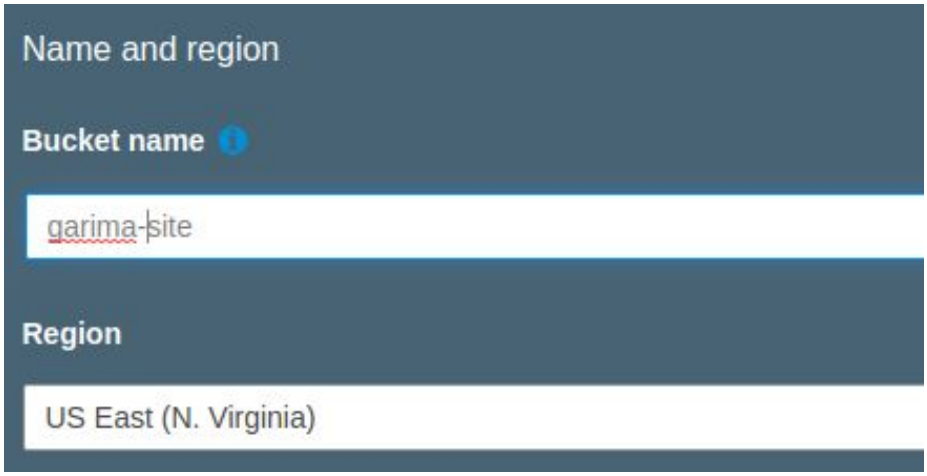
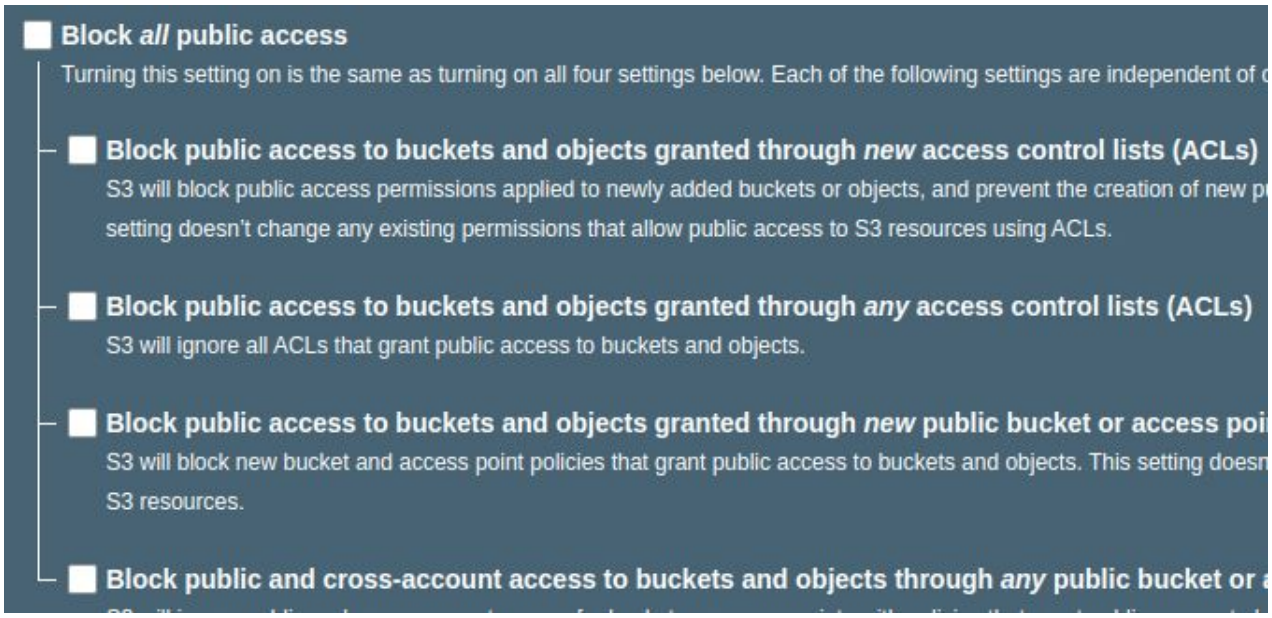
ASSESSMENT - 12

Doubt Resolving

1. **Host a static website using s3 (what is index page and error page i.e significance)**





Endpoint : http://garima-site.s3-website-us-east-1.amazonaws.com

Use this bucket to host a website Learn more

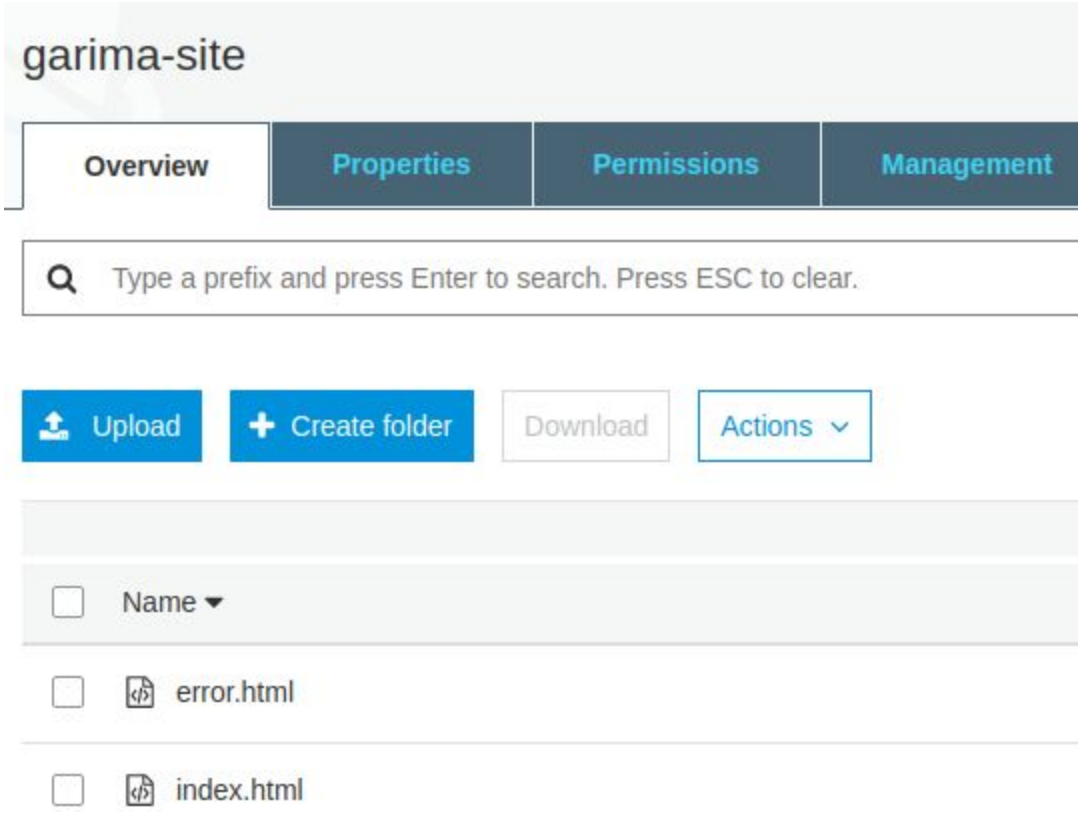
Index document

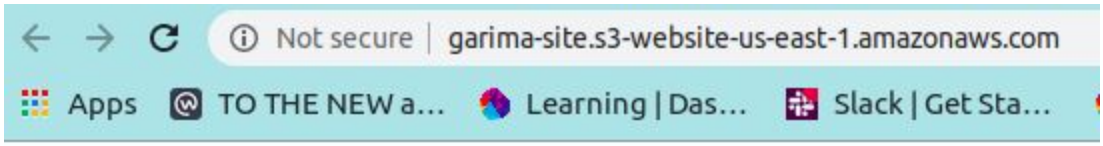
index.html

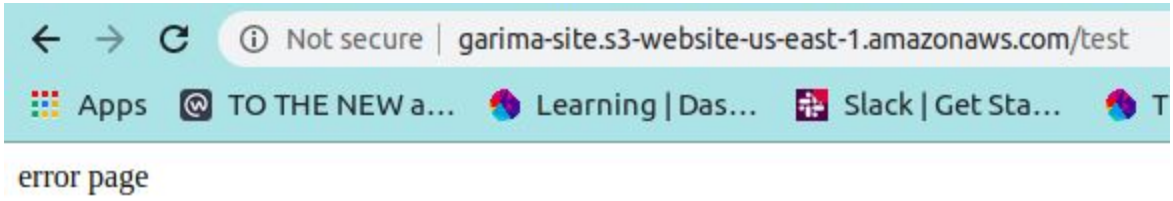
Error document

error.html

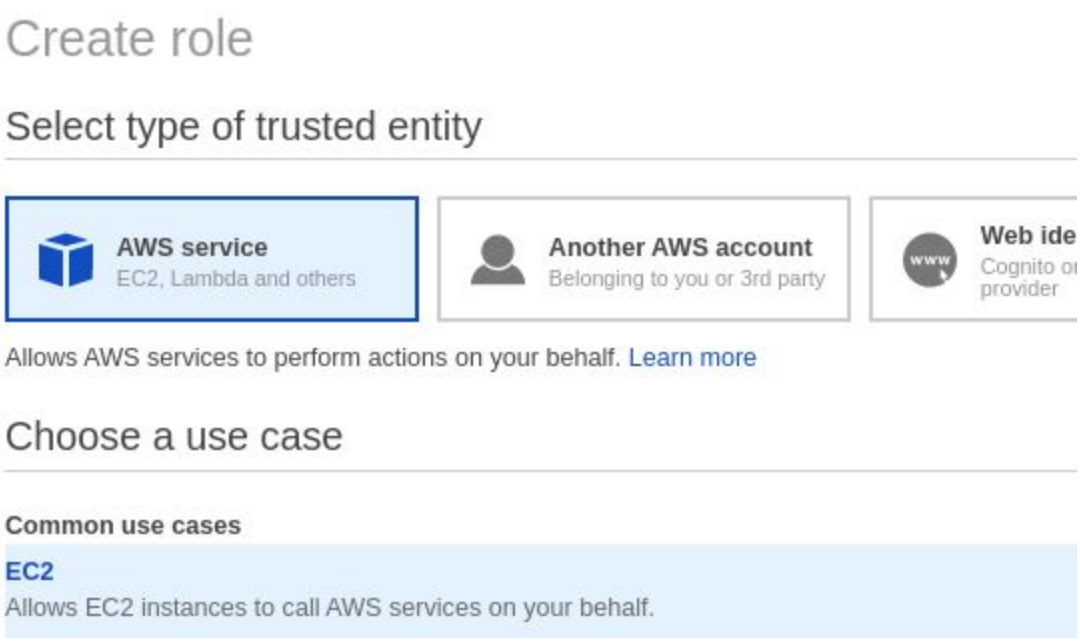
Redirection rules (optional)







