# 

# **Assessment**

# **Doubt Resolving**

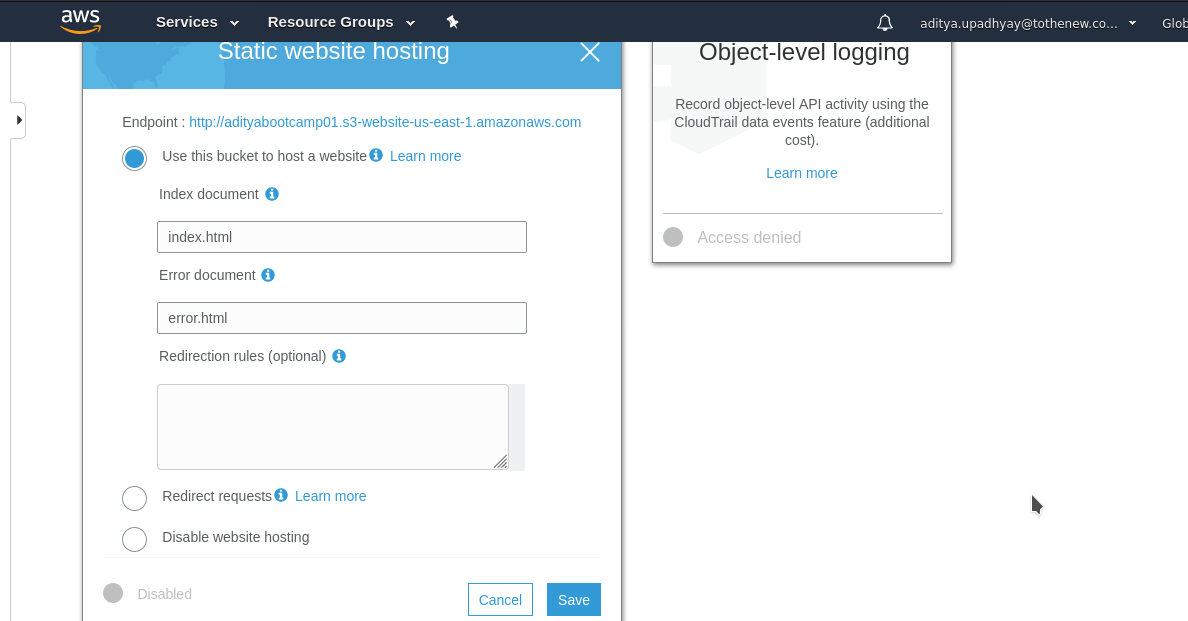
Trainee Name : Aditya Upadhyay

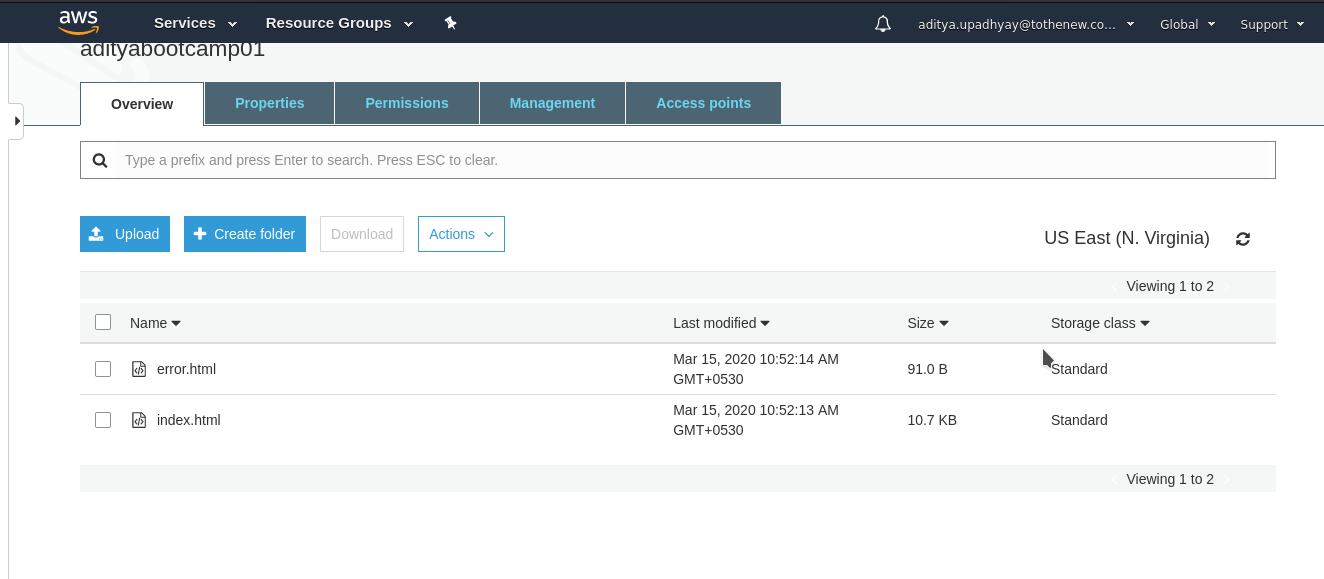
Newers ID : 3978

Mentor Name : Tarun Saxena

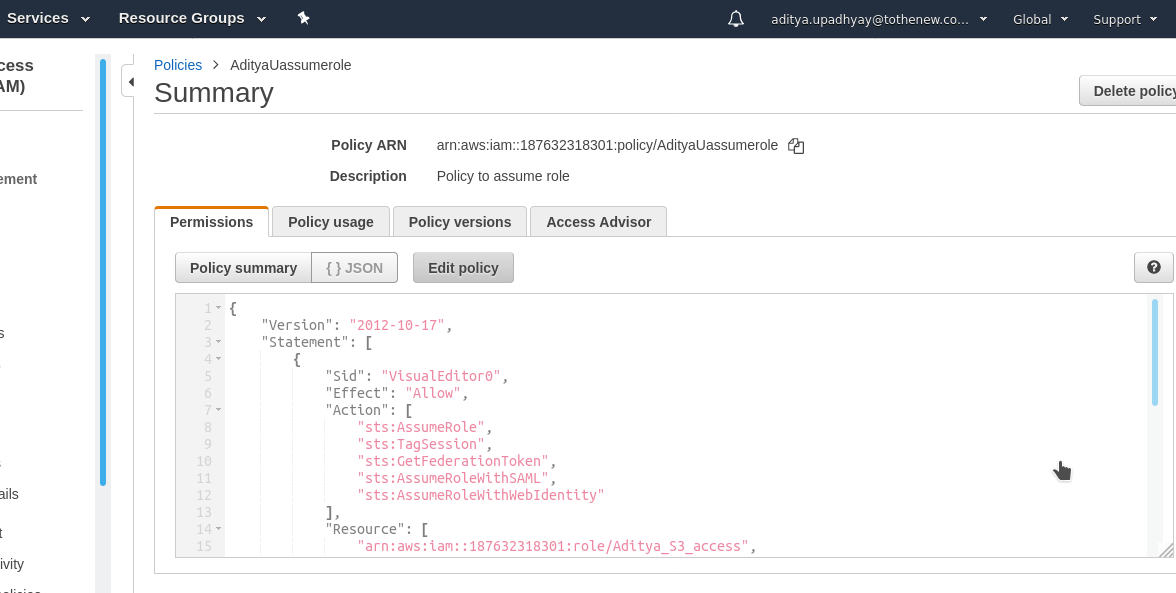
College : UPES

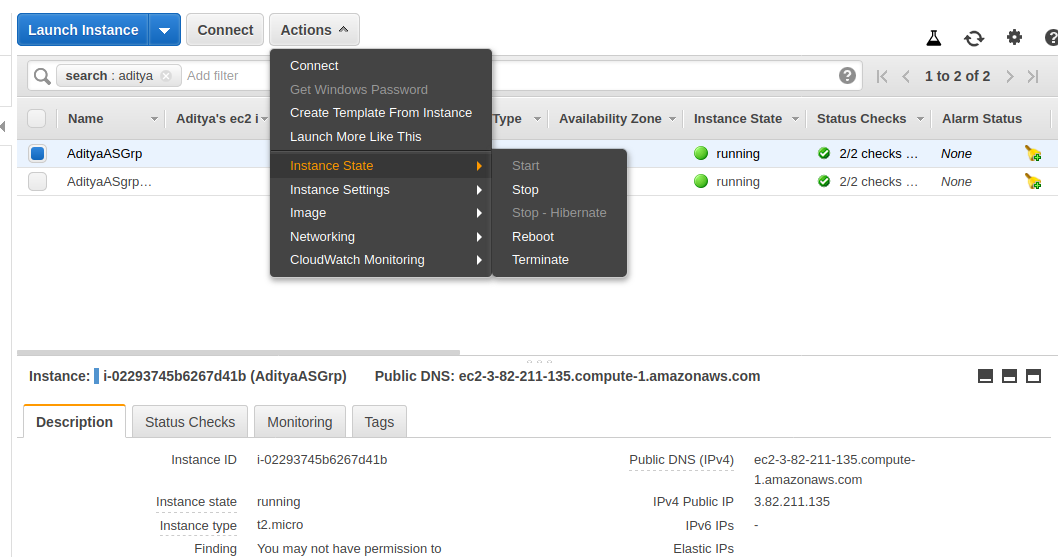
**1. Static website hosting using s3(what is index and error page).**

