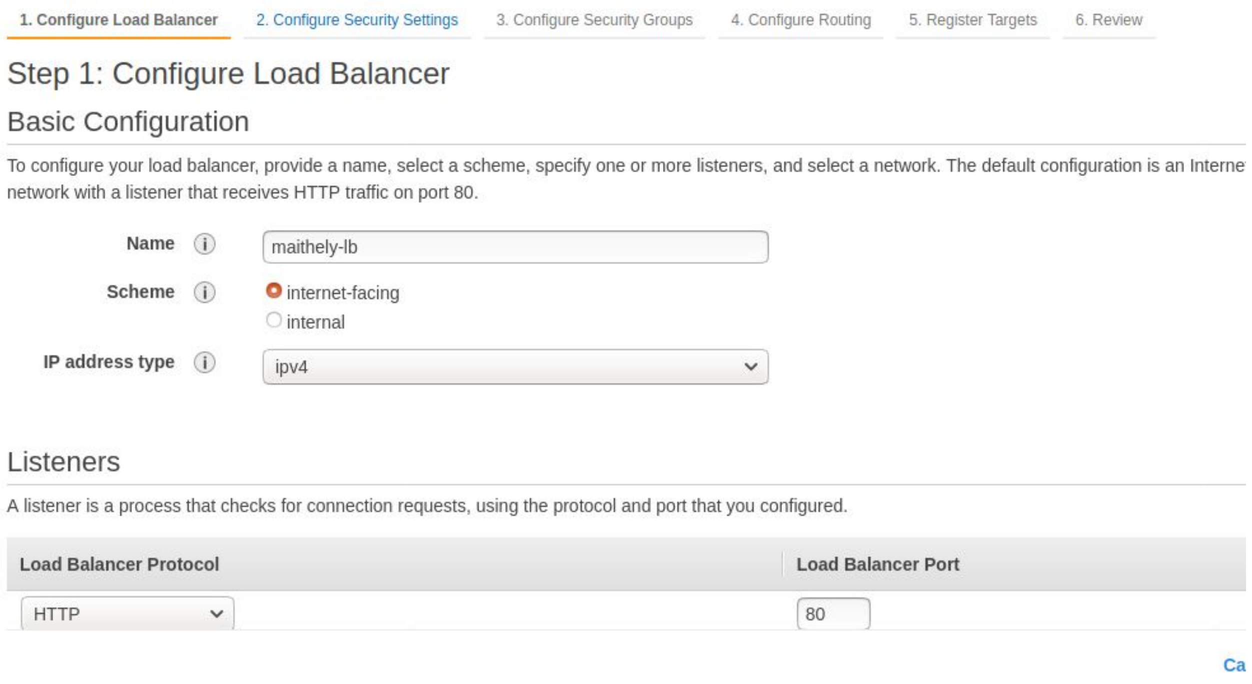
S3,Route 53,DNS

ASSIGNMENT

Name	–	Maithely Sharma
College	–	University of Petroleum and Energy Studies
EmployeeID	–	4057

1) create a private hosted zone named "ttn-internal.com" attached to the default vpc. and created a cname record "myloadbalance.ttn-internal.com" for any load balancer pointed to its dns. Do reverse lookup for the record from any instance of the vpc and share the result.

Firstly create a load balancer in the default VPC


1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Interne network with a listener that receives HTTP traffic on port 80.

