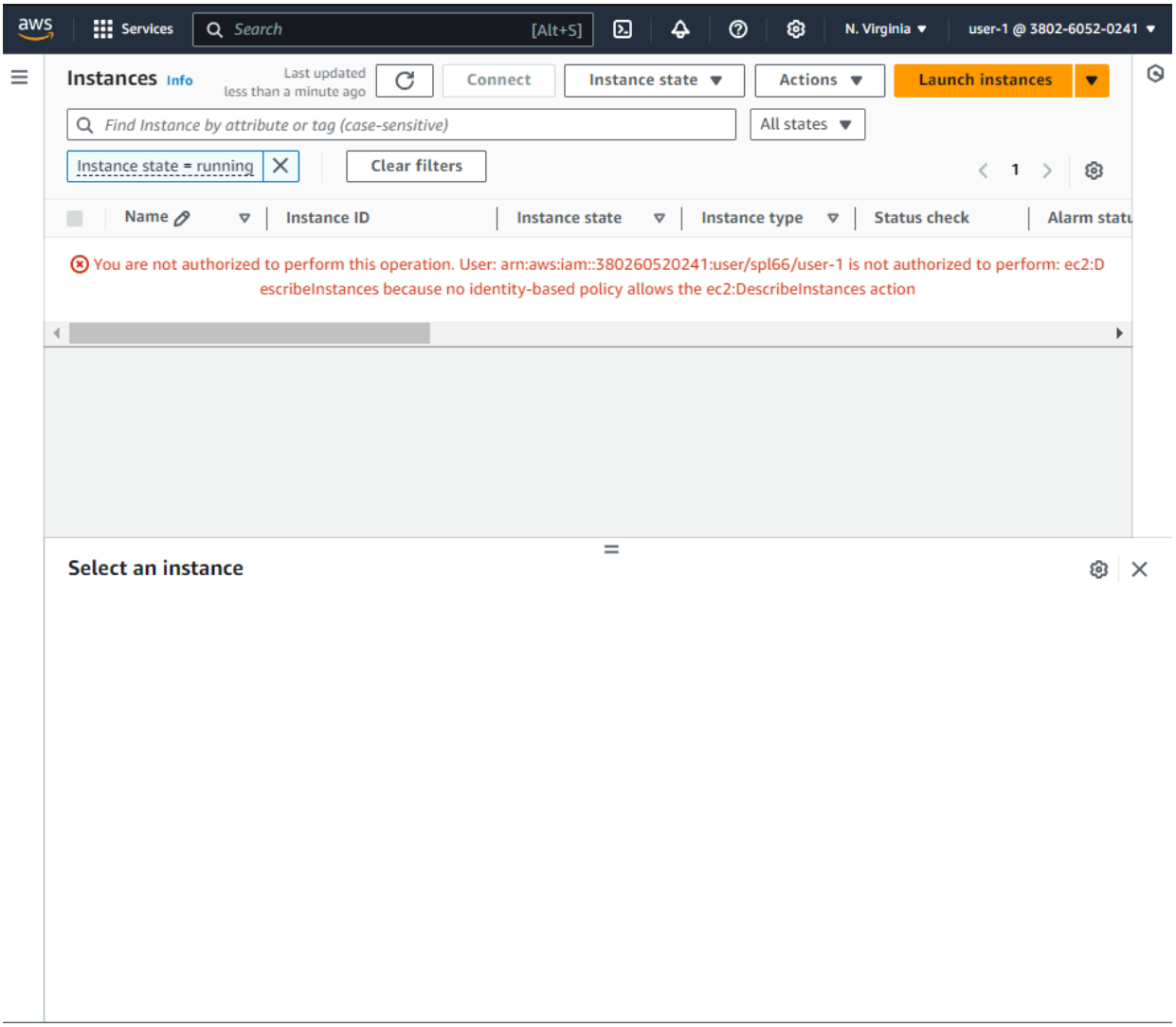

aws
Services
Search
[Alt+S]
Stockholm
user-1 @ 3802-6052-0241
Amazon S3
Account snapshot - updated every 24 hours
All AWS Regions
View Storage Lens dashboard
Storage lens provides visibility into storage usage and activity trends. Learn more
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3.
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
c132429a3358548l7852140t1w380260520241-s3bucket-snjadsf2dexq
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 6, 2024, 01:57:51 (UTC+03:00)
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.



6. Try to perform any write operations (like read ec2 instance), which should fail due to user-1 has **AmazonS3ReadOnlyAccess** policy

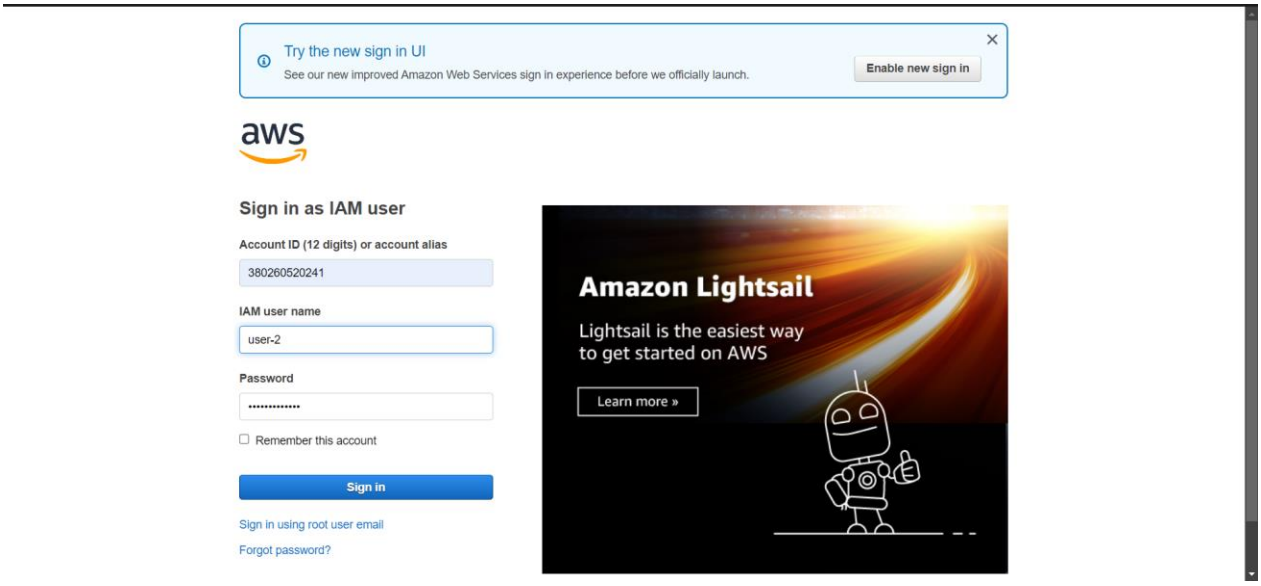



Resources
EC2 Global View
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 0
Auto Scaling Groups API Error
Capacity Reservations API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Account attributes
An error occurred
An error occurred checking for a default VPC
Diagnose with Amazon Q
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the US East (N. Virginia) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Explore AWS
Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG.
Learn more
Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more
Get Up to 40% Better Price Performance
T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more
Instance alarms
View in CloudWatch
User: arn:aws:iam::380260520241:user/spl66/user-1 is not authorized to perform: cloudwatch:DescribeAlarms on resource: arn:aws:cloudwatch:us-east-1:380260520241:alarm:* because no identity-based policy allows the cloudwatch:DescribeAlarms action
Zones
Zone name
Zone ID
An error occurred
An error occurred retrieving service health information
Enable additional Zones
Additional information
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

