

# Doubt Resolving

# ASSIGNMENT



Name – Maithely Sharma  
College – University of Petroleum and Energy Studies  
EmployeeID – 4057

1. Static website hosting using s3(what is index and error page).

Firstly created two files : i) index.html , ii)error.html

```
maithely@maithely:~$ mkdir static
maithely@maithely:~$ cd static/
maithely@maithely:~/static$ sudo vim index.html
[sudo] password for maithely:
maithely@maithely:~/static$ cat index.html
index file created
maithely@maithely:~/static$ sudo vim error.html
maithely@maithely:~/static$ cat error.html
ERRROORRRRRRRRRRRRRRRRRRR
maithely@maithely:~/static$
```

Now create a bucket and upload two files created above

www.maithely-static.com

Overview Properties Permissions Management Access points

Q Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions

US East (N. Virginia)

Viewing 1 to 2			
<input type="checkbox"/> Name	Last modified	Size	Storage class
<input type="checkbox"/> error.html	Mar 11, 2020 3:56:36 PM GMT+0530	25.0 B	Standard
<input type="checkbox"/> index.html	Mar 11, 2020 3:55:44 PM GMT+0530	20.0 B	Standard

Viewing 1 to 2

In properties select static hosting and enter the file names

Static website hosting

Endpoint : <http://www.maithely-static.com.s3-website-us-east-1.amazonaws.com>

☒ Use this bucket to host a website [Learn more](#)

Index document [i](#)

index.html

Error document [i](#)

error.html

Redirection rules (optional) [i](#)

☐ Redirect requests [Learn more](#)

☐ Disable website hosting

Then save and again open dynamic hosting and you select the link

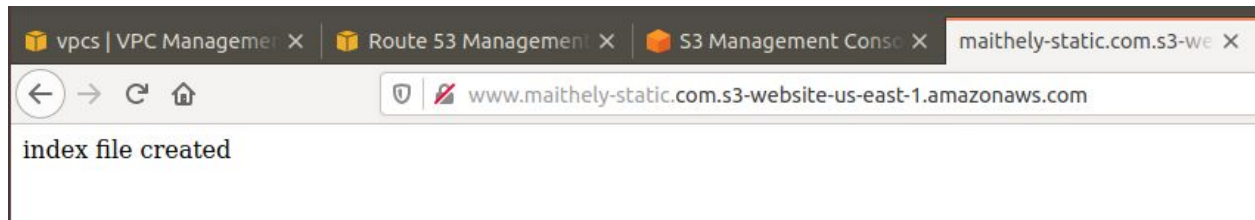
Static website hosting

Endpoint : <http://www.maithely-static.com.s3-website-us-east-1.amazonaws.com>

☒ Use this bucket to host a website [Learn more](#)

Index document [i](#)

You can see the outputs as

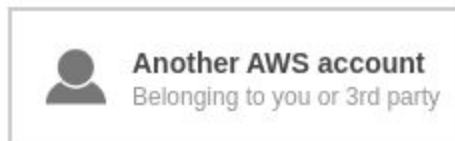
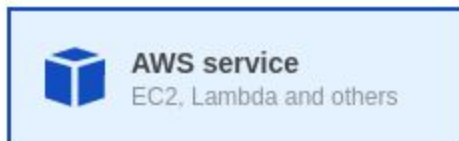


2. Create an assume role to access s3 using ec2.

Create a Role with full access to S3

## Create role

### Select type of trusted entity



Allows AWS services to perform actions on your behalf. [Learn more](#)

### Choose a use case

#### Common use cases

##### EC2

Allows EC2 instances to call AWS services on your behalf.

##### Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

Review

Provide the required information below and review this role before you create it.

