

**TO
THE
NEW™**



Assessment -16

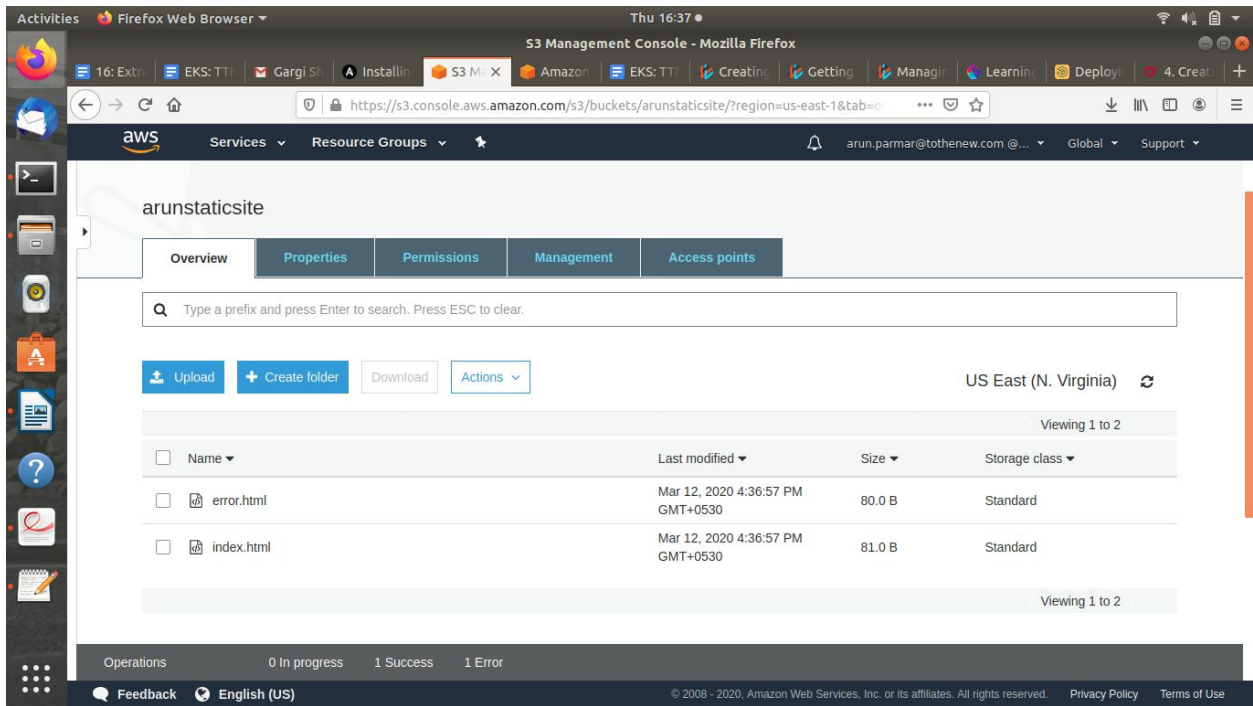
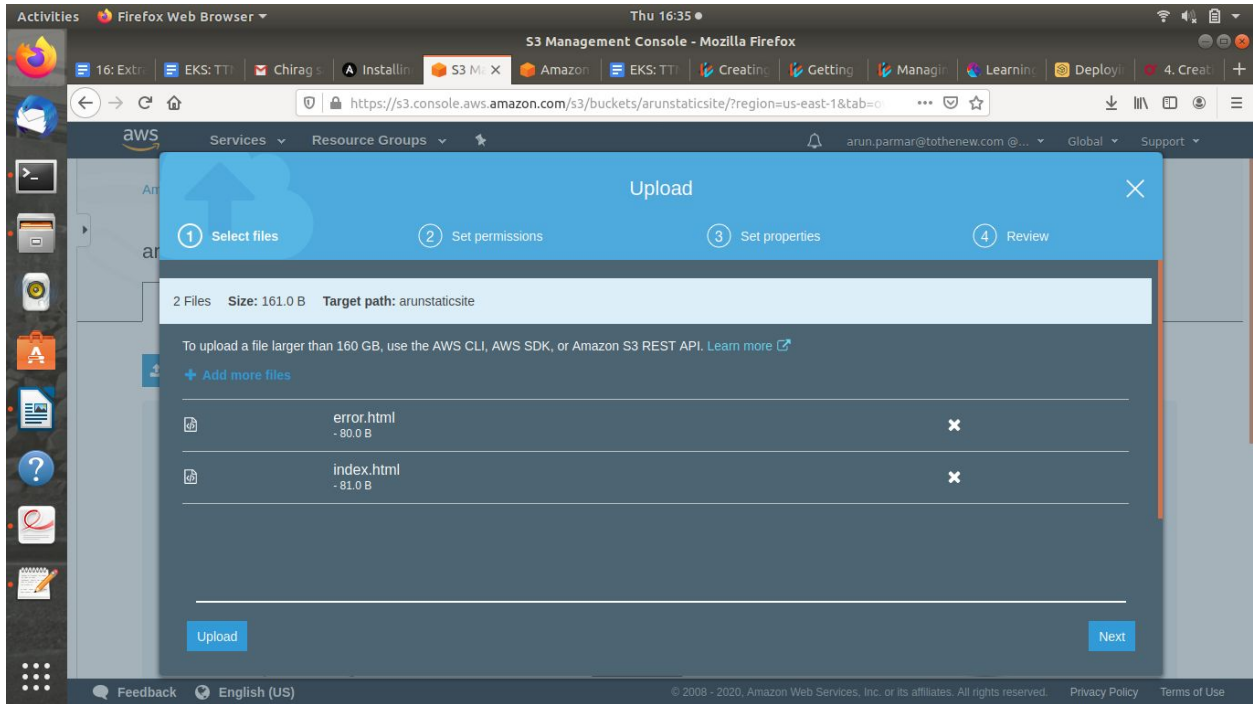
Doubt Resolving

