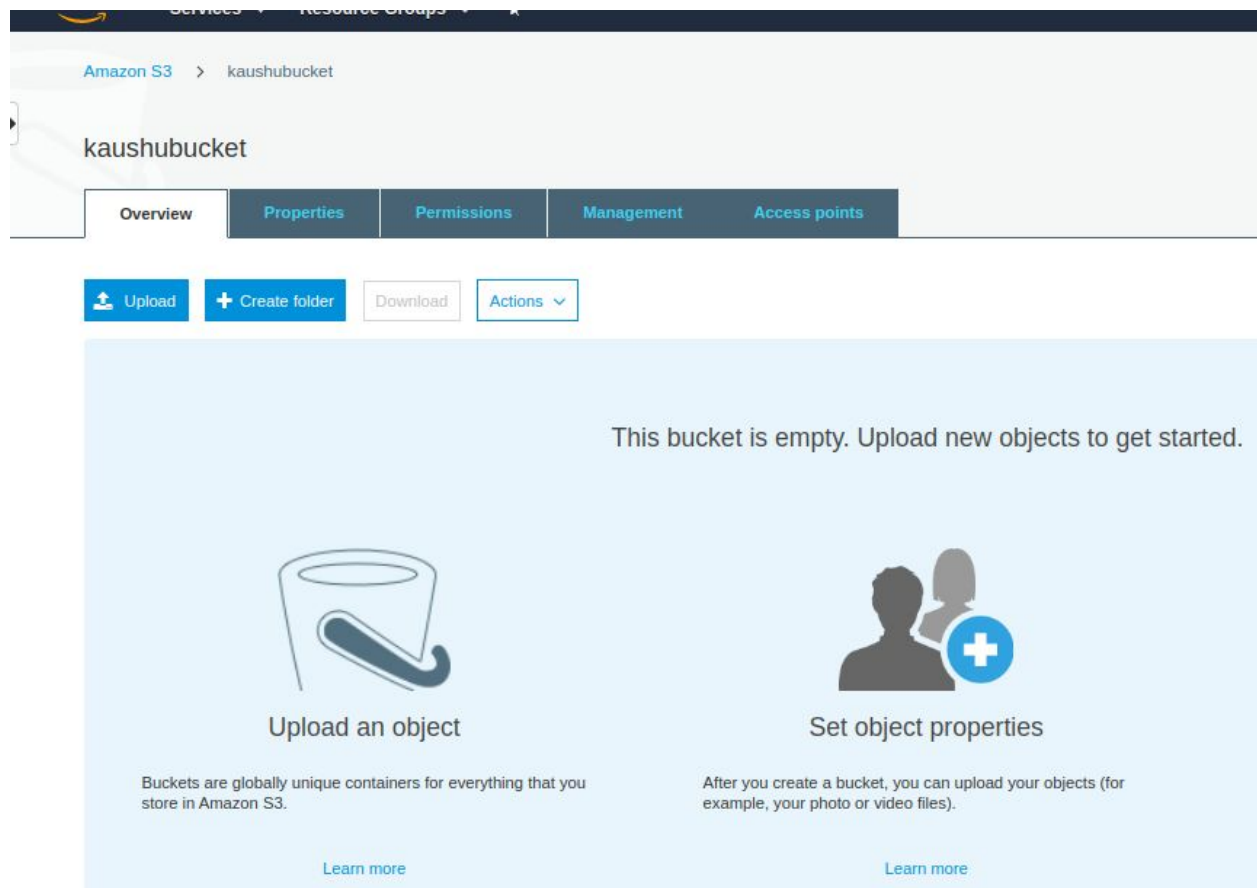


# Simple Storage Service (S3)

Ques 1. static website hosting using S3 (index page, error page)

Ans 1.

Created a bucket in S3



Hosting a static website

Static website hosting

Endpoint : <http://kaushubucket.s3-website-us-east-1.amazonaws.com>

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

Index document [i](#)

ABC.html

Error document [i](#)

error.html

Redirection rules (optional) [i](#)