Role name\*

Use alphanumeric and '+=, @-\_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-\_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies Policies not attached

Permissions boundary Permissions boundary is not set

\* Required Cancel Previous Create role




Add permissions to Maithelyrole

Attach Permissions

Create policy

Filter policies

Showing 10 results

	Policy name	Type	Used as
<input type="checkbox"/>	 AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS managed	Permissions policy (29)
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-1a3ddce4-a989-4828-88a4-7f5e701af3ef	Customer managed	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-34f3178e-e3ee-4238-8c64-0e27432978a2	Customer managed	Permissions policy (1)

Cancel Attach policy

## Summary

**Policy ARN** `arn:aws:iam::aws:policy/AmazonS3FullAccess` 

**Description** Provides full access to all buckets via the AWS Management Console.

**Permissions** | Policy usage | Policy versions | Access Advisor

Policy summary | { } JSON

Filter

Service	Access level	Resource	Request condition
Allow (1 of 223 services) <a href="#">Show remaining 222</a>			
S3	Full access	All resources	None


Create another role as Maithelyrole1 and attach policy of sts service to it


▶ Service STS

▶ Actions Manual actions


▼ Resources 

☒ Specific ☐ All resources

role 

arn:aws:iam::187632318301:role/Maithelyrole [EDIT](#)  ☐ Any

[Add ARN to restrict access](#)

user 

Any resource of type = user ☒ Any

▶ Request conditions [Specify request conditions \(optional\)](#)

Now attach this policy to the new role created

## Attach policy

Attach the policy to users, groups, or roles in your account

Filter: <a href="#">Filter</a> <input type="text" value="maithely"/>		Showing 4 results
<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	alice-maithely	User
<input type="checkbox"/>	maithely.sharma@tothenew.com	User
<input type="checkbox"/>	Maithelyrole	Role
<input checked="" type="checkbox"/>	MaithelyRole1	Role

Now you can see that assume role attached

PermissionsTrust relationshipsTags (1)Access AdvisorRevoke sessions

▼ Permissions policies (2 policies applied)

Attach policies

+ Add inline policy

Policy name	Policy type	
▶  AmazonEC2FullAccess	AWS managed policy	✕
▶ assume-maithely-policy	Managed policy	✕

▶ Permissions boundary (not set)

Now create an ec2 instance and attach to the newrole created i.e Maithelyrole1

[Instances](#) > Attach/Replace IAM Role

## Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-049890fc013ae0243 (ec2-maithely-java) ⓘ

IAM role\*



[Create new IAM role](#)



\* Required

Now add the arn of new role i.e maithelyrole1 to old role i.e maithelyrole in trust relationship

## Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

### Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::187632318301:role/MaithelyRole1" ,|  
8       "Service": "ec2.amazonaws.com"  
9     },  
10    "Action": "sts:AssumeRole"  
11  }  
12 ]  
13 }
```

Now you have to ssh to the instance created and update it. Also install aws cli



```

maithely@maithely:~$ ssh -i "maithelykeypair.pem" ubuntu@ec2-52-207-215-48.compute-1.amazonaws.com
Warning: Identity file maithelykeypair.pem not accessible: No such file or directory.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Feb 28 10:51:26 UTC 2020

System load:  0.08               Processes:            86
Usage of /:   16.5% of 7.69GB    Users logged in:     0
Memory usage: 17%               IP address for eth0: 172.31.104.188
Swap usage:   0%

54 packages can be updated.
32 updates are security updates.

Last login: Fri Feb 28 06:46:24 2020 from 182.71.160.186
ubuntu@ip-172-31-104-188:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [871 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1054 kB]
Fetched 2177 kB in 1s (2789 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
51 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-104-188:~$ sudo apt install awscli
Reading package lists... Done
Building dependency tree

```

3. Block s3 access on the basis of

i. IP

Now write this in bucket policy

```

182.71.160.186maithely@maithely:~$ curl ifconfig.me
61.12.91.218maithely@maithely:~$ █

```

www.maithely-static.com

Overview	Properties	Permissions	Management	Access points
----------	------------	-------------	------------	---------------

Block public access	Access Control List	Bucket Policy	CORS configuration
---------------------	---------------------	---------------	--------------------

## Bucket policy editor ARN: arn:aws:s3::www.maithely-static.com

Type to add a new policy or edit an existing policy in the text area below.