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 16:37

S3 Management Console - Mozilla Firefox

16: Extr EKS: TT Fwd: - a Installin S3 M X Amazon EKS: TT Creatin Gettin Managin Learnin Deploy 4. Creat

https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=objects

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

Change encryption Change metadata Add tags Make public Rename Delete Undo delete Copy

US East (N. Virginia)

Viewing 1 to 2

Name	Last modified	Size	Storage class
<input checked="" type="checkbox"/> error.html	Mar 12, 2020 4:36:57 PM GMT+0530	80.0 B	Standard
<input checked="" type="checkbox"/> 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

16: Extr EKS: TT Chirag Installin S3 M X AWS P Amazon EKS: TT Creatin Gettin Managin Learnin Deploy 4. Creat

https://s3.console.aws.amazon.com/s3/buckets/arunstaticsite/?region=us-east-1&tab=objects

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).

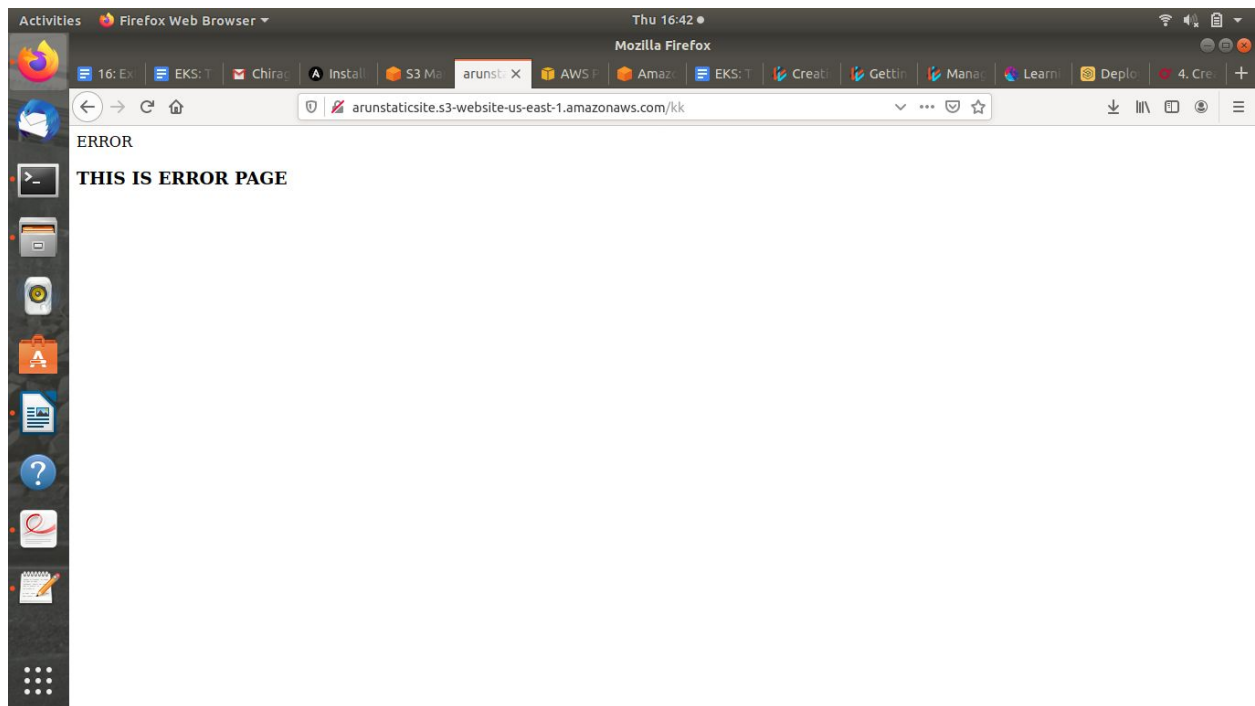
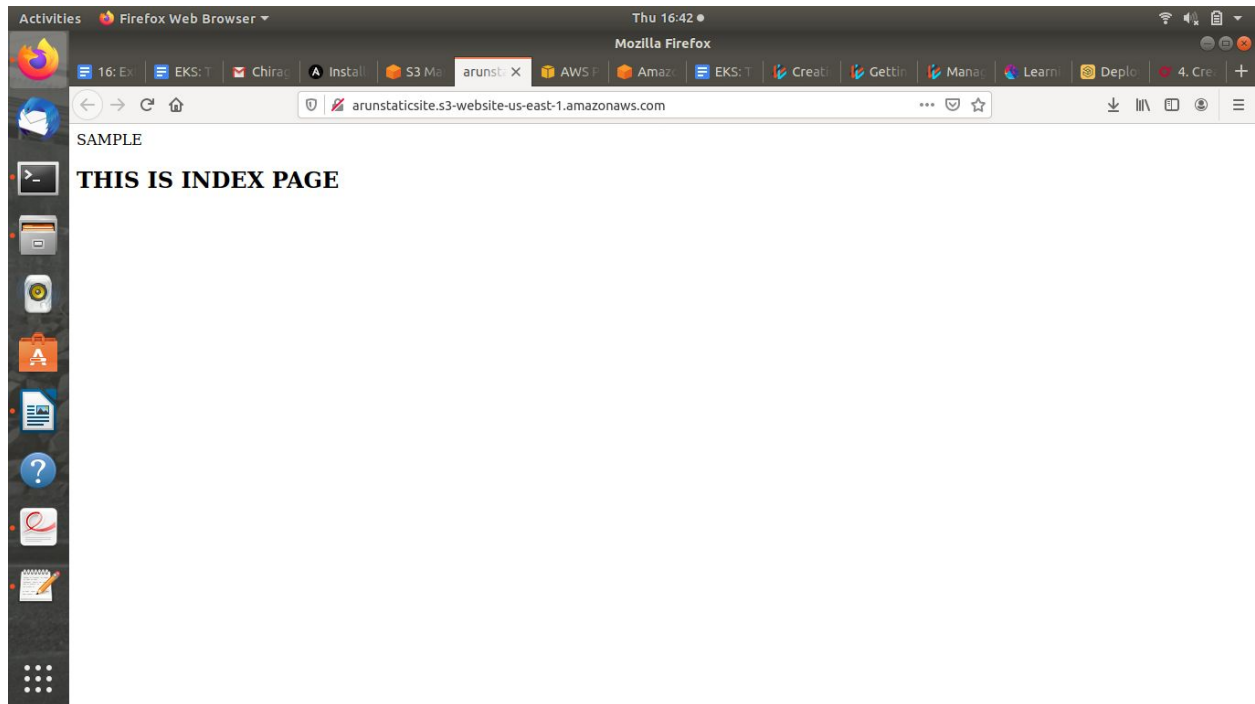
[Learn more](#)

☐ 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 role

1234

▼ Attach permissions policies

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

Create policy

Filter policies s3full Showing 1 result

	Policy name	Used as
<input checked="" type="checkbox"/>	AmazonS3FullAccess	Permissions policy (54)

* Required

Cancel Previous Next: Tags

Create role

1234

Review

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

Role name*

Arun-S3fullacces

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

Permissions boundary

Permissions boundary is not set

* Required

Cancel Previous Create role

- Create a new role

Create role

1 2 3 4

Review

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

Role name*

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

Role description

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

Trusted entities AWS service: ec2.amazonaws.com

Policies Policies not attached

Permissions boundary Permissions boundary is not set

* Required

[Cancel](#) [Previous](#) [Create role](#)

- 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

[Expand all](#) | [Collapse all](#)

▼ STS (1 action)

Clone Remove

▶ Service STS

▶ Actions Write

AssumeRole

▼ Resources

☒ Specific

[close](#)

☐ All resources

role ?

arn:aws:iam::187632318301:role/Aru

EDIT

*

☐ Any

Add ARN to restrict access

▶ Request conditions

Specify request conditions (optional)

✔ **Arun-assmuerole** has been created.

Create policy
Policy actions ▾

↺
⚙
?