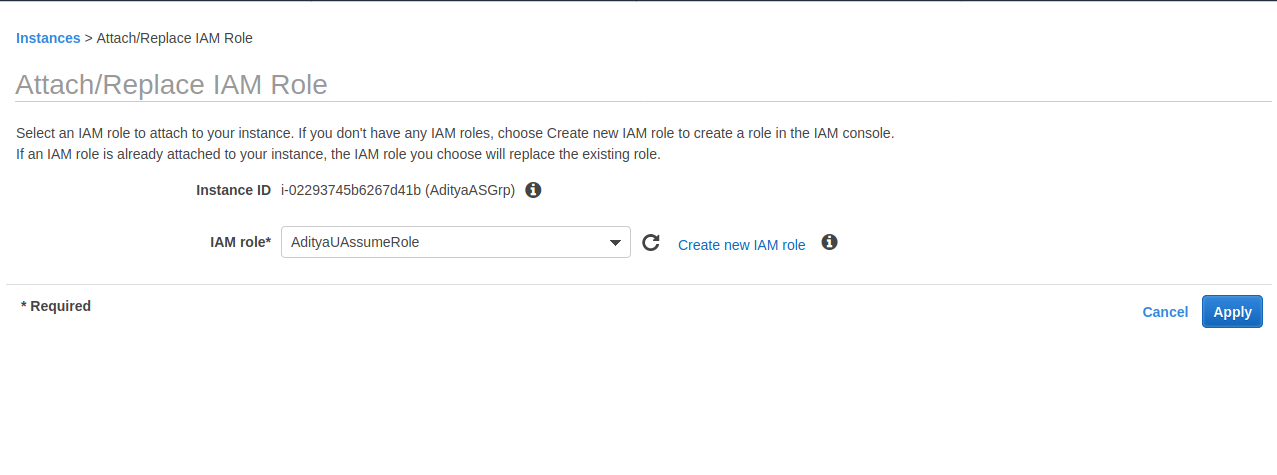


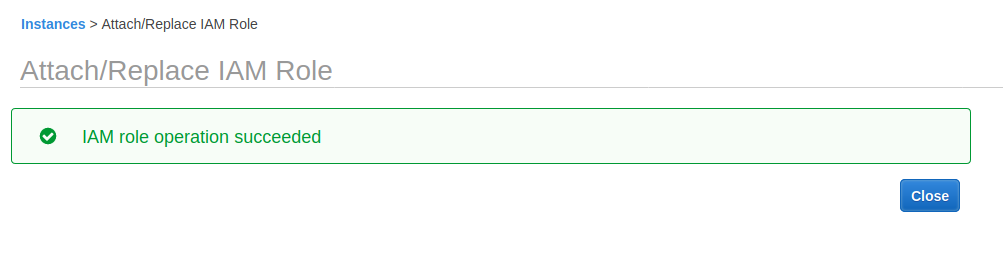


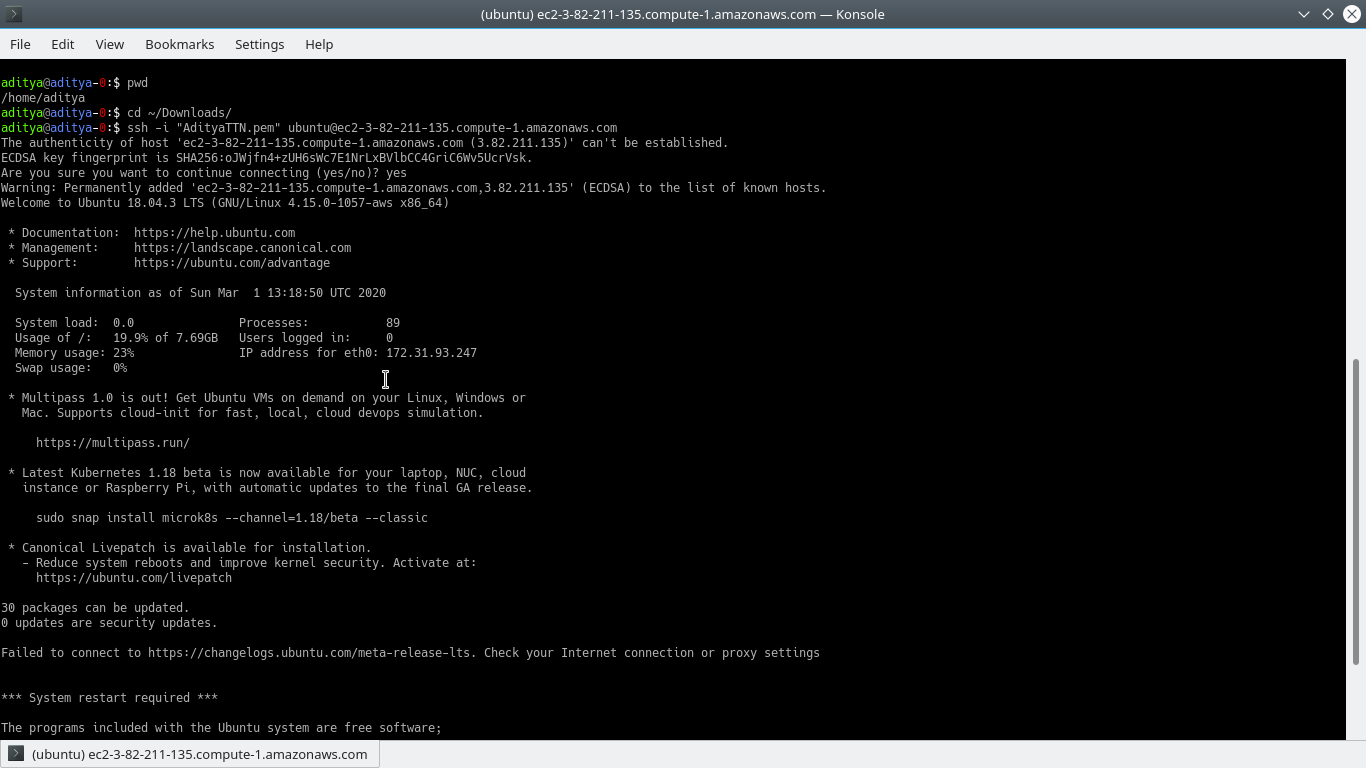
**2. Create an assume role to access s3 using ec2.**











