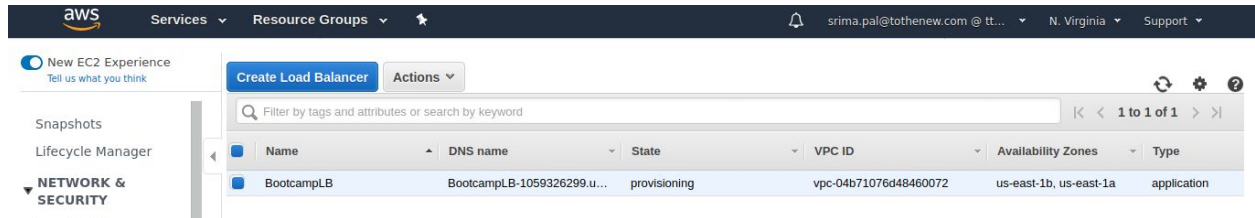
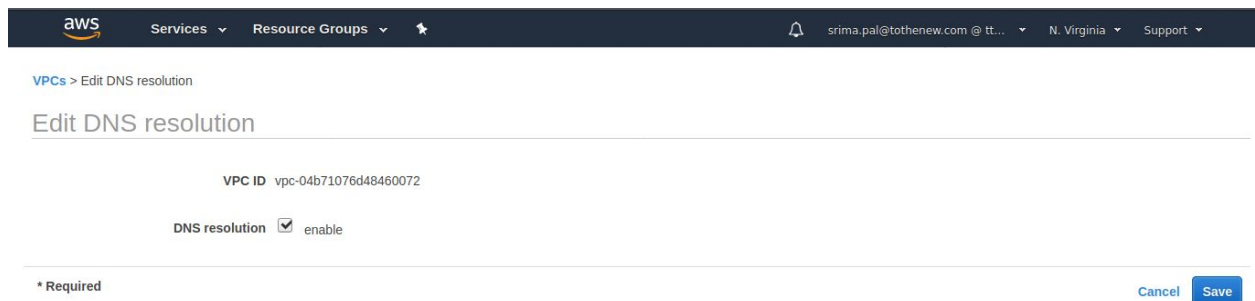
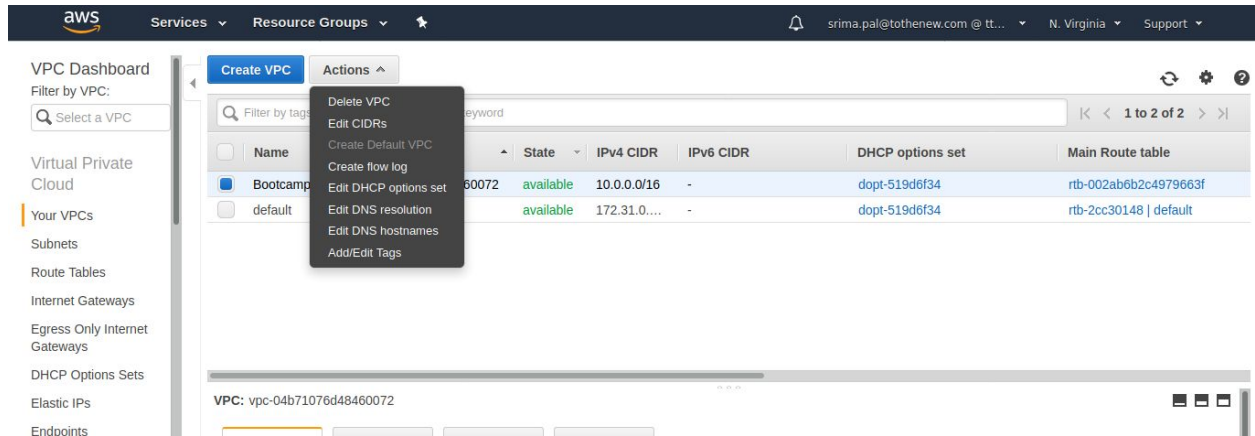


