Contents

Lab 1: Simple Storage Service (S3)

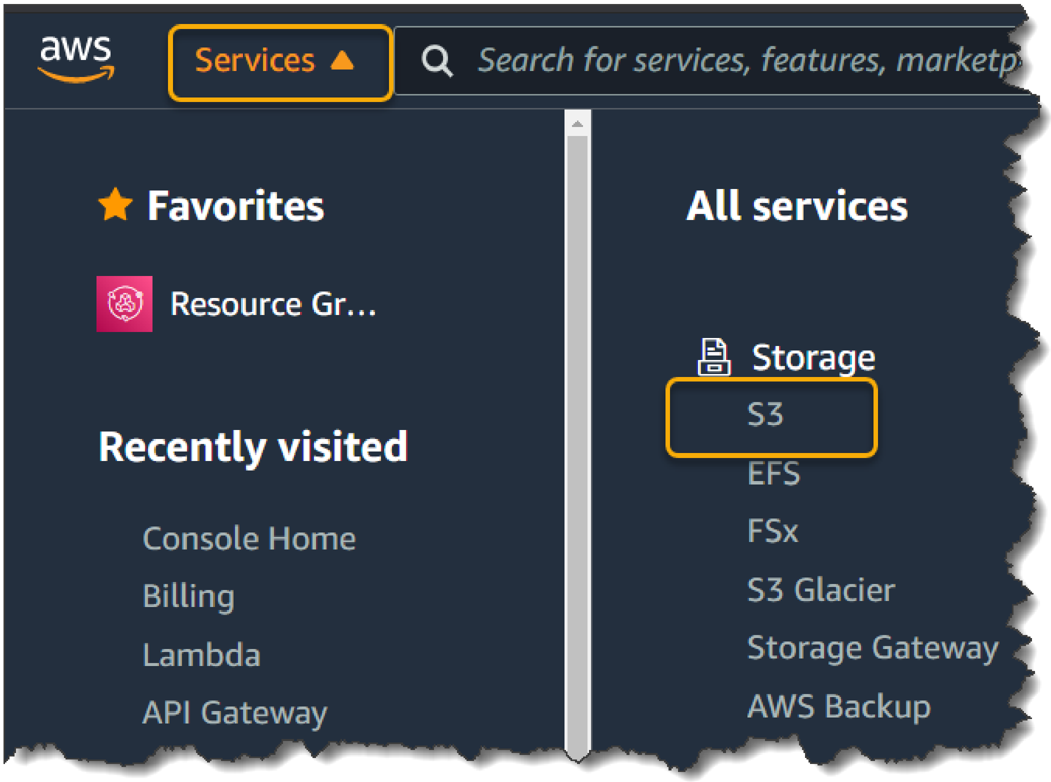
In this lab we are first going to create a bucket, upload content into it, manage its security control and finally access it from a browser.

Task Breakdown

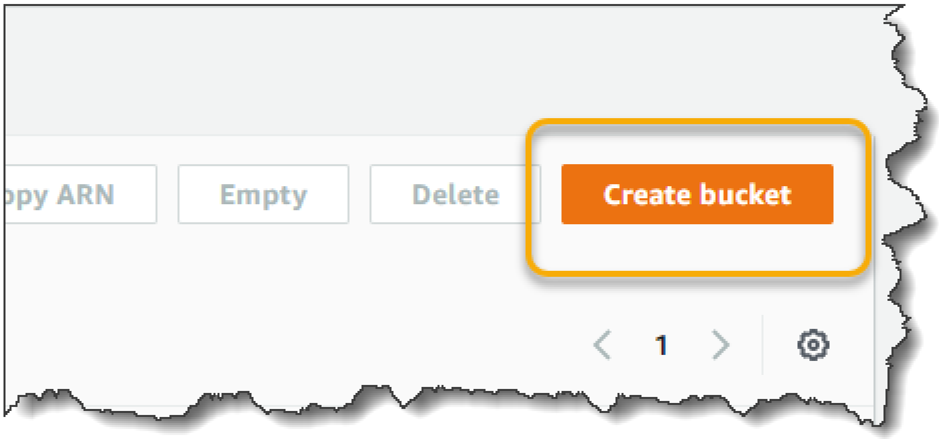
- Create a bucket
- Modify ACL and grant access to the object
- Create and Apply Bucket Policy to deny access to the object
- Download Security Credentials
- Setup AWS CLI
- Manage S3 through CLI

Task 1: Create a bucket

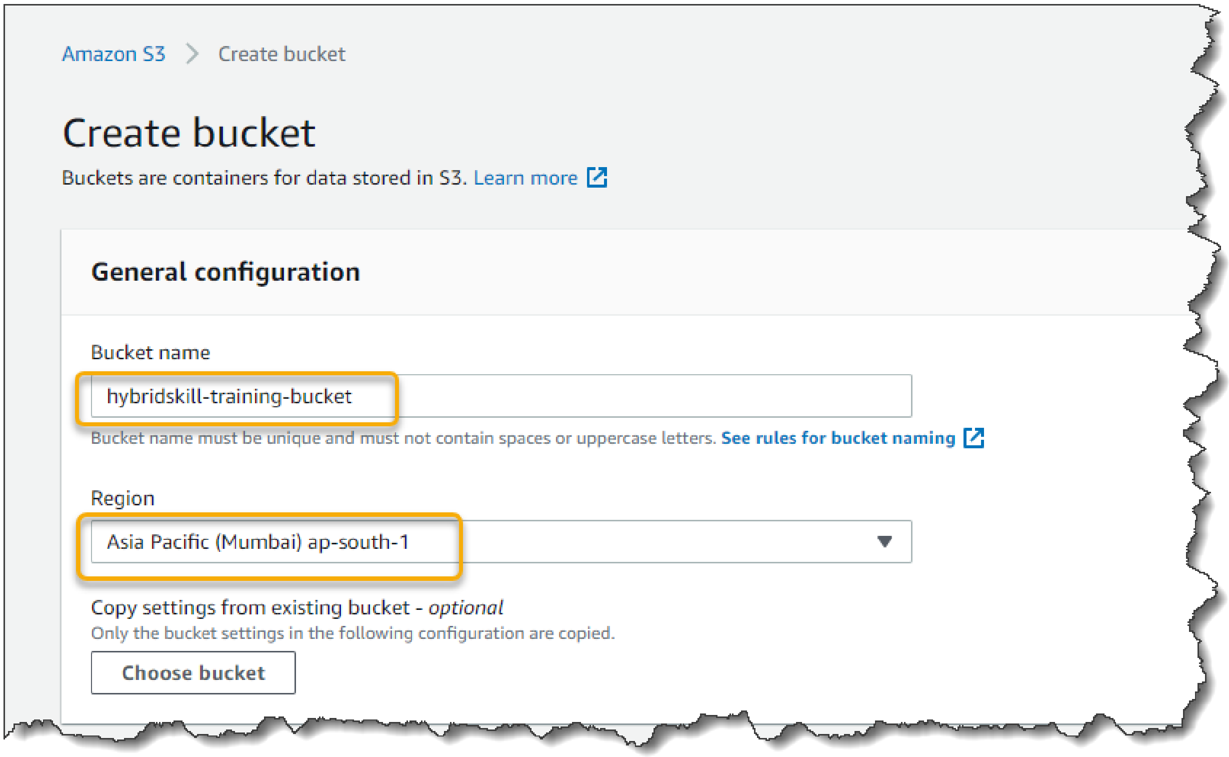
1. Go to console.aws.amazon.com and click on **Services** and under **Storage** click on **S3** as shown below



2. Click on **Create bucket.**



3. In the new window that pops up do the following
   a. Enter a unique bucket name
   b. Select a region from the drop down for your bucket. We have selected **Mumbai** as an example



Buckets are containers for data stored in S3.

General configuration

Bucket name: hybridskill-training-bucket

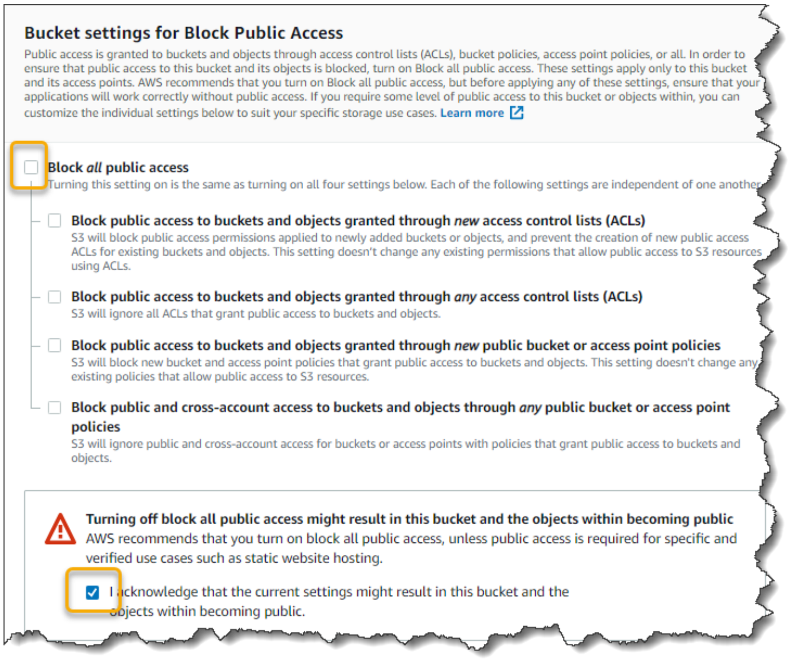
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

Region: Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

4. Scroll down to the **Bucket settings for Block Public Access** section. Uncheck the **Block all public access** checkbox and check the **acknowledge settings** checkbox at the bottom.



