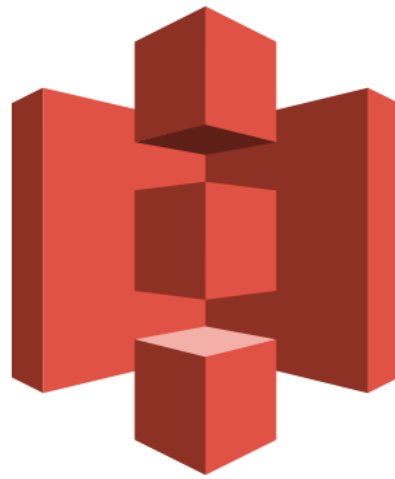


AMAZON S₃

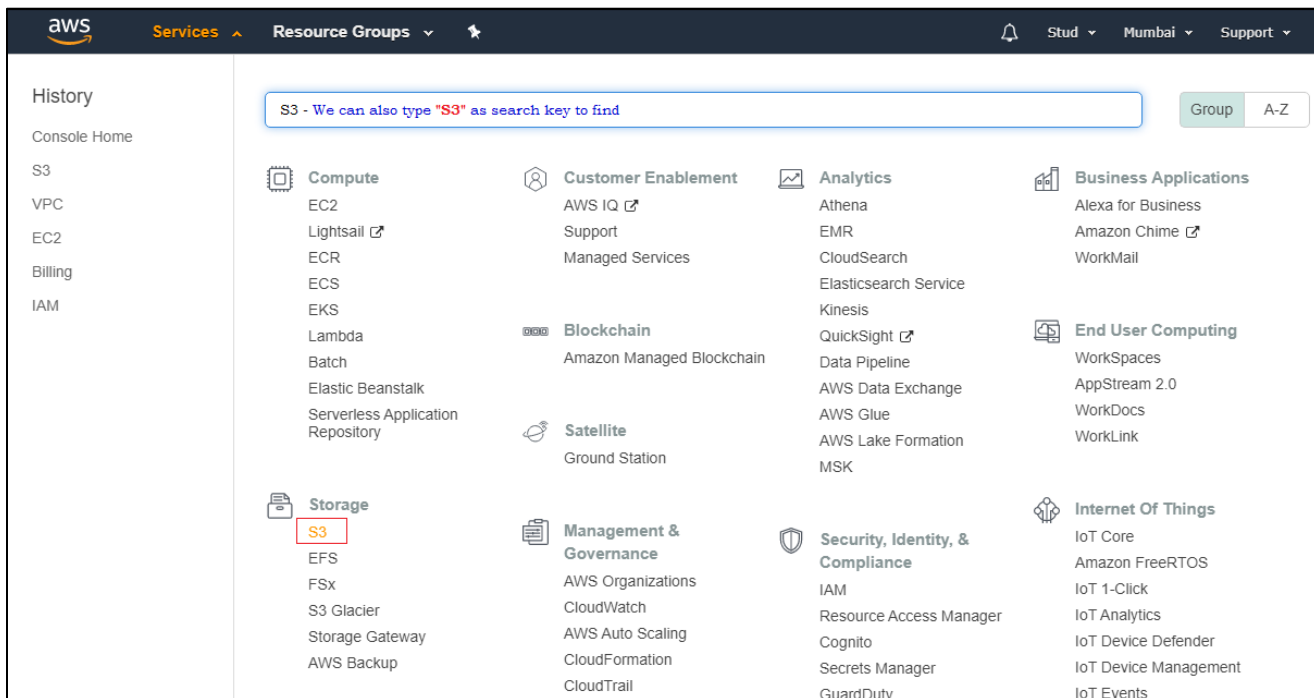


Simple Storage Solution

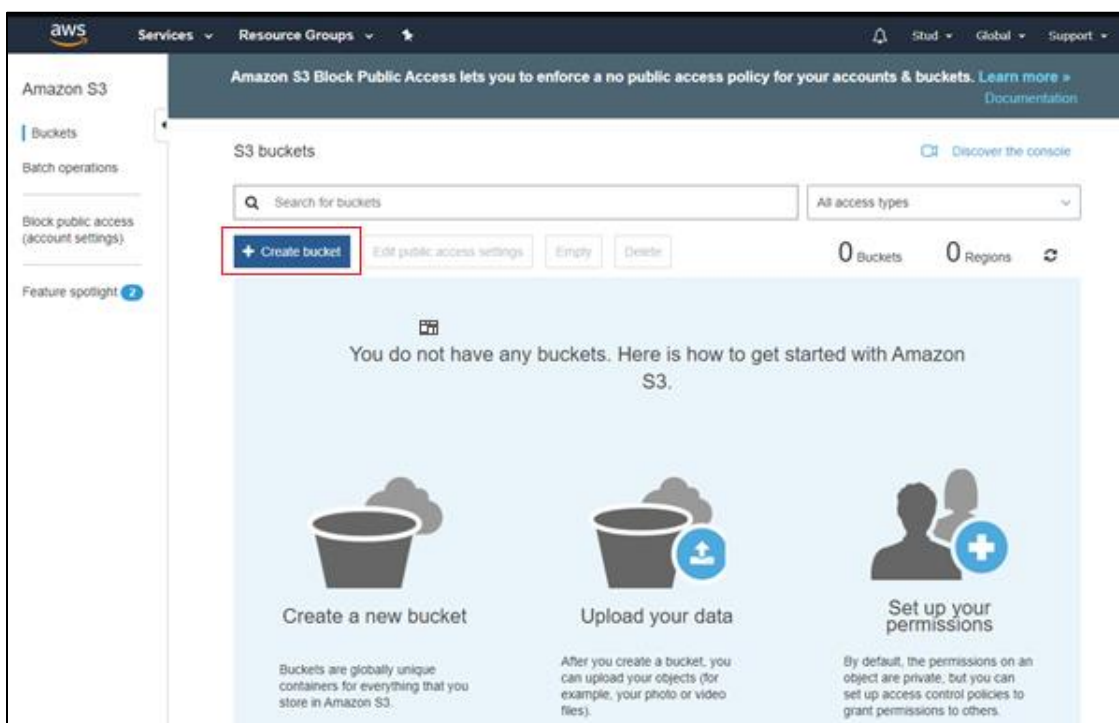
Amazon S3: is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. It allows to upload, store, and download any type of files up to 5 TB in size.