Filter policies ▾

	Policy name ▾	Type	Used as	Description
<input type="radio"/>	Arun-assmuerole	Customer managed	None	Assume role s3 full access

- Attach this policy to the newly created role

Attach policy

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

Filter: Filter ▾

Showing 3 results

<input type="checkbox"/>	Name ▾	Type ▾
<input type="checkbox"/>	arun.parmar@tothenew.com	User
<input checked="" type="checkbox"/>	Arun-assumerole	Role
<input type="checkbox"/>	Arun-S3fullaccess	Role

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

Policies > Arun-assmuerole
Delete policy

Summary

Policy ARN arn:aws:iam::187632318301:policy/Arun-assmuerole [🔗](#)

Description Assume role s3 full access

Permissions
Policy usage
Policy versions
Access Advisor

Policy summary
{ } JSON
Edit policy
?

Service ▾	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			
STS	Limited: Write	RoleName string like Arun-S3fullaccess	None

- 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

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

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)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Network	vpc-00470a42fc196d84e sarthak	Create new VPC
Subnet	subnet-01d770a77bb69a1f8 sarthak-load-balancer-1 218 IP Addresses available	Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	Arun-assumerole	Create new IAM role
Shutdown behavior	Stop	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance	

Cancel Previous **Review and Launch** Next: Add Storage

Launch Instance Connect Actions

search : i-012604ec135e90694 Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Arunassume...	i-012604ec135e90694	t2.micro	us-east-1b	pending	Initializing	None	

- SSh into the instance and install awscli

```

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

System information as of Sun Mar  1 11:37:15 UTC 2020

System load:  0.0              Processes:            86
Usage of /:   13.6% of 7.69GB  Users logged in:     0
Memory usage: 15%              IP address for eth0: 10.0.1.206
Swap usage:   0%

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-206:~$

```

```

Reading package lists... Done
ubuntu@ip-10-0-1-206:~$ sudo apt-get install awscli
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docutils-common libjpeg-turbo8 libjpeg8 liblcms2-2 libpaper-utils libpaper1 libtiff5 libwebp6
  libwebpdemux2 libwebpmux3 python3-boto3 python3-dateutil python3-docutils python3-jmespath
  python3-olefile python3-pil python3-pygments python3-roman python3-rsa python3-s3transfer sgml-base
  xml-core
Suggested packages:

```

- 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-S3fullaccess --role-session-name Arunrole
{
  "Credentials": {
    "AccessKeyId": "ASIASXL6B650TFJ0KBFD",
    "SecretAccessKey": "hUQiujVhLAHB1ttKj+3wA2icHtQZgihyfLORfg9x",
    "SessionToken": "FwoGZXIvYXZlEE0aDAT146aDaWap7t6EbCKsAUL0rz6Q+Zvy1e+wTMSXNgapQX5QbYpjcxqyKAZzsydu/DNZMGAYWglpBtMyxu8bjsD3X2ebjQ8p3/fGqiz08o9rMt9LkUwnCS1rs0sFKA1tAd8ir4wnE0AcnIsAfw0XB7CMjz82WjqeTxSnnLEoAL/e/YrPfdFX5cdnJnVmKXy7Am2HOF3xV+/n2gvE5rShvwdjLYM1GJ+WDXg2e2ve/jV0/5Y+vs+43oPwEov77u8gUyLQpZ+a5LTHcs3LpHp8eSDKJtC+Aqa0MqSGWt3nudcmtKffXmRRhF6bGTaoazgQ==",
    "Expiration": "2020-03-01T12:40:47Z"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROASXL6B6504QSUNDFSJ:Arunrole",
    "Arn": "arn:aws:sts::187632318301:assumed-role/Arun-S3fullaccess/Arunrole"
  }
}
```

- Now export variables:

```
ubuntu@ip-10-0-1-206:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B650TFJ0KBFD
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_SESSION_TOKEN=FwoGZXIvYXZlEE0aDAT146aDaWap7t6EbCKsAUL0rz6Q+Zvy1e+wTMSXNgapQX5QbYpjcxqyKAZzsydu/DNZMGAYWglpBtMyxu8bjsD3X2ebjQ8p3/fGqiz08o9rMt9LkUwnCS1rs0sFKA1tAd8ir4wnE0AcnIsAfw0XB7CMjz82WjqeTxSnnLEoAL/e/YrPfdFX5cdnJnVmKXy7Am2HOF3xV+/n2gvE5rShvwdjLYM1GJ+WDXg2e2ve/jV0/5Y+vs+43oPwEov77u8gUyLQpZ+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

