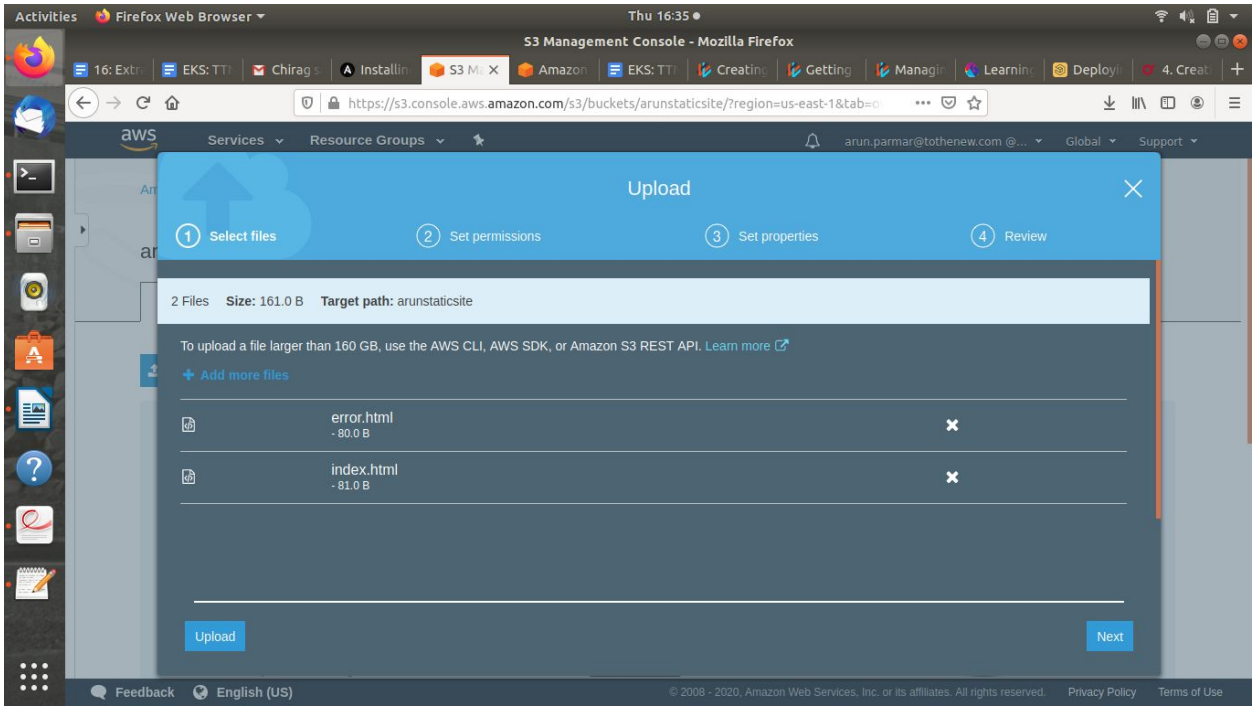
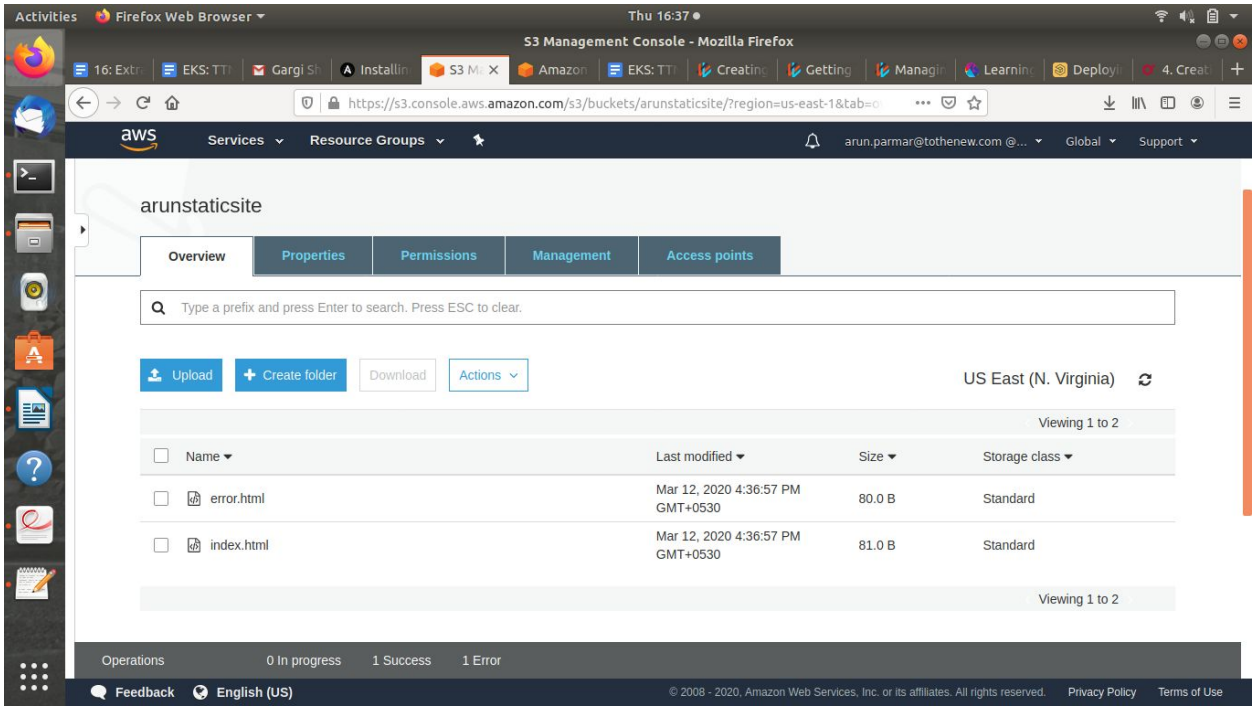
Assessment -16

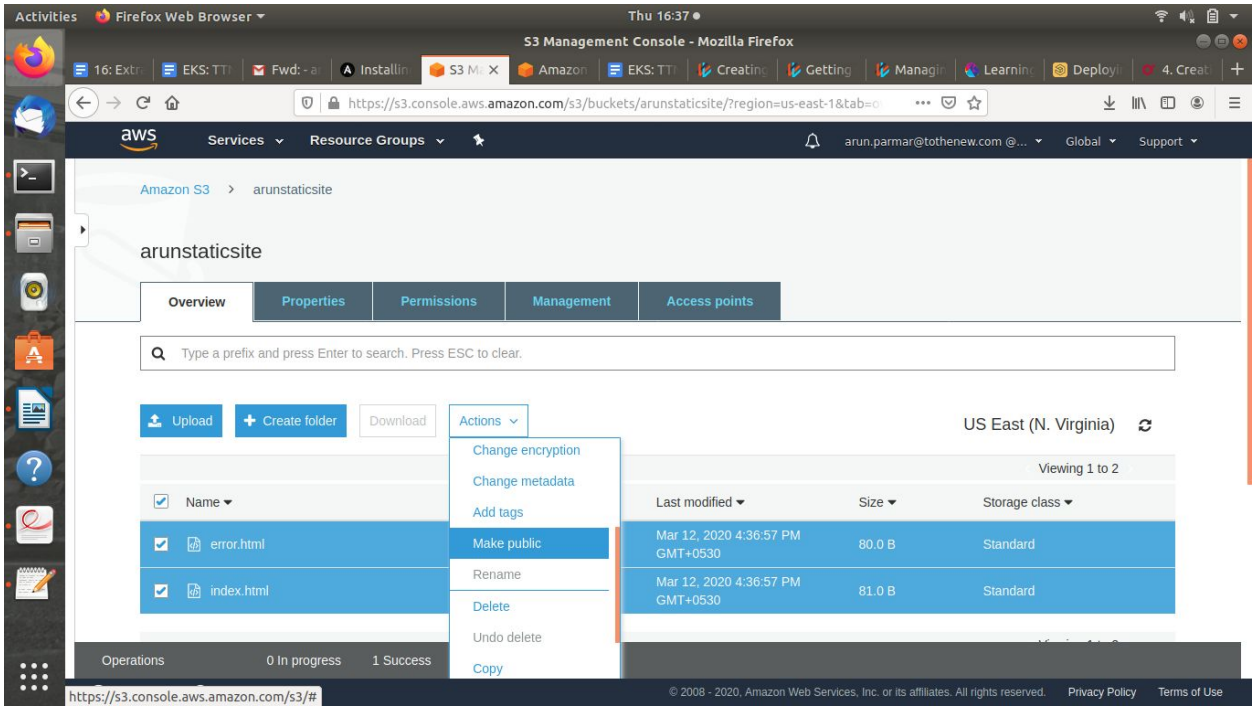
Doubt Resolving

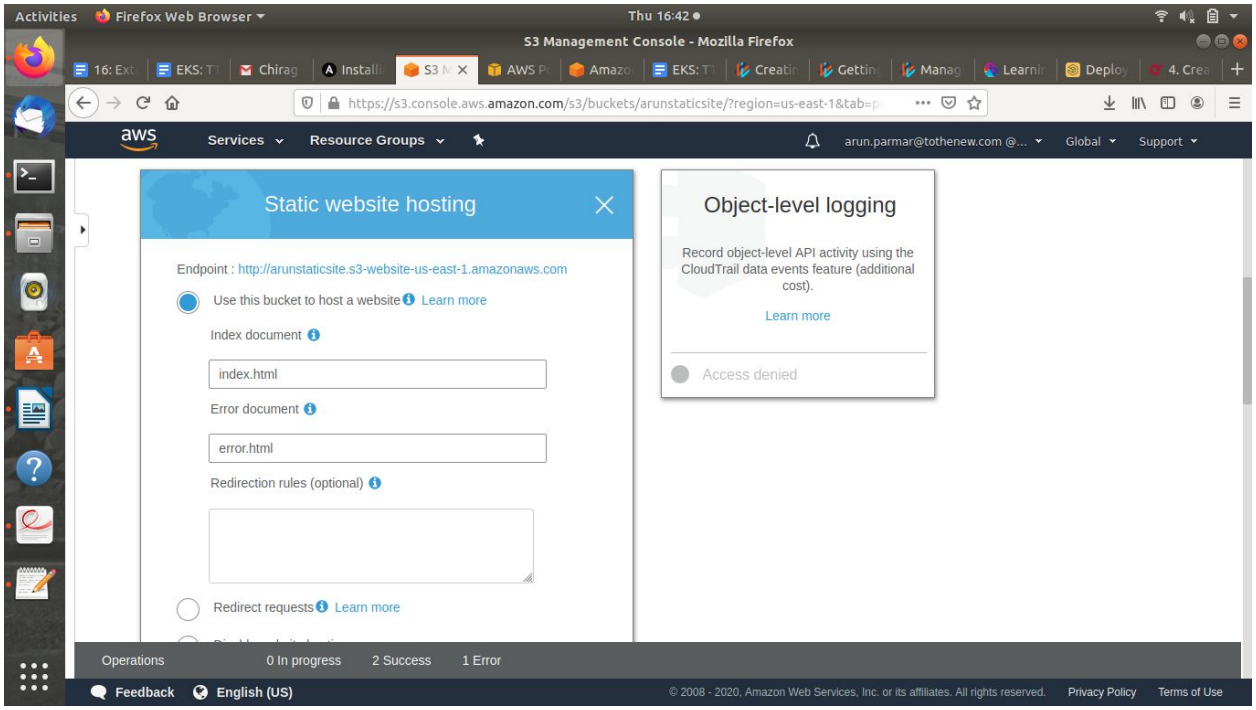
Trainee Name : Arun Parmar
Mentor Name : Ravi Kumar
College: UPES