Name: maithely-lb

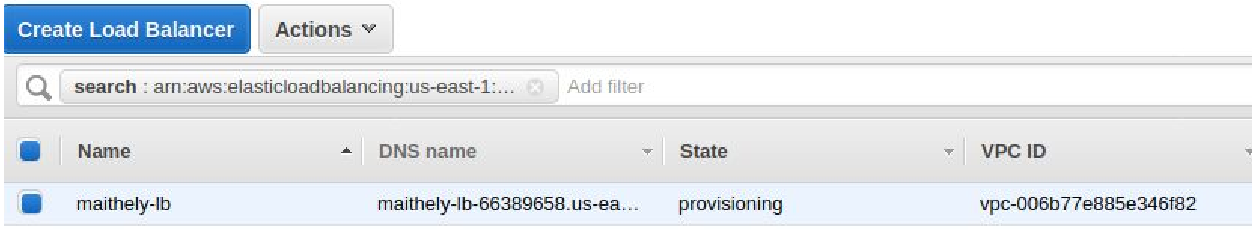
Scheme: ● internet-facing ○ internal

IP address type: ipv4

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

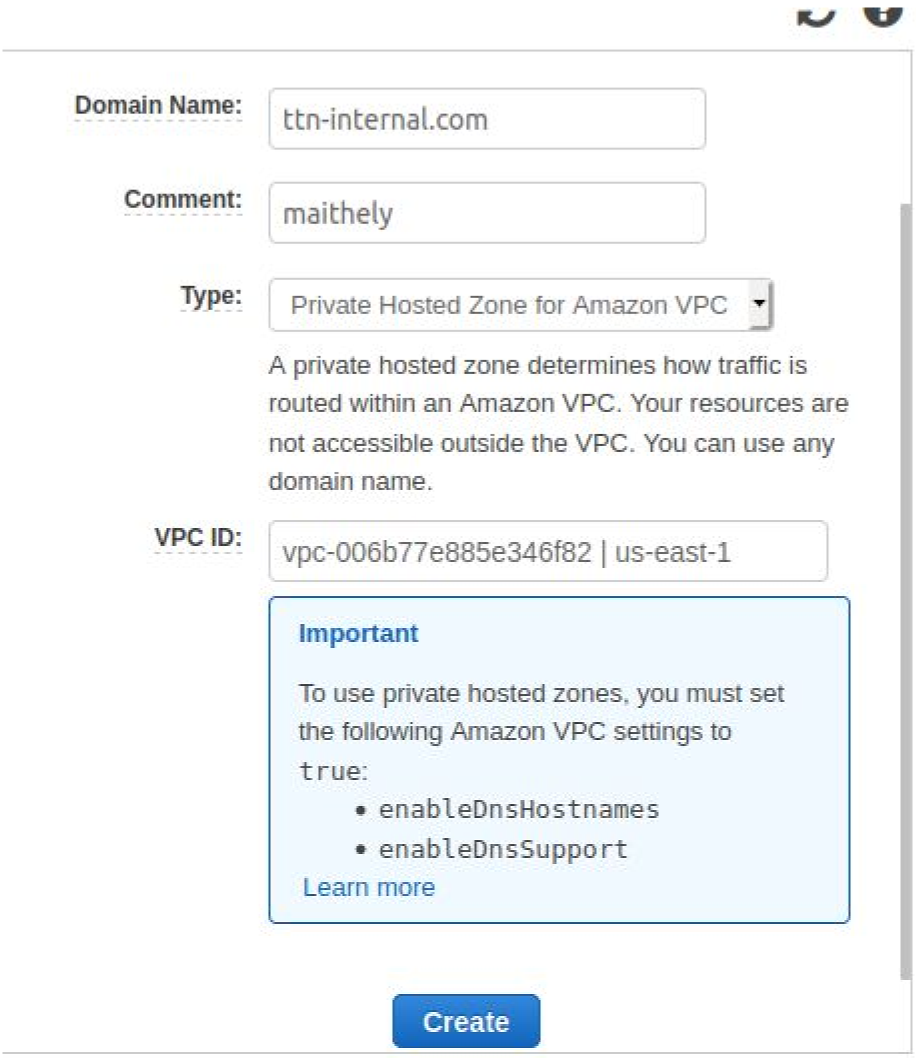
Load Balancer Protocol	Load Balancer Port
HTTP	80



search : arn:aws:elasticloadbalancing:us-east-1:...

Name	DNS name	State	VPC ID
maithely-lb	maithely-lb-66389658.us-ea...	provisioning	vpc-006b77e885e346f82

Now create a private hosted zone in route 53 named “ ttn-internal.com”



Domain Name: ttn-internal.com

Comment: maithely

Type: Private Hosted Zone for Amazon VPC

A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.