```
1  {
2    "Version": "2012-10-17",
3    "Id": "S3PolicyId1",
4    "Statement": [
5      {
6        "Sid": "IPAllow",
7        "Effect": "Deny",
8        "Principal": "*",
9        "Action": "s3:*",
10       "Resource": "arn:aws:s3::www.maithely-static.com/*",
11       "Condition": {
12         "IpAddress": {
13           "aws:SourceIp": "61.12.91.218/32"
14         }
15       }
16     ]
17   }
18 }
```

ii. Domain

Type to add a new policy or edit an existing policy in the text area below.

### iii. Pre-signed URL(Time based)

← → ↻  s3.amazonaws.com/www.maithely-static.com/error.html?AWSAccessKeyId=AKIASXL6B65OXQFOJAKS8

4. Create RDS subnet and launch RDS instance.  
what is parameter group and option group?

- **Parameter group:** You manage your DB engine configuration by associating your **DB instances with parameter groups**. Amazon RDS defines parameter groups with default settings that apply to newly created DB instances . You can define your own parameter groups with customized settings. Then you can modify your DB instances to use your own parameter groups.

A DB parameter group acts as a container for engine configuration values that are applied to one or more DB instances.

If you create a DB instance without specifying a DB parameter group, the DB instance uses a default DB parameter group. Each default DB parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You can't modify the parameter settings of a default parameter group. Instead, you create your own parameter group where you choose your own parameter settings. Not all DB engine parameters can be changed in a parameter group that you create.

If you want to use your own parameter group, you create a new parameter group and modify the parameters that you want to. You then modify your DB instance to use the new parameter group. If you update parameters within a DB parameter group, the changes apply to all DB instances that are associated with that parameter group.

- **Option group:** Some DB engines offer additional features that make it easier to manage data and databases, and to provide additional security for your database. Amazon RDS uses option groups to enable and configure these features. An option group can specify features, called options, that are available for a particular Amazon RDS DB instance. Options can have settings that specify how the option works. When you associate a DB instance with an option group, the specified options and option settings are enabled for that DB instance.

Amazon RDS supports options for the following database engines:

Database Engine	Relevant Documentation
MariaDB	<a href="#">Options for MariaDB Database Engine</a>
Microsoft SQL Server	<a href="#">Options for the Microsoft SQL Server Database Engine</a>
MySQL	<a href="#">Options for MySQL DB Instances</a>
Oracle	<a href="#">Options for Oracle DB Instances</a>

Firstly create a subnet group under RDS service

RDS > Subnet groups > Create DB subnet group

## Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

### Subnet group details

**Name**  
You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

**Description**

**VPC**  
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

▼

## Add subnets

Add subnet(s) to this subnet group. You may add subnets one at a time below or add all the subnets related to this VPC. You may make additions/edits after this group is created. A minimum of 2 subnets is required.

Add all the subnets related to this VPC

Availability zone

us-east-1c

Subnet

subnet-05128b98c1ea54979 (192.168.192.0/18)

Add subnet

## Subnets in this subnet group (3)

Availability zone	Subnet ID	CIDR block	Action
us-east-1a	subnet-05ccb7f834d214a5a	192.168.64.0/18	<a href="#">Remove</a>
us-east-1b	subnet-02618d516e069dda9	192.168.128.0/18	<a href="#">Remove</a>
us-east-1c	subnet-05128b98c1ea54979	192.168.192.0/18	<a href="#">Remove</a>

Now create a database (My-sql)

## Create database

### Choose a database creation method [Info](#)

☒ Standard Create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ Easy Create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

### Engine options

Engine type [Info](#)

☐ Amazon Aurora



☒ MySQL



☐ MariaDB





## Settings

### DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique cross all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

### ▼ Credentials Settings

#### Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter

☐ **Auto generate a password**

Amazon RDS can generate a password for you, or you can specify your own password

#### Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

#### Confirm password [Info](#)

## DB instance size

### DB instance class [Info](#)

Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

- ☐ Standard classes (includes m classes)
- ☐ Memory Optimized classes (includes r and x classes)
- ☒ Burstable classes (includes t classes)

db.t2.micro  
1 vCPUs 1 GiB RAM Not EBS Optimized ▼

☐ Include previous generation classes

## Storage

### Storage type [Info](#)

General Purpose (SSD) ▼

### Allocated storage

20   GiB

(Minimum: 20 GiB, Maximum: 16384 GiB) Higher allocated storage **may improve** IOPS performance.



## Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

### ☒ Enable storage autoscaling

Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

### Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold



GiB

Minimum: 21 GiB, Maximum: 16384 GiB

## Availability & durability

### Multi-AZ deployment [Info](#)

- ☒ Do not create a standby instance
- ☐ Create a standby instance (recommended for production usage)  
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

## Connectivity



### Virtual Private Cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

maithely-eks-stack-VPC (vpc-01446cec73b675a0b) ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

### ▼ Additional connectivity configuration

#### Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

maithely-dbsubnetgroup ▼

#### Publicly accessible [Info](#)

☒ Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☐ No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

#### VPC security group

Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)

☒ Choose existing

Choose existing VPC security groups

☐ Create new

Create new VPC security group

#### Existing VPC security groups

Choose VPC security groups ▼

maithely-eks-stack-ControlPlaneSecurityGroup-12OKBW6DIGY67 ✕

default ✕

#### Availability zone [Info](#)

No preference ▼

#### Database port [Info](#)

TCP/IP port the database will use for application connections.

3306

## Database authentication

Database authentication options [Info](#)

- ☒ **Password authentication**  
Authenticates using database passwords.
- ☐ **Password and IAM database authentication**  
Authenticates using the database password and user credentials through AWS IAM users and roles.

## ► Additional configuration

Database options, backup enabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

## Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

5. ACL, Bucket policy, IAM Policy.

**Amazon S3 access control lists (ACLs)** enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions.

When you create a bucket or an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.

A grantee can be an AWS account or one of the predefined Amazon S3 groups. You grant permission to an AWS account using the email address or the canonical user ID.

**IAM policies** specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance\_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or

roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your AWS environment.

**S3 bucket policies**, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket). S3 bucket policies are a type of access control list, or ACL (here I mean "ACL" in the generic sense, not to be confused with S3 ACLs, which is a separate S3 feature discussed later in this post).

6. Mount S3 to an EC2 instance.