Bucket settings for Block Public Access

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

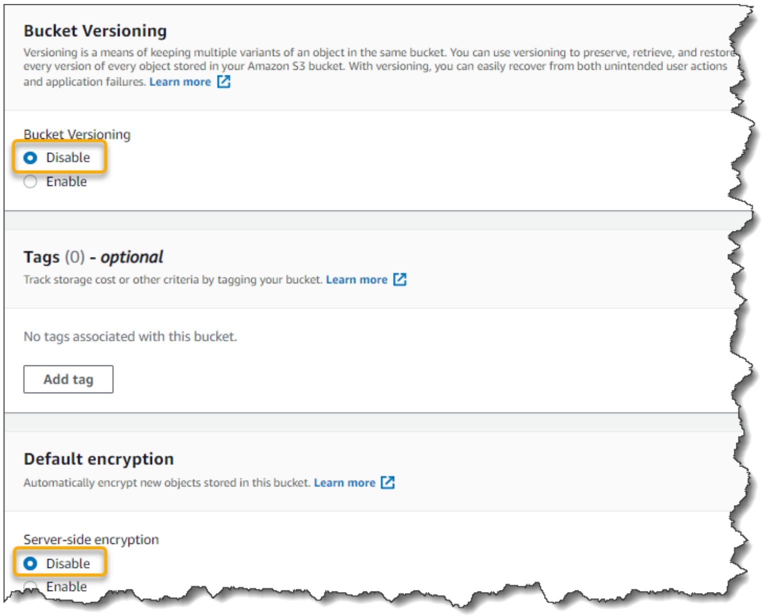
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.

Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

5. Leave all other settings as default



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
● Disable
○ Enable

Tags (0) - ***optional***

Track storage cost or other criteria by tagging your bucket. Learn more

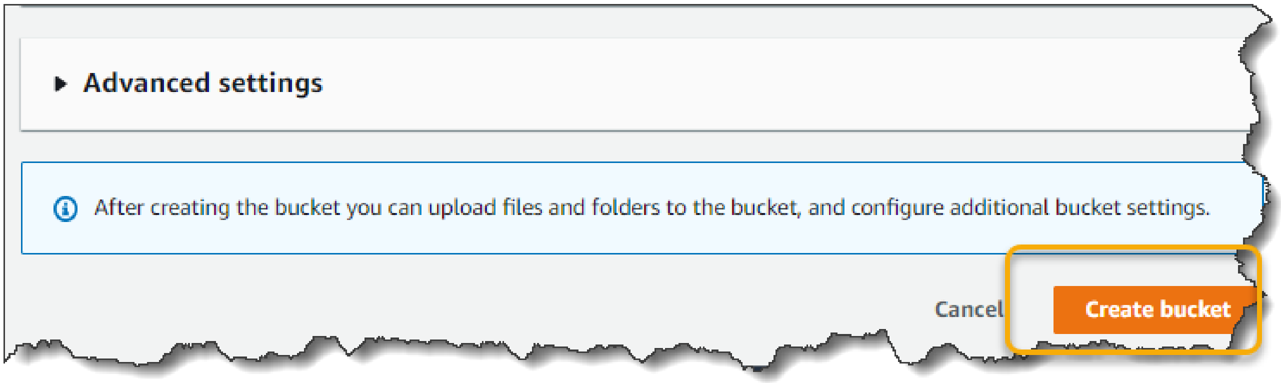
No tags associated with this bucket.

Default encryption

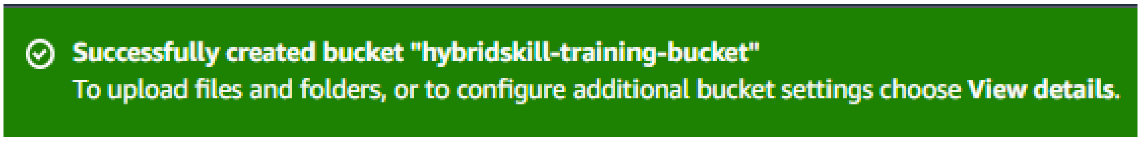
Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption
● Disable
○ Enable

6. Click **Create bucket**.

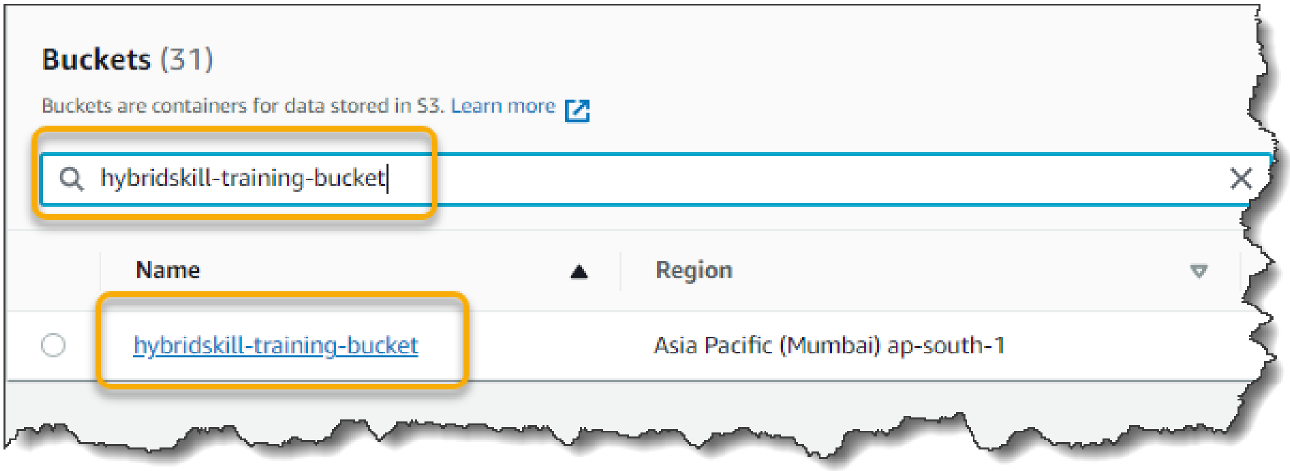


ⓘ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.



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

7. Find and click on your newly created bucket.



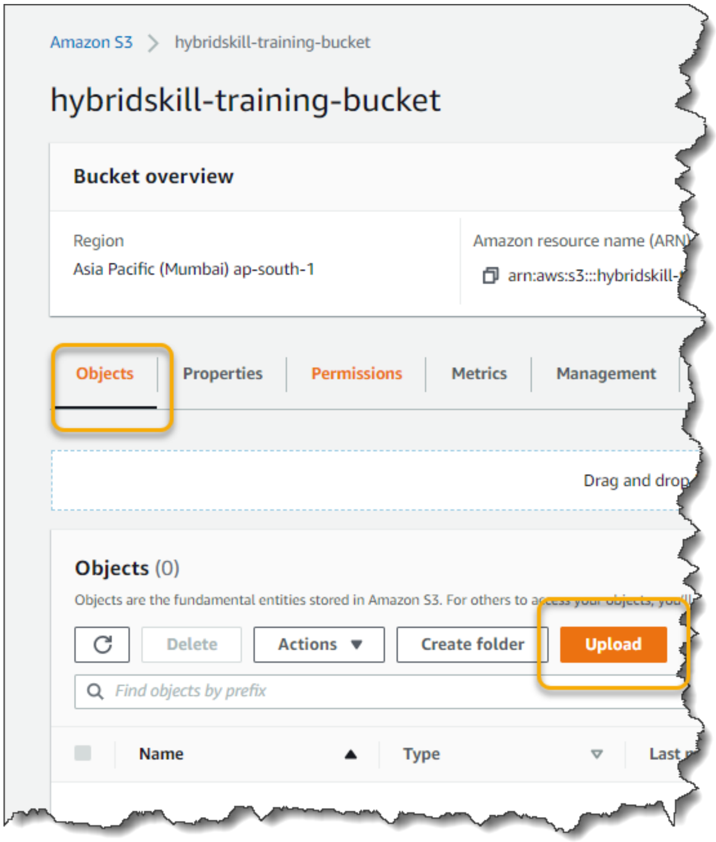
Buckets (31)

Buckets are containers for data stored in S3. Learn more

hybridskill-training-bucket

	Name ▲	Region
○	hybridskill-training-bucket	Asia Pacific (Mumbai) ap-south-1

8. Under the objects tab at the bottom of the screen click on the **Upload** button



Amazon S3 > hybridskill-training-bucket

hybridskill-training-bucket

Bucket overview

Region
Asia Pacific (Mumbai) ap-south-1

Amazon resource name (ARN)
arn:aws:s3:::hybridskill-

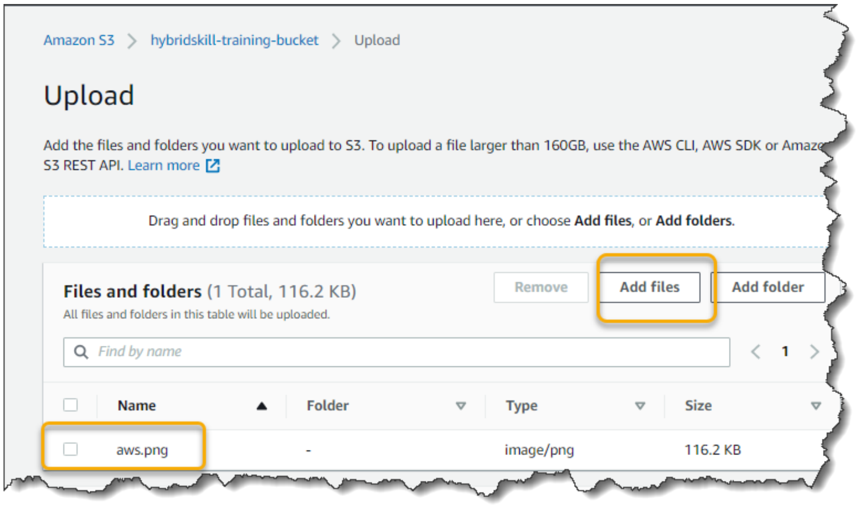
Drag and drop

Objects (0)

Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll

Find objects by prefix

9. In the new window, click on **Add Files,** Select a picture from your system.



Amazon S3 > hybridskill-training-bucket > Upload

Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amaz
S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

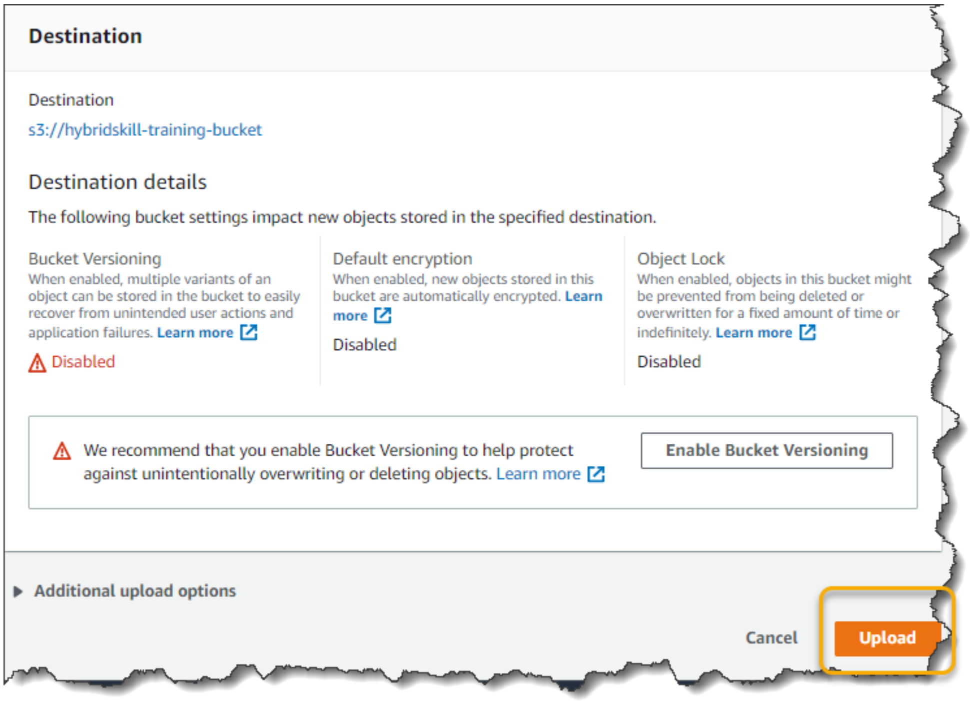
Files and folders (1 Total, 116.2 KB)

All files and folders in this table will be uploaded.

Find by name

□	Name ▲	Folder ▽	Type ▽	Size ▽
□	aws.png	-	image/png	116.2 KB

10. Leave all options as default and click on **Upload.**



Destination

Destination
s3://hybridskill-training-bucket

Destination details

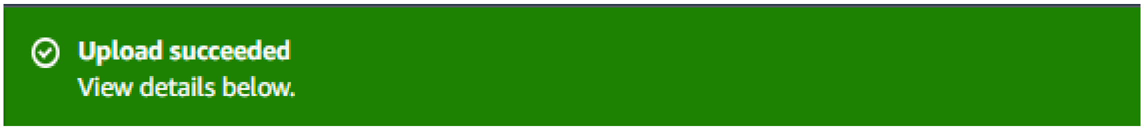
The following bucket settings impact new objects stored in the specified destination.

Bucket Versioning
When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. Learn more
⚠ Disabled

Default encryption
When enabled, new objects stored in this bucket are automatically encrypted. Learn more
Disabled

Object Lock
When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more
Disabled

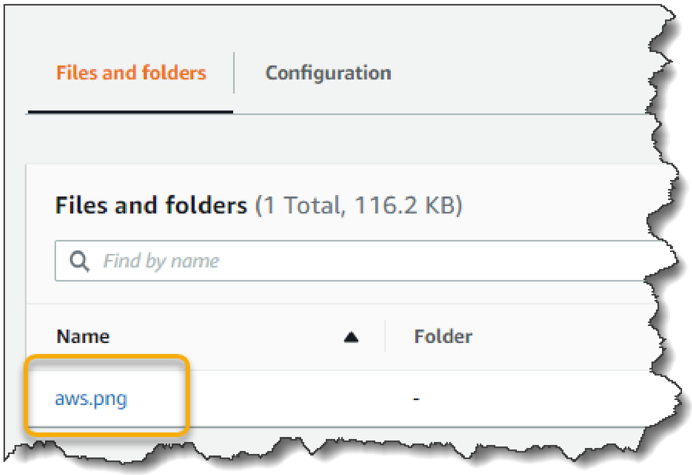
⚠ We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. Learn more



Upload succeeded
View details below.

Task 2: Modify ACL and grant access to the object

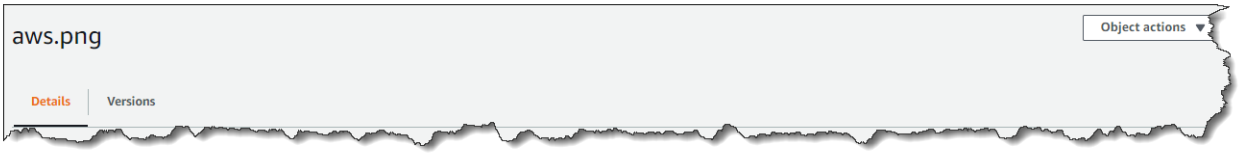
1. Click on your uploaded image



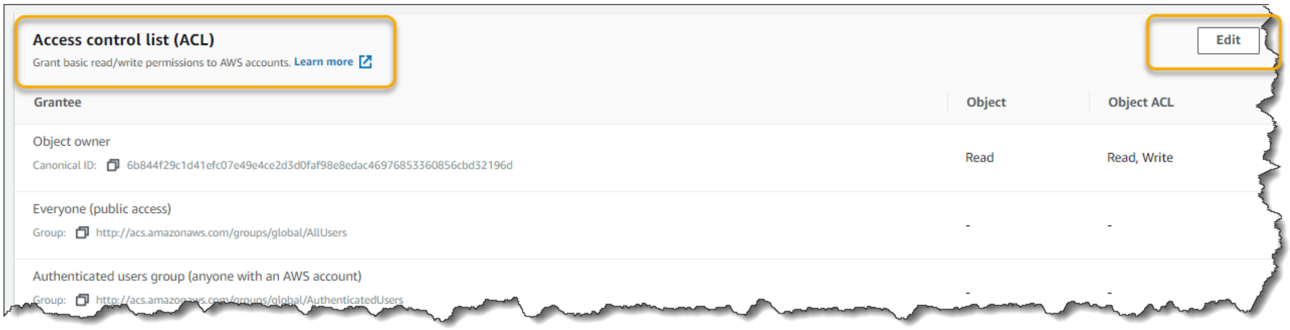
Files and folders (1 Total, 116.2 KB)

Name ▲	Folder
aws.png	-

2. On new window, scroll down to the **Access control list(ACL)** section and click on **Edit**



aws.png

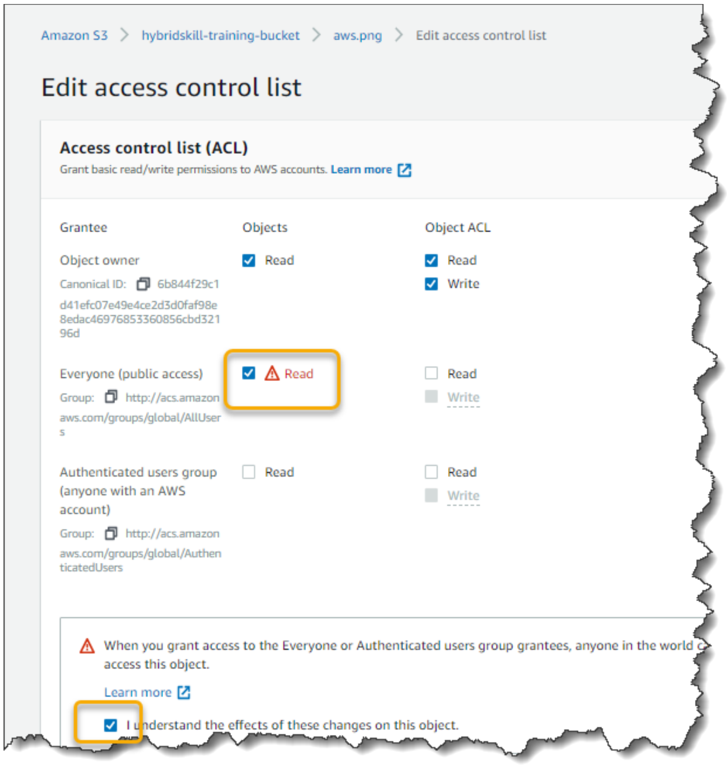


Access control list (ACL)

Grant basic read/write permissions to AWS accounts. Learn more

Grantee	Object	Object ACL
Object owner Canonical ID: 6b844f29c1d41efc07e49e4ce2d3d0faf98e8edac46976853360856cbd32196d	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

3. In Access control list section, Check the **Read** checkbox near **Everyone(public access)**. To give public access to the object. Acknowledge the **effect of the changes** checkbox.



