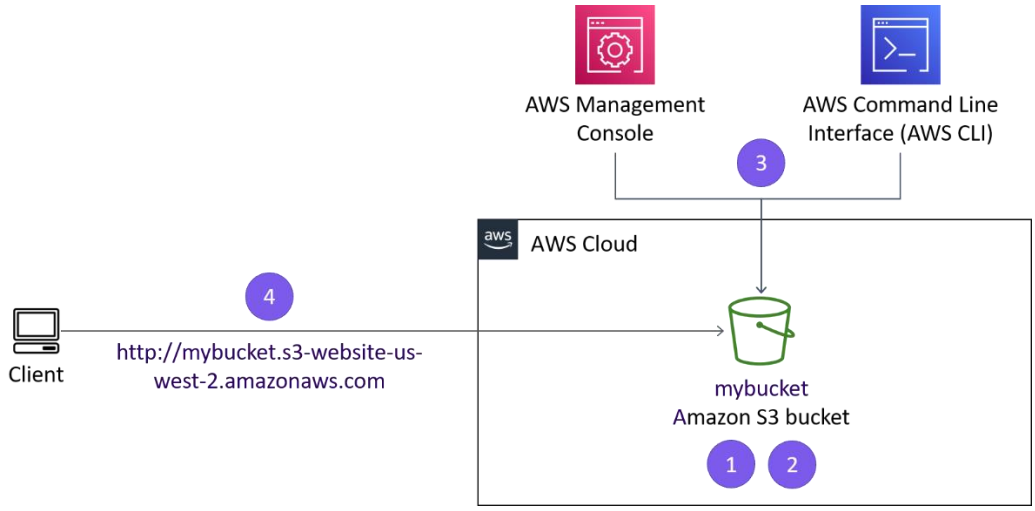
Creating a Website on S3

In this lab, you practice using AWS Command Line Interface (AWS CLI) commands from an Amazon Elastic Compute Cloud (Amazon EC2) instance to:

- Create an Amazon Simple Storage Service (Amazon S3) bucket.
- Create a new AWS Identity and Access Management (IAM) user that has full access to the Amazon S3 service.
- Upload files to Amazon S3 to host a simple website for the Café & Bakery.
- Create a batch file that can be used to update the static website when you change any of the website files locally.



Clients will be able to access the website you have deployed to Amazon S3. The website URL is similar to this example: http://.s3-website-us-west-2.amazonaws.com. You can create and access the bucket through the AWS Management Console or the AWS CLI.

Objectives

After completing this lab, you should be able to:

- Run AWS CLI commands that use IAM and Amazon S3 services.
- Deploy a static website to an S3 bucket.
- Create a script that uses the AWS CLI to copy files in a local directory to Amazon S3.

Duration

This activity requires approximately **45 minutes** to complete.

Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch the lab.
2. Wait until the message "Lab status: ready" appears, and then choose **X** to close the **Start Lab** panel.
3. Next to Start Lab, choose AWS, which opens the AWS Management Console in a new browser tab. The system automatically signs you in.

   Tip If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

4. Arrange the AWS Management Console so that it appears alongside these instructions.

   Important: Do not change the lab Region unless specifically instructed to do so.

Task 1: Use SSH to connect to an Amazon Linux EC2 instance

In this task, you log in to an existing EC2 instance.

Windows users

These instructions are specifically for Windows users.

5. At the top of the page, choose the Details dropdown menu, and then choose Show. A **Credentials** window opens.
6. Choose **Download PPK**, and save the **labsuser.ppk** file.

   Typically, your browser saves downloaded files to the **Downloads** directory.

7. Copy and paste the **PublicIP** into a text editor to use later. This IP address is the IPv4 server address that you have to connect to.
8. To exit the **Details** panel, choose the **X**.
9. Download **PuTTY** to use an SSH utility to connect to the EC2 instance. If you do not have PuTTY installed on your computer, download it.
10. Open **putty.exe**.
11. Configure the PuTTY timeout to keep the PuTTY session open for a longer period of time:
    - Choose **Connection**.
    - For **Seconds between keepalives**, enter `30`
12. Configure your PuTTY session:
    - Choose **Session**.
    - For the **Host Name (or IP address)**, enter the **PublicIP** address that you copied from the previous steps.
    - In PuTTY in the **Connection** list, choose **SSH** to expand it.
    - Choose **Auth**, but don't expand it.
    - Choose **Browse**.
    - Browse to and select the **labuser.ppk** file that you downloaded.
    - To choose the file, choose **Open**.
    - Choose **Open** again.

13. In the **PuTTY Security Alert** window, choose **Accept** to trust and connect to the host.
14. When prompted with **login as**, enter `ec2-user` and press Enter.

    This step connects you to the EC2 instance.

macOS and Linux users

These instructions are specifically for Mac and Linux users.

15. At the top of the page, choose the Details dropdown menu, and then choose Show. A **Credentials** window opens.
16. Choose **Download PEM**, and save the **labsuser.pem** file.
17. Copy and paste the **PublicIP** into a text editor to use later. This IP address is the IPv4 server address that you have to connect to.
18. To exit the **Details** panel, choose the **X**.
19. Open a terminal window, and change the **cd** directory to the directory where you downloaded the labsuser.pem file. For example, run the following command if you saved the file to your **Downloads** directory:

    ```
    cd ~/Downloads
    ```

20. To change the permissions on the key to read only, run the following command:

    ```
    chmod 400 labsuser.pem
    ```

21. In the following command, replace *<ip-address>* with the public IP address that you copied from the previous steps, and run the adjusted command:

    ```
    ssh -i labsuser.pem ec2-user@<ip-address>
    ```

22. When prompted, enter `yes` to connect to this remote SSH server. Because you are using a key pair for authentication, you are not prompted for a password.

Task 2: Configure the AWS CLI

Unlike some other Linux distributions that are available through Amazon Web Services (AWS), Amazon Linux instances already have the AWS CLI pre-installed on them.

23. In the SSH session terminal window, run the configure command to update the AWS CLI software with credentials.

    ```
    aws configure
    ```

24. At the prompt, configure the following:
    - **AWS Access Key ID**: Choose the Details dropdown list, and choose Show. Copy and paste the **AccessKey** value into the terminal window.
    - **AWS Secret Access Key**: Copy and paste the **SecretKey** value into the terminal window.
    - **Default region name**: Enter `us-west-2`
    - **Default output format**: Enter `json`

Task 3: Create an S3 bucket using the AWS CLI

The s3api command creates a new S3 bucket with the AWS credentials in this lab. By default, the S3 bucket is created in the us-east-1 Region.

Tip: In this lab, you might use the s3api command or the s3 command. s3 commands are built on top of the operations that are found in the s3api commands.

When you create a new S3 bucket, the bucket must have a unique name, such as the combination of your first initial, last name, and three random numbers. For example, if a user's name is Terry Whitlock, a bucket name could be `twhitlock256`

25. To create a bucket in Amazon S3, you use the aws s3api create-bucket command. When you use this command to create an S3 bucket, you also include the following:
    - Specify `--region us-west-2`
    - Add `--create-bucket-configuration LocationConstraint=us-west-2` to the end of the command.

    The following is an example of the command to create a new S3 bucket. You can use `twhitlock256` as your bucket name, or you can replace <*twhitlock256*> with a bucket name that you prefer to use for this lab.

    ```
    aws s3api create-bucket --bucket <twhitlock256> --region us-west-2 --create-bucket-configuration LocationConstraint=us-west-2
    ```

    If the command is successful, you will get a JSON-formatted response with a **Location** name-value pair, where the value reflects the bucket name. The following is an example:

    ```
    {
       "Location": http://twhitlock256.s3.amazonaws.com/
    }
    ```

Task 4: Create a new IAM user that has full access to Amazon S3

The AWS CLI command: `aws iam create-user` creates a new IAM user for your AWS account. The option `--user-name` is used to create the name of the user and must be unique within the account.

26. Using the AWS CLI, create a new IAM user with the command `aws iam create-user` and username `awsS3user`:

    ```
    aws iam create-user --user-name awsS3user
    ```

27. Create a login profile for the new user by using the following command:

    ```
    aws iam create-login-profile --user-name awsS3user --password Training123!
    ```

28. Copy the AWS account number:
    - In the AWS Management Console, choose the account **voclabs/user...** drop down menu located at the top right of the screen.
    - Copy the 12 digit **Account ID** number.
    - In the current drop down menu, choose **Sign Out**.
29. Log in to the AWS Management Console as the new **awsS3user** user:
    - In the browser tab where you just signed out of the AWS Management Console, choose **Log back in** or **Sign in to the Console**.
    - In the sign-in screen, choose the radio button **IAM user**.
    - In the text field, paste or enter the account ID with no dashes.
    - Choose **Next**.
    - A new login screen with **Sign in as IAM user** field will show. The account ID will be filled in from the previous screen.
    - For **IAM user name**, enter `awsS3user`
    - For **Password**, enter `Training123!`
    - Choose **Sign In**
30. On the AWS Management Console, in the **Search** box, enter `S3` and choose **S3**. This option takes you to the Amazon S3 console page.

    Note: The bucket that you created might not be visible. Refresh the Amazon S3 console page to see if it appears. The **awsS3user** user does not have Amazon S3

access to the bucket that you created, so you might see an error for **Access** to this bucket.

31. In the terminal window, to find the AWS managed policy that grants full access to Amazon S3, run the following command:

    ```
    aws iam list-policies --query "Policies[?contains(PolicyName,'S3')]"
    ```

    The result displays policies that have a **PolicyName** attribute containing the term S3. Locate the policy that grants full access to Amazon S3. You use this policy in the next step.

32. To grant the **awsS3user** user full access to the S3 bucket, replace <*policyYouFound*> in following command with the appropriate **PolicyName** from the results, and run the adjusted command:

    ```
    aws iam attach-user-policy --policy-arn arn:aws:iam::aws:policy/<policyYouFound> --user-name awsS3user
    ```

33. Return to the AWS Management Console, and refresh the browser tab.

    If you implemented the correct policy, the **Access** portion of the bucket now has **Objects can be public**.

Task 5: Extract the files that you need for this lab

A file containing the `static-website` contents for the Amazon S3 bucket will need to be extracted in the following step.

34. Back in the SSH terminal, extract the files that you need for this lab by running the following commands:

    ```
    cd ~/sysops-activity-files
    tar xvzf static-website-v2.tar.gz
    cd static-website
    ```

35. To confirm that the files were extracted correctly, run the `ls` command.

    You should see a file named index.html and directories named css and images.

Task 6: Upload files to Amazon S3 by using the AWS CLI

Once the files are extracted, you upload the contents of the file to Amazon S3. These files include what you explored when you ran the ls command.

36. So that the bucket can function as a website, replace <*my-bucket*> in the following command with your bucket name, and run the adjusted command.

    ```
    aws s3 website s3://<my-bucket>/ --index-document index.html
    ```

    This process helps ensure that the index.html file will be known as the index document.

37. To upload the files to the bucket, replace <*my-bucket*> in the following command with your bucket name, and run the adjusted command:

    ```
    aws s3 cp /home/ec2-user/sysops-activity-files/static-website/ s3://<my-bucket>/ --recursive --acl public-read
    ```

    Notice that the upload command includes an access control list (ACL) parameter. This parameter specifies that the uploaded files have public read access. It also includes the recursive parameter, which indicates that all files in the current directory on your machine should be uploaded.

38. To verify that the files were uploaded, replace <*my-bucket*> in the following command with your bucket name, and run the adjusted command:

    ```
    aws s3 ls <my-bucket>
    ```

39. On the **AWS Management Console**, on the Amazon S3 console, choose your bucket name.
40. Choose the **Properties** tab. At the bottom of the this tab, note that **Static website hosting** is **Enabled**. Running the aws s3 website AWS CLI command turns on the static website hosting for an Amazon S3 bucket. This option is usually turned off by default.
41. To open the URL on a new page, choose the **Bucket website endpoint** URL that displays.

Task 7: Create a batch file to make updating the website repeatable

To create a repeatable deployment, you create a batch file by using the VI editor.

42. In the terminal window, to pull up the history of recent commands, run the following command:

    ```
    history
    ```

43. Locate the line where you ran the aws s3 cp command. You will put this line in your new batch file.
44. To change directories and create an empty file, run the following command in the SSH terminal session:

    ```
    cd ~
    touch update-website.sh
    ```

45. To open the empty file in the VI editor, run the following command.

    ```
    vi update-website.sh
    ```

46. To enter edit mode in the VI editor, press `i`
47. Next, you add the standard first line of a bash file and then add the s3 cp line from your history. To do so, replace <*my-bucket*> in the following command with your bucket name, and copy and paste the adjusted command into your file:

    ```
    #!/bin/bash
    aws s3 cp /home/ec2-user/sysops-activity-files/static-website/ s3://<my-bucket>/ --recursive --acl public-read
    ```

48. To write the changes and quit the file, press Esc, enter `:wq` and then press Enter.
49. To make the file an executable batch file, run the following command:

    ```
    chmod +x update-website.sh
    ```

50. To open the local copy of the index.html file in a text editor, run the following command:

    ```
    vi sysops-activity-files/static-website/index.html
    ```

51. To enter edit mode in the VI editor, press `i` and modify the file as follows:
    - Locate the first line that has the HTML code **bgcolor="aquamarine"** and change this code to `bgcolor="gainsboro"`
    - Locate the line that has the HTML code **bgcolor="orange"** and change this code to `bgcolor="cornsilk"`
    - Locate the second line that has the HTML code **bgcolor="aquamarine"** and change this code to `bgcolor="gainsboro"`
    - To write the changes and quit the file, press Esc, enter `:wq` and then press Enter.
52. To update the website, run your batch file.

    ```
    ./update-website.sh
    ```

    Note: The command line output should show that the files were copied to Amazon S3.

53. To see the changes to the website, return to the browser and refresh the Café and Bakery page.

Congratulations, you just made your first revision to the website!

You now have a tool (the script that you created) that you can use to push changes from your website source files to Amazon S3.

Optional challenge

Did you notice that your batch file uploads every file to Amazon S3 every time you run it even when most of the files have no changes to them?

- Take a look at the following document: AWS CLI reference documentation for sync.
- Make a small noticeable change to the index.html file. For example, modify one of the colors, and save the change.
- Run the updated batch file.
- To help make your script more efficient, you replace the aws s3 cp command that you've been using with the aws s3 sync command from this document. The following is an example of the aws s3 sync command that you run in the SSH terminal window. In this command, replace <*my-bucket*> with your bucket name.

```
aws s3 sync /home/ec2-user/sysops-activity-files/static-website/ <s3://<my-bucket>/ --acl public-read
```

- Refresh the Café and Bakery site to see your changes.
- How was the `aws s3 sync` command more efficient than the `aws s3 cp` command? Did the `aws s3 sync` command update just the index.html file or upload all the files like the `aws s3 sync` command?

Conclusion

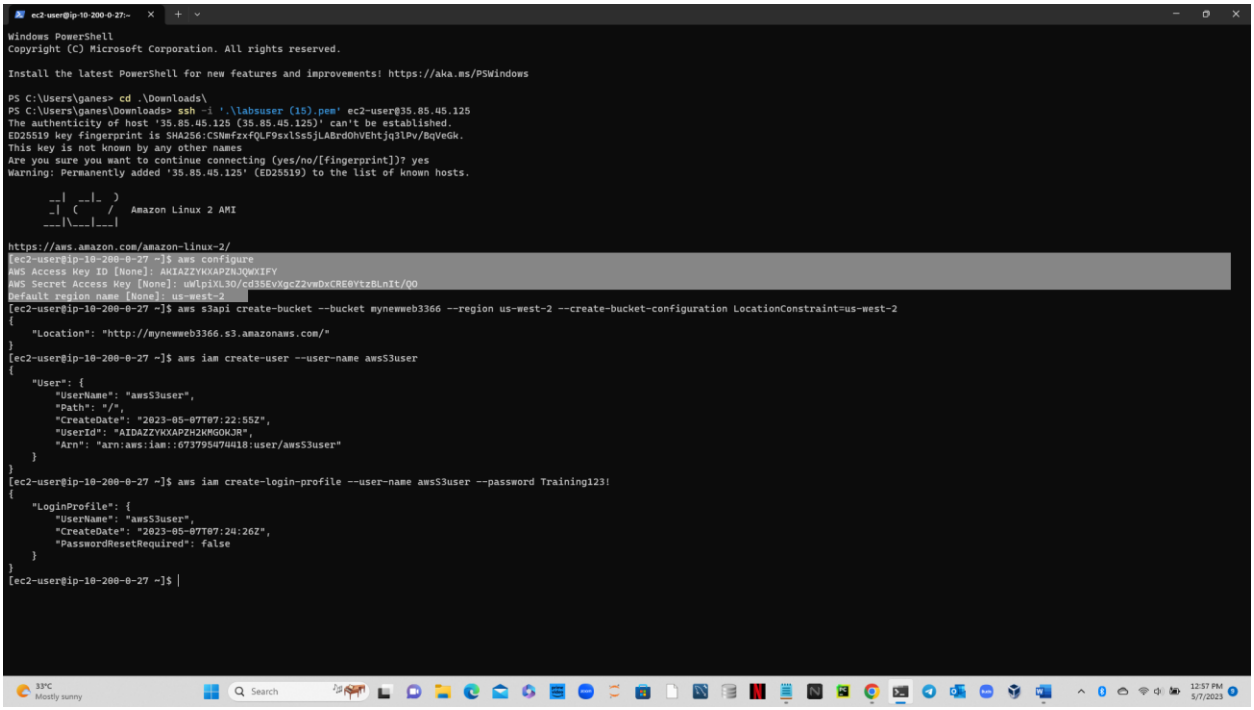
Congratulations! You now have successfully done the following:

- Ran AWS CLI commands that use IAM and Amazon S3 services
- Deployed a static website to an S3 bucket
- Created a script that uses the AWS CLI to copy files in a local directory to Amazon S3