Steps to create an amazon S3 bucket with a public access:

1. Login into Amazon Console and in the services search for S3 below Storage features



2. It will open a new console page to Amazon S3 and to Create Bucket select + sign create bucket icon



3. We need to provide the name, Region and copy the setting of the previous bucket if there are any available and select next for configure options

aws Services Resource Groups

Create bucket

1 Name and region 2 Configure options 3 Set permissions 4 Review

Name and region

Bucket name - Name the bucket based on your needs or Organizations

Region - Region selection

Copy settings from an existing bucket

If any buckets are created previously then the selected bucket settings will be copied to this bucket

Create Cancel Next

Feedback English (US) © 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4. In this option select and make change based on your requirement and select next to set permission

aws Services Resource Groups

Create bucket

1 Name and region 2 Configure options 3 Set permissions 4 Review

Properties

Versioning ☐ Keep all versions of an object in the same bucket. [Learn more](#)

Server access logging ☐ Log requests for access to your bucket. [Learn more](#)

Tags You can use tags to track project costs. [Learn more](#)

[Add another](#)

Object-level logging ☐ Record object-level API activity using AWS CloudTrail for an additional cost. See [CloudTrail pricing](#) or [learn more](#)

Default encryption ☐ Automatically encrypt objects when they are stored in S3. [Learn more](#)

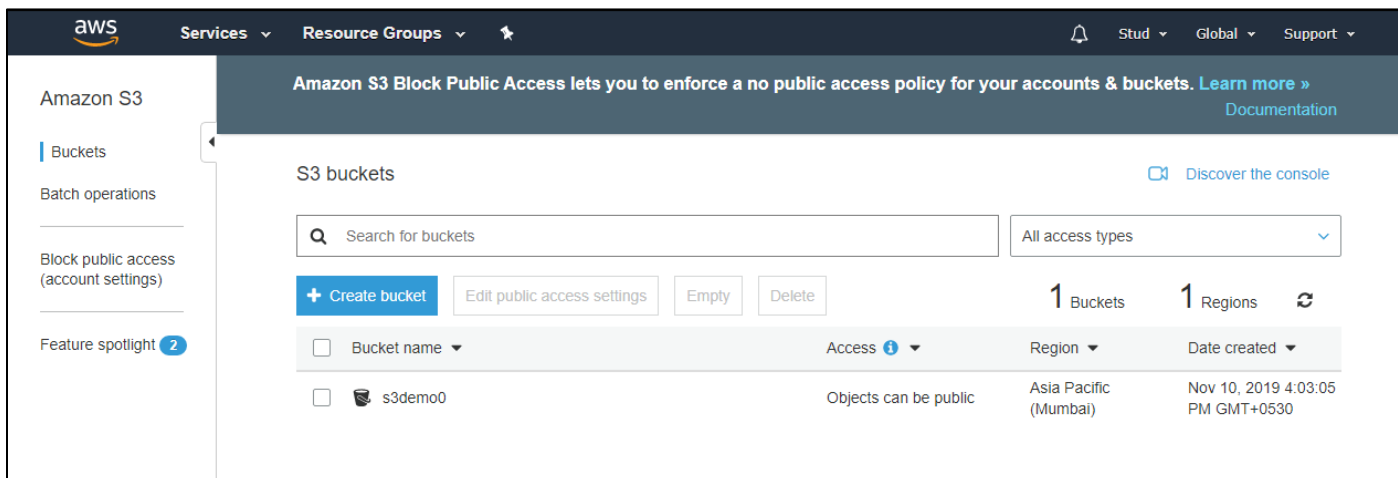
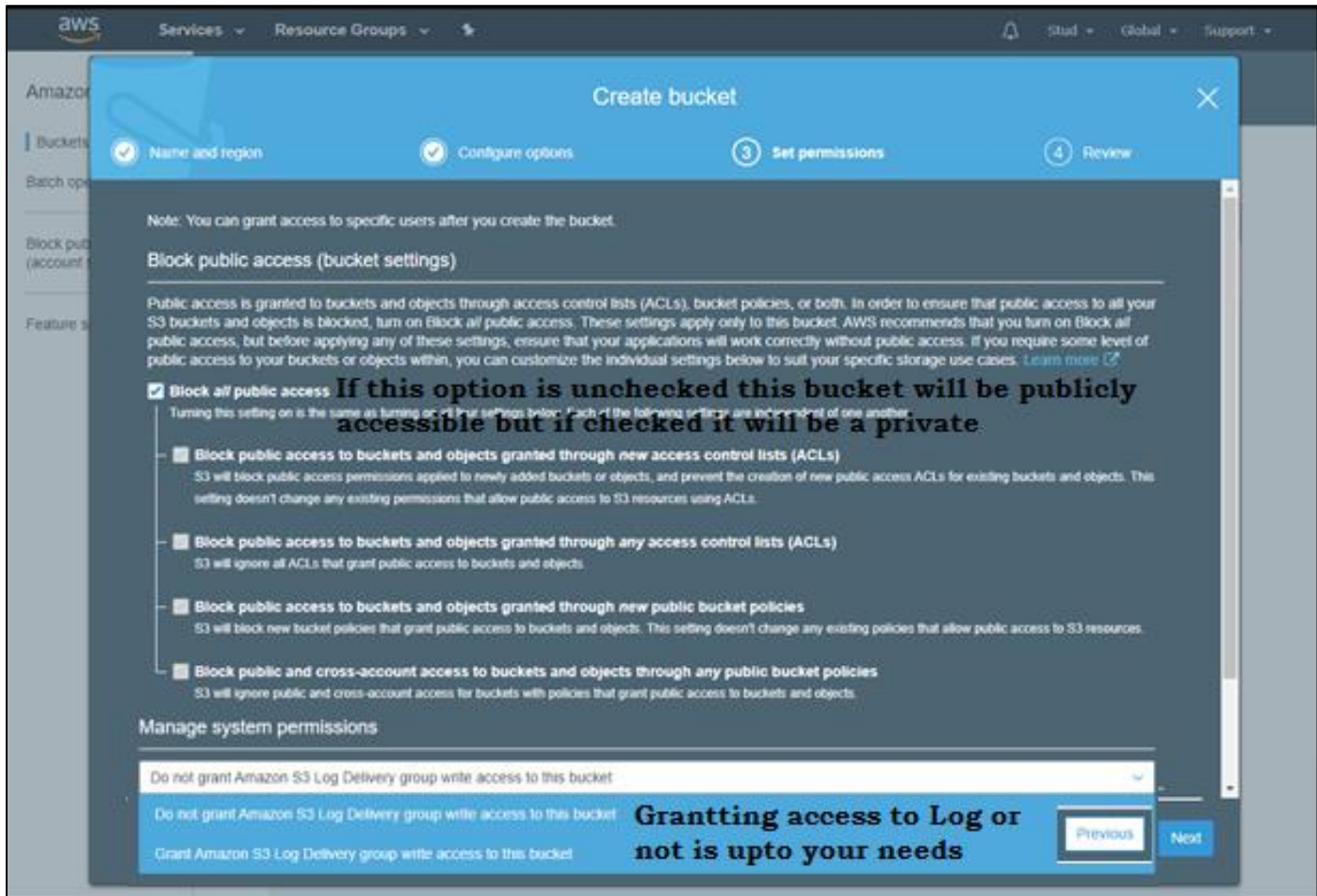
[Advanced settings](#)

Management

Previous Next

Go to Settings to activate Win

5. While setting the Permission we need to provide the access based on the need of the project or usage of bucket. The next option will be reviewing and next to it the bucket will be created



