

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=ASIAVRCKLCEY40KG4D23
aws_secret_access_key=ECBvsPonSd+msJcwprQJnphbi7MAj9L29MXkeNlj
aws_session_token=IQoJb3JpZ2luX2VjEK//////////wEaCXVzLXdlc3QtMiJHMEUCIQCb0pgfFnE2
rXBiIDySKXsXg5pgEpa0p76F3VPnbbNg/QIgdh+Ny8dwLlx/EIk5VX7n2Sdw1Aj5//GQKxuNEjqsEvUquA
II+P//////////ARAAGgwzODAyNjA1MjAyNDEiDC6tozhmwif5ooSRnyqMAN8chj0/Gm+8FPKL0k1ze/4P
dJS3b071Au9cBo1UD65nV/zusJqJ8umkEaR/Zu8VmhdX1UpRNmefA0050tKof7mtdMwHe0cXAc4hIZ7Kzt
qDVWqVD4TqQhfoBb1G67xy0vgS21ILZDAkQMdFSgwu1+A3xCJw9vNetvoDDx084VgOeeLPruY0N9OLFET
IFYigu111z5ujJkABMvaqn0qZKDcxk70KfiXbJP3EK4+Lee0i4NVTiwFuMPvknN58qPxrtjQ0+q7aqhQXH
JiMQ48DbXuADvQmNBPE5jCdWPdFnJWXYnLAHJrqc+HymPW4HTk2CzmcElC9egyQ0kLHNgnfo6KbcCfzh3i
Qg1hTEYw6oiHuAY6nQFVrILOouZ6B0Zv0kaw6LJrxGverQaqEVsCdZLSWkEC4Q85dE/ZFy2CbYQmpCqE/E
dhNv3E2tz2ZmBiLkr3TAqeXkaNB8aUQr6IesHZS6Z1cFz3a0j6eMLhcybsRh+QpWHCcSffnwVULZDuxBOu
lbmLh58YINWBVKg8pn3JVQk+gzAp6BYruEB2iPAfzwgFYXg0siiIorDQ8iEtT9GY
```

4. Configure AWS CLI

- Open Command Prompt (cmd) on your Windows machine.
- Enter the following command to start the configuration

process:

```
bash Copy code
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]

The screenshot displays the AWS Academy guided lab interface for "Exploring AWS Identity and Access Management (IAM)". The interface includes a sidebar with navigation options like Home, Modules, Dashboard, Courses, Calendar, Inbox, History, and Help. The main content area shows the lab title and a progress bar. A command prompt window is open, showing the execution of the `aws configure` command. The prompt asks for the AWS Access Key ID, AWS Secret Access Key, Default region name, and Default output format. The user has entered the following values:

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

To the right of the command prompt, a "Cloud Access" panel is visible, displaying the AWS CLI configuration. It includes the AWS CLI command to copy and paste the following into `~/.aws/credentials`:

```
[default]
aws_access_key_id=ASIAVRCKLCEY40KG4D23
aws_secret_access_key=ECBvsPon5d+ms7cWprQ7nphbi7MAj9L29H0Xke
Nlj
aws_session_token=IQo7b3p22luX2VjEK//////////wEaCXVzLXdlc
3qtMl7HMEUCIQcb0pgfFnE2+XB1IDySKXsXg5pgEa0p76F3VPnbbNg/QIg
dh+Ny8dvlLx/EIk5VX7n25dvlAj5//GQKxuHEjqsEvUquAII+
P//////////ARAAGwuzODayHJA1M3AyNDE1DC6tozhmwf5ooS8nyqMan8c
h30/Gm+8FPKL0k1ze/4Pd353b071Au9cBo1UD65nV/zus7q38umkEaR/Zu8
VmhX1lpBImeFAQ050tKof7etdHw0cXAc4hIZ7KztqDvWqV04TqHfoBb
1G67xyOvg521L1ZDAkQMf5guw1+43xC3w9vHetvoD0x084VgDeeLPruYBN
90LFtTIFYIgu111z5u3j3kABHvaqn0qZK0ck70Kf1xb3P3EK4+Lee0i4Nv
TiuFwPvkN58qPartjQ0+q7aahQX031MQ48DbXuADvQmBPE5JCdWpDfn3
```

Task 1: Explore Users and Groups

1. List All IAM Users

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

```
bash
```

[Copy code](#)

```
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": "AIDAVRCKLCEY5A07VVC17",
      "Arn": "arn:aws:iam::380260520241:user/spl66/user-1",
      "CreateDate": "2024-10-05T22:57:49+00:00"
    },
    {
      "Path": "/spl66/",
      "UserName": "user-2",
      "UserId": "AIDAVRCKLCEYR6Z05TH5Z",
      "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

 Copy code

```
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

 Copy code

```
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": "AIDAVRCKLCEY5A07VVC17",
    "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": "AIDAVRCKLCEYR6Z05TH5Z",
    "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

 Copy code

```
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": "AGPAVRCKLCEYQGERRWBG",
    "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

 Copy code

```
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

```
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": "AIDAVRCKLCEY5A07VVC17",
      "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": "AIDAVRCKLCEYR6Z05TH5Z",
      "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

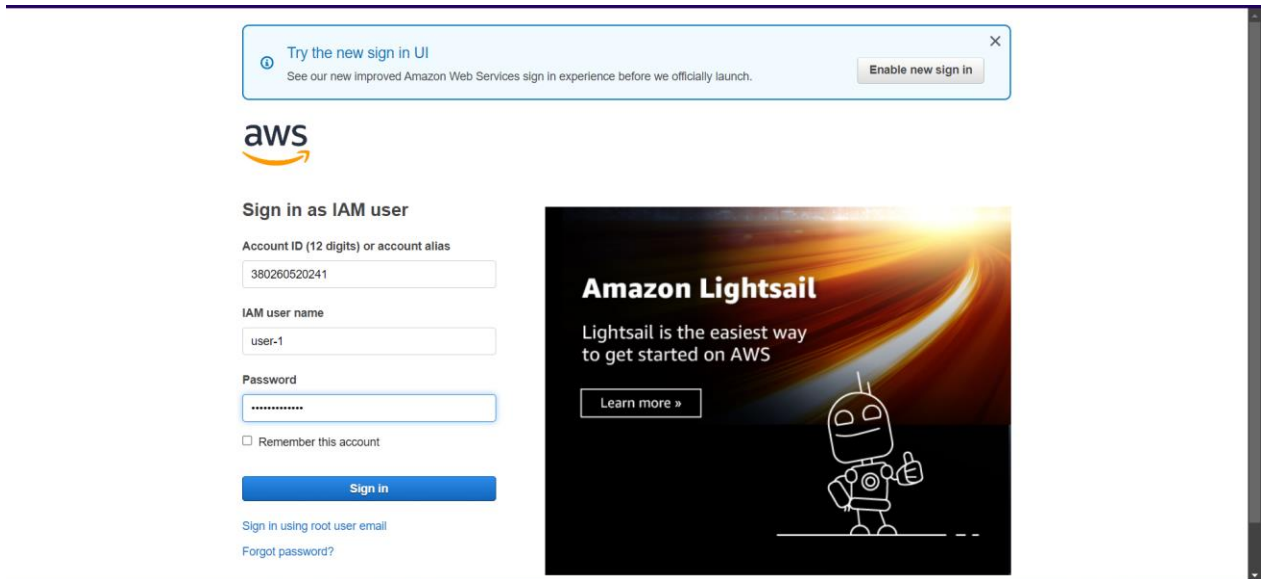
- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.

