

Doubt Resolving Session

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

Create bucket

General configuration

Bucket name

jay-s3

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

US East (N. Virginia) us-east-1

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.

Viewing 1 to 2

<input type="checkbox"/>	Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/>	 error.html	Apr 12, 2020 12:47:55 AM GMT+0530	39.0 B	Standard
<input type="checkbox"/>	 index.html	Apr 12, 2020 12:47:39 AM GMT+0530	39.0 B	Standard

Viewing 1 to 2

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



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

Index document [i](#)

Error document [i](#)

Redirection rules (optional) [i](#)



Redirect requests [i](#) [Learn more](#)

Bucket policy editor ARN: arn:aws:s3:::jaypttn-s3

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

Delete

Cancel

Save

```
1 {
2   "Id": "PolicyforWebsitecontent",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "PublicReadGetObject",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "*"
10      },
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::jaypttn-s3/*"
13    }
14  ]
15 }
```



Hey index page of jaypttn-s3


Hey error page of jaypttn-s3


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


Create role


1 2 3 4

Select type of trusted entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

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

[API Gateway](#) [CodeDeploy](#) [EMR](#) [KMS](#) [RoboMaker](#)
[AWS Backup](#) [CodeGuru](#) [ElastiCache](#) [Kinesis](#) [S3](#)

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  [AmazonS3FullAccess](#)

Permissions boundary Permissions boundary is not set

Visual editorJSON

Import managed policy

Expand allCollapse all

▼ STS (1 action) ⚠ 1 warning

CloneRemove

► Service STS

▼ Actions Specify the actions allowed in STS ⓘ

close

Q assume

☒ AssumeRole ⓘ

☐ AssumeRoleWithSAML ⓘ

☐ AssumeRoleWithWebIdentity ⓘ

► Resources Specify role resource ARN for the AssumeRole action.

► Request conditions Specify request conditions (optional)

Resource Group

new.com @ ttn... Global Supp

⚠ 1 warning

► Service

► Action

▼ Resource close

Add ARN(s)

×

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

Specify ARN for role [List ARNs manually](#)

arn:aws:iam::187632318301:role/arn:aws:iam::187632318301:role/Jay-S3FullAccess

Account *

187632318301

☐ Any

Role name with path *

arn:aws:iam::187632318301:

☐ Any

Cancel

Add

Request conditions Specify request conditions (optional)

CloneRemove

☐ Any

Review policy

Name* Jay-Assume-Role

Use alphanumeric and '+,=, @, -, _' characters. Maximum 128 characters.

Description

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

Summary

Service	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			
STS	Limited: Write	RoleName string like Jay-S3FullAccess, Path string like arn:aws:iam::187632318301:role	None

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy



Filter policies <input type="text" value="jay"/>		Showing 1 result
	Policy name ▼	Used as
<input checked="" type="checkbox"/>	Jay-Assume-Role	None

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 [Jay-Assume-Role](#)

Permissions boundary Permissions boundary is not set

The new role will receive the following tags

Edit 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         "Service": "ec2.amazonaws.com",
8         "AWS": "arn:aws:iam::187632318301:role/Jay-Assume-role"
9       },
10      "Action": "sts:AssumeRole"
11    }
12  ]
13 }
```

Cancel

Update Trust Policy

Changed the trust relationship of s3fullaccess role to role can be assumed

Launch Instance Connect Actions

search : akshay Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Akshay	i-0b5a1e96e0c9d54e6	t2.micro	us-east-1c	running	2/2 checks ...	None
Akshay	i-0c5c39a1e07...	t2.micro	us-east-1c	running	2/2 checks ...	None

Instance: i-0b5a1e96e0c9d54e6 (Akshay)

Description Status Checks Monitoring

Instance ID i-0b5a1e96e0c9d54e6

Instance state running

Instance type t2.micro

Finding You may not have permission to access AWS Compute Optimizer.

Private DNS ip-172-31-154-21.ec2.internal

Private IPs 172.31.154.21

Connect

Get Windows Password

Create Template From Instance

Launch More Like This

Instance State

Instance Settings

Image

Networking

CloudWatch Monitoring

Add/Edit Tags

Attach to Auto Scaling Group

Attach/Replace IAM Role

Change Instance Type

Change Termination Protection

View/Change User Data

Change Shutdown Behavior

Change T2/T3 Unlimited

Get System Log

Get Instance Screenshot

Modify Instance Placement

Modify Capacity Reservation Settings