6. When you select the bucket it display three function of bucket as given the picture

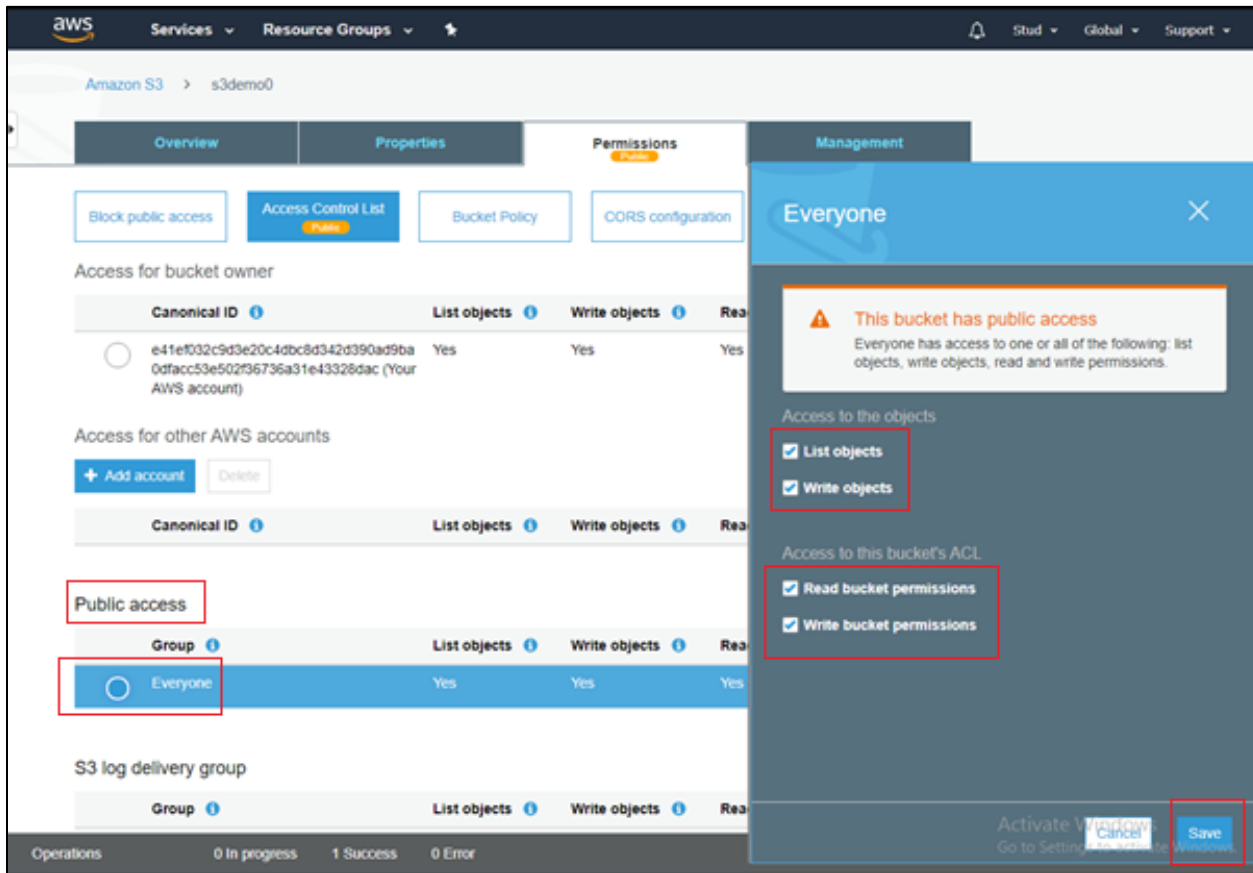
On the 5th steps the box is **checked** hence **public access** has been disabled to enabled it select the the **Permission** on the Top to change the access

7. Select the **Permission** from the 6th step and it will navigate to this page image given below

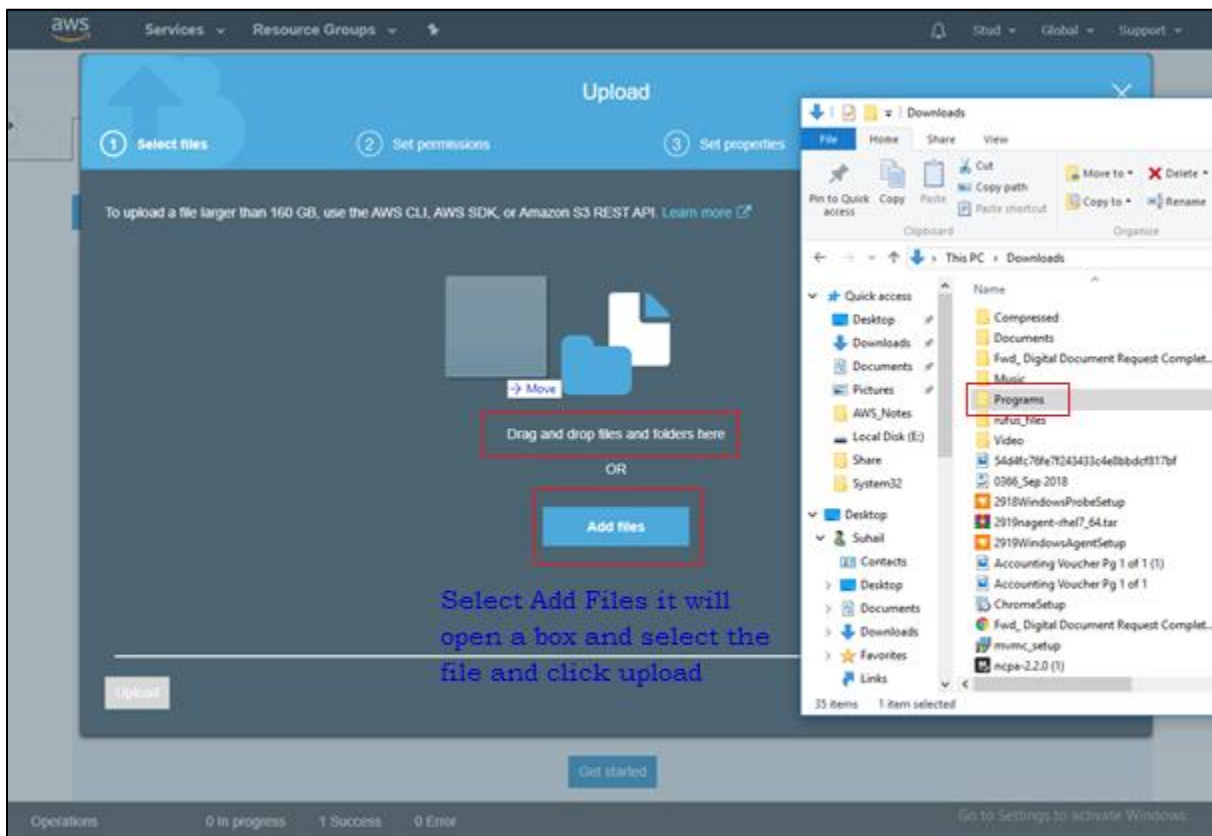
Click on the **ACL** to provide the access publicly or to an **recommended users and Groups**