1) Create a private hosted zone named "[ttn-internal.com](https://ttn-internal.com)" attached to the default vpc. and created a cname record "[myloadbalance.ttn-internal.com](https://myloadbalance.ttn-internal.com)" for any load balancer pointed to its dns. Do reverse lookup for the record from any instance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

This is the load balancer



Go to VPC and enable DNS resolution and DNS hostnames



[VPCs](#) > Edit DNS hostnames

## Edit DNS hostnames

VPC ID vpc-04b71076d48460072

DNS hostnames ☒ enable

\* Required

Cancel

Save

Go to route 53 Console and create a private hosted zone

### Create Hosted Zone

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain Name:

Comment:

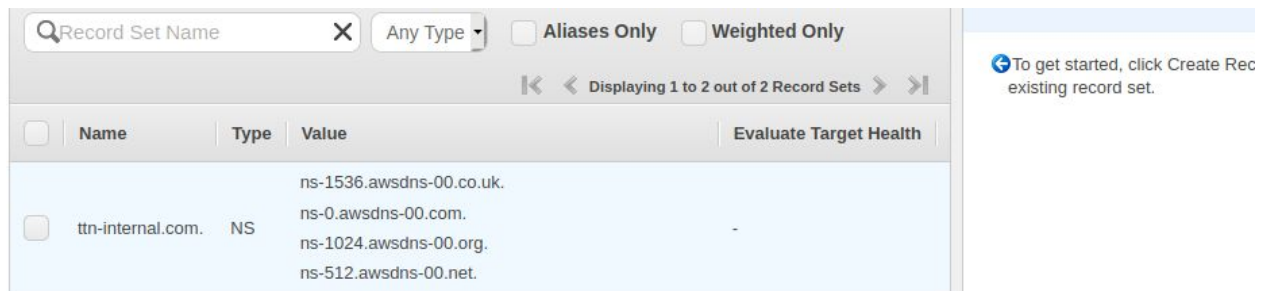
Type:

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:

Create

## Private DNS Created



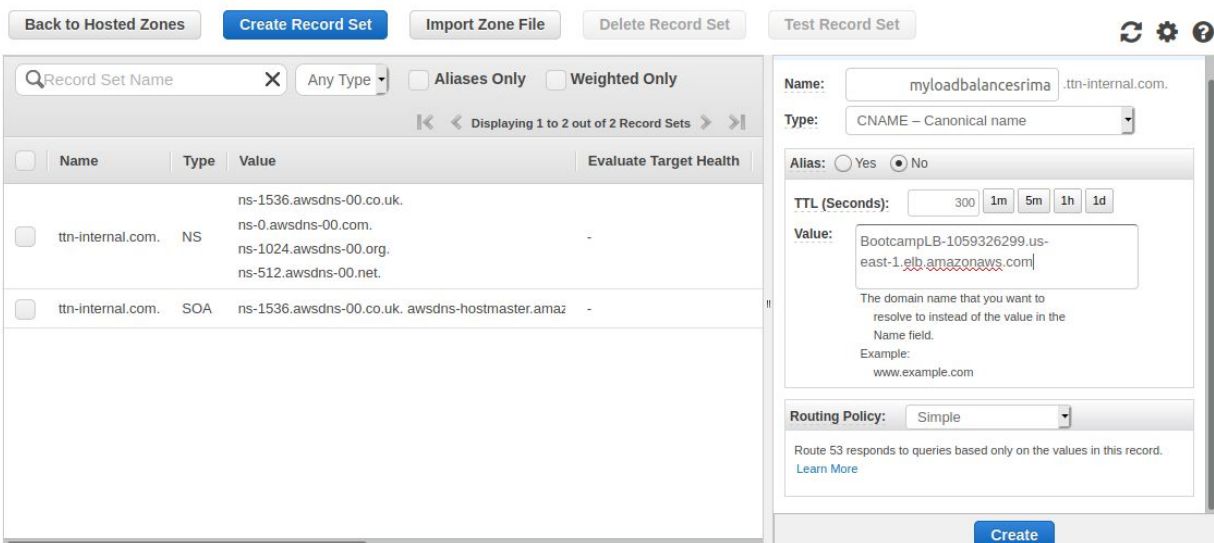
Record Set Name:  X Any Type ☐ Aliases Only ☐ Weighted Only