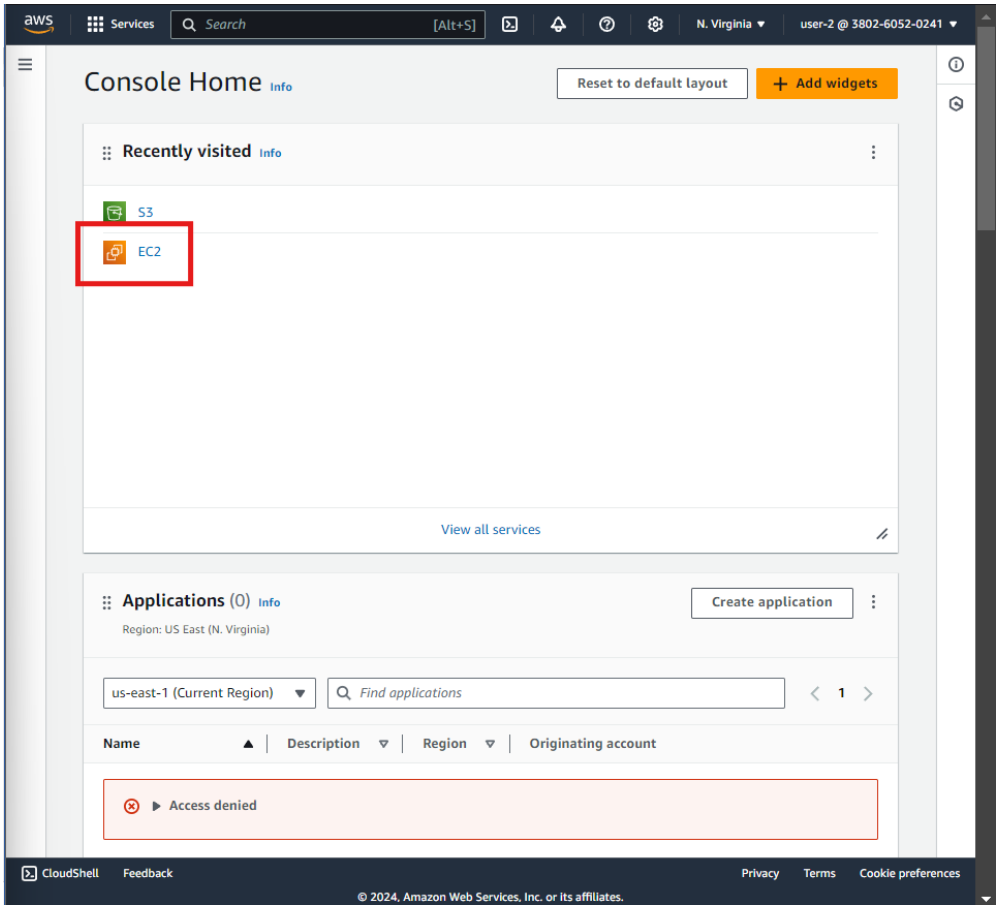

Services
Search
[Alt+S]
N. Virginia
user-1 @ 3802-6052-0241
Instances Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm statu
You are not authorized to perform this operation. User: arn:aws:iam::380260520241:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action
Select an instance

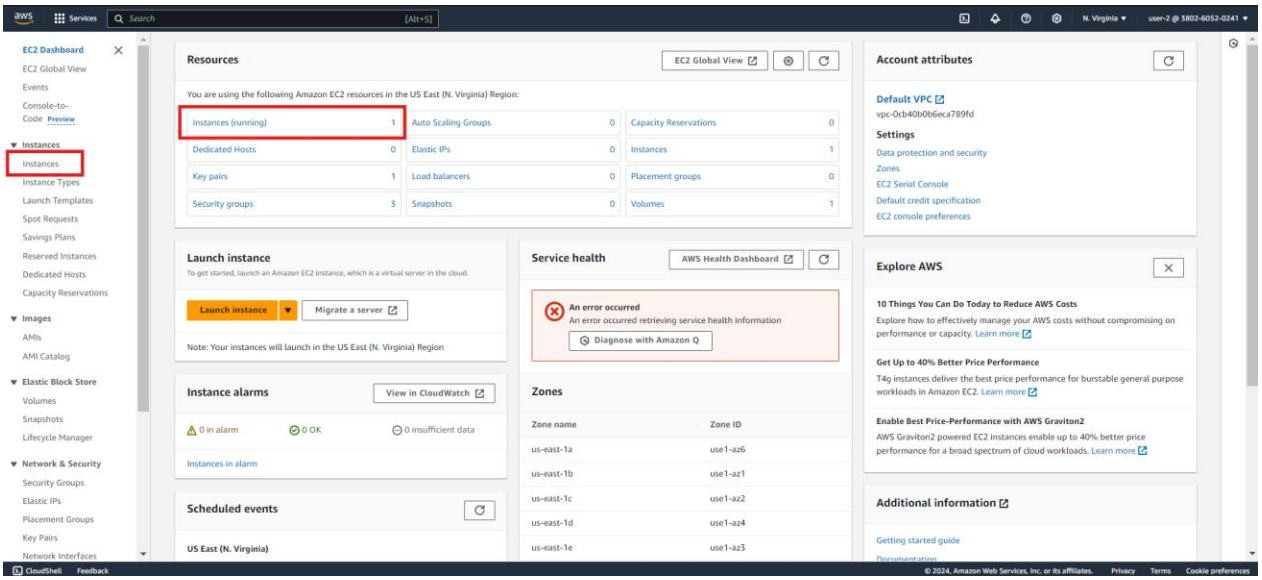
Task 4.3: Test user-2 permissions

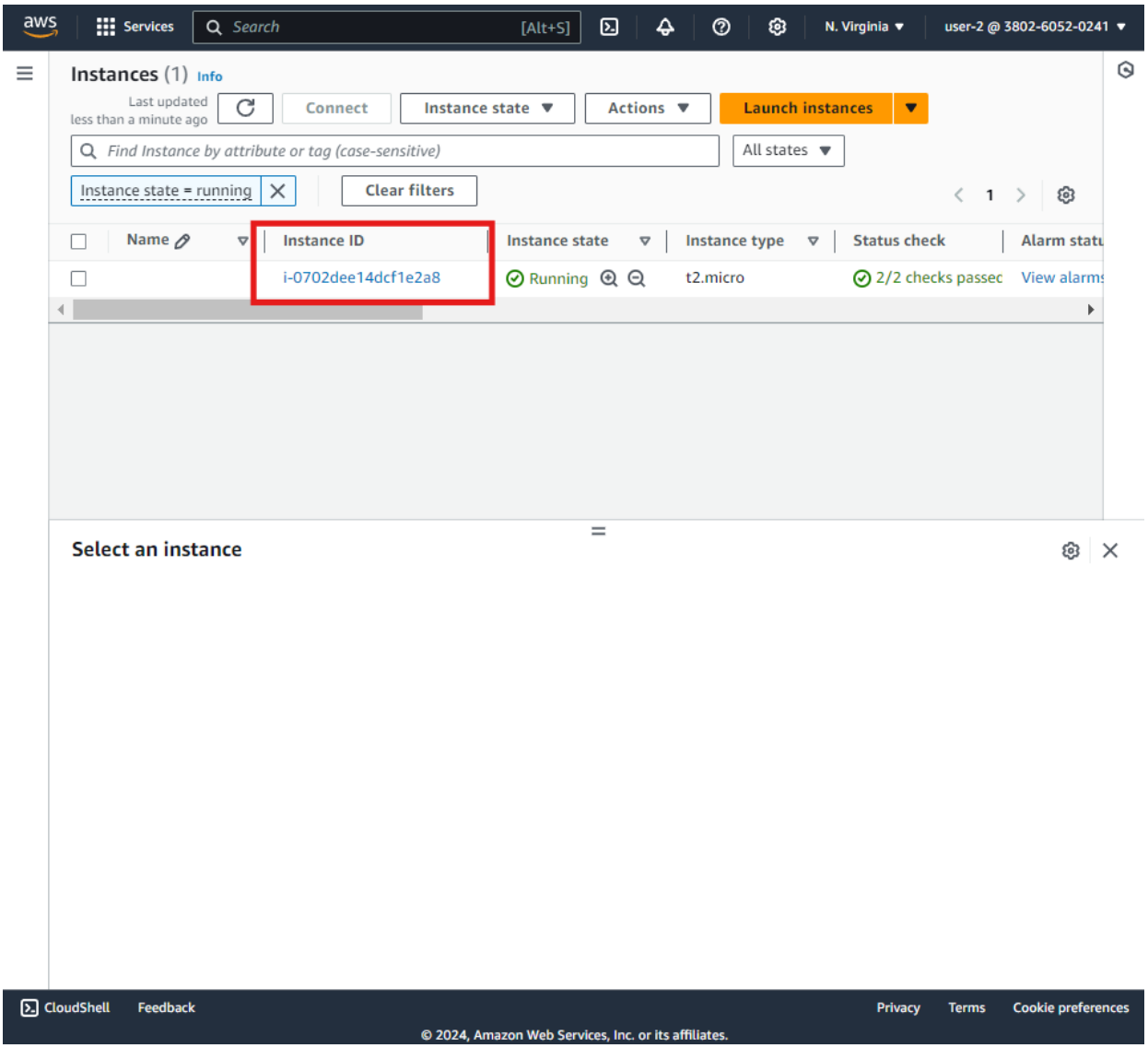
1. Sign in with the following credentials:
    - **IAM user name:** user-2
    - **Password:** Lab-Password2