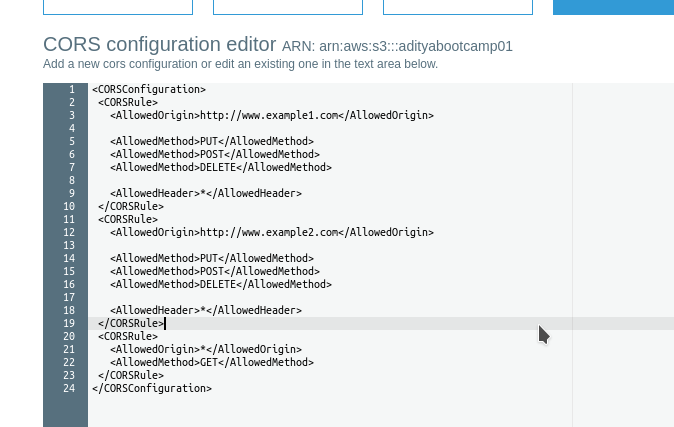


**3. Block s3 access on the basis of**

**i. IP**

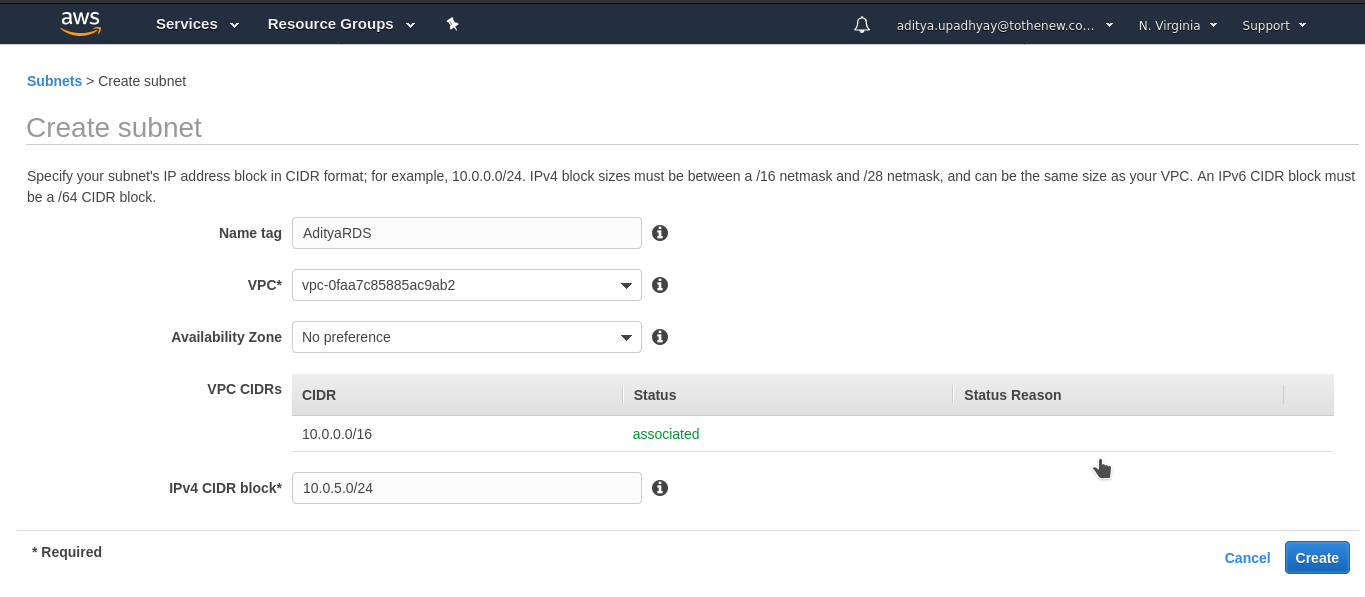


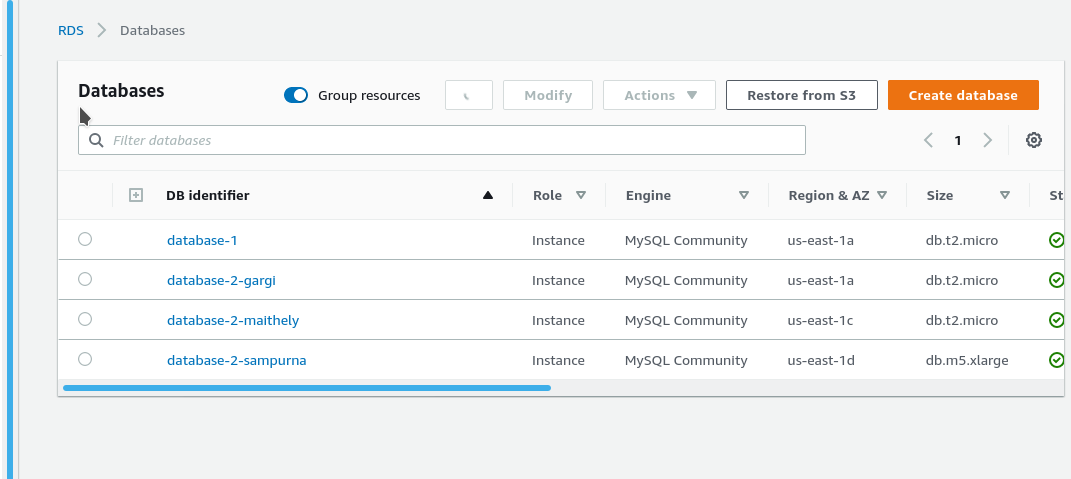
**ii. Domain**

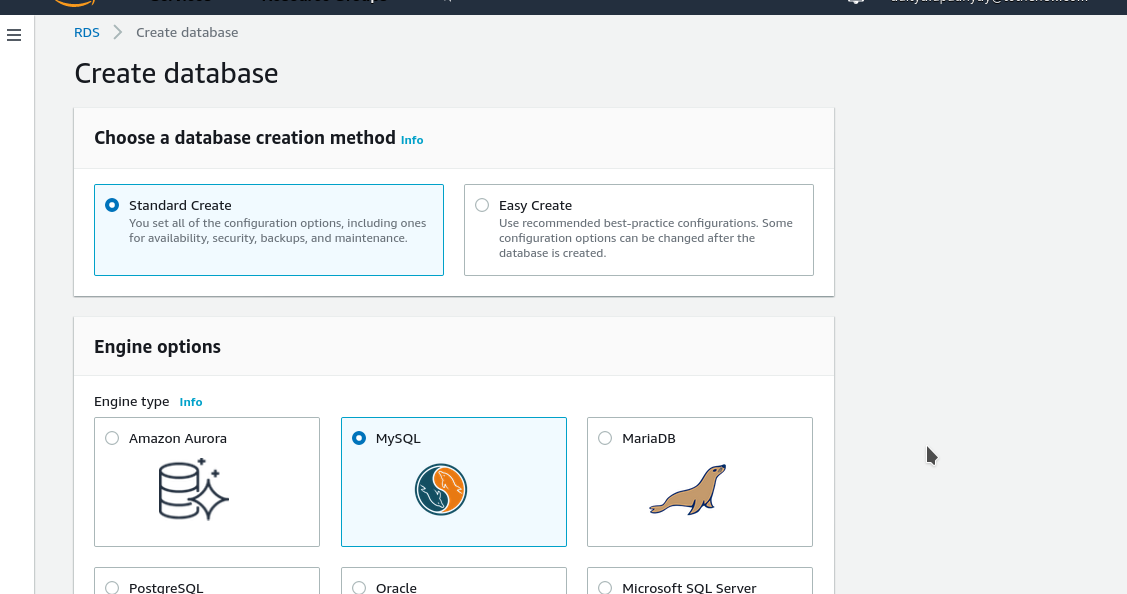


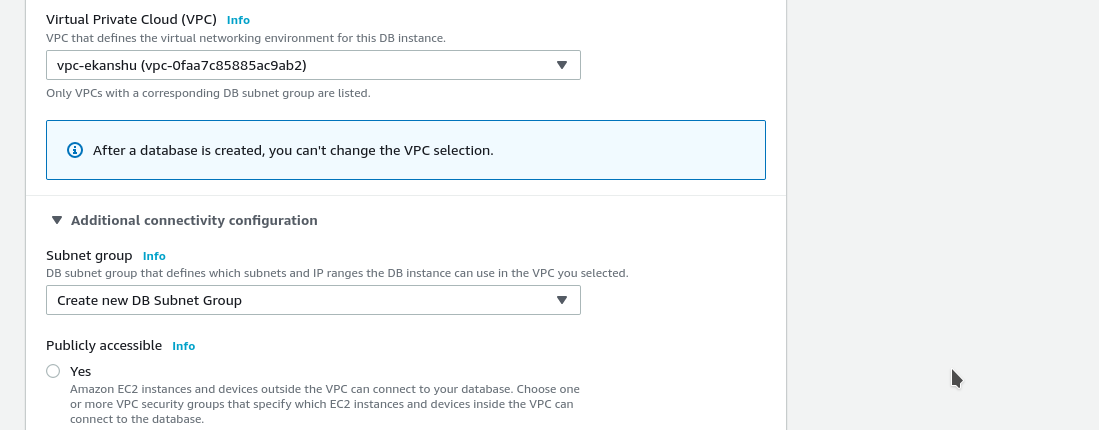
**4. Create RDS subnet and launch RDS instance.**