Displaying 1 to 2 out of 2 Record Sets

Name	Type	Value	Evaluate Target Health
ttn-internal.com.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-

To get started, click Create Record Set or click an existing record set.

## Create Cname record for your load balancer



Back to Hosted Zones Create Record Set Import Zone File Delete Record Set Test Record Set

Record Set Name:  X Any Type ☐ Aliases Only ☐ Weighted Only

Displaying 1 to 2 out of 2 Record Sets

Name	Type	Value	Evaluate Target Health
ttn-internal.com.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
ttn-internal.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-

Name: myloadbalancesrima.ttn-internal.com.

Type: CNAME – Canonical name

Alias: ☐ Yes ☒ No

TTL (Seconds): 300 1m 5m 1h 1d

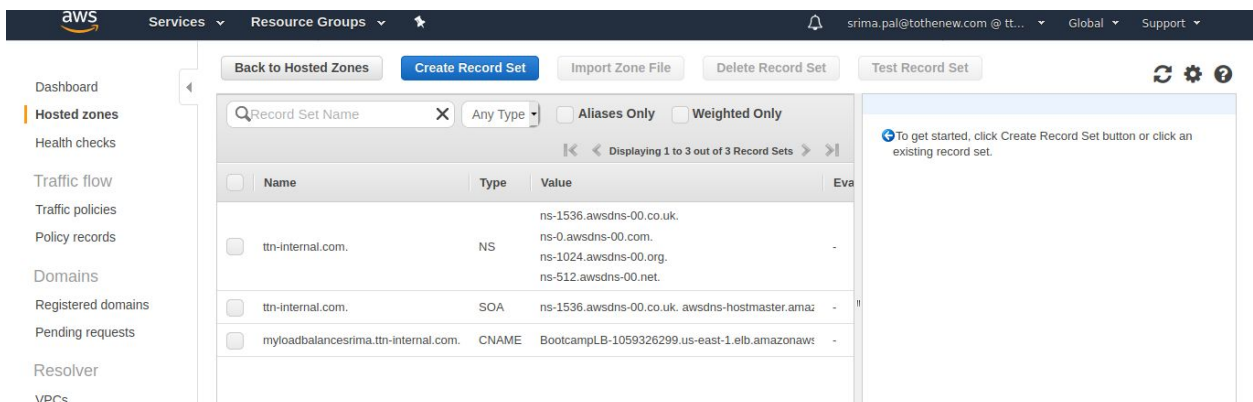
Value: BootcampLB-1059326299.us-east-1.elb.amazonaws.com

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](#)

Create



aws Services Resource Groups

Dashboard Hosted zones Health checks Traffic flow Traffic policies Policy records Domains Registered domains Pending requests Resolver VPCs

Back to Hosted Zones Create Record Set Import Zone File Delete Record Set Test Record Set

Record Set Name:  X Any Type ☐ Aliases Only ☐ Weighted Only

Displaying 1 to 3 out of 3 Record Sets

Name	Type	Value	Eva
ttn-internal.com.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
ttn-internal.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-
myloadbalancesrima.ttn-internal.com.	CNAME	BootcampLB-1059326299.us-east-1.elb.amazonaws	-

To get started, click Create Record Set button or click an existing record set.