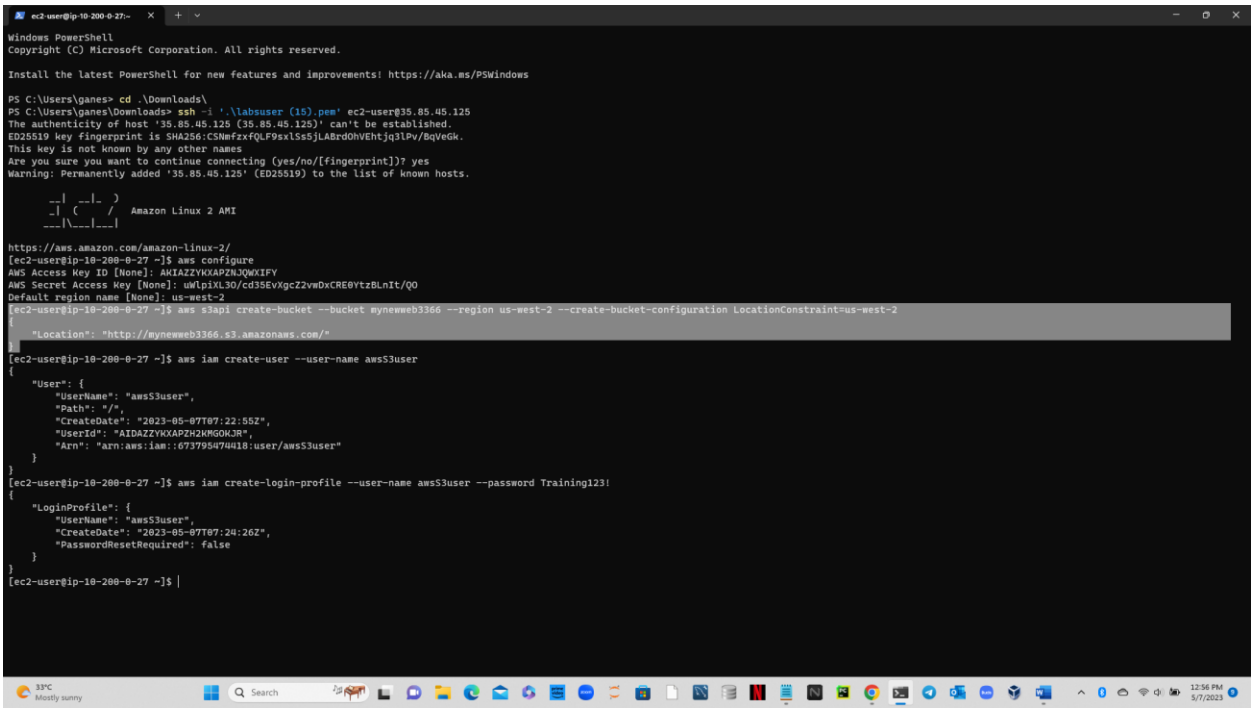
Additional resources

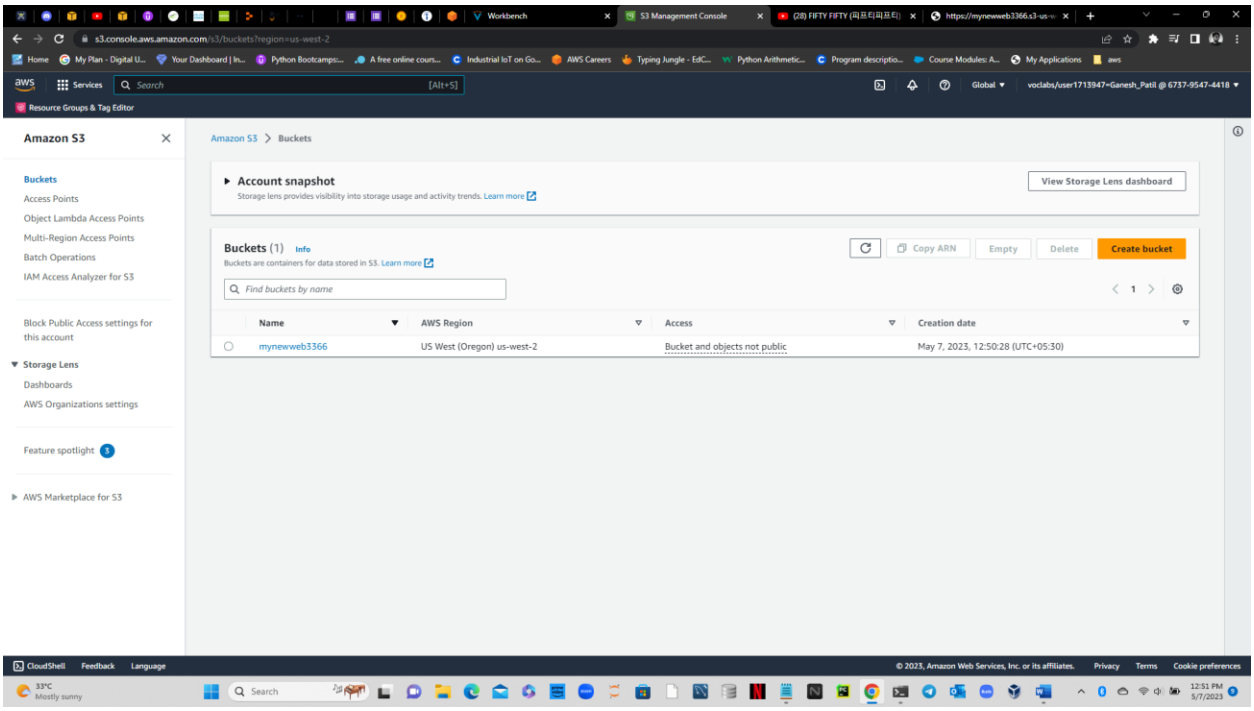
- S3 API
- Installing or Updating the Latest Version of the AWS CLI
- Troubleshooting AWS CLI Errors

Task 2: Configure the AWS CLI

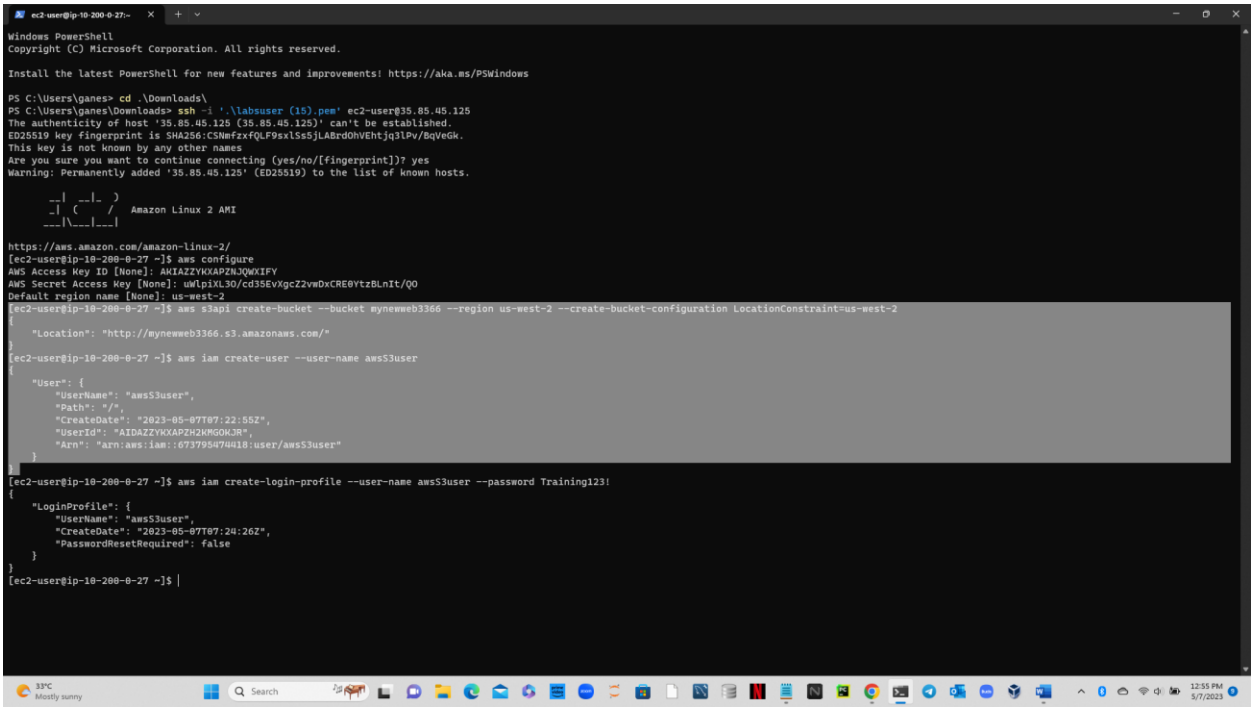


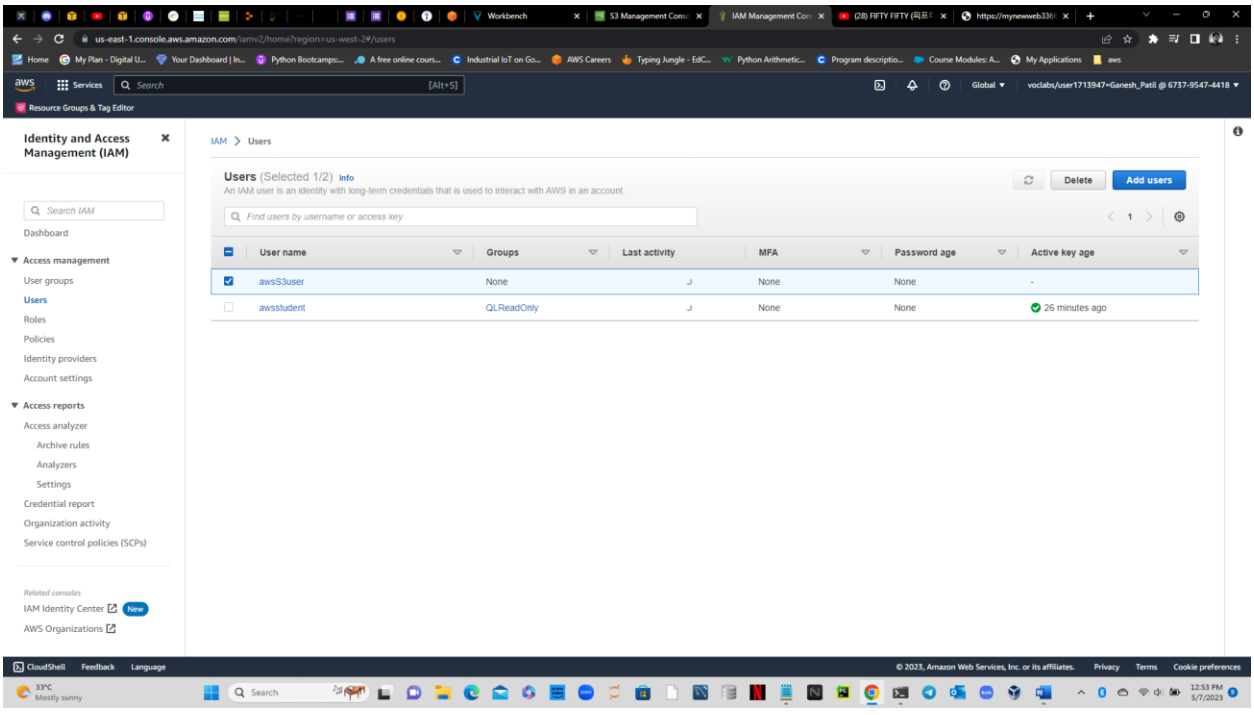
Task 3: Create an S3 bucket using the AWS CLI

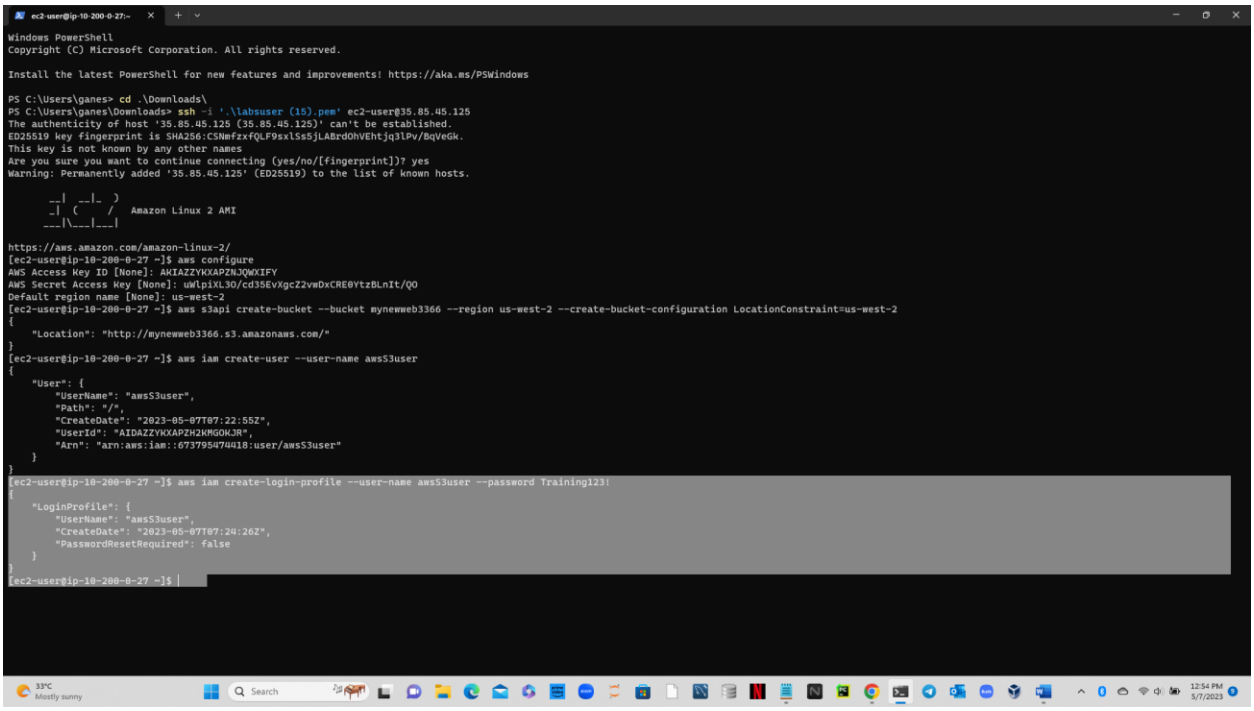


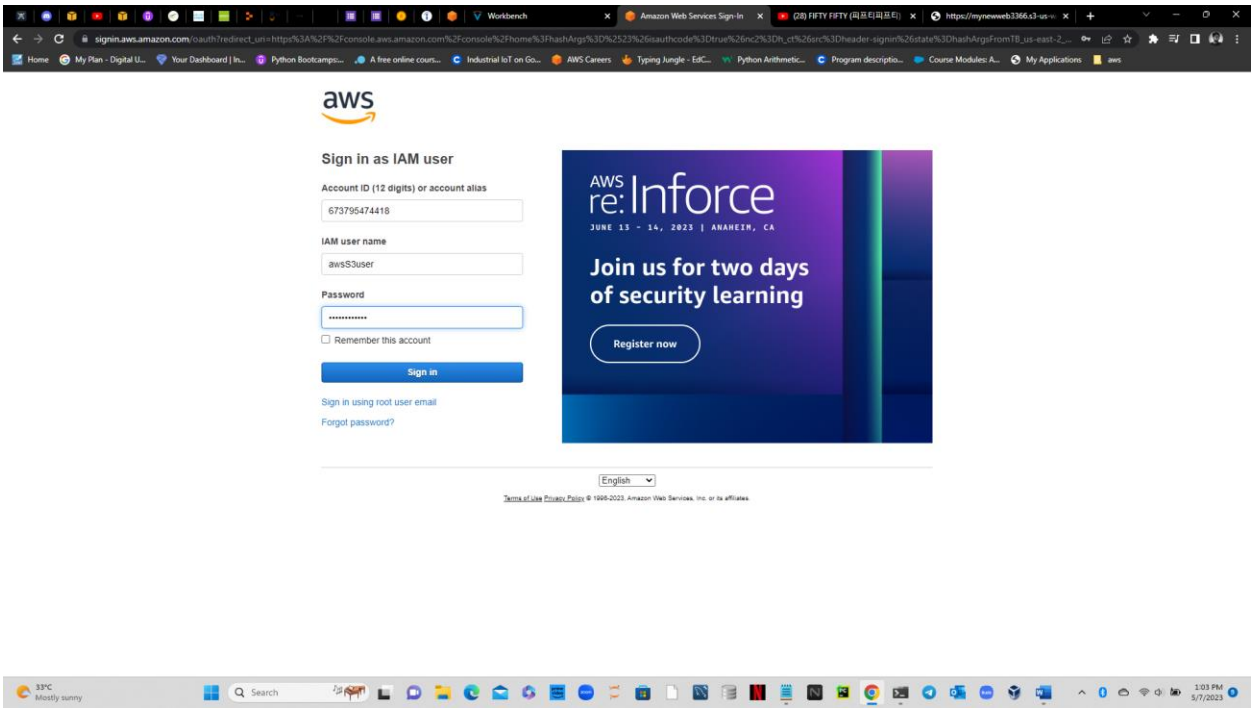

Workbench
S3 Management Console
https://mynewweb3366.s3-us-w
s3.console.aws.amazon.com/s3/buckets?region=us-west-2
Services
Search
[Alt+S]
Global
voclabs/user1713947=Ganesh_Patil @ 6737-9547-4418
Resource Groups & Tag Editor
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
mynewweb3366
US West (Oregon) us-west-2
Bucket and objects not public
May 7, 2023, 12:50:28 (UTC+05:30)
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Mostly sunny
Search
12:51 PM
5/7/2023