Click the **Edit** and just **uncheck the checked boxes**

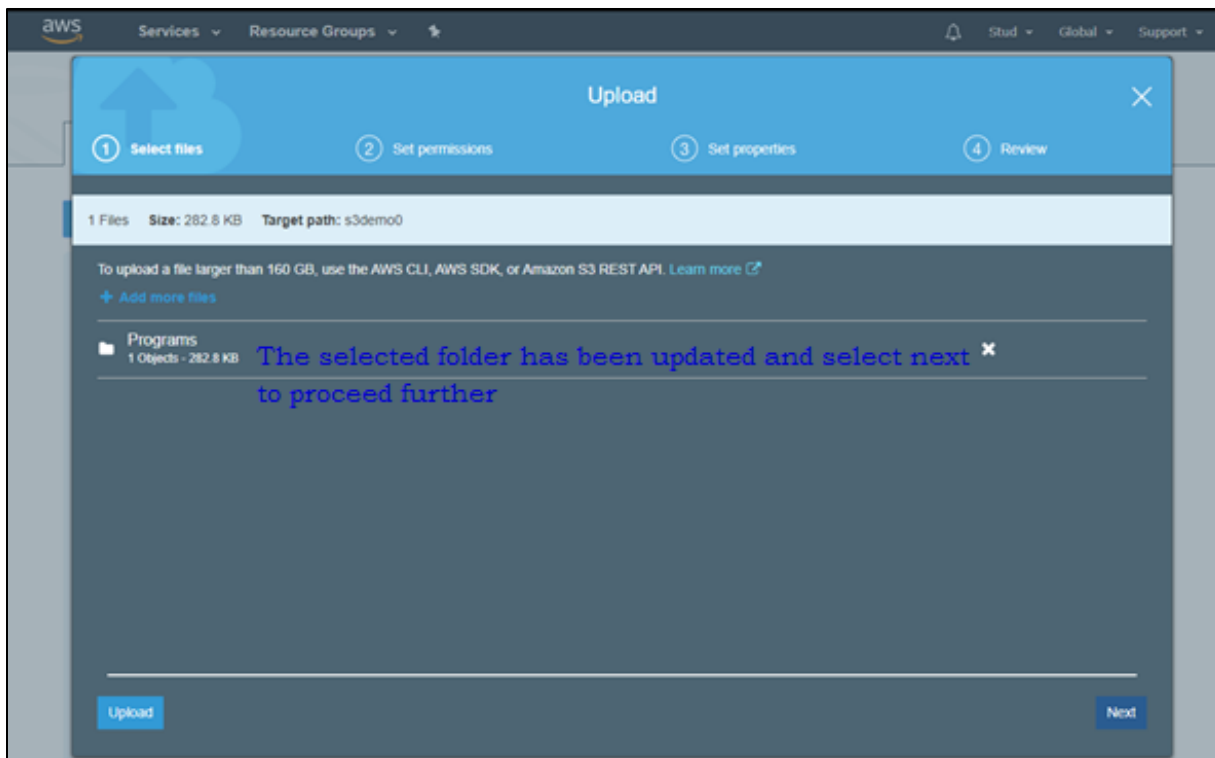
8. Select the ACL on the top it will open a new window in it below Public access, select the Everyone and check all the box to access the S3 storage bucket publicly and save it



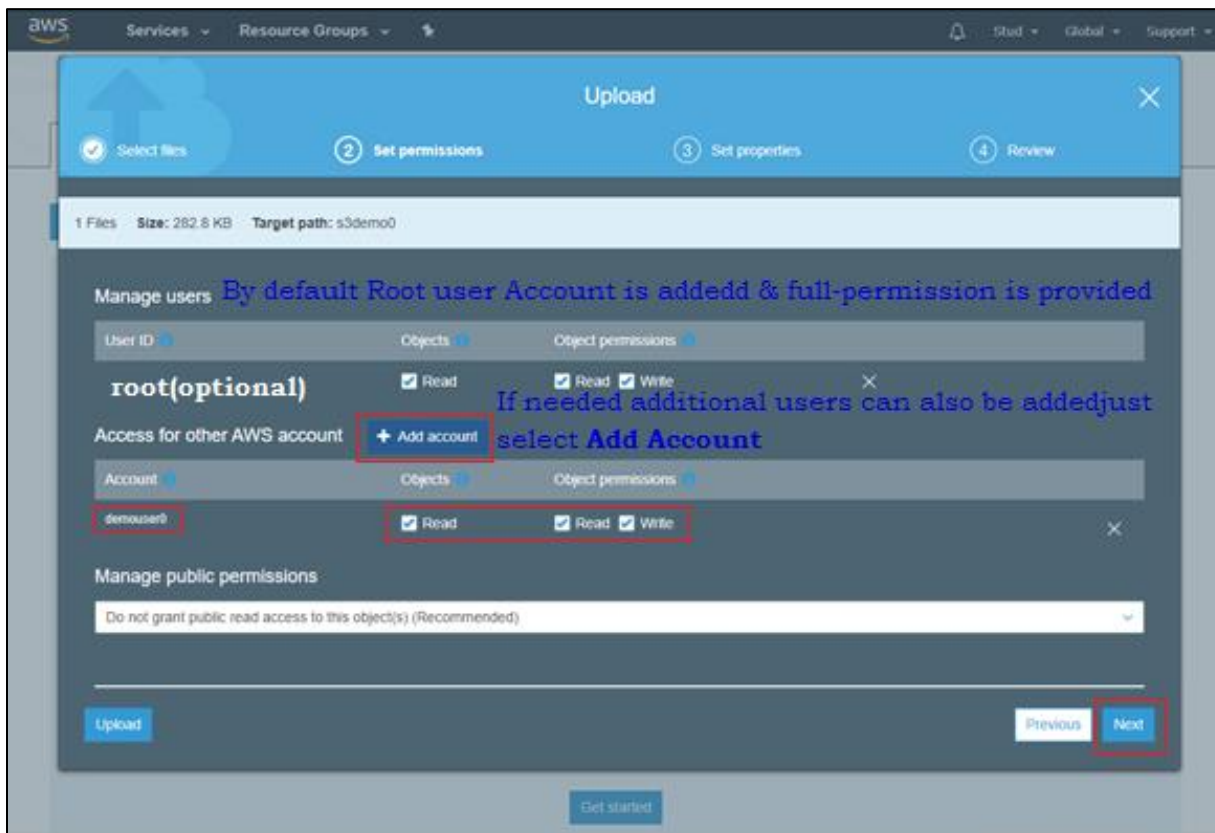
9. Once it's done start adding the file by select the option Add Files or open folder in your computer and select the file Drag & Drop it