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a star icon, and a notification bell. Below the navigation bar, there are four buttons: 'Block public access', 'Access Control List', 'Bucket Policy' (which is highlighted), and 'CORS configuration'. Below these buttons, the 'Bucket policy editor' is displayed for the bucket ARN: arn:aws:s3:::arunstaticsite. A note says 'Type to add a new policy or edit an existing policy in the text area below.' The main area contains a JSON policy document with the following content:

```
1 {
2   "Version": "2012-10-17",
3   "Id": "Policy1584013882020",
4   "Statement": [
5     {
6       "Sid": "Stmt1584013819730",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": "s3:*",
10      "Resource": "arn:aws:s3:::arunstaticsite",
11      "Condition": {
12        "NotIpAddress": {
13          "aws:SourceIp": "18.234.207.52"
14        }
15      }
16    }
17  ]
18 }
```


ii. Domain

Bucket policy editor ARN: arn:aws:s3:::arunstaticsite

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

```
1 {
2   "Id": "Policy1584014245080",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmnt1584014243246",
7       "Action": "s3:*",
8       "Effect": "Allow",
9       "Resource": "arn:aws:s3:::arunstaticsite",
10      "Condition": {
11        "StringLike": {
12          "aws:Referer": "http://arunstaticsite.s3-website-us-east-1.amazonaws.com/"
13        }
14      },
15      "Principal": "*"
16    }
17  ]
18 }
```

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.

The block public access settings turned on for this bucket prevent granting public access.

```
1 {
2   "Id": "Policy1583297551962",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "presigned url",
7       "Action": [
8         "s3:Get*"
9       ],
10      "Effect": "Deny",
11      "Resource": "arn:aws:s3:::srmas3/*",
12      "Condition": {
13        "s3:authType": "REST-QUERY-STRING"
14      }
15    },
16    "Principal": "*"
17  ]
18 }
```

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

16: Extra Plan and T Inbox (335) Assignment RDS - Al Instances EKS: TTN Creating a Getting sta Example w Learning |

https://console.aws.amazon.com/rds/home?region=us-east-1#db-subnet-groups: 67%

aws Services Resource Groups

arun.parmar@tothenew.com @ N. Virginia Support

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
You won't be able to modify the name after your subnet group has been created.
ARUN
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
EKSonly (vpc-093a4253d4c9ab207)

Add subnets

Add subnets to this subnet group. You may add subnets one at a time below or add all the subnets related to this VPC. You may make additional modifications after this subnet group has been created.

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
us-east-1b	subnet-0342b9c54db410a4e	10.0.2.0/24	Remove

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activities Firefox Web Browser Sun 13:52

EC2 Management Console - Mozilla Firefox

16: Extra Plan and T Inbox (335) Assignment EC2 Mar Instances EKS: TTN Creating a Getting sta Example w Learning |

https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup: 67%

aws Services Resource Groups

arun.parmar@tothenew.com @ N. Virginia Support

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 [Info](#)
sgforRDS
Name cannot be edited after creation.

Description [Info](#)
testing

VPC [Info](#)
vpc-093a4253d4c9ab207 (EKSonly)

Inbound rules

[Info](#)

Type	Protocol	Port range	Source	Description - optional	
MySQL/Aurora	TCP	3306	Custom	Q	
				0.0.0.0/0	Delete