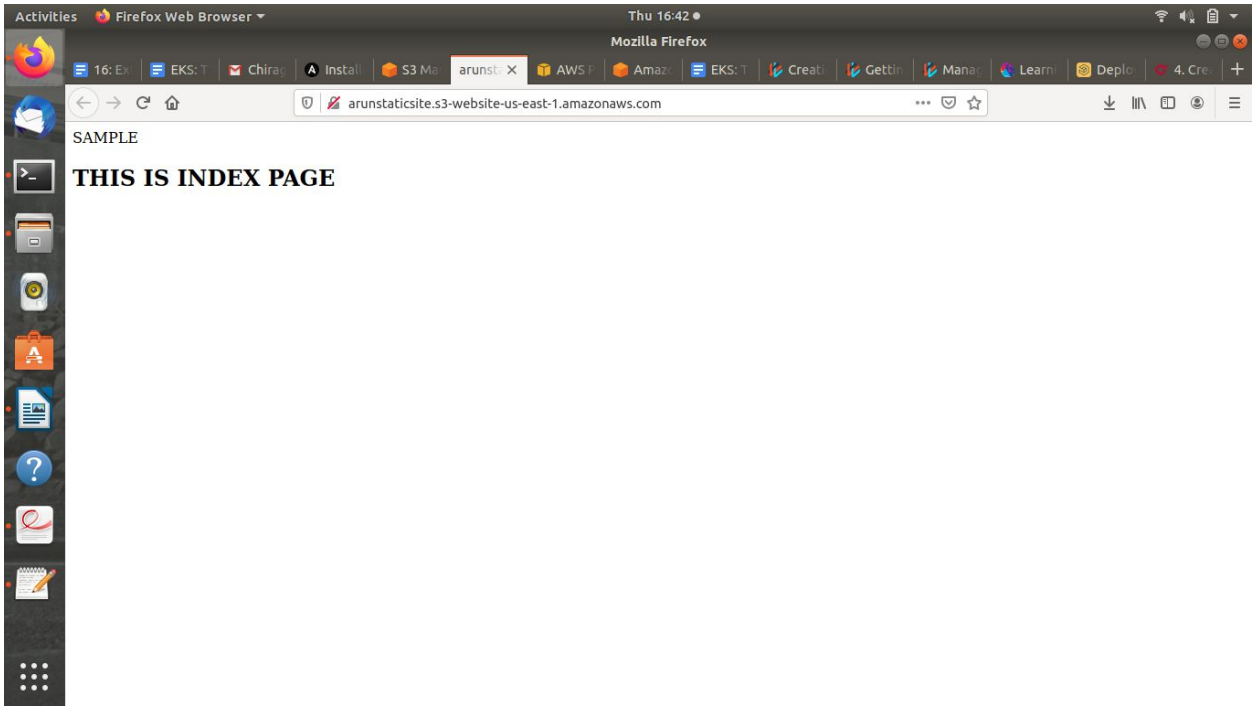
1. Static website hosting using s3(what is index and error page).

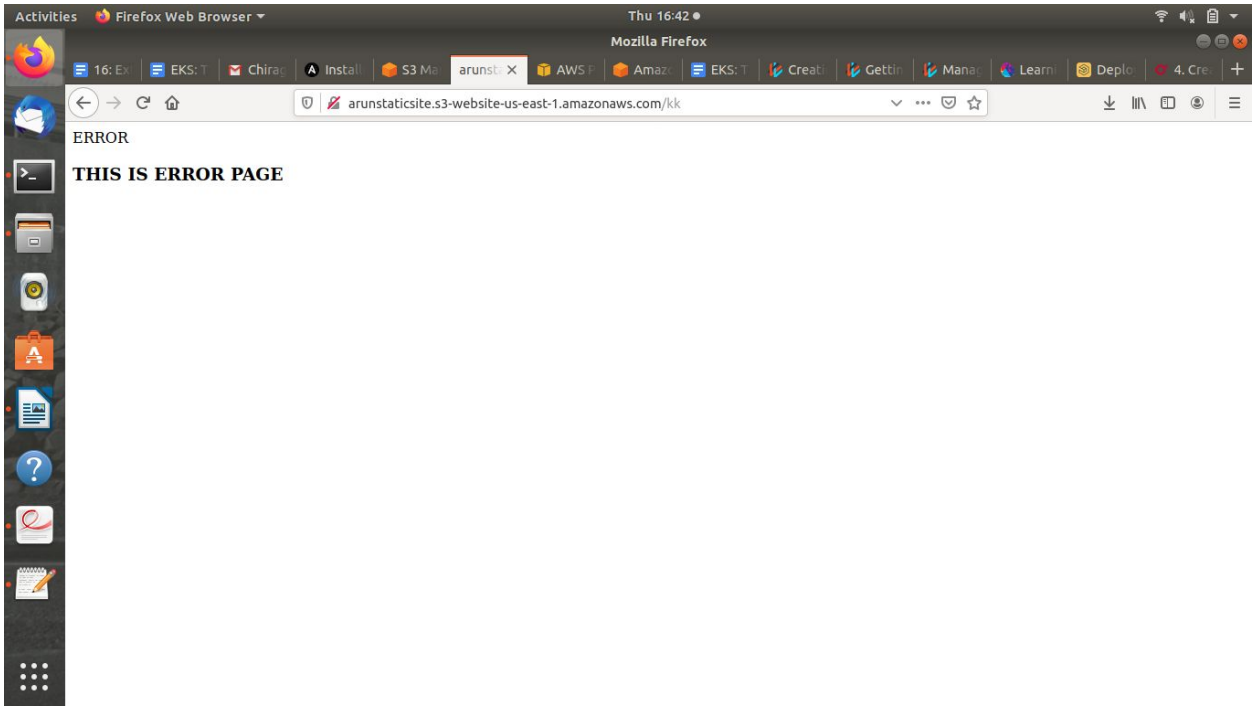

Activities
Firefox Web Browser
Thu 16:35
S3 Management Console - Mozilla Firefox
https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=o
aws
Services
Resource Groups
arun.parmar@tothenew.com @...
Global
Support
Upload
1 Select files
2 Set permissions
3 Set properties
4 Review
2 Files Size: 161.0 B Target path: arunstaticsite
To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more
Add more files
error.html
- 80.0 B
index.html
- 81.0 B
Upload
Next
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


Activities
Firefox Web Browser
Thu 16:37
S3 Management Console - Mozilla Firefox
https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=o
aws
Services
Resource Groups
arun.parmar@tothenew.com @...
Global
Support
arunstaticsite
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 2
Name
Last modified
Size
Storage class
error.html
Mar 12, 2020 4:36:57 PM GMT+0530
80.0 B
Standard
index.html
Mar 12, 2020 4:36:57 PM GMT+0530
81.0 B
Standard
Viewing 1 to 2
Operations
0 In progress
1 Success
1 Error
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


Activities
Firefox Web Browser
Thu 16:37
S3 Management Console - Mozilla Firefox
https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=o
aws
Services
Resource Groups
arun.parmar@tothenew.com @...
Global
Support
Amazon S3 › arunstaticsite
arunstaticsite
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)
Change encryption
Change metadata
Add tags
Make public
Rename
Delete
Undo delete
Copy
Viewing 1 to 2
Name
Last modified
Size
Storage class
error.html
Mar 12, 2020 4:36:57 PM GMT+0530
80.0 B
Standard
index.html
Mar 12, 2020 4:36:57 PM GMT+0530
81.0 B
Standard
Operations
0 In progress
1 Success
https://s3.console.aws.amazon.com/s3/#
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

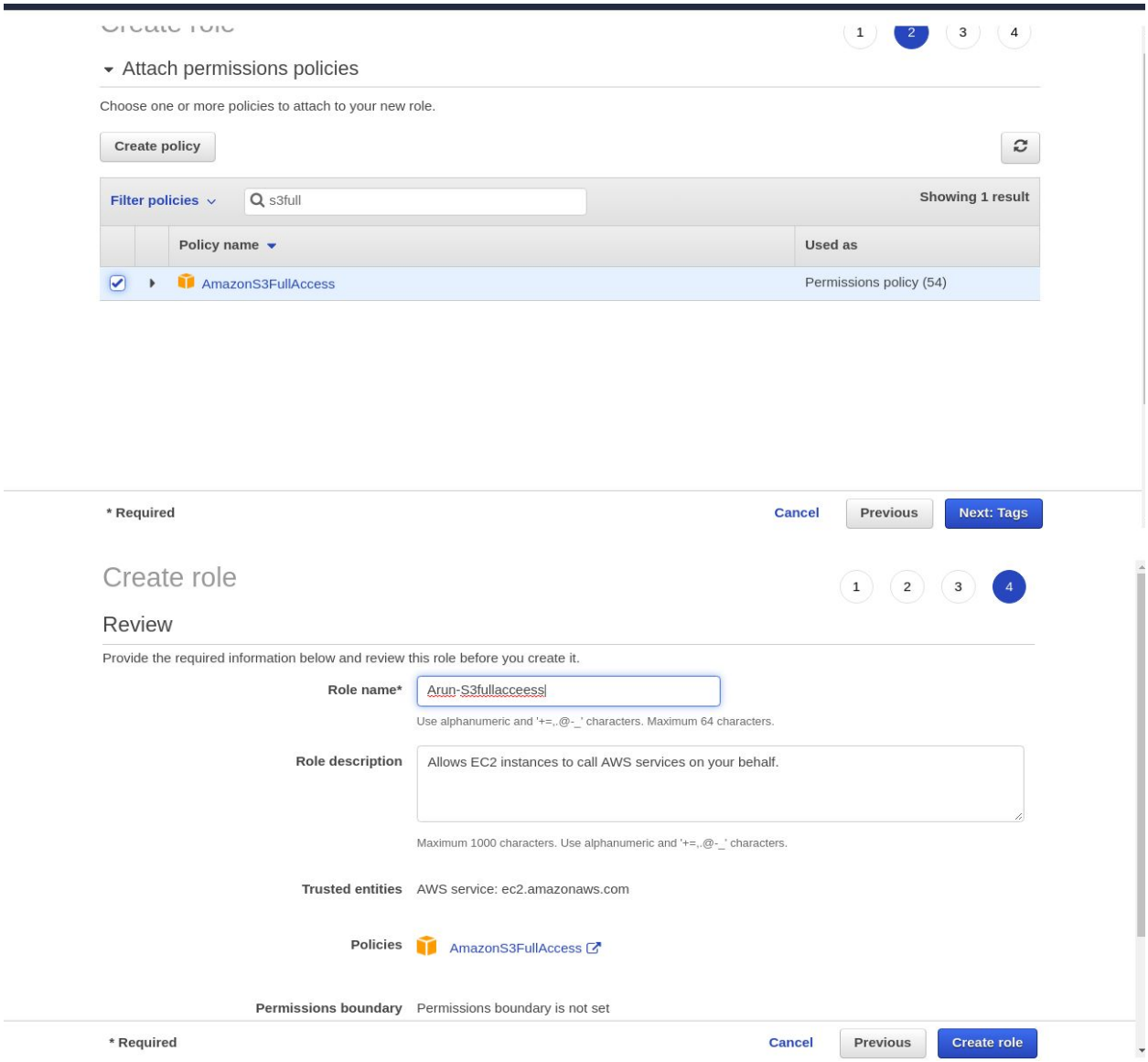

Activities
Firefox Web Browser
Thu 16:42
S3 Management Console - Mozilla Firefox
https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=p
aws
Services
Resource Groups
arun.parmar@tothenew.com @...
Global
Support
Static website hosting
Endpoint : http://arunstaticsite.s3-website-us-east-1.amazonaws.com
Use this bucket to host a website
Learn more
Index document
index.html
Error document
error.html
Redirection rules (optional)
Redirect requests
Learn more
Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more
Access denied
Operations
0 In progress
2 Success
1 Error
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