```
ubuntu@ip-172-31-61-252:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [872 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [303 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [32.9 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en [8468 B]
```



```
ubuntu@ip-172-31-61-252:~$ sudo apt-get install automake autotools-dev fuse g++ git libcurl4-gnutls-dev libfuse-dev libssl-dev libxml2-dev make pkg-config
Reading package lists... Done
Building dependency tree
Reading state information... Done
fuse is already the newest version (2.9.7-1ubuntu1).
fuse set to manually installed.
git is already the newest version (1:2.17.1-1ubuntu0.5).
git set to manually installed.
The following additional packages will be installed:
  autoconf binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-7 dpkg-dev fakeroot g++-7 gcc gcc-7 gcc-7-base gcc-8-base gir1.2-harfbuzz-0.0 icu-devtools libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan4 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcilkrts5 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-7-dev libgcc1 libglib2.0-bin libglib2.0-dev libglib2.0-dev-bin libgomp1 libgraphite2-3 libgraphite2-dev libharfbuzz-dev
```

```
ubuntu@ip-172-31-61-252:~$ git clone https://github.com/s3fs-fuse/s3fs-fuse.git
Cloning into 's3fs-fuse'...
remote: Enumerating objects: 5879, done.
remote: Total 5879 (delta 0), reused 0 (delta 0), pack-reused 5879
Receiving objects: 100% (5879/5879), 3.46 MiB | 24.13 MiB/s, done.
Resolving deltas: 100% (4079/4079), done.
```

```

ubuntu@ip-172-31-61-252:~$ cd s3fs-fuse
ubuntu@ip-172-31-61-252:~/s3fs-fuse$ ./autogen.sh
--- Make commit hash file -----
--- Finished commit hash file ---
--- Start autotools -----
--- Finished autotools -----
ubuntu@ip-172-31-61-252:~/s3fs-fuse$ ./configure --prefix=/usr
--with-openssl
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking target system type... x86_64-pc-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for g++... g++

```