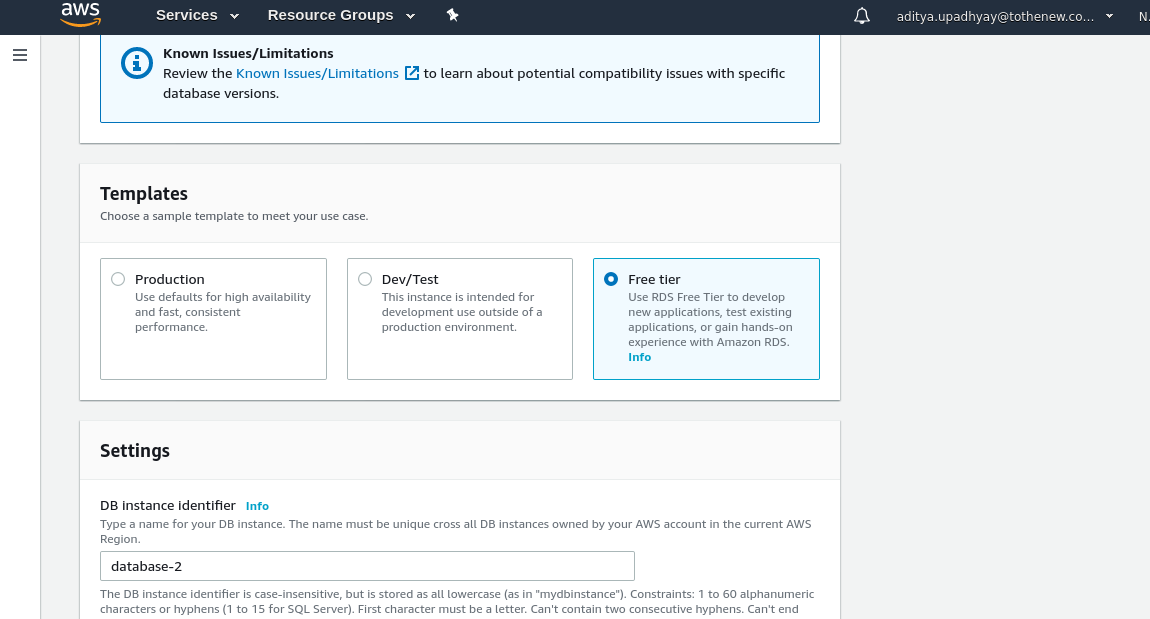
**Add subnet through subnet group**

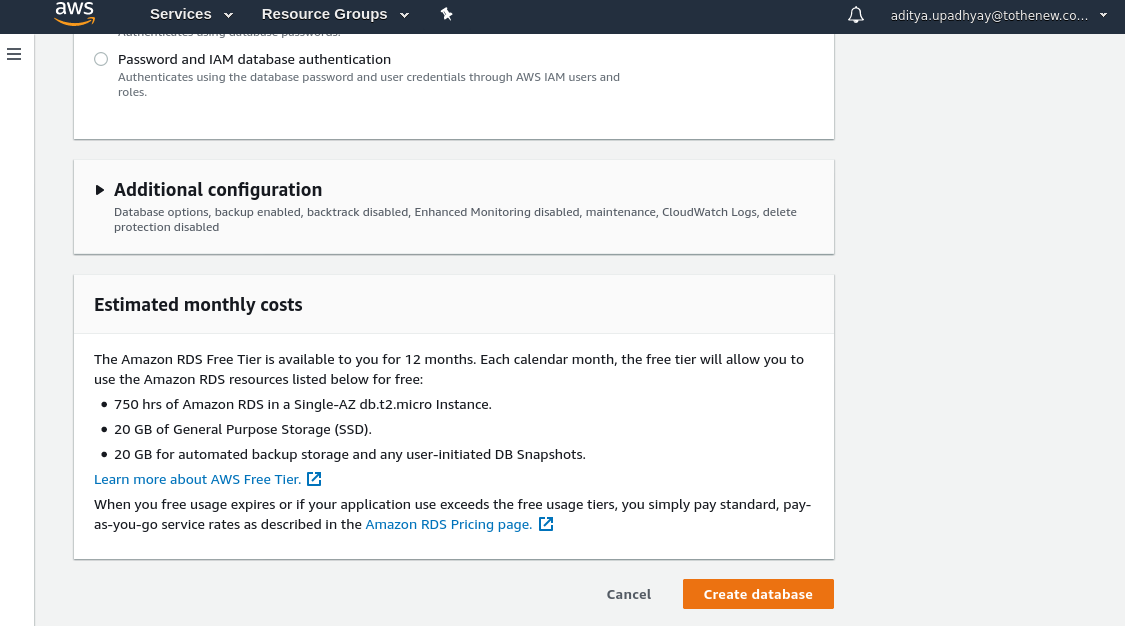
****

****

****

****

****



**5. what is parameter group and option group,ACL, Bucket policy, IAM Policy?**

**Parameter group:**You manage your DB engine configuration by associating your DB instances with parameter groups. Amazon RDS defines parameter groups with default settings that apply to newly created DB instances . You can define your own parameter groups with customized settings. Then you can modify your DB instances to use your own parameter groups.

A *DB parameter group* acts as a container for engine configuration values that are applied to one or more DB instances.

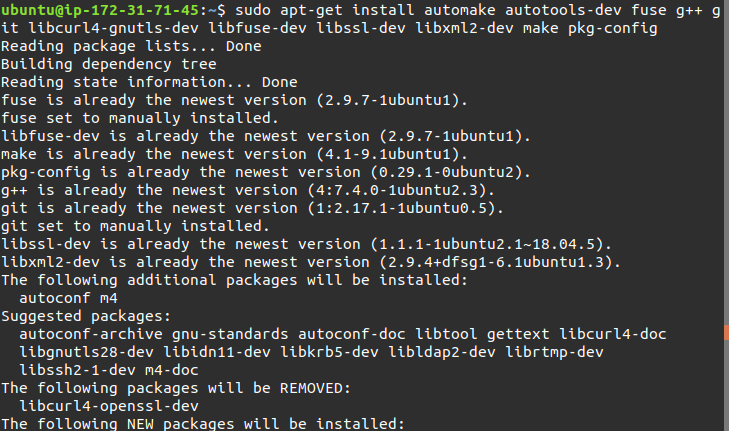
**Option Group:** Some DB engines offer additional features that make it easier to manage data and databases, and to provide additional security for your database. Amazon RDS uses option groups to enable and configure these features. An *option group* can specify features, called options, that are available for a particular Amazon RDS DB instance. 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.

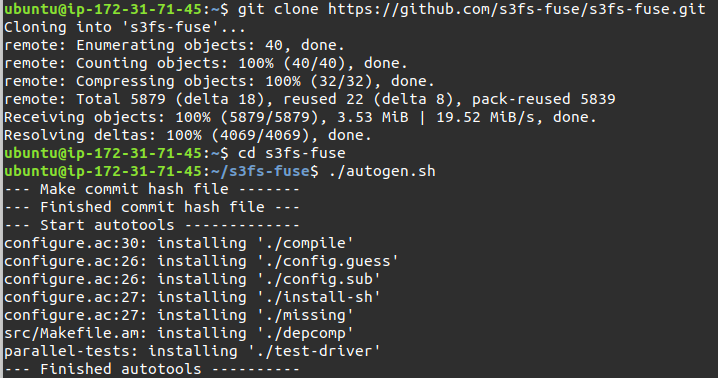
**ACL:** Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access.