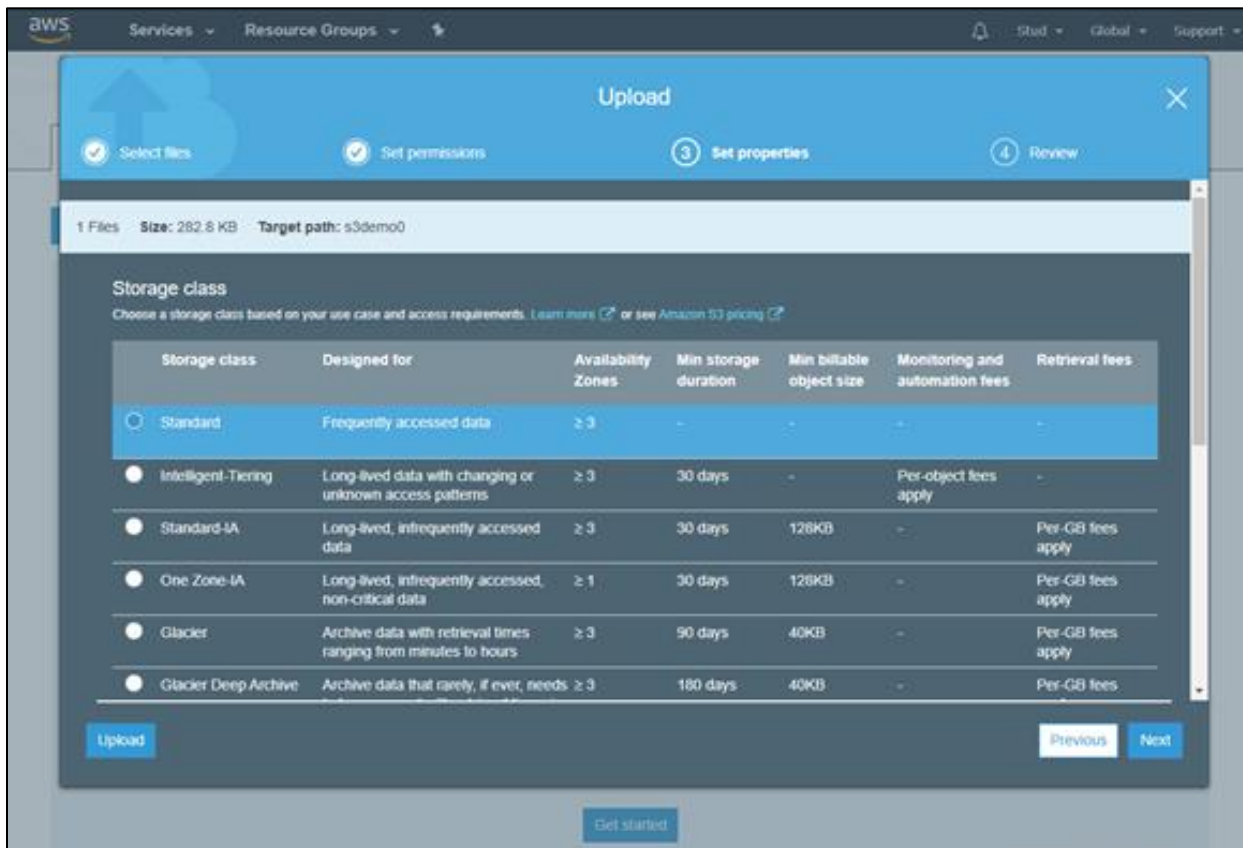
10. The Folder has been update and select next to set the permission of the selected folder



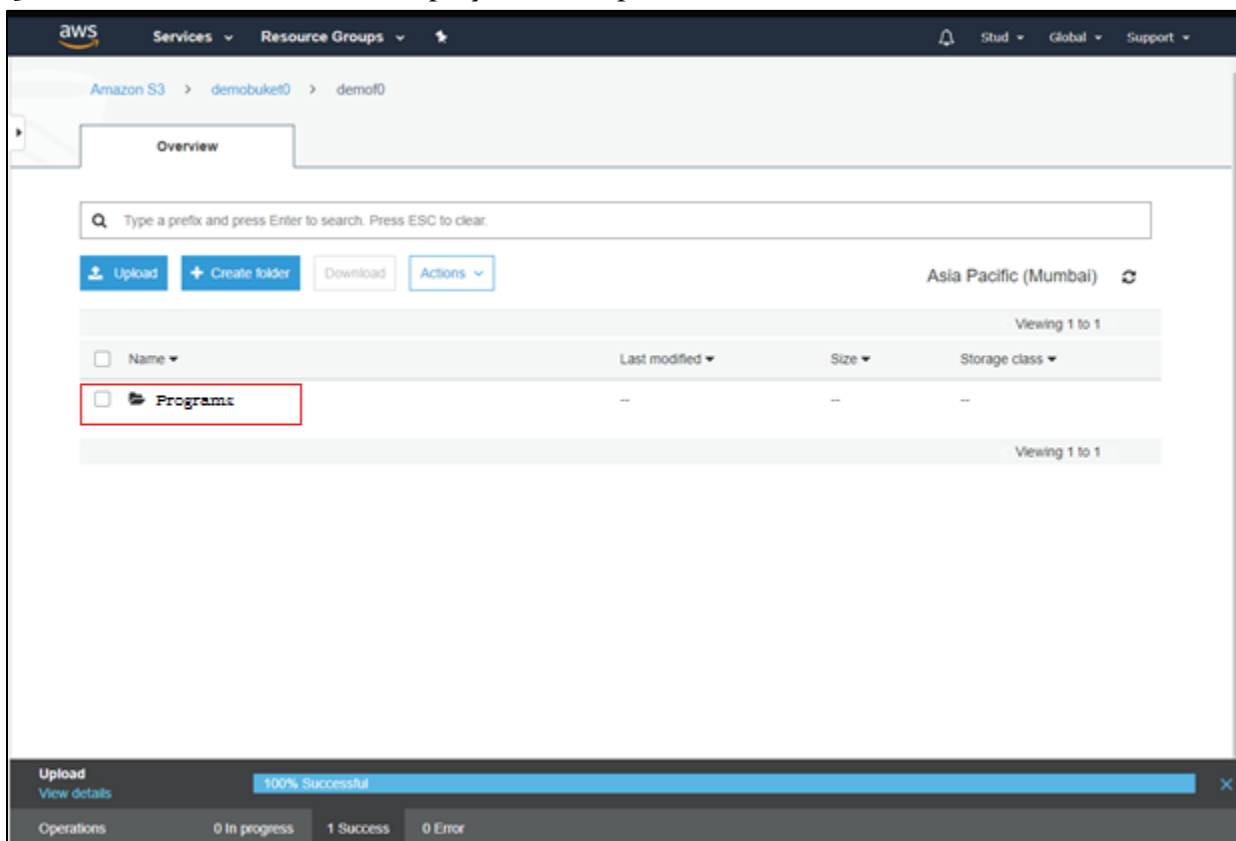
11. Users added and Permission are given in this page



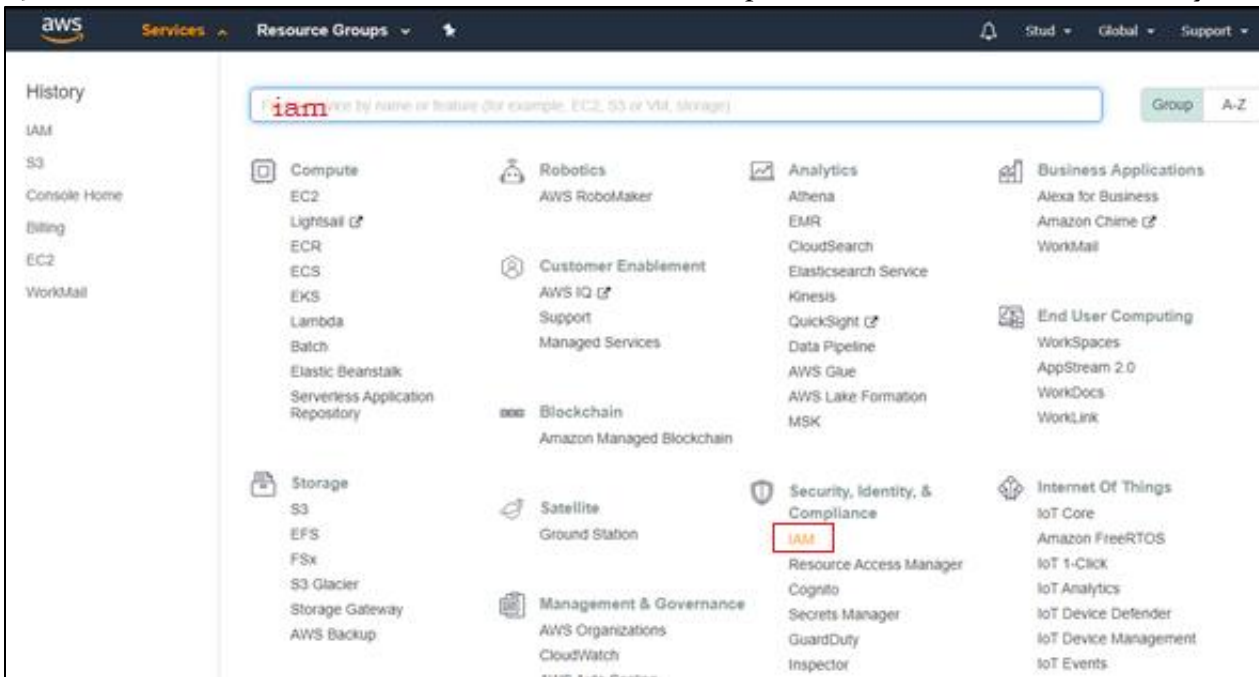
12. Based on project needs properties are selected. I am selecting Standard and next to review and upload the Folder/Files