The top screenshot shows the AWS Management Console 'Console Home' page. The 'Recently visited' section on the left has a red box around the 'IAM' link. The 'Applications' section on the right shows a table with no applications listed. The 'Welcome to AWS' section on the bottom left contains links for 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. The 'AWS Health' section on the bottom middle shows 'Open issues', 'Scheduled changes', and 'Other notifications'. The 'Cost and usage' section on the bottom right shows a bar chart for 'Current month costs' and 'Forecasted month-end costs'.

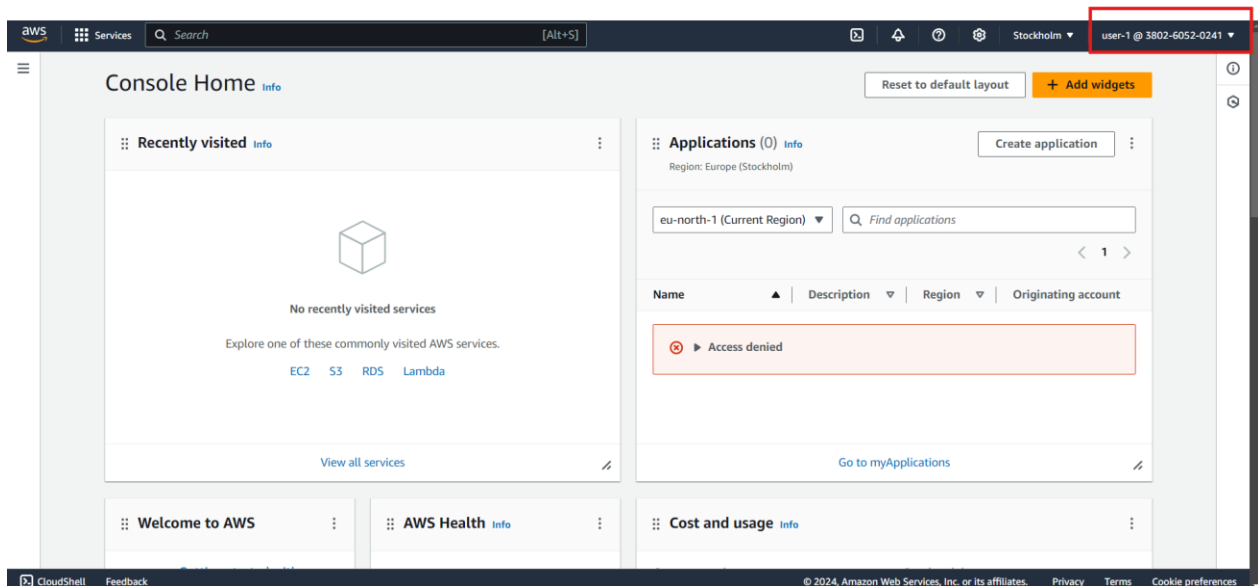
The bottom screenshot shows the 'IAM Dashboard'. The 'IAM resources' section displays a table with 3 user groups, 3 users, 14 roles, 0 policies, and 0 identity providers. The 'What's new' section lists updates for IAM features. The 'AWS Account' section on the right has a red box around the 'Sign-in URL' for IAM users in this account, which is <https://380260520241.signin.aws.amazon.com/console>. The 'Tools' section includes a 'Policy simulator' link. The 'Additional information' section lists 'Security best practices in IAM', 'IAM documentation', and 'Videos, blog posts, and additional resources'.