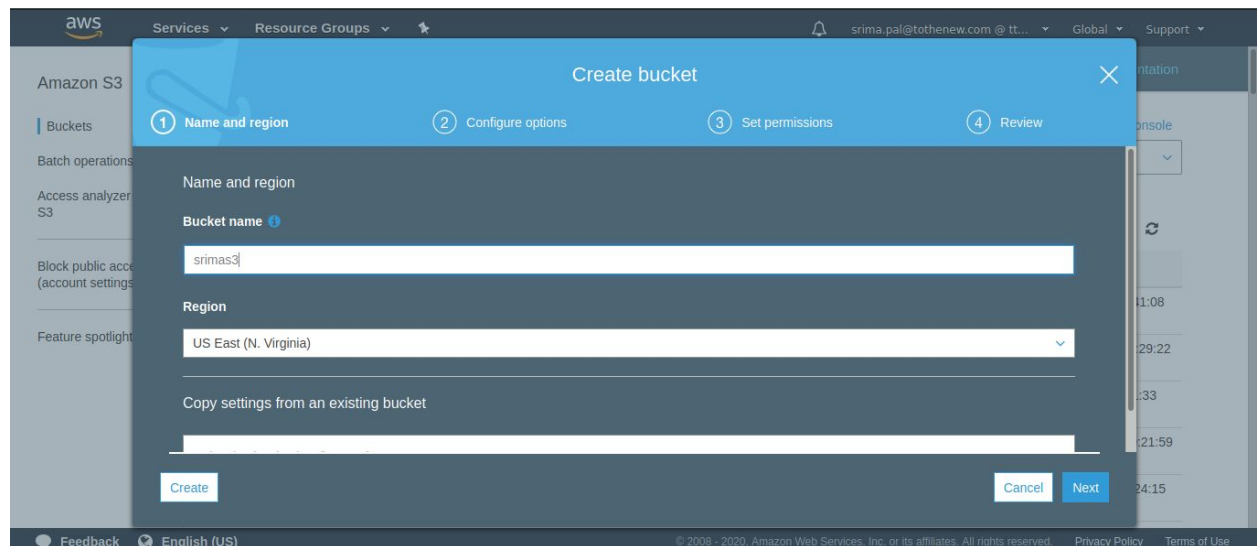
SSH into your instance attached to load balancer and run nslookup command for reverse lookup

```
ubuntu@ip-10-0-2-9:~$ sudo nslookup myloadbalancer.srima.ttn-internal.com.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
myloadbalancer.srima.ttn-internal.com. canonical name = bootcamp-lb-1059326299.us-east-1.elb.amazonaws.com.
Name:      bootcamp-lb-1059326299.us-east-1.elb.amazonaws.com
Address:   54.236.121.47
Name:      bootcamp-lb-1059326299.us-east-1.elb.amazonaws.com
```

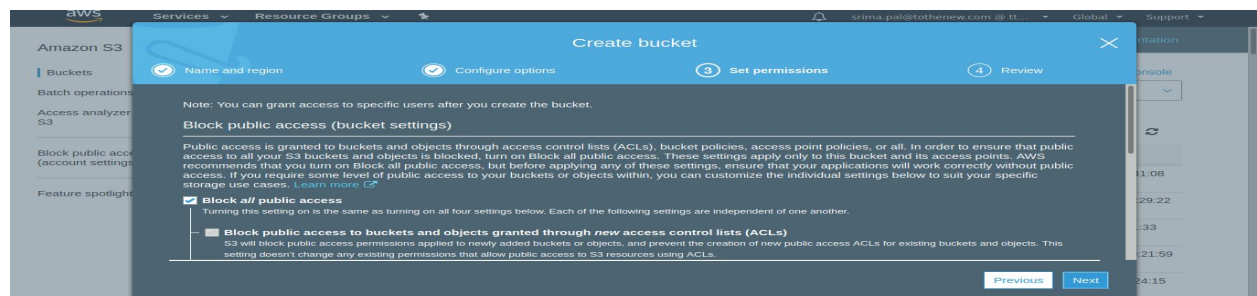
2) Create a non-public S3 bucket and give appropriate permissions to a server to download objects from bucket but not to put or delete anything in it