Task 4: Create a new IAM user that has full access to Amazon S3






ec2-user@ip-10-200-0-27:~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\ganes> cd .\Downloads\
PS C:\Users\ganes\Downloads> ssh -i '.\labsuser (15).pem' ec2-user@35.85.45.125
The authenticity of host '35.85.45.125 (35.85.45.125)' can't be established.
ED25519 key fingerprint is SHA256:CSNmfzxfQLF9sxlSs5jLABrdOhVEhtjq3lPv/BqVeGk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.85.45.125' (ED25519) to the list of known hosts.
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-200-0-27 ~]$ aws configure
AWS Access Key ID [None]: AKIAZZYKXAPZNJQWXIFY
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
[ec2-user@ip-10-200-0-27 ~]$ aws s3api create-bucket --bucket mynewweb3366 --region us-west-2 --create-bucket-configuration LocationConstraint=us-west-2
{
"Location": "http://mynewweb3366.s3.amazonaws.com/"
}
[ec2-user@ip-10-200-0-27 ~]$ aws iam create-user --user-name awsS3user
{
"User": {
"UserName": "awsS3user",
"Path": "/",
"CreateDate": "2023-05-07T07:22:55Z",
"UserId": "AIDAZZYKXAPZH2KMGOKJR",
"Arn": "arn:aws:iam::673795474418:user/awsS3user"
}
}
[ec2-user@ip-10-200-0-27 ~]$ aws iam create-login-profile --user-name awsS3user --password Training123!
{
"LoginProfile": {
"UserName": "awsS3user",
"CreateDate": "2023-05-07T07:24:26Z",
"PasswordResetRequired": false
}
}
[ec2-user@ip-10-200-0-27 ~]$

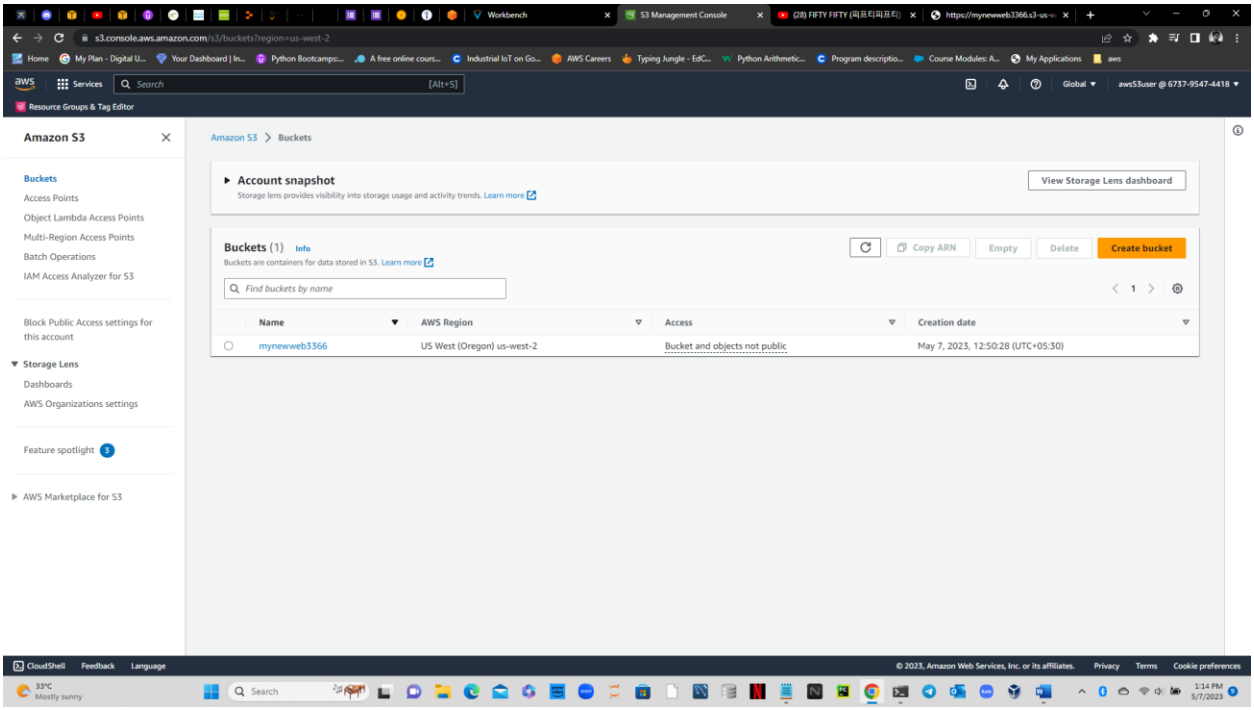

Workbench
Amazon Web Services Sign-In
aws
Sign in as IAM user
Account ID (12 digits) or account alias
673795474418
IAM user name
awsS3user
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
AWS re:Inforce
JUNE 13 - 14, 2023 | ANAHEIM, CA
Join us for two days of security learning
Register now
English
Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

```
[ec2-user@ip-10-200-0-27 ~]$ aws iam list-policies --query "Policies[?contains(PolicyName,'S3')]"
[
    {
        "PolicyName": "AmazonS3FullAccess",
        "PermissionsBoundaryUsageCount": 0,
        "CreateDate": "2015-02-06T18:40:58Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "ANPAIFIR6V6BVTRAHWINE",
        "DefaultVersionId": "v2",
        "Path": "/",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3FullAccess",
        "UpdateDate": "2021-09-27T20:16:37Z"
    },
    {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PermissionsBoundaryUsageCount": 0,
        "CreateDate": "2015-02-06T18:40:59Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "DefaultVersionId": "v2",
        "Path": "/",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "UpdateDate": "2021-09-27T20:24:58Z"
    },
    {
        "PolicyName": "AmazonDMSRedshiftS3Role",
        "PermissionsBoundaryUsageCount": 0,
        "CreateDate": "2016-04-20T17:05:56Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "ANPAI3CCUQ4U5WNC5F6B6",
        "DefaultVersionId": "v3",
        "Path": "/service-role/",
        "Arn": "arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role",
        "UpdateDate": "2019-07-08T18:19:14Z"
    },
    {
        "PolicyName": "QuickSightAccessForS3StorageManagementAnalyticsReadOnly",
        "PermissionsBoundaryUsageCount": 0,
        "CreateDate": "2017-06-12T18:18:38Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "ANPAIFWG3L3WDMR4I7ZJW",
        "DefaultVersionId": "v4",
        "Path": "/service-role/",
```

```
      "Arn": "arn:aws:iam::aws:policy/service-
role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly",
      "UpdateDate": "2019-10-08T23:53:11Z"
    },
    {
      "PolicyName": "AmazonS3OutpostsFullAccess",
      "PermissionsBoundaryUsageCount": 0,
      "CreateDate": "2020-10-02T17:26:30Z",
      "AttachmentCount": 0,
      "IsAttachable": true,
      "PolicyId": "ANPAZKAPJZG4BKMLUXKOR",
      "DefaultVersionId": "v1",
      "Path": "/",
      "Arn": "arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess",
      "UpdateDate": "2020-10-02T17:26:30Z"
    },
    {
      "PolicyName": "AmazonS3OutpostsReadOnlyAccess",
      "PermissionsBoundaryUsageCount": 0,
      "CreateDate": "2020-10-02T18:55:58Z",
      "AttachmentCount": 0,
      "IsAttachable": true,
      "PolicyId": "ANPAZKAPJZG4PJ2AX4CUB",
      "DefaultVersionId": "v1",
      "Path": "/",
      "Arn": "arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess",
      "UpdateDate": "2020-10-02T18:55:58Z"
    },
    {
      "PolicyName": "S3StorageLensServiceRolePolicy",
      "PermissionsBoundaryUsageCount": 0,
      "CreateDate": "2020-11-18T18:15:40Z",
      "AttachmentCount": 0,
      "IsAttachable": true,
      "PolicyId": "ANPAZKAPJZG4IHOVJESMS",
      "DefaultVersionId": "v1",
      "Path": "/aws-service-role/",
      "Arn": "arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy",
      "UpdateDate": "2020-11-18T18:15:40Z"
    },
    {
      "PolicyName": "IVSRecordToS3",
      "PermissionsBoundaryUsageCount": 0,
      "CreateDate": "2020-12-05T00:10:43Z",
      "AttachmentCount": 0,
      "IsAttachable": true,
      "PolicyId": "ANPAZKAPJZG4M65NGVKOJ",
      "DefaultVersionId": "v1",
```

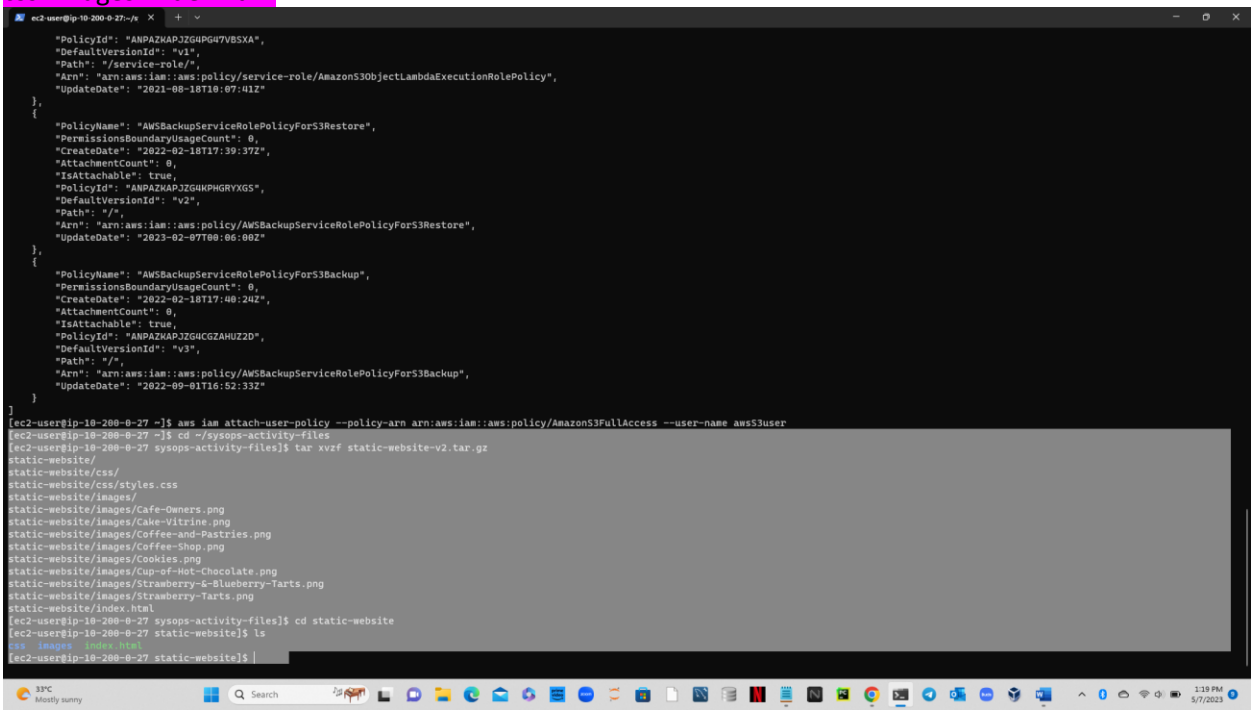
```
    "Path": "/aws-service-role/",
    "Arn": "arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3",
    "UpdateDate": "2020-12-05T00:10:43Z"
  },
  {
    "PolicyName": "AmazonS3ObjectLambdaExecutionRolePolicy",
    "PermissionsBoundaryUsageCount": 0,
    "CreateDate": "2021-08-18T10:07:41Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ANPAZKAPJZG4PG47VBSXA",
    "DefaultVersionId": "v1",
    "Path": "/service-role/",
    "Arn": "arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy",
    "UpdateDate": "2021-08-18T10:07:41Z"
  },
  {
    "PolicyName": "AWSBackupServiceRolePolicyForS3Restore",
    "PermissionsBoundaryUsageCount": 0,
    "CreateDate": "2022-02-18T17:39:37Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ANPAZKAPJZG4KPHGRYXGS",
    "DefaultVersionId": "v2",
    "Path": "/",
    "Arn": "arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore",
    "UpdateDate": "2023-02-07T00:06:00Z"
  },
  {
    "PolicyName": "AWSBackupServiceRolePolicyForS3Backup",
    "PermissionsBoundaryUsageCount": 0,
    "CreateDate": "2022-02-18T17:40:24Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ANPAZKAPJZG4CGZAHUZ2D",
    "DefaultVersionId": "v3",
    "Path": "/",
    "Arn": "arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup",
    "UpdateDate": "2022-09-01T16:52:33Z"
  }
]
```


```
[ec2-user@ip-10-200-0-27 ~]$ aws iam attach-user-policy --policy-arn
arn:aws:iam::aws:policy/AmazonS3FullAccess --user-name awsS3user
```

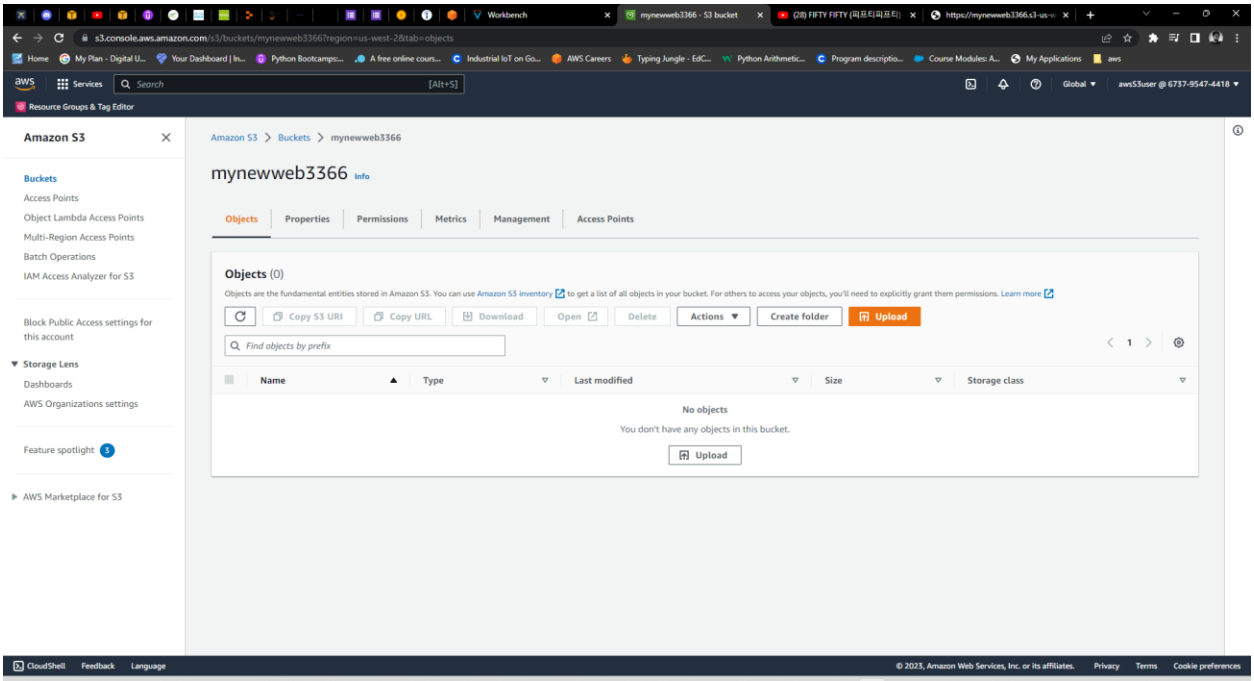

Workbench
S3 Management Console
s3.console.aws.amazon.com/s3/buckets?region=us-west-2
Services
Search
[Alt+S]
Global
awss3user @ 6737-9547-4418
Resource Groups & Tag Editor
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
mynewweb3366
US West (Oregon) us-west-2
Bucket and objects not public
May 7, 2023, 12:50:28 (UTC+05:30)
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Mostly sunny
Search
1:14 PM
5/7/2023

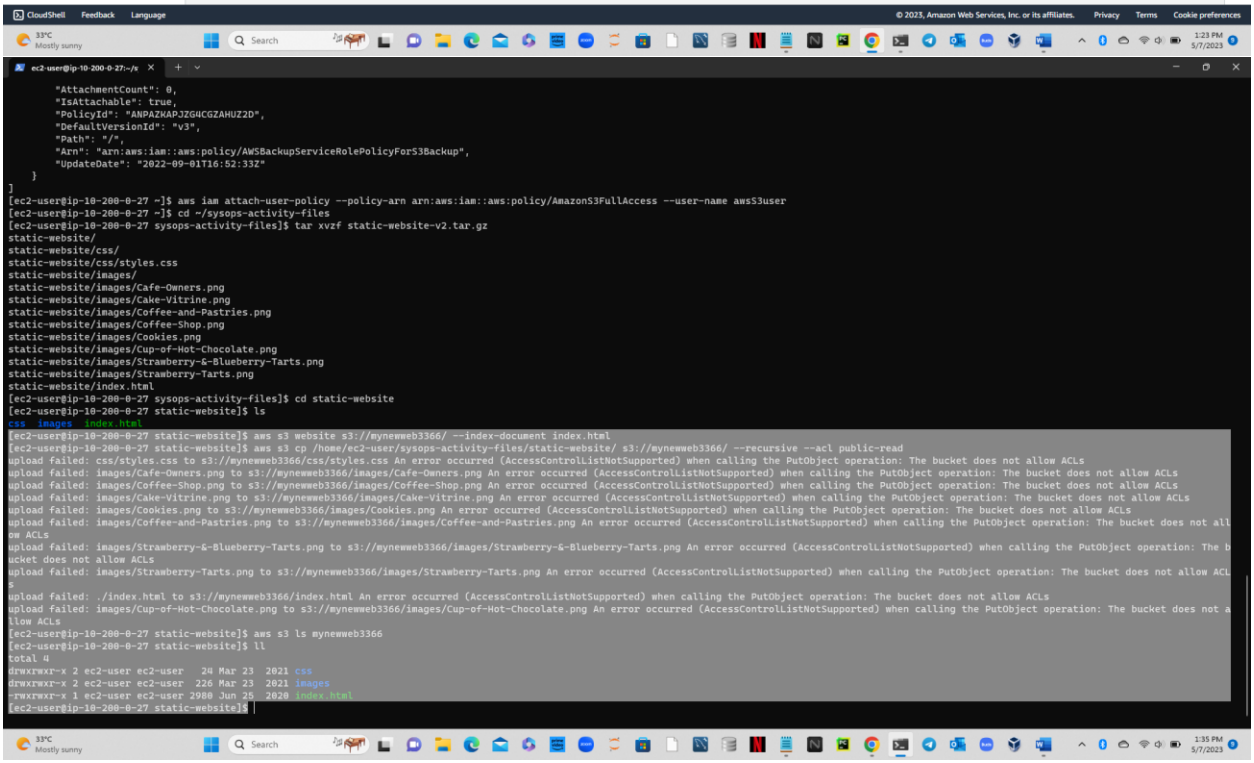
Task 5: Extract the files that you need for this lab

