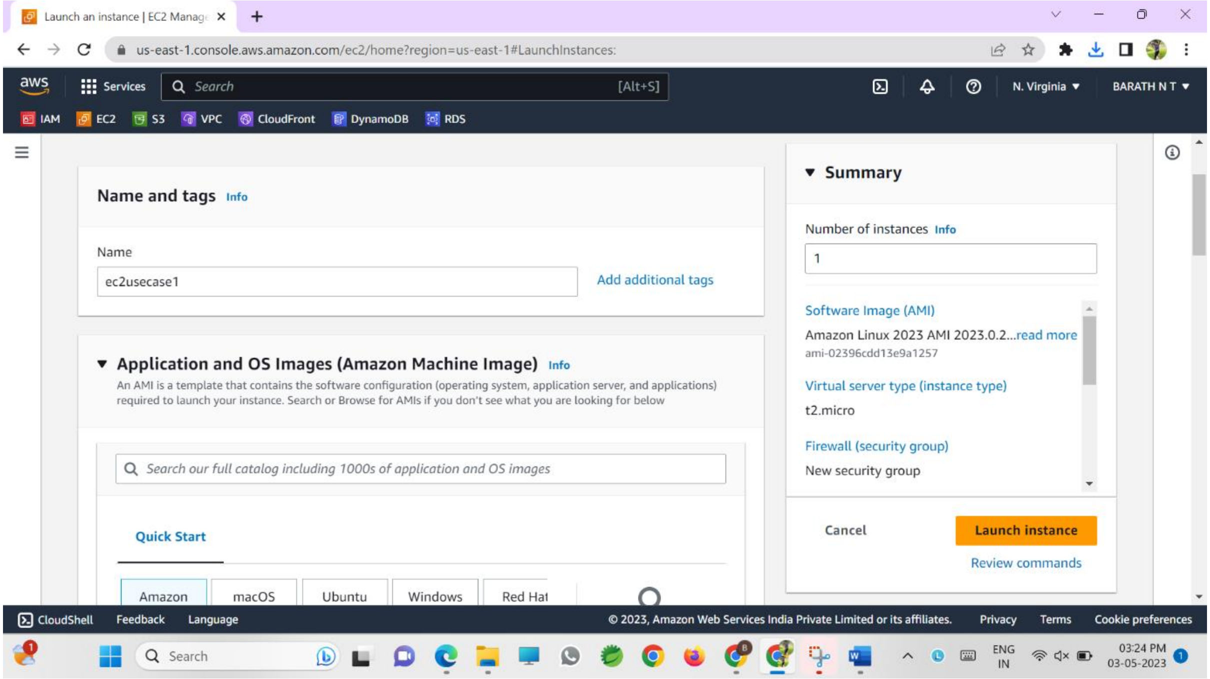
AWS CLOUD CC-1

727721EUIT021-BARATH

1.Create an EC2 Instance in the us-east-1 region with the following requirements.



Name and tags Info

Name: ec2usecase1

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

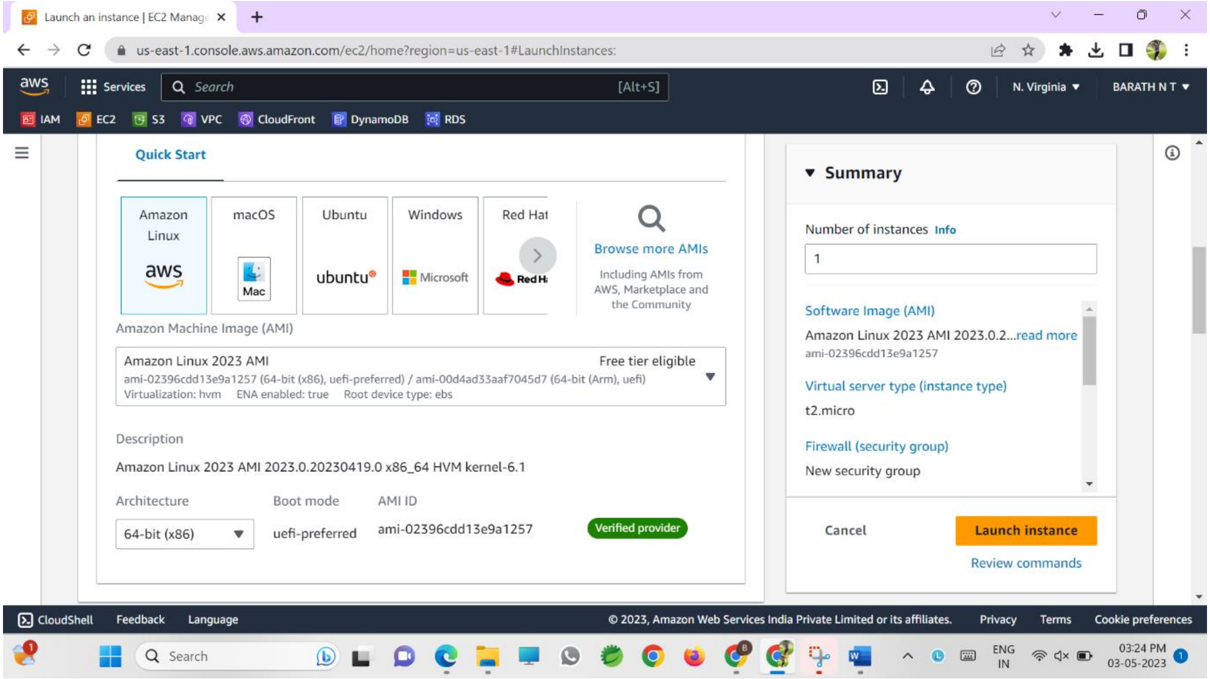
Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-02396cdd13e9a1257