Create a private bucket



The screenshot shows the AWS Management Console 'Create bucket' wizard. The first step, 'Name and region', is active. The 'Bucket name' field contains 'srimas3'. The 'Region' dropdown is set to 'US East (N. Virginia)'. There is a checkbox for 'Copy settings from an existing bucket' which is currently unchecked. At the bottom, there are 'Create', 'Cancel', and 'Next' buttons.

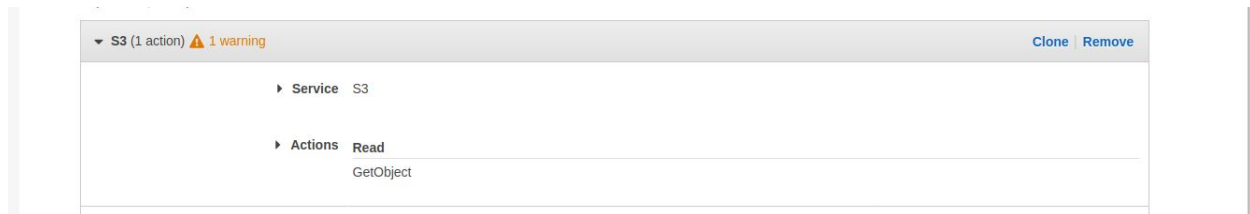
To make private bucket



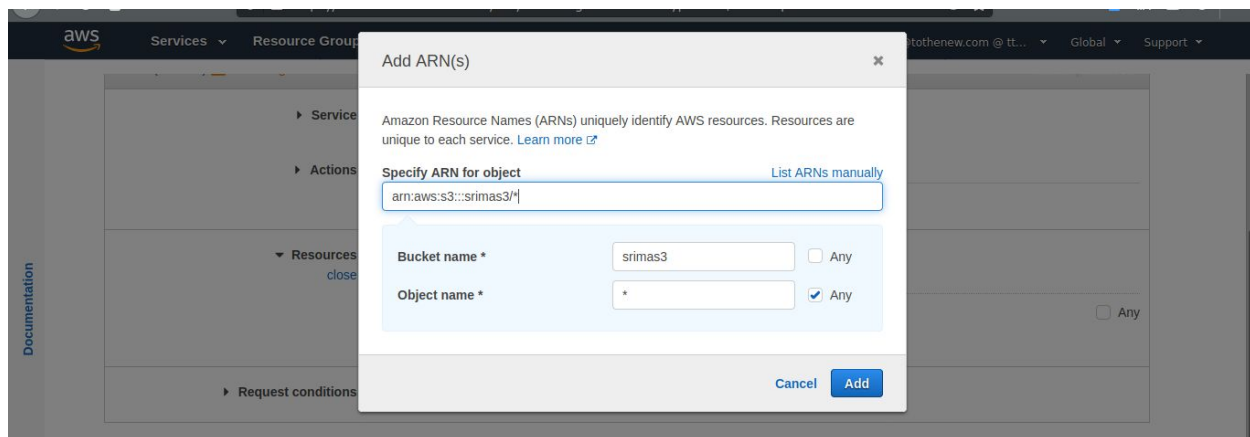
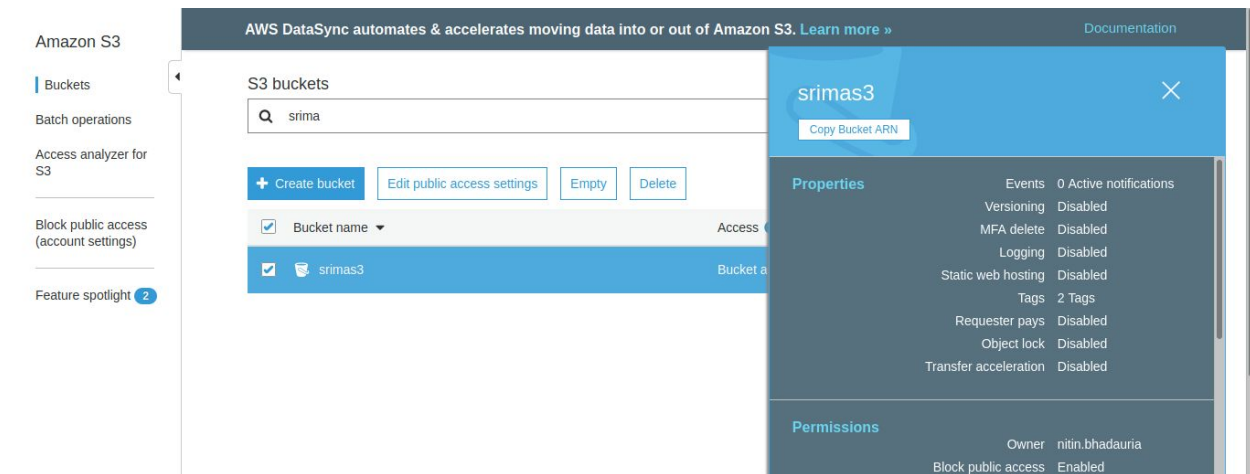
The screenshot shows the 'Set permissions' step of the 'Create bucket' wizard. A note states: 'Note: You can grant access to specific users after you create the bucket. Public access (bucket settings)'. Below this, there is a section titled 'Block all public access' with a checkbox that is checked. The text explains that turning this setting on is the same as turning on all four settings below, which are independent of one another. At the bottom, there are 'Previous' and 'Next' buttons.