[ec2-user@ip-10-200-0-27 ~]$ cd ~/sysops-activity-files
[ec2-user@ip-10-200-0-27 sysops-activity-files]$ tar xvzf static-website-v2.tar.gz
static-website/
static-website/css/
static-website/css/styles.css
static-website/images/
static-website/images/Cafe-Owners.png
static-website/images/Cake-Vitrine.png
static-website/images/Coffee-and-Pastries.png
static-website/images/Coffee-Shop.png
static-website/images/Cookies.png
static-website/images/Cup-of-Hot-Chocolate.png
static-website/images/Strawberry-&-Blueberry-Tarts.png
static-website/images/Strawberry-Tarts.png
static-website/index.html
[ec2-user@ip-10-200-0-27 sysops-activity-files]$ cd static-website
[ec2-user@ip-10-200-0-27 static-website]$ ls
css images index.html

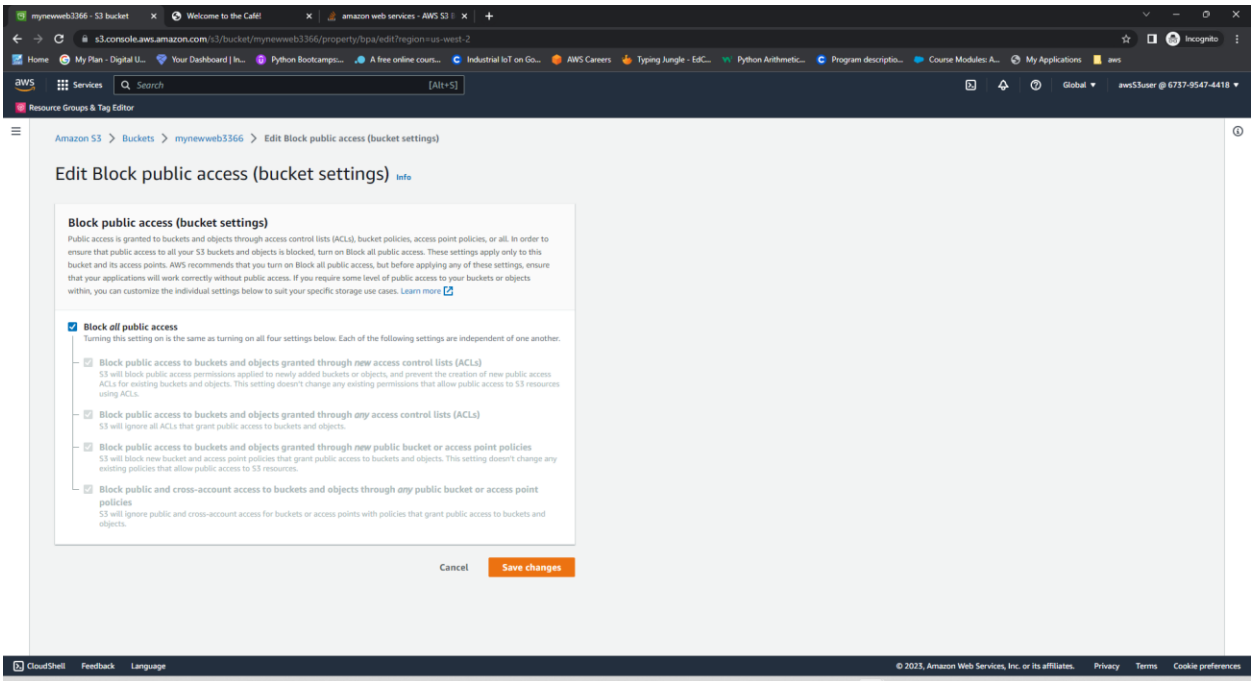


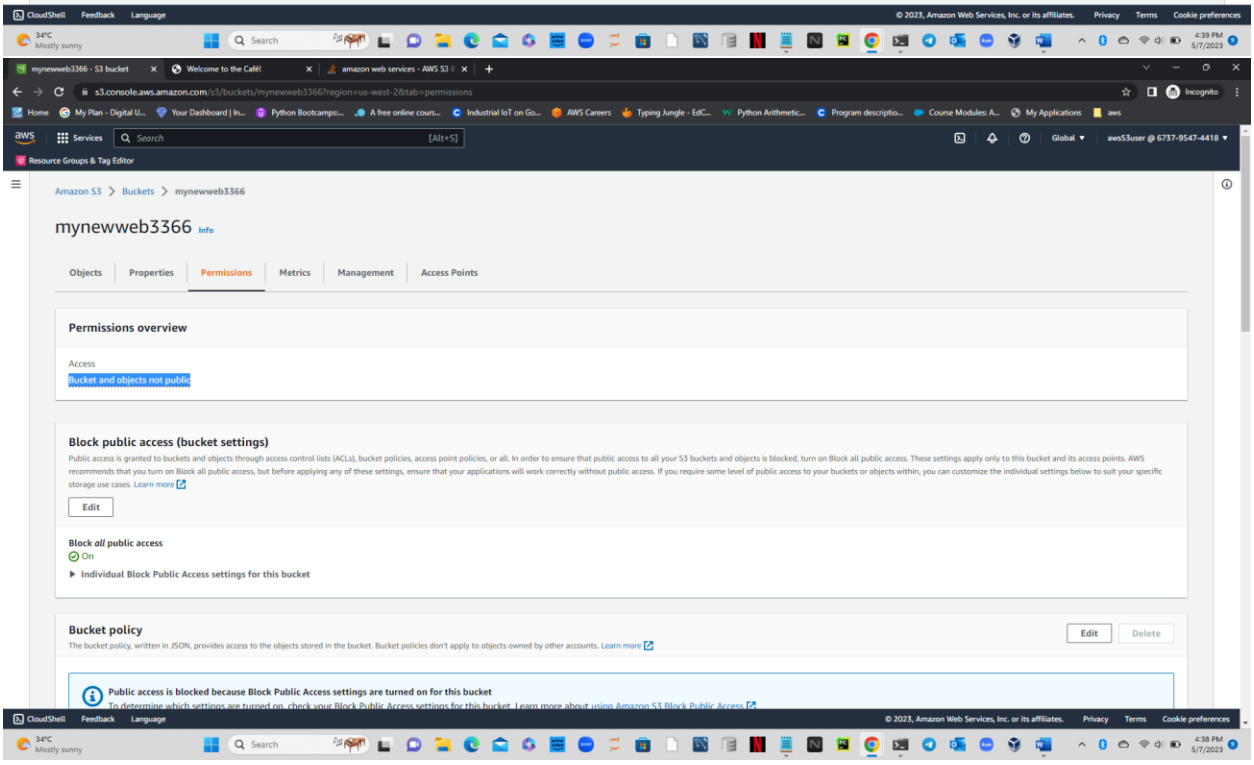
Task 6: Upload files to Amazon S3 by using the AWS CLI

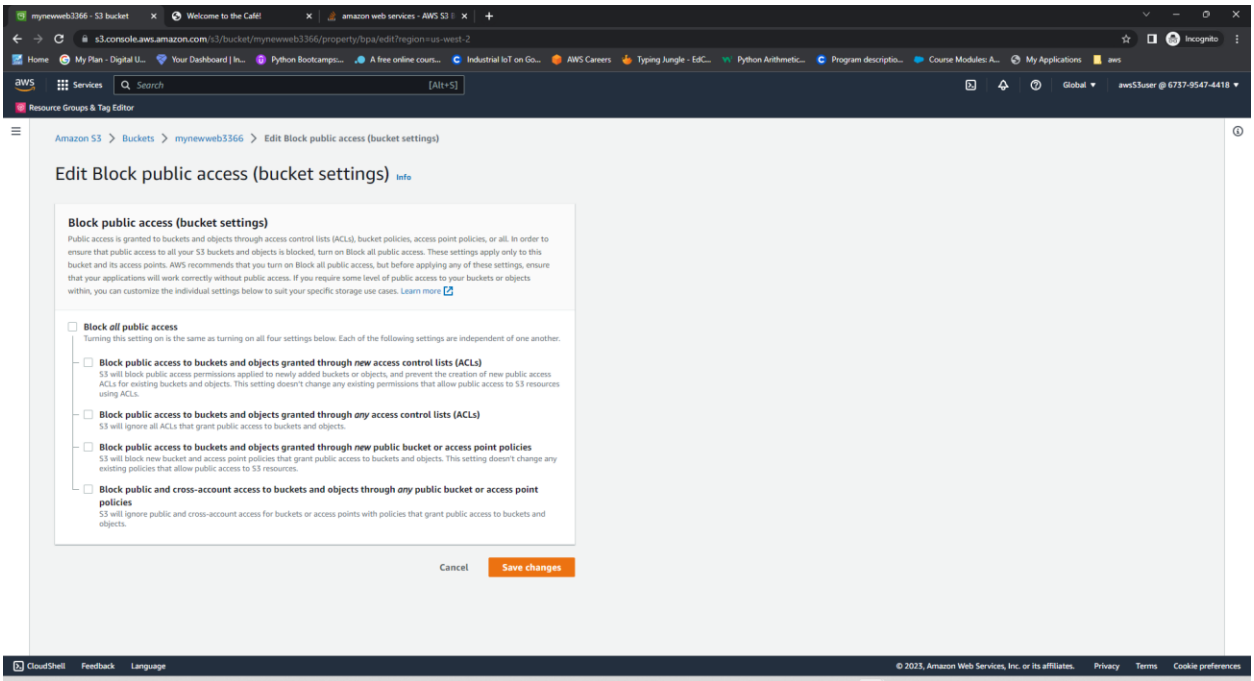


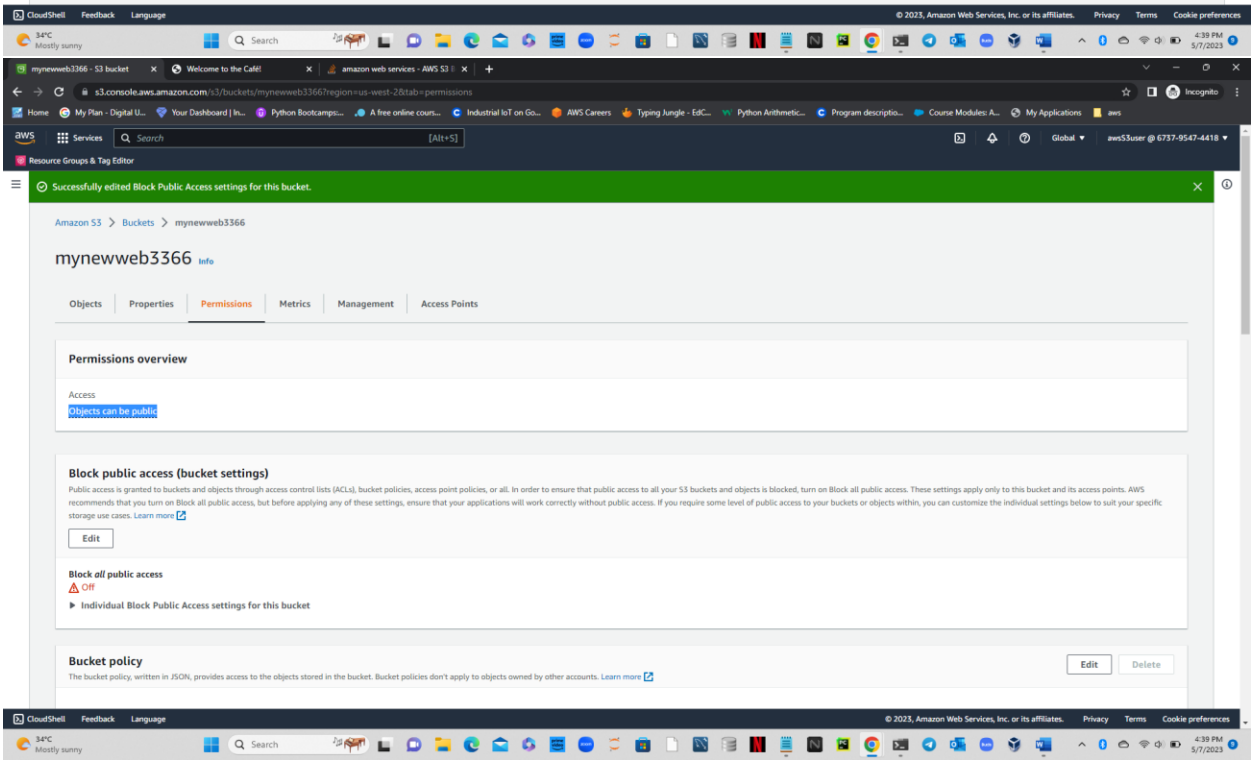


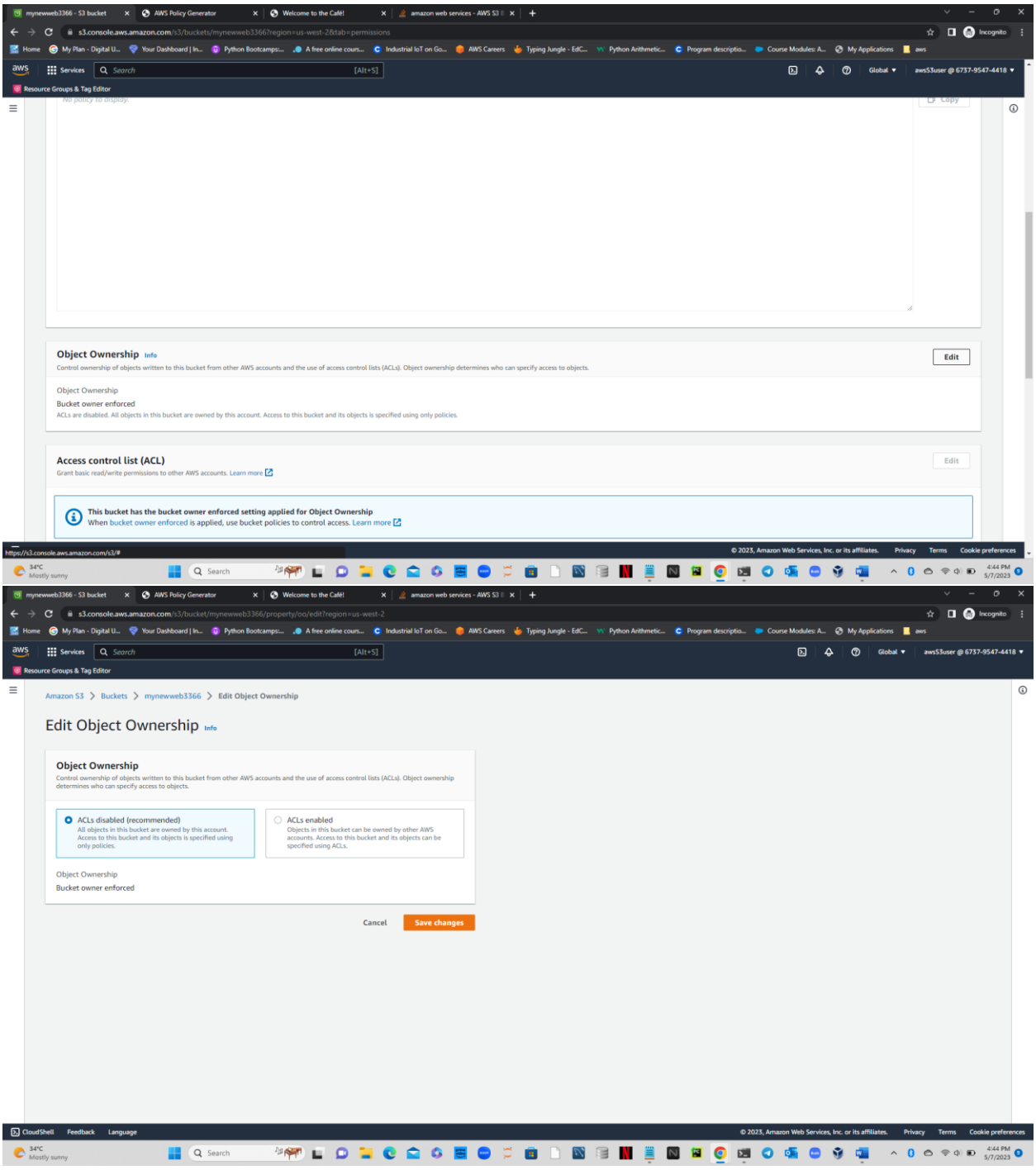
```
[ec2-user@ip-10-200-0-27 static-website]$ aws s3 website s3://mynewweb3366/ --index-document index.html
[ec2-user@ip-10-200-0-27 static-website]$ aws s3 cp /home/ec2-user/sysops-activity-files/static-website/ s3://mynewweb3366/ --recursive --acl public-read
upload failed: css/styles.css to s3://mynewweb3366/css/styles.css An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Cafe-Owners.png to s3://mynewweb3366/images/Cafe-Owners.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Coffee-Shop.png to s3://mynewweb3366/images/Coffee-Shop.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Cake-Vitrine.png to s3://mynewweb3366/images/Cake-Vitrine.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Cookies.png to s3://mynewweb3366/images/Cookies.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Coffee-and-Pastries.png to s3://mynewweb3366/images/Coffee-and-Pastries.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Strawberry-&-Blueberry-Tarts.png to s3://mynewweb3366/images/Strawberry-&-Blueberry-Tarts.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Strawberry-Tarts.png to s3://mynewweb3366/images/Strawberry-Tarts.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: ./index.html to s3://mynewweb3366/index.html An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
upload failed: images/Cup-of-Hot-Chocolate.png to s3://mynewweb3366/images/Cup-of-Hot-Chocolate.png An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs
[ec2-user@ip-10-200-0-27 static-website]$ aws s3 ls mynewweb3366
[ec2-user@ip-10-200-0-27 static-website]$ ll
total 4
drwxrwxr-x 2 ec2-user ec2-user   24 Mar 23  2021 css
drwxrwxr-x 2 ec2-user ec2-user  226 Mar 23  2021 images
-rwxrwxr-x 1 ec2-user ec2-user 2980 Jun 25  2020 index.html
[ec2-user@ip-10-200-0-27 static-website]$
```