```
ubuntu@ip-172-31-154-21:~$ aws sts assume-role --role-arn arn:aws:iam::187632318301:role/Jay-S3FullAccess --role-session-name Jay
{
  "Credentials": {
    "AccessKeyId": "ASIASXL6B650Y6MFMPPP",
    "SecretAccessKey": "CGvhuaybzYDTaKG12HtaVQAFWUp0wIYUU1QE1EIL",
    "SessionToken": "FwoGZXIvYXZ5EGQaDFrYJaehtPpcdzZZCKnAbdq08ZOKRFJK/k1gCL0Kge3oILudtu83T vz0lF10Z1FJR3I50M0m4onfc3fM6ZBPo0vgImxgV8EaQRJ/aZ2F0Gcjd010WFMGSYX04fUMZYox2u+FfM1MmdvwaJb02adhQ88VYM58f8BJ++2rIv3wMp8Zguq1N8QCua5qmHSntxDbsyuc2+bW2o858BU6Kt6Tl95Fa03Y9Iu7ALTWp7x/N0jV50vG0JkLa08/IFMl2oUApEk13cJJat2pbXVcwYVxwUvNQMxXoGmIRtqJNxq0Mboq4EVKYY++JpudE=",
    "Expiration": "2020-03-02T11:04:38Z"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROASXL6B65037PKSJLNN:Jay",
    "Arn": "arn:aws:sts::187632318301:assumed-role/Jay-S3FullAccess/Jay"
  }
}
ubuntu@ip-172-31-154-21:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B650Y6MFMPPP
ubuntu@ip-172-31-154-21:~$ export AWS_SECRET_ACCESS_KEY=CGvhuaybzYDTaKG12HtaVQAFWUp0wIYUU1QE1EIL
ubuntu@ip-172-31-154-21:~$ export AWS_SESSION_TOKEN=FwoGZXIvYXZ5EGQaDFrYJaehtPpcdzZZCKnAbdq08ZOKRFJK/k1gCL0Kge3oILudtu83T vz0lF10Z1FJR3I50M0m4onfc3fM6ZBPo0vgImxgV8EaQRJ/aZ2F0Gcjd010WFMGSYX04fUMZYox2u+FfM1MmdvwaJb02adhQ88VYM58f8BJ++2rIv3wMp8Zguq1N8QCua5qmHSntxDbsyuc2+bW2o858BU6Kt6Tl95Fa03Y9Iu7ALTWp7x/N0jV50vG0JkLa08/IFMl2oUApEk13cJJat2pbXVcwYVxwUvNQMxXoGmIRtqJNxq0Mboq4EVKYY++JpudE=
ubuntu@ip-172-31-154-21:~$
```

```
ubuntu@ip-172-31-154-21:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-03-01 18:54:15 abhishek-static
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-03-01 15:41:46 aks-plv-buc
2020-02-26 16:26:29 akshaybuck1
2020-03-01 16:43:30 amankhandelwal1
2019-03-07 09:40:48 anmol-bootcamp19
2019-03-08 00:25:58 avcab
2017-09-07 03:41:42 aws-codestar-us-east-1-187632318301
2017-09-07 04:23:01 aws-codestar-us-east-1-187632318301-codestartest2-app
2017-09-07 04:23:07 aws-codestar-us-east-1-187632318301-codestartest2-pipe
2017-09-07 03:41:48 aws-codestar-us-east-1-187632318301-codestarttest-pipe
2019-06-26 05:39:55 aws-lambda-trigger-ronozor
2020-02-28 03:56:49 ayush-public-bucket
2020-03-01 12:28:33 ayush-s3
2020-02-25 07:02:11 baban-123
2020-03-01 10:55:09 bucket-yash-1
2018-02-14 12:28:43 cf-templates-71mx96ojlvv5-us-east-1
2019-03-27 15:57:27 cfront1
2020-02-26 11:51:54 chitrag-bucket-2
```

3. Block s3 access on the basis of

i. IP

Bucket policy editor ARN: arn:aws:s3:::jaypttn-s3

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

