NAME: Ikem Mercy Ogechi

STUDENT ID: 8859960

COURSE CODE: INFO8855-23S

PROFESSOR NAME: Prof. Nadeem.

DUE DATE: 31st May 2023

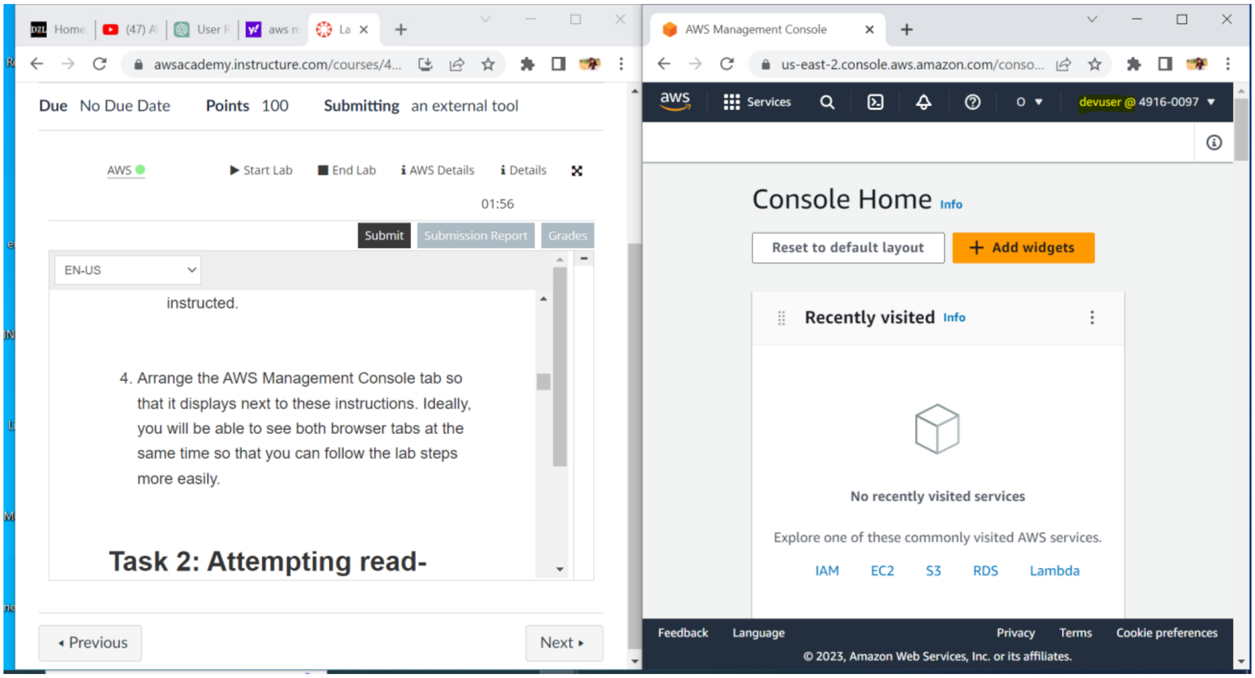
Contents

TASK 1- Accessing the console as an IAM user

DESCRIPTION

In Task 1, I am going to access the AWS Management console an IAM (Identity and Access Management) user using **devuser**. The console will be displayed on my browser, and I will be able to perform various tasks and resources with my assigned permissions as an IAM user.

SCREENSHOT



Due No Due Date Points 100 Submitting an external tool

instructed.

4. Arrange the AWS Management Console tab so that it displays next to these instructions. Ideally, you will be able to see both browser tabs at the same time so that you can follow the lab steps more easily.

Task 2: Attempting read-

No recently visited services

Explore one of these commonly visited AWS services.

© 2023, Amazon Web Services, Inc. or its affiliates.

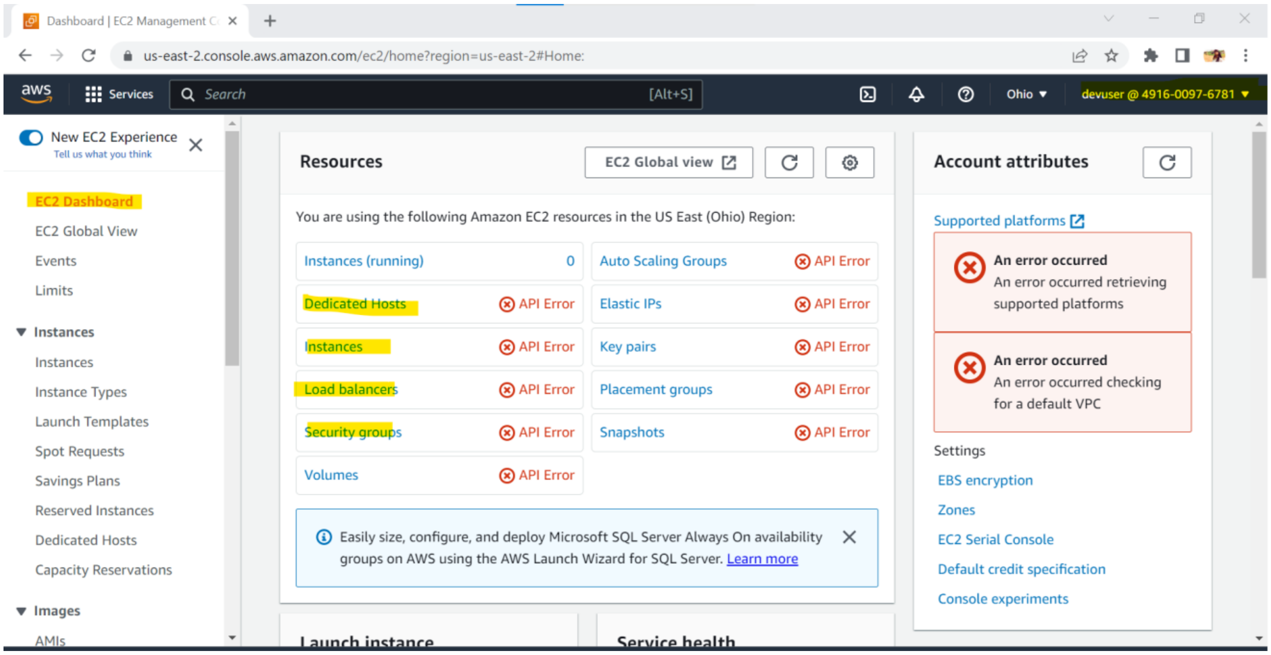
Fig 1 showing that I have access the console as devuser

TASK 2- Attempting read-level access to AWS services

DESCRIPTION

In this task, I will access the level of read-level access I have as IAM user named devuser to certain AWS services like Amazon EC2 and Amazon S3. I will be exploring the console and restrictions enforced by my current permissions.

SCREENSHOT



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	0	Auto Scaling Groups	⊗ 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		

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Account attributes

Supported platforms

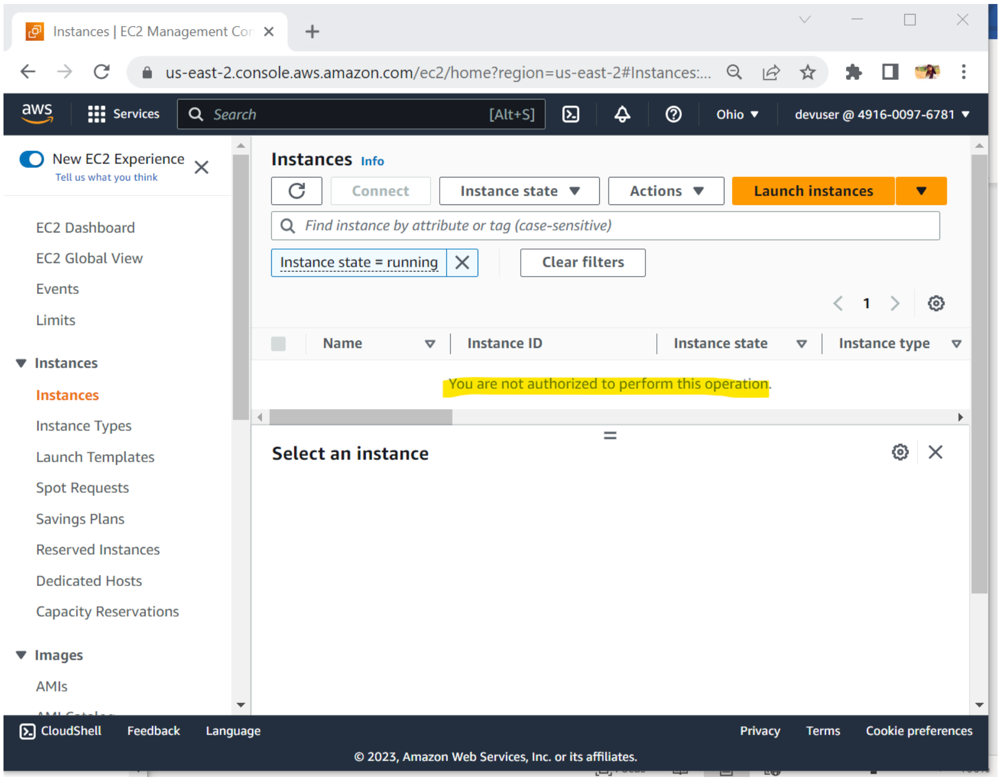
An error occurred
An error occurred retrieving supported platforms

An error occurred
An error occurred checking for a default VPC

Settings

EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments

Fig 2 showing the API Error messages when I went to the EC2 dashboard.



Instances Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

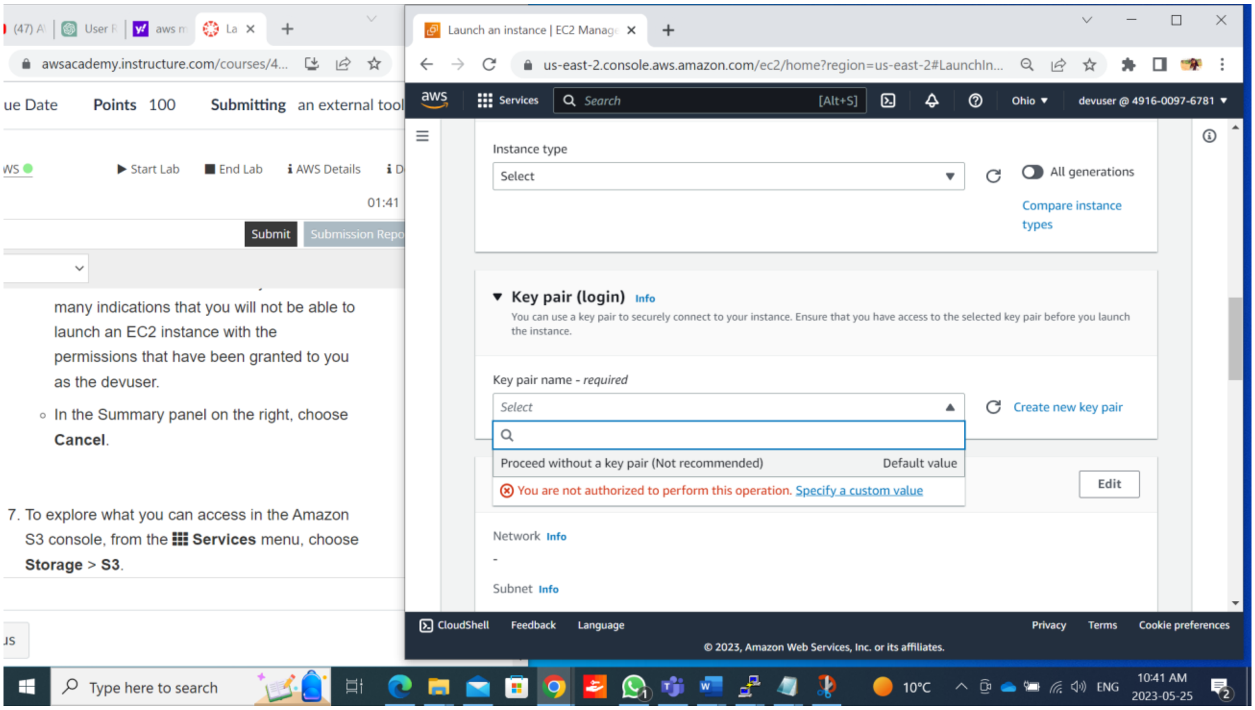
Name	Instance ID	Instance state	Instance type

You are not authorized to perform this operation.