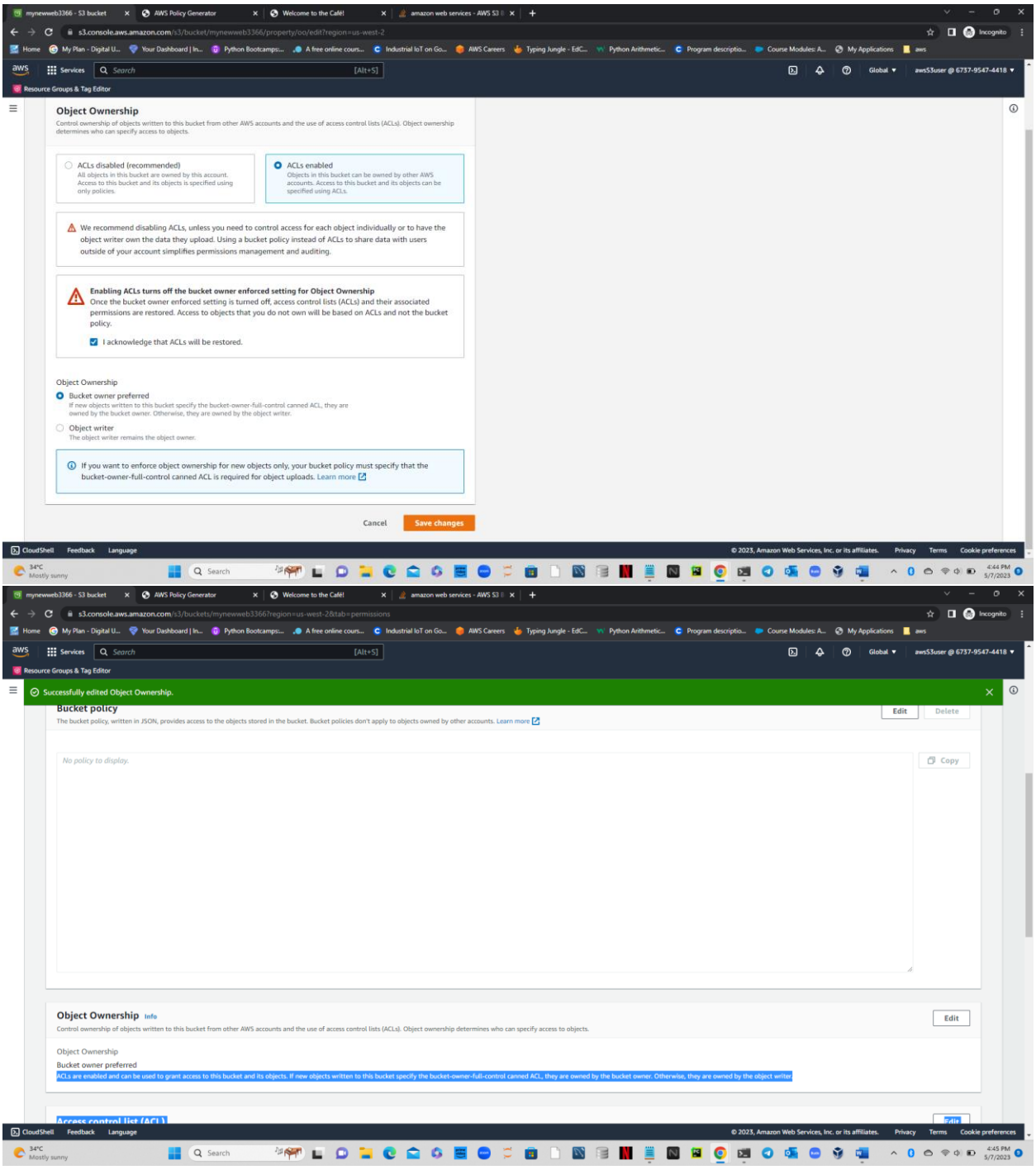

Amazon S3 > Buckets > mynewweb3366 > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Cancel
Save changes


Amazon S3 > Buckets > mynewweb3366
mynewweb3366 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Bucket and objects not public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
On
Individual Block Public Access settings for this bucket
Bucket policy
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
Edit
Delete
Public access is blocked because Block Public Access settings are turned on for this bucket

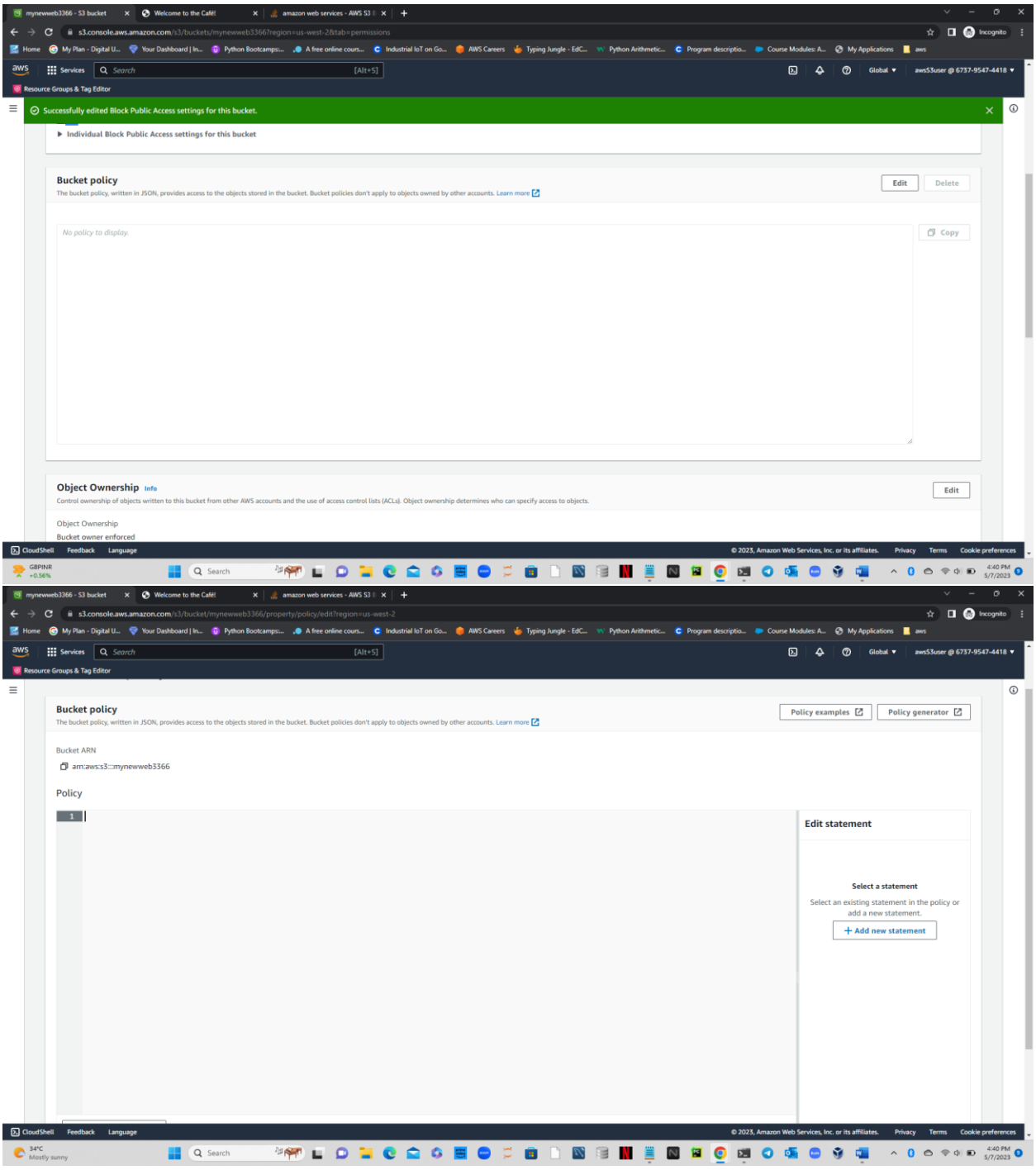

mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
s3.console.aws.amazon.com/s3/bucket/mynewweb3366/property/bpa/edit?region=us-west-2
Incognito
Services
Search
[Alt+S]
Global
aws53user @ 6737-9547-4418
Resource Groups & Tag Editor
Amazon S3 > Buckets > mynewweb3366 > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Cancel
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
34°C
Mostly sunny
Search
4:39 PM
5/7/2023

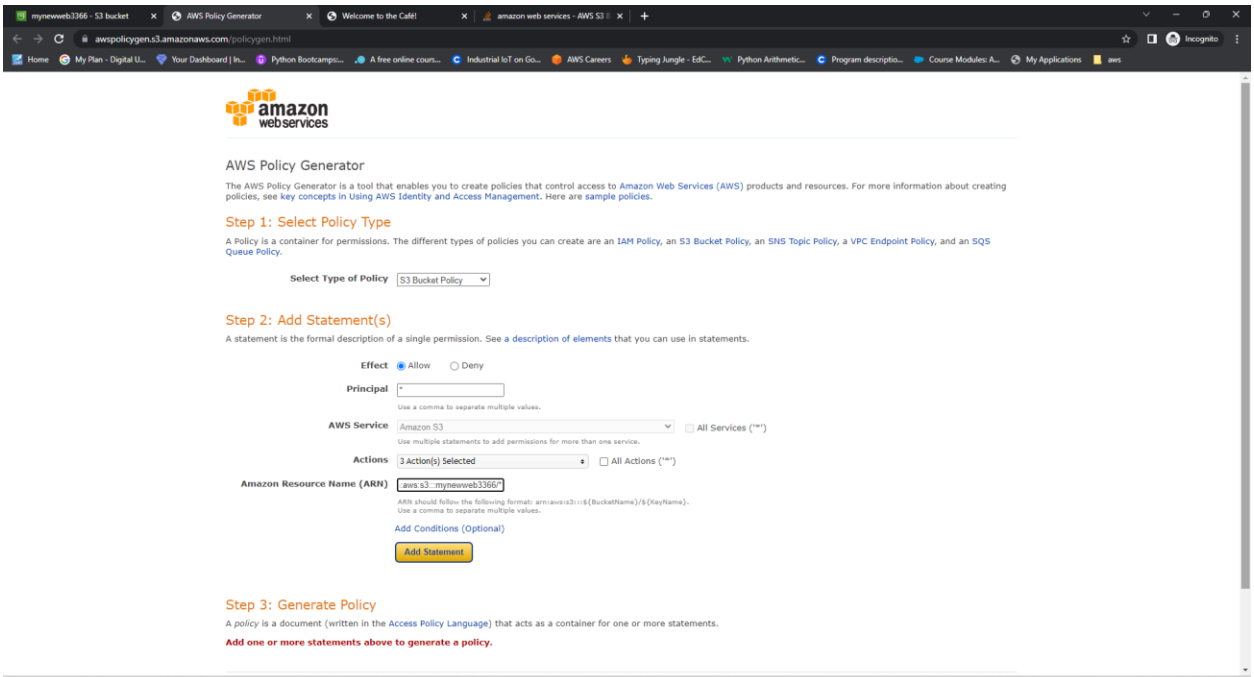

mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
s3.console.aws.amazon.com/s3/buckets/mynewweb3366?region=us-west-2&tab=permissions
Incognito
Services
Search
[Alt+S]
Global
aws53user @ 6737-9547-4418
Resource Groups & Tag Editor
Successfully edited Block Public Access settings for this bucket.
Amazon S3 > Buckets > mynewweb3366
mynewweb3366 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
Bucket policy
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
Edit
Delete
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
34°C
Mostly sunny
Search
4:39 PM
5/7/2023

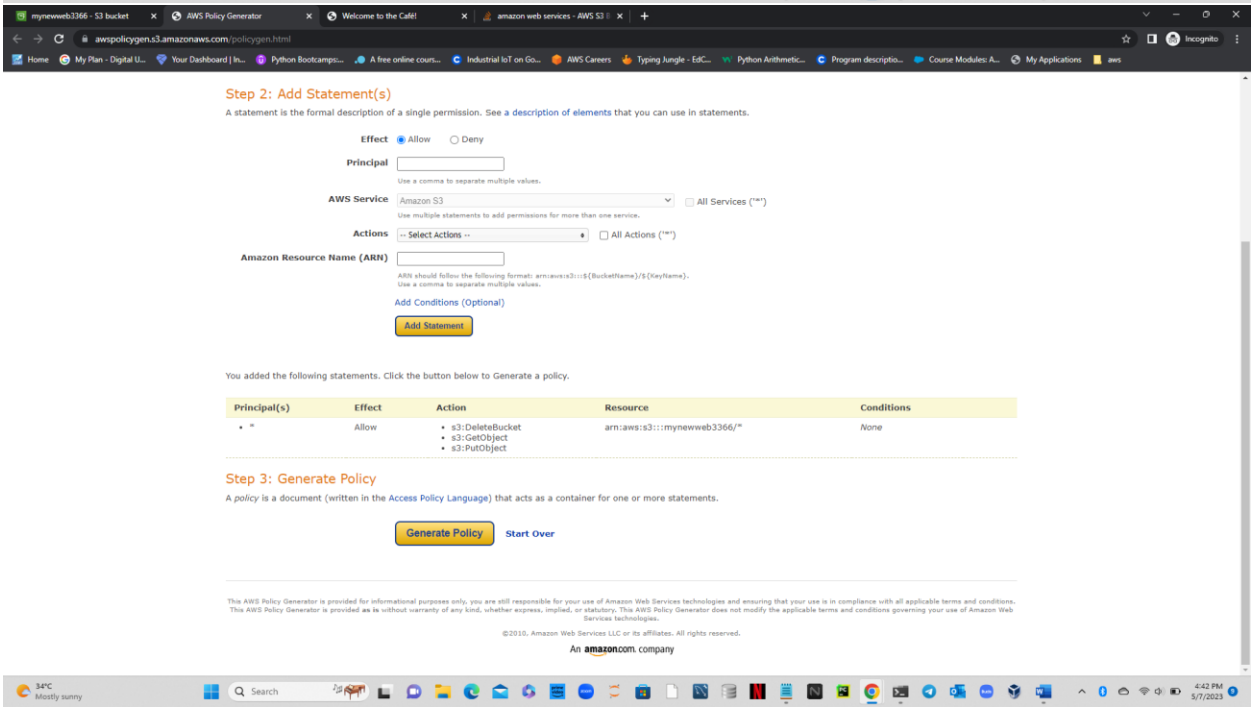

Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Edit
Object Ownership
Bucket owner enforced
ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Edit
This bucket has the bucket owner enforced setting applied for Object Ownership
When bucket owner enforced is applied, use bucket policies to control access. Learn more
Amazon S3 > Buckets > mynewweb3366 > Edit Object Ownership
Edit Object Ownership Info
Object Ownership
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.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Cancel
Save changes

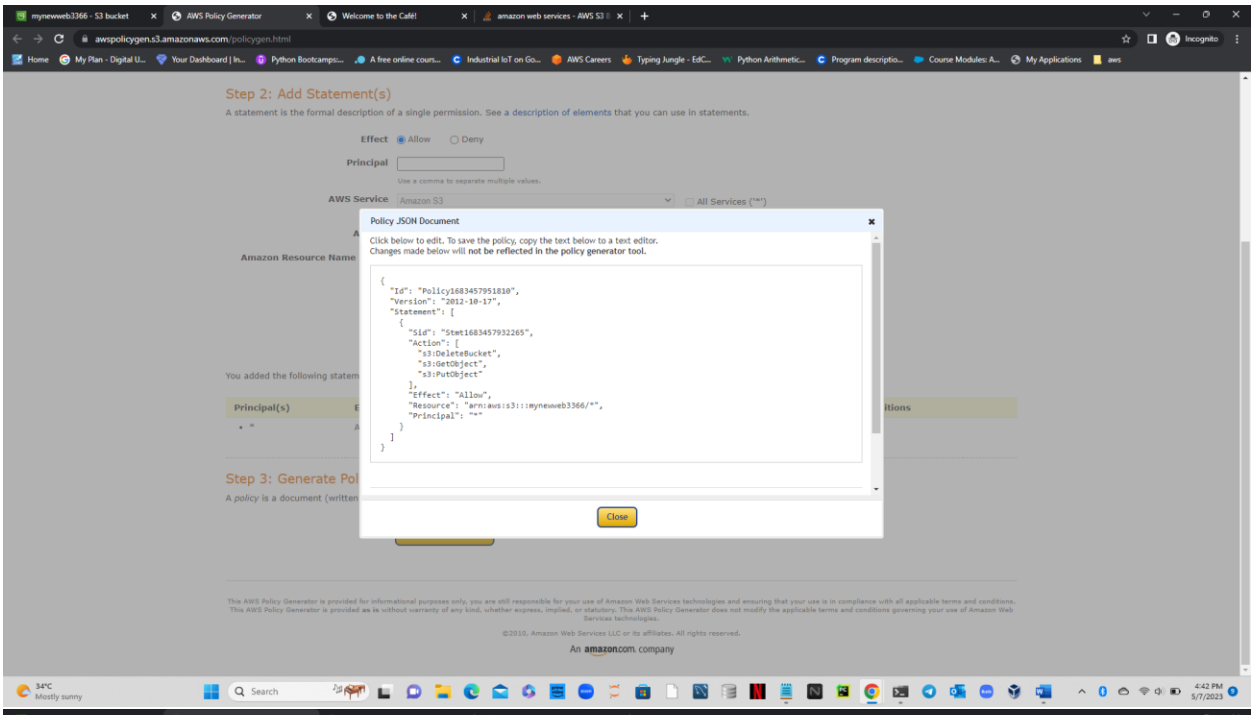

Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.
I acknowledge that ACLs will be restored.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
Cancel
Save changes