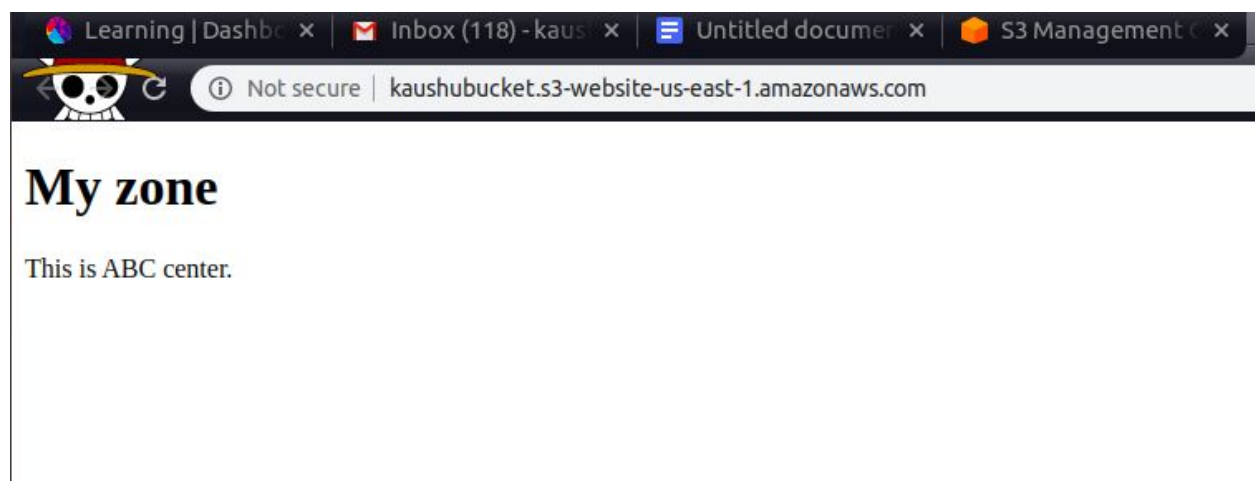
☐ Redirect requests [Learn more](#)

☐ Disable website hosting

☒ Bucket hosting

Cancel Save

Open the website with the help of end points



Ques 3. . Block s3 access on the basis of

- i. IP
- ii. Domain
- iii. Pre-signed URL(Time based)

Ans 3. Blocking Through ip address

Created a bucket in s3

kaushubucket

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 1

<input type="checkbox"/>	Name	Last modified	Size	Storage class
<input type="checkbox"/>	ABC.html	Feb 27, 2020 11:04:34 PM GMT+0530	94.0 B	Standard

Viewing 1 to 1

Make the bucket public

Block public access Access Control List Bucket Policy CORS configuration

Access for bucket owner

Canonical ID	List objects	Write objects	Read bucket permission
<input type="radio"/> 4f6f72a1d4176339c60d24e8501968fe657e02203bef23a5c2e9b46ffff53217 (Your AWS account)	Yes	Yes	Yes

Access for other AWS accounts

+ Add account Delete

Canonical ID	List objects	Write objects	Read bucket permission
--------------	--------------	---------------	------------------------

Public access

Group	List objects	Write objects	Read bucket permission
<input type="radio"/> Everyone	Yes	Yes	-

Created a policy to block the S3 for particular ips

Amazon S3 > kaushubucket

## kaushubucket

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

[Block public access](#)[Access Control List](#)[Bucket Policy](#)[CORS configuration](#)

**Bucket policy editor** ARN: arn:aws:s3:::kaushubucket  
Type to add a new policy or edit an existing policy in the text area below.

```
1 {
2   "Version": "2012-10-17",
3   "Id": "VPCE and SourceIP",
4   "Statement": [
5     {
6       "Sid": "VPCE and SourceIP",
7       "Effect": "Deny",
8       "Principal": "*",
9       "Action": "s3:*",
10      "Resource": [
11        "arn:aws:s3:::kaushubucket",
12        "arn:aws:s3:::kaushubucket/*"
13      ],
14      "Condition": {
15        "NotIpAddress": {
16          "aws:SourceIp": "61.12.91.218"
17        }
18      }
19    }
20  ]
21 }
```

Open the bucket with allowed ip

S3 Management x kaushubucket x kaushubucket x

Not secure | kaushubucket.s3-website-us-east-1.amazonaws.com

## My zone

This is ABC center.

## Access denied while opening the S3 with blocked ips



## Blocking Through domain

```
1 {  
2   "Version": "2012-10-17",  
3   "Id": "VPCE and domain",  
4   "Statement": [  
5     {  
6       "Sid": "VPCE and domain",  
7       "Effect": "Deny",  
8       "Principal": "*",  
9       "Action": "s3:*",  
10      "Resource": [  
11        "arn:aws:s3::kaushudomain",  
12        "arn:aws:s3::kaushudomain/*"  
13      ],  
14      "Condition": {  
15        "Notdomain": {  
16          "aws:SourceIp": "www.example.com"  
17        }  
18      }  
19    }  
20  ]  
21 }
```

## Blocked through presigned url

## Created a bucket and it is private

kaushudomain

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) 🔄

<input type="checkbox"/>	Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/>	📄 version.html	Feb 28, 2020 4:57:10 PM GMT+0530	95.0 B	Standard