Select an instance

© 2023, Amazon Web Services, Inc. or its affiliates.

Fig 3 shows the display message.



awsacademy.instructure.com/courses/4...
ue Date Points 100 Submitting an external tool
Start Lab
End Lab
AWS Details
01:41
Submit
Submission Repo

many indications that you will not be able to launch an EC2 instance with the permissions that have been granted to you as the devuser.

- In the Summary panel on the right, choose **Cancel**.

7. To explore what you can access in the Amazon S3 console, from the **Services** menu, choose **Storage** > **S3**.

Launch an instance | EC2 Manage
us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#LaunchIn...
aws
Services
Search
[Alt+S]
Ohio
devuser @ 4916-0097-6781

Instance type: Select

All generations
Compare instance types

Key pair (login) Info

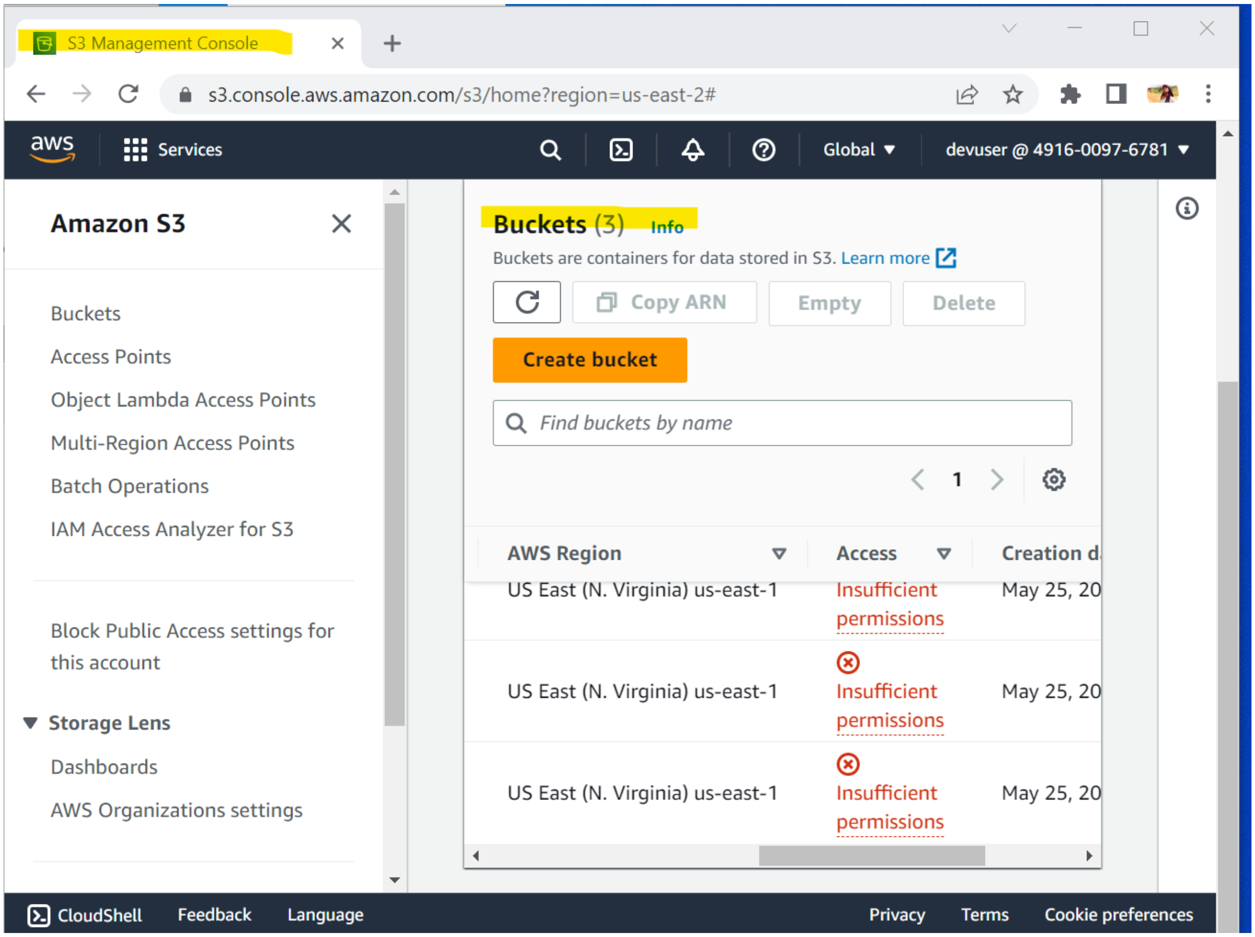
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: Select

Proceed without a key pair (Not recommended) Default value

You are not authorized to perform this operation. Specify a custom value

Fig 4 showing that I am authorized to perform this operation in the key pair name.



Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

AWS Region	Access	Creation d
US East (N. Virginia) us-east-1	Insufficient permissions	May 25, 20
US East (N. Virginia) us-east-1	⊗ Insufficient permissions	May 25, 20
US East (N. Virginia) us-east-1	⊗ Insufficient permissions	May 25, 20

Fig 5 showing the display message in storage S3.

REFLECTION

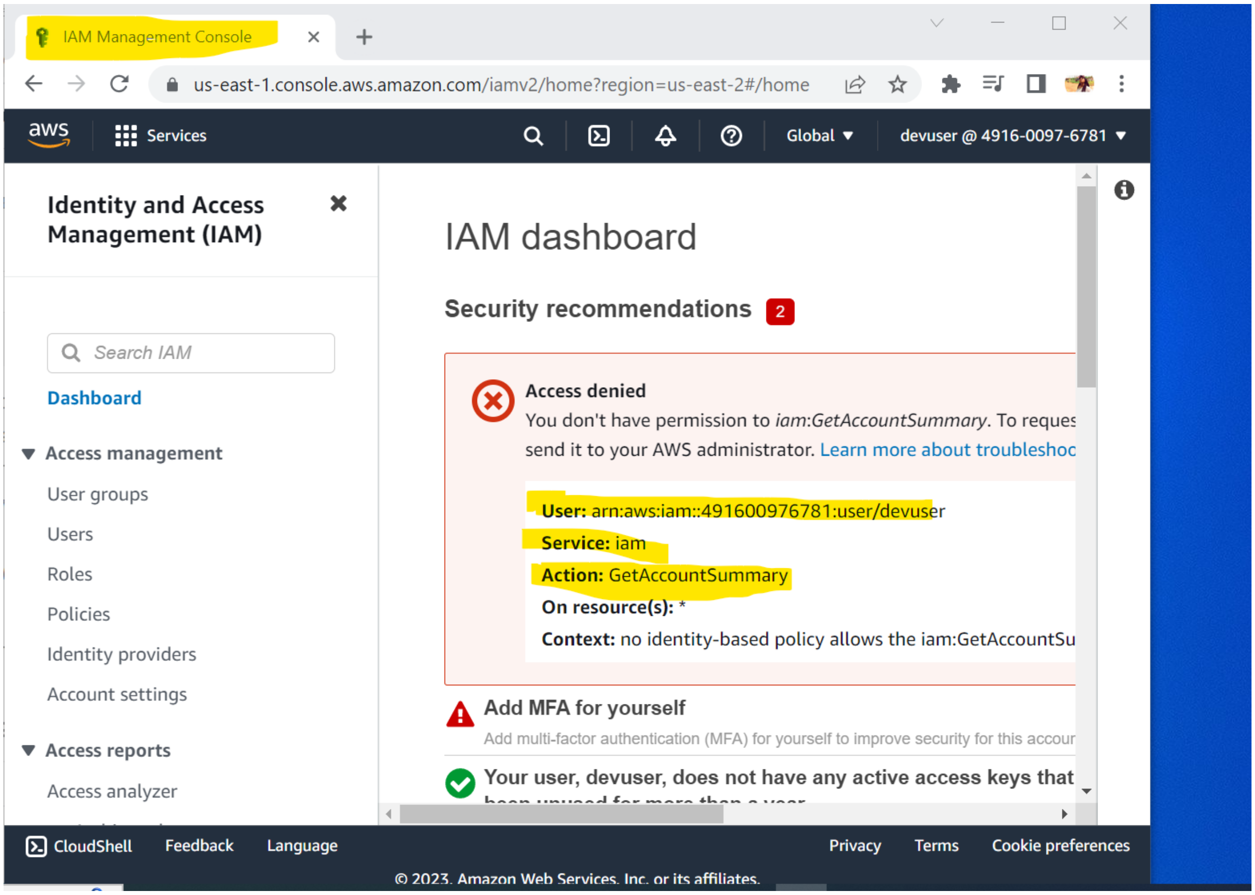
I understood the access privileges and limitations associated with my IAM user account(devuser), providing me with valuable insights into your role's permissions within AWS. I navigated into Amazon EC2 console, I performed some operations such as viewing instances and launching instances to see error messages indicating that I am not authorized to perform those operations. I was able to know the extent of my access restrictions within the EC2 service. When I accessed the Amazon S3 console, I observed that the buckets listed showed me the "insufficient permissions" in the access column. It shows that the S3 service has restricted my read-level access as the IAM user "devuser".

TASK 3- Analyzing the identity-based policy applied to the IAM user

DESCRIPTION

In this Task, I will examine the identity-based policy that is applied to the IAM user "devuser" in order to understand the reasons for the restricted access in my pervious tasks.

SCREENSHOT



IAM dashboard

Security recommendations 2

Access denied
You don't have permission to *iam:GetAccountSummary*. To reques
send it to your AWS administrator. Learn more about troubleshoo

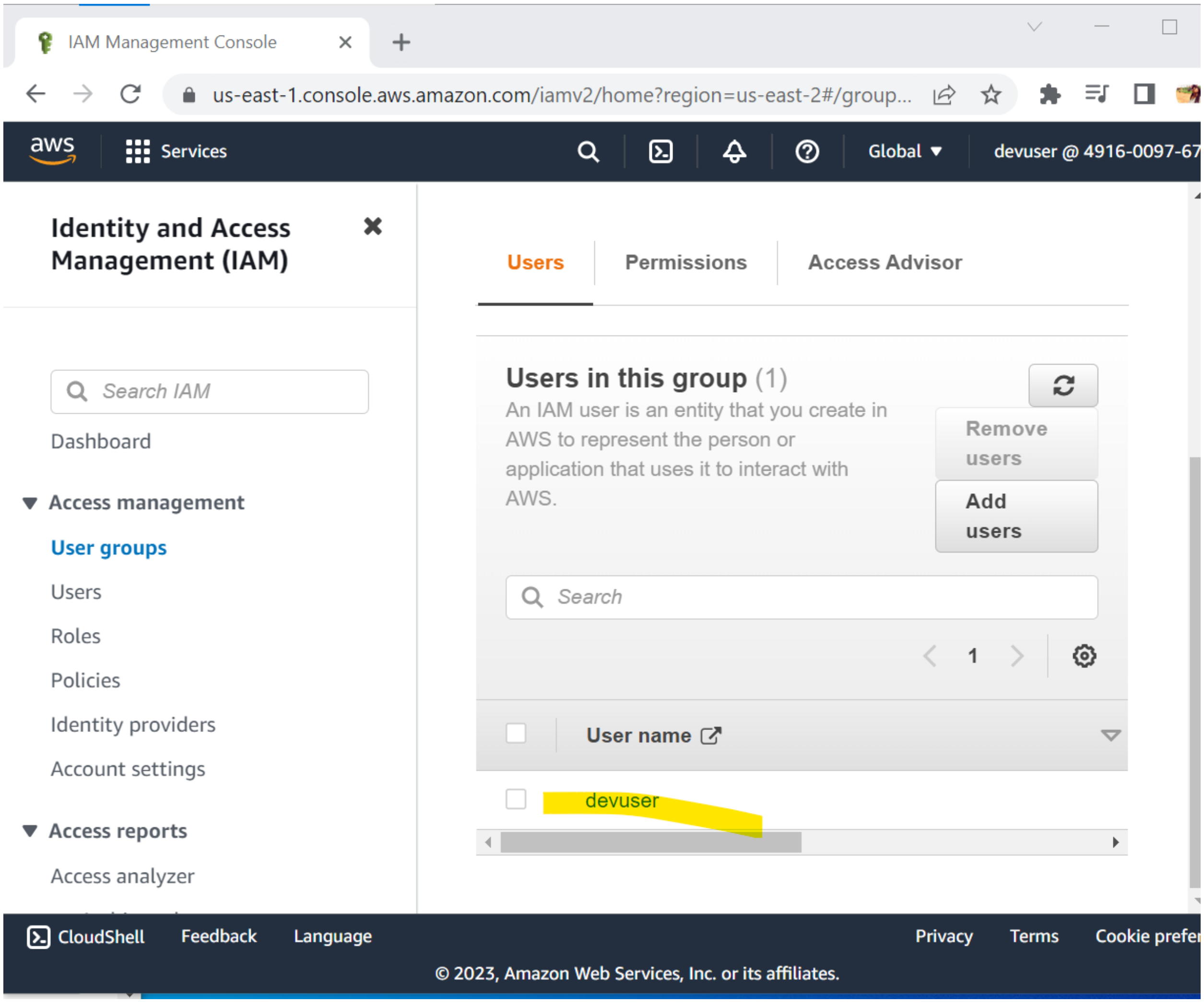
User: arn:aws:iam::491600976781:user/devuser
Service: iam
Action: GetAccountSummary
On resource(s): *
Context: no identity-based policy allows the iam:GetAccountSu

Add MFA for yourself
Add multi-factor authentication (MFA) for yourself to improve security for this accour

Your user, devuser, does not have any active access keys that

© 2023, Amazon Web Services, Inc. or its affiliates.