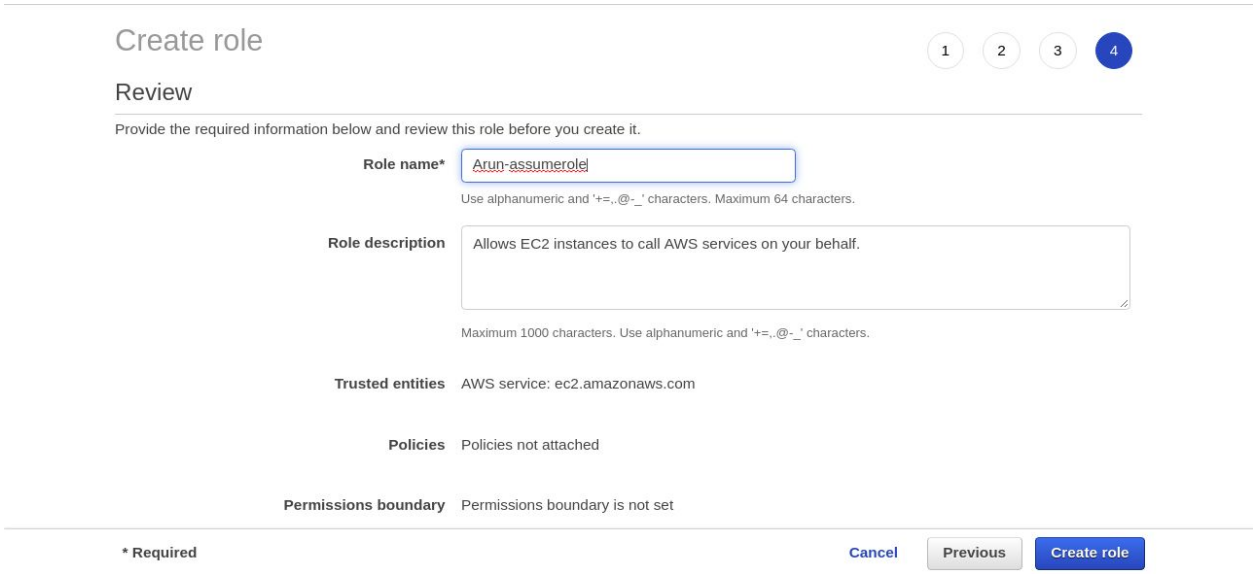


2. Create an assume role to access s3 using ec2.

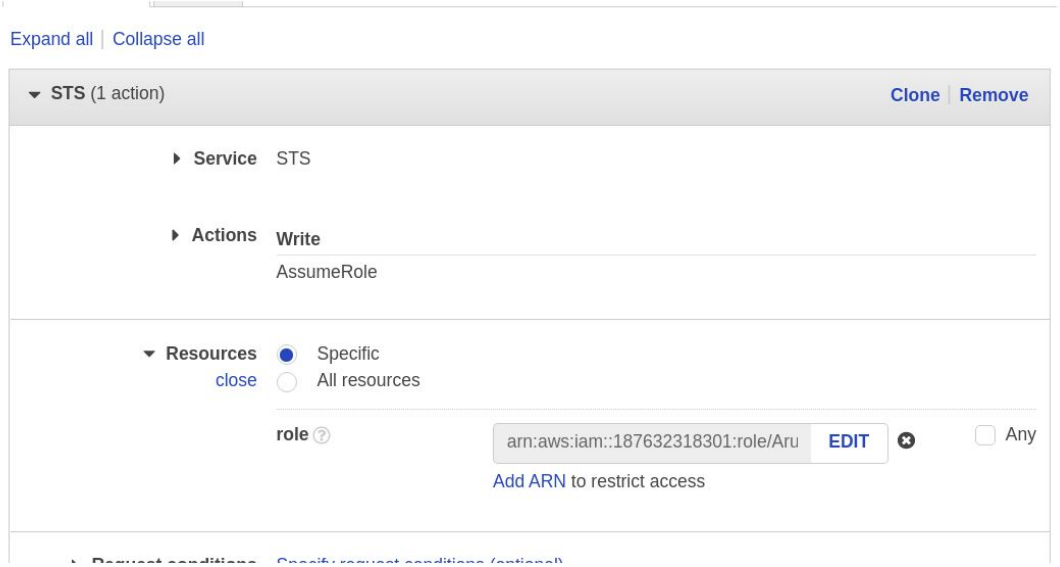
- Create a role with full access to S3

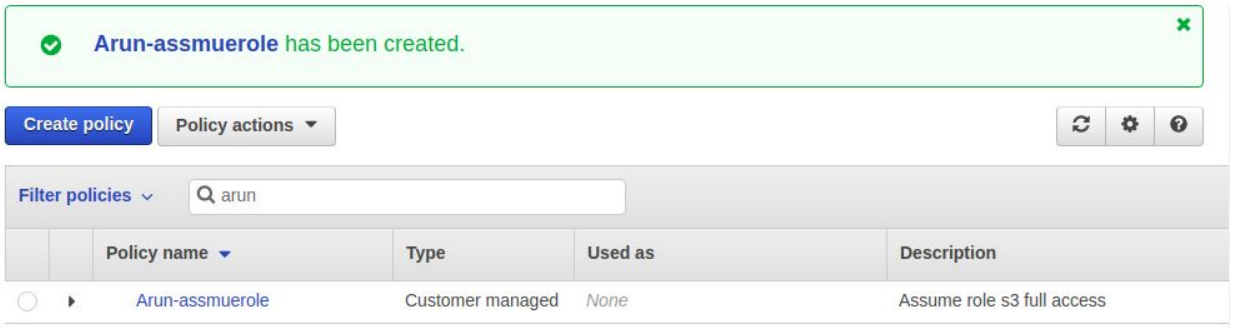


- Create a new role

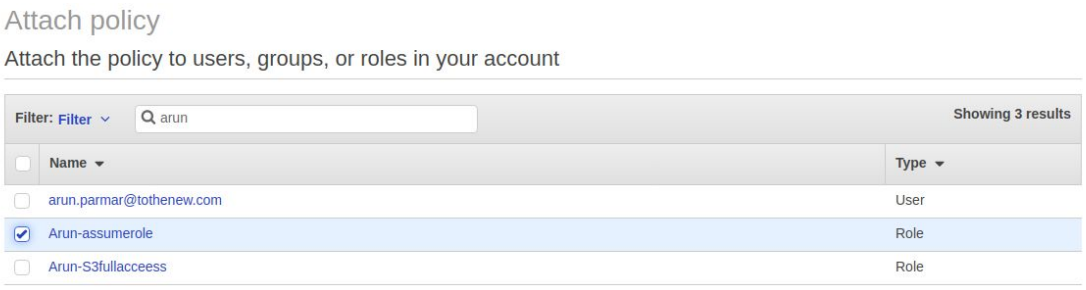


- Create a new policy
- Select service STS and action assume role
- Go to resources(specific) and Copy the ARN of s3 full access and paste

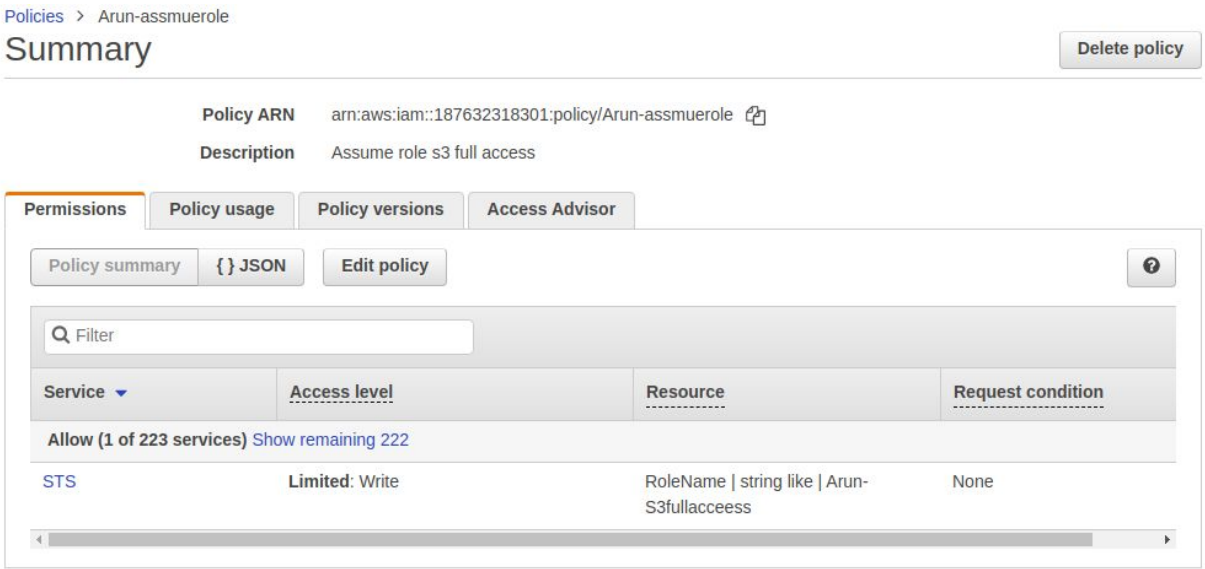




- Attach this policy to the newly created role



- Now open the newly created role and check for the assume role



- Go to the newly created role(assumerole-Arun) and copy the ARN. Now go to the old role(ArunS3fullaccess) and edit trust relationships. Then paste the ARN as follows.

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::187632318301:role/Arun-assumerole",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Cancel | Update Trust Policy

Role ARN	arn:aws:iam::187632318301:role/Arun-S3fullacceess
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/Arun-S3fullacceess
Path	/
Creation time	2020-03-01 16:39 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 document

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

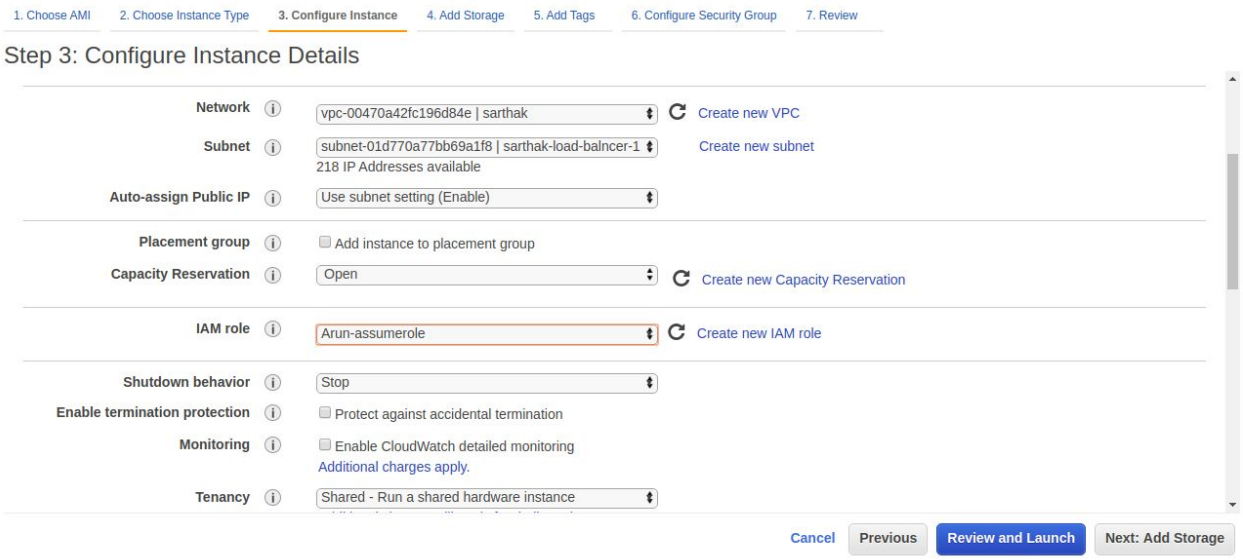
Trusted entities
arn:aws:iam::187632318301:role/Arun-assumerole
The identity provider(s) ec2.amazonaws.com

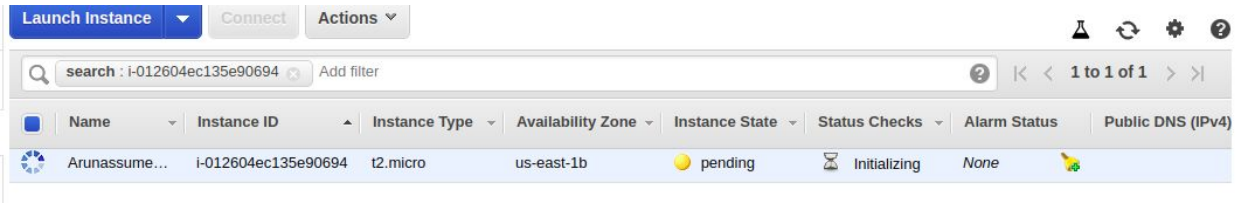
Conditions

The following conditions define how and when trusted entities can assume the role.