```

ubuntu@ip-172-31-61-252:~/s3fs-fuse$ make
make all-recursive
make[1]: Entering directory '/home/ubuntu/s3fs-fuse'
Making all in src
make[2]: Entering directory '/home/ubuntu/s3fs-fuse/src'
g++ -DHAVE_CONFIG_H -I. -I.. -D_FILE_OFFSET_BITS=64 -I/usr/include/fuse -I/usr/include/x86_64-linux-gnu -I/usr/include/libxml2 -g -O2 -Wall -D_FILE_OFFSET_BITS=64 -D_FORTIFY_SOURCE=2 -MT s3fs.o -MD -MP -MF .deps/s3fs.Tpo -c -o s3fs.o s3fs.cpp
mv -f .deps/s3fs.Tpo .deps/s3fs.Po
g++ -DHAVE_CONFIG_H -I. -I.. -D_FILE_OFFSET_BITS=64 -I/usr/include/fuse -I/usr/include/x86_64-linux-gnu -I/usr/include/libxml2 -g -O2 -Wall -D_FILE_OFFSET_BITS=64 -D_FORTIFY_SOURCE=2 -MT curl.o -MD -MP -MF .deps/curl.Tpo -c -o curl.o curl.cpp
mv -f .deps/curl.Tpo .deps/curl.Po
g++ -DHAVE_CONFIG_H -I. -I.. -D_FILE_OFFSET_BITS=64 -I/usr/include/fuse -I/usr/include/x86_64-linux-gnu -I/usr/include/libxml2 -g -O2 -Wall -D_FILE_OFFSET_BITS=64 -D_FORTIFY_SOURCE=2 -MT

```



```
ubuntu@ip-172-31-61-252:~/s3fs-fuse$ sudo make install
Making install in src
make[1]: Entering directory '/home/ubuntu/s3fs-fuse/src'
make[2]: Entering directory '/home/ubuntu/s3fs-fuse/src'
/bin/mkdir -p '/usr/bin'
/usr/bin/install -c s3fs '/usr/bin'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ubuntu/s3fs-fuse/src'
make[1]: Leaving directory '/home/ubuntu/s3fs-fuse/src'
Making install in test
make[1]: Entering directory '/home/ubuntu/s3fs-fuse/test'
make[2]: Entering directory '/home/ubuntu/s3fs-fuse/test'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ubuntu/s3fs-fuse/test'
make[1]: Leaving directory '/home/ubuntu/s3fs-fuse/test'
Making install in doc
make[1]: Entering directory '/home/ubuntu/s3fs-fuse/doc'
```

Now for credential purposes install and configure awscli

```
ubuntu@ip-172-31-61-252:~$ sudo apt install awscli
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docutils-common libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2
  libpaper-utils libpaper1 libtiff5 libwebp6 libwebpdemux2
  libwebpmux3 python3-boto3 python3-dateutil
  python3-docutils python3-jmespath python3-olefile
  python3-pil python3-pygments python3-roman python3-rsa
  python3-s3transfer sgml-base xml-core
Suggested packages:
  liblcms2-utils docutils-doc fonts-linuxlibertine
  | ttf-linux-libertine texlive-lang-french
  texlive-latex-base texlive-latex-recommended python-pil-doc
  python3-pil-dbg ttf-bitstream-vera sgml-base-doc debhelper
```

```
ubuntu@ip-172-31-61-252:~$ aws configure
AWS Access Key ID [None]: AKIASXL6B650XQFOJAKS
AWS Secret Access Key [None]: wDZf2P6wG5u735RLIcIbpWPioCz40KhsrBisy8XW
Default region name [None]:
Default output format [None]:
```

Create a new file in /etc with the name passwd-s3fs and Paste the access key and secret key in the below format .

```
ubuntu@ip-172-31-61-252:~$ sudo touch /etc/passwd-s3fs
ubuntu@ip-172-31-61-252:~$ sudo vim /etc/passwd-s3fs
ubuntu@ip-172-31-61-252:~$ sudo chmod 640 /etc/passwd-s3fs
```

Syntax

Your\_accesskey:Your\_secretkeycar

```
ubuntu@ip-172-31-61-252:/mybucket$ sudo cat /etc/passwd-s3fs
AKIASXL6B650XQFOJAKS:wDZf2P6wG5u735RLIcIbpWPioCz40KhsrBisy8XW
ubuntu@ip-172-31-61-252:/mybucket$
```

Now create a directory or provide the path of an existing directory and mount S3bucket in it.