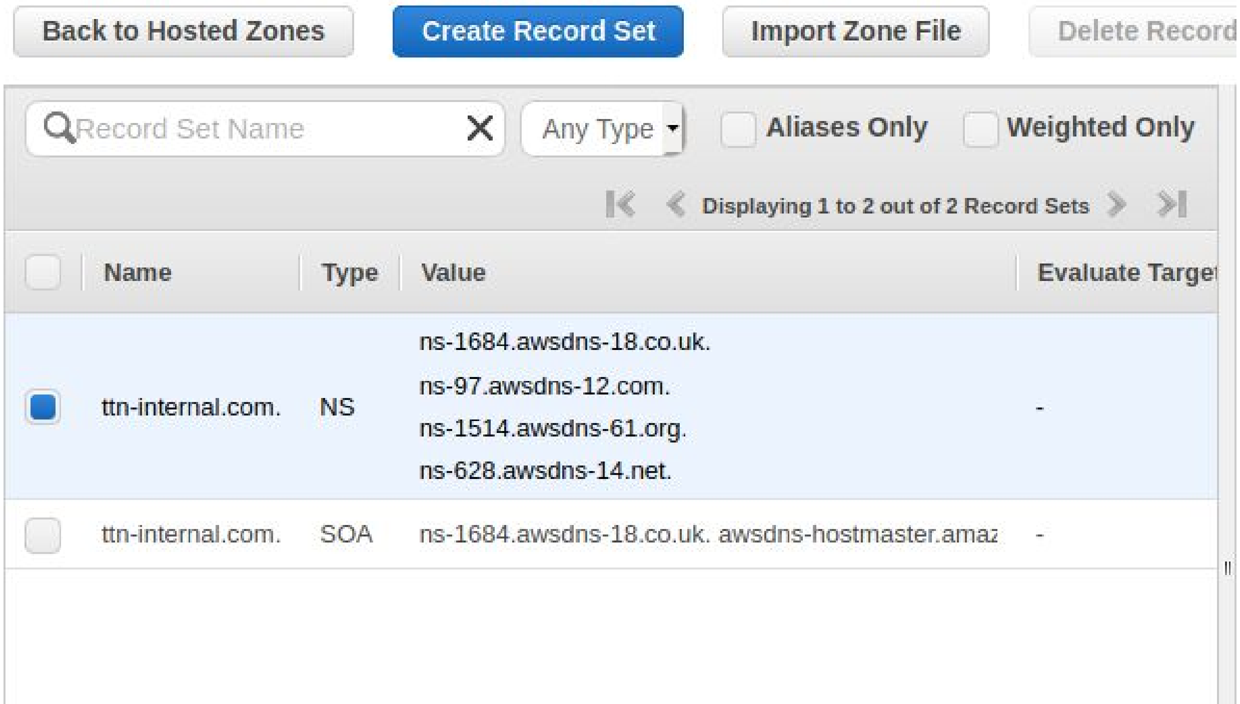
VPC ID: vpc-006b77e885e346f82 | us-east-1

Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

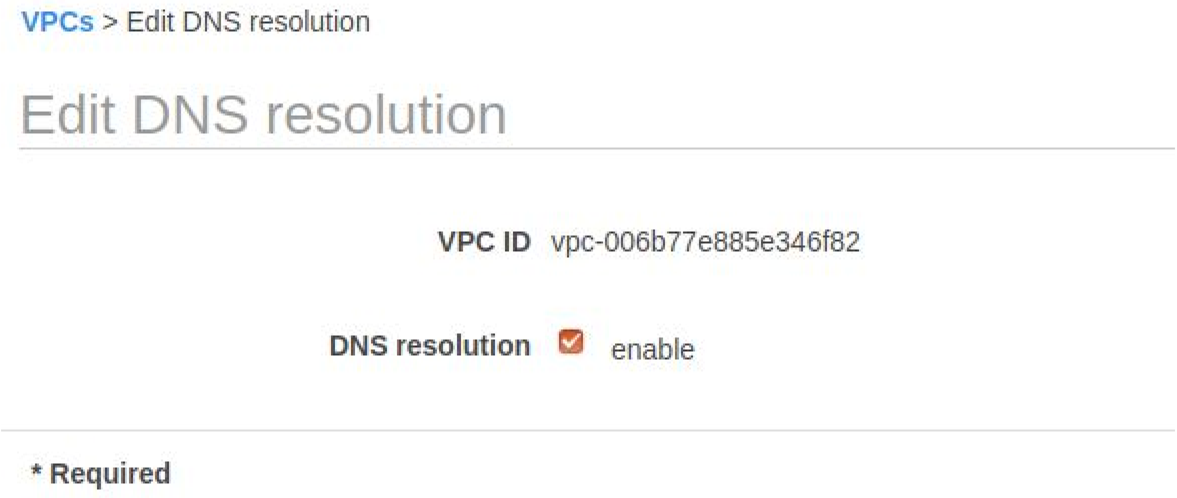
Learn more



Displaying 1 to 2 out of 2 Record Sets

	Name	Type	Value	Evaluate Targe
☑	ttn-internal.com.	NS	ns-1684.awsdns-18.co.uk. ns-97.awsdns-12.com. ns-1514.awsdns-61.org. ns-628.awsdns-14.net.	-
□	ttn-internal.com.	SOA	ns-1684.awsdns-18.co.uk. awsdns-hostmaster.amaz	-