Viewing 1 to 1

Viewing 1 to 1

Firstly i created the IAM group

## Add user

1 2 3 4 5

### Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://ttn-newers.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✓ s3_kaushu_presigned	AKIASXL6B65O32XGBGGK	2txkcoa5E+bxJrBvNUIhS1Xd68TGyfA0Bg5N/Qd1 <a href="#">Hide</a>

Give all the S3 permission to the user

User ARN `arn:aws:iam::187632318301:user/s3_kaushu_presigned` ⓘ

Path `/`

Creation time 2020-02-28 20:19 UTC+0530

Permissions Groups (1) Tags (1) Security credentials Access Advisor

▼ Permissions policies (1 policy applied)

[Add permissions](#) [Add inline policy](#)

Policy name ▼	Policy type ▼		
Attached from group			
▼  AmazonS3FullAccess	AWS managed policy from group s3_kaushu_gp ✕		
Policy summary <a href="#">{ } JSON</a>	<a href="#">Simulate policy</a>		
<input type="text" value="Filter"/>			
Service ▼	Access level	Resource	Request condition
Allow (1 of 223 services) <a href="#">Show remaining 222</a>			
S3	Full access	All resources	None

▼ Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions this user can have. This is not a common setting but can be used to delegate permission management to others. [Learn more](#)

[Set boundary](#)

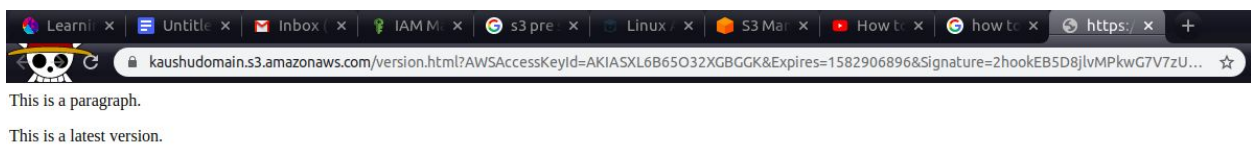
Set the policy for user



Then open the instance in ec2 and generate the presigned url using the below commands

```
ubuntu@ip-10-0-7-222:~$ aws configure
AWS Access Key ID [None]: AKIASXL6B65032XGBGGK
AWS Secret Access Key [None]: 2txkcoa5E+bxJrBvNUIhS1Xd68TGyfA0Bg5N/Qd1
Default region name [None]:
Default output format [None]:
ubuntu@ip-10-0-7-222:~$ aws s3 presign s3://kaushudomain/version.html
https://kaushudomain.s3.amazonaws.com/version.html?AWSAccessKeyId=AKIASXL6B65032XGBGGK&Expires=1582906896&Signature=2hookEB5D8jlvMPkwG7V7zU1Li0%3D
ubuntu@ip-10-0-7-222:~$
```

After that access the bucket using pre signed url



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

Ans4. Firstly i created the RDS subnet



RDS > Subnet groups > kaushu\_rds

## kaushu\_rds

### Subnet group details

VPC ID  
t34ak (vpc-01d9bca1ea53fdce9)

ARN  
arn:aws:rds:us-east-1:187632318301:subgrp:kaushu\_rds

Description  
rds

### Subnets (9)

Availability zone	Subnet ID	CIDR block
us-east-1f	subnet-0dba4ee75a08a389d	10.0.48.0/20
us-east-1a	subnet-07c3a2631f7eb2d6f	10.0.194.0/24
us-east-1b	subnet-062a1eaac2376ac86	10.0.0.0/20
us-east-1c	subnet-0a976bd6d97e7ce2a	10.0.193.0/24

Then i created a mysql database

✔ Successfully created database **kaushumysql**.  
We have generated your database master password during the database creation and will be displayed in the connection details. This is the only time you will be able to view this password. However you can modify your database to create a new password at any time. [View credential details](#)