FIig 6 showing that I don't have permission to view certain parts of the page.

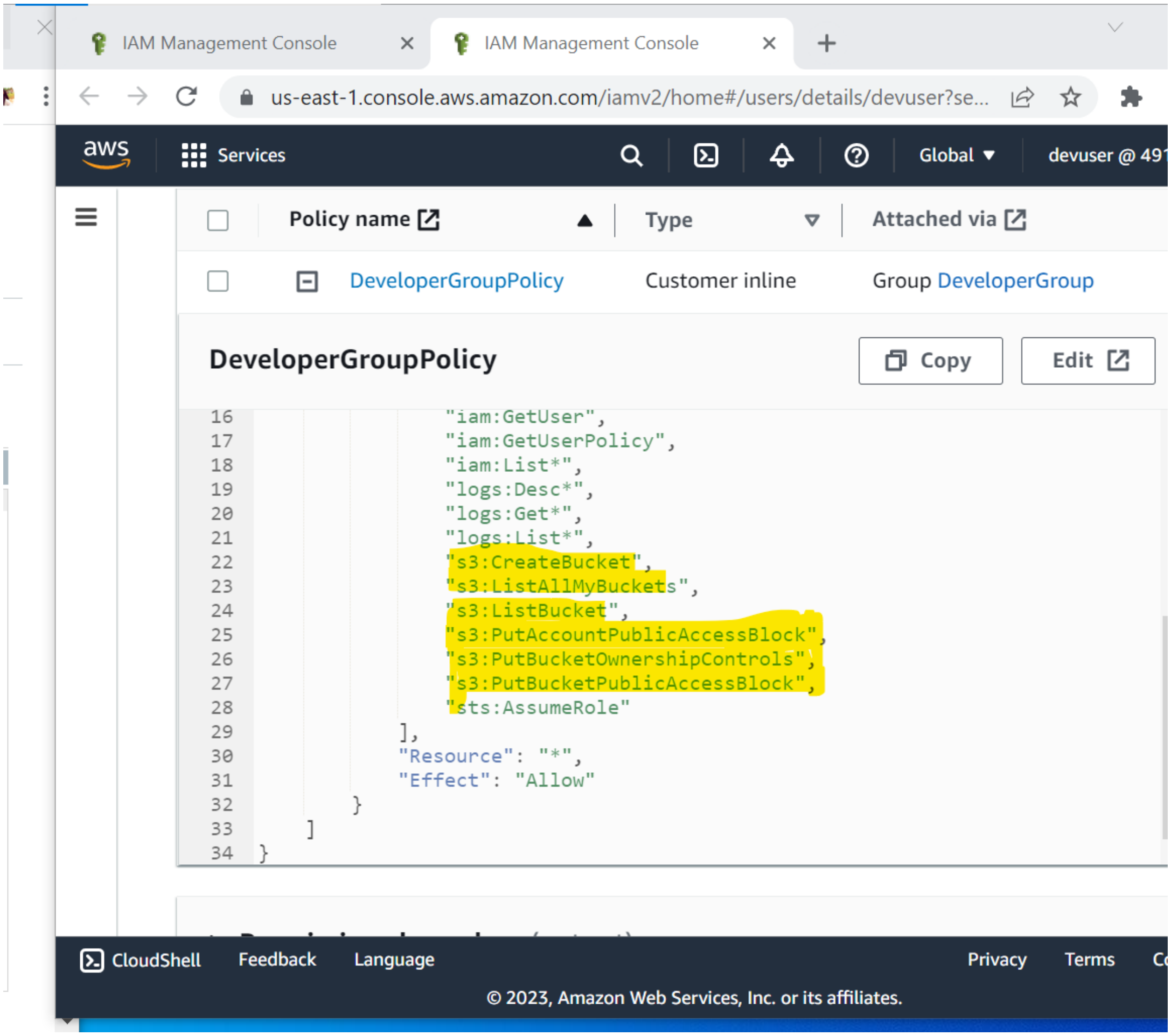


Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name
□	devuser

Fig 7 showing that devuser in a member of the IAM group.

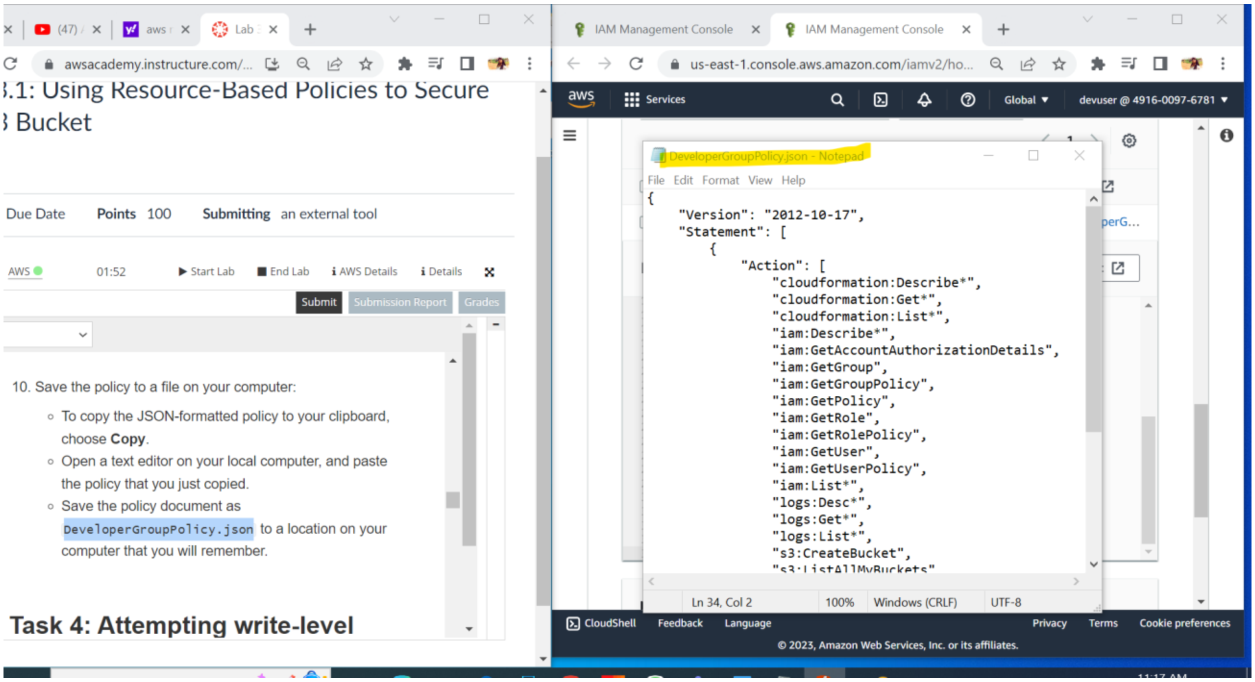

IAM Management Console
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home#/users/details/devuser?se...
aws
Services
Global
devuser @ 491
Copy
Edit
CloudShell
Feedback
Language
Privacy
Terms
© 2023, Amazon Web Services, Inc. or its affiliates.

□	Policy name	Type	Attached via
□	DeveloperGroupPolicy	Customer inline	Group DeveloperGroup

DeveloperGroupPolicy

```
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:List*",
                "logs:Desc*",
                "logs:Get*",
                "logs:List*",
                "s3:CreateBucket",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketPublicAccessBlock",
                "sts:AssumeRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Fig 8 showing the policy details of developrgrouppolicy.


awsacademy.instructure.com/...
us-east-1.console.aws.amazon.com/iamv2/ho...
IAM Management Console
Services
Global
devuser @ 4916-0097-6781
DeveloperGroupPolicy.json - Notepad
File Edit Format View Help
Ln 34, Col 2
100%
Windows (CRLF)
UTF-8
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

.1: Using Resource-Based Policies to Secure
Bucket

Due Date **Points** 100 **Submitting** an external tool

AWS 01:52 ▶ Start Lab ■ End Lab ℹ AWS Details ℹ Details

Submit Submission Report Grades

10. Save the policy to a file on your computer:
    - To copy the JSON-formatted policy to your clipboard, choose **Copy**.
    - Open a text editor on your local computer, and paste the policy that you just copied.
    - Save the policy document as `DeveloperGroupPolicy.json` to a location on your computer that you will remember.

Task 4: Attempting write-level

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudformation:Describe*",
                "cloudformation:Get*",
                "cloudformation:List*",
                "iam:Describe*",
                "iam:GetAccountAuthorizationDetails",
                "iam:GetGroup",
                "iam:GetGroupPolicy",
                "iam:GetPolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:List*",
                "logs:Desc*",
                "logs:Get*",
                "logs:List*",
                "s3:CreateBucket",
                "s3:ListAllMyBuckets"
```

Fig 9 showing that I have saved the policydocuments.

REFLECTION

Doing this lab, I was able to learn about the IAM group membership and the the IAM policy associated with the “DeveloperGroup” to which “devuser’ belongs to, I observed JSON policy details to identify the permissions and restrictions enforced by the policy. In my User and group Membership settings, I saw message saying "User: arn:aws:iam::user/devuser is not authorized to perform: iam:GetAccountSummary on resource: when trying to view certain sections of the IAM dashboard. I can verify that ‘devuser” belongs to the IAM group “DeveloperGroup.” In the IAM policy, I viewed the policy called “DeveloperGroupPolicy” that is a part of the “DeveloperGroup’ IAM group. I notice the policy in the JSON policy saying that ***“there are no Amazon EC2 actions permitted by the policy, the IAM actions that the policy allows, such as read-level IAM permissions, the Amazon S3 actions that the policy allows, specially related to***

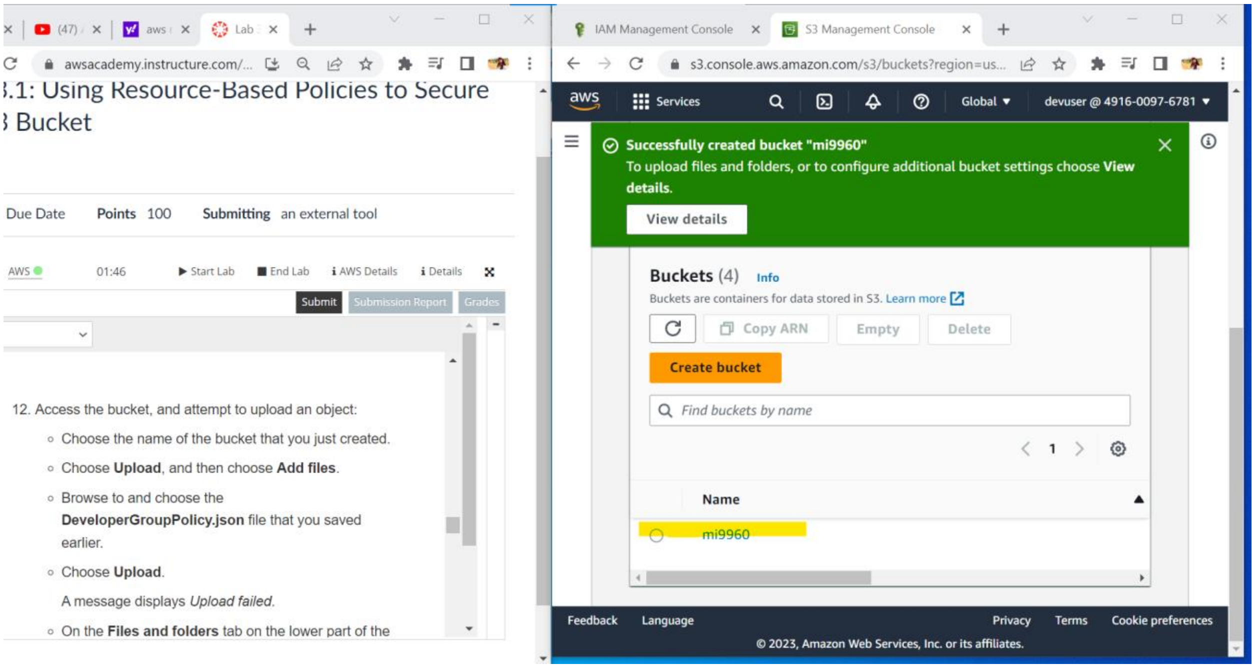
buckets, but not object-related actions." A set of regulations known as an IAM policy establishes restrictions in accessing Amazon EC2 and S3 services. This policy restricts me from accessing files in the Amazon S3 or launching new instances in the Amazon EC2, it ensures that that I only have access to the services and activities required for my work (***least privileges)***. From my understanding, the IAM policy functions like a set of rules that govern what I can and cannot do in the AWS, it helps in securing the account and AWS resources by giving me only resources I need to do my job.