Task 4.2: Test user-1 permissions

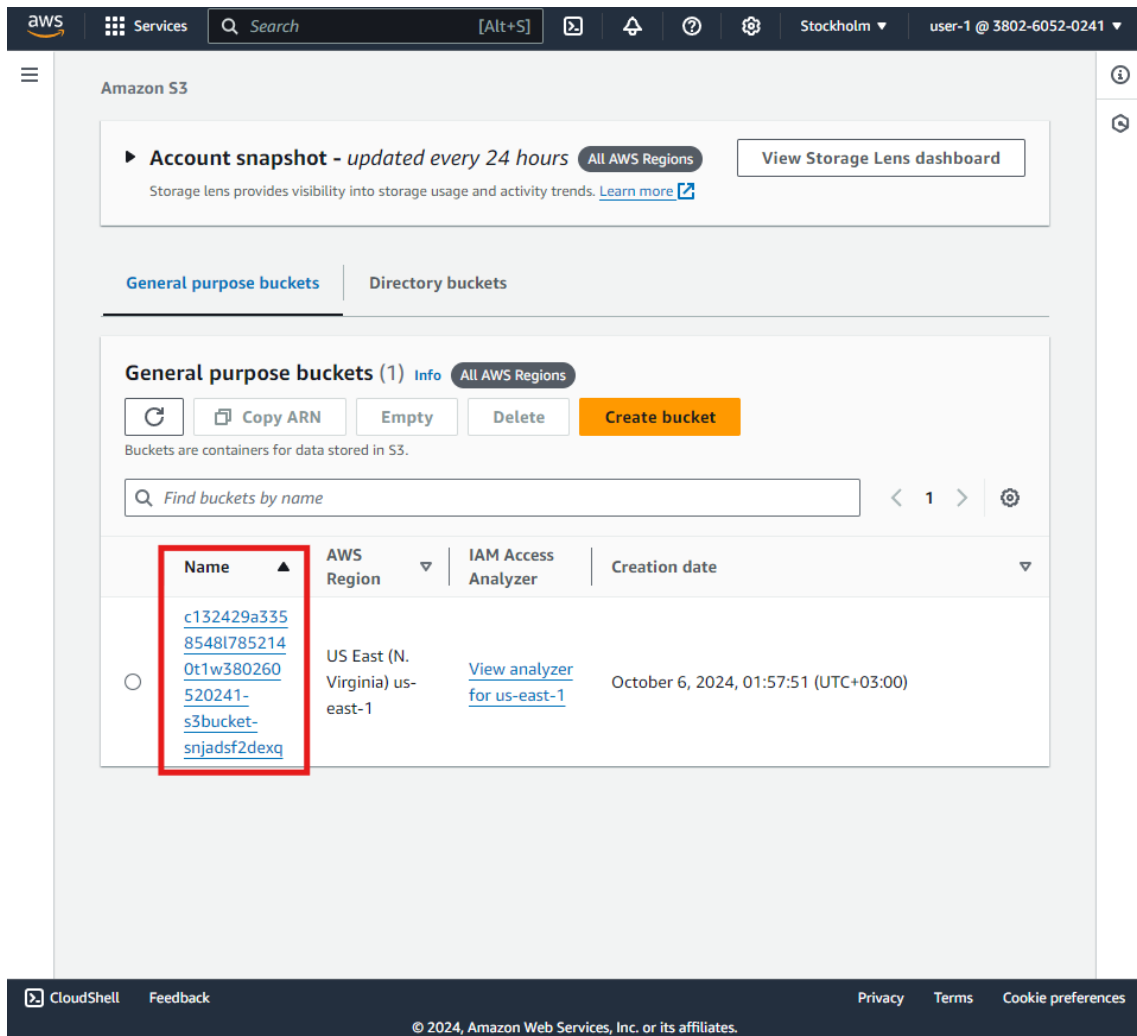
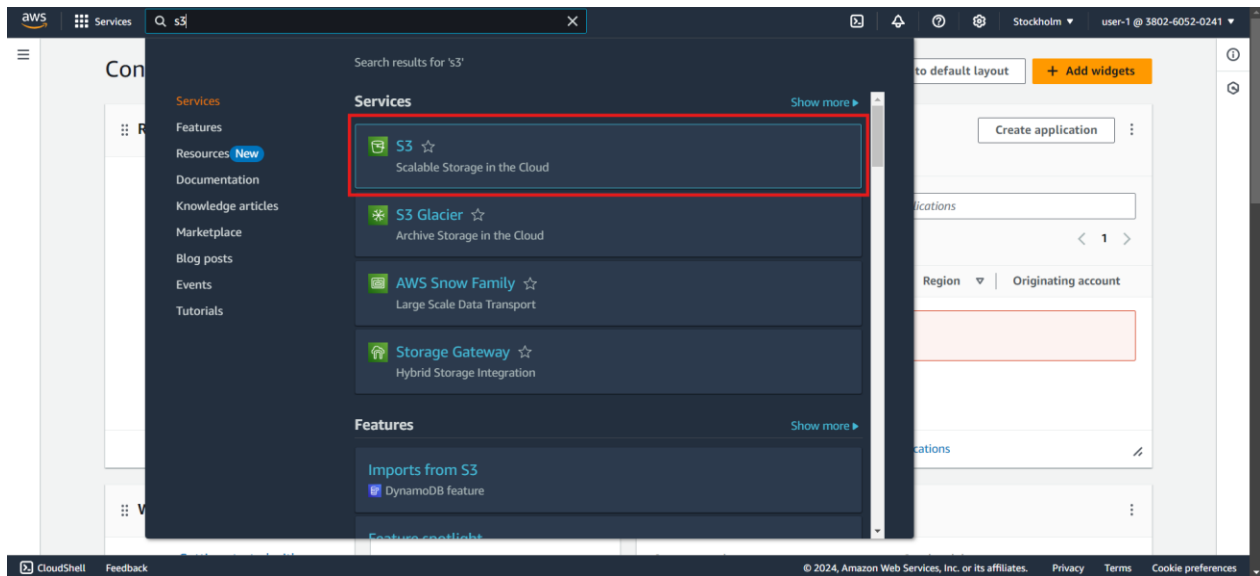
2. Open a private or incognito window in your browser.
3. Paste the sign-in link into the private browser, and press ENTER.
4. Sign in with the following credentials:
 - **IAM user name:** user-1
 - **Password:** Lab-Password1