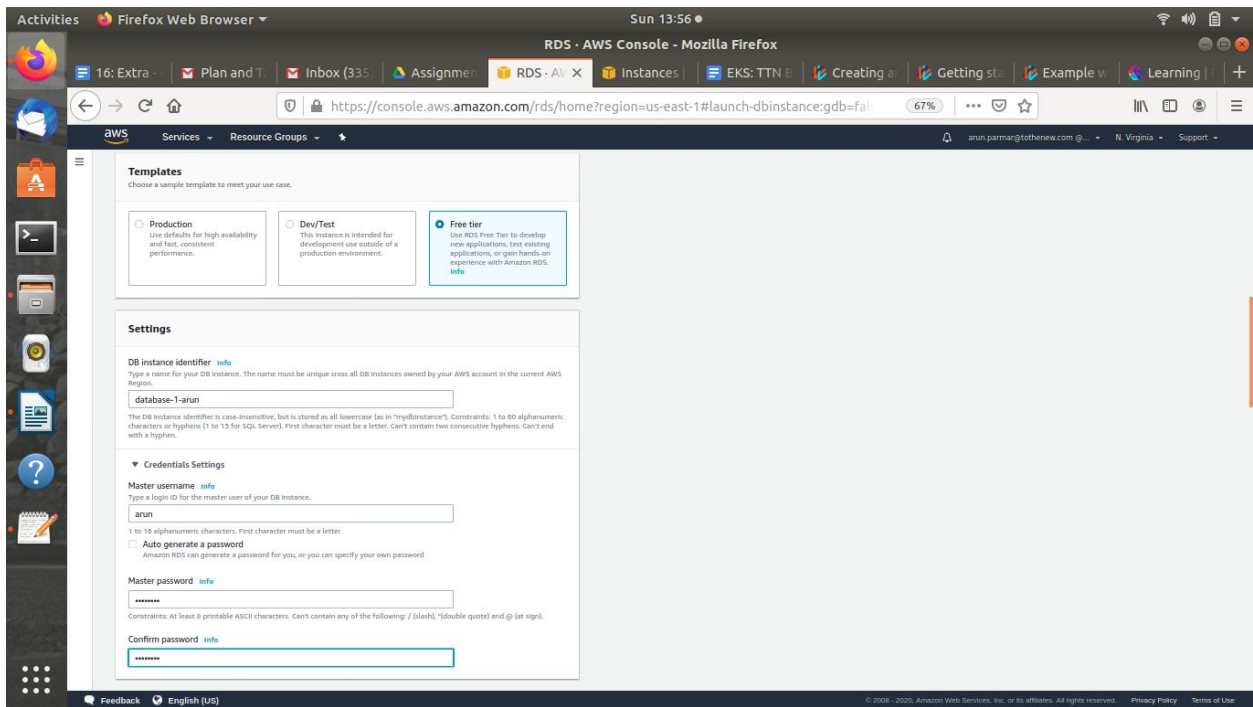
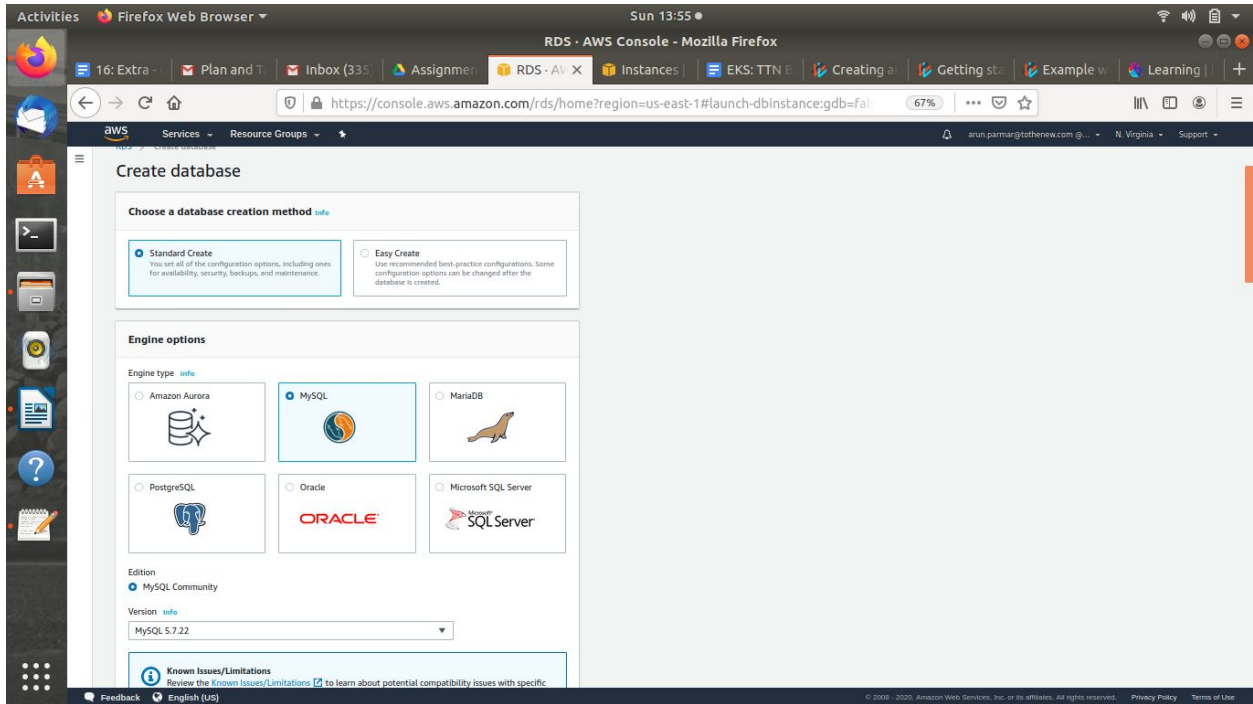
Add rule

Outbound rules

[Info](#)

Type	Protocol	Port range	Destination	Description - optional
------	----------	------------	-------------	------------------------

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use



Activities Firefox Web Browser Sun 13:57 RDS - AWS Console - Mozilla Firefox

16: Extra Plan and T Inbox (335) Assignment RDS - Al Instances EKS: TTN B Creating a Getting sta Example w Learning |

https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal 67%

aws Services Resource Groups arun.parmar@tothenew.com @ 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.