```
ubuntu@ip-172-31-61-252:~$ mkdir /mybucket
mkdir: cannot create directory '/mybucket': Permission denied
ubuntu@ip-172-31-61-252:~$ sudo !!
sudo mkdir /mybucket
```

```
ubuntu@ip-172-31-61-252:~$ s3fs maithelybucket -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mybucket
s3fs: MOUNTPPOINT: /mybucket permission denied.
ubuntu@ip-172-31-61-252:~$ sudo !!
sudo s3fs maithelybucket -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mybucket
ubuntu@ip-172-31-61-252:~$ which s3fs
/usr/bin/s3fs
```



```

ubuntu@ip-172-31-61-252:~$ which s3fs
/usr/bin/s3fs
ubuntu@ip-172-31-61-252:~$ sudo vim /etc/rc.local

ubuntu@ip-172-31-61-252:/mybucket$ cat /etc/rc.local
/usr/local/bin/s3fs maithelybucket -o use_cache=/tmp -o allow_o
ther -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mybucket

ubuntu@ip-172-31-61-252:/mybucket$ █

```

Check mounted s3 bucket

```

ubuntu@ip-172-31-61-252:~$ df -Th /mybucket
Filesystem      Type      Size  Used Avail Use% Mounted on
s3fs             fuse.s3fs 256T    0  256T   0% /mybucket

```

If it shows the mounted file system, you have successfully mounted the S3 bucket on your EC2 Instance. You can also test it further by creating a test file.