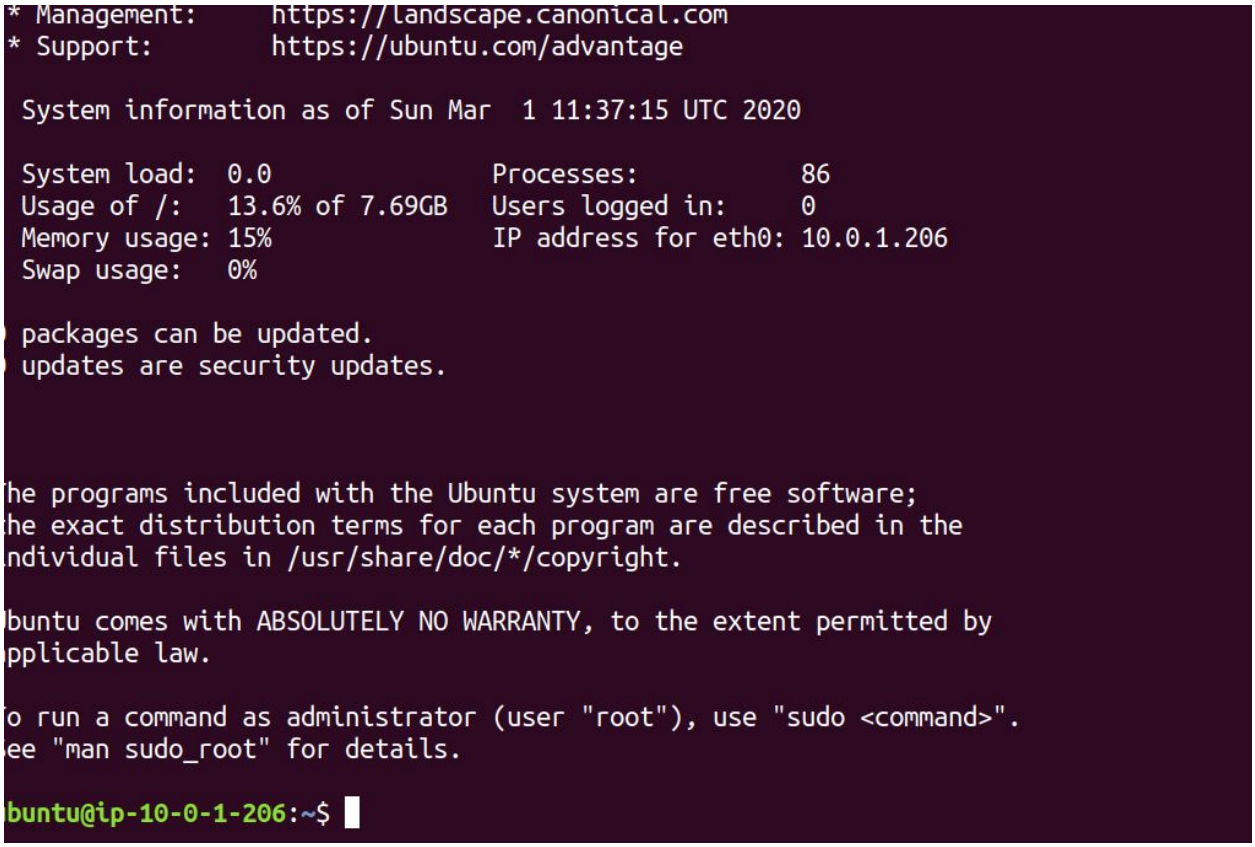
There are no conditions associated with this role.

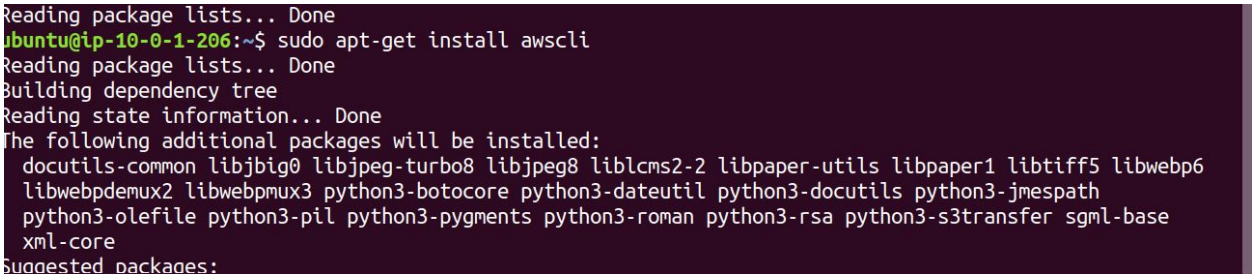
- Create a new instance and then attach the new role(Arun-assumerole)





- SSh into the instance and install awscli





- Now execute the following command :aws sts assume-role --role-arn arn:aws:iam::187632318301:role/Arun-S3fullacceess --role-session-name Arunrole to generate the sts token.

```
ubuntu@ip-10-0-1-206:~$ aws sts assume-role --role-arn arn:aws:iam::187632318301:role/Arun-S3fullacceess --
role-session-name Arunrole
{
    "Credentials": {
        "AccessKeyId": "ASIASXL6B65OTFJOKBFD",
        "SecretAccessKey": "hUQiujVhLAHB1ttKj+3wA2icHtQZgihyflORfg9x",
        "SessionToken": "FwoGZXIvYXdzEE0aDAT146aDaWap7t6EbCKsAUl0rz6Q+Zvy1e+wTMSXNgaPqX5QbYpjcxqyKAZzsydu/D
NZMGAYWglpBtMyxu8bjsD3X2ebjQ8p3/fGqizO8o9rMt9LkUwnCS1rsOsFKA1tAd8ir4wnE0AcnIsAfwOXB7CMjz82WjqeTxSnnoLEoAL/e
/YrPfdFX5cdnJnVmKXy7Am2HOF3xV+/n2gvE5rShvwvDjLYM1GJ+WDXg2e2ve/jVO/5Y+vs+43oPwEov77u8gUyLQpZ+a5LTHcs3LpHp8eS
DKJtC+AQa0MqSGWt3nudcmtKffXmRRhF6bGTaoazgQ==",
        "Expiration": "2020-03-01T12:40:47Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROASXL6B65O4QSUNDFSJ:Arunrole",
        "Arn": "arn:aws:sts::187632318301:assumed-role/Arun-S3fullacceess/Arunrole"
    }
}
ubuntu@ip-10-0-1-206:~$
```

- Now export variables:

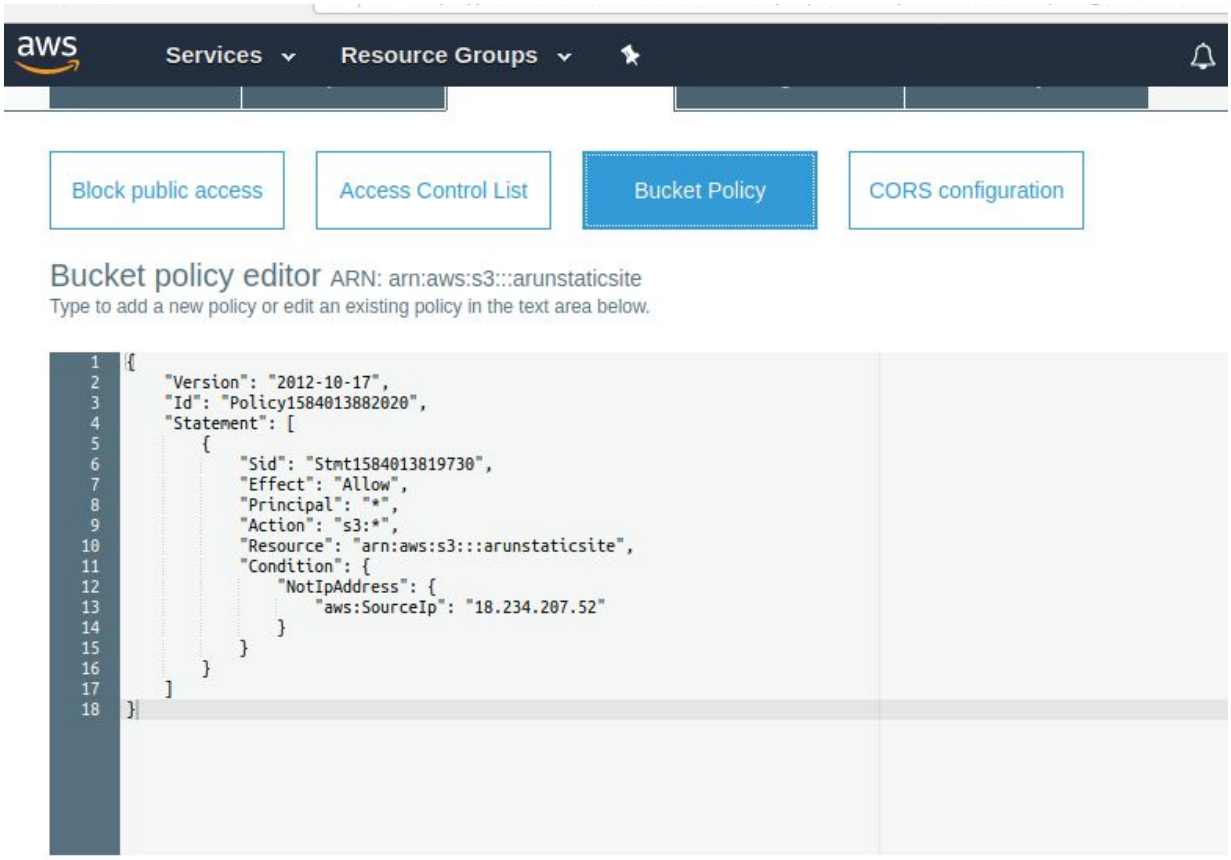
```
ubuntu@ip-10-0-1-206:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B65OTFJOKBFD
ubuntu@ip-10-0-1-206:~$ export AWS_SECRET_ACCESS_KEY=hUQiujVhLAHB1ttKj+3wA2icHtQZgihyflORfg9x
ubuntu@ip-10-0-1-206:~$ export AWS_SECRET_ACCESS_KEY_ID=hUQiujVhLAHB1ttKj+3wA2icHtQZgihyflORfg9x
ubuntu@ip-10-0-1-206:~$ export AWS_SECRET_ACCESS_KEY=hUQiujVhLAHB1ttKj+3wA2icHtQZgihyflORfg9x
ubuntu@ip-10-0-1-206:~$ export AWS_SESSION_TOKEN=FwoGZXIvYXdzEE0aDAT146aDaWap7t6EbCKsAUl0rz6Q+Zvy1e+wTMSXNg
aPqX5QbYpjcxqyKAZzsydu/DNZMGAYWglpBtMyxu8bjsD3X2ebjQ8p3/fGqizO8o9rMt9LkUwnCS1rsOsFKA1tAd8ir4wnE0AcnIsAfwOXB
7CMjz82WjqeTxSnnoLEoAL/e/YrPfdFX5cdnJnVmKXy7Am2HOF3xV+/n2gvE5rShvwvDjLYM1GJ+WDXg2e2ve/jVO/5Y+vs+43oPwEov77u
8gUyLQpZ+a5LTHcs3LpHp8eSDKJtC+AQa0MqSGWt3nudcmtKffXmRRhF6bGTaoazgQ==
```

- Now we can list all s3 buckets:

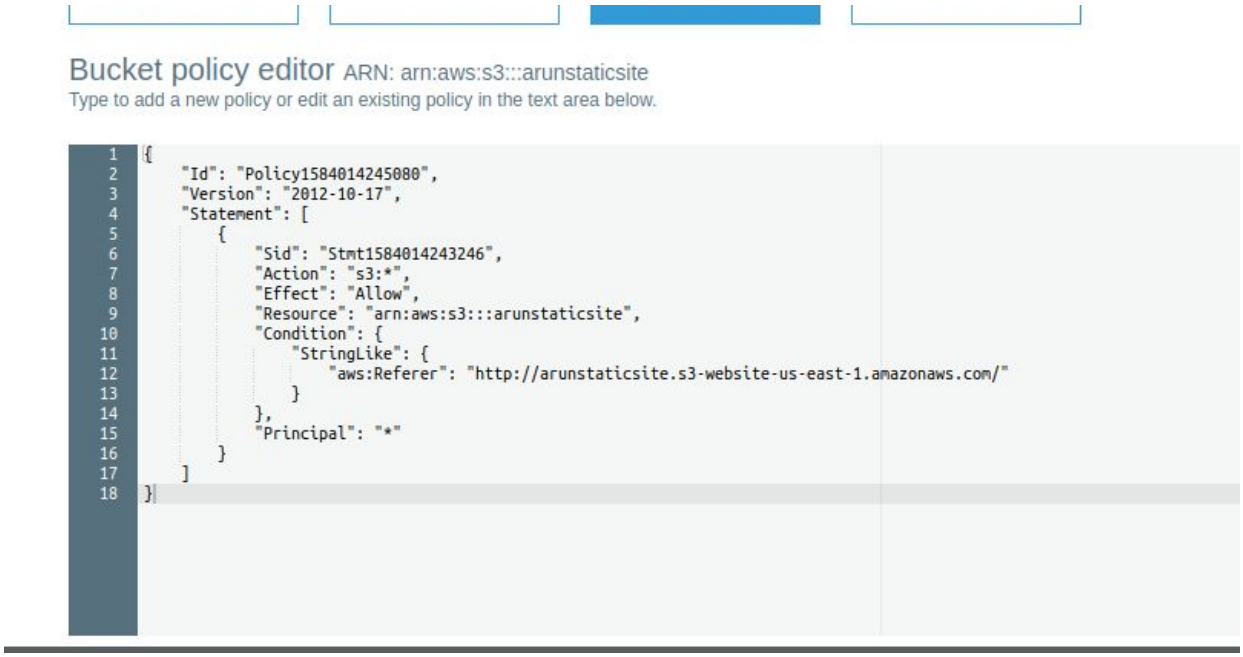
```
ubuntu@ip-10-0-1-206:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-02-28 10:55:02 abhishek-bootcamp
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-02-26 16:26:29 akshaybuck1
```

3. Block s3 access on the basis of:

i. IP



ii. Domain



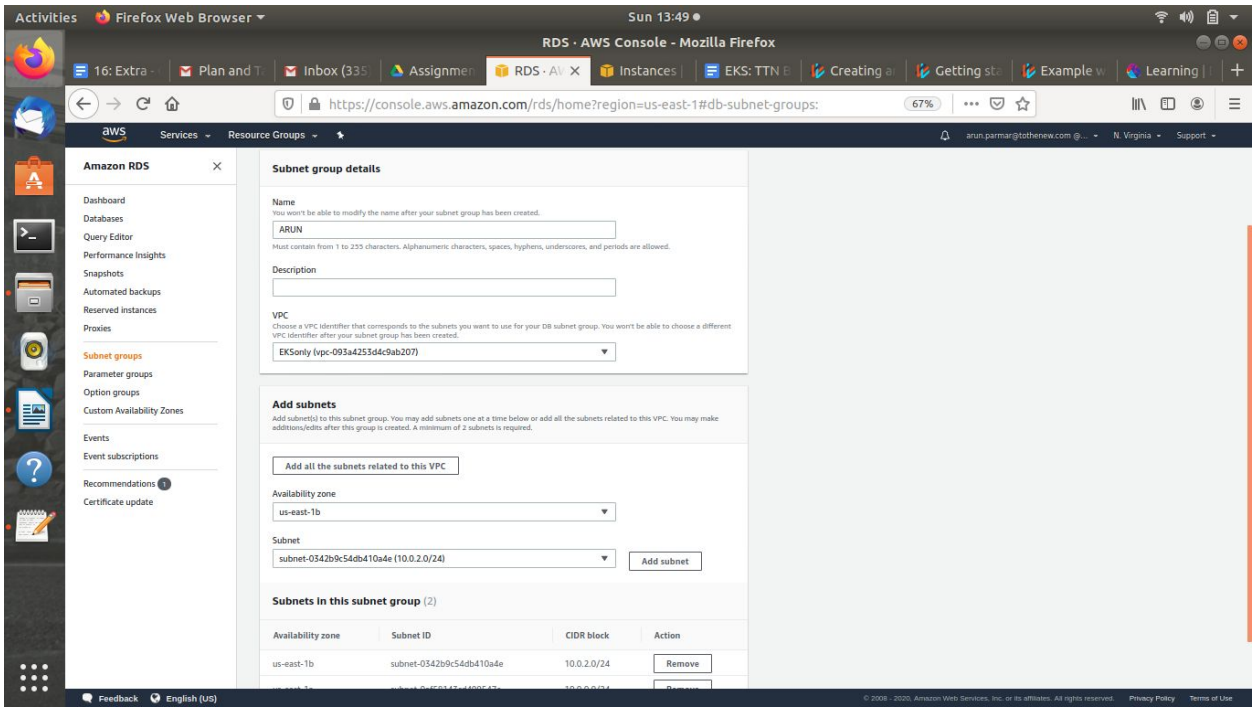
iii. Pre-signed URL(Time based)

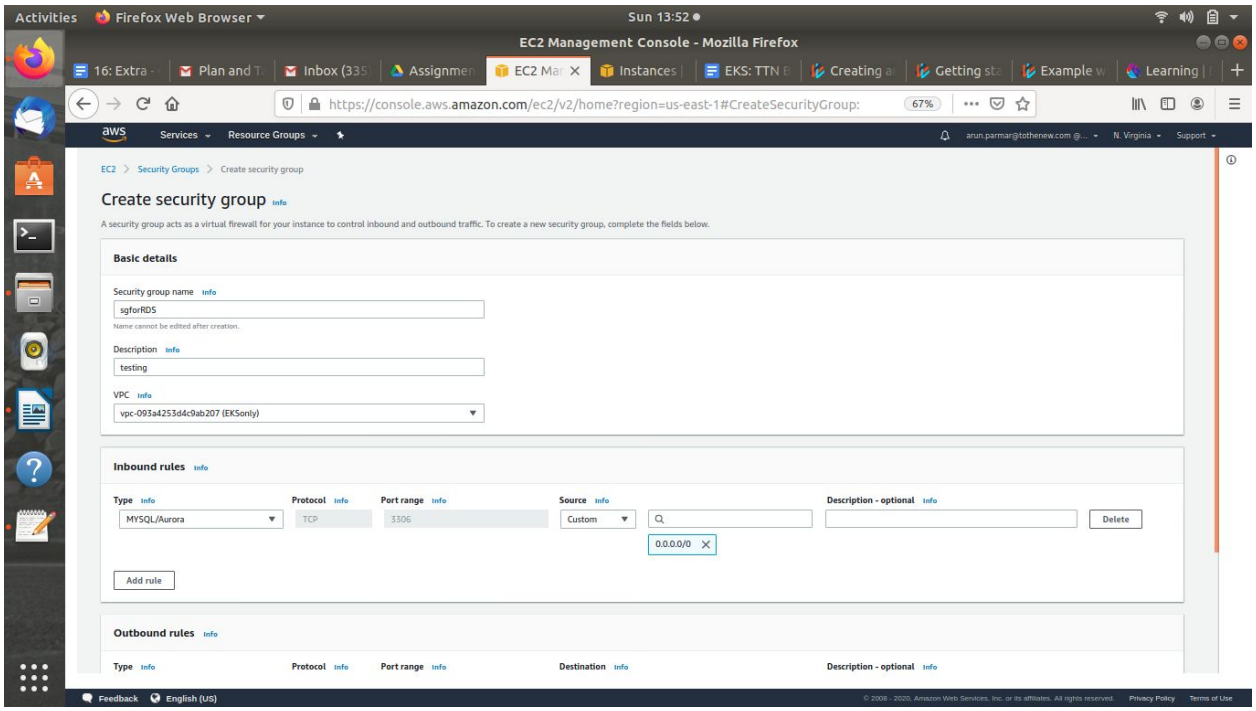
A presigned URL is a URL that you can provide to your users to grant temporary access to a specific S3 object.

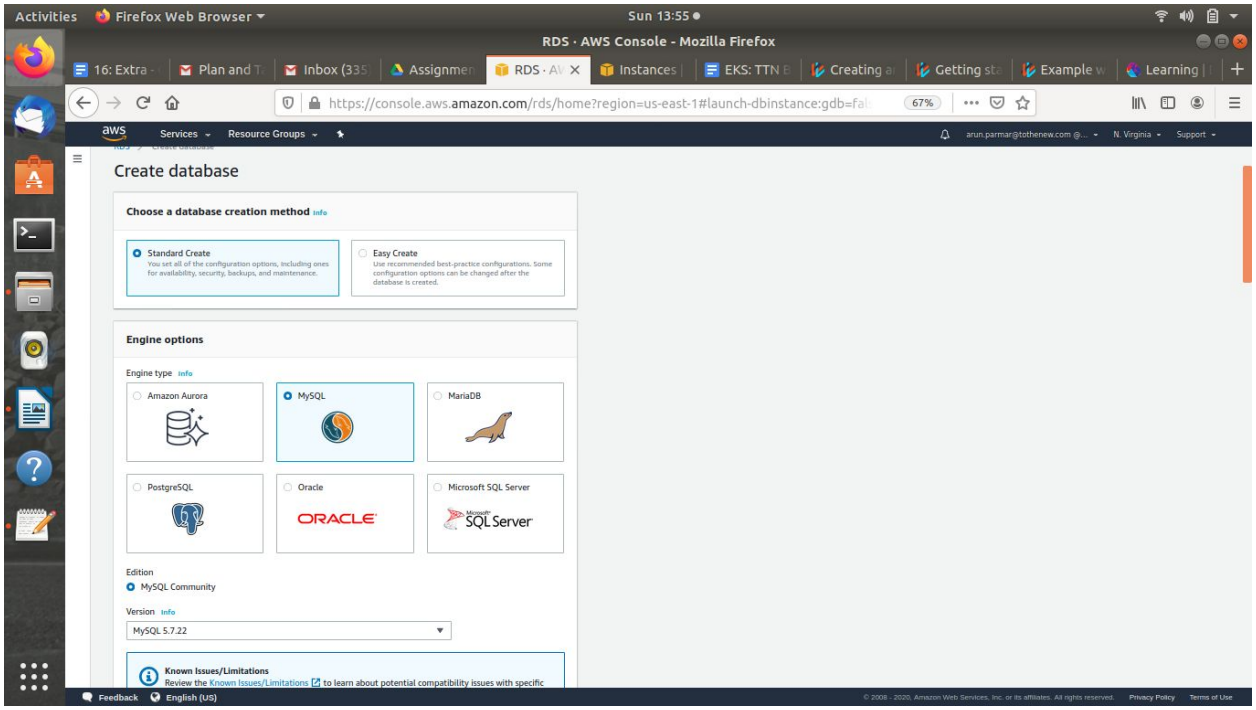
A pre-signed URL uses three parameters to limit the access to the user;