2. **Create an assumed role to access s3 using EC2.**



Create role

Attach permissions policies

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

Create policy

Filter policies | AmazonS3Full

		Policy name
✔	▶	AmazonS3FullAccess

Create role

1 2

Review

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

Role name* Role1-for-s3FullAccess

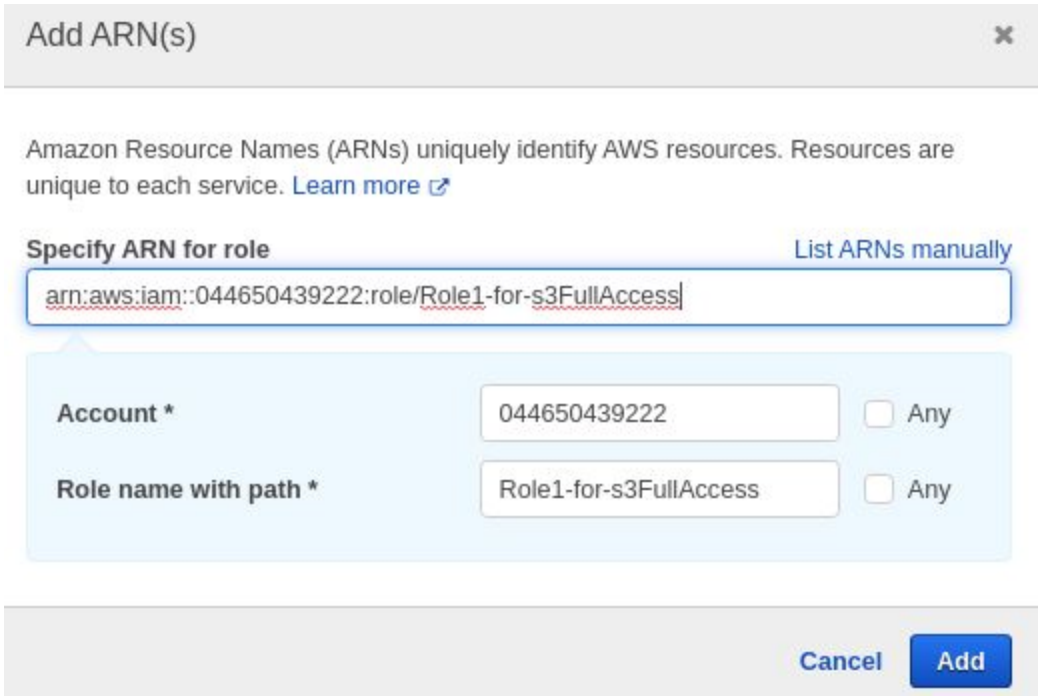
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

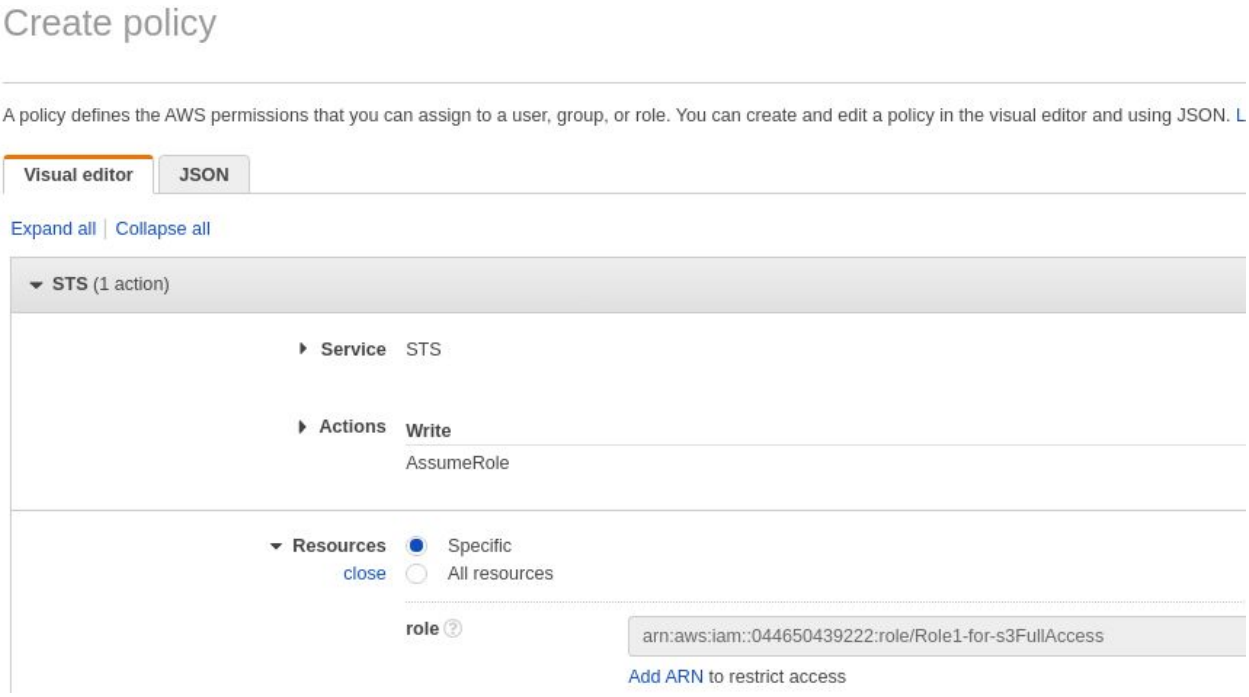
Role description Allows EC2 instances to call AWS services on your behalf.

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

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess


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::044650439222:role/Role1-for-s3FullAccess
Account *
044650439222
Any
Role name with path *
Role1-for-s3FullAccess
Any
Cancel
Add


Create policy
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. L
Visual editor
JSON
Expand all | Collapse all
STS (1 action)
Service
STS
Actions
Write
AssumeRole
Resources
close
Specific
All resources
role
arn:aws:iam::044650439222:role/Role1-for-s3FullAccess
Add ARN to restrict access

Create policy

Review policy

Name* PolicyForAssumedRole

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

Description

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

Summary

Filter

Service	Access level	Resource
Allow (1 of 223 services) Show remaining 222		
STS	**Limited**: Write	RoleName | string like | Role1-for-s3FullAccess

PolicyForAssumedRole has been created.

Create policy | Policy actions

Filter policies | PolicyForAssumed

Policy name	Type	Used as
PolicyForAssumedRole	Customer managed	*None*

Create role

Attach permissions policies

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

Create policy

Filter policies | PolicyForAssumed

		Policy name
☑	▸	PolicyForAssumedRole

Create role

1 2

Review

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

Role name* Role2-for-assumed-role

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

Role description Allows EC2 instances to call AWS services on your behalf.

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

Trusted entities AWS service: ec2.amazonaws.com

Policies PolicyForAssumedRole

Create role | Delete role

Role

Role name	Trusted entities
AWSServiceRoleForAutoScaling	**AWS service:** autoscaling (
AWSServiceRoleForElasticLoadBalancing	**AWS service:** elasticloadba
AWSServiceRoleForSupport	**AWS service:** support (Serv
AWSServiceRoleForTrustedAdvisor	**AWS service:** trustedadvisc
example-role	**Account:** 044650439222
Role1-for-s3FullAccess	**AWS service:** ec2
Role2-for-assumed-role	**AWS service:** ec2

Roles > Role1-for-s3FullAccess

Summary

Role ARN	arn:aws:iam::044650439222:role/Role1-for-s3FullAccess
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::044650439222:instance-profile/Role1-for-s3FullAccess
Path	/
Creation time	2020-03-02 22:18 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions | Trust relationships | Tags (1) | Access Advisor | Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy docume

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The identity provider(s) ec2.amazonaws.com

Conditions

The following conditions de

There are no conditions ass

Edit Trust Relationship

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

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::044650439222:role/Role2-for-assumed-role",
        "Service": "ec2.amazonaws.com",
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Roles > Role1-for-s3FullAccess

Summary

Role ARN	arn:aws:iam::044650439222:role/F
Role description	Allows EC2 instances to call AWS
Instance Profile ARNs	arn:aws:iam::044650439222:instar
Path	/
Creation time	2020-03-02 22:18 UTC+0530
Last activity	Not accessed in the tracking perio
Maximum CLI/API session duration	1 hour Edit