```

ubuntu@ip-172-31-61-252:/mybucket$ sudo vim test.txt
ubuntu@ip-172-31-61-252:/mybucket$ cat test.txt
this is a test file to check s3fs

```

You can see test.txt has been created in the bucket

Amazon S3 > maithelybucket

maithelybucket

Overview Properties Permissions Management Access points

🔍 Type a prefix and press Enter to search. Press ESC to clear.

📁 Upload + Create folder Download Actions ▾

US East (N. Virginia) 🔁

Viewing 1 to 1

<input type="checkbox"/> Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/> 📄 test.txt	Mar 12, 2020 5:14:52 PM GMT+0530	34.0 B	Standard

Viewing 1 to 1


## 7. Change content type using s3

Add an object to the bucket

Amazon S3 > maithelybucket

### maithelybucket

**Overview** Properties Permissions Management Access points



 Type a prefix and press Enter to search. Press ESC to clear.

Upload

Create folder

Download

Actions ▾

<input type="checkbox"/>	Name ▾	Last modified ▾
<input checked="" type="checkbox"/>	 View_Print Submitted Form.pdf	Mar 13, 2020 12:25
<input type="checkbox"/>	 test.txt	Mar 12, 2020 6:01:

Now click on the object and access the object url

View\_Print Submitted Form.pdf

Latest version ▾

Overview

Properties

Permissions

Select from

Open

Download

Download as

Make public

Copy path

Owner

nitin.bhadauria

Last modified

Mar 13, 2020 12:25:24 PM GMT+0530

Etag

19cca41b3ff22345ade5e44032a1dcee

Storage class

Standard

Server-side encryption

None

Size

60.5 KB

Key

View\_Print Submitted Form.pdf

Object URL

[https://maithelybucket.s3.amazonaws.com/View\\_Print+Submitted+Form.pdf](https://maithelybucket.s3.amazonaws.com/View_Print+Submitted+Form.pdf)

For rendering on the browser:

Go in properties and choose metadata where you have content-type as application/pdf

Amazon S3 > maithelybucket > View\_Print Submitted Form.pdf

View\_Print Submitted Form.pdf [Latest version](#) ▾

Overview Properties Permissions Select from

### Storage class

Use the most appropriate storage class based on frequency of access.

[Learn more](#)

☒ Standard

### Encryption

Use encryption to protect your data while in-transit and at rest.

[Learn more](#)

☐ None

### Metadata

[+ Add Metadata](#) [Delete](#) [Edit](#) [i](#)

Key	Value
<input type="radio"/> Content-Type	application/pdf

[Cancel](#) [Save](#)

Here you can see the file

S3 Management Console X View\_Print+Submitted+Form X IAM Management Console X

← → ↺ 🏠 [https://maithelybucket.s3.amazonaws.com/View\\_Print](https://maithelybucket.s3.amazonaws.com/View_Print)

1 of 2 - + Automate

13/02/2020

View/Pri

File Number (For Office

--	--	--	--	--

GOVERNMENT OF INDIA, MI

PASSPORT AF

For downloading :

Go in properties and choose metadata where you have content-type as application/pdfContent

Amazon S3 > malthelybucket > View\_Print Submitted Form.pdf

View\_Print Submitted Form.pdf [Latest version](#) ▼

**Overview** Properties Permissions Select from

**Storage class**

Use the most appropriate storage class based on frequency of access.

[Learn more](#)

☒ Standard

**Encryption**

Use encryption to protect your data while in-transit and at rest.

[Learn more](#)

☐ None

**Metadata** ✕

[+ Add Metadata](#) [Delete](#) [Edit](#) ⓘ

Key	Value
<input type="radio"/> Content-Type	application/pdfContent


[Cancel](#) [Save](#)

Here the file gets downloaded

Problem loading page ✕ Downloads ✕ +

Firefox | about:downloads

Firefox Home Page

 View\_Print+Submitted+Form.pdf  
60.5 KB — amazon.com — 12:33 pm

8. Retrieve previous version of S3(enable versioning).

Amazon S3 > maithelybucket

## maithelybucket

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#)

### Versioning

☒ Enable versioning

☐ Suspend versioning

This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enabled

[Cancel](#) [Save](#)

### Server access logging







Set up access log records that provide details about access requests.

[Learn more](#)

☐ Disabled

Upload the same file and you could see the versions

## View\_Print Submitted Form.pdf [Latest version ▾](#)

	Mar 13, 2020 12:39:40 PM GMT+0530 (Latest version)	Standard		
	Mar 13, 2020 12:32:43 PM GMT+0530	Standard		

**Owner**

nitin.bhadauria

**Last modified**

Mar 13, 2020 12:39:40 PM GMT+0530

**Etag**

19cca41b3ff22345ade5e44032a1dcee

**Storage class**

Standard

**Server-side encryption**

None

**Size**

60.5 KB

### 9. S3 VPC endpoint.

Create a VPC with subnets.

From the navigation pane, choose endpoints, then create endpoints.

aws

Services ▾

Resource Groups ▾

🔔

maithely.sharma@tothenew.co... ▾

Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Create Endpoint

Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name ▾	Endpoint ID ▴	VPC ID	Service name
<input type="checkbox"/>		vpce-0326435ae0...	vpc-0faa7c85885...	com.amazonaws.us-east-1
<input type="checkbox"/>		vpce-084d36ce5df...	vpc-d38d68b7   d...	com.amazonaws.us-east-1
<input type="checkbox"/>		vpce-0992a50134...	vpc-d38d68b7   d...	com.amazonaws.us-east-1

## Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.

An interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.

A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

- Service category
- ☒ AWS services

☐ Find service by name

☐ Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3 ⓘ

search : s3

Add filter

	Service Name	Owner	Type
<input checked="" type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Gateway



VPC\* vpc-0847695ca84e79af3  

**Configure route tables** A rule with destination **pl-63a5400a (com.amazonaws.us-east-1.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

rtb-0ec3f8525a87f4860 rtb-02f1a06d9ef24a280

	Route Table ID	Main	Associated With
<input checked="" type="checkbox"/>	rtb-0ec3f8525a87f4860	No	3 subnets
<input checked="" type="checkbox"/>	rtb-02f1a06d9ef24a280	Yes	subnet-0e85ed72871e50725   kaushu_tag



#### Warning


When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

**Policy\*** ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Key	Value
(128 characters maximum)	(256 characters maximum)
owner	maithely 

## Create Endpoint

✓ The following VPC Endpoint was created:

VPC Endpoint ID [vpce-0b771d8c1bc8c5e76](#)

[Close](#)

You can see in route table of that subnet that endpoint has been added to it

[Create route table](#) [Actions](#)

search : 084 [Add filter](#)

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC
<input checked="" type="checkbox"/>		rtb-02f1a06d9ef24a280	-	-	Yes	<a href="#">vpce-0b771d8c1bc8c5e76</a>
<input type="checkbox"/>	sarthak-pub	rtb-0ec3f8525a87f4860	<a href="#">3 subnets</a>	-	No	<a href="#">vpce-0b771d8c1bc8c5e76</a>
<input type="checkbox"/>	default	rtb-2cc30148	-	-	Yes	<a href="#">vpce-0b771d8c1bc8c5e76</a>

Route Table: [rtb-02f1a06d9ef24a280](#)

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

[Edit routes](#)

View [All routes](#)

Destination	Target	Status	Propagate
10.0.0.0/16	local	active	No
<a href="#">pl-63a5400a (com.amazonaws.us-east-1.s3, 54.231.0.0/17, 52.216.0.0/15, 3.5.16.0/21, 3.5.0.0/20)</a>	<a href="#">vpce-0b771d8c1bc8c5e76</a>	active	No

Then Generate a policy and add it to the bucket policy.

- Add Bucket ARN
- Add conditions: StringEquals
- Add VPCE ID



## 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 VPC Endpoint 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 -- Select Actions -- ▾ ☒ All Actions (\*\*)  
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:::<bucket\_name>/<key\_name>.  
Use a comma to separate multiple values.

#### Add Conditions (Optional)

[Hide](#)

Conditions are any restrictions or details about the statement. ([More Details](#)).

Condition StringEquals ▾

Key aws:SourceVpce ▾

Value

Add Condition

Add Statement No Action selected. You must select at least one Action

Copy the policy

ARN should follow the following format: arn:aws:s3::<bucket\_name>/<key\_name>. Use a comma to separate multiple values.


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": "Policy1584084413527",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1584084411749",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::maithelybucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "vpce-0b771d8c1bc8c5e76"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Close

© 2020, Amazon Web Services LLC or its affiliates. All rights reserved.

An  amazon.com company

Paste to bucket policy

Overview	Properties	Permissions	Management	Access points
----------	------------	-------------	------------	---------------

Block public access

Access Control List

Bucket Policy

CORS configuration

## Bucket policy editor ARN: arn:aws:s3:::maithelybucket

Type to add a new policy or edit an existing policy in the text area below.