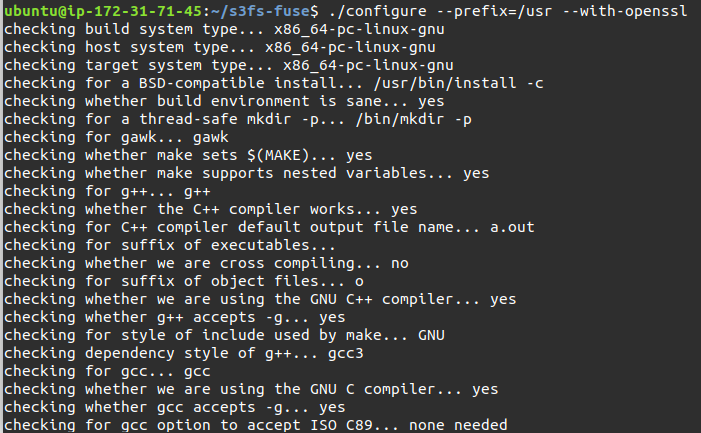
**Bucket policy:** A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner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

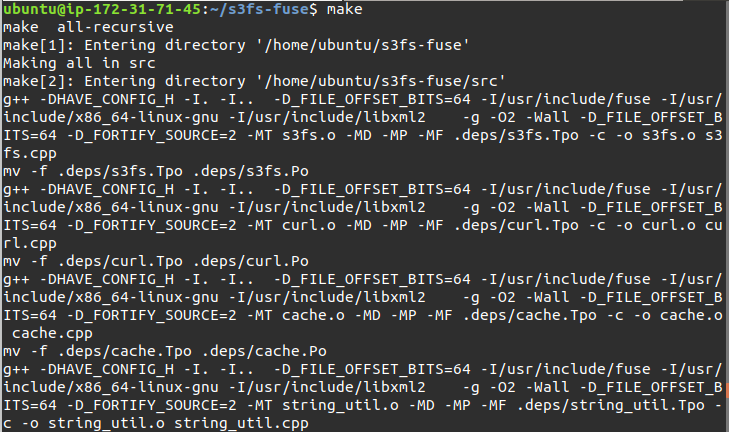
**IAM Policy:** A policy is an entity that, when attached to an identity or resource, defines their permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer managed policies in IAM. Customer managed policies are standalone policies that you administer in your own AWS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

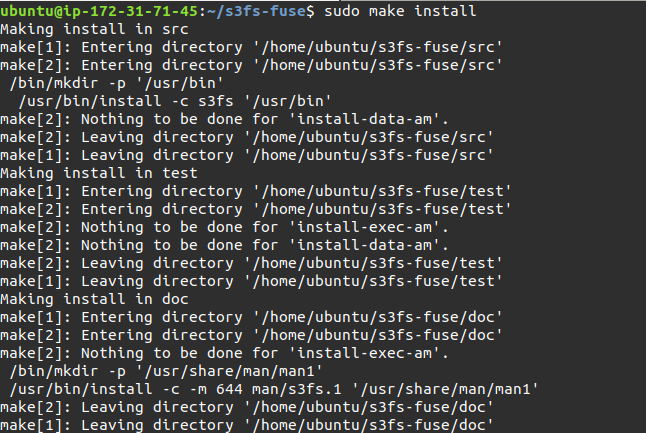
**6. Mount S3 to an EC2 instance.**

****

****

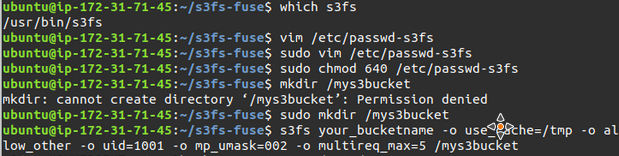
****

****

****

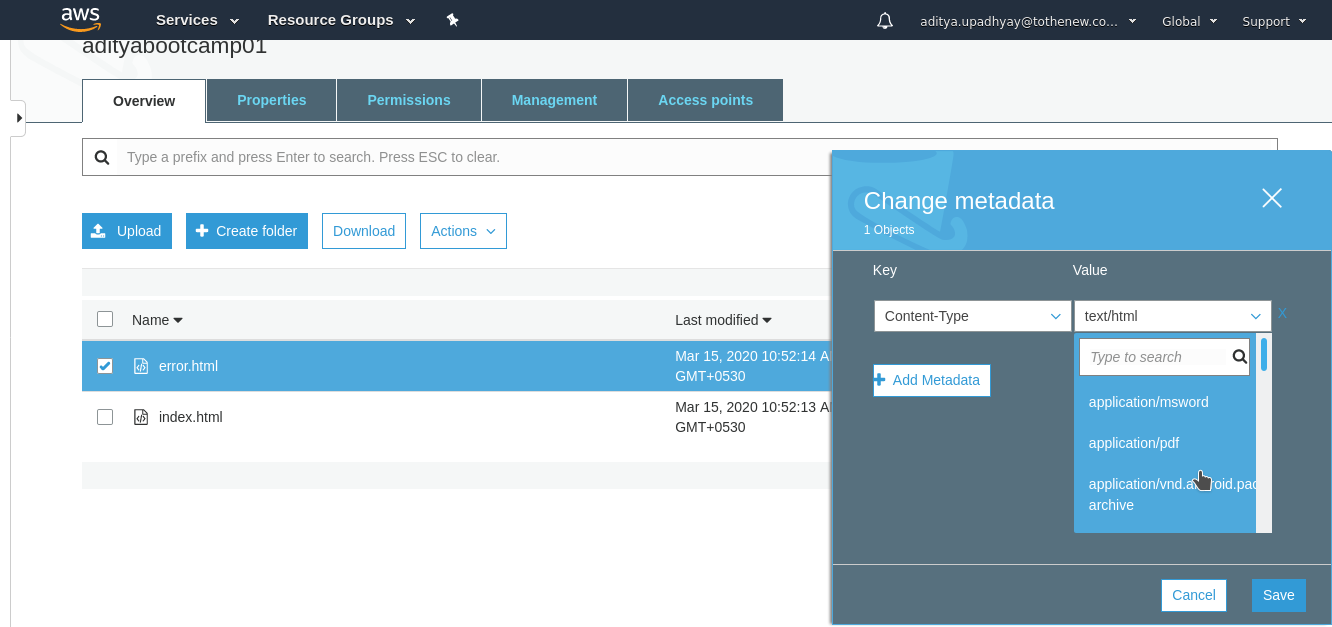
Add account credentials in /etc/passwd-s3fs in