Amazon S3 > hybridskill-training-bucket > aws.png > Edit access control list

Edit access control list

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. Learn more

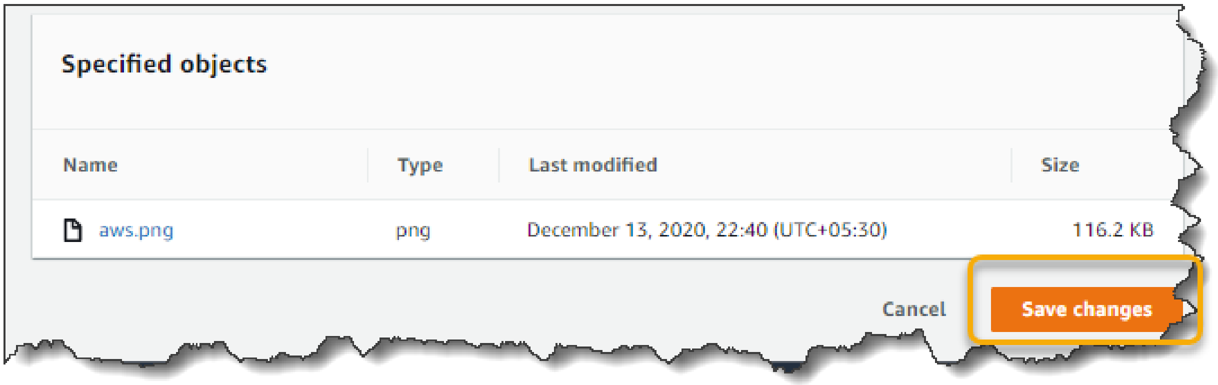
Grantee	Objects	Object ACL
Object owner Canonical ID: 6b844f29c1d41efc07e49e4ce2d3d0faf98e8edac46976853360856cbd32196d	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	□ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ Read	□ Read □ Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world c access this object.

Learn more

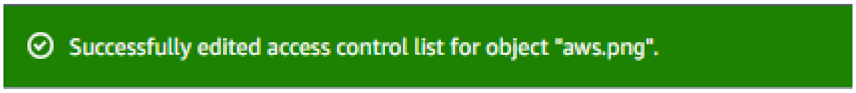
☑ I understand the effects of these changes on this object.

4. Finally click **Save changes**.



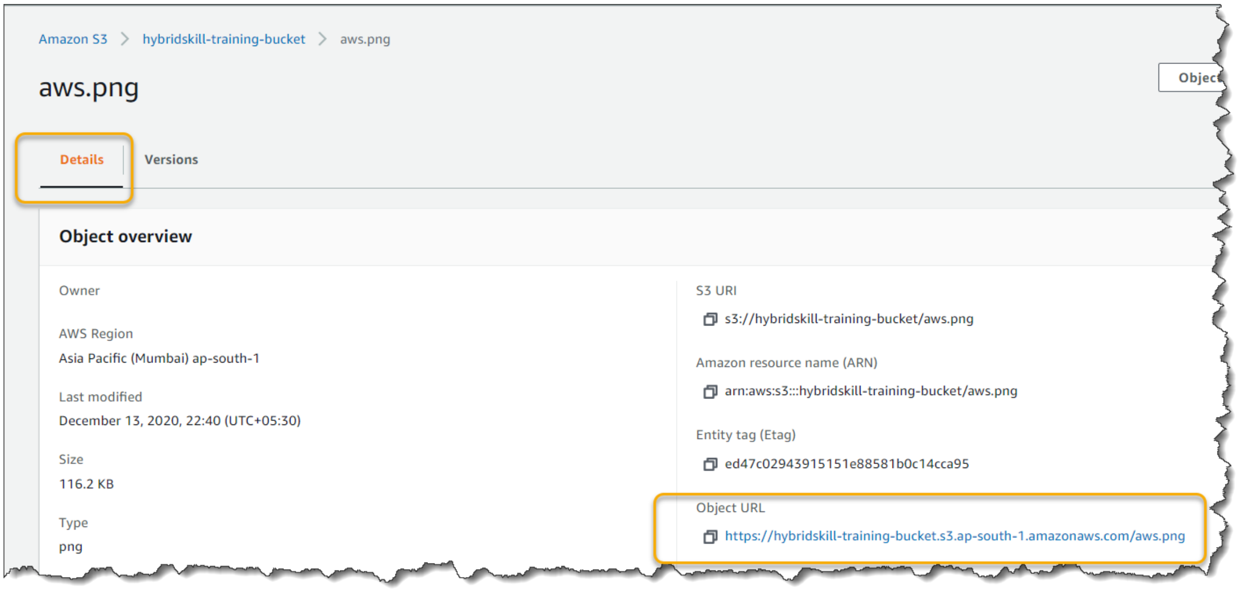
Specified objects

Name	Type	Last modified	Size
aws.png	png	December 13, 2020, 22:40 (UTC+05:30)	116.2 KB



Successfully edited access control list for object "aws.png".

5. Select the **Details** tab and find and visit the **Object URL.**



Amazon S3 > hybridskill-training-bucket > aws.png

aws.png

Object overview

Owner

AWS Region
Asia Pacific (Mumbai) ap-south-1

Last modified
December 13, 2020, 22:40 (UTC+05:30)

Size
116.2 KB

Type
png

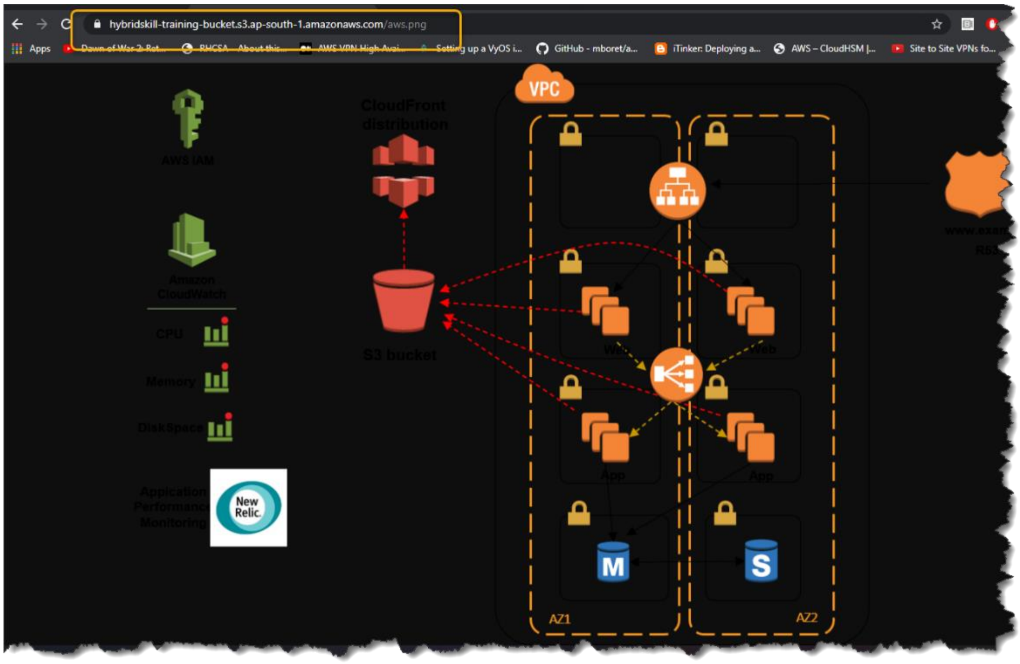
S3 URI
s3://hybridskill-training-bucket/aws.png

Amazon resource name (ARN)
arn:aws:s3:::hybridskill-training-bucket/aws.png

Entity tag (Etag)
ed47c02943915151e88581b0c14cca95

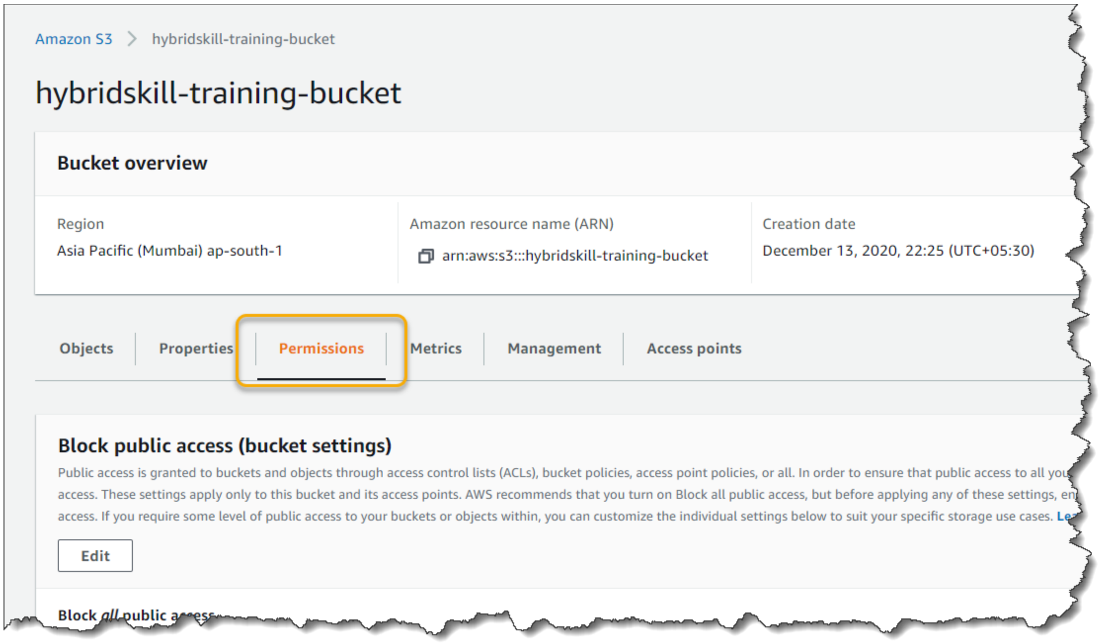
Object URL
https://hybridskill-training-bucket.s3.ap-south-1.amazonaws.com/aws.png

6. Your image should be displayed on the browser



Task 3: Create and Apply Bucket Policy to deny access to the object

1. Go back to your bucket overview screen or find and click on your **Bucket Name** at the top of your screen. Click on the **Permissions** Tab.