TASK 4- Attempting write-level access to AWS services

DESCRIPTION

In this Task 4, I will attempt write-level access to AWS services, especially Amazon S3. I will perform actions that require write-level access privileges by creating an mi9960(S3) bucket and upload a file to it. I will know the level of access granted by the IAM policy and to investigate why I cannot or can perform specific API calls.

SCREENSHOT



(47)
aws
Lab
awsacademy.instructure.com/...
IAM Management Console
S3 Management Console
s3.console.aws.amazon.com/s3/buckets?region=us...
aws
Services
Global ▼
devuser @ 4916-0097-6781 ▼

.1: Using Resource-Based Policies to Secure
Bucket

Due Date Points 100 Submitting an external tool

12. Access the bucket, and attempt to upload an object:
    - Choose the name of the bucket that you just created.
    - Choose **Upload**, and then choose **Add files**.
    - Browse to and choose the **DeveloperGroupPolicy.json** file that you saved earlier.
    - Choose **Upload**.

      A message displays *Upload failed*.
    - On the **Files and folders** tab on the lower part of the

Successfully created bucket "mi9960"
To upload files and folders, or to configure additional bucket settings choose **View details**.

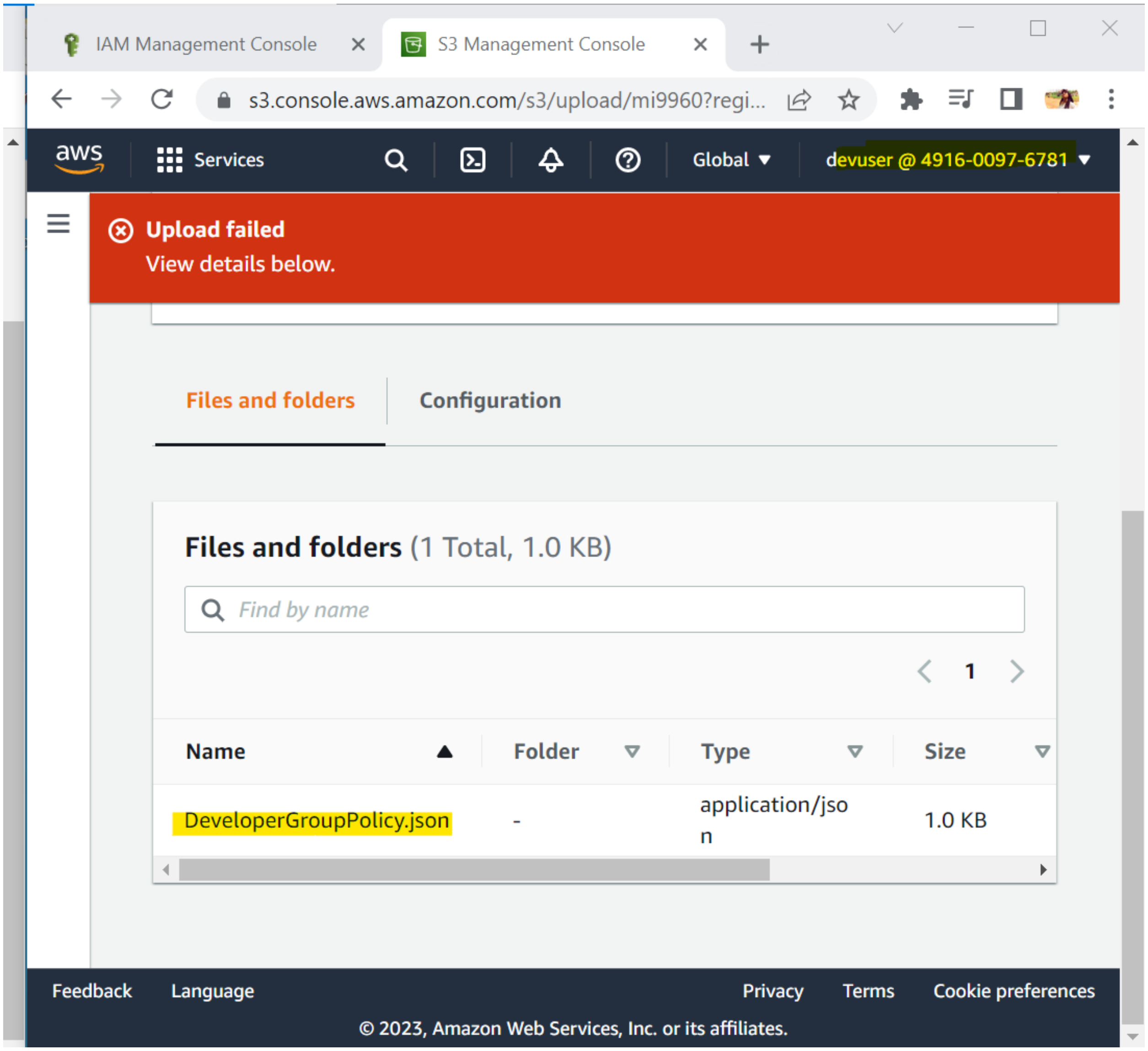
Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

○ mi9960

© 2023, Amazon Web Services, Inc. or its affiliates.

Fig 10 showing the bucket I created.



Upload failed
View details below.

Files and folders (1 Total, 1.0 KB)

Name	Folder	Type	Size
DeveloperGroupPolicy.json	-	application/json	1.0 KB

Fig 11 shows I was unable to upload the file because I don't have the permission to upload files and folders.

REFLECTION

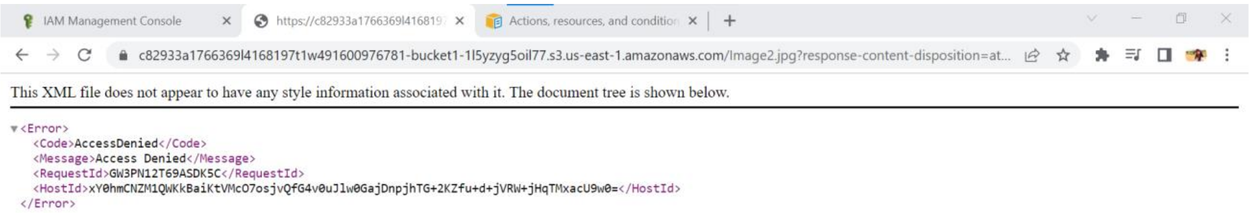
Doing the task, I was able to learn about the permissions defined by the IAM policy that governs my access to AWS services. From the review policy details that I copied to my text editor and named DeveloperGroupPolicy.json, I saw some list of policy like, s3: createbucket, that's y I was able to create a bucket, s3:listallmybuckets, s3:listbucket, s3:PutBucketOwnershipControls,s3:PutBucketPublicAccessBlock. But the policy does not allow s3:PutObjectaction, that was why I wasn't able to upload the file to S3buckets. The policy grants me permission to create and manage S3 buckets but does not provide write-level access to upload objects.

TASK 5- Assuming an IAM role and reviewing a resource-based policy

DESCRIPTION

In this task, I will perform some action on AWS S3 buckets using various IAM roles in this task. I will switch to a preconfigured IAM role for the lab, I will use it to control access to specific Amazon S3 bucket 1, I will be able to download objects but not in bucket 2. I will have a proper understanding of the IAM role.