Your\_access\_key\_id:Your\_secret\_key\_id format

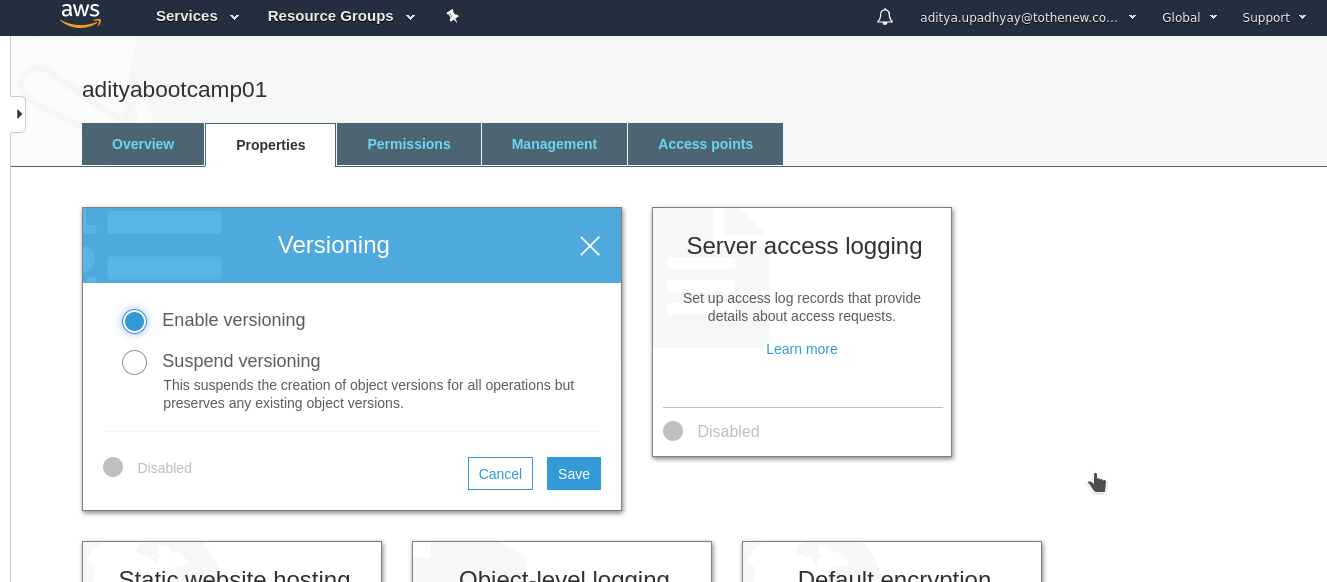
****

**Reference:** [**https://cloudkul.com/blog/mounting-s3-bucket-linux-ec2-instance/**](https://cloudkul.com/blog/mounting-s3-bucket-linux-ec2-instance/)