Enable DNS resolution in vpc



VPCs > Edit DNS resolution

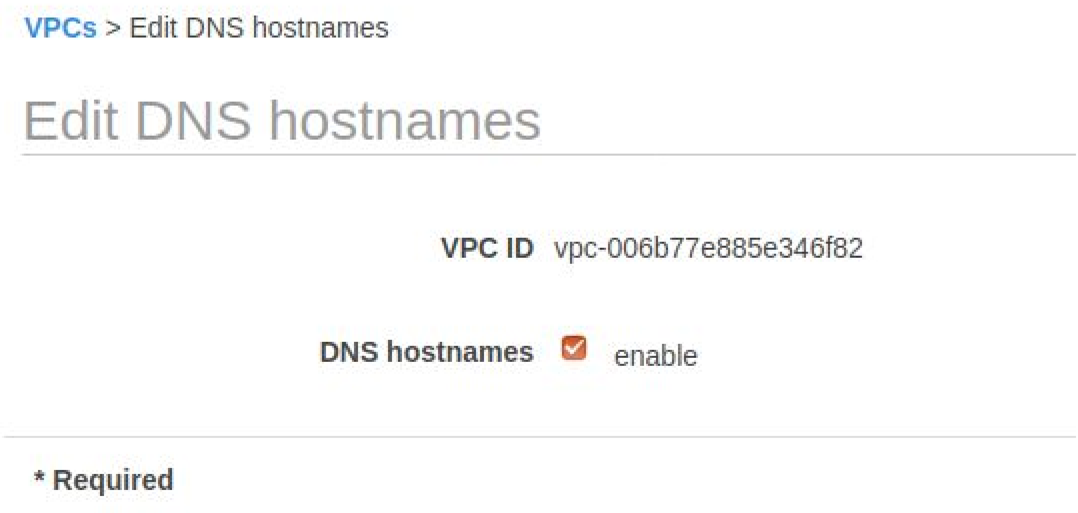
Edit DNS resolution

VPC ID vpc-006b77e885e346f82

DNS resolution ☑ enable

* Required

Enable DNS hostnames in vpc



VPCs > Edit DNS hostnames

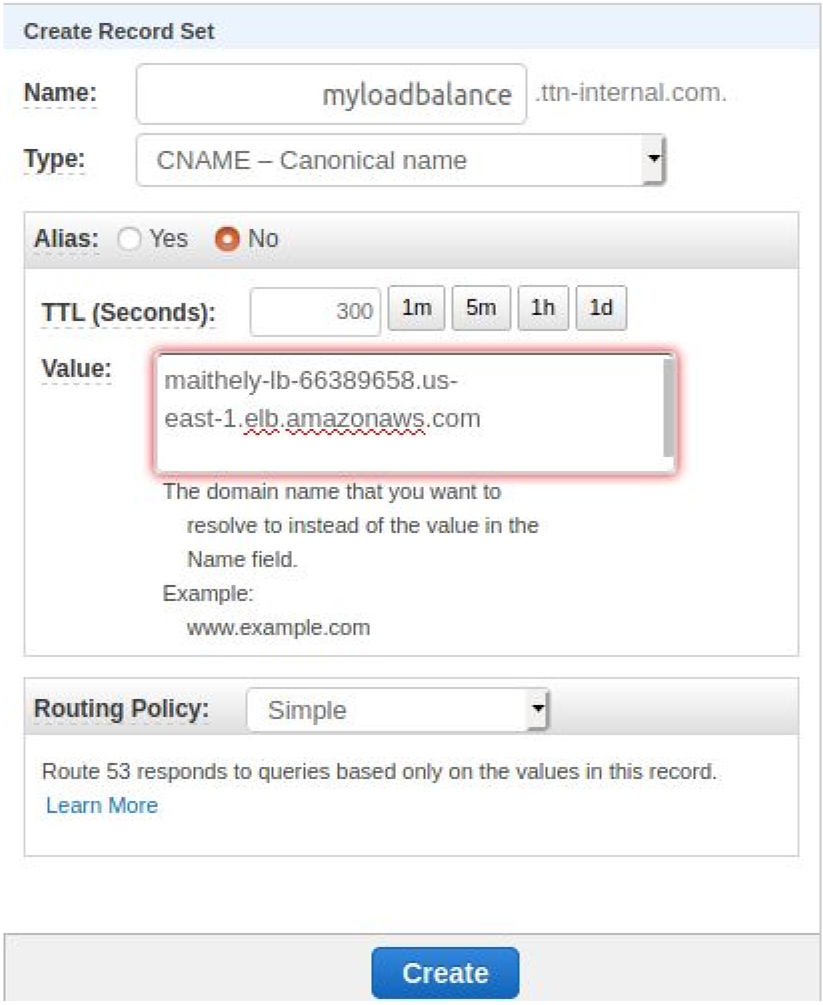
Edit DNS hostnames

VPC ID vpc-006b77e885e346f82

DNS hostnames ☑ enable

* Required

Now route 53> create record set



Create Record Set