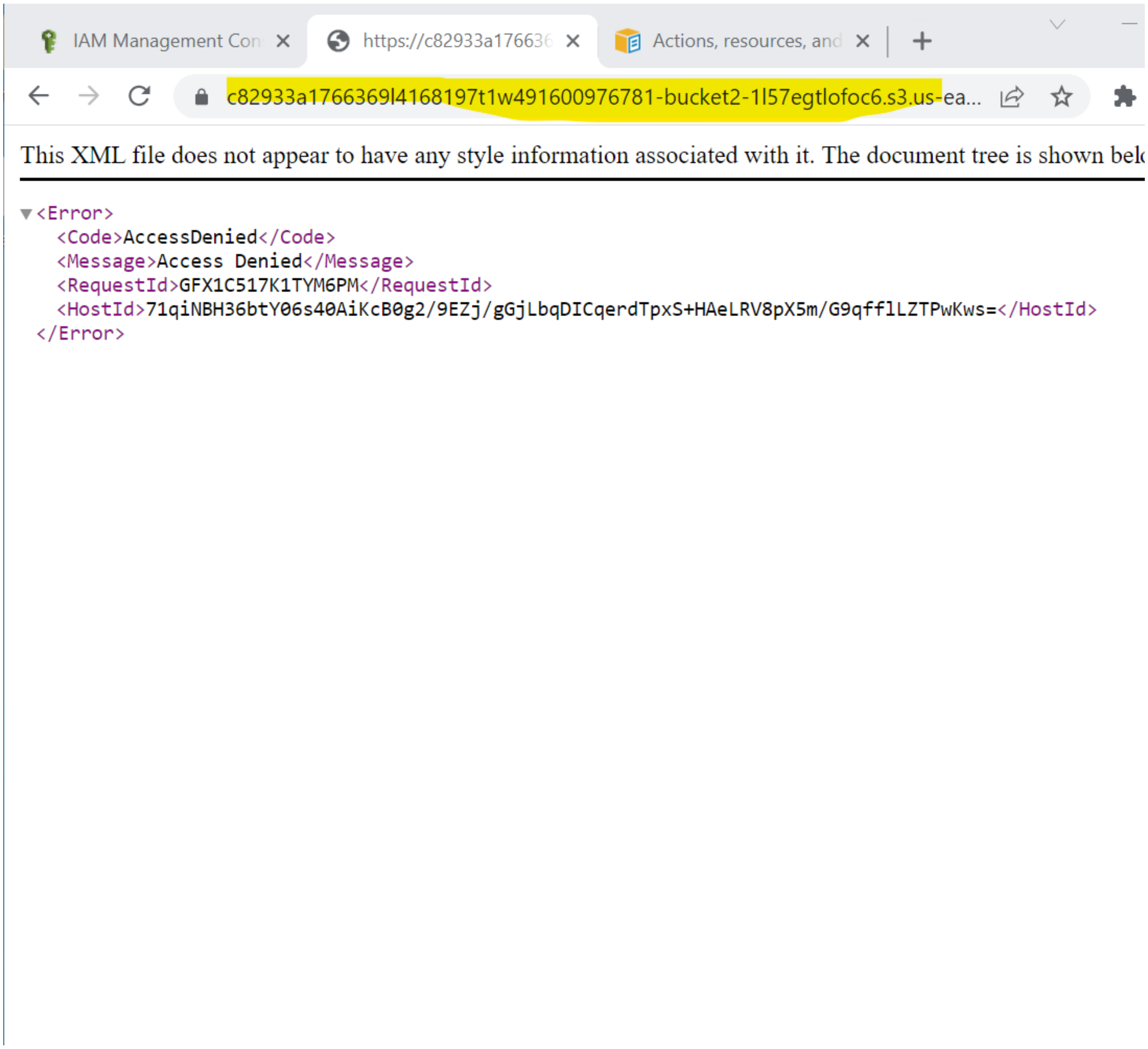
SCREENSHOT


IAM Management Console
https://c82933a1766369l416819
Actions, resources, and condition
c82933a1766369l4168197t1w491600976781-bucket1-1l5yzyg5oil77.s3.us-east-1.amazonaws.com/Image2.jpg?response-content-disposition=at...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>GW3PN12T69ASDK5C</RequestId>
   <HostId>xY0hmCNZM1QWKkBaiKtVMcO7osjvQfG4v0uJlw0GajDnpjhTG+2KZfu+d+jVRW+jHqTMxacU9w0=</HostId>
 </Error>
```

fig 12 showing that I don't have access to download image2 in bucket1.

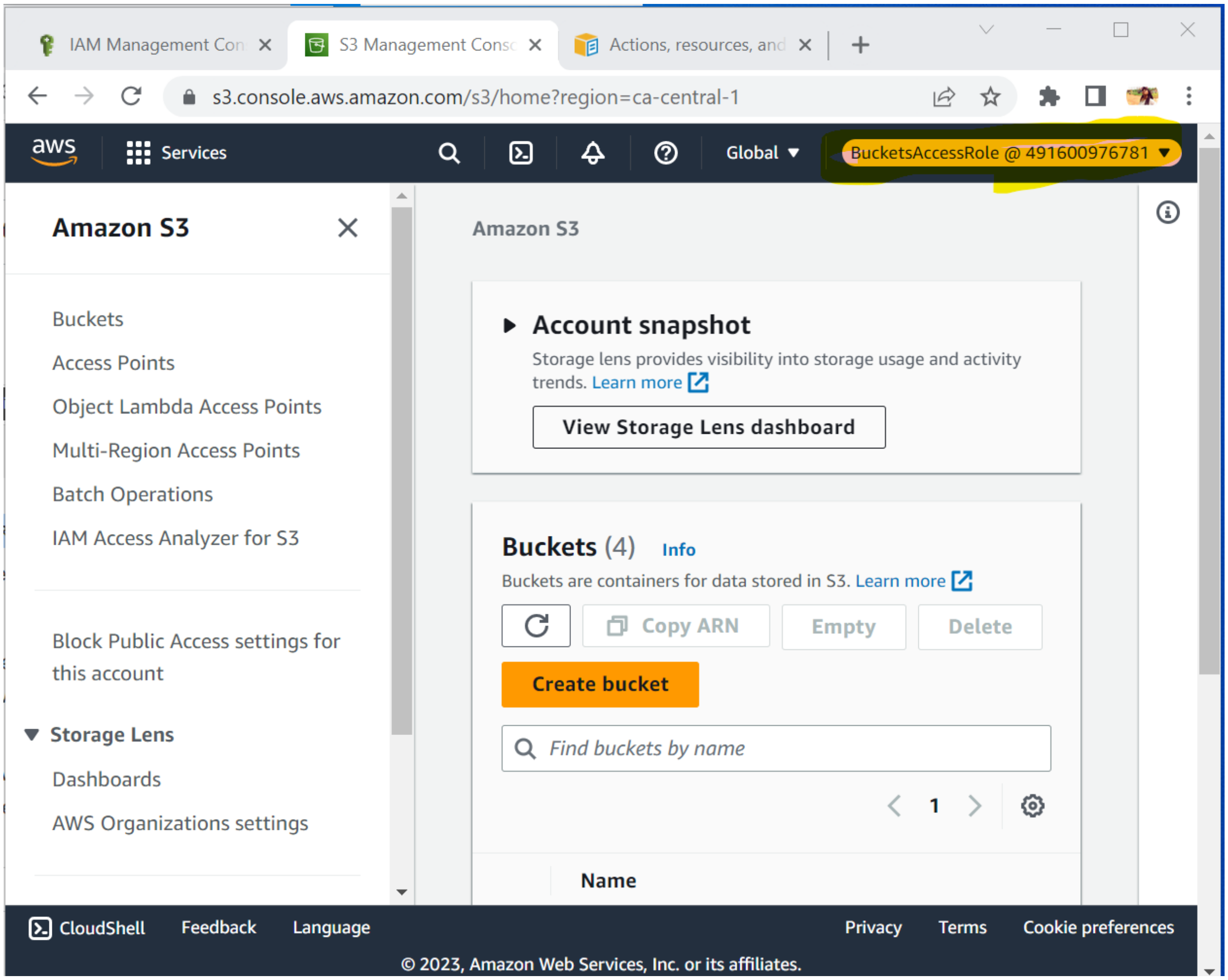


c82933a1766369l4168197t1w491600976781-bucket2-1l57egtlofoc6.s3.us-ea...

This XML file does not appear to have any style information associated with it. The document tree is shown bel

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>GFX1C517K1TYM6PM</RequestId>
   <HostId>71qiNBH36btY06s40AiKcB0g2/9EZj/gGjLbqDICqerdTpxS+HAeLRV8pX5m/G9qfflLZTPwKws=</HostId>
 </Error>
```

Fig 13 showing that I don't have access to download image1 in bucket2.

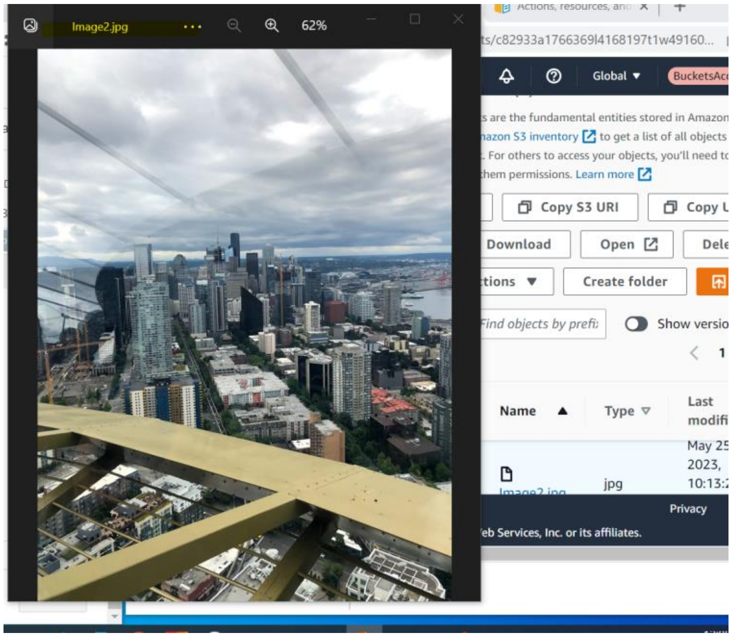


Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3. Learn more

© 2023, Amazon Web Services, Inc. or its affiliates.

Fig 14 shows that I have switched roles.

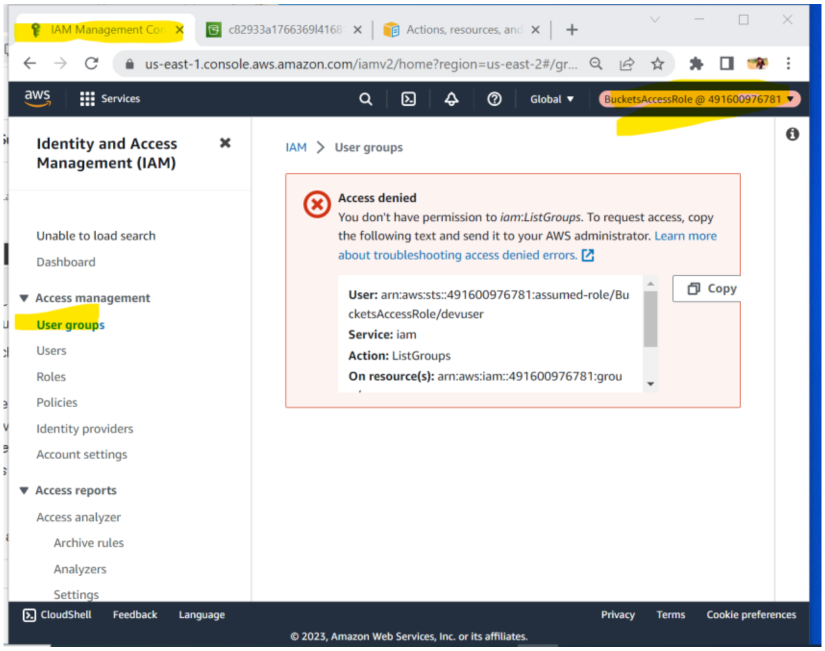


s are the fundamental entities stored in Amazon
nazon S3 inventory to get a list of all objects
. For others to access your objects, you'll need to
them permissions. Learn more

May 25 2023, 10:13:2

eb Services, Inc. or its affiliates.

Fig 15 shows the image 2 I downloaded from bucket1.

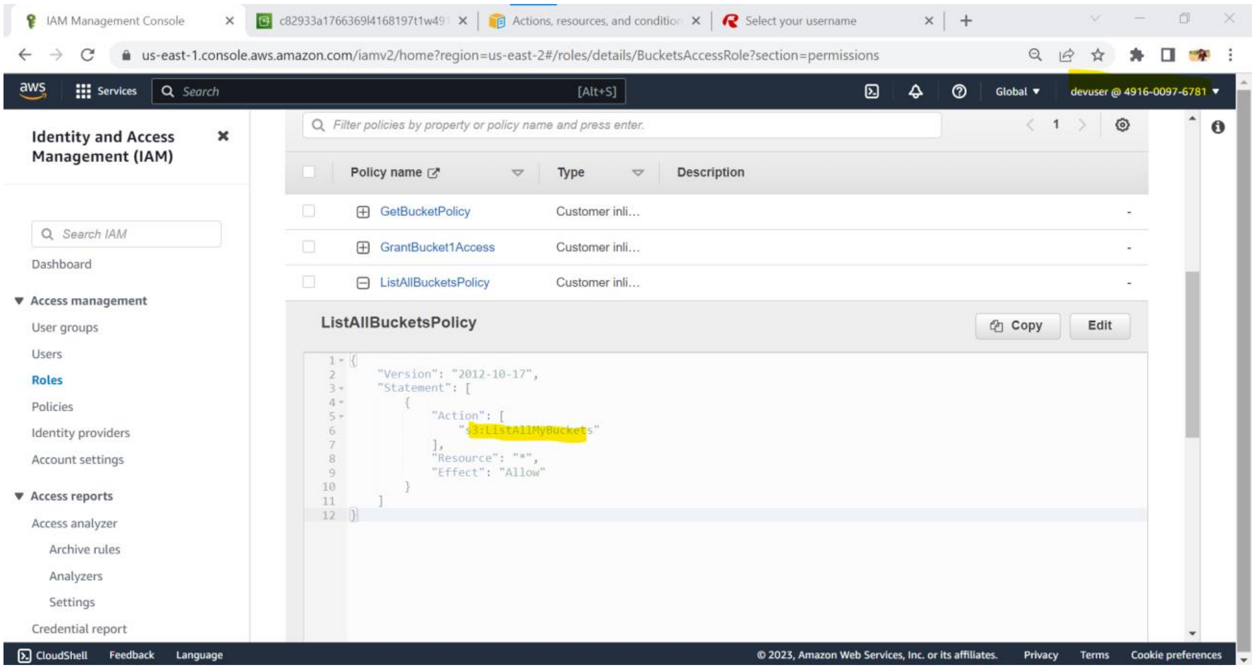


Access denied

You don't have permission to *iam:ListGroups*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:sts::491600976781:assumed-role/BucketsAccessRole/devuser
Service: iam
Action: ListGroups
On resource(s): arn:aws:iam::491600976781:grou

Fig 16 shows that I don't have permission to view the IAM user groups because the BucketAccessRole does not have the permission.