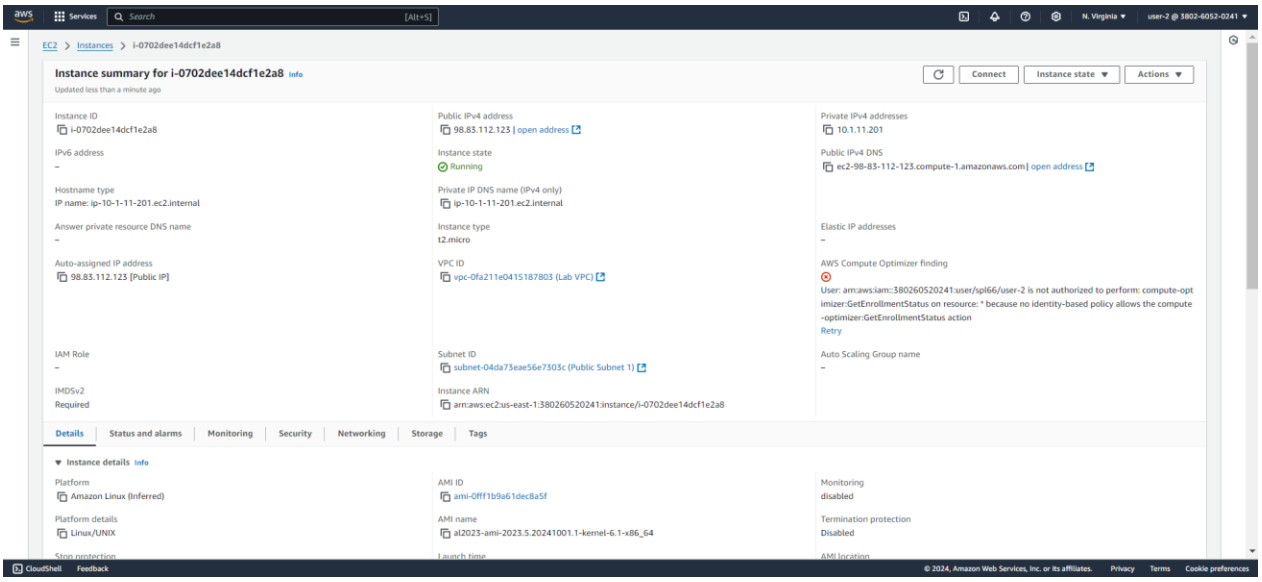


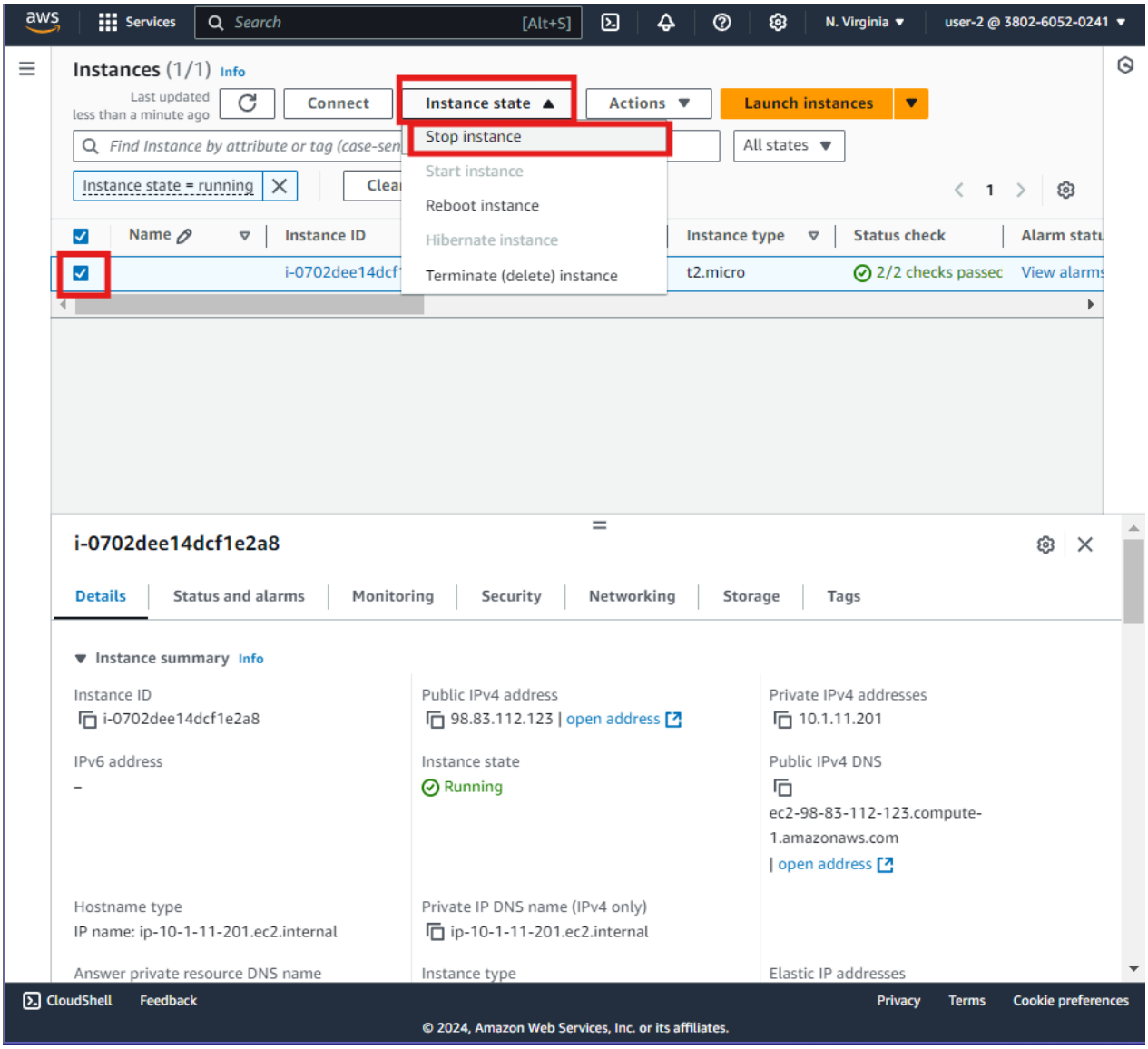
2. .Navigate to the **EC2 service.** You are now able to see an EC2 instance. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions