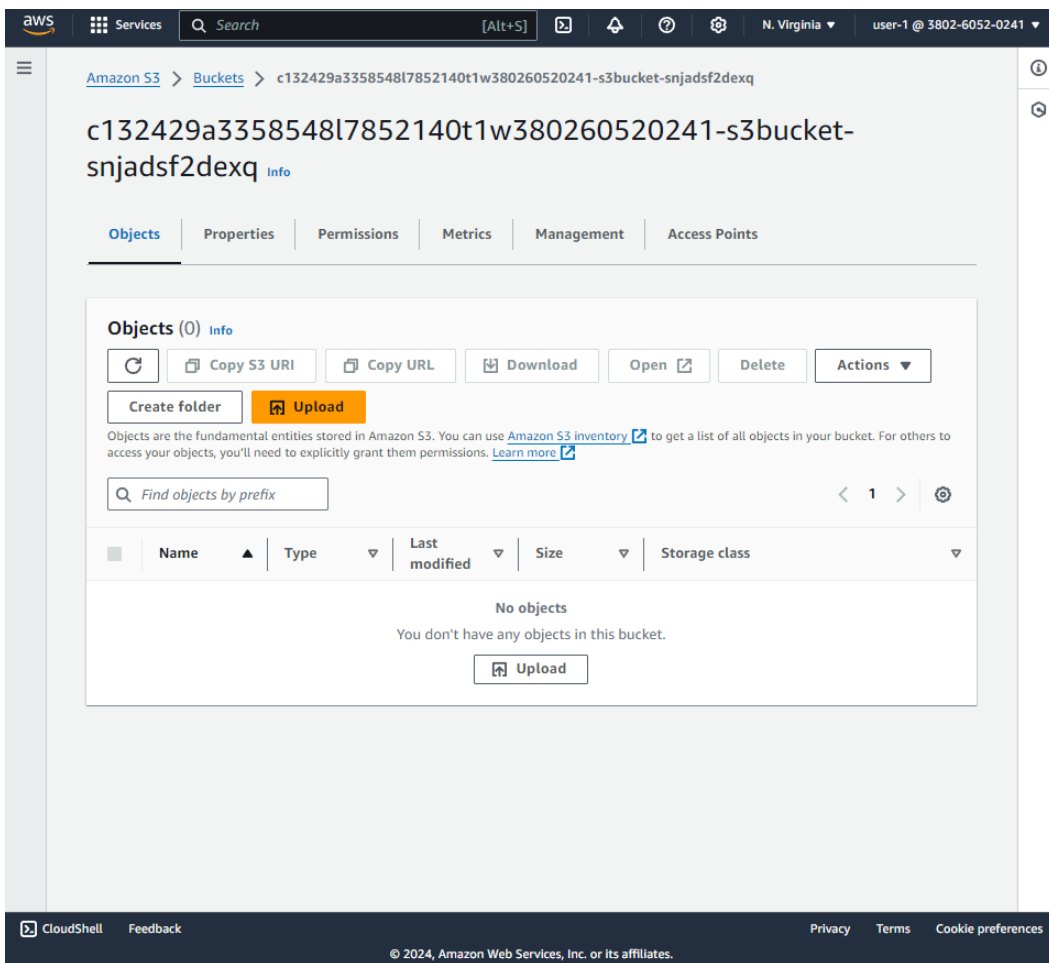


The screenshot shows the AWS IAM user sign-in interface. At the top, there is a notification banner about a new sign-in UI. Below this is the AWS logo and the heading "Sign in as IAM user". The form includes fields for "Account ID (12 digits) or account alias" (pre-filled with 380260520241), "IAM user name" (pre-filled with user-1), and "Password" (masked with dots). There is a checkbox for "Remember this account" and a "Sign in" button. Below the button are links for "Sign in using root user email" and "Forgot password?". To the right of the form is a promotional banner for "Amazon Lightsail" with the text "Lightsail is the easiest way to get started on AWS" and a "Learn more" button. The banner also features a cartoon robot character.

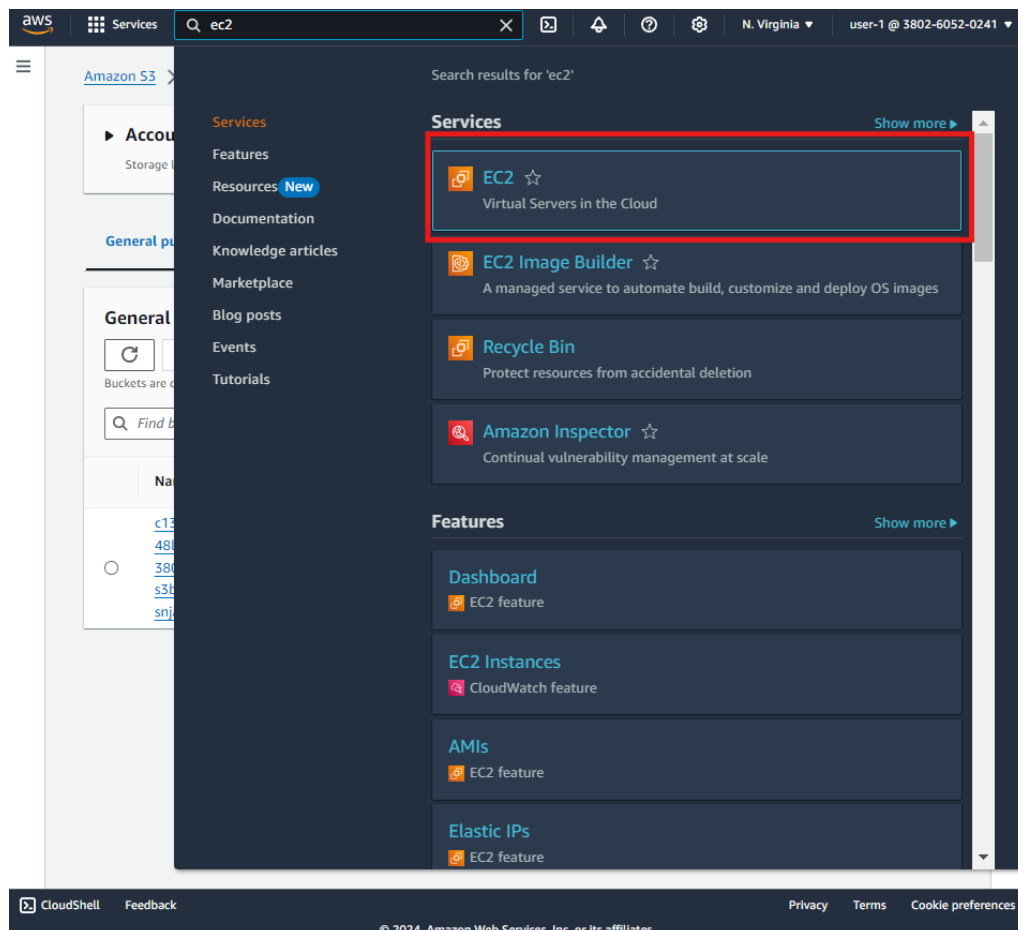


5. Navigate to the S3 service and try to list buckets.





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

Capacity Reservations

Dedicated Hosts

Elastic IPs

Instances

Key pairs

Load balancers

Placement groups

Security groups

Snapshots

Volumes

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instanceMigrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

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

Service health

AWS Health Dashboard

An error occurred

An error occurred retrieving service health information

Diagnose with Amazon Q

Zones

Zone nameZone ID

An error occurred

An error occurred retrieving service health information

Enable additional Zones

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

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

Additional information

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

aws

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

Name

Instance ID

Instance state

Instance type

Status check

Alarm statu

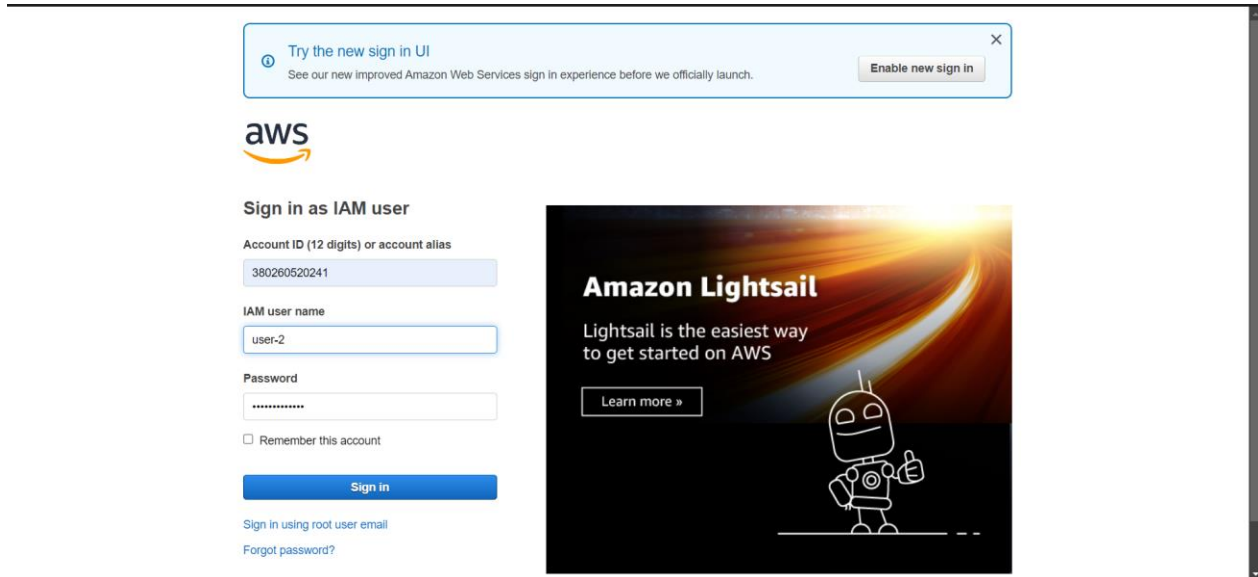
You are not authorized to perform this operation. User: arn:aws:iam::380260520241:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