G

Go to IAM and make a policy, give getObject(download) permission



Copy bucket ARN



## Create a role to attach to EC2 instance

The screenshot shows the 'Create role' wizard in the AWS IAM console. The first step is 'Select type of trusted entity'. There are four options: 'AWS service' (selected), 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. Below this, the 'Choose a use case' section is active, showing 'Common use cases' with 'EC2' selected. It also lists 'Or select a service to view its use cases' with various services like API Gateway, CodeDeploy, EMR, KMS, RoboMaker, AWS Backup, CodeGuru, ElastiCache, Kinesis, and S3. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

Select type of trusted entity

**AWS service**  
EC2, Lambda and others

**Another AWS account**  
Belonging to you or 3rd party

**Web identity**  
Cognito or any OpenID provider

**SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

**Common use cases**

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway CodeDeploy EMR KMS RoboMaker

AWS Backup CodeGuru ElastiCache Kinesis S3

\* Required

Cancel Next: Permissions

## Attach the created policy

The screenshot shows the 'Attach policies' step of the 'Create role' wizard. It prompts the user to 'Choose one or more policies to attach to your new role.' There is a 'Create policy' button and a search bar with 'srima' entered. A table shows 6 results. The 'Srima-S3-Policy' is selected with a checkmark. At the bottom, there are 'Cancel', 'Previous', and 'Next: Tags' buttons.

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

Create policy

Filter policies  Showing 6 results

	Policy name	Used as
<input type="checkbox"/>	Srima-DataAdmin-Policy	Permissions policy (1)
<input type="checkbox"/>	Srima-Dev-Policy	Permissions policy (2)
<input type="checkbox"/>	Srima-Policy	Permissions policy (1)
<input type="checkbox"/>	Srima-Prod-Policy	Permissions policy (1)
<input checked="" type="checkbox"/>	Srima-S3-Policy	None
<input type="checkbox"/>	SrimaDevSubnetPolicy	Permissions policy (1)

\* Required

Cancel Previous Next: Tags

## Create Role

The screenshot shows the 'Roles' page in the AWS IAM console. A green notification banner at the top states 'The role Srima-S3-Role has been created.' Below this, there are 'Create role' and 'Delete role' buttons. A search bar shows 'srima' and a table lists 4 results. The left sidebar shows the 'Identity and Access Management (IAM)' menu with 'Roles' selected.