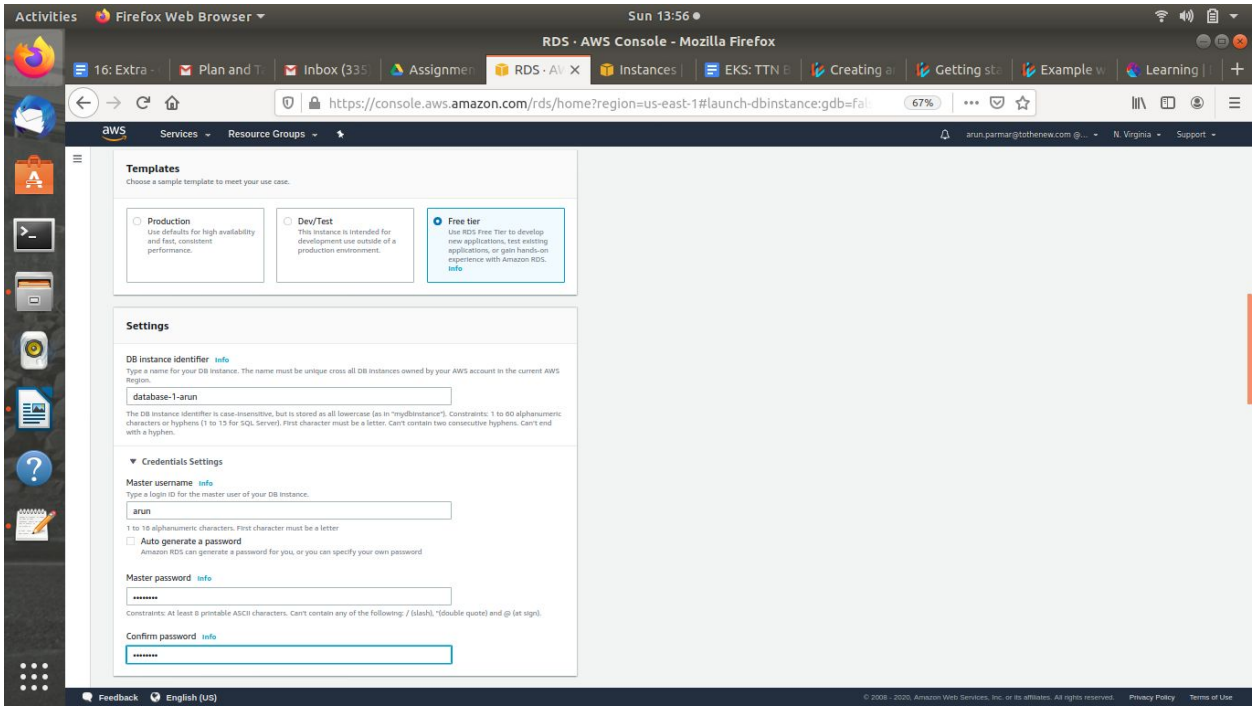
- Bucket: The bucket that the object is in (or will be in)
- Key : The name of the object.
- Expires: The amount of time that the URL is valid.

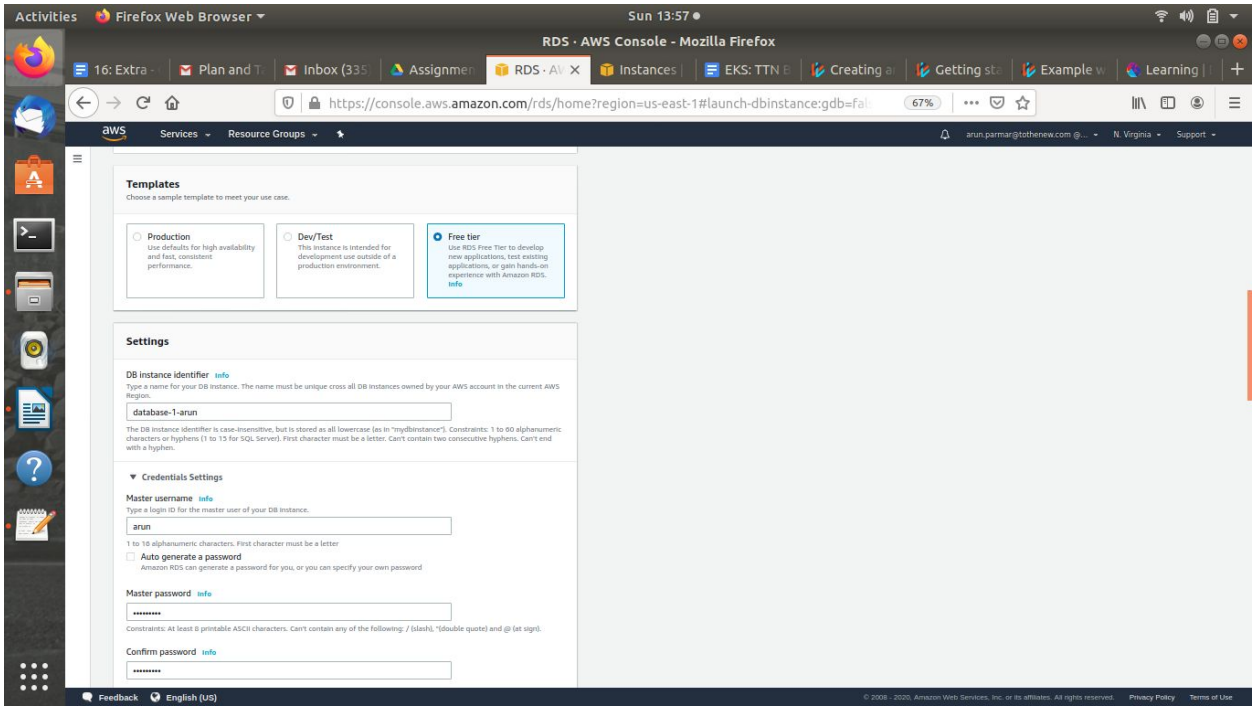
4. Create RDS subnet and launch RDS instance, what is parameter group and option group?

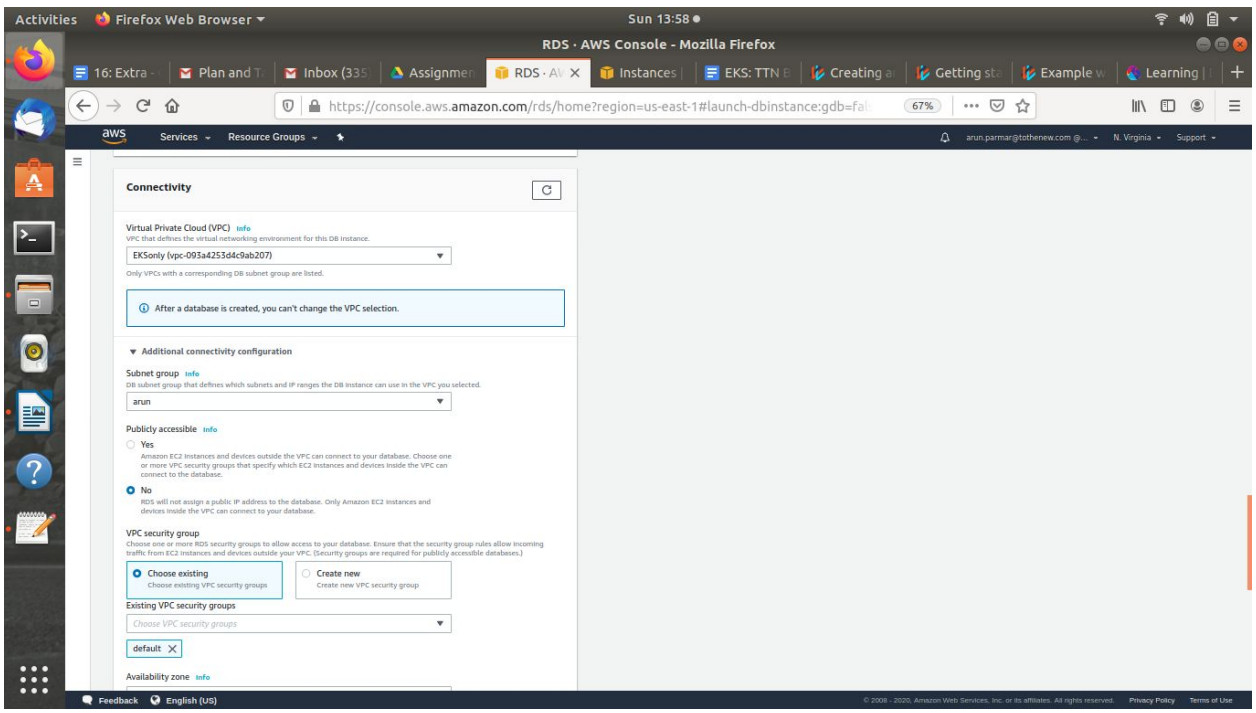

Activities
Firefox Web Browser
Sun 13:49
RDS · AWS Console - Mozilla Firefox
https://console.aws.amazon.com/rds/home?region=us-east-1#db-subnet-groups:
Services
Resource Groups
Amazon RDS
Dashboard
Databases
Query Editor
Performance Insights
Snapshots
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Custom Availability Zones
Events
Event subscriptions
Recommendations
Certificate update
Subnet group details
Name
ARUN
Description
VPC
EKSonly (vpc-093a4253d4c9ab207)
Add subnets
Add all the subnets related to this VPC
Availability zone
us-east-1b
Subnet
subnet-0342b9c54db410a4e (10.0.2.0/24)
Add subnet
Subnets in this subnet group (2)
Availability zone
Subnet ID
CIDR block
Action
us-east-1b
subnet-0342b9c54db410a4e
10.0.2.0/24
Remove
Feedback
English (US)


Activities
Firefox Web Browser
Sun 13:52
EC2 Management Console - Mozilla Firefox
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
Services
Resource Groups
EC2
Security Groups
Create security group
Create security group
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name
sgforRDS
Name cannot be edited after creation.
Description
testing
VPC
vpc-093a4253d4c9ab207 (EKSonly)
Inbound rules
Type
Protocol
Port range
Source
Description - optional
MYSQL/Aurora
TCP
3306
Custom
0.0.0.0/0
Delete
Add rule
Outbound rules
Type
Protocol
Port range
Destination
Description - optional
Feedback
English (US)


Activities
Firefox Web Browser
Sun 13:55
RDS · AWS Console - Mozilla Firefox
https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal
aws
Services
Resource Groups
N. Virginia
Support
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
PostgreSQL
Oracle
Microsoft SQL Server
Edition
MySQL Community
Version info
MySQL 5.7.22
Known Issues/Limitations
Review the Known Issues/Limitations to learn about potential compatibility issues with specific
Feedback
English (US)
Privacy Policy
Terms of Use


Activities
Firefox Web Browser
Sun 13:56
RDS · AWS Console - Mozilla Firefox
https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal
aws
Services
Resource Groups
N. Virginia
Support
Templates
Choose a sample template to meet your use case.
Production
Use defaults for high availability and fast, consistent performance.
Dev/Test
This instance is intended for development use outside of a production environment.
Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
info
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.
database-1-arun
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.
arun
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
Feedback
English (US)
Privacy Policy
Terms of Use


Activities
Firefox Web Browser
Sun 13:57
RDS · AWS Console - Mozilla Firefox
https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal
aws
Services
Resource Groups
N. Virginia
Support
Templates
Choose a sample template to meet your use case.
Production
Use defaults for high availability and fast, consistent performance.
Dev/Test
This instance is intended for development use outside of a production environment.
Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
Info
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.
database-1-arun
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.
arun
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
Feedback
English (US)
Privacy Policy
Terms of Use


Activities
Firefox Web Browser
Sun 13:58
RDS · AWS Console - Mozilla Firefox
https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal
aws
Services
Resource Groups
N. Virginia
Support
Connectivity
Virtual Private Cloud (VPC) Info
VPC that defines the virtual networking environment for this DB instance.
EKSonly (vpc-093a4253d4c9ab207)
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.
arun
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
default
Availability zone Info
Feedback
English (US)
Privacy Policy
Terms of Use

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.

Amazon RDS supports options for the following database engines:

Database Engine	Relevant Documentation
`MariaDB`	Options for MariaDB Database Engine
`Microsoft SQL Server`	Options for the Microsoft SQL Server Database Engine
`MySQL`	Options for MySQL DB Instances
`Oracle`	Options for Oracle DB Instances

5. Short Note on ACL, Bucket policy, IAM Policy.

The Access Control List (ACL): is used to define other users' access permissions for your file and folder objects. The Access Permissions that you set using the ACL determine what a user can and cannot do with your file and folder objects. For example, you can set permissions on a file object to let one user read the contents of a file (read

access) and let another user make changes to the file (write access). In Amazon S3 you will first add grants to objects and then set the permissions for the grant.