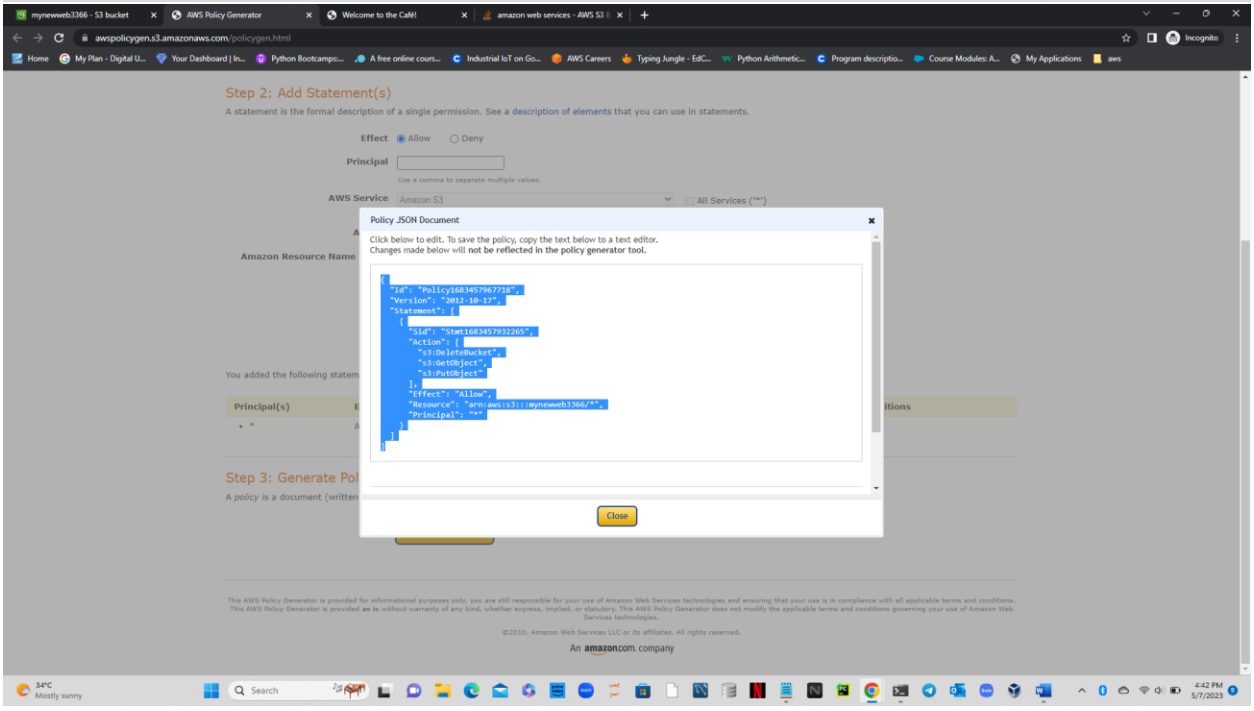
Successfully edited Object Ownership.
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Edit
Delete
No policy to display.
Copy
Object Ownership Info
Control ownership of objects 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.
Edit
Object Ownership
Bucket owner preferred
ACLs are enabled and can be used to grant access to this bucket and its objects. If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Access control list (ACL)
Edit

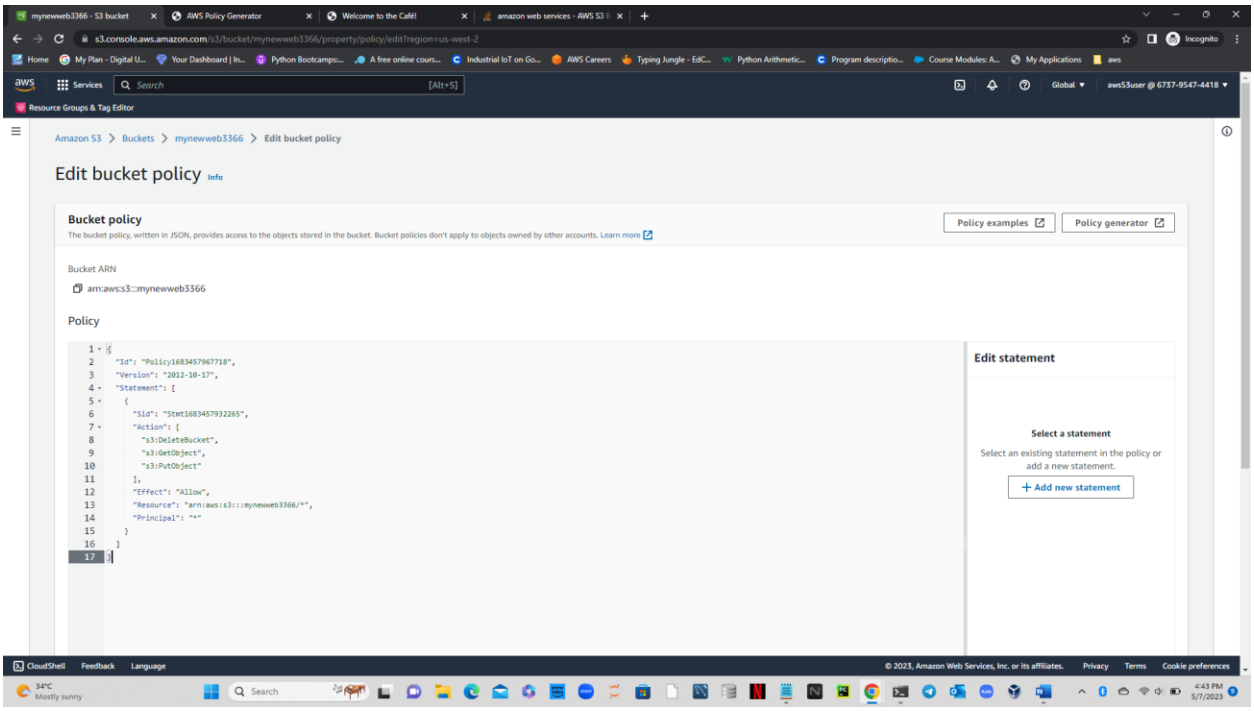

mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
s3.console.aws.amazon.com/s3/buckets/mynewweb3366?region=us-west-2&tab=permissions
Incognito
Services
Search
[Alt+S]
Global
aws53user @ 6737-9547-4418
Resource Groups & Tag Editor
Successfully edited Block Public Access settings for this bucket.
Individual Block Public Access settings for this bucket
Bucket policy
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
Edit
Delete
No policy to display.
Copy
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.
Edit
Object Ownership
Bucket owner enforced
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
GBPINR
+0.56%
4:40 PM
5/7/2023
s3.console.aws.amazon.com/s3/bucket/mynewweb3366/property/policy/edit?region=us-west-2
Bucket policy
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
Policy examples
Policy generator
Bucket ARN
arn:aws:s3:::mynewweb3366
Policy
1
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
34°C
Mostly sunny


mynewweb3366 - S3 bucket
AWS Policy Generator
Welcome to the Café!
amazon web services - AWS S3
awspolicygen.s3.amazonaws.com/policygen.html
Incognito
amazon web services
AWS Policy Generator
The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.
Step 1: Select Policy Type
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.
Select Type of Policy
S3 Bucket Policy
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
*
Use a comma to separate multiple values.
AWS Service
Amazon S3
All Services ('*')
Use multiple statements to add permissions for more than one service.
Actions
3 Action(s) Selected
All Actions ('*')
Amazon Resource Name (ARN)
arn:aws:s3:::mynewweb3366/*
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.
Add Conditions (Optional)
Add Statement
Step 3: Generate Policy
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.
Add one or more statements above to generate a policy.
34°C
Mostly sunny
Search
4:42 PM
5/7/2023


mynewweb3366 - S3 bucket
AWS Policy Generator
Welcome to the Café!
amazon web services - AWS S3
awspolicygen.s3.amazonaws.com/policygen.html
Incognito
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
Use a comma to separate multiple values.
AWS Service
Amazon S3
All Services ('*')
Use multiple statements to add permissions for more than one service.
Actions
-- Select Actions --
All Actions ('*')
Amazon Resource Name (ARN)
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.
Add Conditions (Optional)
Add Statement
You added the following statements. Click the button below to Generate a policy.
Principal(s)
Effect
Action
Resource
Conditions
*
Allow
s3:DeleteBucket
s3:GetObject
s3:PutObject
arn:aws:s3:::mynewweb3366/*
None
Step 3: Generate Policy
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.
Generate Policy
Start Over
This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.
©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An amazon.com company
34°C
Mostly sunny
Search
4:42 PM
5/7/2023

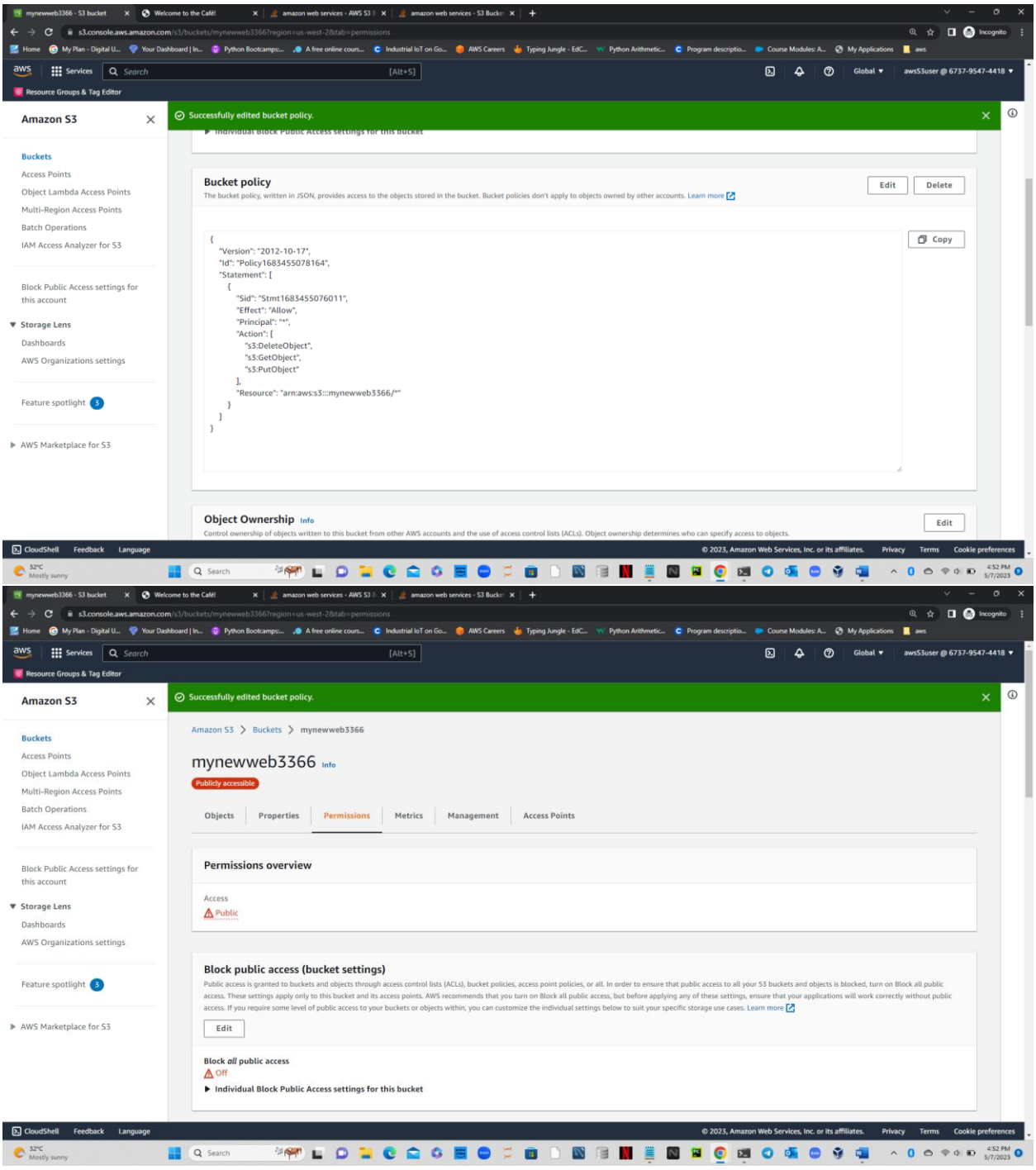

mynewweb3366 - S3 bucket
AWS Policy Generator
Welcome to the Café!
amazon web services - AWS S3
awspolicygen.s3.amazonaws.com/policygen.html
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
AWS Service
Amazon S3
All Services ("*")
Amazon Resource Name
Policy JSON Document
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.
{
"Id": "Policy1683457951810",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1683457932265",
"Action": [
"s3:DeleteBucket",
"s3:GetObject",
"s3:PutObject"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::mynewweb3366/*",
"Principal": "*"
}
]
}
Close
Principal(s)
Step 3: Generate Pol
A policy is a document (written
This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.
©2010. Amazon Web Services LLC or its affiliates. All rights reserved.
An amazon.com company
34°C
Mostly sunny
Search
4:42 PM
5/7/2023


mynewweb3366 - S3 bucket
AWS Policy Generator
Welcome to the Café!
amazon web services - AWS S3
awspolicygen.s3.amazonaws.com/policygen.html
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
AWS Service
Amazon S3
All Services ("*")
Amazon Resource Name
Policy JSON Document
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.
{
"Id": "Policy1683457967718",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1683457932265",
"Action": [
"s3:DeleteBucket",
"s3:GetObject",
"s3:PutObject"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::mynewweb3366/*",
"Principal": "*"
}
]
}
Close
Principal(s)
Step 3: Generate Pol
A policy is a document (written
This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.
©2010. Amazon Web Services LLC or its affiliates. All rights reserved.
An amazon.com company
34°C
Mostly sunny
Search
4:42 PM
5/7/2023

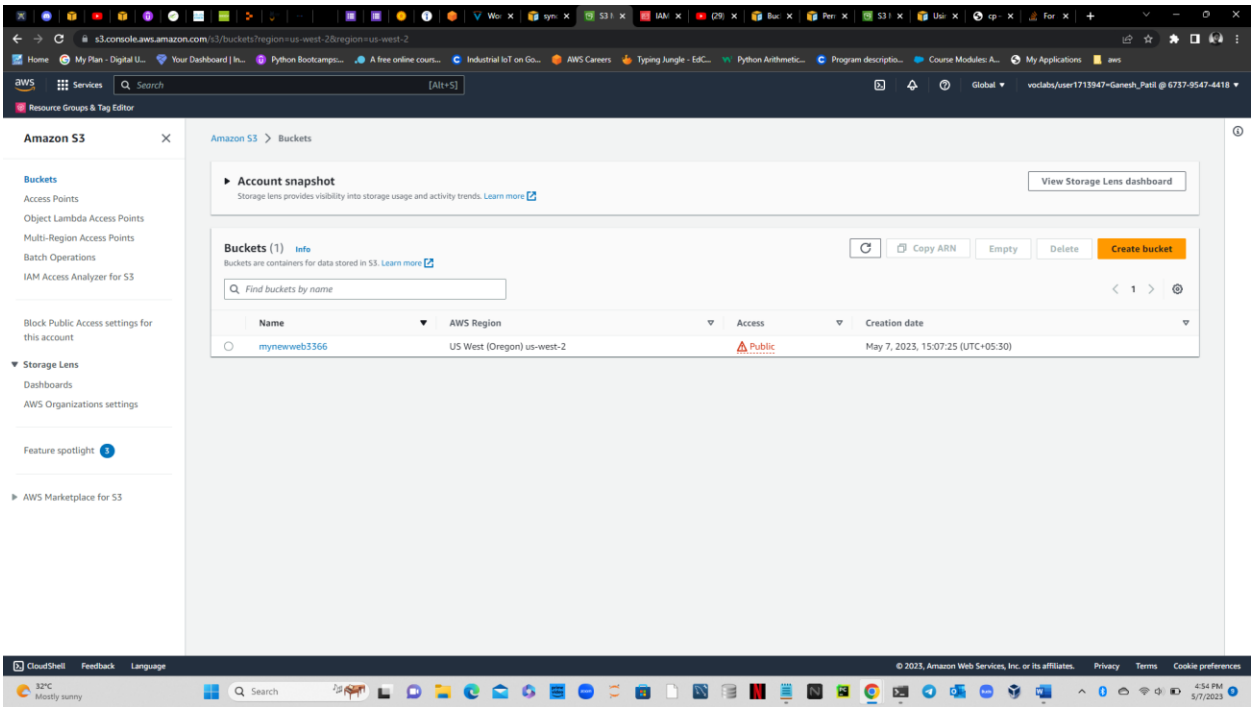


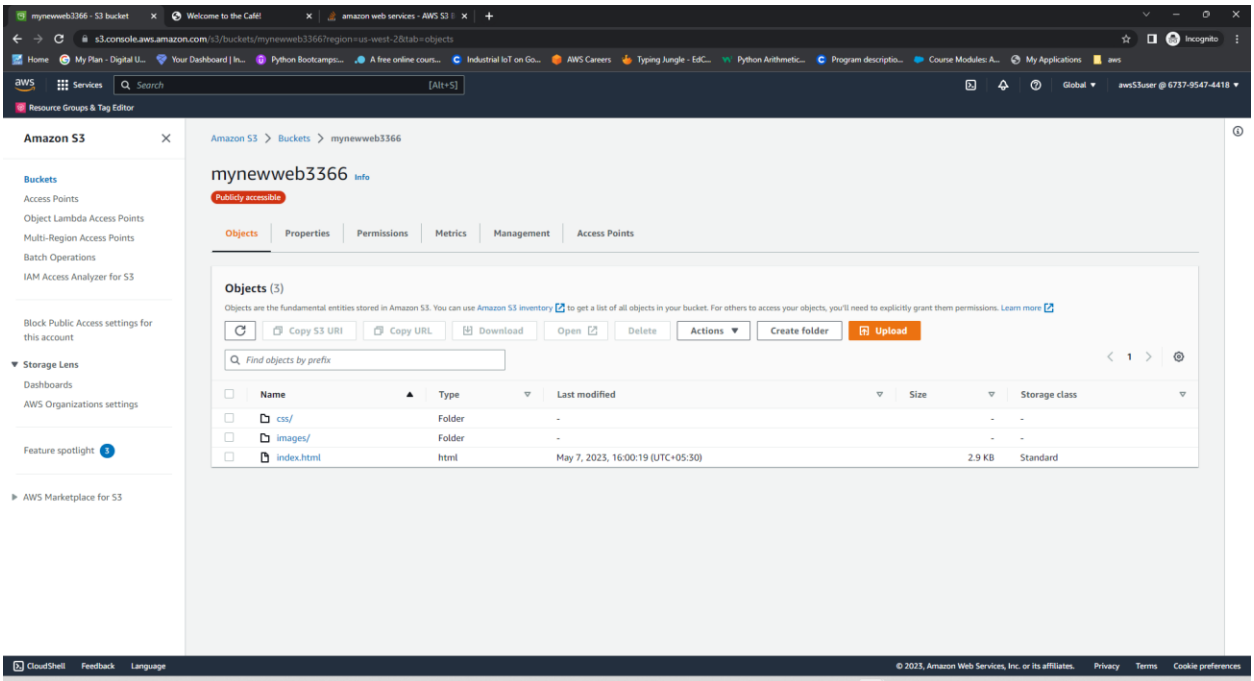
Bucket policy:

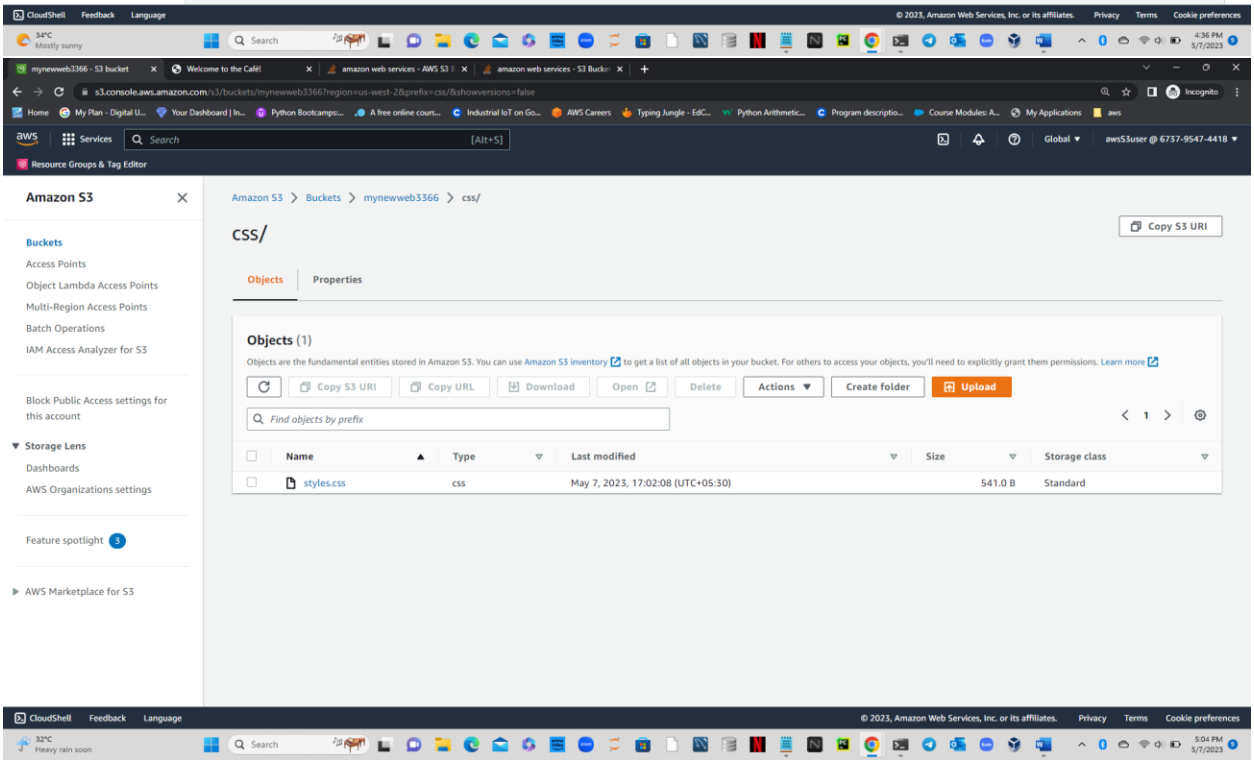
```
{
   "Version": "2012-10-17",
   "Id": "Policy1683455078164",
   "Statement": [
      {
         "Sid": "Stmt1683455076011",
         "Effect": "Allow",
         "Principal": "*",
         "Action": [
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:PutObject"
         ],
         "Resource": "arn:aws:s3:::mynewweb3366/*"
      }
   ]
}
```

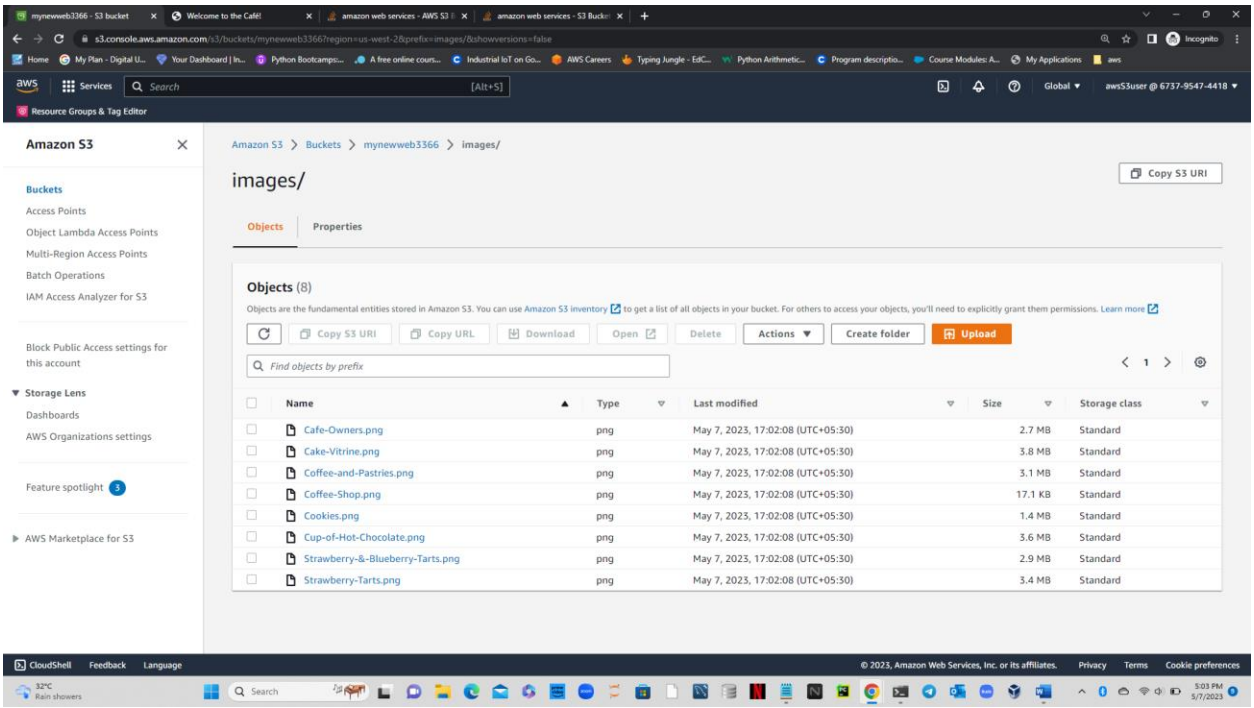

Amazon S3
Successfully edited bucket policy.
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Edit
Delete
Copy
{
"Version": "2012-10-17",
"Id": "Policy1683455078164",
"Statement": [
{
"Sid": "Stmt1683455076011",
"Effect": "Allow",
"Principal": "*",
"Action": [
"s3:DeleteObject",
"s3:GetObject",
"s3:PutObject"
],
"Resource": "arn:aws:s3:::mynewweb3366/*"
}
]
}
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.
Edit
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Amazon S3
Successfully edited bucket policy.
Amazon S3 > Buckets > mynewweb3366
mynewweb3366 Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


s3.console.aws.amazon.com/s3/buckets?region=us-west-2&region=us-west-2
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
mynewweb3366
US West (Oregon) us-west-2
Public
May 7, 2023, 15:07:25 (UTC+05:30)
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

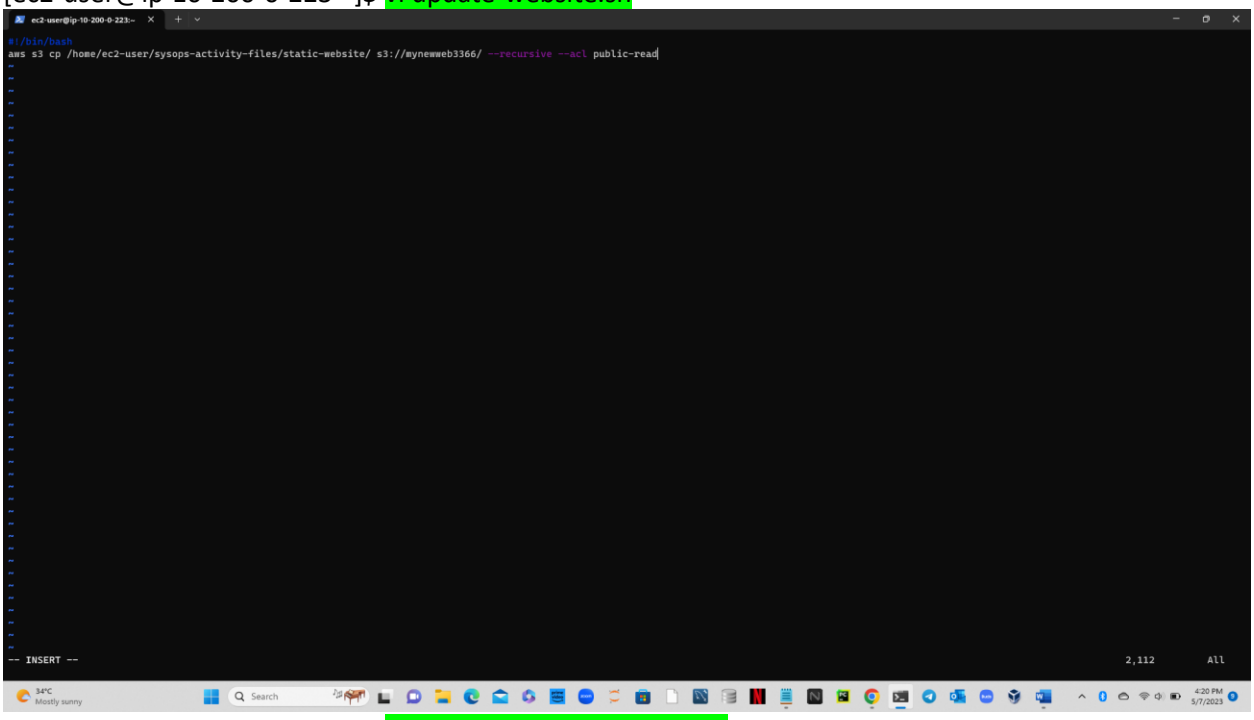

mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
s3.console.aws.amazon.com/s3/buckets/mynewweb3366?region=us-west-2&tab=objects
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > mynewweb3366
mynewweb3366 Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (3)
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
Name
Type
Last modified
Size
Storage class
css/
Folder
images/
Folder
index.html
html
May 7, 2023, 16:00:19 (UTC+05:30)
2.9 KB
Standard


mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
amazon web services - S3 Bucket
s3.console.aws.amazon.com/s3/buckets/mynewweb3366?region=us-west-2&prefix=css/&showversions=false
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > mynewweb3366 > css/
css/
Copy S3 URI
Objects
Properties
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
Name
Type
Last modified
Size
Storage class
styles.css
css
May 7, 2023, 17:02:08 (UTC+05:30)
541.0 B
Standard

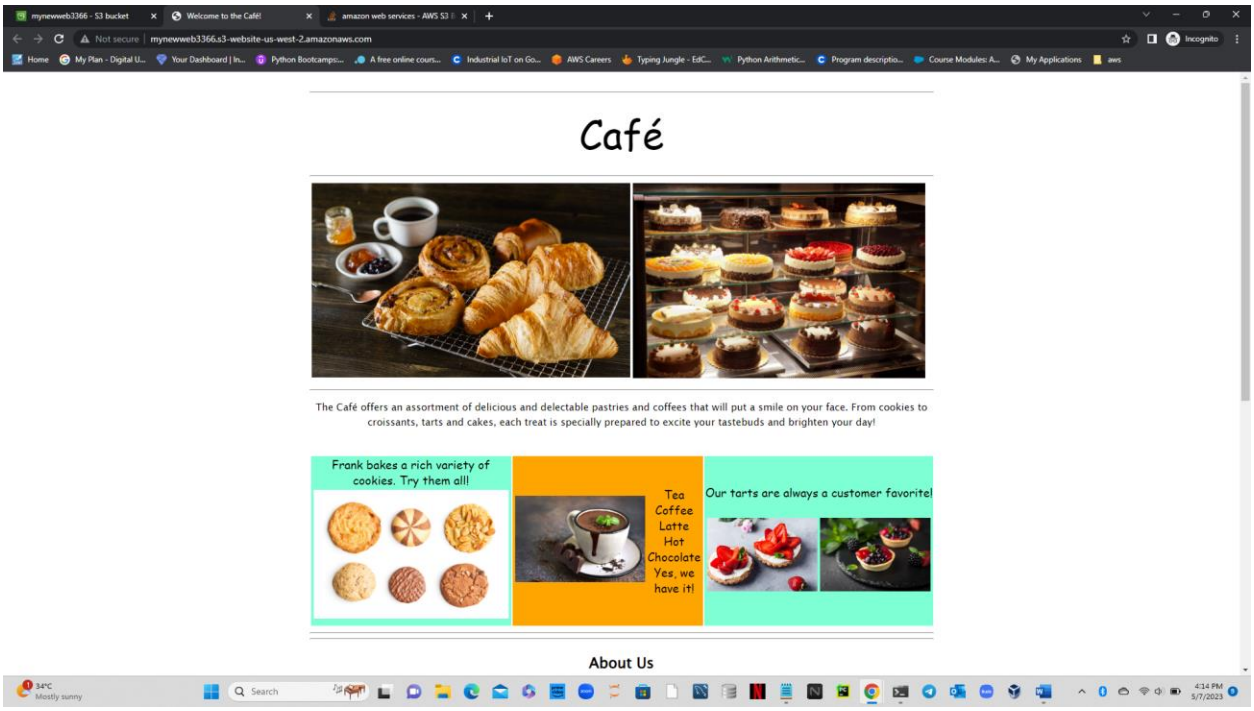

mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
amazon web services - S3 Bucket
s3.console.aws.amazon.com/s3/buckets/mynewweb3366?region=us-west-2&prefix=images/&showversions=false
Incognito
Services
Search
[Alt+S]
Global
awsS3user @ 6737-9547-4418
Resource Groups & Tag Editor
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > mynewweb3366 > images/
images/
Copy S3 URI
Objects
Properties
Objects (8)
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
1
Name
Type
Last modified
Size
Storage class
Cafe-Owners.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
2.7 MB
Standard
Cake-Vitrine.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
3.8 MB
Standard
Coffee-and-Pastries.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
3.1 MB
Standard
Coffee-Shop.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
17.1 KB
Standard
Cookies.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
1.4 MB
Standard
Cup-of-Hot-Chocolate.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
3.6 MB
Standard
Strawberry-&-Blueberry-Tarts.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
2.9 MB
Standard
Strawberry-Tarts.png
png
May 7, 2023, 17:02:08 (UTC+05:30)
3.4 MB
Standard
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Rain showers
Search
5:03 PM
5/7/2023