RDS > Databases

### Databases

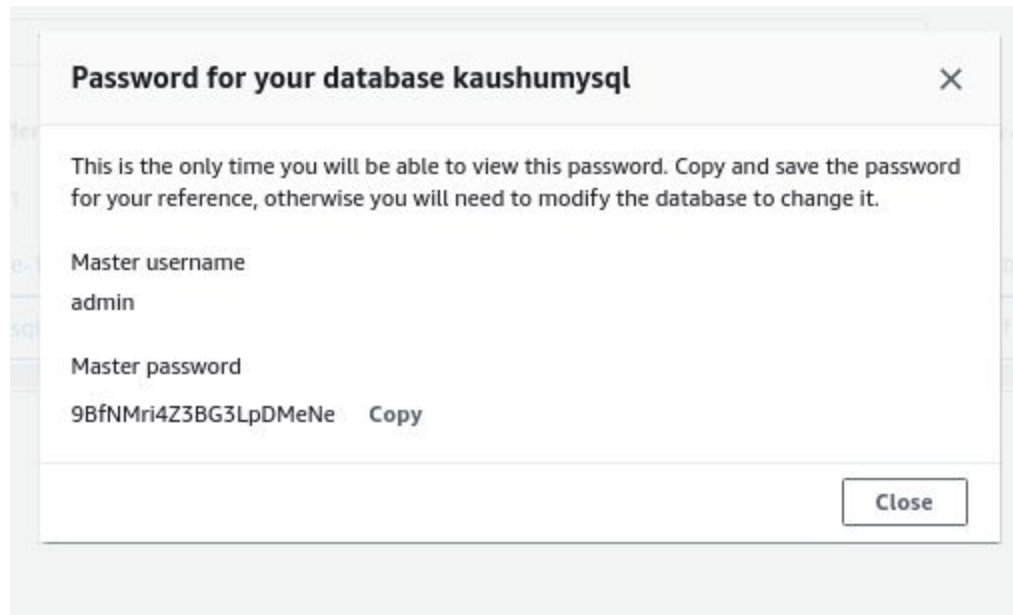
☒ Group resources

Filter databases

	DB Identifier	Role	Engine	Region & AZ	Size	Status	CPU
	database-1	Regional	Aurora MySQL	us-east-1	1 instance	Available	-
	database-1-instance-1-us-east-1b	Writer	Aurora MySQL	us-east-1b	db.r5.large	Available	3.00%
<input checked="" type="radio"/>	kaushumysql	Instance	MySQL Community	us-east-1f	db.m5.xlarge	Available	-

Database auto generated password given below





Finally database configured

RDS > Databases > kaushumysql

### kaushumysql

[Modify](#) [Actions](#)

#### Summary

DB identifier kaushumysql	CPU <div><div></div></div> 0.00%	Info Available	Class db.m5.xlarge
Role Instance	Current activity	Engine MySQL Community	Region & AZ us-east-1f

[Connectivity & security](#) | [Monitoring](#) | [Logs & events](#) | [Configuration](#) | [Maintenance & backups](#) | [Tags](#)

#### Connectivity & security

<b>Endpoint &amp; port</b> Endpoint kaushumysql.cxy9qkbqhfr.us-east-1.rds.amazonaws.com  Port 3306	<b>Networking</b> Availability zone us-east-1f  VPC t34ak (vpc-01d9bca1ea53fdce9)  Subnet group kaushu_rds	<b>Security</b> VPC security groups default (sg-04e00317065cc6d51) (active) asg1 (sg-0940bc8edcde0289a) (active)  Public accessibility No
---	--	---

what is parameter group and option group

## option group-

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. ... When you associate a DB instance with an option group, the specified options and option settings are enabled for that DB instance.

## Parameter group-

DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances. A default DB parameter group is created if you make a database instance without specifying a custom DB parameter group.

## Ques 5. ACL, Bucket policy, IAM Policy.

Ans 5. Use IAM policies if:

- You need to control access to AWS services other than S3. IAM policies will be easier to manage since you can centrally manage all of your permissions in IAM, instead of spreading them between IAM and S3.
- You have numerous S3 buckets each with different permissions requirements. IAM policies will be easier to manage since you don't have to define a large number of S3 bucket policies and can instead rely on fewer, more detailed IAM policies.
- You prefer to keep access control policies in the IAM environment.

Use S3 bucket policies if:

- You want a simple way to grant cross-account access to your S3 environment, without using IAM roles.
- Your IAM policies bump up against the size limit (up to 2 kb for users, 5 kb for groups, and 10 kb for roles). S3 supports bucket policies of up to 20 kb.

- You prefer to keep access control policies in the S3 environment.

Use S3 bucket policies if:

As a general rule, AWS recommends using S3 bucket policies or IAM policies for access control. S3 ACLs is a legacy access control mechanism that predates IAM. However, if you already use S3 ACLs and you find them sufficient, there is no need to change.

An S3 ACL is a sub-resource that's attached to every S3 bucket and object. It defines which AWS accounts or groups are granted access and the type of access. When you create a bucket or an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.