There are 4 types of grants:

1. An Owner grant - which defines the permissions the owner of the object has.

2. Authenticated Users – which are all Amazon S3 storage users that have an account with S3.

3. Public – which means any anonymous user that you have provided the URL to.

4. Email-ID – which is an email address of specific S3 customers that have S3 accounts, not general public emails. The email given must match exactly the email address the S3 user signed up with and can only match one user account.

Bucket Policies: bucket Policies are similar to IAM policies in that they allow access to resources via a JSON script. However, Bucket policies are applied to Buckets in S3, where as IAM policies are assigned to user/groups/roles and are used to govern access to any AWS resource through the IAM service.

When a bucket policy is applied the permissions assigned apply to all objects within the Bucket. The policy will specify which 'principles' (users) are allowed to access which resources. The use of Principles within a Bucket policy differs from IAM policies, Principles within IAM policies are defined by who is associated to that policy via the user and group element. As Bucket policies are assigned to Buckets, there is this need of an additional requirement of 'Principles'.

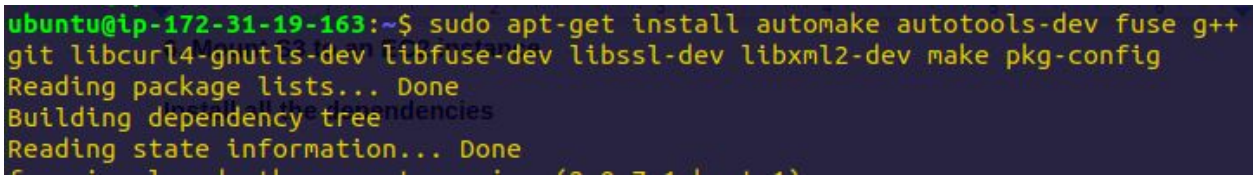
IAM POLICY :A policy is an entity that, when attached to an identity or resource, defines their permissions. A policy that is attached to an identity in IAM is known as an *identity-based policy*. Identity-based policies can include AWS managed policies, customer managed policies, and inline policies. AWS managed policies are created and managed by AWS. You can use them, but you can't manage them. An inline policy is one that you create and embed directly to an IAM group, user, or role. Inline policies can't be reused on other identities or managed outside of the identity where it exists.

6. Mount S3 to an EC2 instance

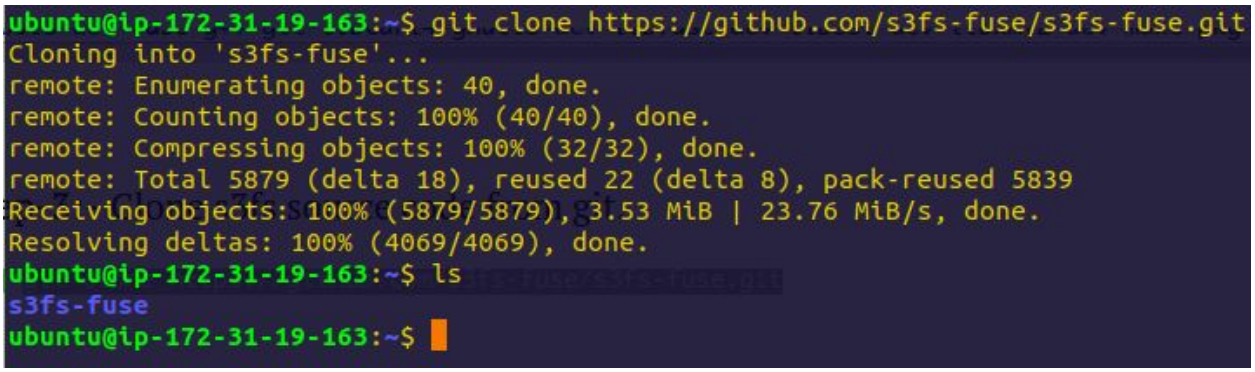
A S3 bucket can be mounted in a AWS instance as a file system known as S3fs. S3fs is a FUSE file-system that allows you to mount an Amazon S3 bucket as a local file-system. It behaves like a network attached drive, as it does not store anything on the Amazon EC2, but user can access the data on S3 from EC2 instance.

Filesystem in Userspace (FUSE) is a simple interface for userspace programs to export a virtual file-system to the Linux kernel. It also aims to provide a secure method for non privileged users to create and mount their own file-system implementations.

Install all the dependencies



Clone s3fs code from git



Now change to source code directory, and compile and install the code

```
ubuntu@ip-172-31-19-163:~$ 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 | 23.30 MiB/s, done.
Resolving deltas: 100% (4069/4069), done.
ubuntu@ip-172-31-19-163:~$ cd s3fs-fuse/
ubuntu@ip-172-31-19-163:~/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'
```

```
ubuntu@ip-172-31-19-163:~/s3fs-fuse$ ./configure --prefix=/usr --with-opens
sl
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
```

```
ubuntu@ip-172-31-19-163:~/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_FIL
E_OFFSET_BITS=64 -D_FORTIFY_SOURCE=2 -MT s3fs.o -MD -MP -MF .deps/s3fs.Tpo
```

```
ubuntu@ip-172-31-19-163:~/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'
```

Installation successful

```
ubuntu@ip-172-31-19-163:~/s3fs-fuse$ which s3fs
/usr/bin/s3fs
```

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-172-31-19-163:~$ sudo touch /etc/passwd-s3fs
ubuntu@ip-172-31-19-163:~$ sudo vim /etc/passwd-s3fs
ubuntu@ip-172-31-19-163:~$
```

```
AKIASXL6B65OXF7XHY4K:rqMypbahX9w4uqdqs6m4SolB+21Bz3m/X5Q6L3xV
```

Change the permission of your file

```
ubuntu@ip-172-31-19-163:~$ sudo chmod 640 /etc/passwd-s3fs
```

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

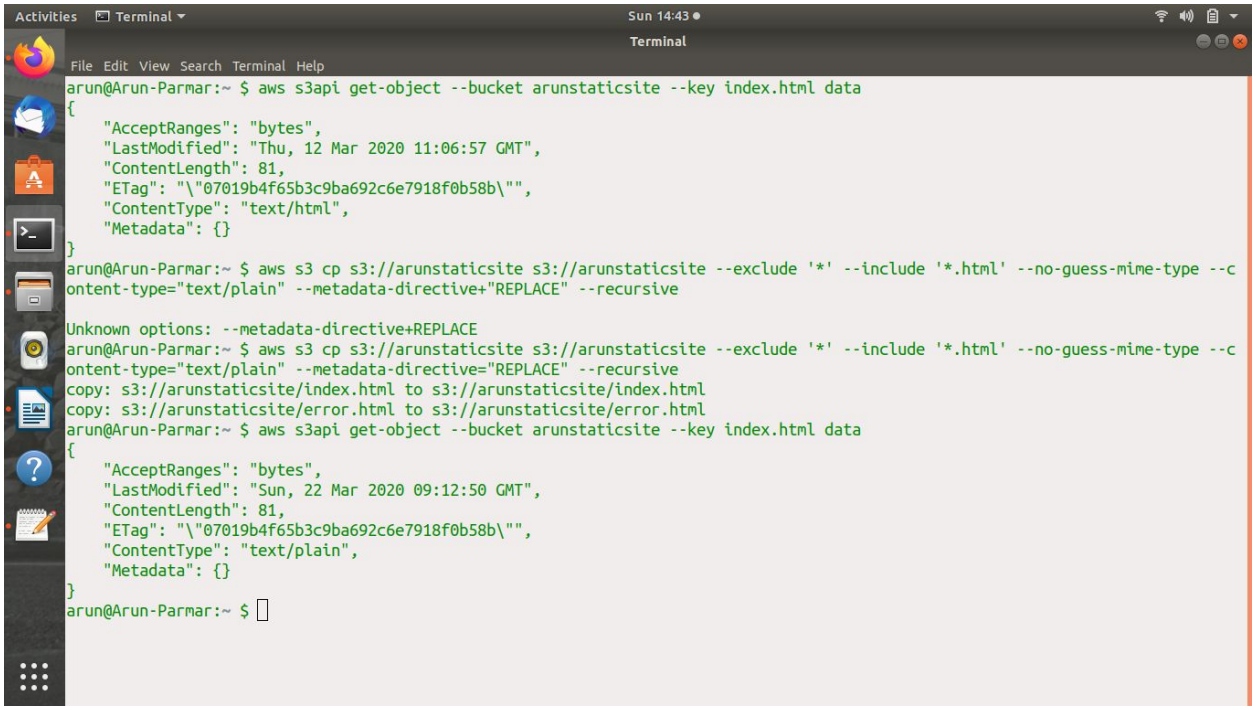
```
ubuntu@ip-172-31-19-163:~$ mkdir /mys3bucket
mkdir: cannot create directory ‘/mys3bucket’: Permission denied
ubuntu@ip-172-31-19-163:~$ sudo !!
sudo mkdir /mys3bucket
```