Settings

DB instance identifier [info](#)

Type a name for your DB instance. The name must be unique across 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 63 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) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activities Firefox Web Browser Sun 13:58 RDS - AWS Console - Mozilla Firefox

16: Extra Plan and T Inbox (335) Assignment RDS - Al Instances EKS: TTN B Creating a Getting sta Example w Learning |

https://console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=fal 67%

aws Services Resource Groups arun.parmar@tothenew.com @ N. Virginia Support

Connectivity

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

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

EKSonly (vpc-003a4251dc9ab207)

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 X

Availability zone [info](#)

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. 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

```
ubuntu@ip-172-31-19-163:~$ 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
```

Clone s3fs code from git

```
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 | 23.76 MiB/s, done.  
Resolving deltas: 100% (4069/4069), done.  
ubuntu@ip-172-31-19-163:~$ ls  
s3fs-fuse  
ubuntu@ip-172-31-19-163:~$
```

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
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-opensl
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:~$
```

```
AKIASXL6B650XF7XHY4K:rqMypbahX9w4uqds6m4SolB+21Bz3m/X5Q6L3xV
Learning | Dashbo X TTN Doubt Resolv X ASSESSMENT:DOC X Job1 #3 Co
```

Change the permission of your file

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

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 allow_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 srmas3 -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

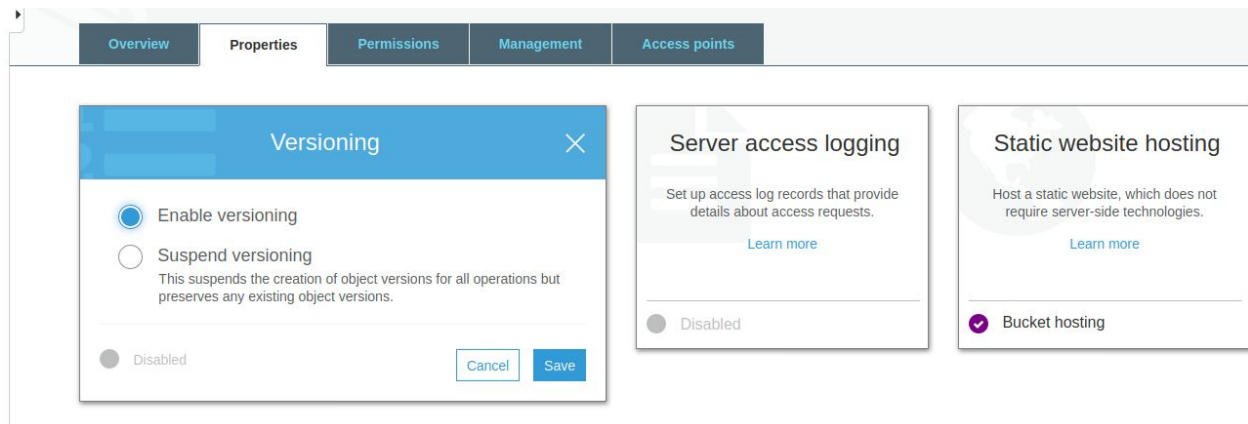
```
ubuntu@ip-172-31-19-163:~/s3fs-fuse$
```

7.Change content type using S3