## Ques 5. Mount S3 to an EC2 instance

## Ans 5. First created a instance in ec2

<input checked="" type="checkbox"/>	kaushu mount	i-081bc8fd5b6c829d4	t2.micro	us-east-1b	running	2/2 checks ...	None		3.222
<input type="checkbox"/>	for lb2	i-0c45329b1534b24b9	t2.micro	us-east-1b	running	2/2 checks ...	None		3.215
<input type="checkbox"/>	kaushu wp	i-08bb2342cddb292c0	t2.micro	us-east-1b	stopped		None		-

Instance: <b>i-081bc8fd5b6c829d4 (kaushu mount)</b> Public IP: 3.222.188.247	
Description	Status Checks Monitoring Tags
Instance ID	i-081bc8fd5b6c829d4
Instance state	running
Instance type	t2.micro
Finding	You may not have permission to access AWS Compute Optimizer.
Private DNS	ip-10-0-7-222.ec2.internal
Private IPs	10.0.7.222
Secondary private IPs	
VPC ID	vpc-01d9bca1ea53fdce9 (t34ak)
Public DNS (IPv4)	-
IPv4 Public IP	3.222.188.247
IPv6 IPs	-
Elastic IPs	
Availability zone	us-east-1b
Security groups	launch-wizard-190. <a href="#">view inbound rules.</a> <a href="#">view outbound rules</a>
Scheduled events	No scheduled events
AMI ID	ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20200129 (ami-08bc77a2c7eb2b1da)

Then run the following below commands to install the repositories and packages

```

ubuntu@tp-10-0-7-222:~/s3fs-fuse$ history
1 sudo apt-get update
2 sudo apt-get install automake fuse fuse-devel gcc-c++ git libcurl-devel libxml2-devel make openssl-devel
3 sudo apt-get install automake autotools-dev fuse g++ git libcurl4-gnutls-dev libfuse-dev libssl-dev libxml2-dev make pkg-config
4 clear
5 sudo apt-get update
6 sudo apt-get install automake autotools-dev fuse g++ git libcurl4-gnutls-dev libfuse-dev libssl-dev libxml2-dev make pkg-config
7 exit
8 sudo apt-get install -y automake autotools-dev fuse g++ git libcurl4-gnutls-dev libfuse-dev libssl-dev libxml2-dev make pkg-config
9 git clone https://github.com/s3fs-fuse/s3fs-fuse.git
10 cd s3fs-fuse
11 ./autogen.sh
12 ./configure --prefix=/usr --with-openssl
13 make
14 sudo make install
15 which s3fs
16 touch /etc/passwd-s3fs

```

Then create the key pairs to access the s3 bucket

User ARN

arn:aws:iam::187632318301:user/kaushlendra.singh@tothenew.com

Path

/

Creation time

2020-02-19 16:33 UTC+0530

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Sign-in credentials

Summary

Console sign-in link

https://ttn-newers.signin.aws.amazon.com/console

Console password

Enabled (last signed in Today) | [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 protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
AKIASXL6B6SOSWI6KQ62	2020-02-28 11:28 UTC+0530	N/A	Active   <a href="#">Make inactive</a> <a href="#">✕</a>

After that run some following below commands

```

17 sudo touch /etc/passwd-s3fs
18 sudo vim /etc/passwd-s3fs
19 sudo chmod 640 /etc/passwd-s3fs
20 sudo vim /etc/passwd-s3fs
21 cd ..
22 cd /etc
23 sudo su
24 cd ~
25 sudo vi /etc/hosts
26 cd /usr/bin/s3fs
27 cd /usr/bin/s3fs
28 cd s3fs-fuse
29 sudo vim /etc/passwd-s3fs
30 sudo chmod 640 /etc/passwd-s3fs
31 mkdir /mys3bucket
32 sudo mkdir /mys3bucket
33 ls
34 sudo mkdir mys3bucket
35 ls
36 s3fs your_bucketname -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket
37 s3fs kaushubucket -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket
38 sudo s3fs kaushubucket -o use_cache=/tmp -o allow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket
39 which s3fs
40 cd /usr/local/bin
41 ls
42 cd /usr/local/bin/s3fs
43 sudo nano /etc/rc.local
44 which s3fs
45 cd s3fs-fuse
46 cd ~
47 cd s3fs-fuse
48 df -TH
49 df -TH /mys3bucket/

```

## Check mounted s3 bucket

```

ubuntu@ip-10-0-7-222:~/s3fs-fuse$ df -TH /mys3bucket/
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/xvda1      ext4  8.3G  1.7G  6.6G  20% /
ubuntu@ip-10-0-7-222:~/s3fs-fuse$