Permissions | **Trust relationships** | **Tags (1)** | **Access Advisor**

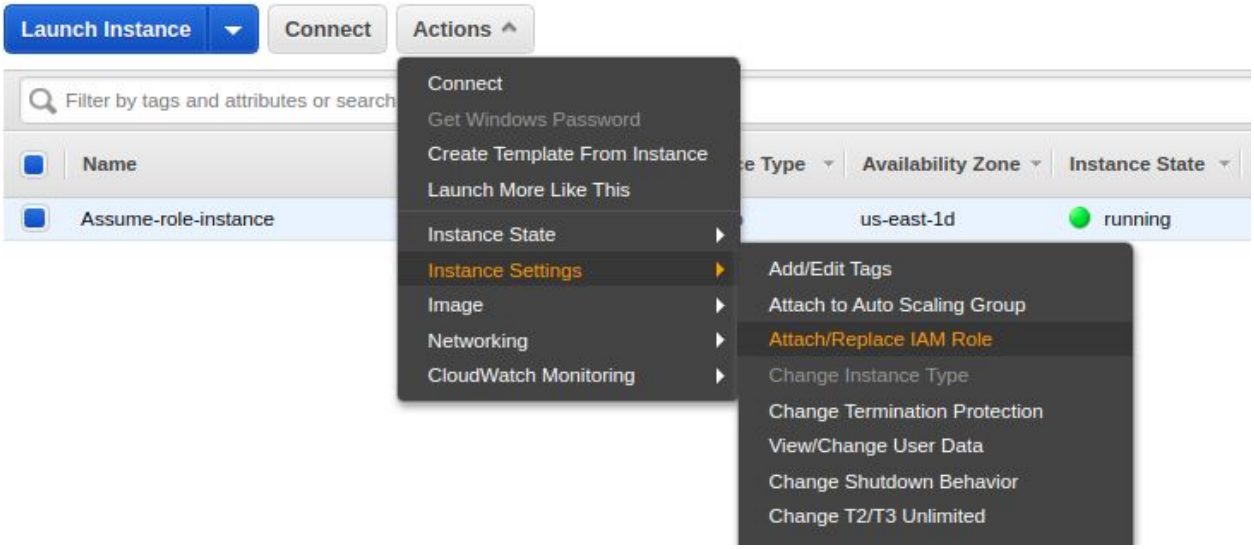
You can view the trusted entities that can assume the role and the access condit

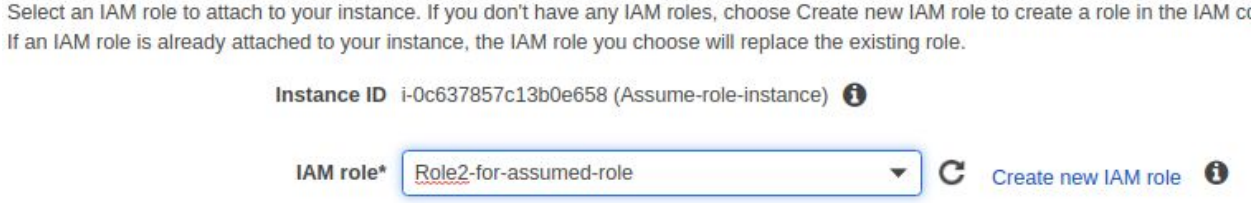
Edit trust relationship

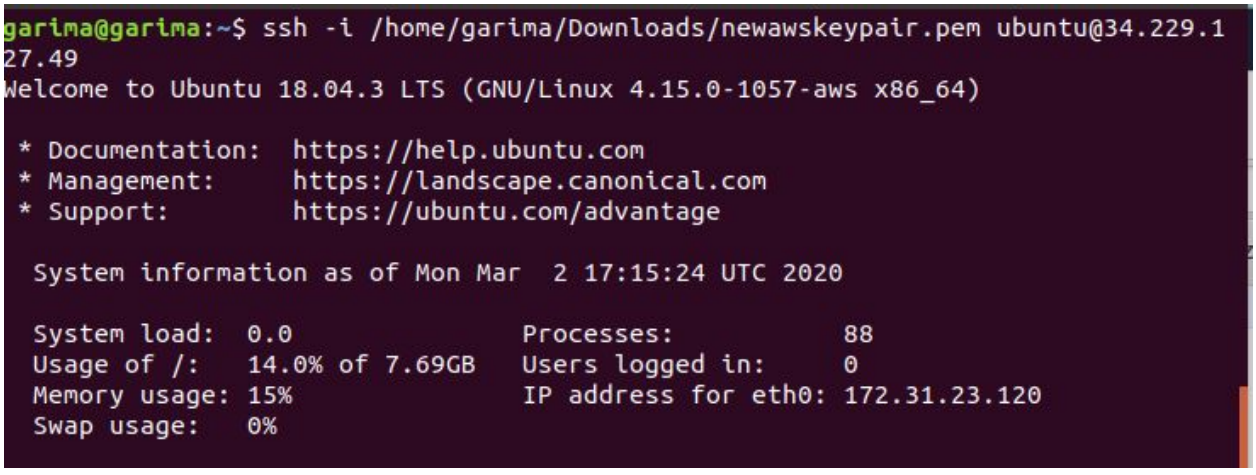
Trusted entities

The following trusted entities can assume this role.

Trusted entities
The identity provider(s) ec2.amazonaws.com
arn:aws:iam::044650439222:role/Role1-for-s3FullAccess


Launch Instance
Connect
Actions
Filter by tags and attributes or search
Name
Type
Availability Zone
Instance State
Assume-role-instance
us-east-1d
running
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


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 c
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.
Instance ID i-0c637857c13b0e658 (Assume-role-instance)
IAM role* Role2-for-assumed-role
Create new IAM role


garima@garima:~$ ssh -i /home/garima/Downloads/newawskeypair.pem ubuntu@34.229.1
27.49
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 Mon Mar 2 17:15:24 UTC 2020
System load: 0.0 Processes: 88
Usage of /: 14.0% of 7.69GB Users logged in: 0
Memory usage: 15% IP address for eth0: 172.31.23.120
Swap usage: 0%

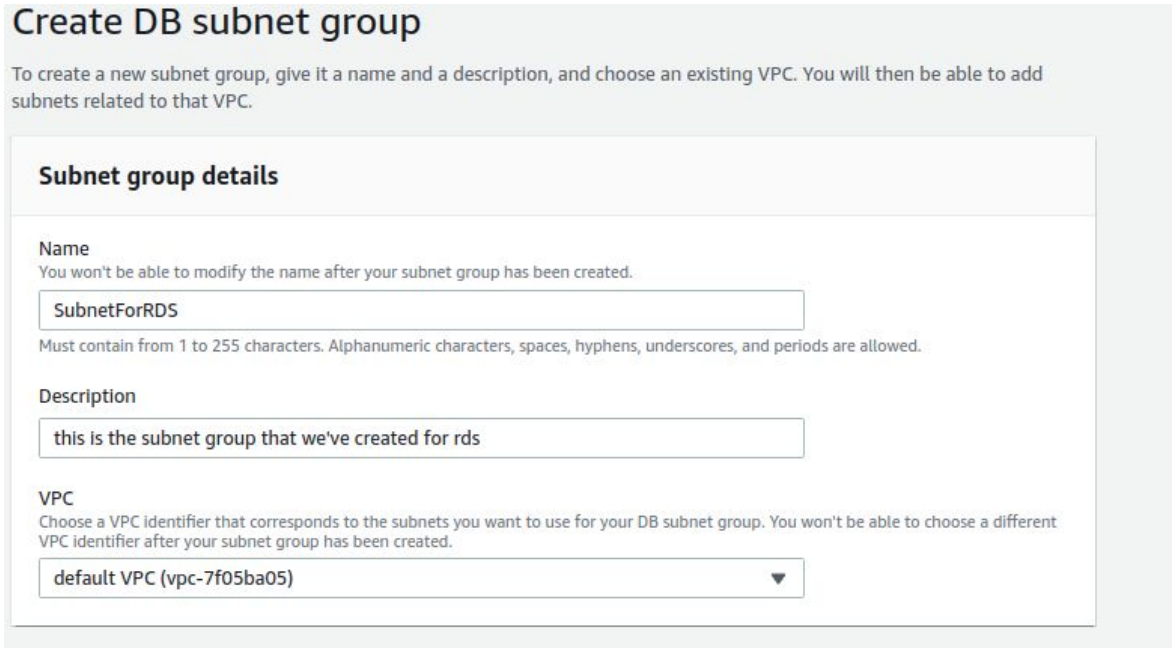
```
ubuntu@ip-172-31-23-120:~$ aws sts get-caller-identity
{
    "UserId": "AROAQUZK7UI3NK3C6UGPV:i-0c637857c13b0e658",
    "Account": "044650439222",
    "Arn": "arn:aws:sts::044650439222:assumed-role/Role2-for-assumed-role/i-0c63
7857c13b0e658"
}
ubuntu@ip-172-31-23-120:~$
```