Name: myloadbalance .ttn-internal.com.

Type: CNAME – Canonical name

Alias: ○ Yes ● No

TTL (Seconds): 300

Value: maithely-lb-66389658.us-east-1.elb.amazonaws.com

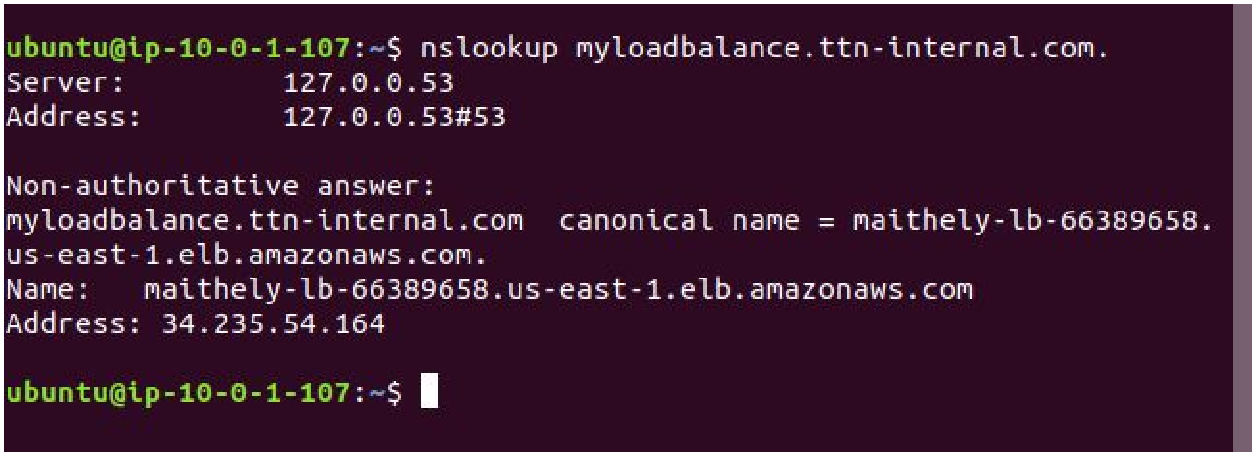
The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record.
Learn More

Now SSH into your instance and then run nslookup command

*nslookup (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain.