Amazon S3 > hybridskill-training-bucket

hybridskill-training-bucket

Bucket overview

Region: Asia Pacific (Mumbai) ap-south-1

Amazon resource name (ARN): arn:aws:s3:::hybridskill-training-bucket

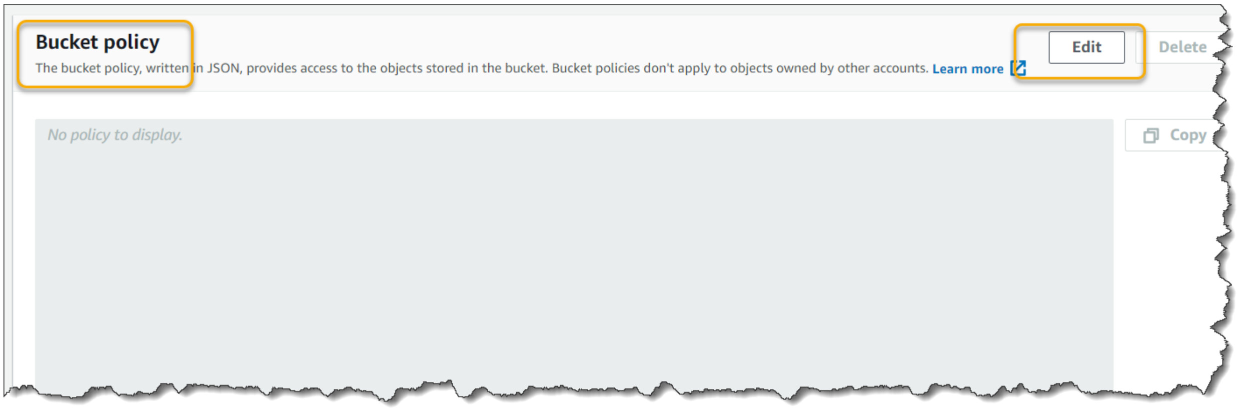
Creation date: December 13, 2020, 22:25 (UTC+05:30)

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 you 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, en 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. Le

Block *all* public access

2. Scroll down to the **Bucket Policy section** and click on **Edit.**

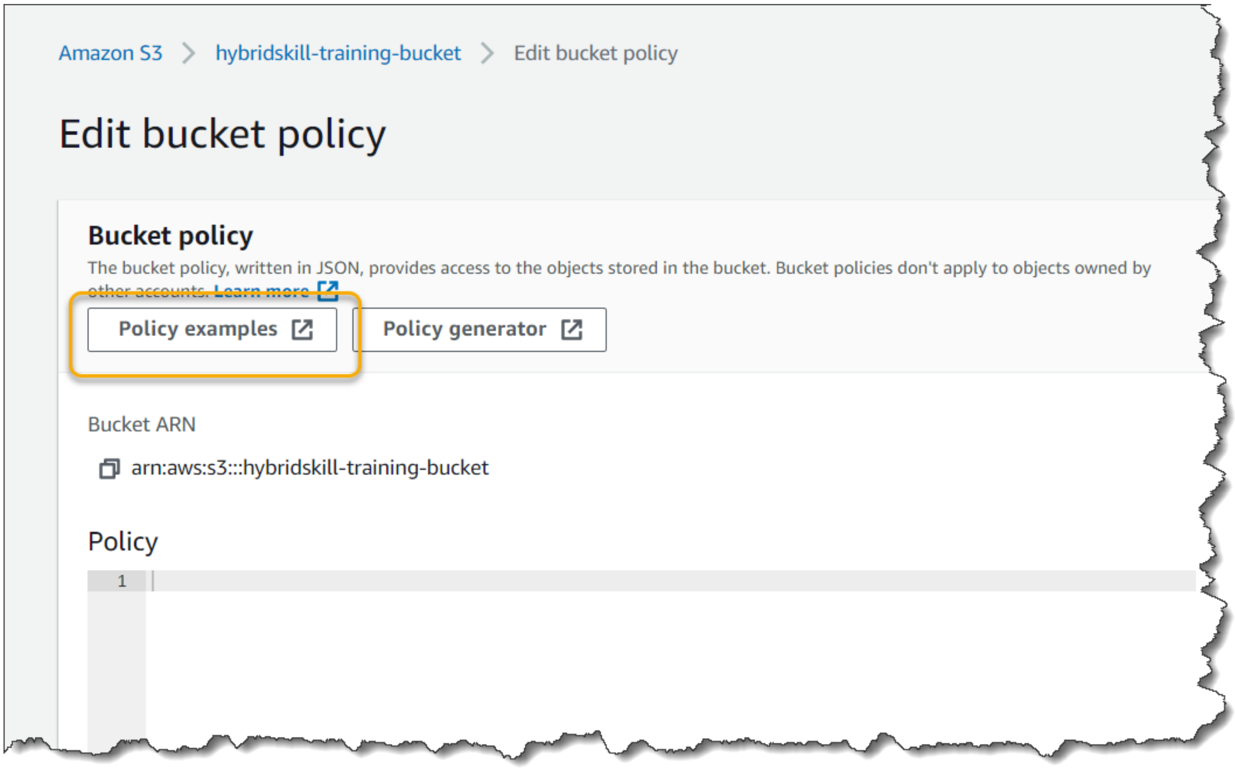


Bucket policy

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

No policy to display.

3. Click on **Policy examples.**



Amazon S3 > hybridskill-training-bucket > Edit bucket policy

Edit bucket policy

Bucket policy

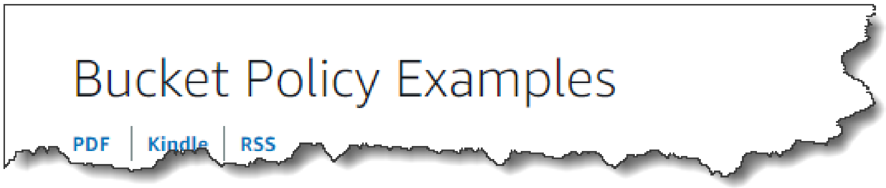
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

arn:aws:s3:::hybridskill-training-bucket

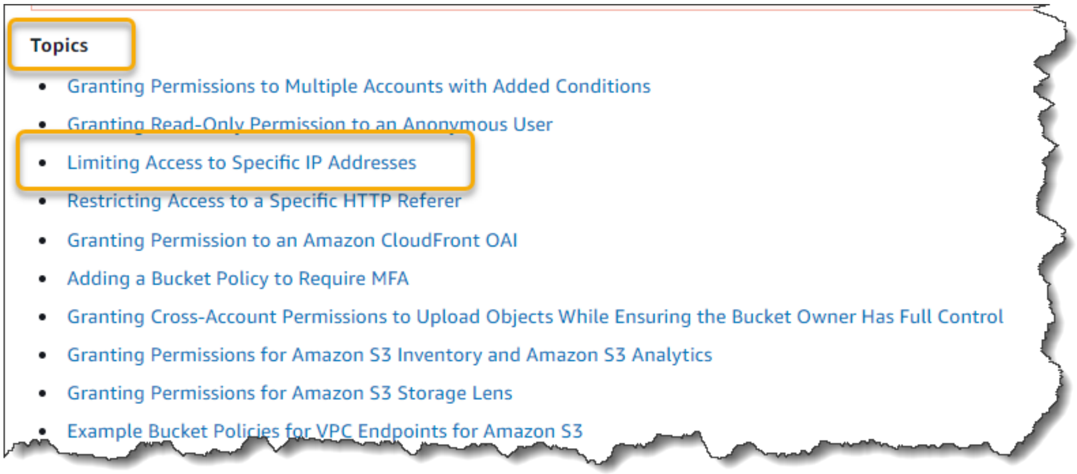
Policy

4. On the Bucket Policy examples page scroll down and under **Topics** Click on **Restricting Access to Specific IP Addresses** link



Bucket Policy Examples

PDF | Kindle | RSS

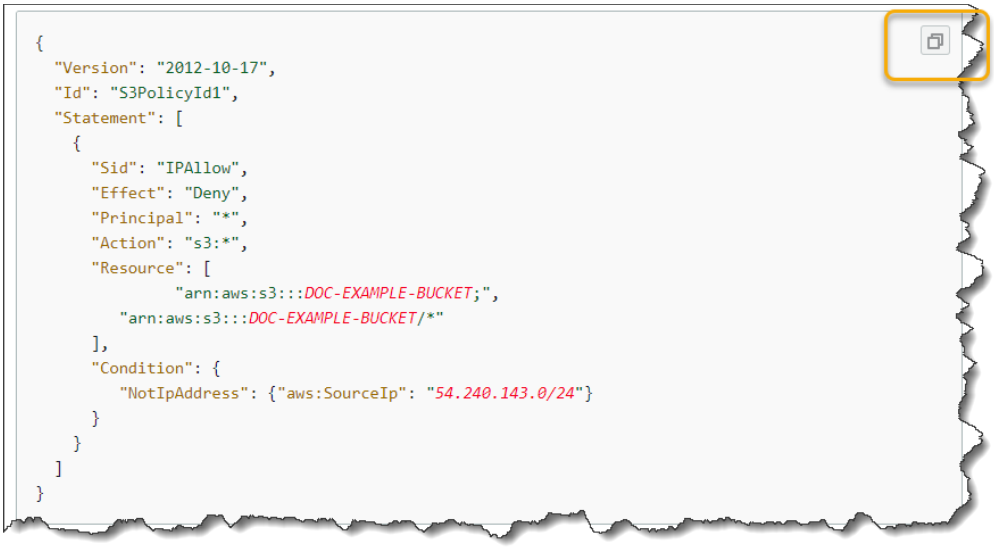


Topics

- Granting Permissions to Multiple Accounts with Added Conditions
- Granting Read-Only Permission to an Anonymous User
- Limiting Access to Specific IP Addresses
- Restricting Access to a Specific HTTP Referer
- Granting Permission to an Amazon CloudFront OAI
- Adding a Bucket Policy to Require MFA
- Granting Cross-Account Permissions to Upload Objects While Ensuring the Bucket Owner Has Full Control
- Granting Permissions for Amazon S3 Inventory and Amazon S3 Analytics
- Granting Permissions for Amazon S3 Storage Lens
- Example Bucket Policies for VPC Endpoints for Amazon S3