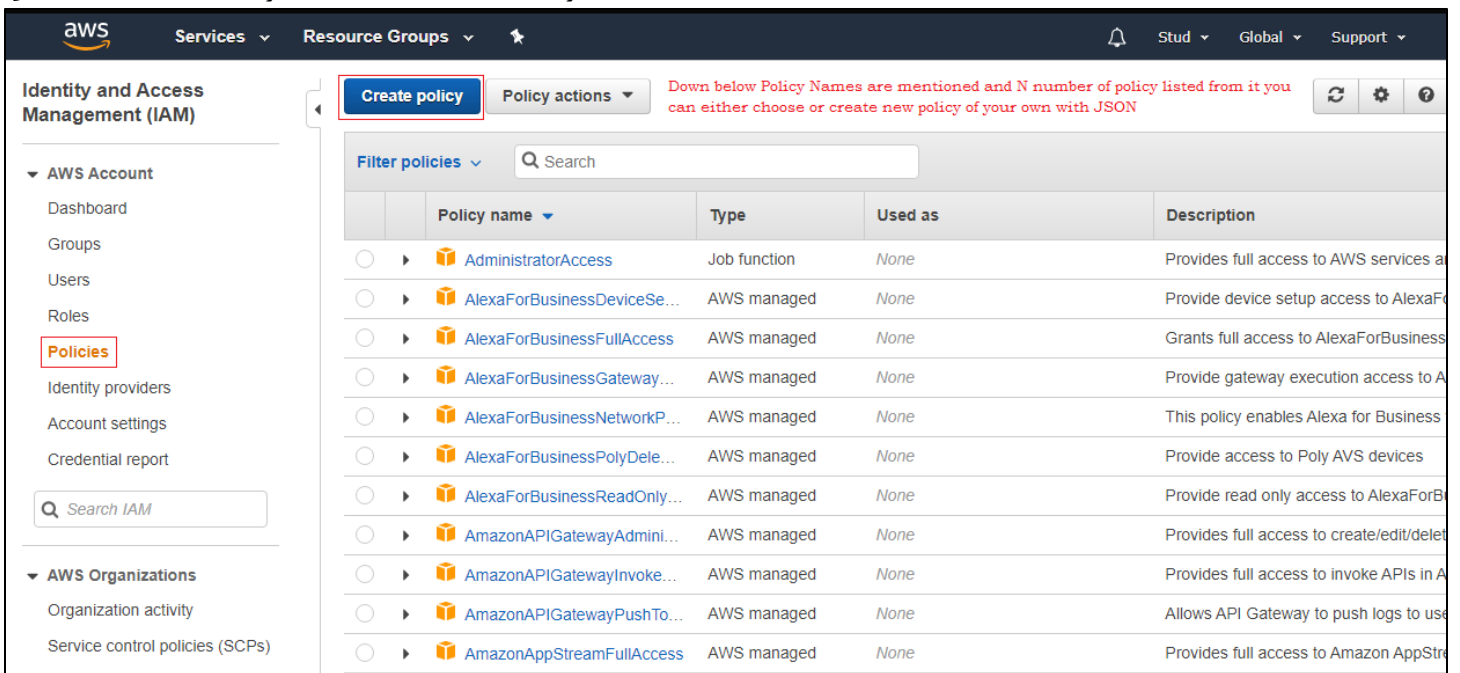
13. On the below the it will display the file upload was Success



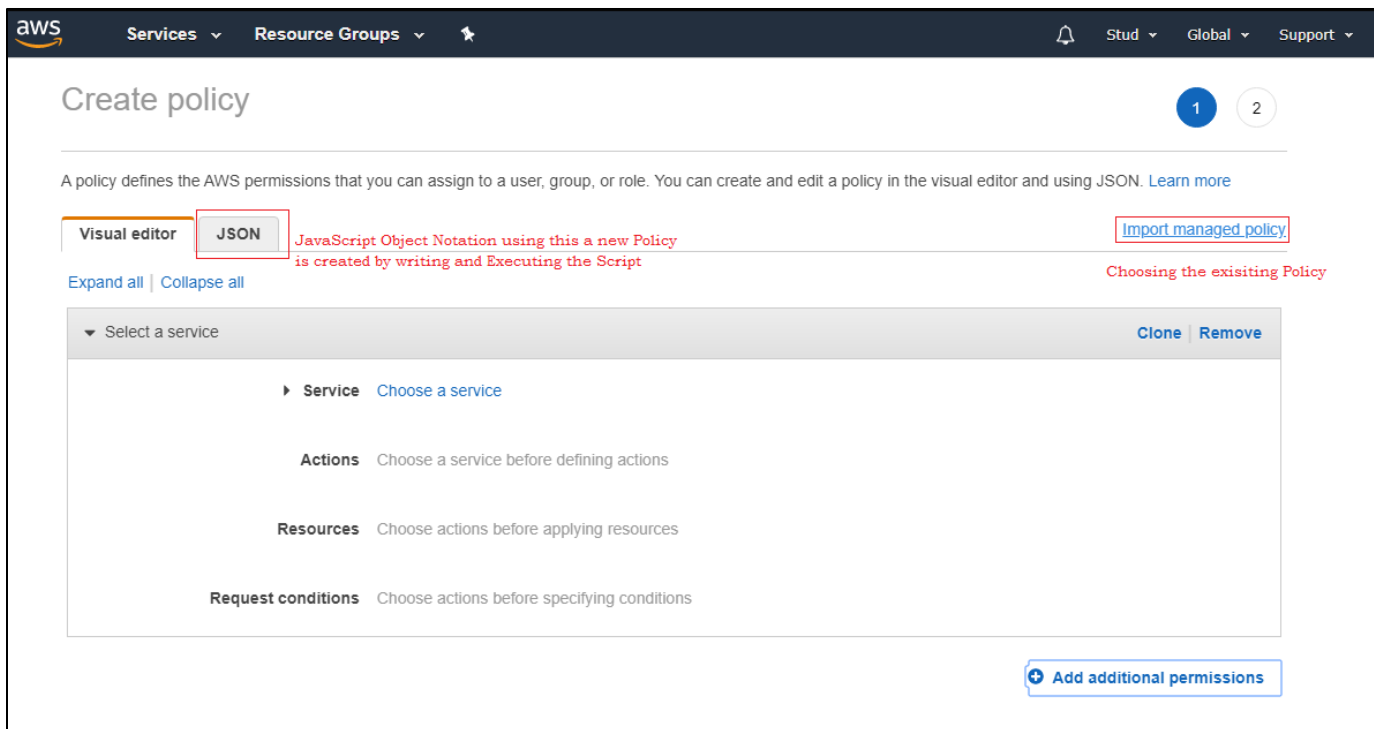
14. Go to Service search and select IAM roles to write policies for the bucket based on your needs