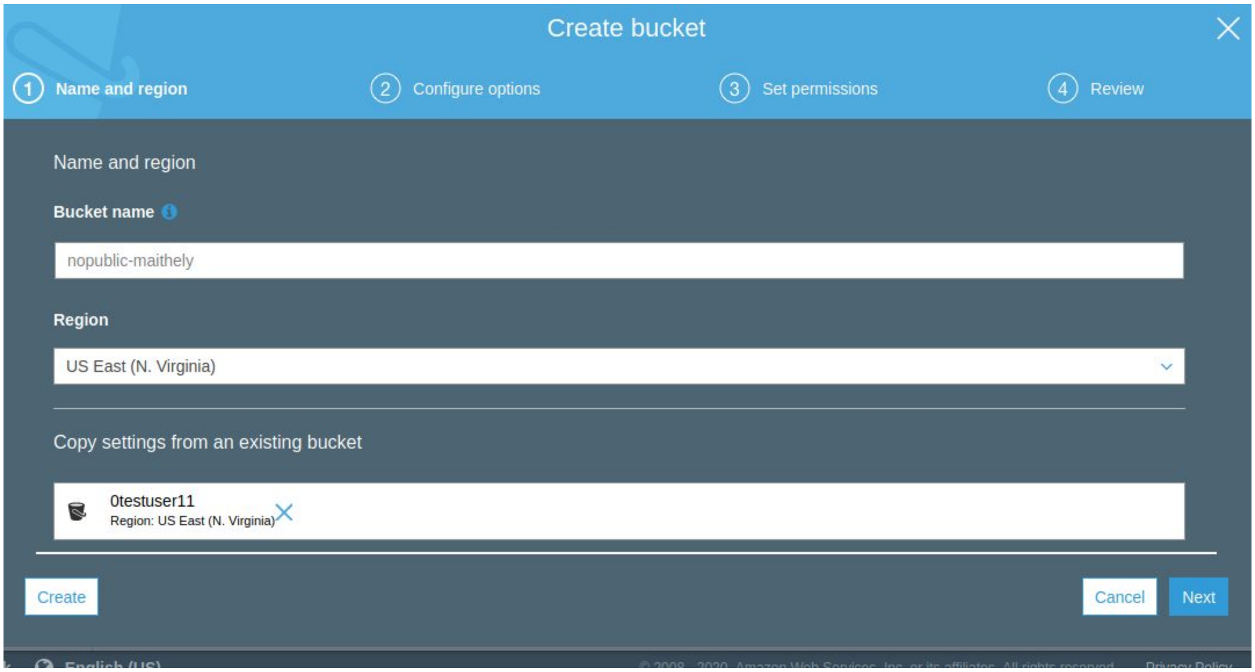
```
ubuntu@ip-10-0-1-107:~$ nslookup myloadbalance.ttn-internal.com.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
myloadbalance.ttn-internal.com  canonical name = maithely-lb-66389658.
us-east-1.elb.amazonaws.com.
Name:   maithely-lb-66389658.us-east-1.elb.amazonaws.com
Address: 34.235.54.164

ubuntu@ip-10-0-1-107:~$ 
```

2) Create a non-public S3 bucket and give appropriate permissions to a server to download objects from bucket but not to put or delete anything in it.

Create s3 bucket with no public access



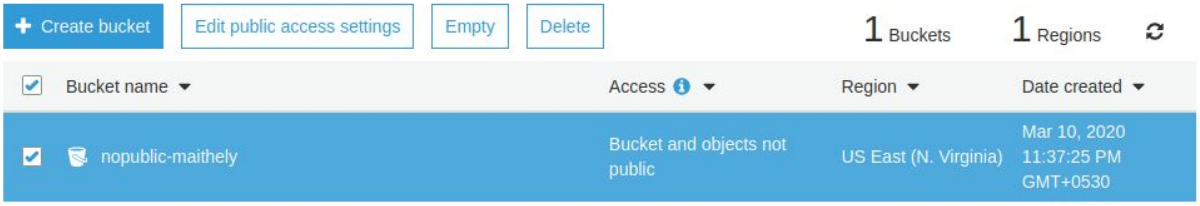
Name and region

Bucket name: nopublic-maithely

Region: US East (N. Virginia)