Select an instance

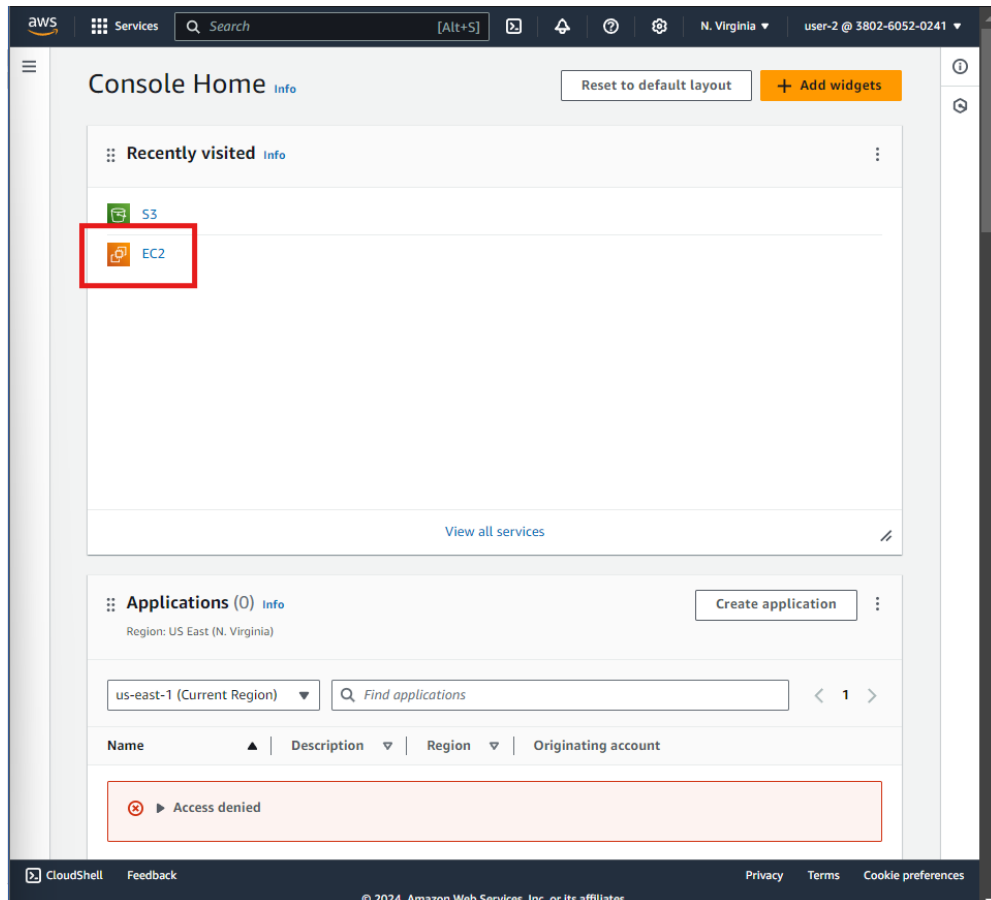
Task 4.3: Test user-2 permissions

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



aws

Services

Search

[Alt+S]

N. Virginia

user-2 @ 3802-6052-0241

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

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

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

Instance alarms

View in CloudWatch

0 in alarm

OK

0 insufficient data

Instances in alarm

Scheduled events

US East (N. Virginia)

Account attributes

Default VPC

vpc-0cb40b66eca789fd

Settings

Data protection and security

Zones

EC2 Serial Console

Default credit specification

EC2 console preferences

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

Additional information

Getting started guide

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

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

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
		i-0702dee14dcf1e2a8	Running	t2.micro	2/2 checks passed	View alarms

Select an instance

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Instance summary for i-0702dee14dcf1e2a8

Updated less than a minute ago

Instance ID: i-0702dee14dcf1e2a8

Public IPv4 address: 98.83.112.123 | open address

Instance state: Running

Private IPv4 addresses: 10.1.11.201

Public IPv4 DNS: ec2-98-83-112-123.compute-1.amazonaws.com | open address

Private IPv4 DNS name (IPv4 only): ip-10-1-11-201.ec2.internal

Instance type: t2.micro

VPC ID: vpc-0fa211e0415187803 (Lab VPC)

Subnet ID: subnet-04da73ae56e7303c (Public Subnet 1)

Instance ARN: arn:aws:ec2:us-east-1:380260520241:instance/i-0702dee14dcf1e2a8

Platform: Amazon Linux (Inferred)

AMI ID: ami-0ff1b9u61dec8a5f

AMI name: al2023-ami-2023.5.20241001.1-kernel-6.1-x86_64

Monitoring: disabled

Termination protection: Disabled

AMI location

Instances (1/1) Info

Last updated less than a minute ago

Connect

Instance state

Stop instance

Start instance

Reboot instance

Hibernate instance

Terminate (delete) instance

Launch instances

Find Instance by attribute or tag (case-sensitive)

Instance state = running

Clear

1

Instance type: t2.micro

Status check: 2/2 checks passed

Alarm status

i-0702dee14dcf1e2a8

Details

Instance summary

Instance ID: i-0702dee14dcf1e2a8

Public IPv4 address: 98.83.112.123 | open address

Instance state: Running

Private IPv4 addresses: 10.1.11.201

Public IPv4 DNS: ec2-98-83-112-123.compute-1.amazonaws.com | open address

Private IP DNS name (IPv4 only): ip-10-1-11-201.ec2.internal

Instance type: t2.micro

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 Last updated 3 minutes 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 status
	i-0702dee14dcf1e2a8	Running	t2.micro	2/2 checks passed	View alarms

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**

Instance details

Instance ID	i-0702dee14dcf1e2a8
IPv6 address	-
Hostname type	-
IP name	ip-10-1-11-201.ec2.internal
Answer private resource DNS name	-
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-1-11-201.ec2.internal
Instance type	t2.micro
Public IPv4 DNS	ec2-98-83-112-123.compute-1.amazonaws.com open address
Elastic IP addresses	-