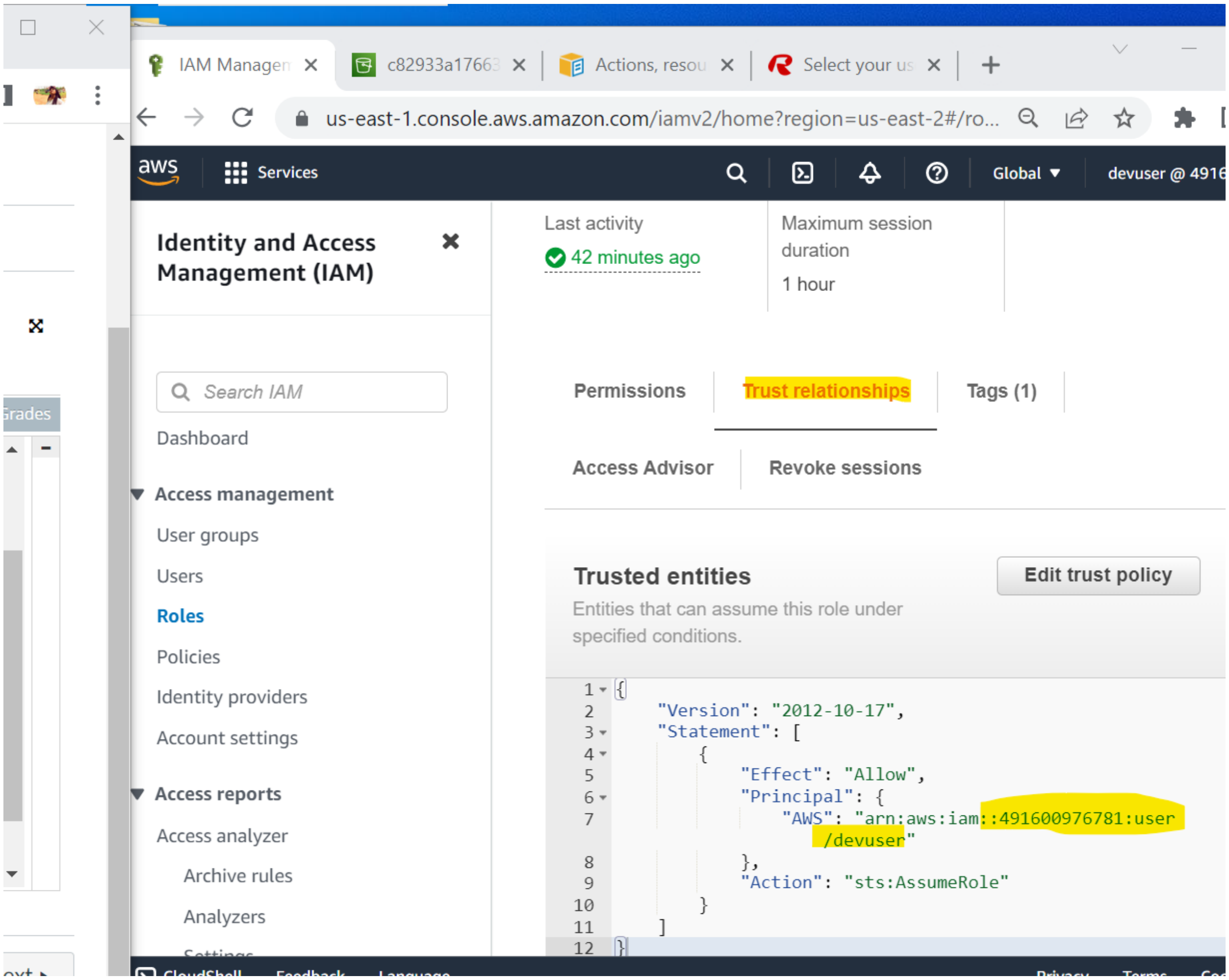


□	Policy name	Type	Description
□	⊞ GetBucketPolicy	Customer inli...	-
□	⊞ GrantBucket1Access	Customer inli...	-
□	⊟ ListAllBucketsPolicy	Customer inli...	-

ListAllBucketsPolicy

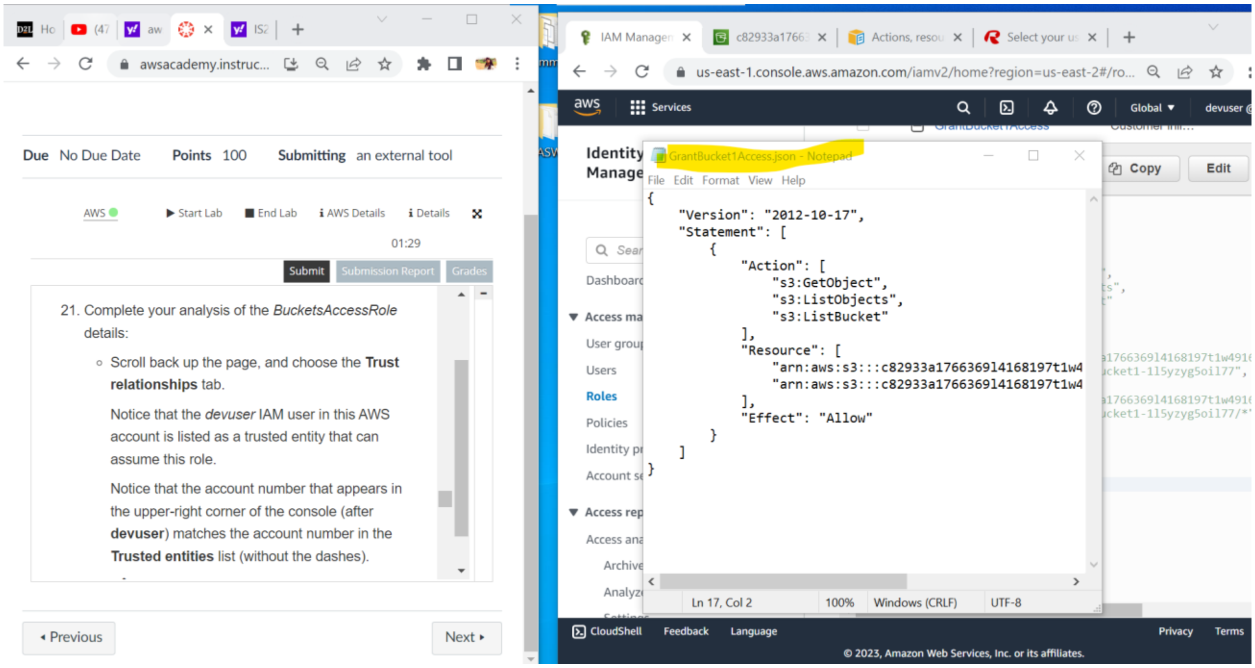
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Fig 17 shows that I can see S3 bucket when I assume bucketaccessrole.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::491600976781:user/devuser"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Fig 18 shows that devuser IAM user is listed as a trusted entity.



Due No Due Date Points 100 Submitting an external tool

01:29

21. Complete your analysis of the *BucketsAccessRole* details:
    - Scroll back up the page, and choose the **Trust relationships** tab.

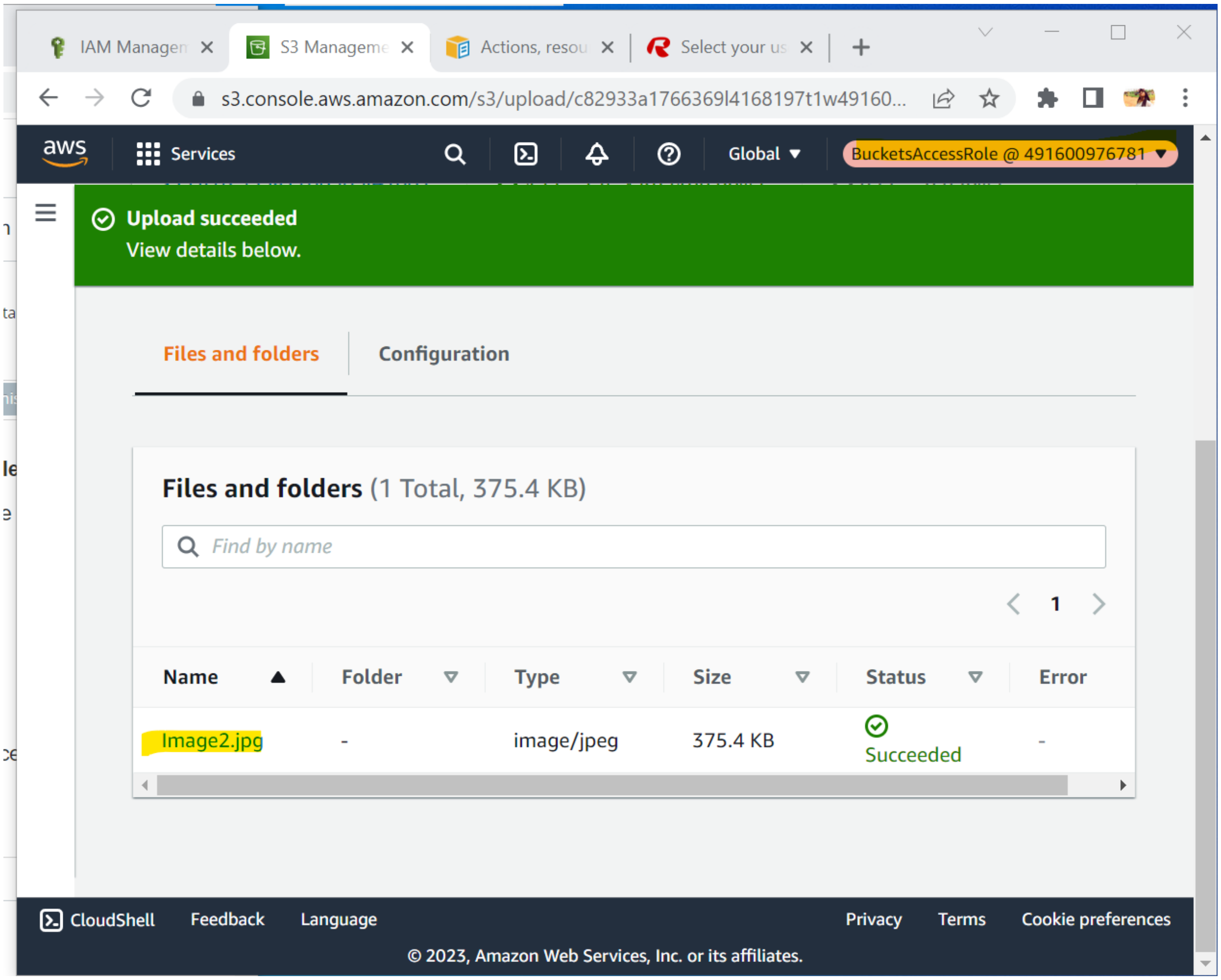
      Notice that the *devuser* IAM user in this AWS account is listed as a trusted entity that can assume this role.

      Notice that the account number that appears in the upper-right corner of the console (after **devuser**) matches the account number in the **Trusted entities** list (without the dashes).