15. In this window you can create a Policy

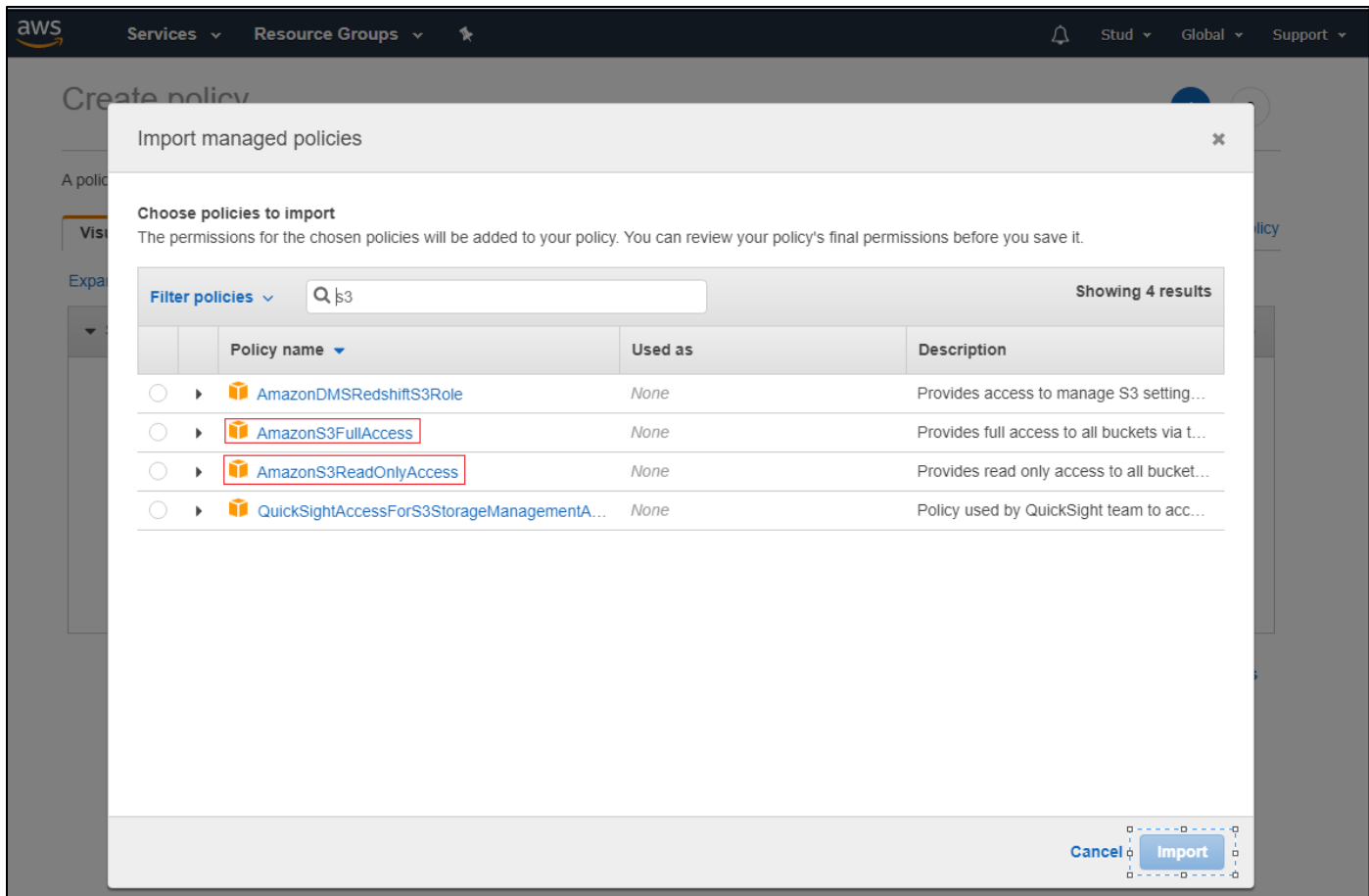


16. Policy can be created using JSON or import the existing policy



The screenshot shows the AWS IAM 'Create policy' page. The 'JSON' tab is selected, and a red box highlights it. The 'Visual editor' tab is also visible. The page includes a description of policies and a link to 'Learn more'. Below the tabs, there are instructions for creating a policy using JSON. A red box highlights the 'JSON' tab and the text 'JavaScript Object Notation using this a new Policy is created by writing and Executing the Script'. Another red box highlights the 'Import managed policy' link. The page also shows a 'Select a service' dropdown and a 'Clone | Remove' button. At the bottom, there is an 'Add additional permissions' button.

17. Import the existing Policy once it selected import the Policy



The screenshot shows the 'Import managed policies' dialog box in the AWS IAM console. The dialog box has a title bar 'Import managed policies' and a close button. Below the title bar, there is a section 'Choose policies to import' with a description: 'The permissions for the chosen policies will be added to your policy. You can review your policy's final permissions before you save it.' Below this, there is a search bar with the text 'Filter policies' and a search input field containing 's3'. To the right of the search bar, it says 'Showing 4 results'. Below the search bar, there is a table with the following columns: 'Policy name', 'Used as', and 'Description'. The table contains four rows of results:

	Policy name	Used as	Description
<input type="radio"/>	AmazonDMSRedshiftS3Role	None	Provides access to manage S3 setting...
<input type="radio"/>	AmazonS3FullAccess	None	Provides full access to all buckets via t...
<input type="radio"/>	AmazonS3ReadOnlyAccess	None	Provides read only access to all bucket...
<input type="radio"/>	QuickSightAccessForS3StorageManagementA...	None	Policy used by QuickSight team to acc...

At the bottom right of the dialog box, there are 'Cancel' and 'Import' buttons. The 'Import' button is highlighted with a red box.

18. After importing the Policy select Review

Create policy 1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON [Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ S3 (39 actions) ⚠ 2 warnings [Clone](#) [Remove](#)

- ▶ **Service** S3
- ▶ **Actions** Manual actions
 - Get*
 - List*
- ▶ **Resources** Specify **bucket** resource ARN for the **GetBucketLocation** and 23 more actions. ⓘ
Specify **object** resource ARN for the **GetObjectVersionForReplication** and 11 more actions. ⓘ
*
- ▶ **Request conditions** [Specify request conditions \(optional\)](#)

[+ Add additional permissions](#)

Character count: 126 of 6,144. [Cancel](#) [Review policy](#)

19. Select Create Policy to create the policy

Create policy 1 2

Review policy

Name* s3demo0
Use alphanumeric and '*-.,@_-' characters. Maximum 128 characters.