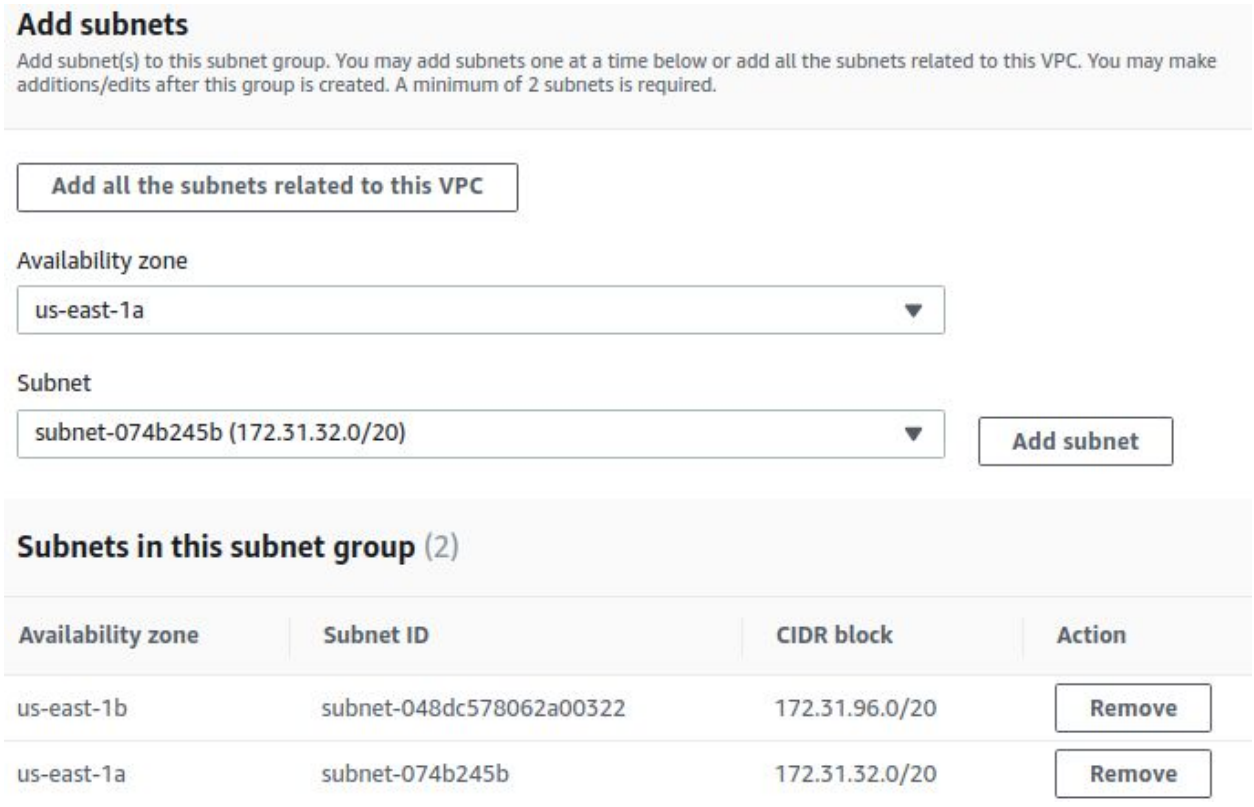
```
ubuntu@ip-172-31-23-120:~$ aws sts assume-role --role-arn arn:aws:iam::044650439
222:role/Role1-for-s3FullAccess --role-session-name garima
{
    "Credentials": {
        "SessionToken": "FwoGZXIvYXdzEGsaDACaKRV1uijfoOWtQyKqAaaxdD4qPBpzB6U4lyv
WgumyFJhPphlzHn6+WCGaFQyLsKsV1h6Z80kB8LyP/fgOgD5TDB4bftVxwQDsfpt5iPmS6Z/u4PQkJNS
BMKOYX55ZO0LTdRjZUqbwnql+AyUw+ERng708cBSUb0pfgvlAFykbiQqjBJdiu/DFe5JcOvkOjvEHemV
Xk1BoISAekaGl6YaHA/X8HEOUOVaKGSO6UecM/pNfSFx9vhxJKOqL9fIFMi1hWIY/5ATMKOAYZkKZsJv
7Hu4lpqTebfMU/l+Z7IoBvjxZMDE6gVfutB4Fqm0=",
        "AccessKeyId": "ASIAQUZK7UI3JQTGEJNY",
        "SecretAccessKey": "4HDDPotEU4XS2DseTmV8R6EpK9uvQzcEd0Ub72lk",
        "Expiration": "2020-03-02T18:44:10Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAQUZK7UI3HFOXNYD66:garima",
        "Arn": "arn:aws:sts::044650439222:assumed-role/Role1-for-s3FullAccess/ga
rima"
    }
}
```

```
ubuntu@ip-172-31-23-120:~$ export AWS_ACCESS_KEY_ID=ASIAQUZK7UI3JQTGEJNY
ubuntu@ip-172-31-23-120:~$ export AWS_SECRET_ACCESS_KEY=4HDDPotEU4XS2DseTmV8R6Ep
K9uvQzcEd0Ub72lk
ubuntu@ip-172-31-23-120:~$ export AWS_SESSION_TOKEN=FwoGZXIvYXdzEGsaDACaKRV1uijf
oOWtQyKqAaaxdD4qPBpzB6U4lyvWgumyFJhPphlzHn6+WCGaFQyLsKsV1h6Z80kB8LyP/fgOgD5TDB4b
ftVxwQDsfpt5iPmS6Z/u4PQkJNSBMKOYX55ZO0LTdRjZUqbwnql+AyUw+ERng708cBSUb0pfgvlAFykb
iQqjBJdiu/DFe5JcOvkOjvEHemVXk1BoISAekaGl6YaHA/X8HEOUOVaKGSO6UecM/pNfSFx9vhxJKOqL
9fIFMi1hWIY/5ATMKOAYZkKZsJv7Hu4lpqTebfMU/l+Z7IoBvjxZMDE6gVfutB4Fqm0=
ubuntu@ip-172-31-23-120:~$
```

```
ubuntu@ip-172-31-23-120:~$ aws s3 ls
2019-05-08 15:48:33 garima-essence
2020-02-26 18:14:51 garima-site
2020-03-02 07:16:16 non-public-bucket-garima
ubuntu@ip-172-31-23-120:~$
```

3. **Create RDS subnet and launch RDS Instance. What is the parameter group and Option Group?**





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 currer Region.

garima-database

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

▼ Credentials Settings

Master username Info

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

admin

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. T 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

1000 GiB

Minimum: 21 GiB, Maximum: 16384 GiB

Connectivity

Virtual Private Cloud (VPC) Info

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

Default VPC (vpc-7f05ba05)

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.

subnetforrds

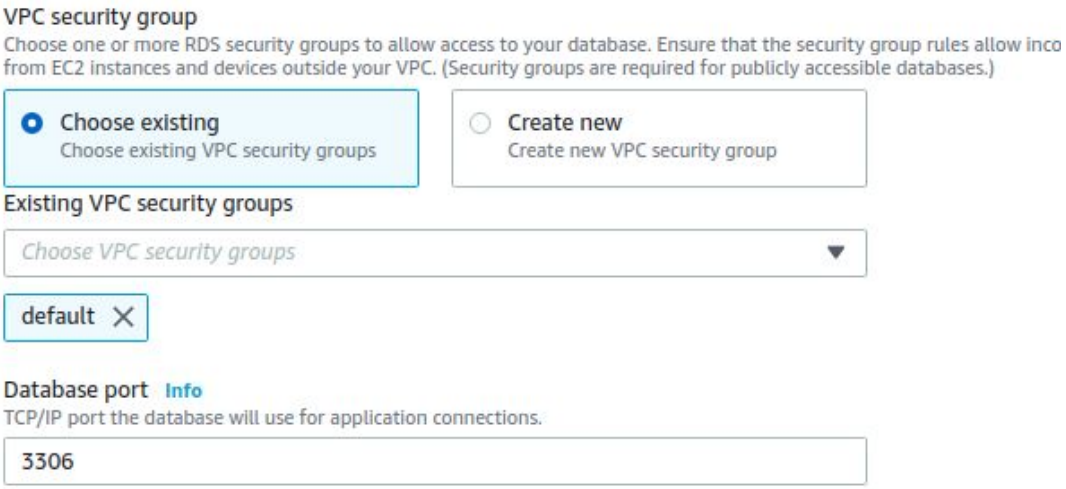
Publicly accessible Info

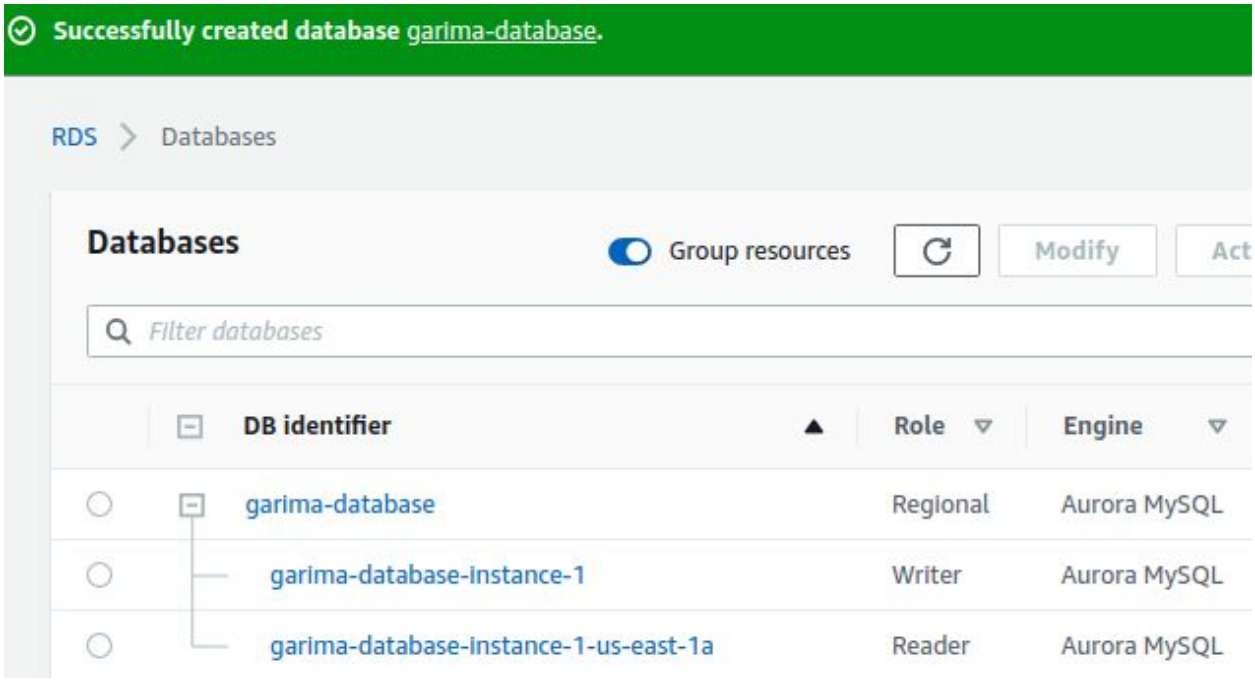
◉ Yes

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.