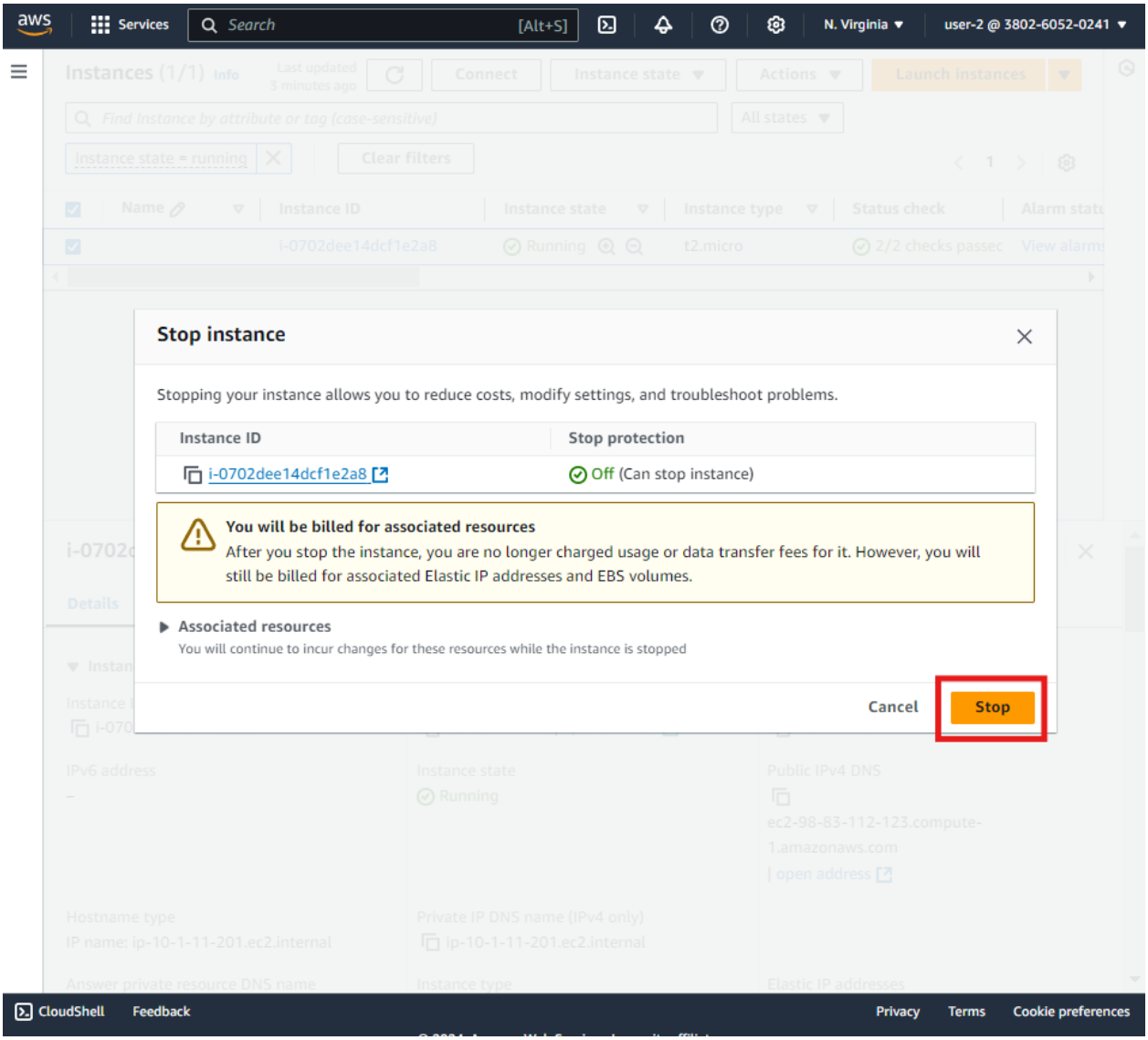


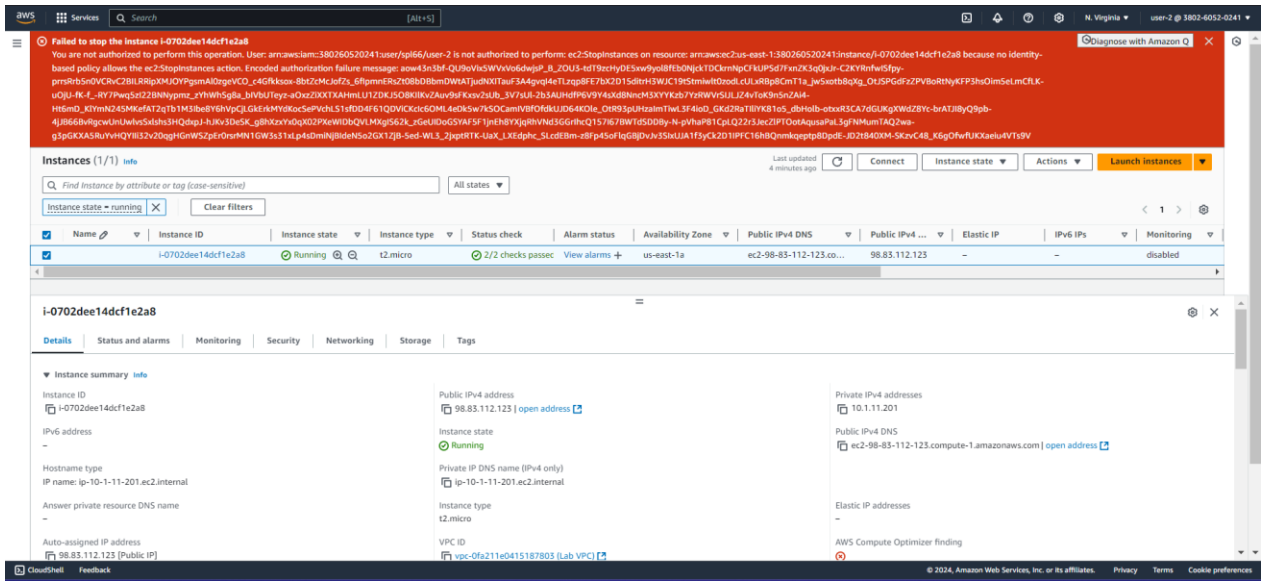

Services
Search
[Alt+S]
N. Virginia
user-2 @ 3802-6052-0241
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 1
Auto Scaling Groups 0
Capacity Reservations 0
Dedicated Hosts 0
Elastic IPs 0
Instances 1
Key pairs 1
Load balancers 0
Placement groups 0
Security groups 3
Snapshots 0
Volumes 1
Account attributes
Default VPC
vpc-0cb40b0b6eca789fd
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the US East (N. Virginia) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Explore AWS
10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more
Get Up to 40% Better Price Performance
T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more
Enable Best Price-Performance with AWS Graviton2
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more
Instance alarms
View in CloudWatch
0 in alarm
0 OK
0 insufficient data
Instances in alarm
Zones
Zone name
Zone ID
us-east-1a
use1-az6
us-east-1b
use1-az1
us-east-1c
use1-az2
us-east-1d
use1-az4
us-east-1e
use1-az3
Scheduled events
US East (N. Virginia)
Additional information
Getting started guide
Documentation
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
user-2 @ 3802-6052-0241
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
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm statu
i-0702dee14dcf1e2a8
Running
t2.micro
2/2 checks passec
View alarms
Select an instance
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.


Instance summary for i-0702dee14dcf1e2a8
Connect
Instance state
Actions
Instance ID
i-0702dee14dcf1e2a8
Public IPv4 address
98.83.112.123 | open address
Private IPv4 addresses
10.1.11.201
Instance state
Running
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
98.83.112.123 [Public IP]
VPC ID
vpc-0fa211e0415187803 (Lab VPC)
AWS Compute Optimizer finding
Retry
IAM Role
Subnet ID
subnet-04da73eae56e7303c (Public Subnet 1)
Auto Scaling Group name
IMDSv2
Required
Instance ARN
arn:aws:ec2:us-east-1:380260520241:instance/i-0702dee14dcf1e2a8
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details
Platform
Amazon Linux (Inferred)
AMI ID
ami-0fff1b9a61dec8a5f
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.5.20241001.1-kernel-6.1-x86_64
Termination protection
Disabled


Services
Search
[Alt+S]
N. Virginia
user-2 @ 3802-6052-0241
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
All states
Instance state = running
Name
Instance ID
Instance type
Status check
Alarm statu
i-0702dee14dcf
t2.micro
2/2 checks passed
View alarms
i-0702dee14dcf1e2a8
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0702dee14dcf1e2a8
Public IPv4 address
98.83.112.123 | open address
Private IPv4 addresses
10.1.11.201
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com
| open address
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Answer private resource DNS name
Instance type
Elastic IP addresses
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.

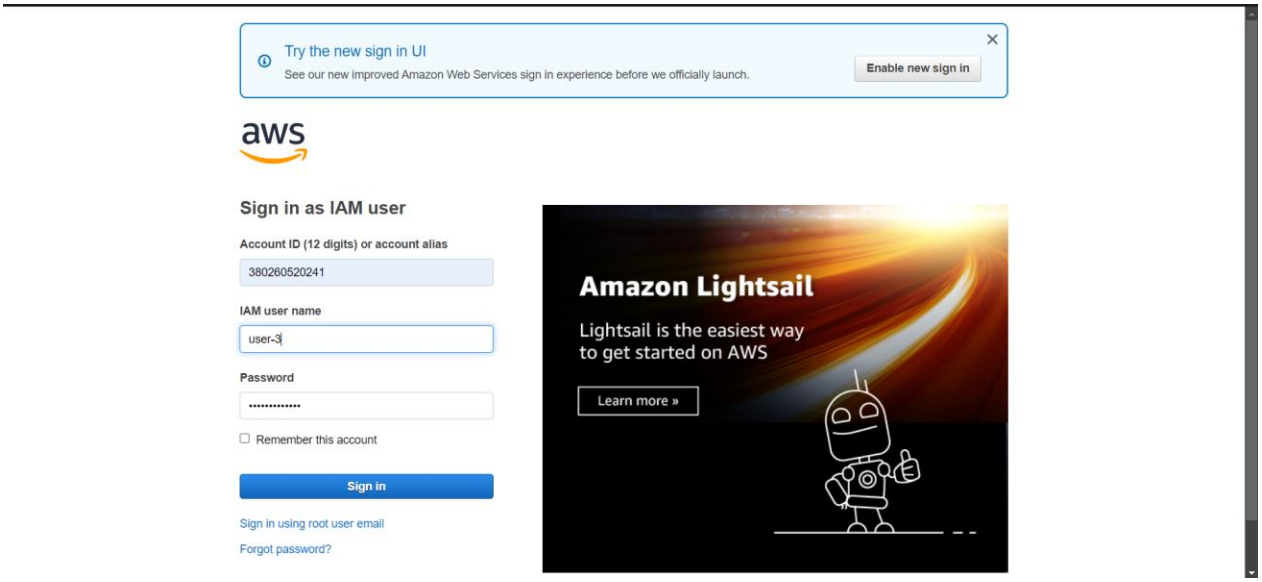

aws
Services
Search
[Alt+S]
N. Virginia
user-2 @ 3802-6052-0241
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
i-0702dee14dcf1e2a8
Running
t2.micro
2/2 checks passed
Stop instance
Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.
Instance ID
Stop protection
i-0702dee14dcf1e2a8
Off (Can stop instance)
You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.
Associated resources
You will continue to incur charges for these resources while the instance is stopped
Cancel
Stop
CloudShell
Feedback
Privacy
Terms
Cookie preferences