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

**Roles**

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

The role Srima-S3-Role has been created.

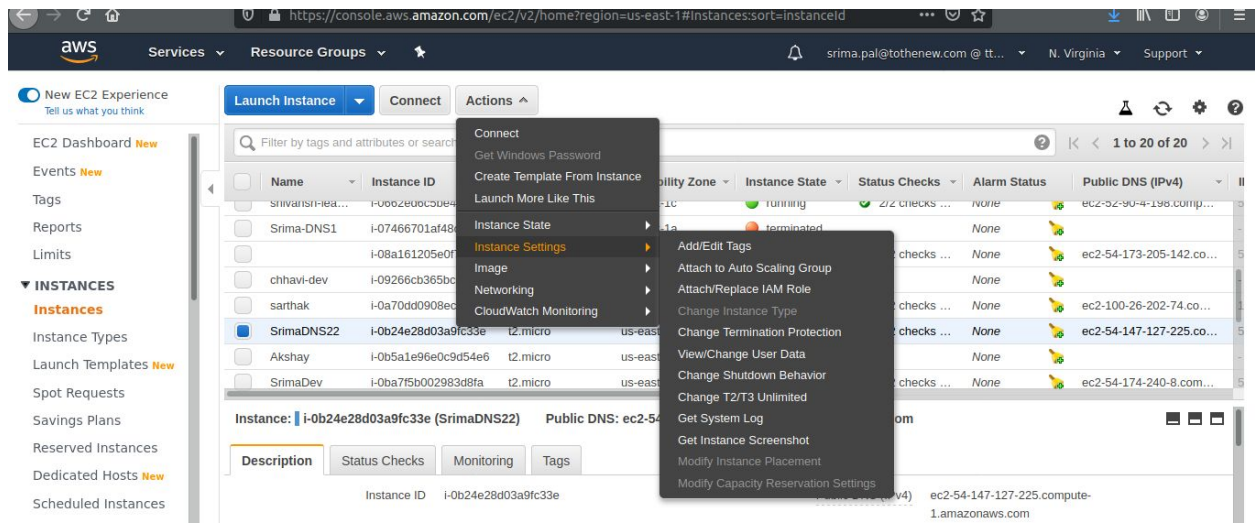
Create role Delete role

Showing 4 results

Role name	Trusted entities	Last activity
<input type="checkbox"/> S3FullAccessSrima	Account: 187632318301	None
<input type="checkbox"/> Srima-S3-Role	AWS service: ec2	None
<input type="checkbox"/> SrimaAssumeRole	AWS service: ec2	Yesterday
<input type="checkbox"/> SrimaJavaS3FullAccess	AWS service: ec2	Today



## Attach the role to instance



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-0b24e28d03a9fc33e (SrimaDNS22)

IAM role\* Srima-S3-Role



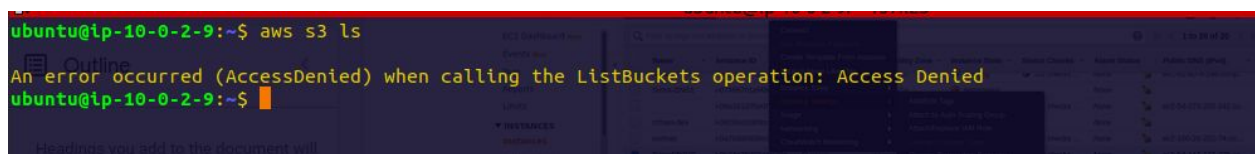
Create new IAM role

\* Required

Cancel

Apply

## Try to list objects(Not allowed)



## Upload content in bucket and run the command(used already created bucket)