Parameter group : For AWS RDS instances, you manage your database engine configuration through the use of parameters in a DB parameter group. DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances.

Option Group: 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.

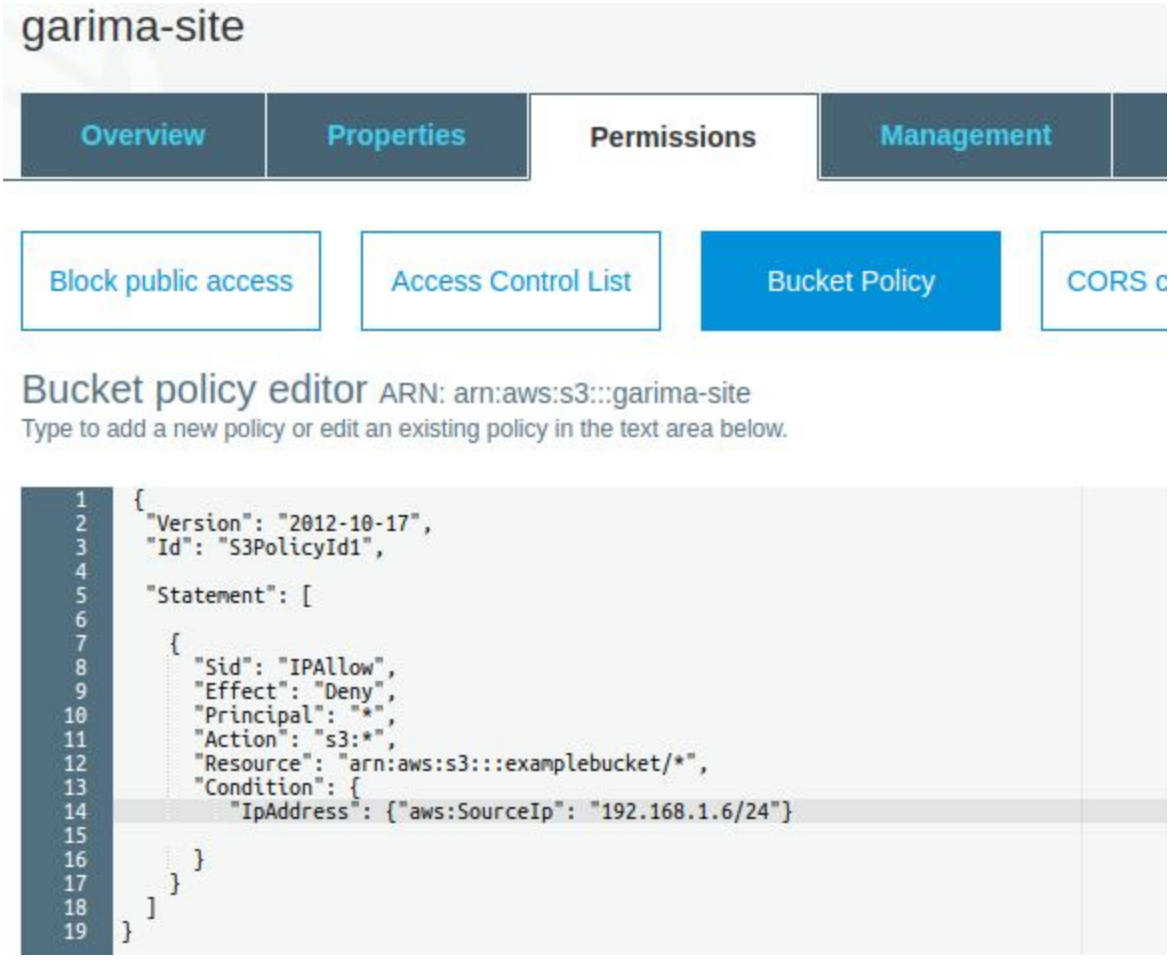
4. **ACL, Bucket policy, IAM policy in context of S3**

ACL: 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.

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. You can then attach the policies to identities (users, groups, and roles) in your AWS account.

5. **Block S3 access on the basis of:**
   - **Ip**



- **Domain**

- **Pre-signed URL(time based)**

```
File  Edit  View  Search  Terminal  Help
garima@garima:~$ aws s3 presign s3://garima-site/index.html
https://garima-site.s3.amazonaws.com/index.html?AWSAccessKeyId=AKIAIFESFXLUSG253
TPA&Expires=1583929471&Signature=%2B3gonhkA%2BYJ9Ah%2FtkNetgJR%2FRD4%3D
garima@garima:~$
```

```
File  Edit  View  Search  Terminal  Help
import boto3
from botocore.client import Config
region='us-east-1'
s3 = boto3.client('s3',region_name=region)
url = s3.generate_presigned_url(
    ClientMethod='get_object',
    Params={
        'Bucket': 'garima-site',
        'Key': 'index.html'
    },
    ExpiresIn=120
)
print(url)
~
~
~
```

```
garima@garima:~$ python3 presign.py
https://garima-site.s3.amazonaws.com/index.html?AWSAccessKeyId=AKIAIFESFXLUSG253
TPA&Signature=byusveSJk%2Bv5XUGLdDC4HWZD4E4%3D&Expires=1583927628
```

6. Mount S3 to an EC2 Instance

```
garima@garima:~$ sudo apt-get install automake autotools-dev fuse g++ git libcur
l4-gnutls-dev libfuse-dev libssl-dev libxml2-dev make pkg-config
[sudo] password for garima:
Reading package lists... Done
Building dependency tree
Reading state information... Done
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.
g++ is already the newest version (4:7.4.0-1ubuntu2.3).
g++ set to manually installed.
git is already the newest version (1:2.17.1-1ubuntu0.5).
```

```
garima@garima:~$ git clone https://github.com/s3fs-fuse/s3fs-fuse.git
Cloning into 's3fs-fuse'...
remote: Enumerating objects: 40, done.
remote: Counting objects: 100% (40/40), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 5879 (delta 18), reused 22 (delta 8), pack-reused 5839
Receiving objects: 100% (5879/5879), 3.53 MiB | 1.23 MiB/s, done.
Resolving deltas: 100% (4069/4069), done.
```

```
garima@garima:~$  cd s3fs-fuse
garima@garima:~/s3fs-fuse$ ./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 ----------
garima@garima:~/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
```

```
garima@garima:~/s3fs-fuse$ make
(CDPATH="${ZSH_VERSION+.}:" && cd . && /bin/bash /home/garima/s3fs-fuse/missing
autoheader)
rm -f stamp-h1
touch config.h.in
cd . && /bin/bash ./config.status config.h
config.status: creating config.h
config.status: config.h is unchanged
make  all-recursive
make[1]: Entering directory '/home/garima/s3fs-fuse'
Making all in src
make[2]: Entering directory '/home/garima/s3fs-fuse/src'
```

```
garima@garima:~/s3fs-fuse$ sudo make install
Making install in src
make[1]: Entering directory '/home/garima/s3fs-fuse/src'
make[2]: Entering directory '/home/garima/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/garima/s3fs-fuse/src'
```

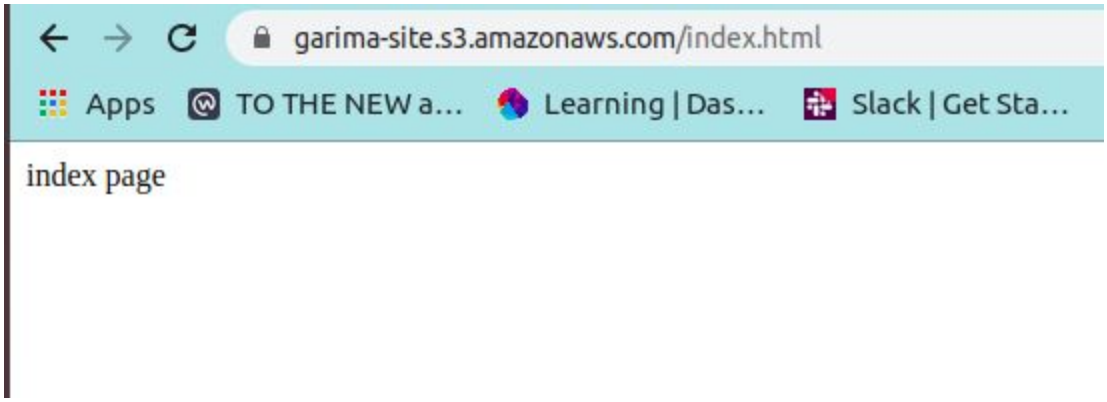
```
AKIAIFESFXLUSG253TPA:5iQbgm8ogfBLSyPdpsTqcxqtWsaeiB5yhpjzkkdQ
~
~
~
~
```