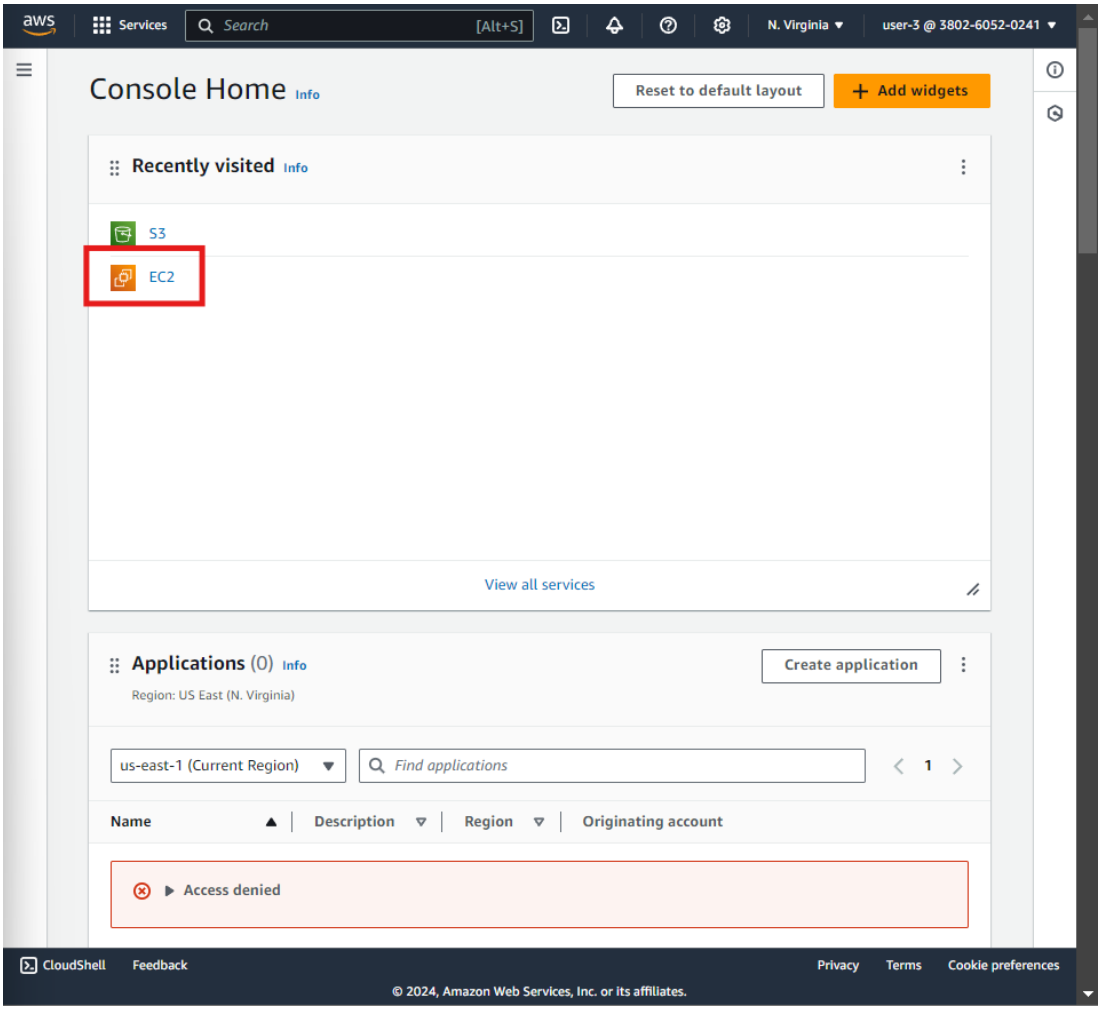

Failed to stop the instance i-0702dee14dcf1e2a8
Diagnose with Amazon Q
Instances (1/1)
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
IPv6 IPs
Monitoring
i-0702dee14dcf1e2a8
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-98-83-112-123.co...
98.83.112.123
disabled
i-0702dee14dcf1e2a8
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary
Instance ID
i-0702dee14dcf1e2a8
Public IPv4 address
98.83.112.123 | open address
Private IPv4 addresses
10.1.11.201
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Answer private resource DNS name
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
98.83.112.123 [Public IP]
VPC ID
vpc-0fa211e0415187803 (Lab VPC)
AWS Compute Optimizer finding
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

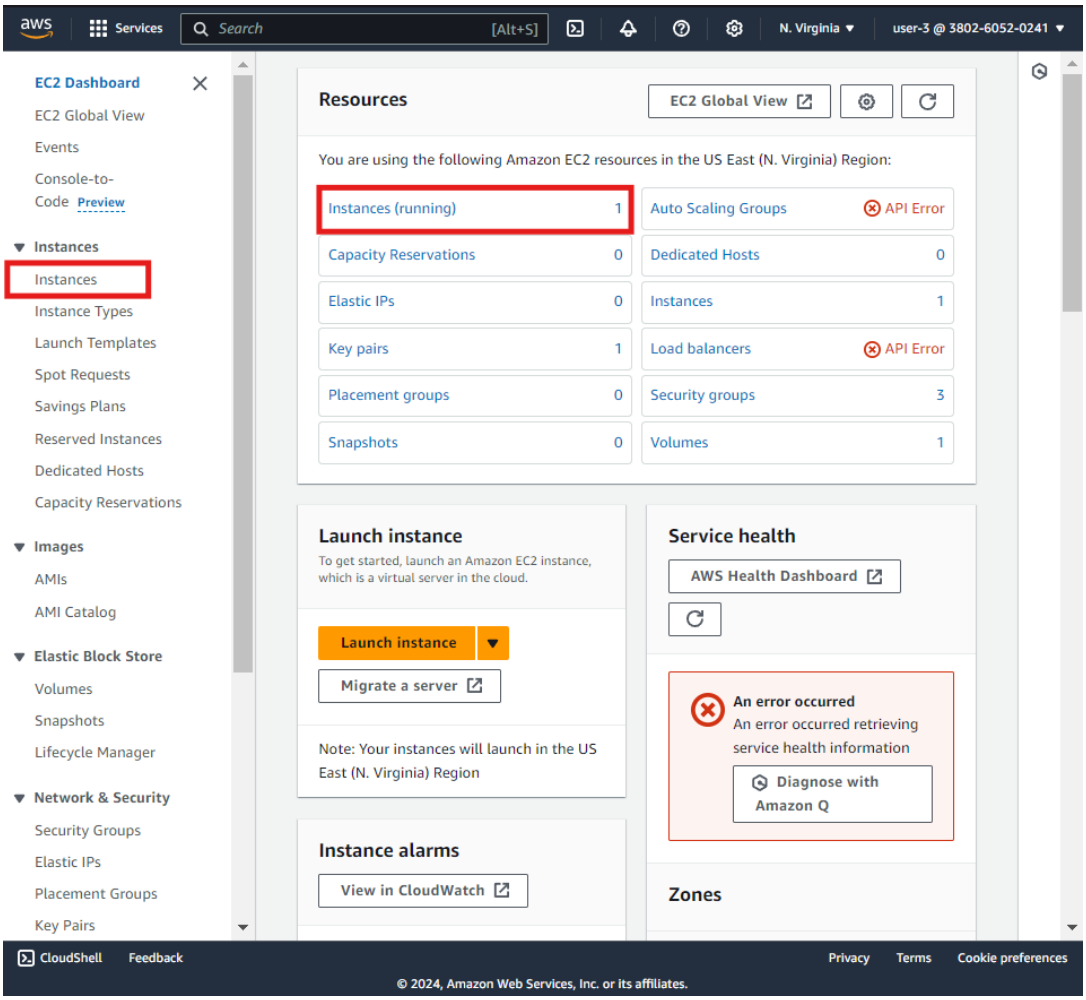
Task 4.4: Test user-3 permissions

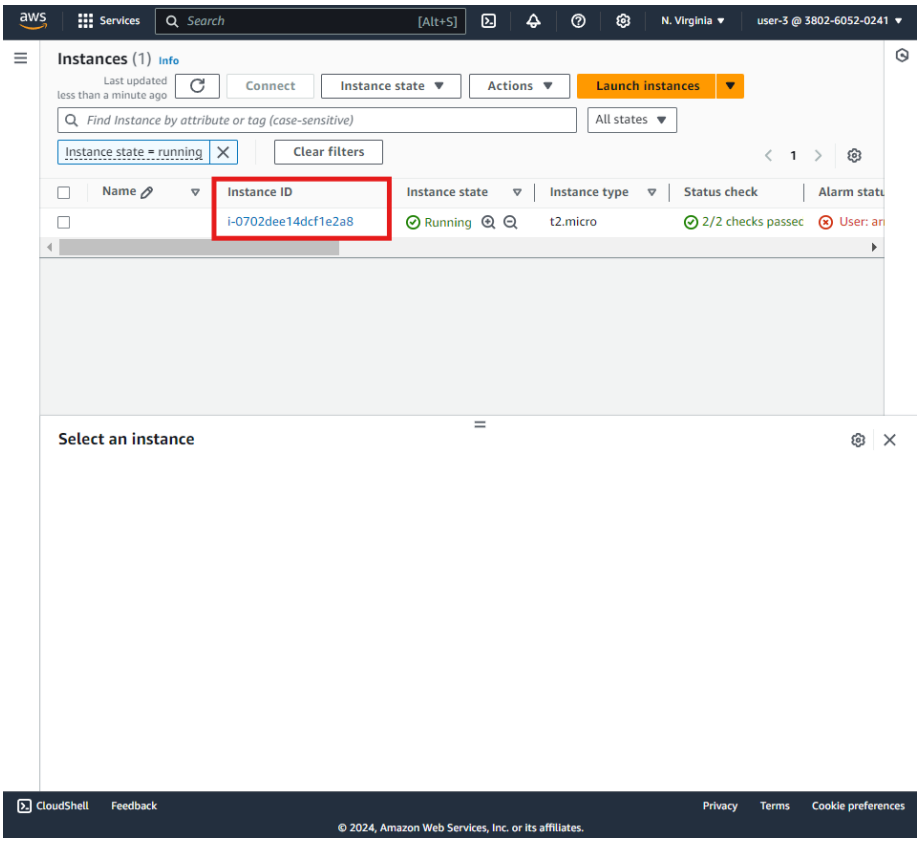
1.Sign in with the following credentials:

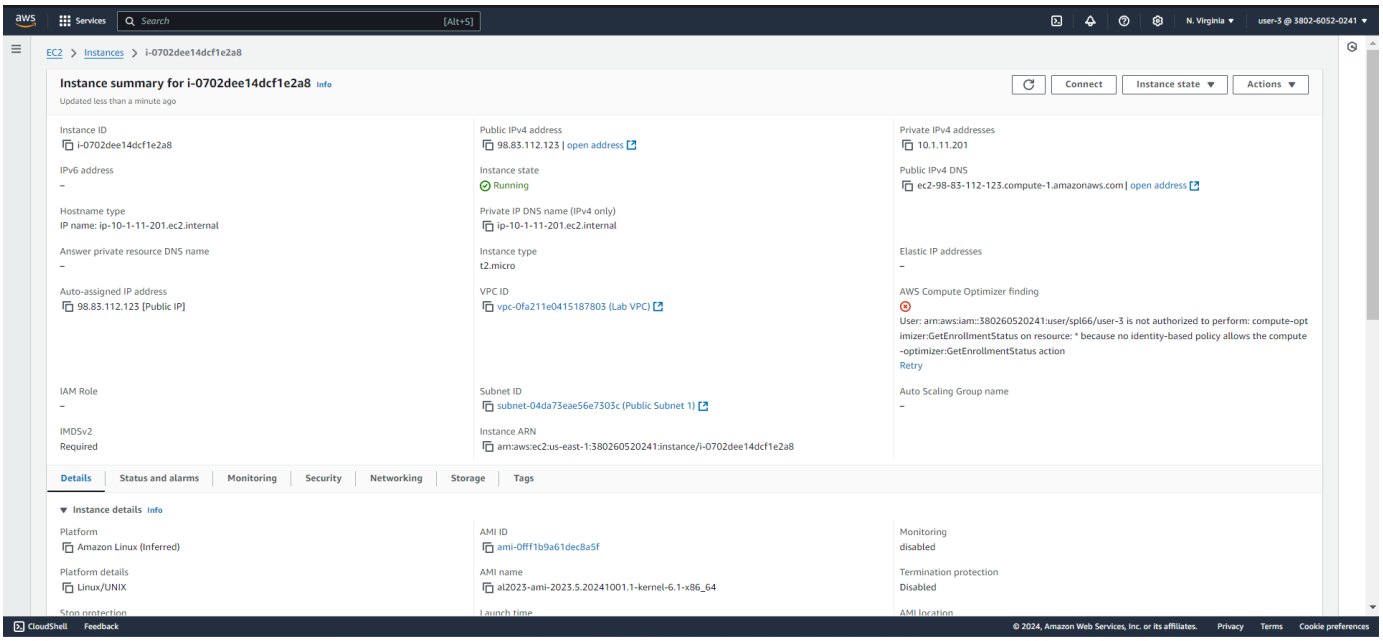
- **IAM user name:** user-3
- **Password:** Lab-Password3