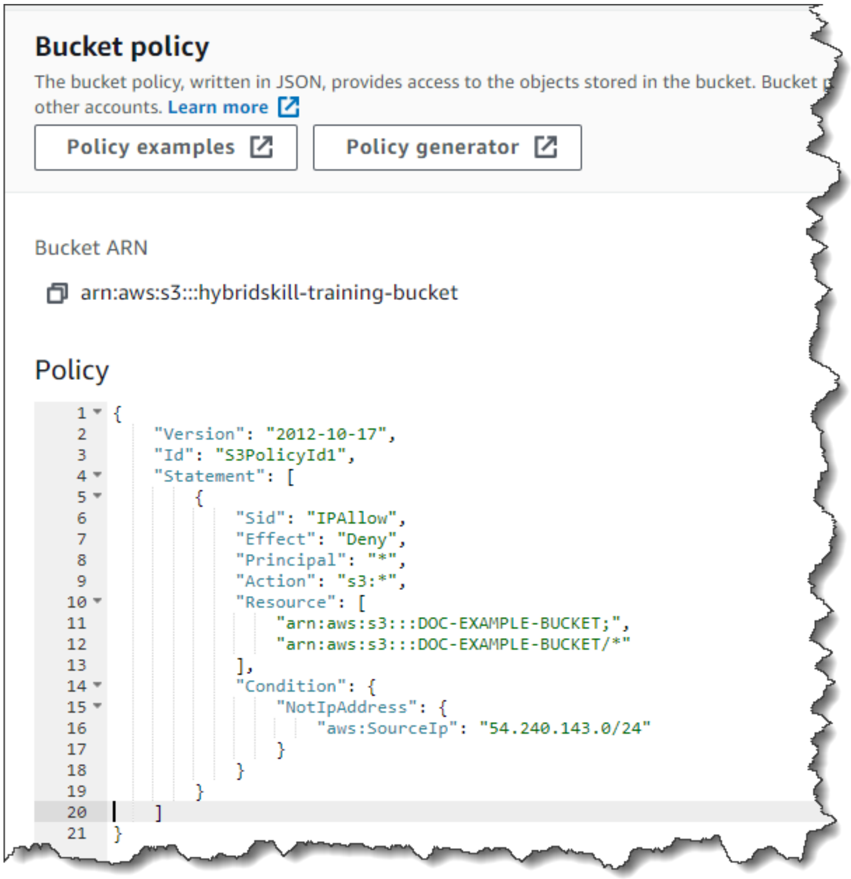
5. Click the **Copy Button** at the top right of the code Snippet

Limiting Access to Specific IP Addresses



```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
               "arn:aws:s3:::DOC-EXAMPLE-BUCKET;",
         "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Condition": {
         "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}
      }
    }
  ]
}
```

6. Paste the code into the **Bucket policy editor**



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket p
other accounts. Learn more

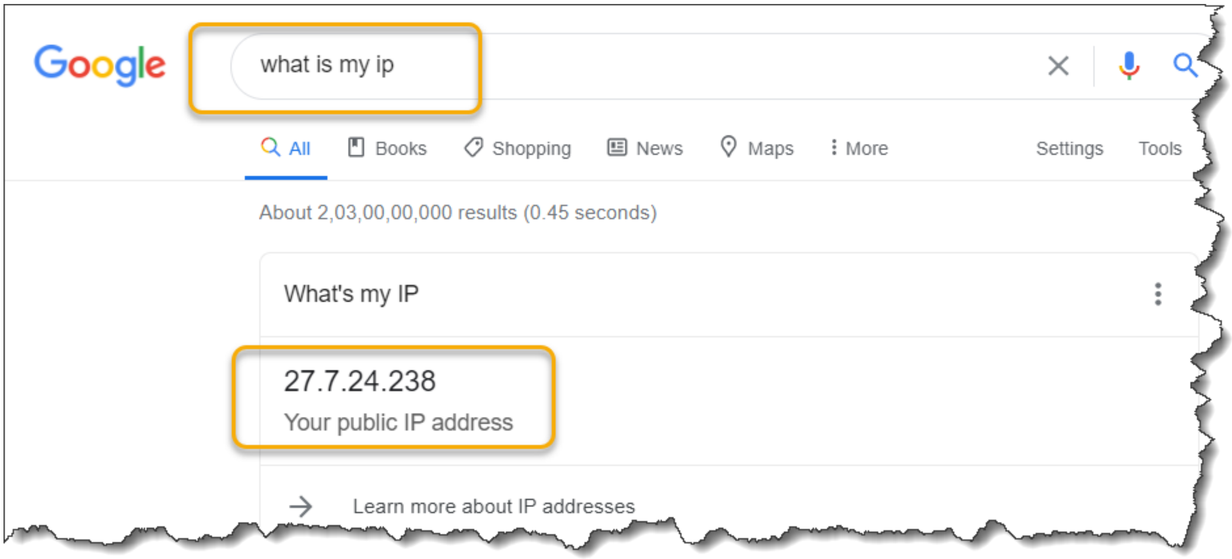
Bucket ARN

arn:aws:s3:::hybridskill-training-bucket

Policy

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET;",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

7. Open up a browser, go to google and type in **what is my IP address**. This query will display the current IP address of the system. Copy this address. We will use it next.



what is my ip

About 2,03,00,00,000 results (0.45 seconds)