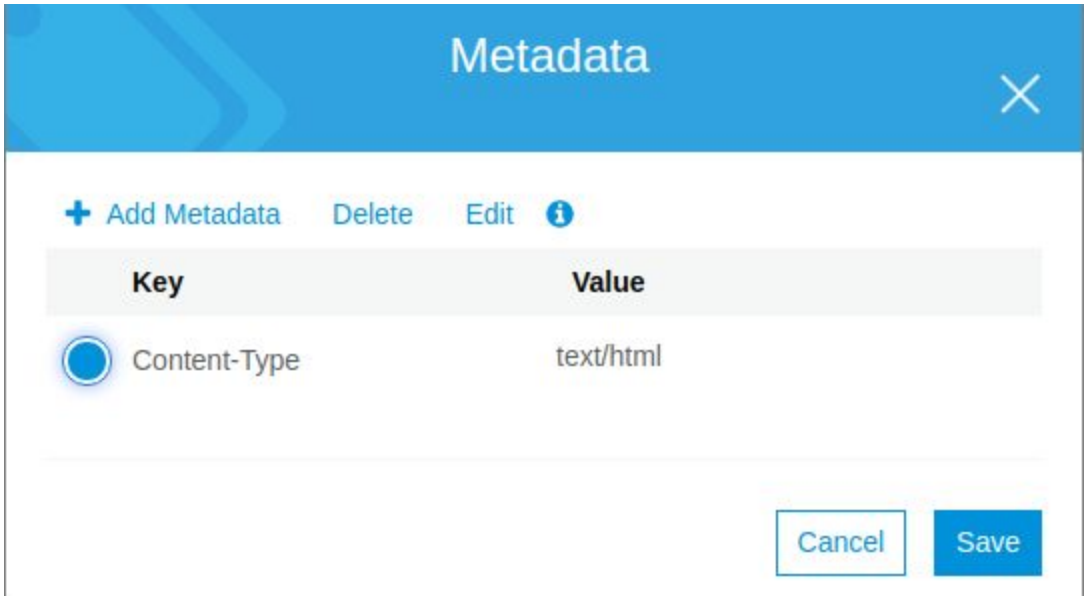
```
garima@garima:~/s3fs-fuse$ which s3fs
/usr/bin/s3fs
garima@garima:~/s3fs-fuse$ sudo vim /etc/passwd-s3fs
garima@garima:~/s3fs-fuse$ sudo chmod 640 /etc/passwd-s3fs
```

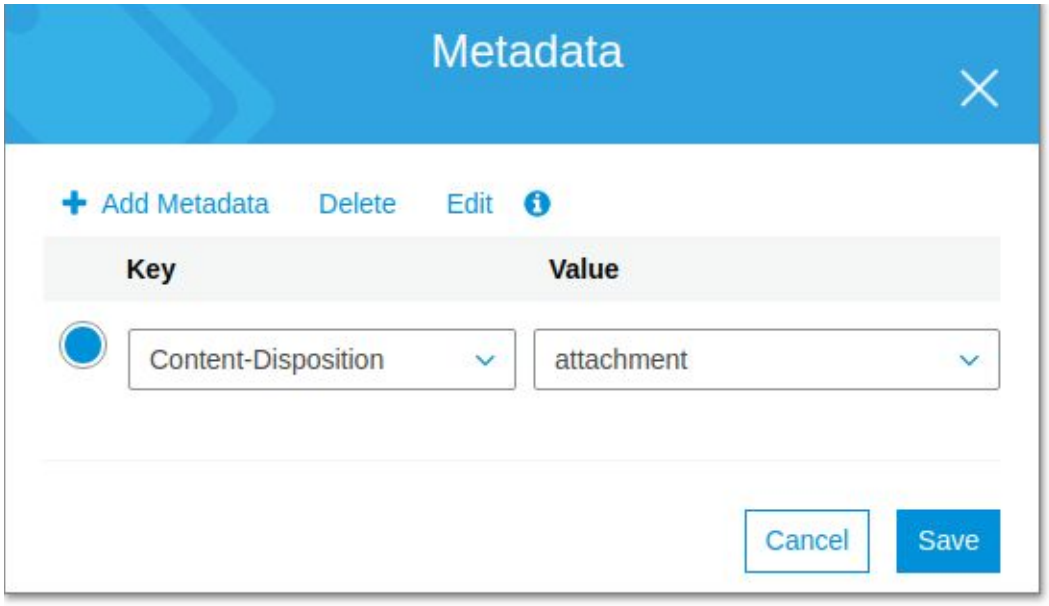
```
garima@garima:~/s3fs-fuse$ sudo mkdir /mys3bucket1
garima@garima:~/s3fs-fuse$ sudo s3fs garima-site -o use_cache=/tmp -o allow_othe
r -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket1
garima@garima:~/s3fs-fuse$ which s3fs
/usr/bin/s3fs
garima@garima:~/s3fs-fuse$ sudo nano /etc/rc.local
garima@garima:~/s3fs-fuse$ df -Th
Filesystem     Type       Size  Used Avail Use% Mounted on
udev           devtmpfs   7.7G     0  7.7G   0% /dev
tmpfs          tmpfs      1.6G  2.1M  1.6G   1% /run
/dev/nvme0n1p1 ext4       234G  9.4G  213G   5% /
tmpfs          tmpfs      7.7G  220M  7.5G   3% /dev/shm
tmpfs          tmpfs      5.0M  4.0K  5.0M   1% /run/lock
```

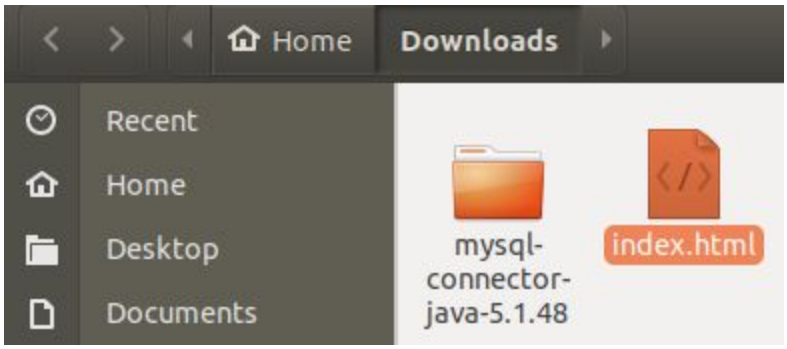
```
s3fs           fuse.s3fs  256T     0  256T   0% /mys3bucket1
garima@garima:~/s3fs-fuse$
```

7. Change content type using S3.

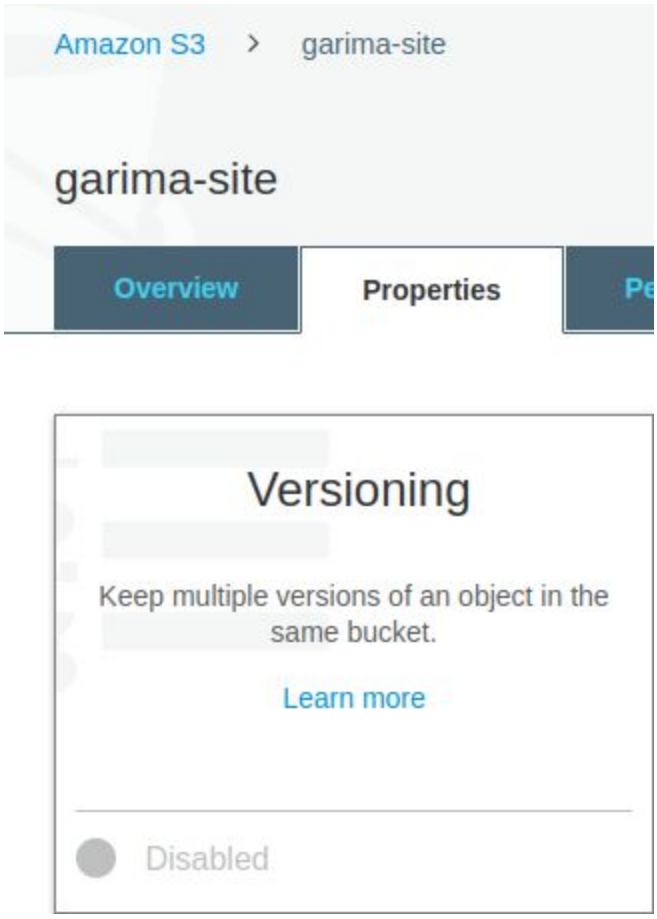

garima-site.s3.amazonaws.com/index.html
Apps
TO THE NEW a...
Learning | Das...
Slack | Get Sta...
index page