```

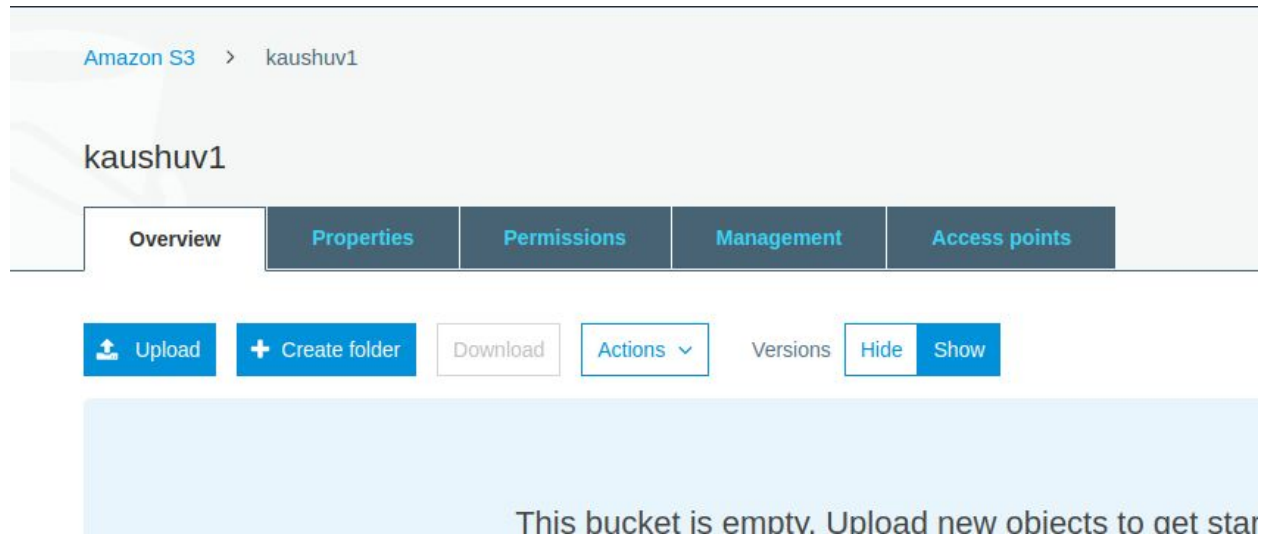
Ques 6. Change content type using s3.

Ans 6.

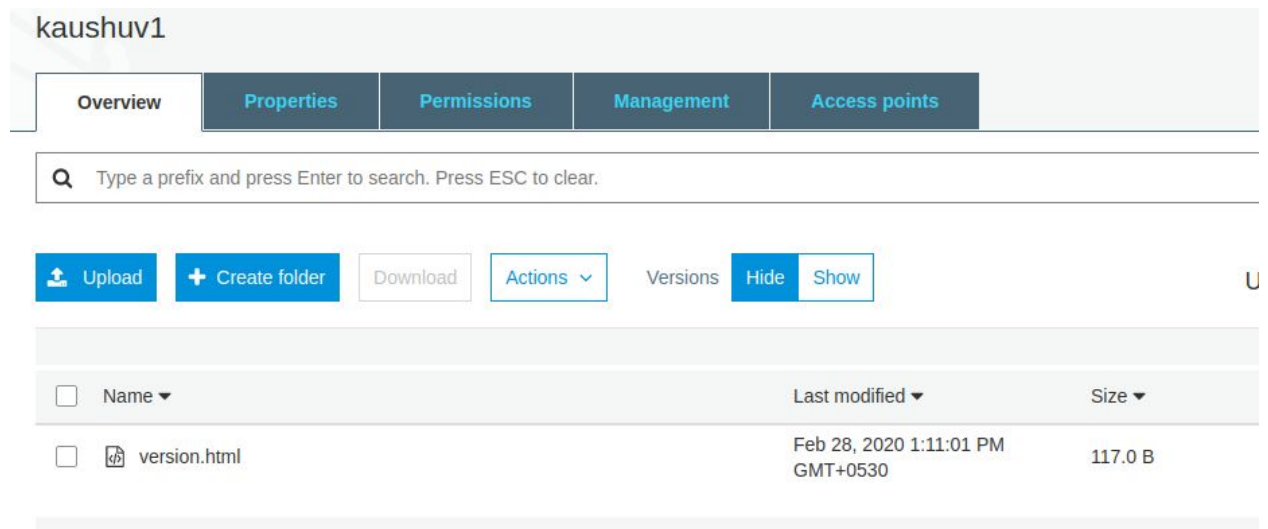
Ques 7. Retrieve previous version of S3(enable versioning).

Ans 7.