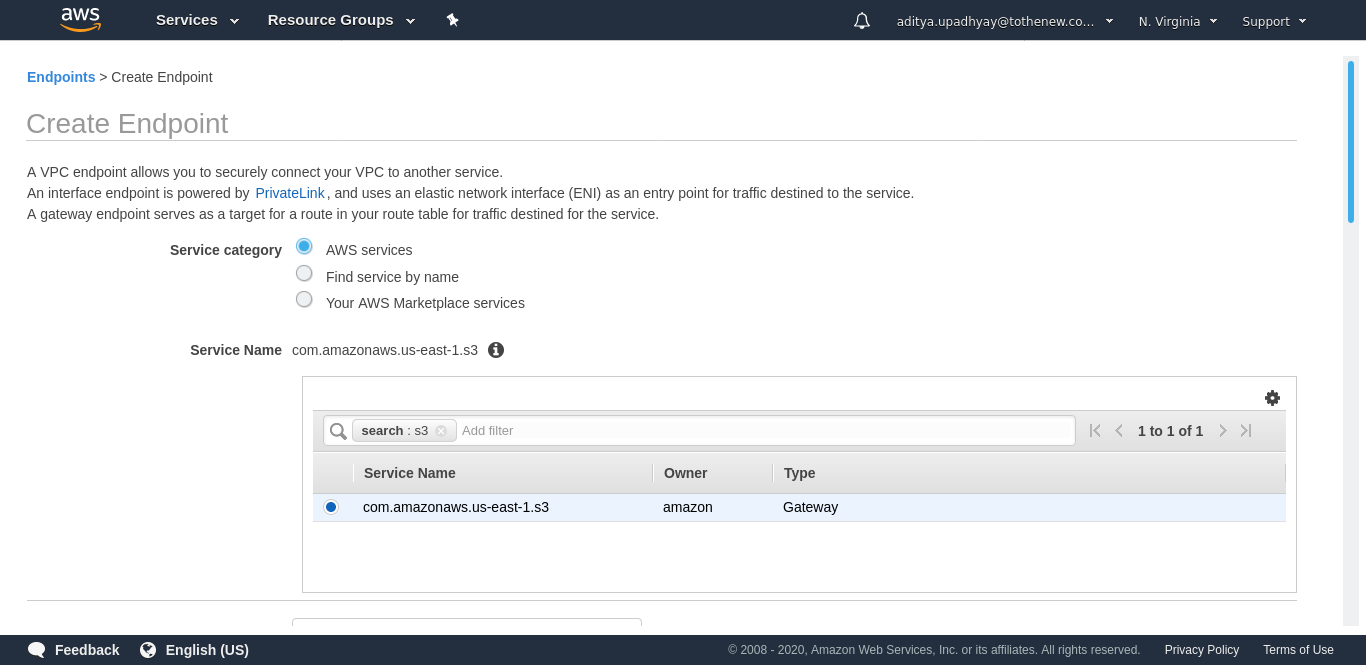
**7. Change content type using s3.**

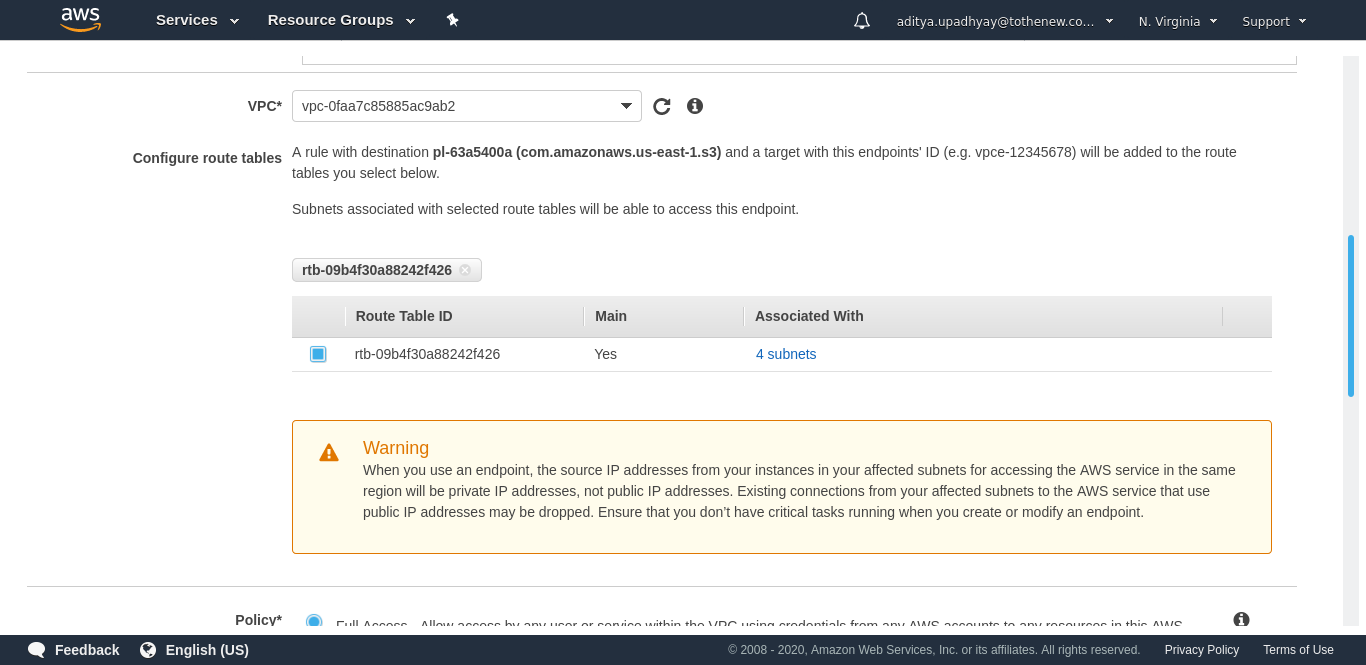
****

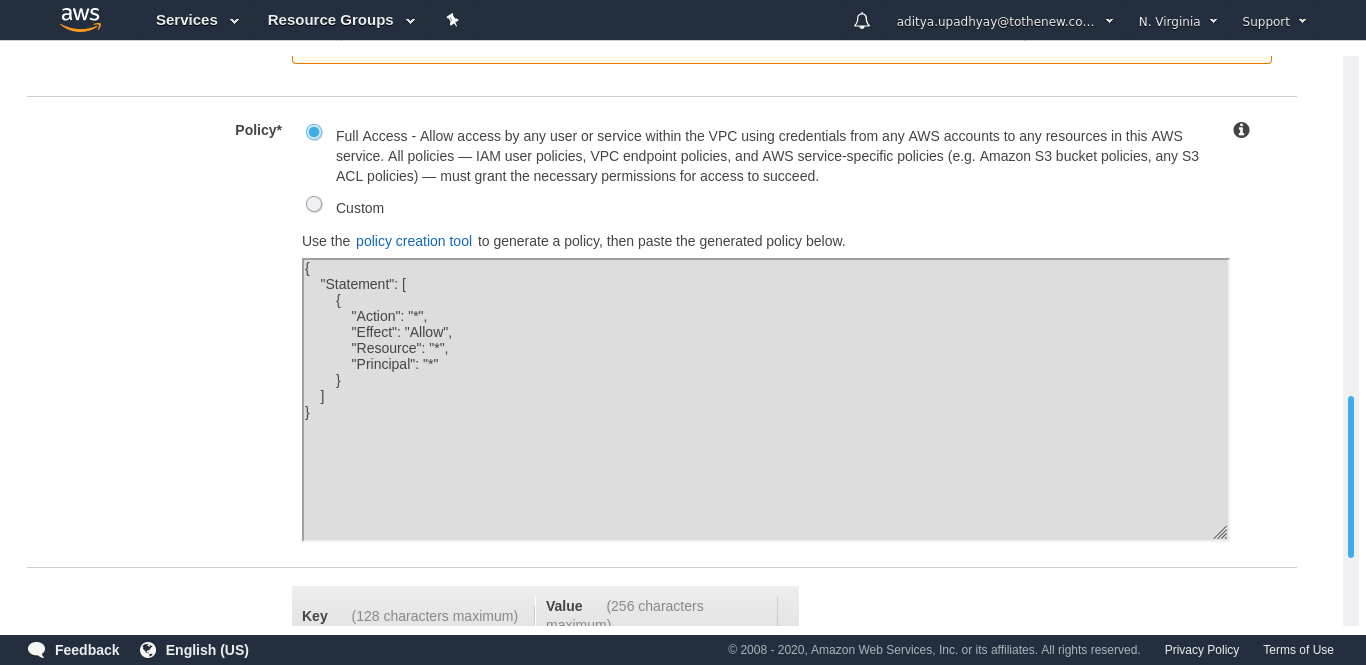
**8. Retrive previous version of S3(enable versioning).