CloudShell Feedback Privacy Terms Cookie preferences

Failed to stop the instance i-0702dee14dcf1e2a8

You are not authorized to perform this operation. User: arn:aws:iam::380260520241:user/jpl66/jerr-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:380260520241:instance/i-0702dee14dcf1e2a8 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: aow4S3M-QUB0Kd3WVW6d6wP_8_ZDU5-4atfB0yBDSwYwdf8f8b0Nqk4T0CenKpC3U9P5d7YnZK3qy3u-CA3NtWefdfBy-prm8rh5v0VCvC2B8R8qXMJOYp5gmAlDzgvCO_c4CkRksoo-8a2dMcJdFz_EfpmnnE8z08BD8bmDWHATJueN0XTauF3A4qg4e4TLzpg8F7bX2D15dH43W/C19S5tmWt0zodc.cLU4R98CmT14_jw5wtb8Qg_OhJSPGdZ2PV0RthYKFP3h0m5eImCRLK-uOQd-fK-4_RY7Pwq5dZ28NMyPmz_yYHWH5g8a_bjvBUtey-aOxz00XTXAHmL1TZDKJ50BKIKvZauv9fKxsv23Ub_3V7JdU-2b3AUhdP6V9Y4x8B8nK5XYKz7YzRWV5UJ24vTok9r5nZAH-H6mD_K7YmN245MkefAT2T6Tm3IbeY6VpCJLGEKMYKocSpVchL51f0D4F61QDVICKc60ML4edK5w7K50CamVBF0f8kUJ064K0Le_O893pUHzalmTWL3F4loD_GKdZRaT8YK8T6s_d8holb-otxxR3CA7dGUKgWdZ8Yc-brATJbyQ9pb-4J866BvlgcwUjUwIsSdhsSHQdqp-jhJv3deSK_g8hxxYndqX0ZPKwI0BQVLMXg562k_rgeUIdoGSYAF5F1jpeH8YXq8hVNd3GGrhCQ15767BWfG5D0By-N-pVhaP81CplQ22z3JecZPFOtAqusaPal3gNMumTAQ2wa-g5pGCKASRuvYhQY832v20qgHgnW52pfr0svMN1GW3631td44d0mNj8deN5o2CX7JB-5ed-WL3_2jprRTK-Uax_LKEdphr_SlCd8m-z8fP45ofIqG8DvJv35uUJA1Tf3YCK2D1PFC16hAQmKqptp8Dpde-JD2t840XM-SkzvC48_K6gOfwUkXaeU4Vt59V

Instances (1/1) Info Last updated 4 minutes 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 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	Public IPv4 address
i-0702dee14dcf1e2a8	98.83.112.123 open address
IPv6 address	Private IPv4 addresses
-	10.1.11.201
Hostname type	Public IPv4 DNS
IP name	ec2-98-83-112-123.compute-1.amazonaws.com open address
Answer private resource DNS name	Elastic IP addresses
-	-
Auto-assigned IP address	AWS Compute Optimizer finding
98.83.112.123 (Public IP)	vpc-0fa211e045187803 (lab VPC)


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

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
Enable new sign in



Sign in as IAM user

Account ID (12 digits) or account alias
380260520241

IAM user name
user-3

Password

☐ Remember this account


Sign in

[Sign in using root user email](#)
[Forgot password?](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more »





aws Services Search [Alt+S] N. Virginia user-3 @ 3802-6052-0241

Console Home

Reset to default layout Add widgets

Recently visited

 S3

 EC2

View all services

Applications (0)

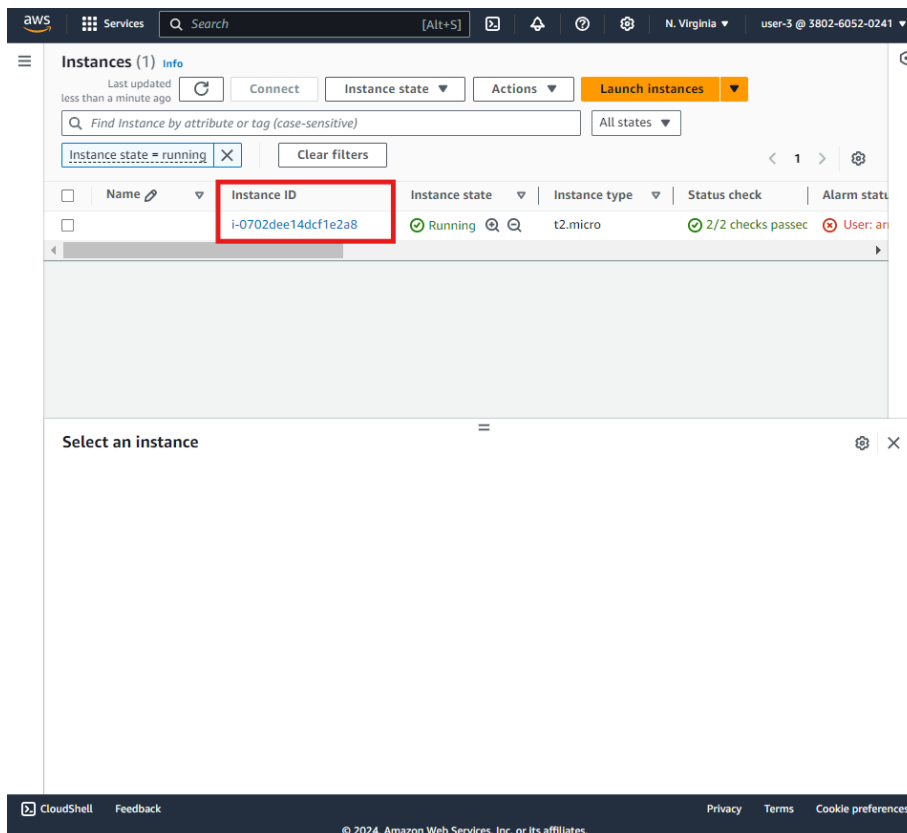
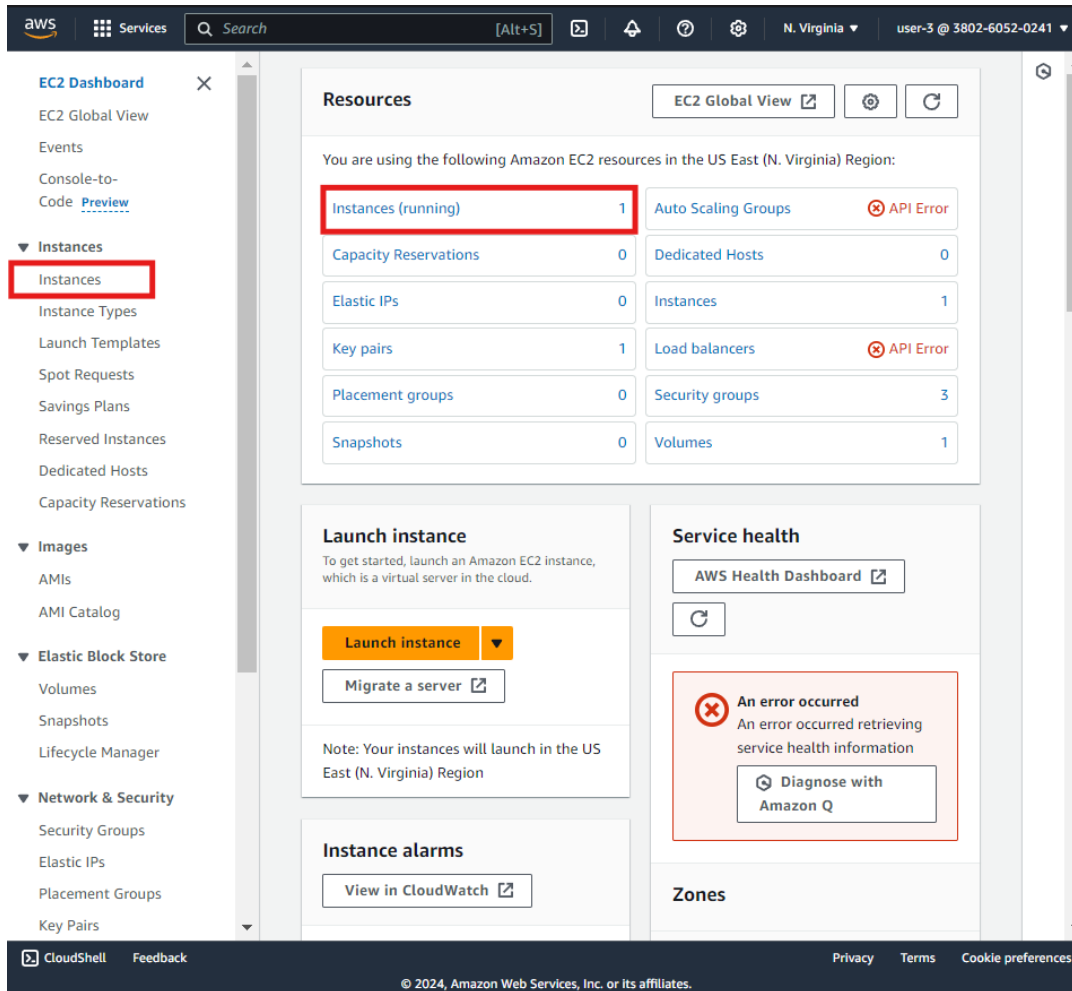
Create application