```

1  {
2    "Id": "Policy1584084413527",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmnt1584084411749",
7        "Action": "s3:*",
8        "Effect": "Allow",
9        "Resource": "arn:aws:s3:::maithelybucket",
10       "Condition": {
11         "StringEquals": {
12           "aws:SourceVpce": "vpce-0b771d8c1bc8c5e76"
13         }
14       },
15       "Principal": "*"
16     }
17   ]
18 }
```

10. CORS, Enable CORS for 2 specific website.

# maithelybucket

Overview

Properties

Permissions

Management

Access points

Block public access

Access Control List

Bucket Policy

CORS configuration

## CORS configuration editor ARN: arn:aws:s3:::maithelybucket

Add a new cors configuration or edit an existing one in the text area below.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
3 <CORSRule>
4   <AllowedOrigin>https://www.facebook.com/*</AllowedOrigin>
5   <AllowedOrigin>https://s3.console.aws.amazon.com/*</AllowedOrigin>
6   <AllowedMethod>GET</AllowedMethod>
7   <AllowedMethod>POST</AllowedMethod>
8   <AllowedMethod>PUT</AllowedMethod>
9   <MaxAgeSeconds>3000</MaxAgeSeconds>
10  <AllowedHeader>Authorization</AllowedHeader>
11 </CORSRule>
12 </CORSConfiguration>
13
14
```

# maithelybucket

Overview

Properties

Permissions

Management

Access points

🔍 Type a prefix and press Enter to search. Press ESC to clear.

📁 Upload

➕ Create folder

⬇️ Download

⋮ Actions

Versions

Hide

Show

<input type="checkbox"/>	Name ▼	Last modified ▼	Size ▼
<input checked="" type="checkbox"/>	📄 Untitled document.pdf	Mar 13, 2020 4:58:58 PM GMT+0530	9.7 KB
<input type="checkbox"/>	📄 test.txt	Mar 13, 2020 1:24:37 PM GMT+0530	34.0 B

We are able to view this document because we have added “amazon console link”