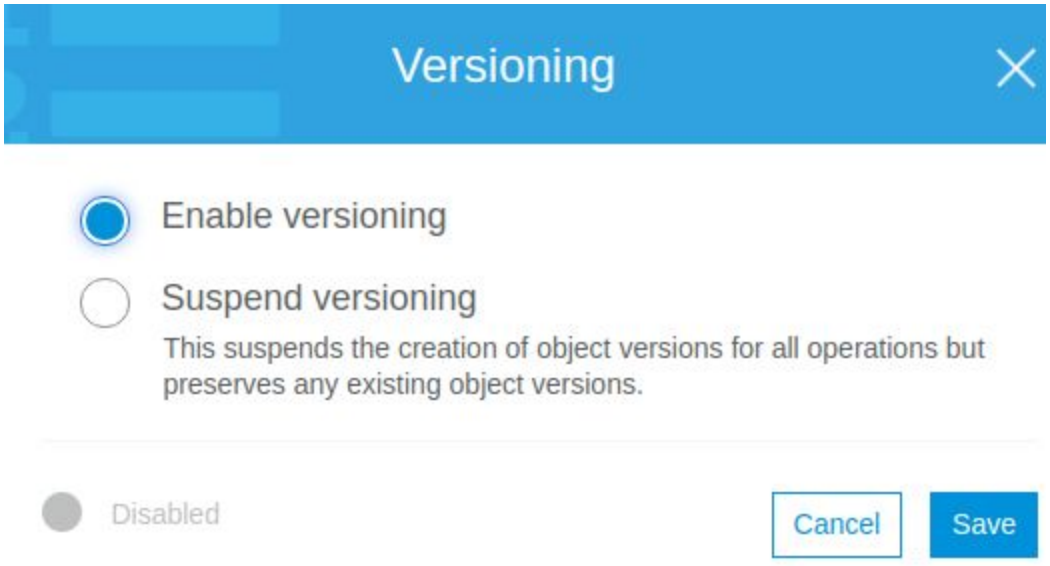

Metadata
Add Metadata
Delete
Edit
Key
Value
Content-Type
text/html
Cancel
Save

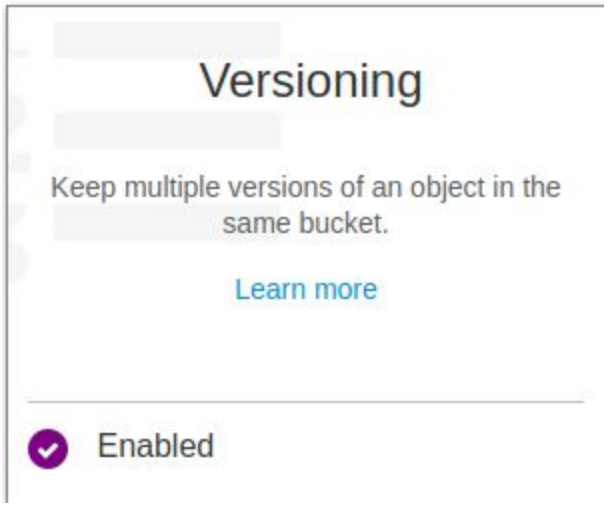




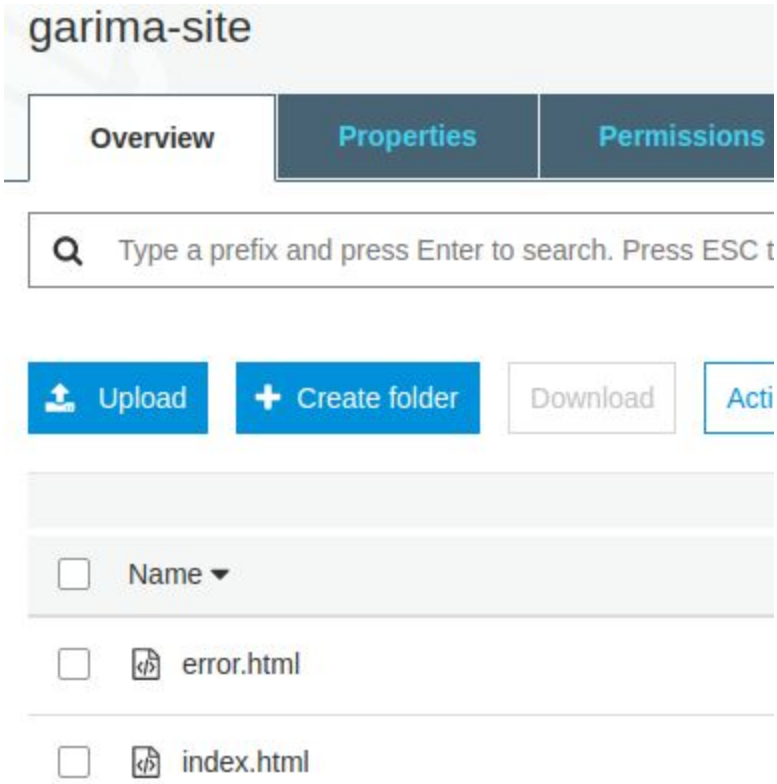
8. Retrieve previous version of S3.Enabling versioning

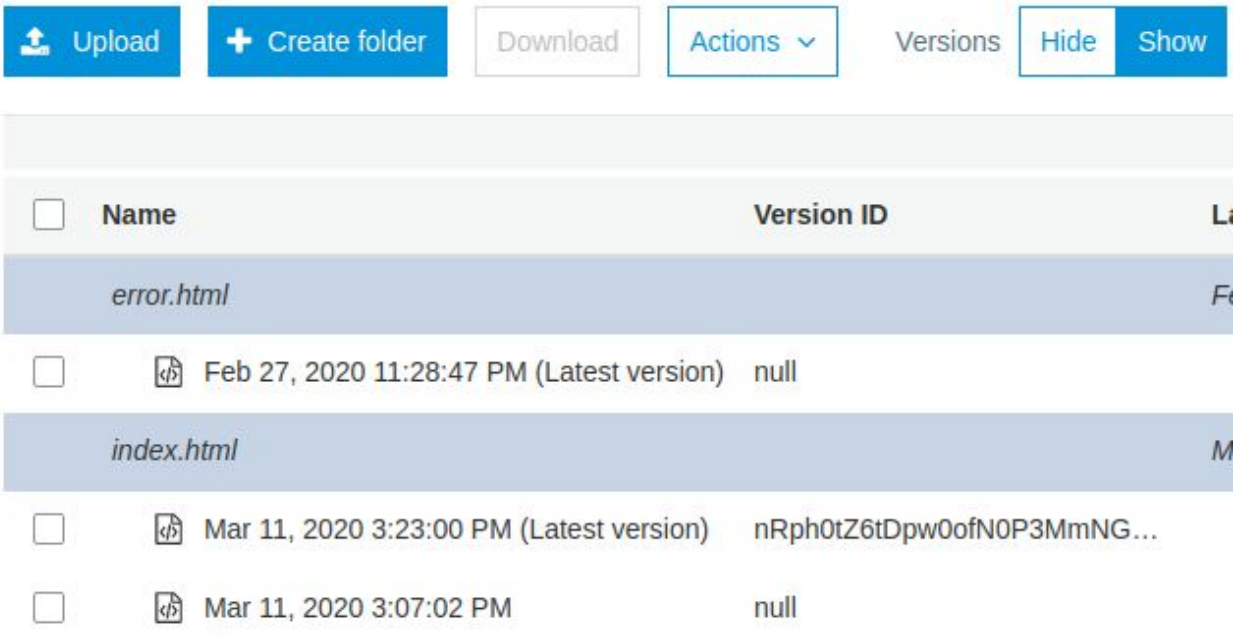

Amazon S3 > garima-site
garima-site
Overview
Properties
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled

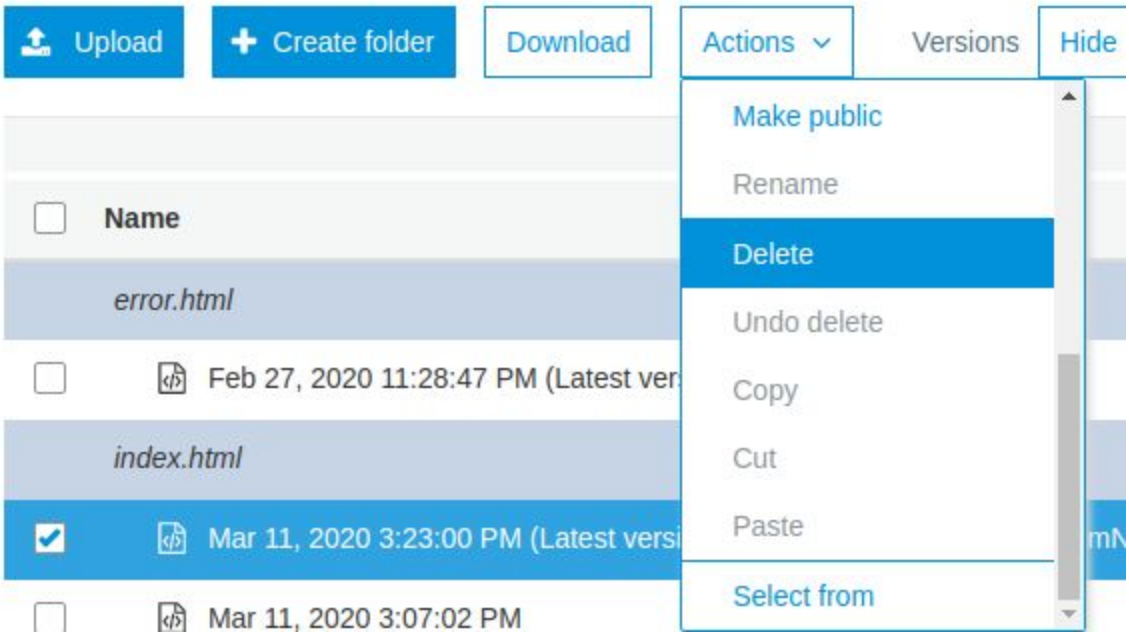

Versioning
Enable versioning
Suspend versioning
This suspends the creation of object versions for all operations but preserves any existing object versions.
Disabled
Cancel
Save