```
Activities Terminal Sun 14:43
Terminal
File Edit View Search Terminal Help
arun@Arun-Parmar:~$ aws s3api get-object --bucket arunstaticsite --key index.html data
{
  "AcceptRanges": "bytes",
  "LastModified": "Thu, 12 Mar 2020 11:06:57 GMT",
  "ContentLength": 81,
  "ETag": "\"07019b4f65b3c9ba692c6e7918f0b58b\"",
  "ContentType": "text/html",
  "Metadata": {}
}
arun@Arun-Parmar:~$ aws s3 cp s3://arunstaticsite s3://arunstaticsite --exclude '*' --include '*.html' --no-guess-mime-type --c
ontent-type="text/plain" --metadata-directive="REPLACE" --recursive
Unknown options: --metadata-directive+REPLACE
arun@Arun-Parmar:~$ aws s3 cp s3://arunstaticsite s3://arunstaticsite --exclude '*' --include '*.html' --no-guess-mime-type --c
ontent-type="text/plain" --metadata-directive="REPLACE" --recursive
copy: s3://arunstaticsite/index.html to s3://arunstaticsite/index.html
copy: s3://arunstaticsite/error.html to s3://arunstaticsite/error.html
arun@Arun-Parmar:~$ aws s3api get-object --bucket arunstaticsite --key index.html data
{
  "AcceptRanges": "bytes",
  "LastModified": "Sun, 22 Mar 2020 09:12:50 GMT",
  "ContentLength": 81,
  "ETag": "\"07019b4f65b3c9ba692c6e7918f0b58b\"",
  "ContentType": "text/plain",
  "Metadata": {}
}
arun@Arun-Parmar:~$
```

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

Enable versioning in the bucket



We can see two versions uploaded

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

Upload

Create folder

Download

Actions




Versions

Hide

Show

US East (N. Virginia)

Viewing 1 to 3

	Name	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	hello		Mar 5, 2020 2:46:43 PM		
<input type="checkbox"/>	 Mar 5, 2020 2:46:43 PM (Latest version)	y_KAtHety21mwq0nzuFIUWNcHl...		22.0 B	Standard
<input type="checkbox"/>	 Mar 5, 2020 1:30:13 PM	08KthyCili_XX6NsBH5AXrSdWw...		22.0 B	Standard
	index.html		Mar 5, 2020 1:23:21 PM		
<input type="checkbox"/>	 Mar 5, 2020 1:23:21 PM (Latest version)	null		44.0 B	Standard

Viewing 1 to 3

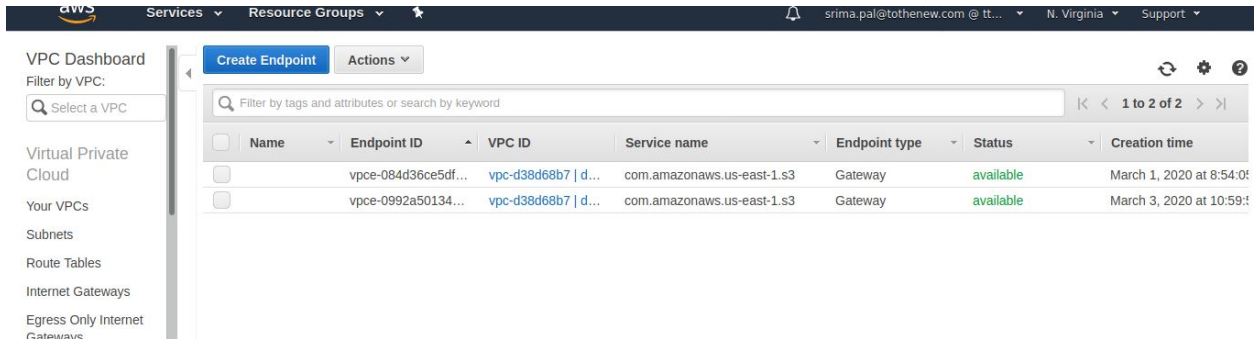
9. S3 VPC endpoint.

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

Gateway endpoints is a gateway targeted for a specific route in the route 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



VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Create Endpoint

Filter by tags and attributes or search by keyword

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
	vpce-084d36ce5df...	vpce-d38d68b7 d...	com.amazonaws.us-east-1.s3	Gateway	available	March 1, 2020 at 8:54:01
	vpce-0992a50134...	vpce-d38d68b7 d...	com.amazonaws.us-east-1.s3	Gateway	available	March 3, 2020 at 10:59:01

Create Endpoint

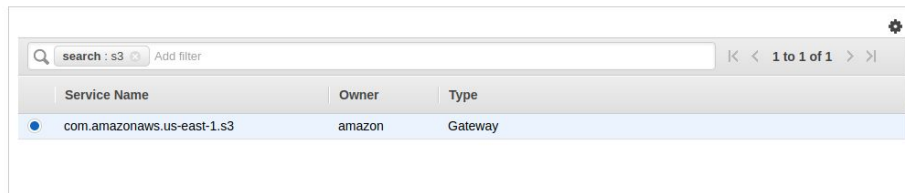
A VPC endpoint allows you to securely connect your VPC to another service.

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

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

- Service category
- ☒ AWS services
 - ☐ Find service by name
 - ☐ Your AWS Marketplace services

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



search : s3 Add filter

Service Name	Owner	Type
com.amazonaws.us-east-1.s3	amazon	Gateway

aws

Services ▾ Resource Groups ▾ ★

srjma.pal@tothenew.com @ tt... ▾ N. Virginia ▾ Support ▾

VPC*
vpc-d38d68b7

⌂ ⓘ

Configure route tables

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

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

rtb-2cc30148

	Route Table ID	Main	Associated With
<input checked="" type="checkbox"/>	rtb-2cc30148	Yes	subnet-06680a5b651f104dc default

⚠ Warning

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

Policy*

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

☐ Custom

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

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

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.

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