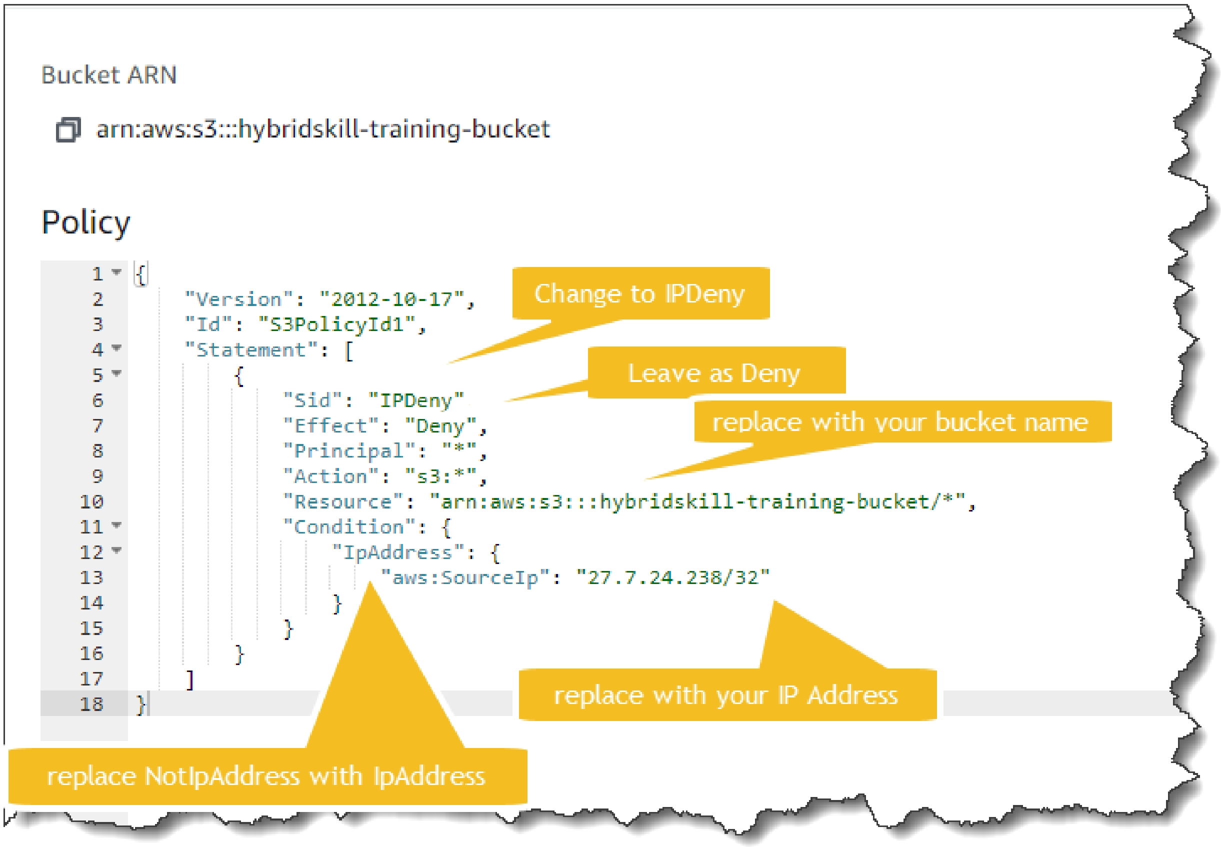
What's my IP

27.7.24.238

Your public IP address

Learn more about IP addresses

8. Next customize the code as following.



Bucket ARN

arn:aws:s3:::hybridskill-training-bucket

Policy

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "IPDeny"
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::hybridskill-training-bucket/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "27.7.24.238/32"
                }
            }
        }
    ]
}
```

Change to IPDeny

Leave as Deny

replace with your bucket name

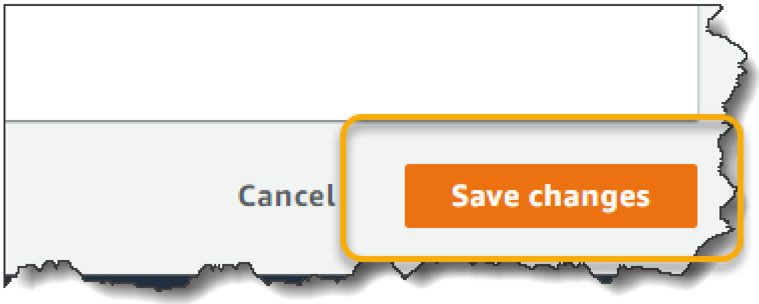
replace with your IP Address

replace NotIpAddress with IpAddress

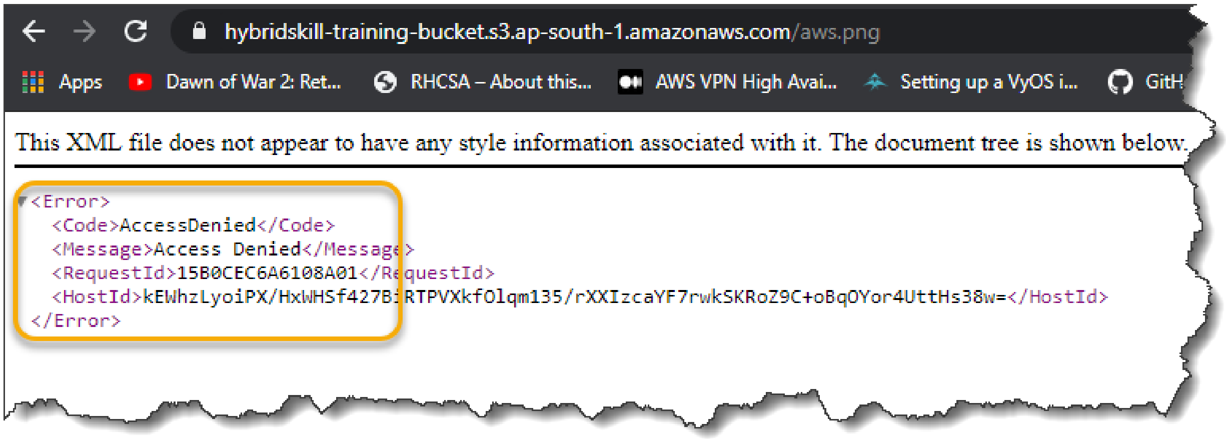
9. This is what your final code should look like.

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "IPDeny",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::hybridskill-training-bucket/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "27.7.24.238/32"
                }
            }
        }
    ]
}
```

10. Finally click **Save changes**



11. Revisit the URL on the browser. You should be denied.



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

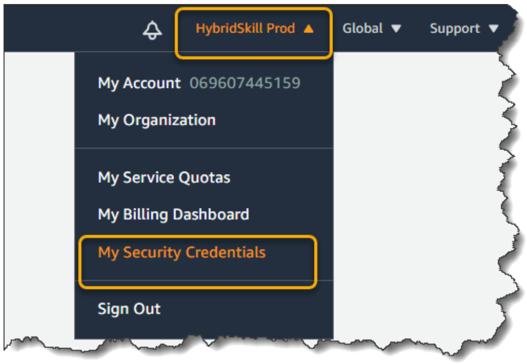
```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>15B0CEC6A6108A01</RequestId>
  <HostId>kEWhzLyoiPX/HxWHSf427BiRTPVXkfOlqm135/rXXIzcaYF7rwkSKRoZ9C+oBqOYor4UttHs38w=</HostId>
</Error>
```

Task 4 Download Security Credentials

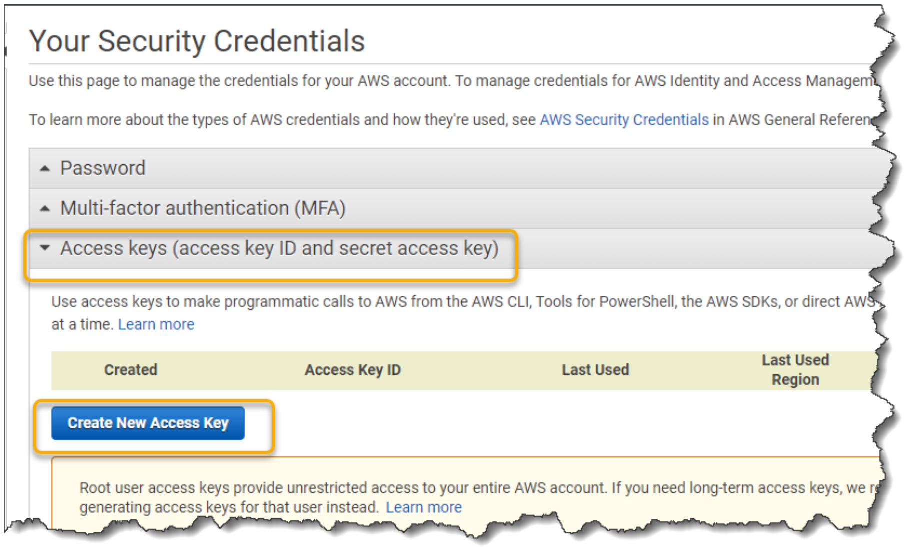
First we will download an Access key and Secret Key to sign our API calls. Depending on whether you have created your own account or are sub account under a corporate account follow either step A or B.

A. For Root account users

1. Log into the console, at the top left click on your **login name** and from the dropdown click on **Security Credentials.**



2. Expand **Access keys (access key ID and secret access key)** and click **Create New Access Key**



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Managem

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Referen

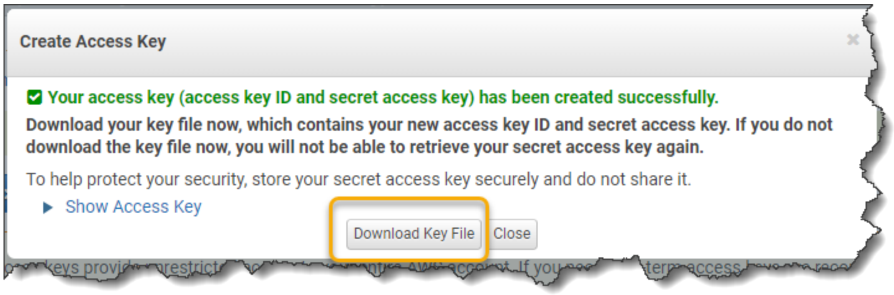
Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS at a time. Learn more

Created	Access Key ID	Last Used	Last Used Region

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we r generating access keys for that user instead. Learn more

Password
Multi-factor authentication (MFA)
Access keys (access key ID and secret access key)
Create New Access Key

3. Click **Download Key File.** We will use this next



Create Access Key

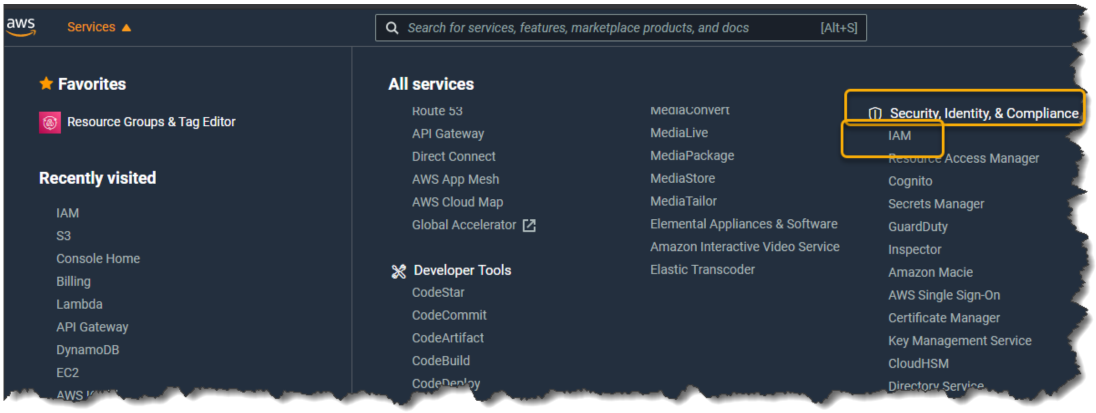
☑ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

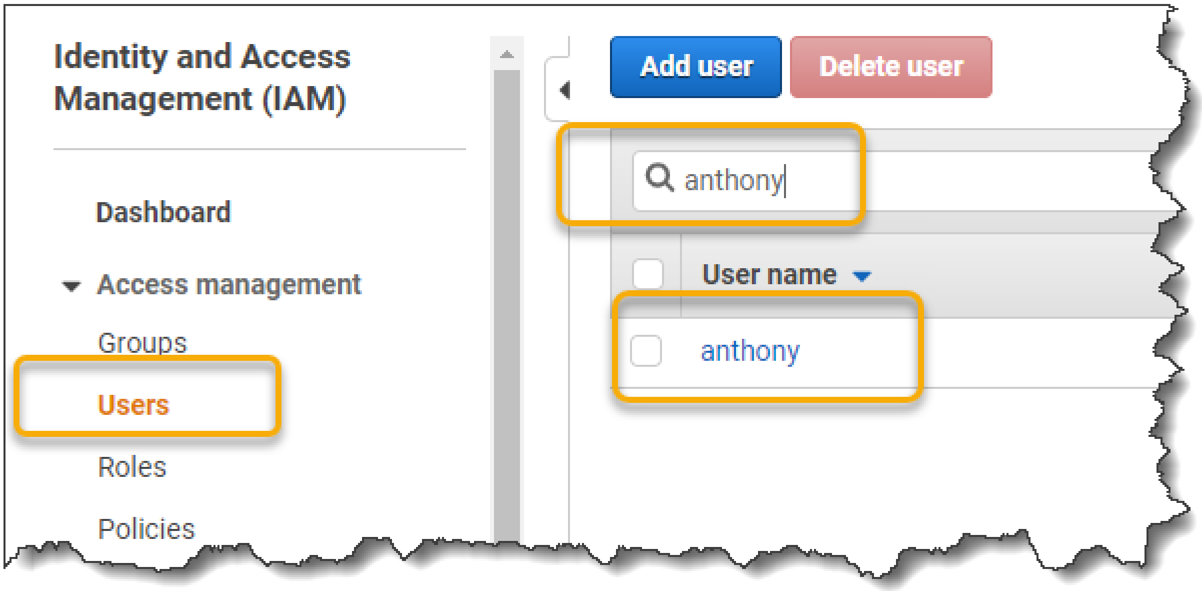
To help protect your security, store your secret access key securely and do not share it.