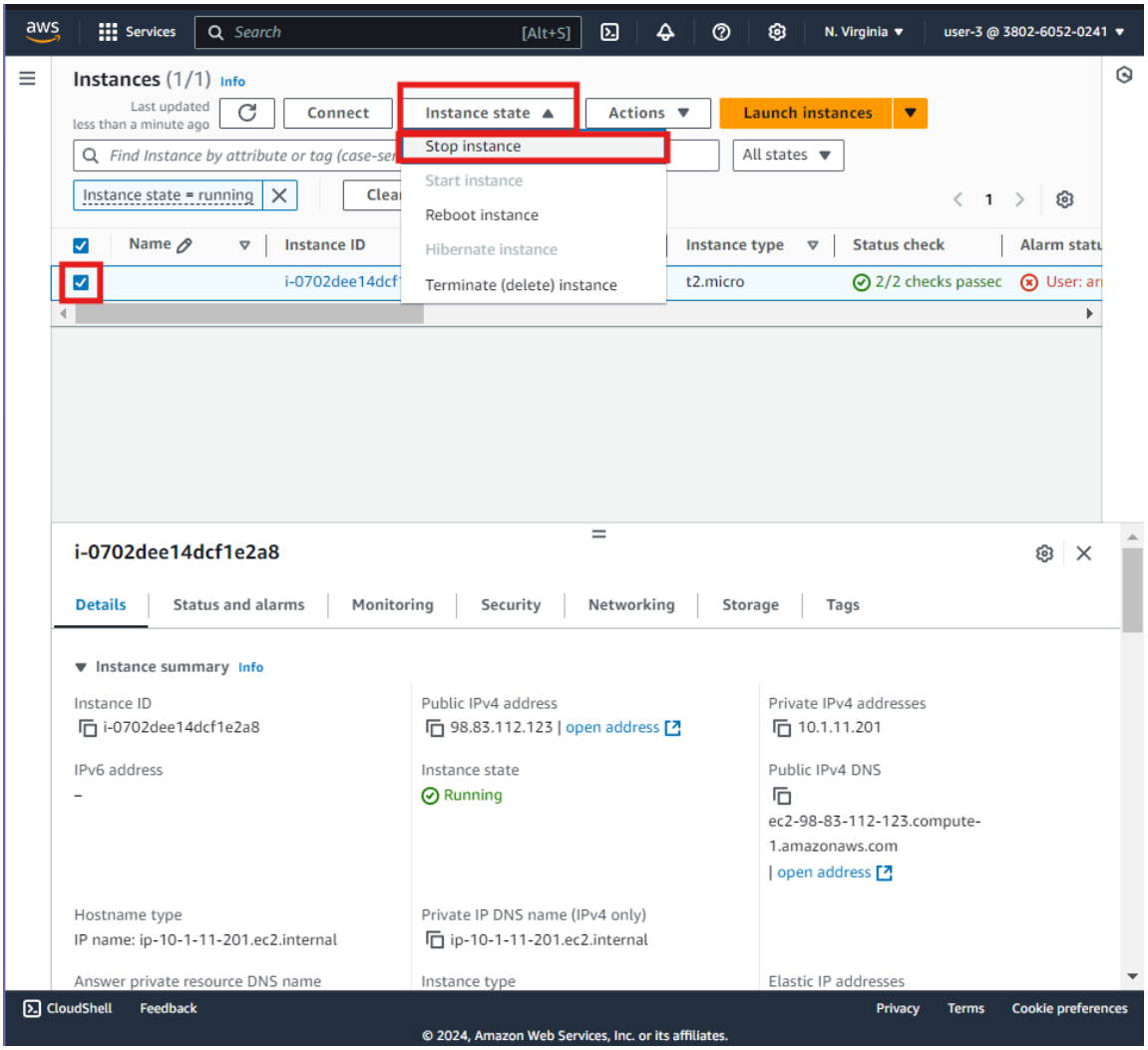


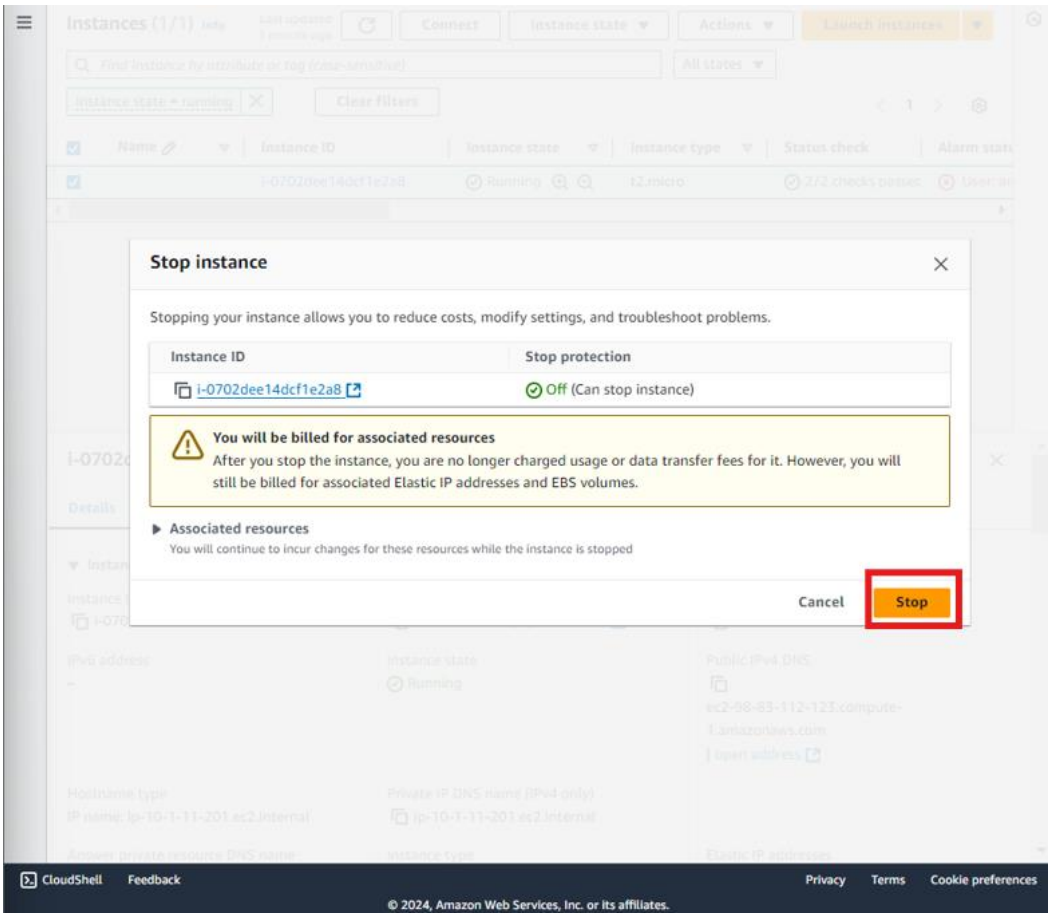


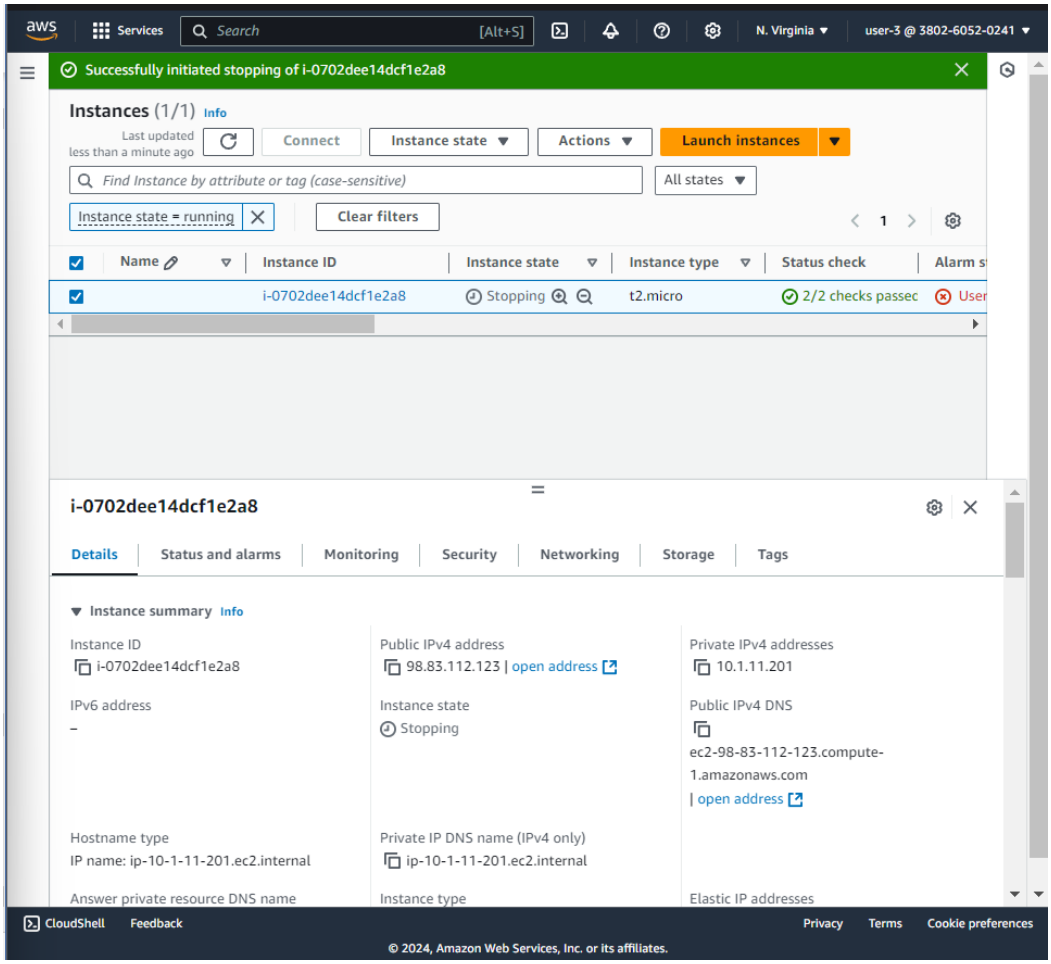

aws
Services
Search
[Alt+S]
N. Virginia
user-3 @ 3802-6052-0241
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:
Instances (running) 1
Auto Scaling Groups API Error
Capacity Reservations 0
Dedicated Hosts 0
Elastic IPs 0
Instances 1
Key pairs 1
Load balancers API Error
Placement groups 0
Security groups 3
Snapshots 0
Volumes 1
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the US East (N. Virginia) Region
Instance alarms
View in CloudWatch
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Diagnose with Amazon Q
Zones
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.

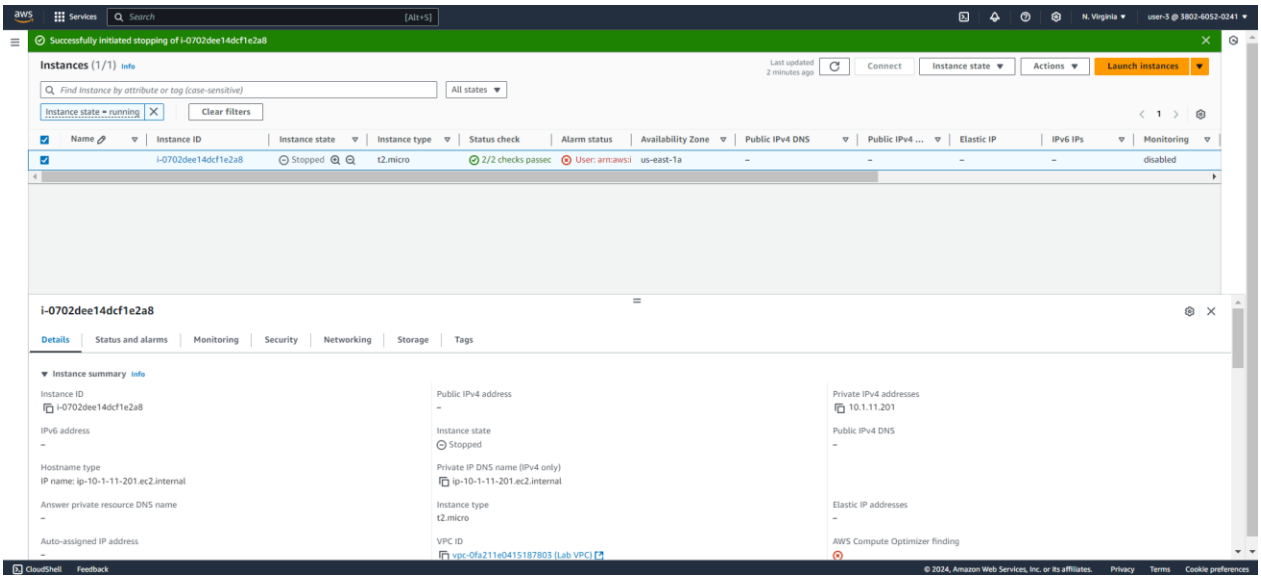

aws
Services
Search
[Alt+S]
N. Virginia
user-3 @ 3802-6052-0241
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm statu
i-0702dee14dcf1e2a8
Running
t2.micro
2/2 checks passed
User: ar
Select an instance
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.


aws
Services
Search
[Alt+S]
N. Virginia
user-3 @ 3802-6052-0241
EC2 > Instances > i-0702dee14dcf1e2a8
Instance summary for i-0702dee14dcf1e2a8 Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-0702dee14dcf1e2a8
IPv6 address
–
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Answer private resource DNS name
–
Auto-assigned IP address
98.83.112.123 [Public IP]
IAM Role
–
IMDSv2
Required
Public IPv4 address
98.83.112.123 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Instance type
t2.micro
VPC ID
vpc-0fa211e0415187803 (Lab VPC)
Subnet ID
subnet-04da73eae56e7303c (Public Subnet 1)
Instance ARN
arn:aws:ec2:us-east-1:380260520241:instance/i-0702dee14dcf1e2a8
Private IPv4 addresses
10.1.11.201
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com | open address
Elastic IP addresses
–
AWS Compute Optimizer finding
User: arn:aws:iam::380260520241:user/spl66/user-3 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Retry
Auto Scaling Group name
–
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details Info
Platform
Amazon Linux (Inferred)
Platform details
Linux/UNIX
AMI ID
ami-0fff1b9a61dec8a5f
AMI name
al2023-ami-2023.5.20241001.1-kernel-6.1-x86_64
Monitoring
disabled
Termination protection
Disabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
user-3 @ 3802-6052-0241
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
All states
Find Instance by attribute or tag (case-sen
Instance state = running
Clear
1
Name
Instance ID
Instance type
Status check
Alarm statu
i-0702dee14dcf
t2.micro
2/2 checks passed
User: ar
i-0702dee14dcf1e2a8
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0702dee14dcf1e2a8
IPv6 address
–
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Answer private resource DNS name
Public IPv4 address
98.83.112.123 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Instance type
Private IPv4 addresses
10.1.11.201
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com
| open address
Elastic IP addresses
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.