```
ubuntu@ip-172-31-19-163:~$ sudo s3fs your_bucketname -o use_cache=/tmp -o a
llow_other -o uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket
```

Check the mounted S3 bucket

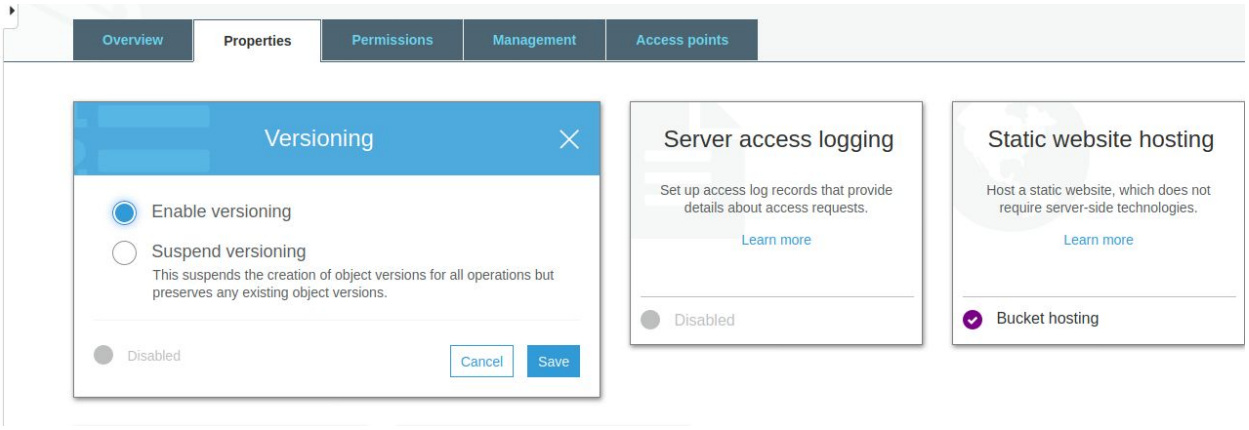
```
ubuntu@ip-172-31-19-163:~$ sudo s3fs srimas3 -o use_cache=/tmp -o allow_other -o
 uid=1001 -o mp_umask=002 -o multireq_max=5 /mys3bucket
ubuntu@ip-172-31-19-163:~$ cd s3fs-fuse/
ubuntu@ip-172-31-19-163:~/s3fs-fuse$ df -Th
Filesystem     Type      Size  Used Avail Use% Mounted on
udev           devtmpfs  481M     0  481M   0% /dev
tmpfs          tmpfs      99M  748K   98M   1% /run
/dev/xvda1     ext4      7.7G  1.6G  6.2G  20% /
tmpfs          tmpfs     492M     0  492M   0% /dev/shm
tmpfs          tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs          tmpfs     492M     0  492M   0% /sys/fs/cgroup
/dev/loop0     squashfs   90M   90M     0 100% /snap/core/8268
/dev/loop1     squashfs   18M   18M     0 100% /snap/amazon-ssm-agent/1480
tmpfs          tmpfs      99M     0   99M   0% /run/user/1000
s3fs           fuse.s3fs  256T     0  256T   0% /mys3bucket
ubuntu@ip-172-31-19-163:~/s3fs-fuse$
```

7.Change content type using S3

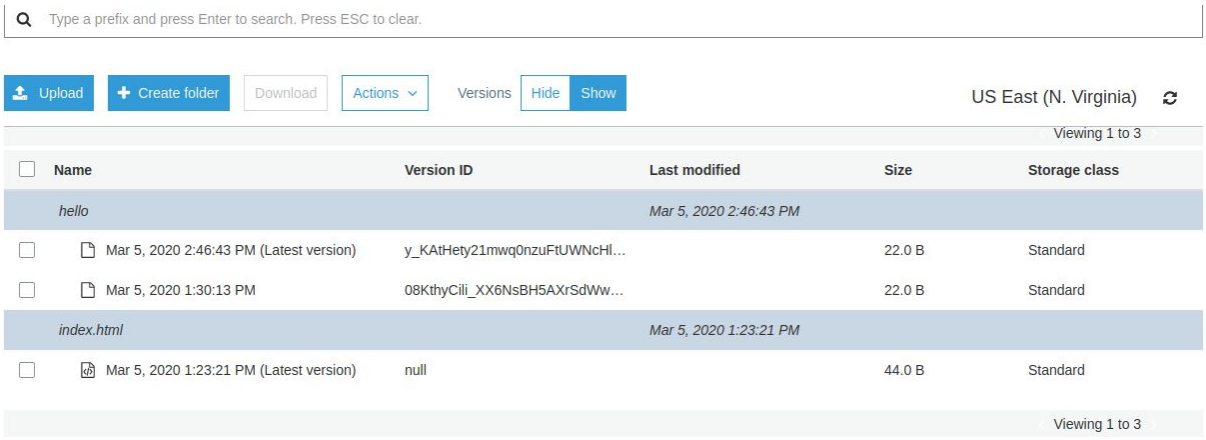


8. Retrieve previous version of S3 (enable versioning).

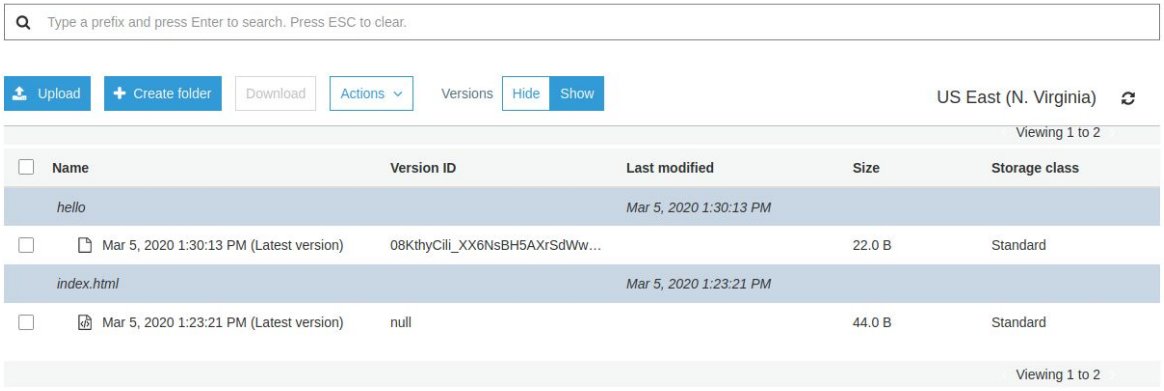
Enable versioning in the bucket



We can see two versions uploaded



Delete the latest version to retrieve previous version.



9. S3 VPC endpoint.

VPC endpoint enables a user to connect with AWS services that are outside the VPC through a private link. VPC endpoints use AWS PrivateLinks in the backend with which users will be able to connect to AWS services without using public IP's. Thus the traffic will not leave the Amazon network. AWS PrivateLinks are highly available, redundant and scalable technology.

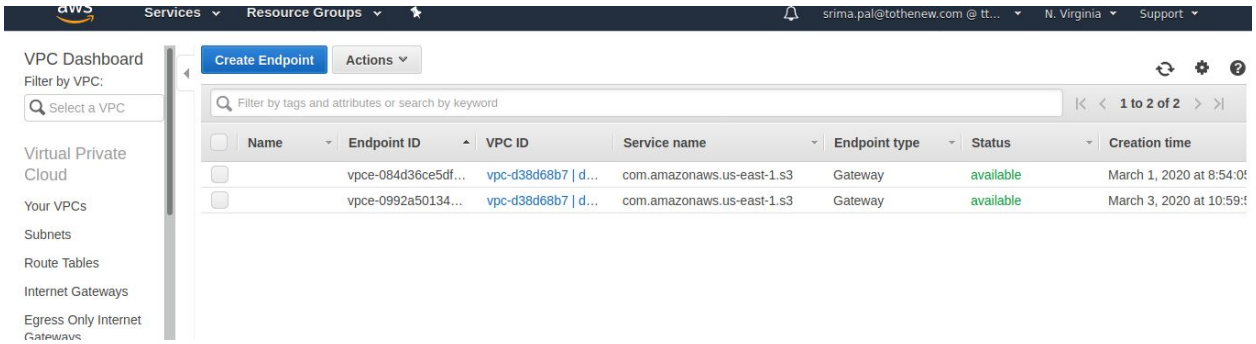
There are two types of VPC endpoints Interface Endpoints and Gateway Endpoints:

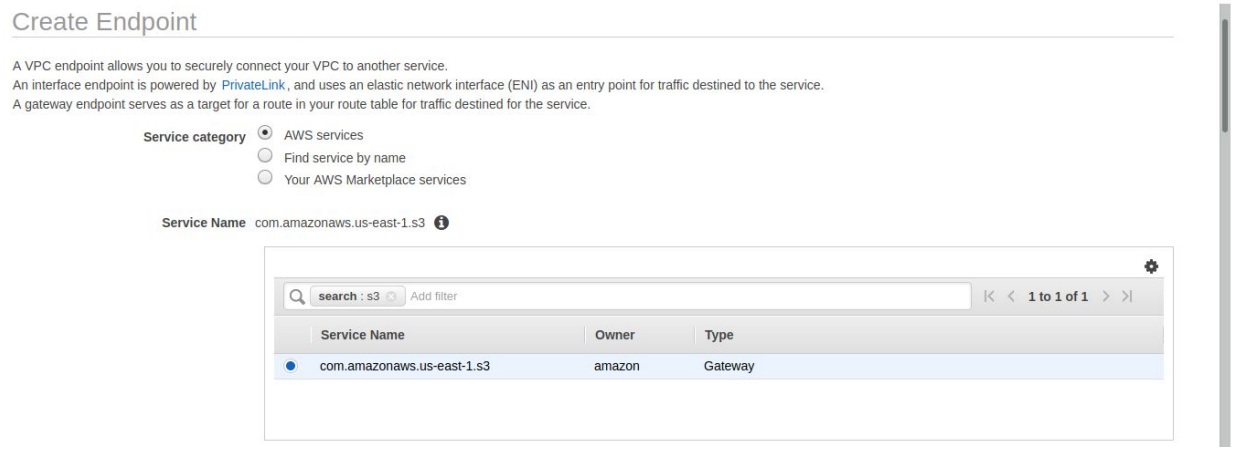
Interface Endpoints are Elastic Network Interfaces (ENI) with private IP addresses. ENI will act as the entry point for the traffic that is destined to a particular service. Services such as Amazon CloudWatch Logs, Amazon SNS, etc. are supported.

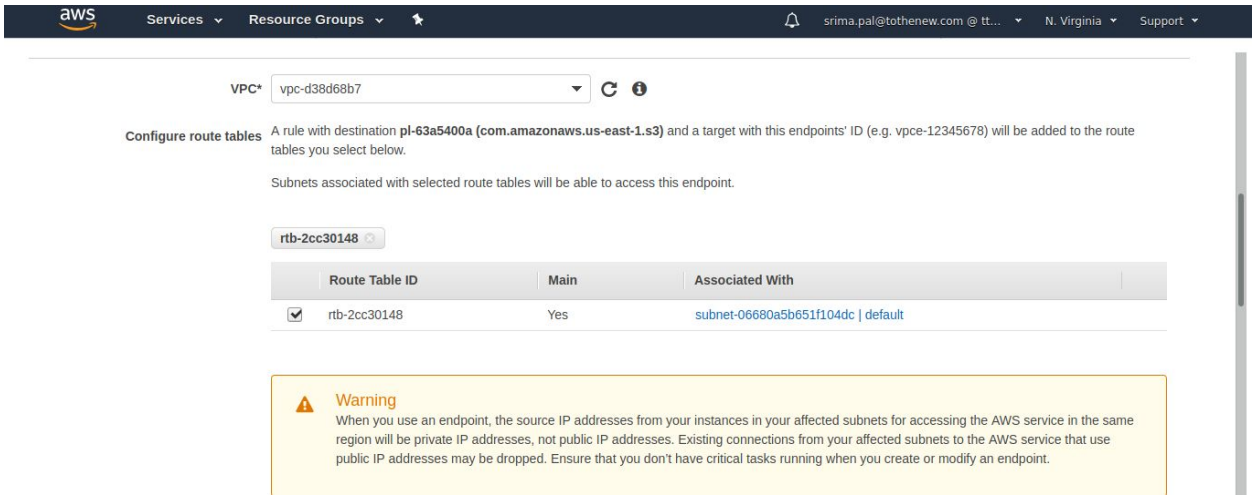
Gateway endpoints is a gateway targeted for a specific route in the routCreate another role which has the policy to assume the previous Roleeing table. They can be used to

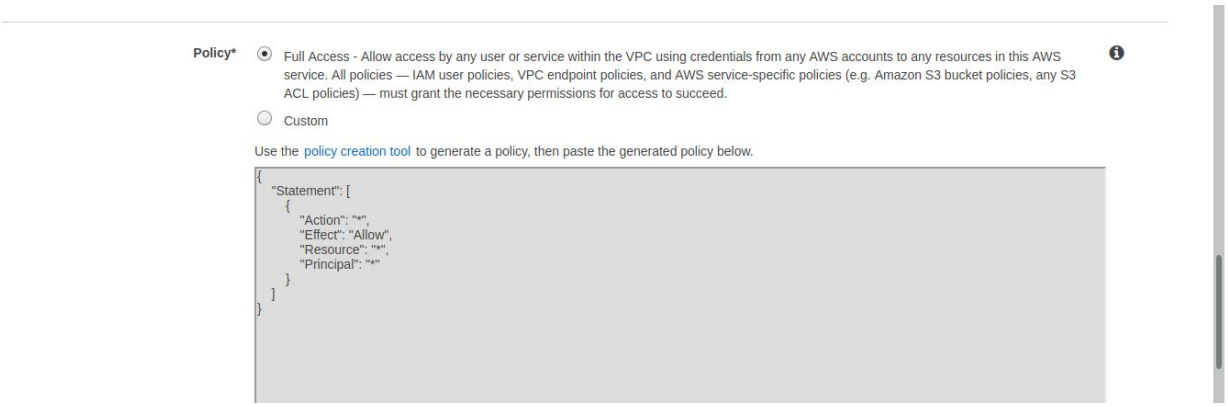
route traffic to a destined AWS service. As of now, Amazon S3 and DynamoDB are the only services that are supported by gateway endpoints.

Go to VPC > Endpoint > Create Endpoint and mention the service eg. S3









10. CORS, Enabling CORS for 2 specific website

Cross-Origin Resource Sharing (CORS) is a mechanism that uses additional HTTP headers to tell browsers to give a web application running at one origin, access to selected resources from a different origin. A web application executes a cross-origin HTTP request when it requests a resource that has a different origin (domain, protocol, or port) from its own.

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

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<CORSRule>
<AllowedOrigin>https://s3.console.aws.amazon.com</AllowedOrigin>
<AllowedOrigin>https://www.google.com/</AllowedOrigin>
<AllowedMethod>GET</AllowedMethod>
<AllowedMethod>POST</AllowedMethod>
<AllowedMethod>PUT</AllowedMethod>
<MaxAgeSeconds>3000</MaxAgeSeconds>
<AllowedHeader>Authorization</AllowedHeader>
</CORSRule>
</CORSConfiguration>
```