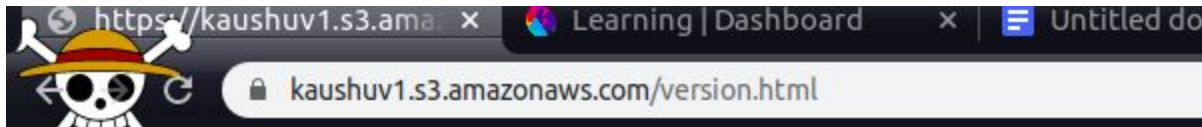
Created a new bucket and enabled the versioning



After that uploaded the html page in bucket



After this open the uploaded page in browser



This is a paragraph.

This is a paragraph.

This is a paragraph.

Then edit the html page and upload in the bucket

Versioning created as latest version

kaushuv1

Overview Properties Permissions Management Access points

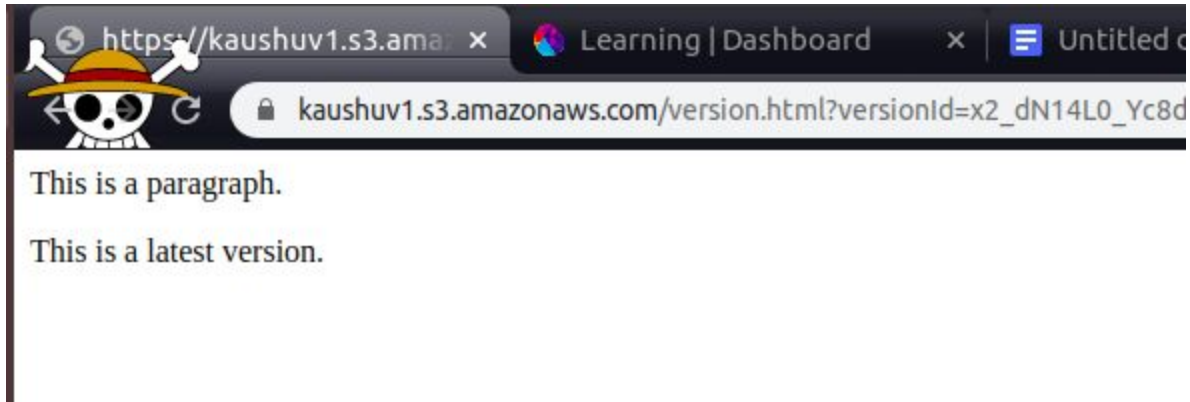
Q Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions Versions Hide Show US Ea

<input type="checkbox"/>	Name	Version ID	Last modified	Size
	version.html		Feb 28, 2020 1:14:11 PM	
<input type="checkbox"/>	Feb 28, 2020 1:14:11 PM (Latest version)	x2_dN14L0_Yc8delj8setsw.b95...		95.0 B
<input type="checkbox"/>	Feb 28, 2020 1:11:01 PM	aVt2issAJNiAUTzF5jHo.oBMU...		117.0 B

After this open the uploaded page in browser

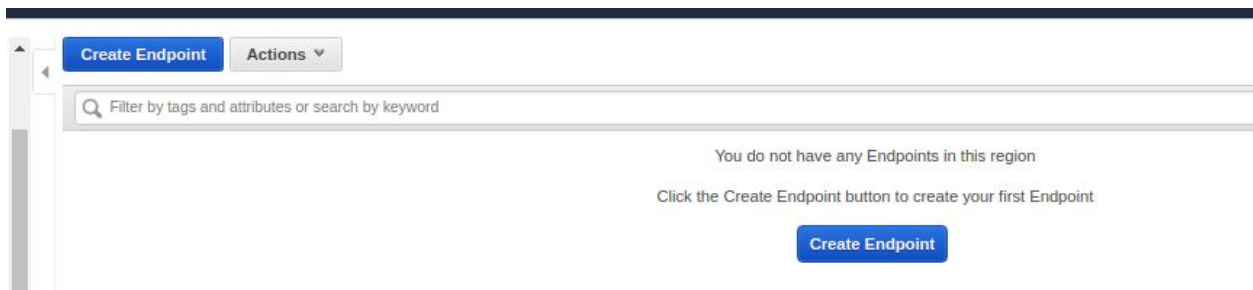




Ques 9. S3 VPC endpoint.

Ans 9.