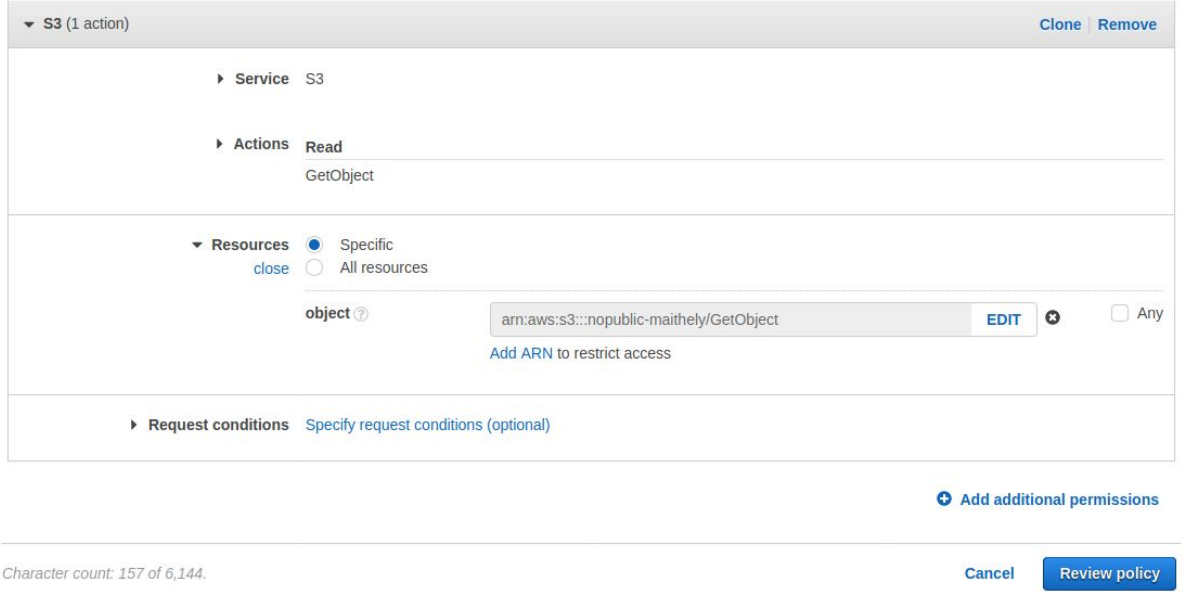
Copy settings from an existing bucket

0testuser11
Region: US East (N. Virginia)



☑ Bucket name	Access	Region	Date created
☑ nopublic-maithely	Bucket and objects not public	US East (N. Virginia)	Mar 10, 2020 11:37:25 PM GMT+0530

Now create a policy only with getobject permission of s3 bucket



Service S3

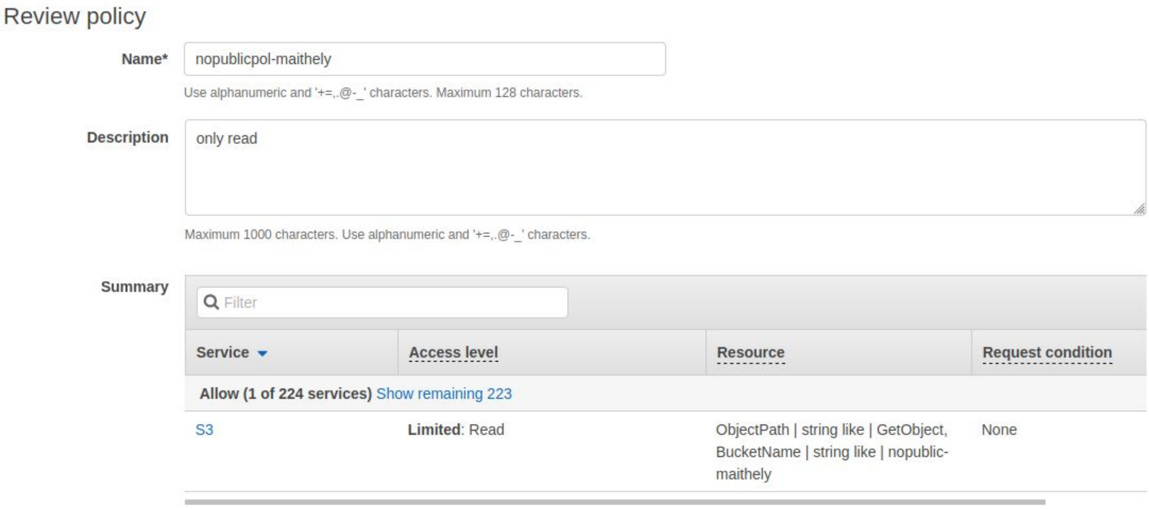
Actions Read
GetObject

Resources ● Specific ○ All resources
close

object arn:aws:s3:::nopublic-maithely/GetObject EDIT □ Any
Add ARN to restrict access

Request conditions Specify request conditions (optional)

Character count: 157 of 6,144.



Review policy

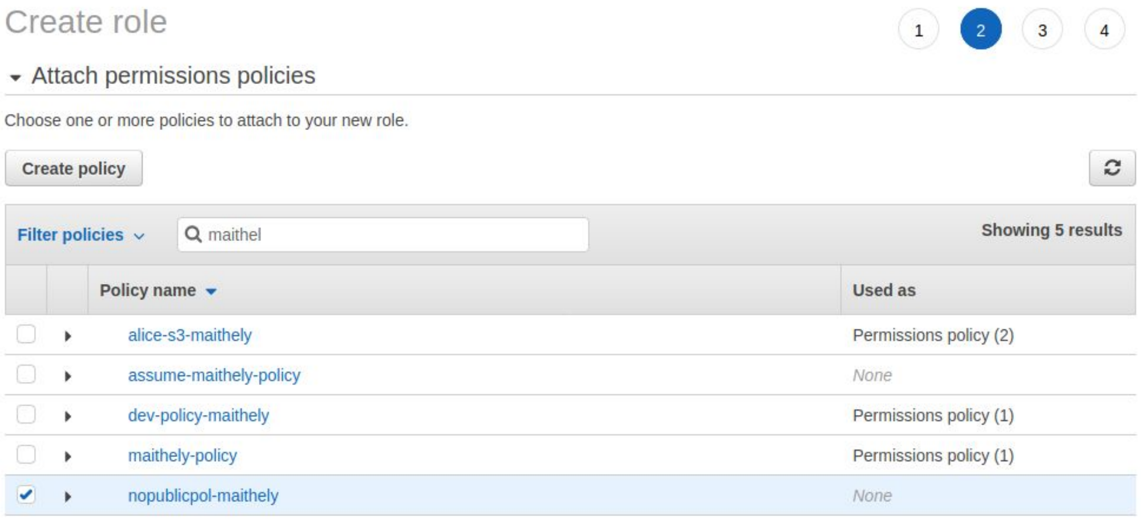
Name* nopublicpol-maithely
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