**

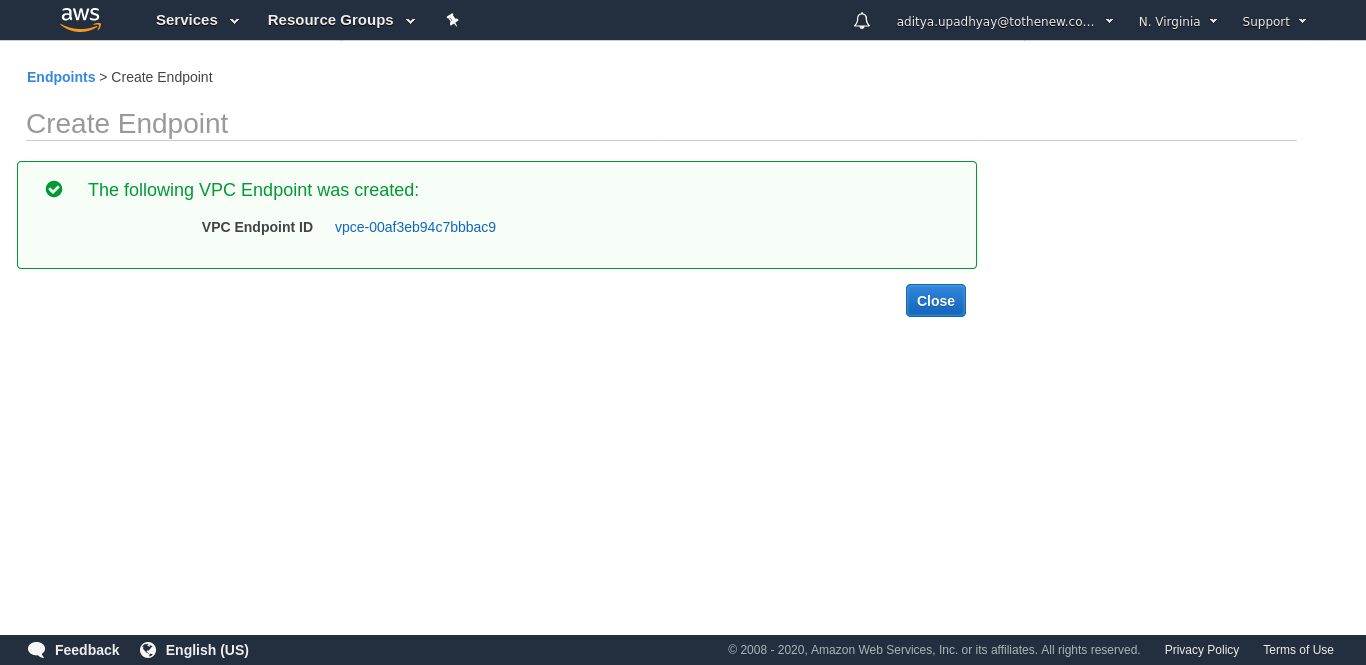
****

**9. S3 VPC endpoint.**

****

****

****

****

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

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

****