Task 7: Create a batch file to make updating the website repeatable

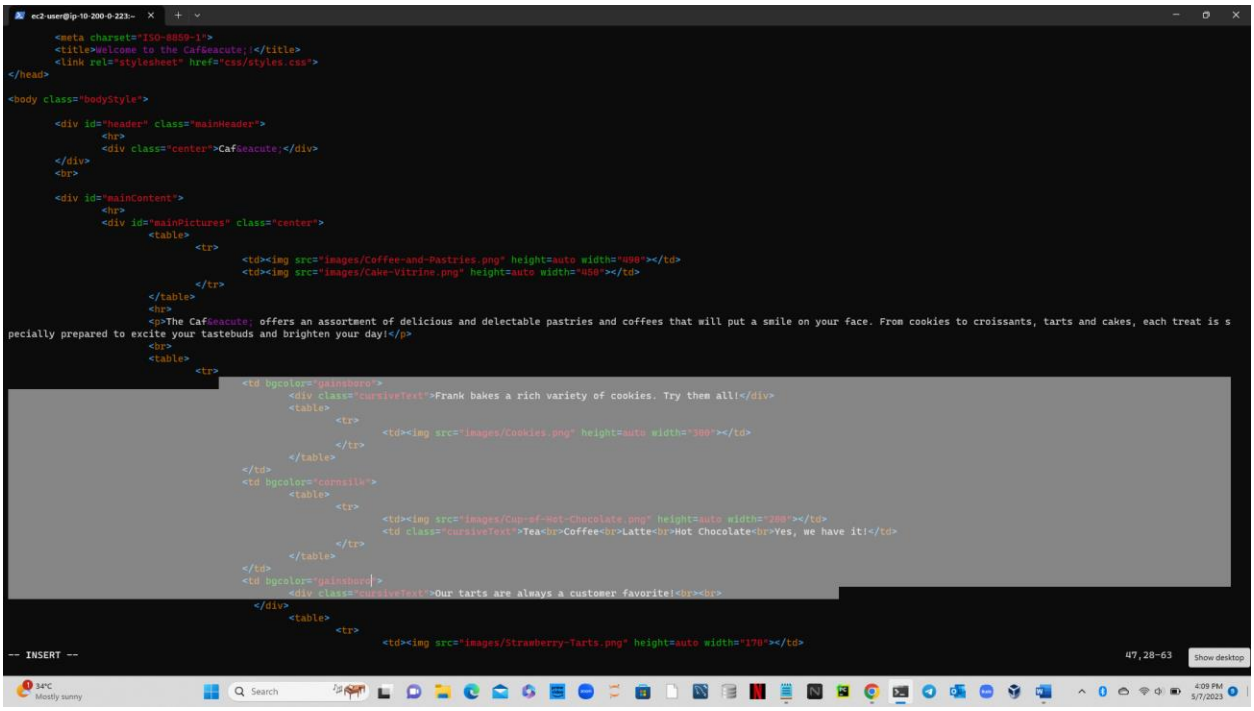
[ec2-user@ip-10-200-0-223 ~]$ touch update-website.sh
[ec2-user@ip-10-200-0-223 ~]$ vi update-website.sh



[ec2-user@ip-10-200-0-223 ~]$ chmod +x update-website.sh
[ec2-user@ip-10-200-0-223 ~]$ ll
total 4
drwxr-xr-x 3 ec2-user ec2-user 60 May 7 10:00 sysops-activity-files
-rwxrwxr-x 1 ec2-user ec2-user 124 May 7 10:36 update-website.sh



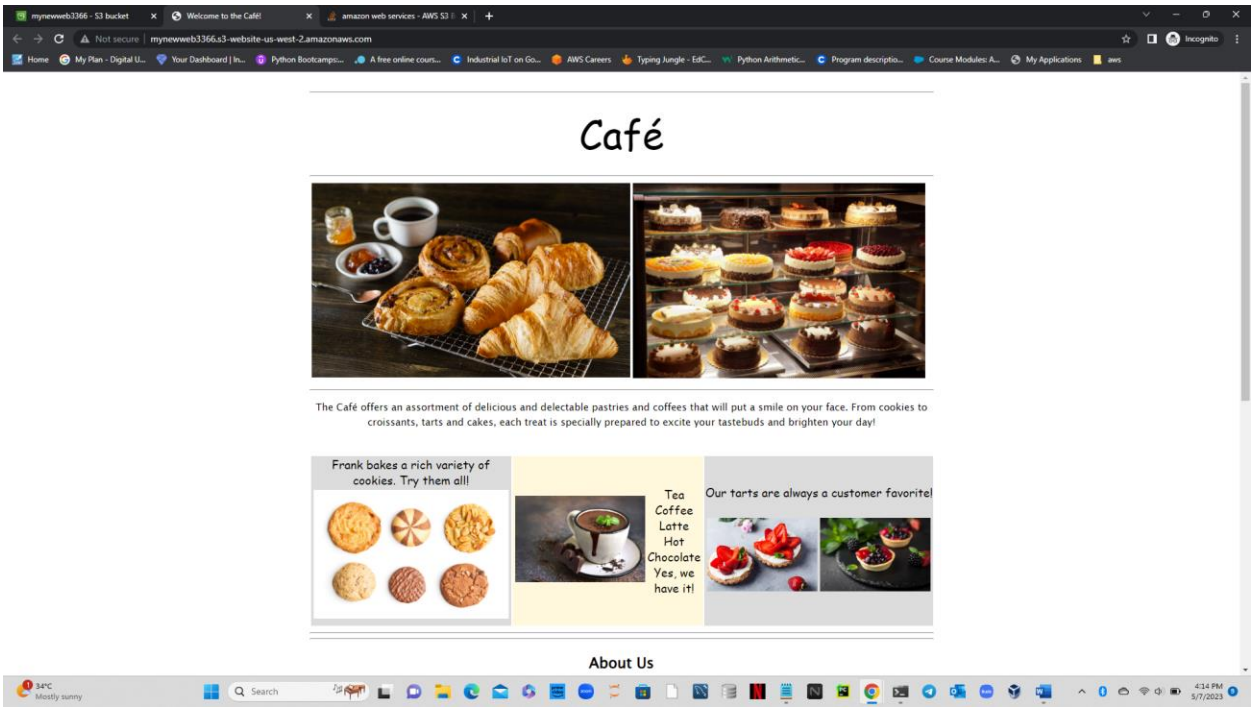

```
[ec2-user@ip-10-200-0-223 ~]$ vi sysops-activity-files/static-website/index.html
[ec2-user@ip-10-200-0-223 ~]$ ./update-website.sh
upload: sysops-activity-files/static-website/css/styles.css to s3://mynewweb3366/css/styles.css
upload: sysops-activity-files/static-website/index.html to s3://mynewweb3366/index.html
upload: sysops-activity-files/static-website/images/Coffee-Shop.png to
s3://mynewweb3366/images/Coffee-Shop.png
upload: sysops-activity-files/static-website/images/Cafe-Owners.png to
s3://mynewweb3366/images/Cafe-Owners.png
upload: sysops-activity-files/static-website/images/Cookies.png to
s3://mynewweb3366/images/Cookies.png
upload: sysops-activity-files/static-website/images/Strawberry-&-Blueberry-Tarts.png to
s3://mynewweb3366/images/Strawberry-&-Blueberry-Tarts.png
upload: sysops-activity-files/static-website/images/Cake-Vitrine.png to
s3://mynewweb3366/images/Cake-Vitrine.png
upload: sysops-activity-files/static-website/images/Cup-of-Hot-Chocolate.png to
s3://mynewweb3366/images/Cup-of-Hot-Chocolate.png
upload: sysops-activity-files/static-website/images/Coffee-and-Pastries.png to
s3://mynewweb3366/images/Coffee-and-Pastries.png
upload: sysops-activity-files/static-website/images/Strawberry-Tarts.png to
s3://mynewweb3366/images/Strawberry-Tarts.png
```



index.html :

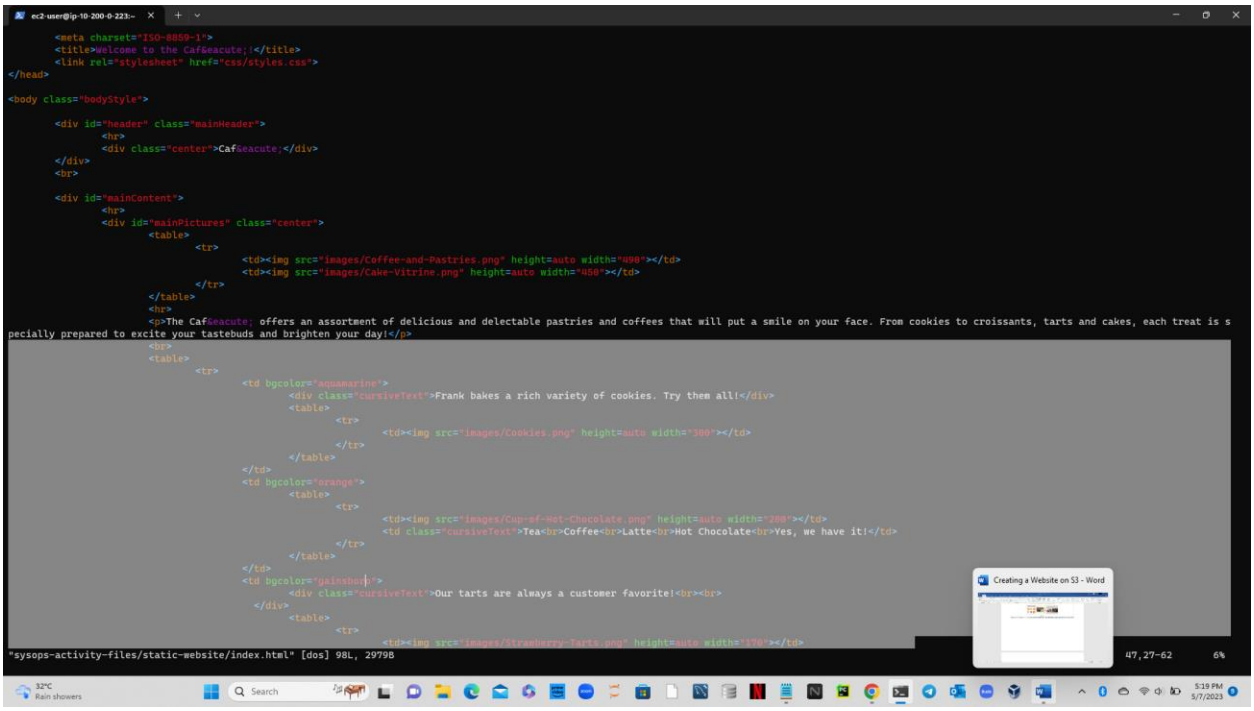
```
   <meta charset="ISO-8859-1">
      <title>Welcome to the Caf&eacute;!</title>
      <link rel="stylesheet" href="css/styles.css">
</head>

<body class="bodyStyle">

      <div id="header" class="mainHeader">
            <hr>
            <div class="center">Caf&eacute;</div>
      </div>
      <br>

      <div id="mainContent">
            <hr>
            <div id="mainPictures" class="center">
                  <table>
                        <tr>
                              <td><img src="images/Coffee-and-Pastries.png" height=auto width="490"></td>
                              <td><img src="images/Cake-Vitrine.png" height=auto width="450"></td>
                        </tr>
```

```
            </table>
            <hr>
            <p>The Caf&eacute; offers an assortment of delicious and delectable pastries and coffees
that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially
prepared to excite your tastebuds and brighten your day!</p>
            <br>
            <table>
                <tr>
                    <td bgcolor="gainsboro">
                        <div class="cursiveText">Frank bakes a rich variety of cookies. Try them
all!</div>
                        <table>
                            <tr>
                                <td><img src="images/Cookies.png" height=auto width="300"></td>
                            </tr>
                        </table>
                    </td>
                    <td bgcolor="cornsilk">
                        <table>
                            <tr>
                                <td><img src="images/Cup-of-Hot-Chocolate.png" height=auto
width="200"></td>
                                <td class="cursiveText">Tea<br>Coffee<br>Latte<br>Hot
Chocolate<br>Yes, we have it!</td>
                            </tr>
                        </table>
                    </td>
                    <td bgcolor="gainsboro">
                        <div class="cursiveText">Our tarts are always a customer favorite!<br><br>
                     </div>
                        <table>
                            <tr>
                                <td><img src="images/Strawberry-Tarts.png" height=auto
width="170"></td>
-- INSERT --
47,28-63      6%
```


mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
Not secure
mynewweb3366.s3-website-us-west-2.amazonaws.com
Incognito
Café
The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!
Frank bakes a rich variety of cookies. Try them all!
Tea
Coffee
Latte
Hot Chocolate
Yes, we have it!
Our tarts are always a customer favorite!
About Us
Search
4:14 PM
5/7/2023

Optional challenge

```
[ec2-user@ip-10-200-0-223 ~]$ vi sysops-activity-files/static-website/index.html
[ec2-user@ip-10-200-0-223 ~]$  ./update-website.sh
upload: sysops-activity-files/static-website/css/styles.css to s3://mynewweb3366/css/styles.css
upload: sysops-activity-files/static-website/images/Coffee-Shop.png to
s3://mynewweb3366/images/Coffee-Shop.png
upload: sysops-activity-files/static-website/index.html to s3://mynewweb3366/index.html
upload: sysops-activity-files/static-website/images/Coffee-and-Pastries.png to
s3://mynewweb3366/images/Coffee-and-Pastries.png
upload: sysops-activity-files/static-website/images/Cafe-Owners.png to
s3://mynewweb3366/images/Cafe-Owners.png
upload: sysops-activity-files/static-website/images/Cookies.png to
s3://mynewweb3366/images/Cookies.png
upload: sysops-activity-files/static-website/images/Cake-Vitrine.png to
s3://mynewweb3366/images/Cake-Vitrine.png
upload: sysops-activity-files/static-website/images/Strawberry-&-Blueberry-Tarts.png to
s3://mynewweb3366/images/Strawberry-&-Blueberry-Tarts.png
upload: sysops-activity-files/static-website/images/Cup-of-Hot-Chocolate.png to
s3://mynewweb3366/images/Cup-of-Hot-Chocolate.png
upload: sysops-activity-files/static-website/images/Strawberry-Tarts.png to
s3://mynewweb3366/images/Strawberry-Tarts.png
```


ec2-user@ip-10-200-0-223:~
<meta charset="ISO-8859-1">
<title>Welcome to the Café!</title>
<link rel="stylesheet" href="css/styles.css">
</head>
<body class="bodyStyle">

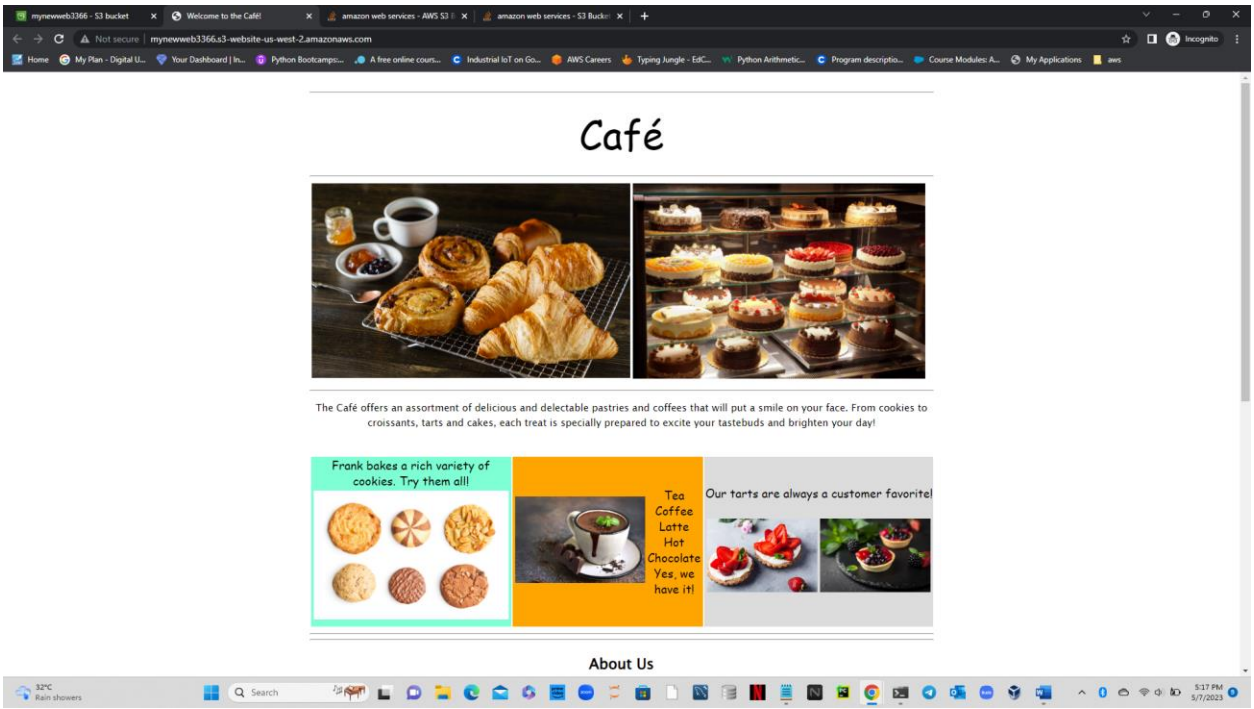
<hr>
Café

<hr>

<table>
<tr>
<td><img src="images/Coffee-and-Pastries.png" height=auto width="400"></td>
<td><img src="images/Cake-Vitrine.png" height=auto width="450"></td>
</tr>
</table>
<hr>
The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!

<table>
<tr>
<td bgcolor="aquamarine">
Frank bakes a rich variety of cookies. Try them all!
<table>
<tr>
<td><img src="images/Cookies.png" height=auto width="300"></td>
</tr>
</table>
</td>
<td bgcolor="orange">
<table>
<tr>
<td><img src="images/Cup-of-Hot-Chocolate.png" height=auto width="200"></td>
<td class="cursiveText">Tea
Coffee
Latte
Hot Chocolate
Yes, we have it!</td>
</tr>
</table>
</td>
<td bgcolor="gainsboro">
Our tarts are always a customer favorite!

<table>
<tr>
<td><img src="images/Strawberry-Tarts.png" height=auto width="170"></td>
Creating a Website on S3 - Word
"sysops-activity-files/static-website/index.html" [dos] 98L, 2979B
47,27-62
6%
32°C
Rain showers
Search
5:19 PM
5/7/2023


mynewweb3366 - S3 bucket
Welcome to the Café!
amazon web services - AWS S3
amazon web services - S3 Bucket
Not secure
mynewweb3366.s3-website-us-west-2.amazonaws.com
Incognito
Café
The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!
Frank bakes a rich variety of cookies. Try them all!
Tea
Coffee
Latte
Hot Chocolate
Yes, we have it!
Our tarts are always a customer favorite!
About Us
32°C
Rain showers
Search
5:17 PM
5/7/2023