Region: US East (N. Virginia)

us-east-1 (Current Region) Find applications < 1 >

Name	Description	Region	Originating account
Access denied			

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

EC2 > Instances > i-0702dee14dcf1e2a8

Instance summary for i-0702dee14dcf1e2a8

Updated less than a minute ago

Connect Instance state Actions

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	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding User: amawsiam: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-assigned IP address 98.83.112.123 [Public IP]	VPC ID vpc-0fa211e0415187803 (Lab VPC)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-04da73eae56e7303c (Public Subnet 1)	
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 Info

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
Stop protection -	Launch time -	AMI location -

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

Find Instance by attribute or tag (case-sensitive)

Instance state = running Clear

<input checked="" type="checkbox"/>	Name	Instance ID
<input checked="" type="checkbox"/>		i-0702dee14dcf1e2a8

Stop instance

Start instance

Reboot instance

Hibernate instance

Terminate (delete) instance

Instance type Status check Alarm status

t2.micro 2/2 checks passed User: ar

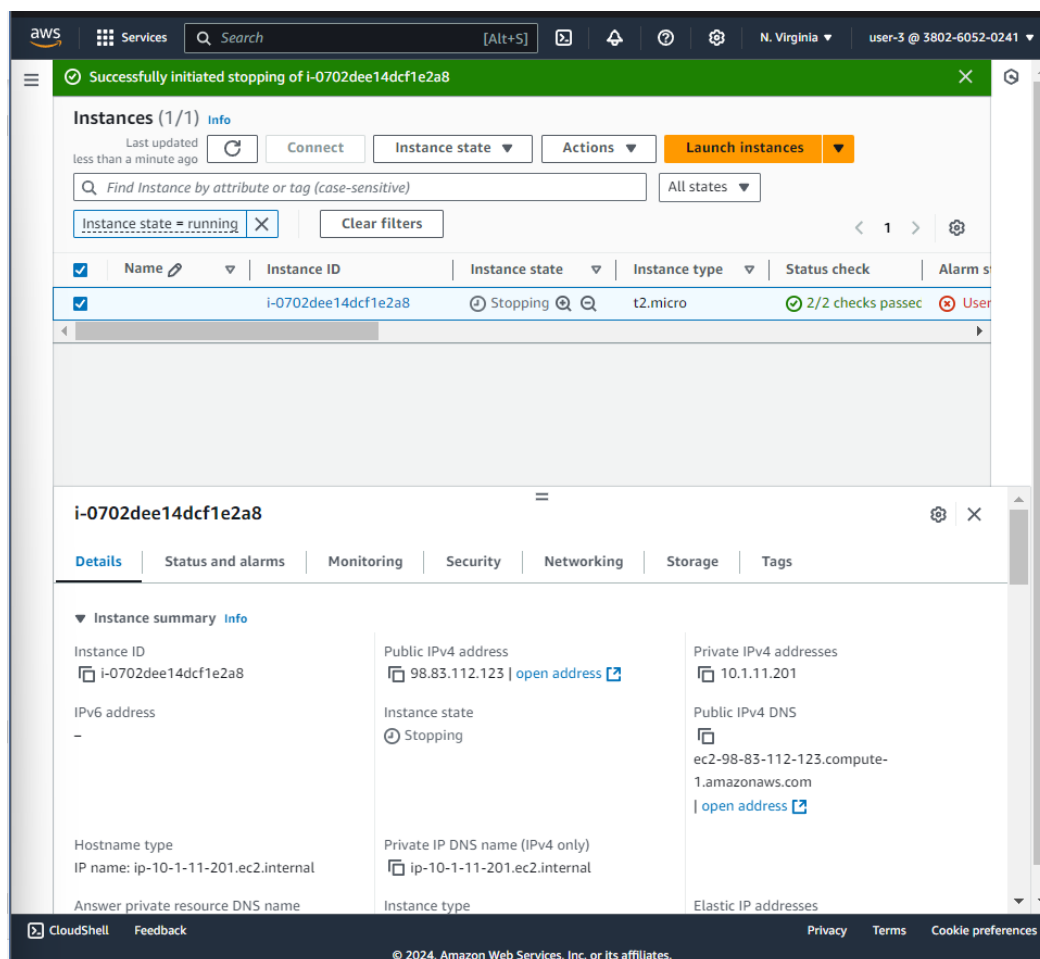
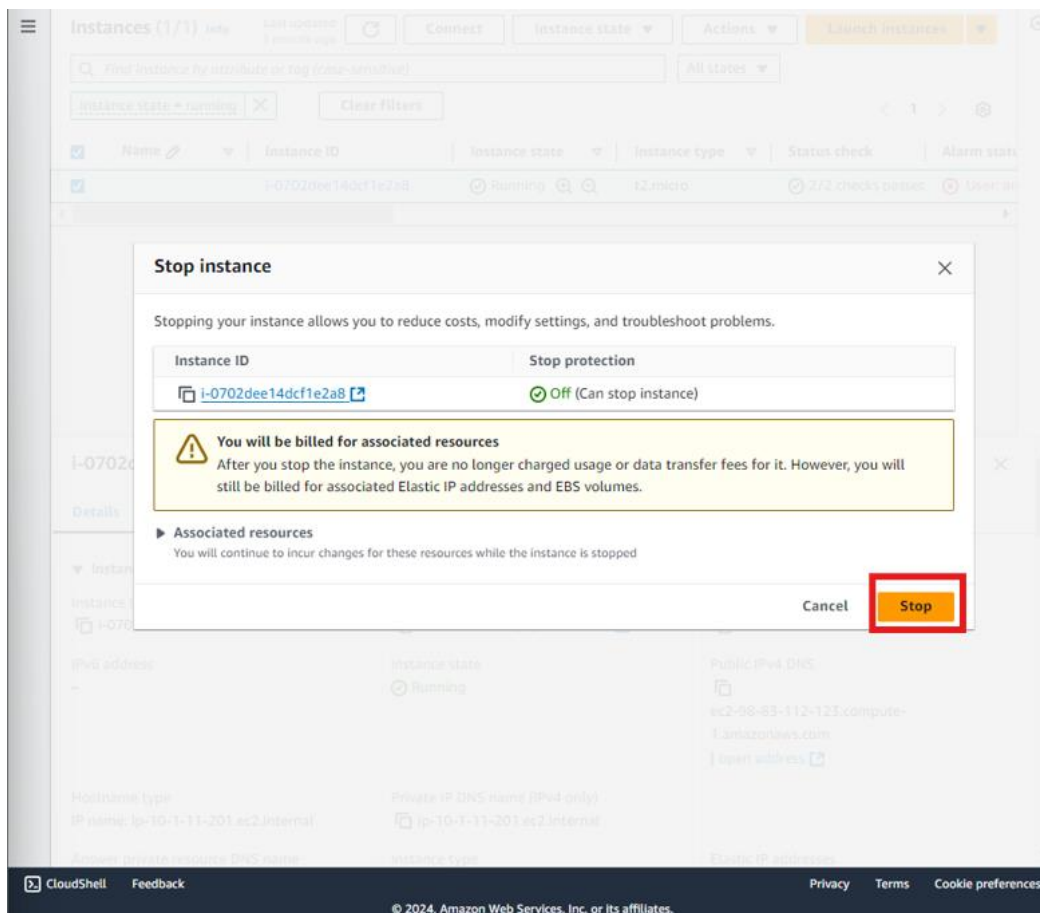
i-0702dee14dcf1e2a8

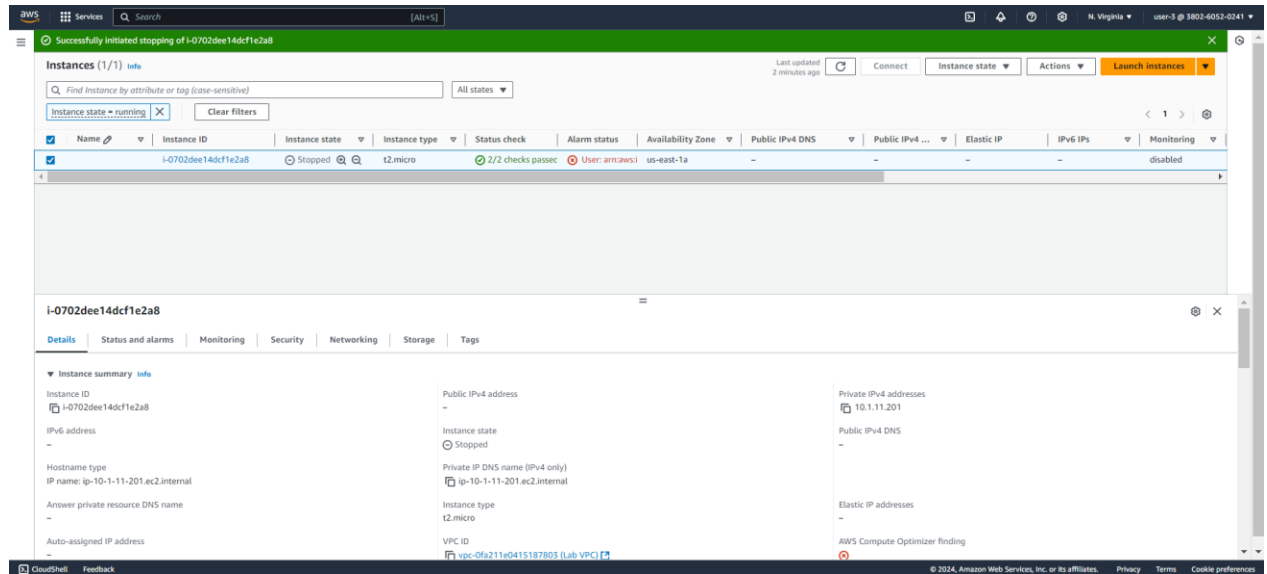
Details Status and alarms Monitoring Security Networking Storage Tags

▼ Instance summary Info

Instance ID i-0702dee14dcf1e2a8	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	Elastic IP addresses -
Answer private resource DNS name -	Instance type -	

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences





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](#)

```
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](#)

```
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](#)

```
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](#)


```
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


```
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

```
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


```
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


```
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

```
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.

aws academy

Account

Dashboard

Courses

Calendar

Inbox

History

Help

ACAv3EN... > Assignments

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

Home

Modules

Discussions

Grades

Lucid (Whiteboard)

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

Due No Due Date Points 56 Submitting an external tool

AWS

01:39 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Details ✕

Submit Submission Report Grades

EN_US

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

Total score15/15

[Task 2A] Check user-1 iam group5/5

[Task 2B] Check user-2 iam group5/5

[Task 2C] Check user-3 iam group5/5

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 Assignments

Oct 6 at
12:18am

56 / 56