Description As you please to fill
Maximum 1030 characters. Use alphanumeric and '*-.,@_-' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 205 services) Show remaining 204			
S3	Limited: List, Read, Write	All resources	None

* Required [Cancel](#) [Previous](#) [Create policy](#)

20. Custom Policy has been created

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with options like 'AWS Account', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. The 'Policies' option is selected. A green notification banner at the top states 's3demo0 has been created.' Below this, there is a 'Create policy' button and a 'Policy actions' dropdown. A search bar contains 's3'. A table lists policies:

	Policy name	Type	Used as	Description
<input type="radio"/>	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings
<input type="radio"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via
<input type="radio"/>	AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all buck
<input type="radio"/>	QuickSightAccessForS3Stor...	AWS managed	None	Policy used by QuickSight team to ac
<input checked="" type="radio"/>	s3demo0	Customer managed	None	As you please to fit

21. Policy is attached to Users or Groups by selecting the particular Users and in it Add Permissions

The screenshot shows the 'Summary' page for a user named 'demouser' in the AWS IAM console. The left sidebar has 'Users' selected. A green notification banner at the top states 'Policy has been detached from the user demouser'. The user's details are shown: User ARN is 'arn:aws:iam::user:demouser', Path is '/', and Creation time is '2019-11-10 16:36 UTC+0530'. Below this, there are tabs for 'Permissions', 'Groups (1)', 'Tags', 'Credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies (2 policies attached)'. A blue button labeled 'Add permissions' is highlighted. Below this, there is a table of attached policies:

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy

Below the table, there is a link 'Show 1 more'. At the bottom, it says 'Permissions boundary (not set)'.

22. Search and select existing Policy to attach under the existing policy directly and in the next page select Add permission to attach the Policy to the user

Add permissions to demouser

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Filter policies: Showing 1 result

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	demopolicy	Customer managed	None

23. Once the Policy has been attached it will be displayed below in the Add permissions

Identity and Access Management (IAM)

Users > demouser

Summary

User ARN: iam:aws:iam::...
 Path: /
 Creation time: 2019-11-10 16:36 UTC+0530

Permissions policies (3 policies applied)

Policy name	Policy type	
Attached directly		
AmazonS3FullAccess	AWS managed policy	<input type="button" value="x"/>
demopolicy	Managed policy	<input type="button" value="x"/>

[Show 2 more](#)

Permissions boundary (not set)

Steps to Create a Key:

1. In the top of the AWS Console select your name and drop a list in those select My Security Credentials

Identity and Access Management (IAM)

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS API calls, use the [IAM console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#).

▲ Password
 ▲ Multi-factor authentication (MFA)
 ▼ Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Nov 10th 2019		AKIAJ6F7Z36SIYRROBAA	N/A	N/A	N/A	Active	Make Inactive Delete

[Create New Access Key](#)

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. [Learn more](#)

Beginning in early December 2019, the console will no longer display deleted access keys for root users. If CloudTrail is enabled, you can view deleted access keys in your logs.

2. Select Create New Access Key to create a Key

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.

▼ [Hide Access Key](#) **Copy and Paste the Access and Secret Key hence the Secret will not be displayed or Select Download Key File to download it in Excel format**

Access Key ID: AKIAIIRVYQACPMW2GKLQ

Secret Access Key: bP2dTQnS/WubyiDVddJJjxmA0YMbWW+CPzpHHzRM

[Download Key File](#) [Close](#)

Steps to Mount the S3 bucket in Linux:

1. Login your Linux Console
2. Update the OS - > `yum -y update`

Install the necessary packages - > `yum install automake fuse fuse-devel gcc-c++ git libcurl-devel libxml2-devel make openssl-devel`

3. Use this command to clone the code from git - > `git clone https://github.com/s3fs-fuse/s3fs-fuse.git`

```
[root@studserver ~]# git clone https://github.com/s3fs-fuse/s3fs-fuse.git
Cloning into 's3fs-fuse'...
remote: Enumerating objects: 26, done.
remote: Counting objects: 100% (26/26), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 5738 (delta 10), reused 4 (delta 1), pack-reused 5712
Receiving objects: 100% (5738/5738), 3.42 MiB | 755.00 KiB/s, done.
Resolving deltas: 100% (3968/3968), done.
```

4. Change directory to compile and install the code - > `cd s3fs-fuse`

```
[root@studserver ~]# cd s3fs-fuse
[root@studserver s3fs-fuse]# ls
AUTHORS      ChangeLog      configure.ac  doc            Makefile.am  src
autogen.sh   COMPILATION.md COPYING        INSTALL        README.md    test
```

5. Compile the code - > `./autogen.sh`
6. Configure the code - > `./configure --prefix=/usr --with-openssl`
7. Install the code -> `make`
8. Install all - > `make install`
9. Open an editor copy and paste the Access and Secret Keys in the location - > `nano /etc/passwd-s3fs`

```
[root@studserver s3bucket]# nano /etc/passwd-s3fs
```

```
GNU nano 2.3.1      File: /etc/passwd-s3fs
Your_accesskey:Your_secretkey
```

10. Change the permission of the folder - > `chmod 640 /etc/passwd-s3fs`

```
[root@studserver s3bucket]# chmod 640 /etc/passwd-s3fs
```

11. Create a folder to mount the s3 bucket - > `mkdir /s3bucket/`

```
[root@studserver s3bucket]# mkdir /s3bucket/
```

12. Enter this command - > `s3fs your_bucketname -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket`

13. Open editor and enter the following command - > **nano /etc/rc.local/ “/usr/local/bin/s3fs your_bucketname -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket”**

```
GNU nano 2.3.1 File: /etc/rc.local
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local

/usr/local/bin/s3fs s3demo0 -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=0$
```

14. Use the command **df -Th** for verification - > **df -Th**

```
[root@studserver s3bucket]# df -Th
Filesystem Type Size Used Avail Use% Mounted on
devtmpfs devtmpfs 744M 0 744M 0% /dev
tmpfs tmpfs 756M 0 756M 0% /dev/shm
tmpfs tmpfs 756M 8.9M 747M 2% /run
tmpfs tmpfs 756M 0 756M 0% /sys/fs/cgroup
/dev/mapper/centos-root ext4 50G 1.8G 45G 4% /
/dev/sda1 ext4 976M 130M 780M 15% /boot
/dev/mapper/centos-home ext4 18G 45M 17G 1% /home
tmpfs tmpfs 152M 0 152M 0% /run/user/0
s3fs fuse.s3fs 256T 0 256T 0% /s3bucket
```

Amazon Reference Links:

1. <https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-configure-bucket.html>
2. https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/?sc_ichannel=ha&sc_icontent=console_aws-console-s3_s3_storage1_awssm-1111&sc_icampaign=Adoption_Campaign_CSI_o6_2019_Storage_S3_BlockPublicAccess_Console&trk_Campaign=CSI_Q2_2019_Storage_S3_BlockPublicAccess_Blog&trk=ha_a131L000005vHtIQAU&sc_iooutcome=CSI_Digital_Marketing&sc_iplace=console_aws-console-s3_s3_INFOBAR
3. <https://docs.aws.amazon.com/AmazonS3/latest/gsg/CreatingABucket.html>

Other Sites Reference Links:

1. <https://cloudkul.com/blog/mounting-s3-bucket-linux-ec2-instance/>
2. <https://www.javatpoint.com/aws-creating-s3-bucket>
3. <https://tecadmin.net/mount-s3-bucket-centosrhel-ubuntu-using-s3fs/>
4. <https://www.youtube.com/watch?v=gSgePWctKkU>
5. <https://www.youtube.com/watch?v=vtz3ruCebH8>
<https://www.youtube.com/watch?v=pvoKmH2GsQQ>