Stop instance
Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.
Instance ID
Stop protection
i-0702dee14dcf1e2a8
Off (Can stop instance)
You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.
Associated resources
You will continue to incur changes for these resources while the instance is stopped
Cancel
Stop
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.


aws
Services
Search
[Alt+S]
N. Virginia
user-3 @ 3802-6052-0241
Successfully initiated stopping of i-0702dee14dcf1e2a8
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
i-0702dee14dcf1e2a8
Stopping
t2.micro
2/2 checks passed
i-0702dee14dcf1e2a8
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0702dee14dcf1e2a8
Public IPv4 address
98.83.112.123 | open address
Private IPv4 addresses
10.1.11.201
IPv6 address
–
Instance state
Stopping
Public IPv4 DNS
ec2-98-83-112-123.compute-1.amazonaws.com
| open address
Hostname type
IP name: ip-10-1-11-201.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-11-201.ec2.internal
Answer private resource DNS name
Instance type
Elastic IP addresses
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.



Testing Permissions for Each User Using CLI

User-1 (S3-Support Group) - S3 Read-Only Access

User-1 should have read-only access to S3. You can test their permissions by attempting to perform the following operations:

1. **List S3 Buckets**:

- This will check if User-1 can list the available S3 buckets:

bash Copy code

```bash
aws s3 ls
```

- **Expected Result**: User-1 should be able to list the S3 buckets because they have `AmazonS3ReadOnlyAccess`.

2. **Attempt to Create a New Bucket**:

- This command attempts to create a new bucket, which should fail because User-1 has read-only access:

bash Copy code

```bash
aws s3api create-bucket --bucket test-user1-bucket --region us-west-2
```

- **Expected Result:** The command should **fail** because User-1 cannot perform write operations in S3.

3. **Attempt to Upload a File to S3**:

- This will check if User-1 can upload a file to S3 (which should fail):

bash Copy code

```bash
aws s3 cp testfile.txt s3://your-existing-bucket-name/
```

- **Expected Result:** This should also **fail**, as User-1 can only read from S3, not upload files.

User-2 (EC2-Support Group) - EC2 Read-Only Access

User-2 should have read-only access to EC2 resources. You can test their permissions with the following operations:

1. **List EC2 Instances**:

- Check if User-2 can list the EC2 instances:

bash Copy code

```bash
aws ec2 describe-instances
```

- **Expected Result:** User-2 should be able to list EC2 instances because they have read-only access.

2. **Attempt to Start or Stop an EC2 Instance**:

- This command tries to stop an EC2 instance, which should fail due to lack of permissions:

bash Copy code

```bash
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

- **Expected Result**: This should **fail** because User-2 has read-only access and cannot modify EC2 resources.

3. **Attempt to Launch a New EC2 Instance**:

- This command attempts to launch a new EC2 instance, which should fail:

bash Copy code

```bash
aws ec2 run-instances --image-id ami-0123456789abcdef0 --count 1 --instance-type t
```

- **Expected Result**: The command should **fail** because User-2 cannot perform actions that modify EC2 resources (read-only access).

User-3 (EC2-Admin Group) - EC2 Admin Access

User-3 has full admin access over EC2, so they should be able to perform both read and write operations.

1. **List EC2 Instances**:

- This will check if User-3 can view the EC2 instances:

bash Copy code

```bash
aws ec2 describe-instances
```

- **Expected Result**: User-3 should be able to see all the EC2 instances.

2. **Start or Stop an EC2 Instance**:

- Since User-3 has admin access, they should be able to stop an EC2 instance:

bash Copy code

```bash
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

- **Expected Result**: This should **succeed**, as User-3 has the necessary permissions to modify EC2 resources.

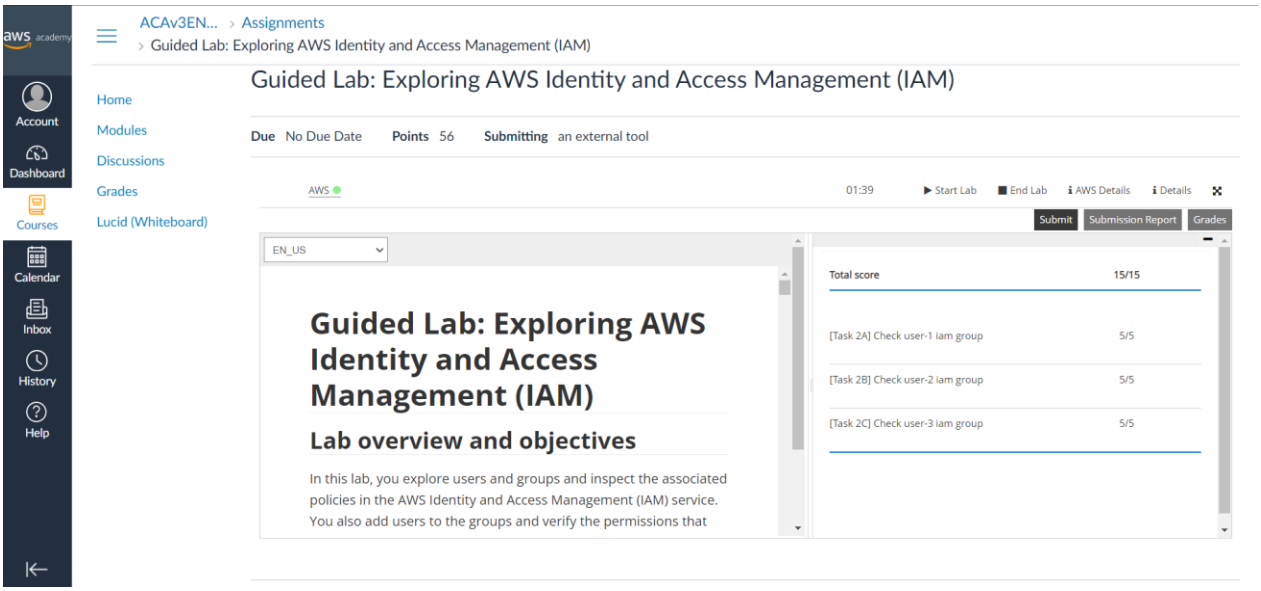
3. **Launch a New EC2 Instance**:

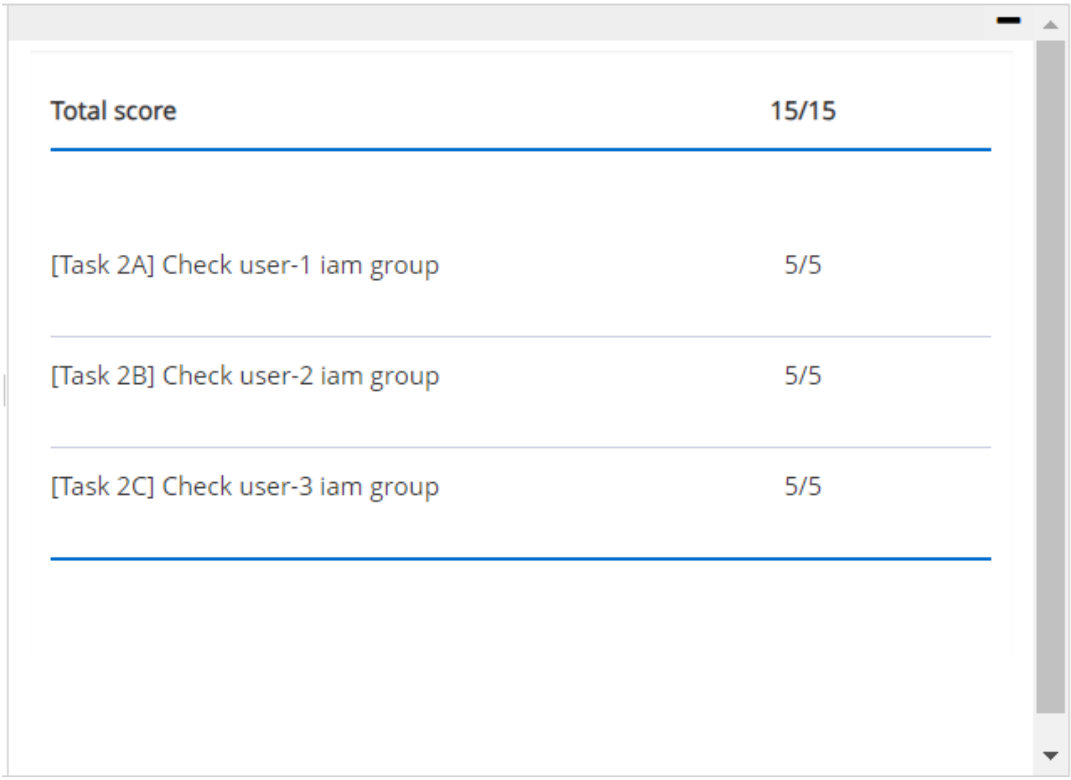
- Since User-3 has admin access, they should also be able to launch a new EC2 instance:

bash Copy code

```bash
aws ec2 run-instances --image-id ami-0123456789abcdef0 --count 1 --instance-type t
```

- **Expected Result**: This command should **succeed** for User-3, as they have full admin rights over EC2 resources.





Guided Lab: Exploring AWS Identity and Access Management (IAM) Lab Assignments	Oct 6 at 12:18am	56 / 56