Open the vpc endpoint terminal



Then create the endpoint for s3 service

## 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 ⓘ

<input type="text" value="search : s3"/> <input type="button" value="Add filter"/>		
Service Name	Owner	Type
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway

**VPC\*** vpc-01d9bca1ea53fdce9  ⓘ

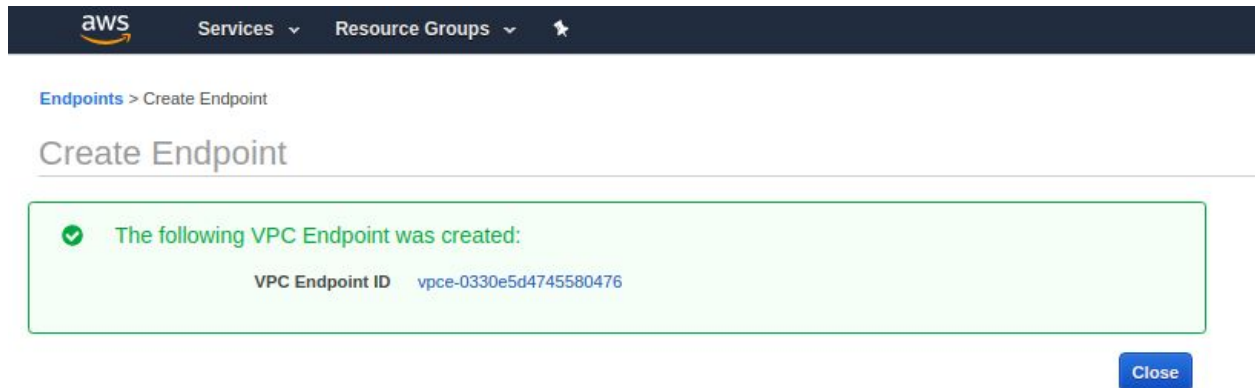
## Then create the policy for access the s3

- Policy\***
- ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in the service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket 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": "*"
    }
  ]
}
```

The endpoint of S3 has been created ....

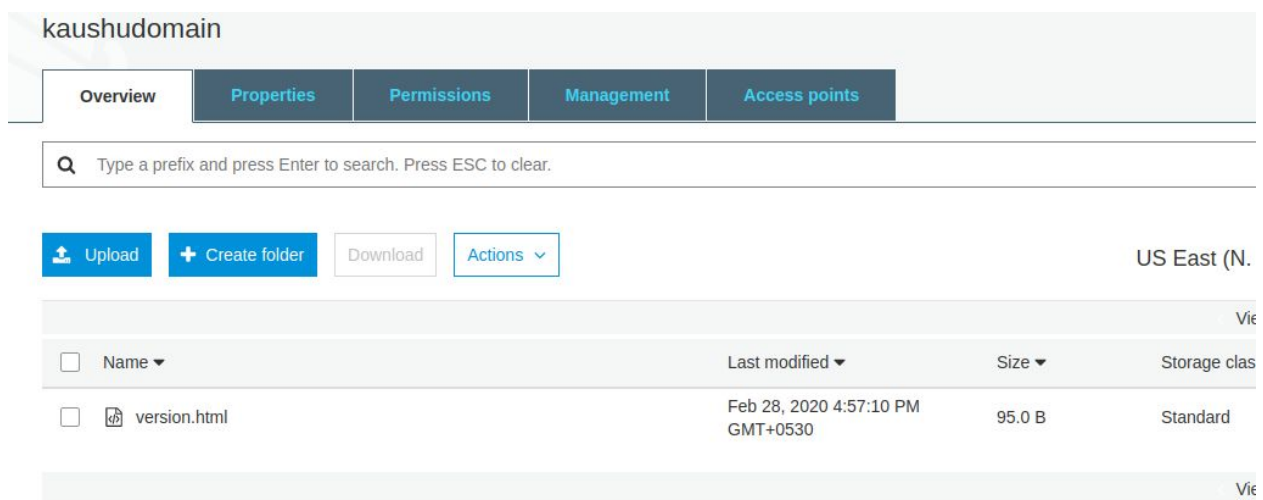


Ques 10. CORS, Enable CORS for 2 specific website.

Ans 10.

Enable CORS in Amazon API Gateway. You can now enable CORS (cross-origin resource sharing) with one click directly in the Amazon API Gateway console. CORS allows methods in API Gateway to request restricted resources from a different domain (e.g., a JavaScript client that calls an API deployed on a different domain).

Created a bucket and uploaded a html page



Then in the cross configuration added a new configuration

kaushudomain

Overview

Properties

Permissions

Management

Access points

Block public access

Access Control List

Bucket Policy

CORS configuration

CORS configuration editor

ARN: arn:aws:s3:::kaushudomain

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

1

2

3

4

5

6

7

8

9

10

11

<?xml version="1.0" encoding="UTF-8"?>  
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">  
<CORSRule>  
 <AllowedOrigin>\*</AllowedOrigin>  
 <AllowedMethod>PUT</AllowedMethod>  
 <AllowedMethod>POST</AllowedMethod>  
 <AllowedMethod>DELETE</AllowedMethod>  
 <AllowedHeader>\*</AllowedHeader>  
</CORSRule>  
</CORSConfiguration>