```
1 {
2   "Version": "2012-10-17",
3   "Id": "PolicyforWebsitecontent",
4   "Statement": [
5     {
6       "Sid": "ToallowdenyIP",
7       "Effect": "Deny",
8       "Principal": "*",
9       "Action": "s3:*",
10      "Resource": "arn:aws:s3:::jaypttn-s3/*",
11      "Condition": {
12        "NotIpAddress": {
13          "aws:SourceIp": "1.39.252.5/32"
14        }
15      }
16    }
17  ]
18 }
```

ii. Domain

```
1 {
2   "Version": "2012-10-17",
3   "Id": "PolicyforPublicWebsiteContent",
4   "Statement": [
5     {
6       "Sid": "Allow get requests originating from jaypttn bucket url",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": "s3:GetObject",
10      "Resource": "arn:aws:s3:::jaypttn/*",
11      "Condition": {
12        "StringLike": {
13          "aws:Referer": [
14            "http://jaypttn.s3-website-us-east-1.amazonaws.com/*"
15          ]
16        }
17      }
18    }
19  ]
20 }
21 */*
```

iii. Pre-signed URL(Time based)

A presigned URL gives you access to the object identified in the URL, provided that the creator of the presigned URL has permissions to access that object. That is, if you receive a presigned URL to upload an object, you can upload the object only if the creator of the presigned URL has the necessary permissions to upload that object.

All objects and buckets by default are private. The presigned URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. When you create a presigned URL, you must

provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The presigned URLs are valid only for the specified duration.

```
1 [{
2   "Version": "2012-10-17",
3   "Id": "PolicyforPublicWebsiteContent",
4   "Statement": [
5     {
6       "Sid": "Pre-signed URL",
7       "Effect": "Deny",
8       "Principal": "*",
9       "Action": "s3:Get*",
10      "Resource": "arn:aws:s3:::jaypttn/*",
11      "Condition": {
12        "StringEquals": {
13          "s3:authType": "REST-QUERY-STRING"
14        }
15      }
16    }
17  ]
18 }]
```

4. ACL, Bucket policy, IAM Policy.

ACL: 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.

Bucket policy: A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates.

IAM Policy: A policy is an entity that, when attached to an identity or resource, defines their permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer managed policies in IAM. Customer managed policies are standalone policies that you administer in your own AWS account.

5. Mount S3 to an EC2 instance.

```
jay@Jay-Patel:~$ 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
automake is already the newest version (1:1.15.1-3ubuntu2).
automake set to manually installed.
autotools-dev is already the newest version (20180224.1).
autotools-dev set to manually installed.
fuse is already the newest version (2.9.7-1ubuntu1).
make is already the newest version (4.1-9.1ubuntu1).
make set to manually installed.
pkg-config is already the newest version (0.29.1-0ubuntu2).
pkg-config set to manually installed.
g++ is already the newest version (4:7.4.0-1ubuntu2.3).
g++ set to manually installed.
git is already the newest version (1:2.17.1-1ubuntu0.6).
libssl-dev is already the newest version (1.1.1-1ubuntu2.1~18.04.5).
libssl-dev set to manually installed.
The following additional packages will be installed:
  gir1.2-harfbuzz-0.0 icu-devtools libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0 libicu-dev libicu-le-hb-dev libicu-le-hb0 libcurl4-gnutls-dev libcurl4-doc libidn11-dev libkrb5-dev librtmp-dev libssh2-1-dev libgraphite2-utils icu-doc
Suggested packages:
  libcurl4-doc libgnutls28-dev libidn11-dev libkrb5-dev librtmp-dev libssh2-1-dev libgraphite2-utils icu-doc
The following NEW packages will be installed:
  gir1.2-harfbuzz-0.0 icu-devtools libcurl4-gnutls-dev libfuse-dev libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0 libicu-dev
  libicu-le-hb-dev libicu-le-hb0 libcurlx60 libselinux1-dev libsepol1-dev libxml2-dev
0 upgraded, 14 newly installed, 0 to remove and 1 not upgraded.
Need to get 11.1 MB of archives.
After this operation, 52.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 gir1.2-harfbuzz-0.0 amd64 1.7.2-1ubuntu1 [18.6 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 icu-devtools amd64 60.2-3ubuntu3.1 [179 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libcurl4-gnutls-dev amd64 7.58.0-2ubuntu3.8 [294 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsepol1-dev amd64 2.7-1 [324 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libselinux1-dev amd64 2.7-2build2 [149 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libfuse-dev amd64 2.9.7-1ubuntu1 [105 kB]
```