GrantBucket1Access.json - Notepad

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:ListObjects",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::c82933a176636914168197t1w4
                "arn:aws:s3:::c82933a176636914168197t1w4
            ],
            "Effect": "Allow"
        }
    ]
}
```

Fig 18 shows that I have saved the JSON-formatted policy.



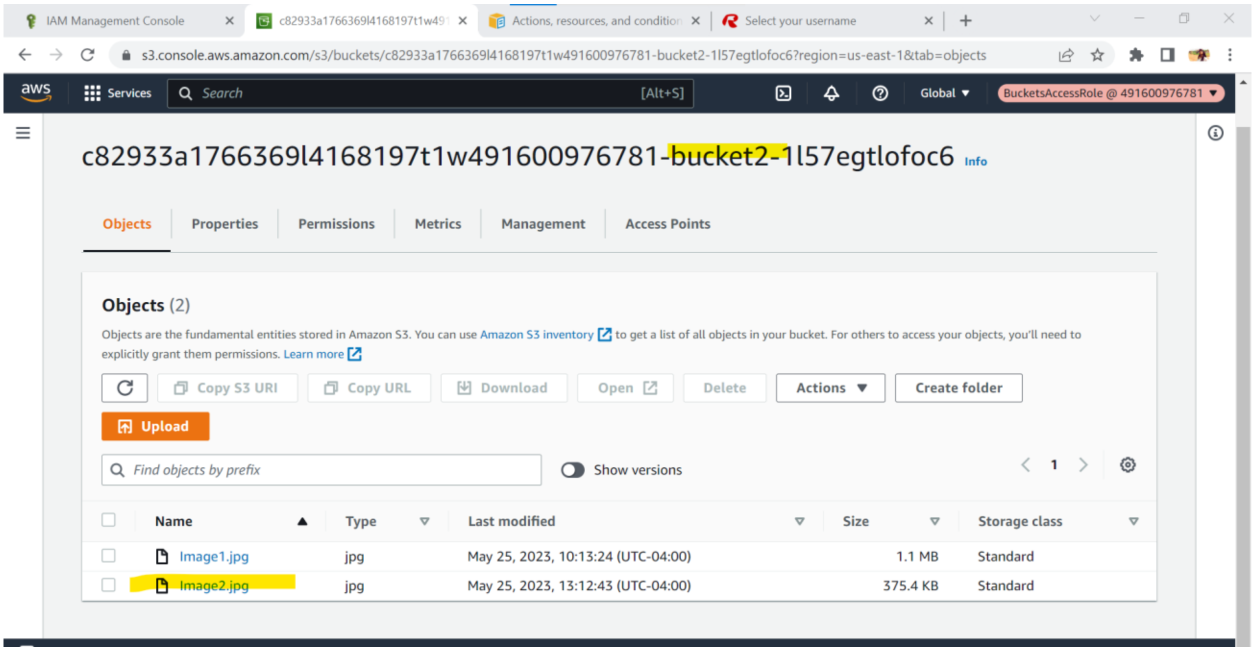
Upload succeeded
View details below.

Files and folders (1 Total, 375.4 KB)

Find by name

Name	Folder	Type	Size	Status	Error
Image2.jpg	-	image/jpeg	375.4 KB	Succeeded	-

© 2023, Amazon Web Services, Inc. or its affiliates.



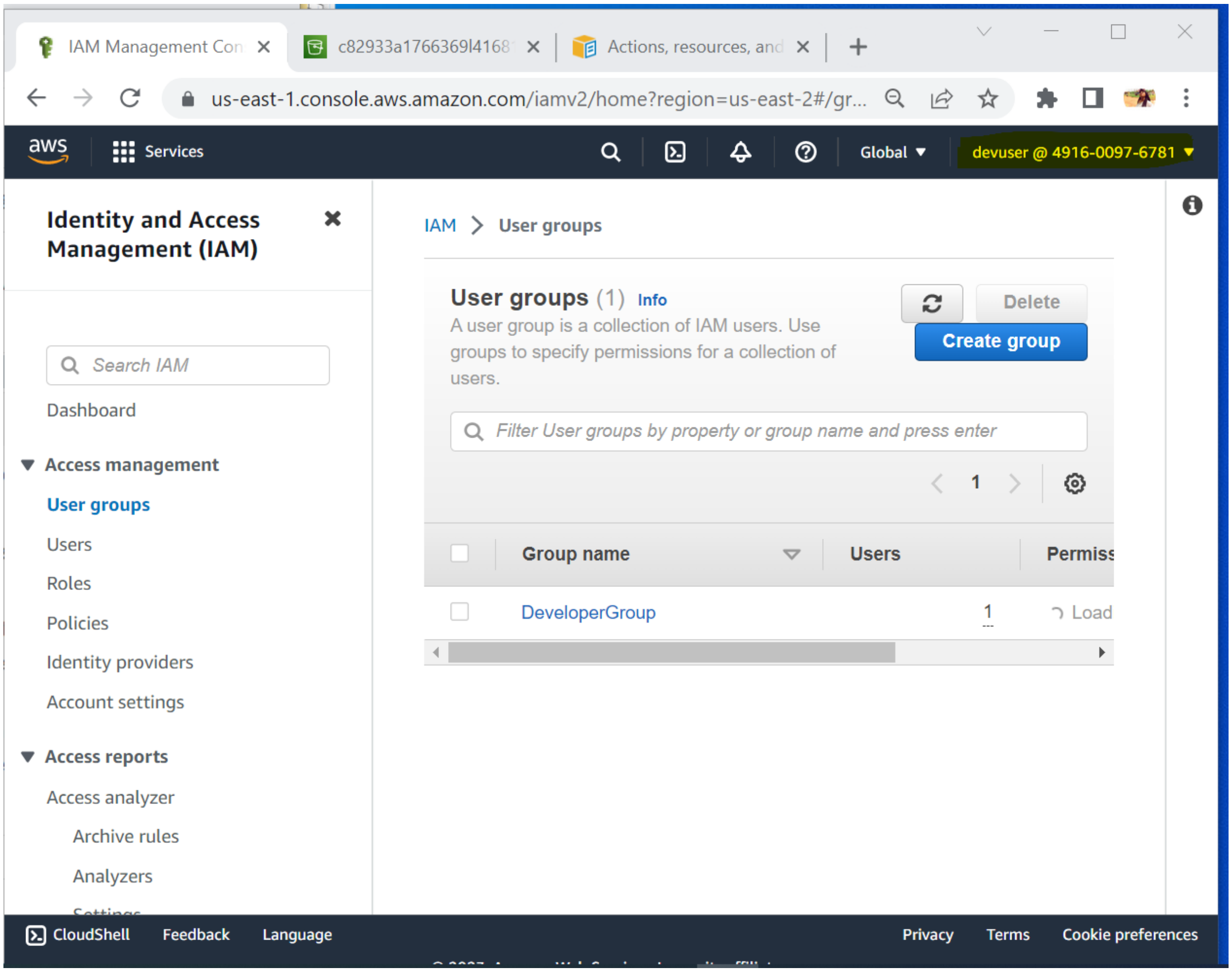
c82933a1766369l4168197t1w491600976781-bucket2-1l57egtlofoc6

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
Image1.jpg	jpg	May 25, 2023, 10:13:24 (UTC-04:00)	1.1 MB	Standard
Image2.jpg	jpg	May 25, 2023, 13:12:43 (UTC-04:00)	375.4 KB	Standard

Fig 19 shows that I have uploaded image 2 to bucket2.



User groups (1) Info

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

Filter User groups by property or group name and press enter

Group name	Users	Permiss
DeveloperGroup	1	Load

Fig 17 shows that the permission is back now I have switched back to devuser.

REFLECTION

Doing this, I had a proper understanding of the IAM role, I was able to download object from bucket1 but not bucket2 after assuming ***BucketsAccessRole*** because the IAM polices associated with the role allow specific actions on bucket1 only. The policy grants permissions for the s3:

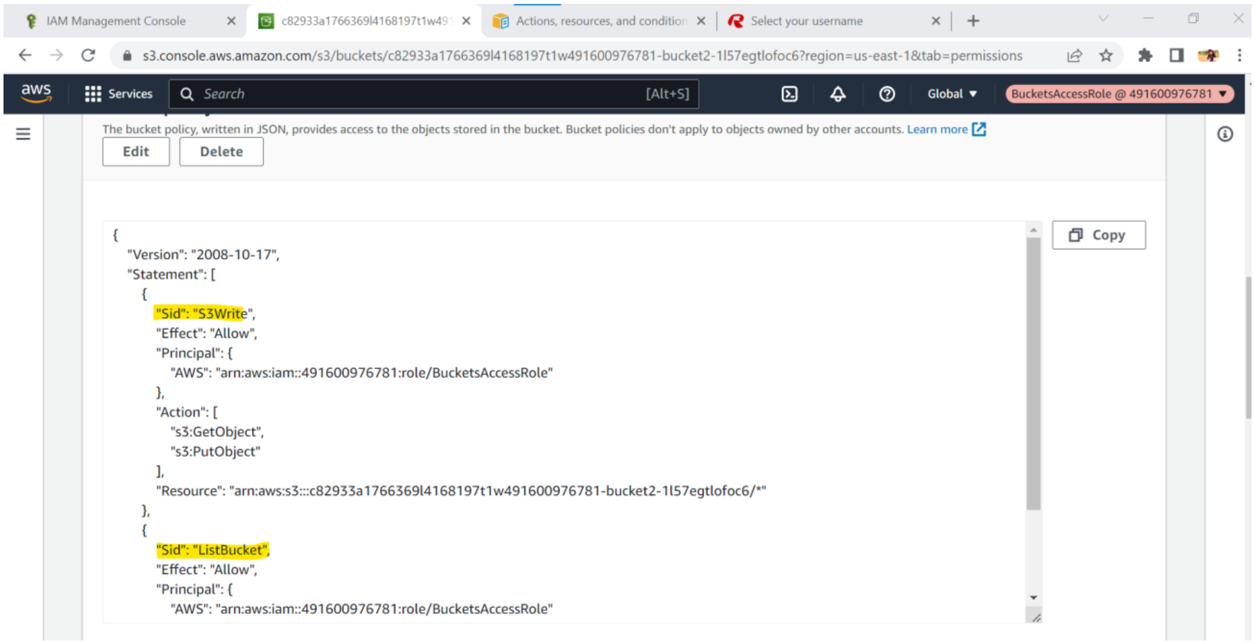
GetObject, s3:ListObjects, and s3:ListBucket actions, but it is configured to apply to bucket1 and its objects (indicated by /* wildcard). Since Bucket2 isn't included in the policy, I won't be able to download objects from bucket2. I tried accessing the usergroup using ***BucketAccessRole*** but it showed me an error message because the bucketAcessRole does not have the necessary permission ***(iam:ListGroups)*** to view the IAM user groups page. The IAM role are similar to special permission sets that allow you to do specific things in the AWS. The ***bucketAccessRole*** does not have the ability to manage IAM user groups, which are managed by a separate AWS service, that was why I got an error message when I viewed the user group page. I was to check who can utilize a role by looking at the BucketAccessRole details, I saw that the bucketAccessRole is used by the devuser IAM user inside the same AWS account. It shows that the devuser has the ability to temporarily assume the BucketsAccessRole and gain its capabilities. The aacount number shown in the upper-right corner of the console matched the account number in the trust entities, it means that the devuser is trusted within the same AWS account. From my understanding, I believe that the STS (AWS security Token Service) helps to give temporary permissions to trusted users, so when devuser assumes ***bucketsAccessRole***, they have access to its permissions.

TASK 6- Understanding resource-based policies

DESCRIPTION

In this final Task, I am going to understand resource-based policies associated with bucket 2. I will inspect the bucket policy to determine the permissions granted to the ***BucketAccessRole*** IAM role, which I assumed earlier.

SCREENSHOT


IAM Management Console
c82933a1766369l4168197t1w491
Actions, resources, and condition
Select your username
s3.console.aws.amazon.com/s3/buckets/c82933a1766369l4168197t1w491600976781-bucket2-1l57egtlofoc6?region=us-east-1&tab=permissions
aws
Services
Search
[Alt+S]
Global
BucketsAccessRole @ 491600976781
Edit
Delete
Copy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

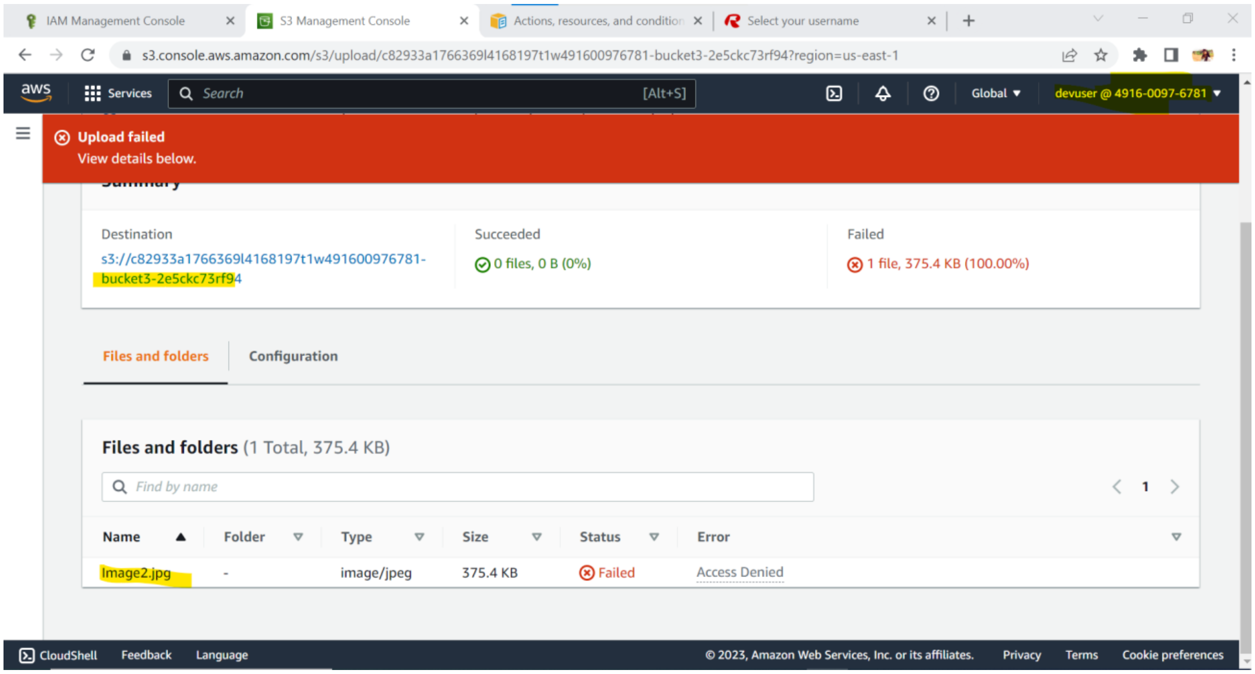
```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "S3Write",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::491600976781:role/BucketsAccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::c82933a1766369l4168197t1w491600976781-bucket2-1l57egtlofoc6/*"
    },
    {
      "Sid": "ListBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::491600976781:role/BucketsAccessRole"
```

fig 18 shows the two policy statements in the bucket policy.

REFLECTION

When I reviewed the bucket policy, I discovered that it consists of two statements. The first statement, with the SID (Statement ID)” S3Write,”, it enable the s3:Getobject and s3:PutObject activities to be carried out on bucket2 by the BucketAccessRole. The second sentence allows the BucketAccessRole to perform the s3:ListBucket action on bucket2 and has the SID “listBucket." I had a clear understanding of how resource resource-based policies (like s3 bucket policies) and role-based (connected to IAM role) cooperate with one another. Although access to bucket2 was implicitly denied by the role-based regulations, it was also not expressly granted. The BucketsAccessRole gives access to bucket2 and the ability to upload objetcs (s3:PutObject) by the resource-based bucket policy.

CHALLENGE TASK


IAM Management Console
S3 Management Console
Actions, resources, and condition
Select your username
s3.console.aws.amazon.com/s3/upload/c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94?region=us-east-1
aws
Services
Search
[Alt+S]
Global
devuser @ 4916-0097-6781
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Upload failed
View details below.

Summary

Destination
s3://c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94

Succeeded
0 files, 0 B (0%)

Failed
1 file, 375.4 KB (100.00%)

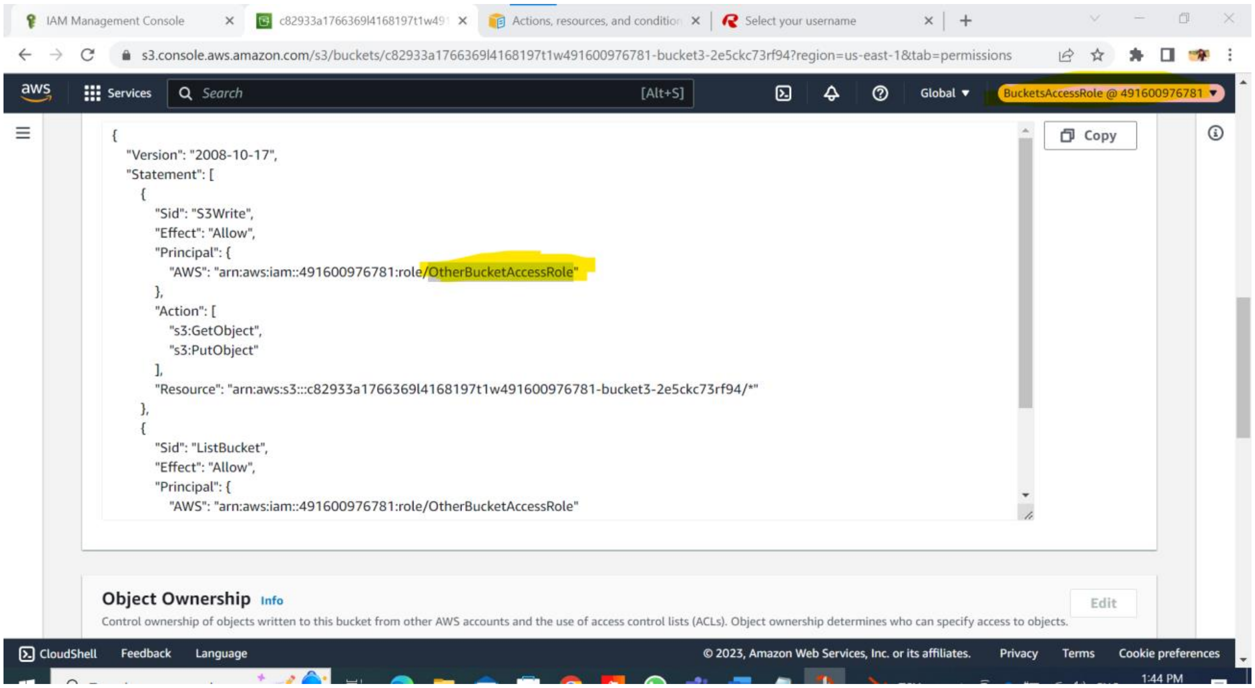
Files and folders | Configuration

Files and folders (1 Total, 375.4 KB)

Find by name

Name	Folder	Type	Size	Status	Error
Image2.jpg	-	image/jpeg	375.4 KB	Failed	Access Denied

Fig 19 shows that I can't upload the image 2 to bucket 3.

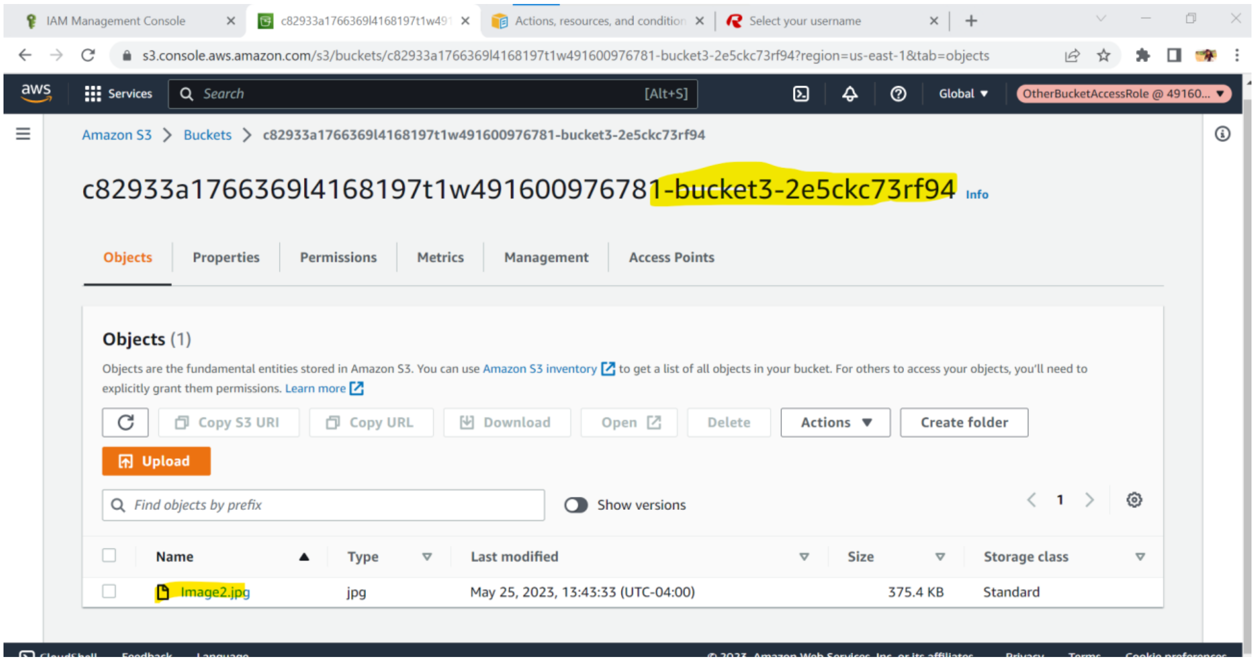

IAM Management Console
c82933a1766369l4168197t1w49
Actions, resources, and condition
Select your username
s3.console.aws.amazon.com/s3/buckets/c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94?region=us-east-1&tab=permissions
aws
Services
Search
[Alt+S]
Global
BucketsAccessRole @ 491600976781
Copy
Edit
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
1:44 PM

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "S3Write",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::491600976781:role/OtherBucketAccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94/*"
    },
    {
      "Sid": "ListBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::491600976781:role/OtherBucketAccessRole"
```