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

Summary

Service	Access level	Resource	Request condition
Allow (1 of 224 services) Show remaining 223			
S3	**Limited**: Read	ObjectPath | string like | GetObject, BucketName | string like | nopublic-maithely	None

Then create a role and attach the above created policy



Create role

Attach permissions policies

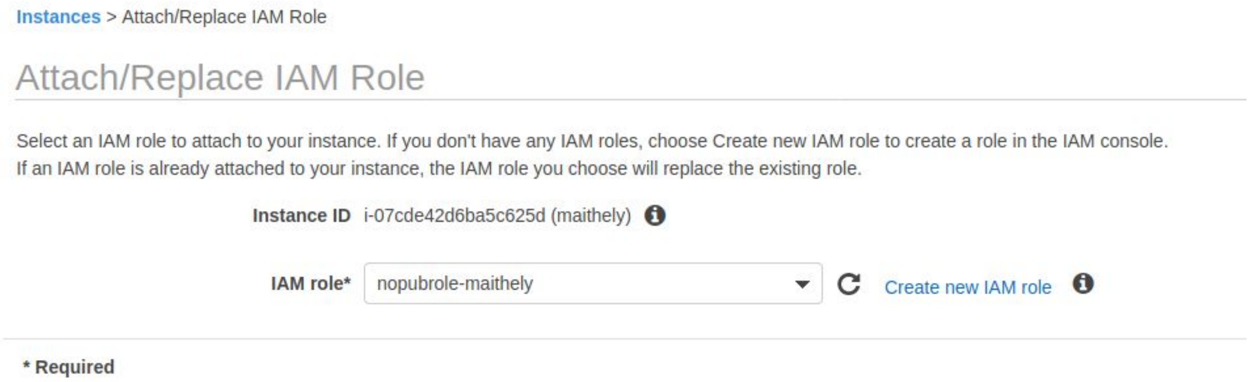
Choose one or more policies to attach to your new role.

maithel

Showing 5 results

	Policy name	Used as
□	alice-s3-maithely	Permissions policy (2)
□	assume-maithely-policy	None
□	dev-policy-maithely	Permissions policy (1)
□	maithely-policy	Permissions policy (1)
☑	nopublicpol-maithely	None

Now create an ec2-instance and attach the role to it



Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

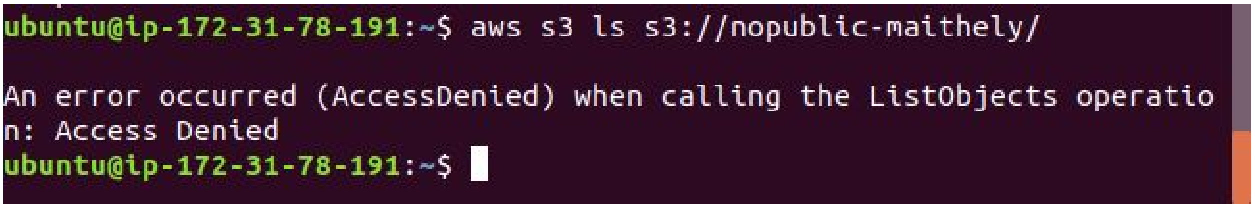
Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-07cde42d6ba5c625d (maithely)

IAM role* nopubrole-maithely

* Required

Now ls into S3 bucket and you can see that the access has been denied



```
ubuntu@ip-172-31-78-191:~$ aws s3 ls s3://nopublic-maithely/

An error occurred (AccessDenied) when calling the ListObjects operatio
n: Access Denied
ubuntu@ip-172-31-78-191:~$
```