B. For IAM subaccount users

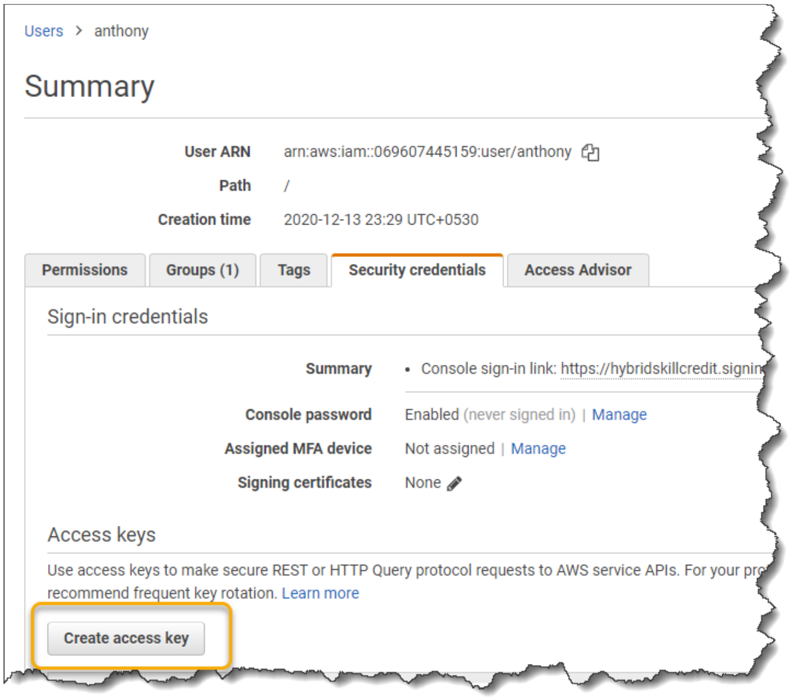
1. Click **Services** and under **Security Identity and Compliance** click **IAM**



2. Click **Users** search for your **username** and click on it for more details



3. Click on the **Security credentials** tab and click on **Create access key**



Users > anthony

Summary

User ARN arn:aws:iam::069607445159:user/anthony

Path /

Creation time 2020-12-13 23:29 UTC+0530

Sign-in credentials

Summary • Console sign-in link: https://hybridskillcredit.signin

Console password Enabled (never signed in) | Manage

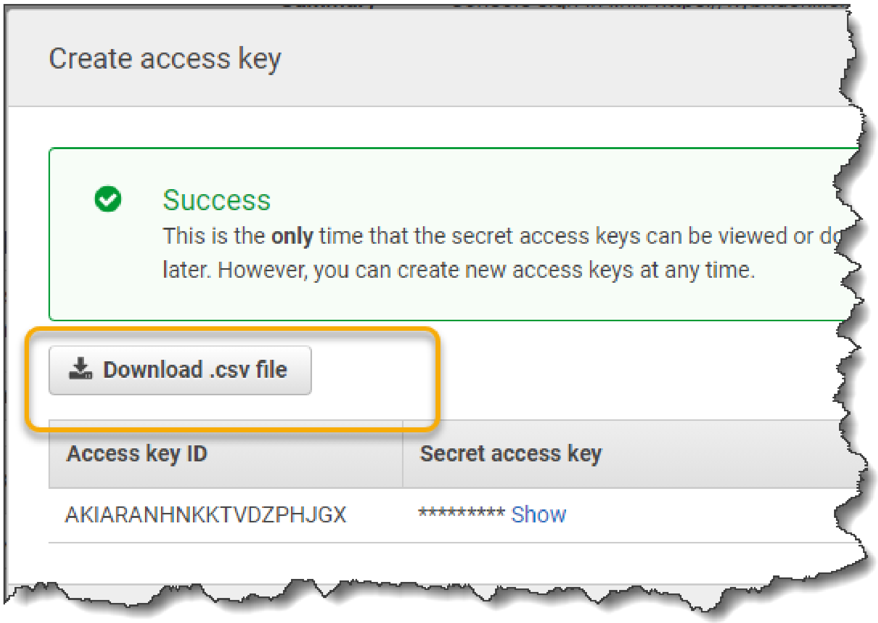
Assigned MFA device Not assigned | Manage

Signing certificates None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your pro
recommend frequent key rotation. Learn more

Finally click on **Download .csv file**



Create access key

Success

This is the **only** time that the secret access keys can be viewed or do later. However, you can create new access keys at any time.

Access key ID	Secret access key
AKIARANHNKKTVDZPHJGX	********* Show

Task 5 Setup the AWS CLI

In this task we are going to setup the AWS CLI and authorize it to perform command line API calls using the Access keys you downloaded earlier

1. Visit http://aws.amazon.com/cli/ and download and run the Windows or Mac installer

Next open a Command prompt or Terminal and type the below command. Note that "**YOUR_AWS_ACCESS_KEY**" should be replaced by your actual access key and "**YOUR_AWS_SECRET_KEY**" should be replaced by an actual secret key that was downloaded.

```
aws configure

AWS Access Key ID [None]: YOUR_AWS_ACCESS_KEY

AWS Secret Access Key [None]: YOUR_AWS_SECRET_KEY

Default region name [None]: ap-southeast-1

Default output format [None]:
```

Task 6: Manage S3 through CLI

Now that we have explored S3 through the console, let's do the same through the CLI.

Run the following commands on your command line interface, you had setup in the previous step.

1. Create a bucket. As before give a unique bucket name.

```
aws s3api create-bucket  --bucket hybridskill-training-bucket --region

ap-south-1 --create-bucket-configuration LocationConstraint=ap-south-1
Output
{
    "Location": "http://hybridskill-training-bucket0testing-01.s3.amazonaws.com/"
}
```

2. List your created bucket.

```
aws s3 ls s3://
Output
2018-02-16 01:12:18 hybridskill
2018-02-16 14:50:39 hybridskill-training-bucket
```

3. Copy file to bucket:

```
echo "test file" > test.txt
aws s3 cp test.txt s3://hybridskill-training-bucket/
upload: ./test.txt to s3://hybridskill-training-bucket/test.txt
aws s3 ls  s3://hybridskill-training-bucket/
Output
2018-02-26 17:16:45         10 test.txt
```

4. Download file:

```
aws s3 cp  s3://hybridskill-training-bucket/test.txt .
download: s3://hybridskill-training-bucket/test.txt to ./test.txt
```

5. Sync bucket and local directory:

```
aws s3 sync s3://hybridskill-training-bucket hybridskill/
download: s3://hybridskill-training-bucket/test.txt to hybridskill-training-
bucket/test.txt

cd hybridskill/
ls
test.txt

echo "another file" >test1.txt

aws s3 sync ./ s3://hybridskill-training-bucket/
upload: ./test1.txt to s3://hybridskill-training-bucket/test1.txt

aws s3 ls s3://hybridskill-training-bucket/
2018-02-26 17:16:45         10 test.txt
2018-02-26 17:21:53         13 test1.txt
```

6. Delete file:

```
aws s3 rm  s3://hybridskill-training-bucket/test.txt
delete: s3://hybridskill-training-bucket0testing-01/test1.txt
```

7. List policies:

```
aws s3api  get-bucket-policy --bucket hybridskill-training-bucket --output text
{
    "Id": "PolicyId2",
    "Statement": [
        {
            "Action": "s3:*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "106.51.29.138/32"
                }
            },
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "arn:aws:s3:::hybridskill-training-bucket/*",
            "Sid": "DenyIP"
        }
    ],
    "Version": "2012-10-17"
}
```

8. Delete Policy

```
aws s3api delete-bucket-policy --bucket hybridskill-training-bucket

aws s3api get-bucket-policy --bucket hybridskill-training-bucket --output text
A client error (NoSuchBucketPolicy) occurred when calling the GetBucketPolicy
operation: The bucket policy does not exist
```

9. Put same policy via cmd:

```
create a policy.json file
cat policy.json
{
    "Id": "PolicyId2",
    "Statement": [
        {
            "Action": "s3:*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "106.51.29.138/32"
                }
            },
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "arn:aws:s3:::hybridskill-training-bucket/*",
            "Sid": "DenyIP"
        }
    ],
    "Version": "2012-10-17"
}

:~$ aws s3api put-bucket-policy --bucket hybridskill-training-bucket  --policy
file://./policy.json

:~$ aws s3api get-bucket-policy --bucket hybridskill-training-bucket   --output text
{
    "Id": "PolicyId2",
    "Statement": [
        {
            "Action": "s3:*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "106.51.29.138/32"
                }
            },
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "arn:aws:s3:::hybridskill-training-bucket/*",
            "Sid": "DenyIP"
        }
    ],
    "Version": "2012-10-17"
}
```

Important: Cleanup of all Resources

Next let’s follow this checklist make sure all resources are cleaned up. to prevent billing to your account.

- **S3 buckets**