```
jay@Jay-Patel:~$ git clone https://github.com/s3fs-fuse/s3fs-fuse.git
Cloning into 's3fs-fuse'...
remote: Enumerating objects: 53, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 5936 (delta 24), reused 27 (delta 12), pack-reused 5883
Receiving objects: 100% (5936/5936), 3.59 MiB | 472.00 KiB/s, done.
Resolving deltas: 100% (4106/4106), done.
jay@Jay-Patel:~$
```

```

jay@Jay-Patel:~ $ cd s3fs-fuse/
jay@Jay-Patel:s3fs-fuse (master)$ ./autogen.sh
--- Make commit hash file -----
--- Finished commit hash file ---
--- Start autotools -----
configure.ac:30: installing './compile'
configure.ac:26: installing './config.guess'
configure.ac:26: installing './config.sub'
configure.ac:27: installing './install-sh'
configure.ac:27: installing './missing'
src/Makefile.am: installing './depcomp'
parallel-tests: installing './test-driver'
--- Finished autotools -----
jay@Jay-Patel:s3fs-fuse (master)$ ./configure --prefix=/usr --openssl
configure: error: unrecognized option: '--openssl'
Try './configure --help' for more information
jay@Jay-Patel:s3fs-fuse (master)$ ./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++

```

```

jay@Jay-Patel:s3fs-fuse (master)$ which s3fs
/usr/bin/s3fs
jay@Jay-Patel:s3fs-fuse (master)$ sudo touch /etc/passwd
passwd passwd-
jay@Jay-Patel:s3fs-fuse (master)$ sudo touch /etc/passwd
passwd passwd-
jay@Jay-Patel:s3fs-fuse (master)$ sudo touch /etc/passwd-s3fs
jay@Jay-Patel:s3fs-fuse (master)$ sudo vim /etc/passwd-s3fs
jay@Jay-Patel:s3fs-fuse (master)$ sudo chmod 640 /etc/passwd-s3fs
jay@Jay-Patel:s3fs-fuse (master)$ cd /
jay@Jay-Patel:/ $ ll

```

```

jay@Jay-Patel:mnt $ sudo s3fs jaypttn -o use_cache=/tmp -o allow_other
-o uid=1001 -o mp_umask=1002 -o multireq_max=5 jaypttnlocal
jay@Jay-Patel:mnt $ ll
total 9
drwxr-xr-x  3 root root 4096 Apr 18 11:33 ./
drwxr-xr-x 24 root root 4096 Apr 13 00:42 ../
drwxrwxr-x  1 1001 root   0 Jan  1  1970 jaypttnlocal/
jay@Jay-Patel:mnt $ df -Th | grep jaypttnlocal
s3fs          fuse.s3fs 256T    0 256T   0% /mnt/jaypttnlocal
jay@Jay-Patel:mnt $

```

```

jay@Jay-Patel:jaypttnlocal $ ll
total 5
drwxrwxr-x 1 1001 root   0 Jan  1  1970 ./
drwxr-xr-x 3 root root 4096 Apr 18 11:33 ../
-rw-r--r-- 1 1001 root   0 Apr 18 11:41 jayubuntu

```

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"/>	 jayubuntu	Apr 18, 2020 11:41:28 AM GMT+0530	0 B	Standard

Viewing 1 to 1

6. Change content type using s3.