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Fig 20 shows the policy for bucket 3 that will enable me to upload the Image.


IAM Management Console
c82933a1766369l4168197t1w49
Actions, resources, and condition
Select your username
s3.console.aws.amazon.com/s3/buckets/c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94?region=us-east-1&tab=objects
Services
Search
[Alt+S]
Global
OtherBucketAccessRole @ 49160...
Amazon S3 > Buckets > c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94

c82933a1766369l4168197t1w491600976781-bucket3-2e5ckc73rf94 Info

Objects
Properties
Permissions
Metrics
Management
Access Points

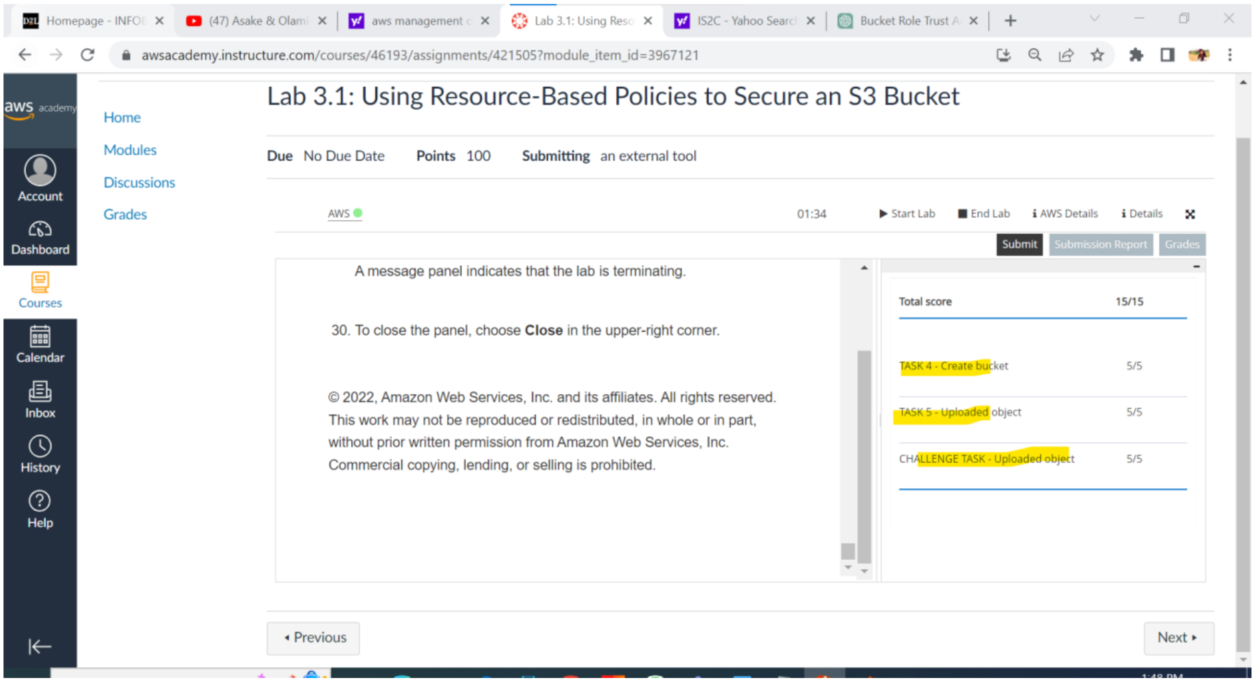
Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload
Find objects by prefix
Show versions

□	Name	Type	Last modified	Size	Storage class
□	Image2.jpg	jpg	May 25, 2023, 13:43:33 (UTC-04:00)	375.4 KB	Standard

Fig 21 shows that I have successfully uploaded the image 2 to bucket 3.



Lab 3.1: Using Resource-Based Policies to Secure an S3 Bucket

Due No Due Date Points 100 Submitting an external tool

A message panel indicates that the lab is terminating.

30. To close the panel, choose **Close** in the upper-right corner.

© 2022, Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Total score	15/15
TASK 4 - Create bucket	5/5
TASK 5 - Uploaded object	5/5
CHALLENGE TASK - Uploaded object	5/5

Fig 22 shows that I have completed the task.

REFLECTION

I was able to upload the image to bucket 3 because I switched the role to ***“otherBucketAccessRole” permissions*** after viewing the policies in bucket 3 to perform the actions. These permissions enable me to upload the image because it has the permission to do it.

REFERNCES

Policies and permissions in IAM - AWS Identity and Access Management. (n.d.). https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html