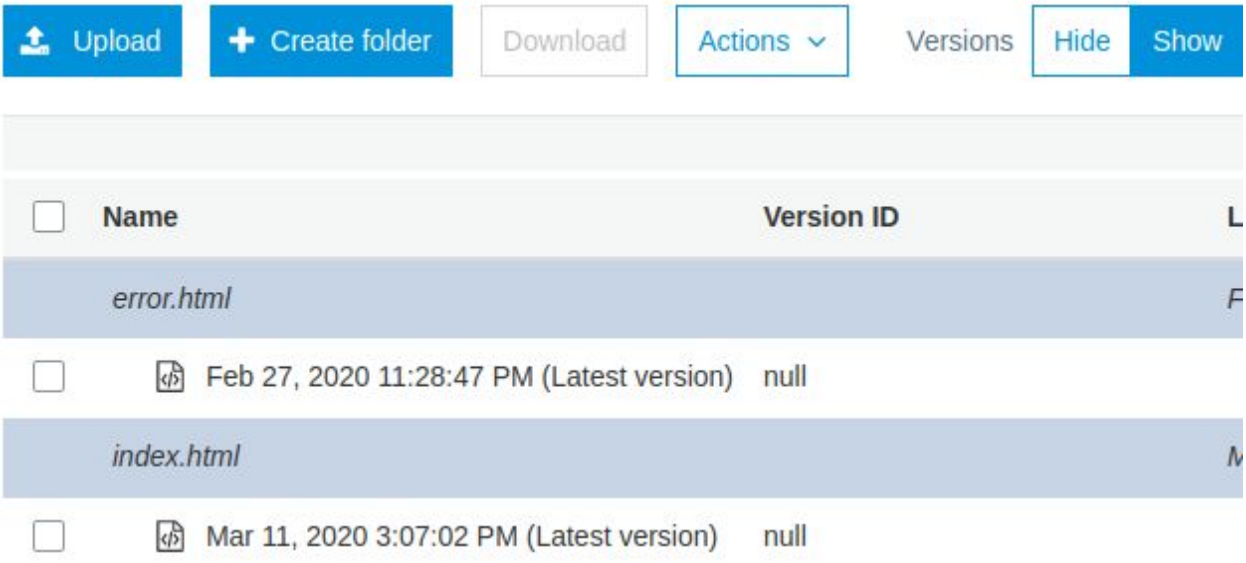



```
garima@garima:~/Documents$ vim index.html
garima@garima:~/Documents$ cat index.html
new index.html file
garima@garima:~/Documents$
```


garima-site
Overview
Properties
Permissions
Type a prefix and press Enter to search. Press ESC t
Upload
Create folder
Download
Acti
Name
error.html
index.html

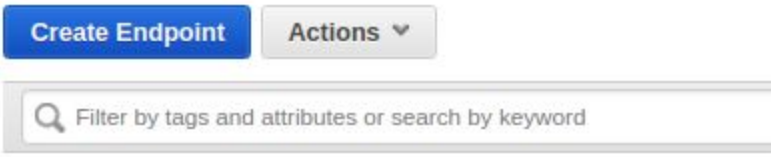

Upload
Create folder
Download
Actions
Versions
Hide
Show
Name
Version ID
error.html
Feb 27, 2020 11:28:47 PM (Latest version)
null
index.html
Mar 11, 2020 3:23:00 PM (Latest version)
nRph0tZ6tDpw0ofN0P3MmNG…
Mar 11, 2020 3:07:02 PM
null

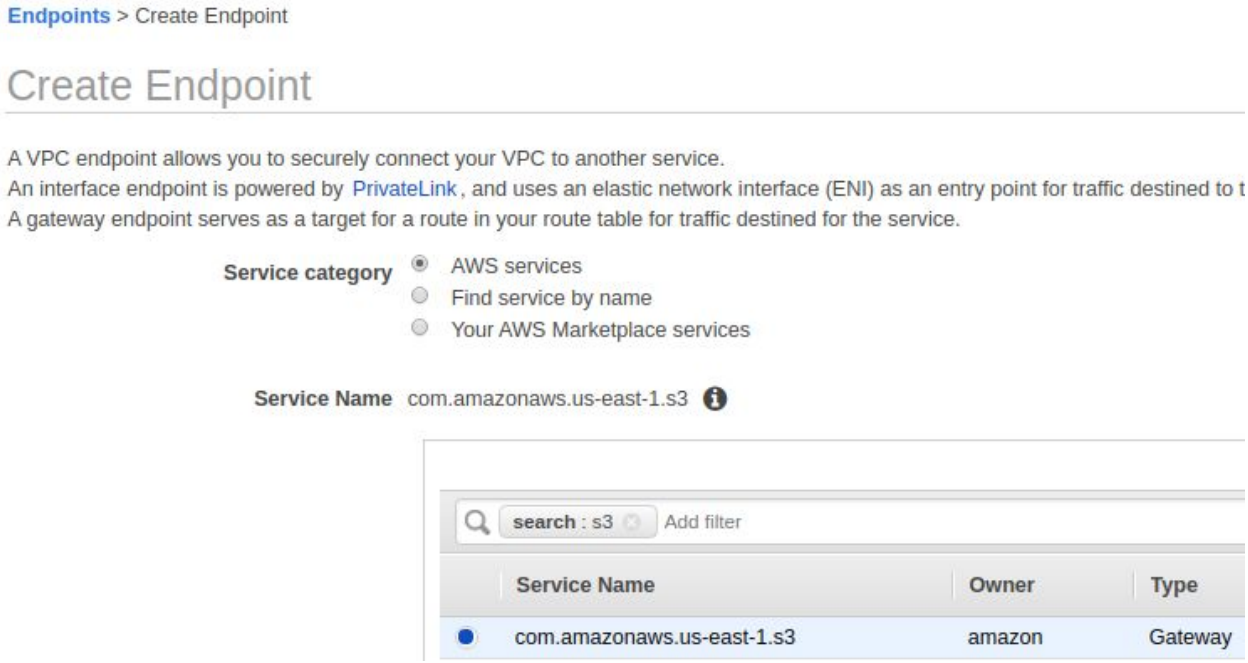

Upload
Create folder
Download
Actions
Versions
Hide
Make public
Rename
Delete
Undo delete
Copy
Cut
Paste
Select from
Name
error.html
Feb 27, 2020 11:28:47 PM (Latest ver
index.html
Mar 11, 2020 3:23:00 PM (Latest versi
Mar 11, 2020 3:07:02 PM

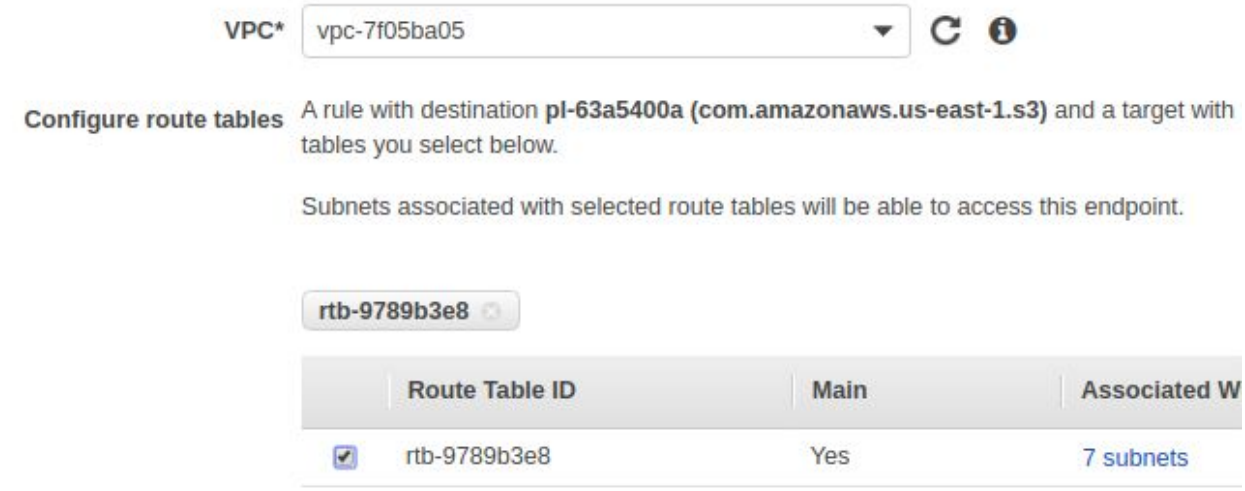

Upload
Create folder
Download
Actions
Versions
Hide
Show
Name
Version ID
error.html
Feb 27, 2020 11:28:47 PM (Latest version)
null
index.html
Mar 11, 2020 3:07:02 PM (Latest version)
null

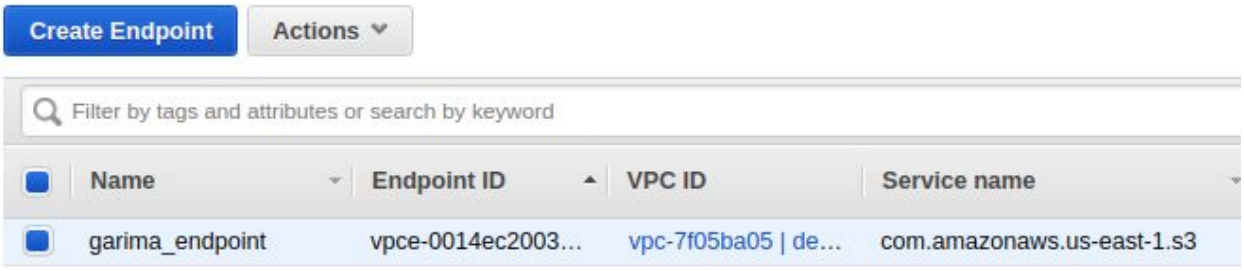
9. **What is VPC endpoint ?Enable it.**

ANS: A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet, through a NAT device, a VPN connection, or AWS Direct Connect.









10. CORS, Enabling CORS for 2 specific website