```
jay@Jay-Patel:~ $ aws s3api get-object --bucket jaypttn --key index.html error.html
{
  "AcceptRanges": "bytes",
  "LastModified": "2020-04-18T06:31:34+00:00",
  "ContentLength": 39,
  "ETag": "\"d63ae29a48c342cc6062abe8f5ac5dfa\"",
  "ContentType": "text/html",
  "Metadata": {}
}
jay@Jay-Patel:~ $
```

```
jay@Jay-Patel:~ $ aws s3 cp s3://jaypttn/ s3://jaypttn/ --exclude '*' --include '*.html' --no-guess-mime-type --content-type="text/plain" --metadata-directive="REPLACE" --recursive
copy: s3://jaypttn/index.html to s3://jaypttn/index.html
copy: s3://jaypttn/error.html to s3://jaypttn/error.html
jay@Jay-Patel:~ $
```

```
jay@Jay-Patel:~ $ aws s3api get-object --bucket jaypttn --key index.html jay.txt
{
  "AcceptRanges": "bytes",
  "LastModified": "2020-04-18T06:41:11+00:00",
  "ContentLength": 39,
  "ETag": "\"d63ae29a48c342cc6062abe8f5ac5dfa\"",
  "ContentType": "text/plain",
  "Metadata": {}
}
jay@Jay-Patel:~ $
```

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

Versioning

☒ Enable versioning

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

☐ Disabled

Cancel

Save

Upload	Create folder	Download	Actions	Versions	Hide	Show	US East (N. Virginia)	
<input type="checkbox"/>		Apr 18, 2020 12:11:11 PM (Latest version)	null		39.0 B	Standard		Terminate
	index.html	Apr 18, 2020 12:11:11 PM						
<input type="checkbox"/>		Apr 18, 2020 12:11:11 PM (Latest version)	null		39.0 B	Standard		
	jayubuntu	Apr 18, 2020 11:41:28 AM						
<input type="checkbox"/>		Apr 18, 2020 11:41:28 AM (Latest version)	null		0 B	Standard		
Viewing 1 to 3								

8. S3 VPC 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	<<	<	1 to 1 of 1	>	>>	⚙
Service Name	Owner	Type					
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway					

VPC* vpc-04b71076d48460072 ↕ ⓘ

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

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

Key (128 characters maximum)

Value (256 characters maximum)

This resource currently has no tags

[Add Tag](#) 50 remaining (Up to 50 tags maximum)

9. CORS, Enable CORS for 2 specific website.

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

Configure CORS policy in s3

[Block public access](#)

[Access Control List](#)

[Bucket Policy](#)

[CORS configuration](#)

CORS configuration editor ARN: arn:aws:s3:::baban-123

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

[Delete](#)

[Cancel](#)

[Save](#)

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
3   <CORSRule>
4     <AllowedOrigin>http://www.example1.com</AllowedOrigin>
5     <AllowedOrigin>http://www.example2.com</AllowedOrigin>
6     <AllowedMethod>PUT</AllowedMethod>
7     <AllowedMethod>POST</AllowedMethod>
8     <AllowedMethod>DELETE</AllowedMethod>
9     <MaxAgeSeconds>3000</MaxAgeSeconds>
10    <ExposeHeader>x-amz-server-side-encryption</ExposeHeader>
11    <ExposeHeader>x-amz-request-id</ExposeHeader>
12    <ExposeHeader>x-amz-id-2</ExposeHeader>
13    <AllowedHeader>*</AllowedHeader>
14  </CORSRule>
15 </CORSConfiguration>
16
17
```