Virtual server type (instance type): t2.micro

Firewall (security group): New security group



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-02396cdd13e9a1257 (64-bit (x86), uefi-preferred) / ami-00d4ad33aaf7045d7 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.0.20230419.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86)	uefi-preferred	ami-02396cdd13e9a1257	Verified provider

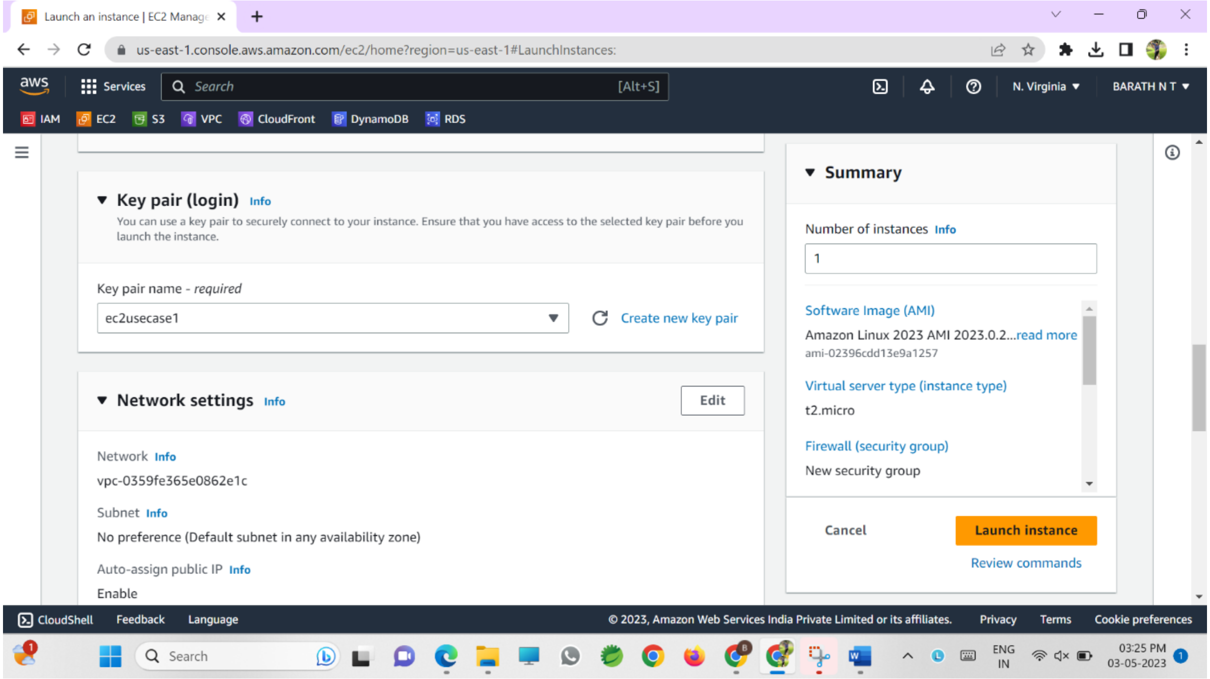
Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-02396cdd13e9a1257

Virtual server type (instance type): t2.micro

Firewall (security group): New security group


Launch an instance | EC2 Manage
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search
[Alt+S]
N. Virginia
BARATH N T
IAM
EC2
S3
VPC
CloudFront
DynamoDB
RDS
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
03:25 PM
03-05-2023

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

ec2usecase1

Create new key pair

Network settings Info

Edit

Network Info

vpc-0359fe365e0862e1c

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2...read more

ami-02396cdd13e9a1257

Virtual server type (instance type)

t2.micro

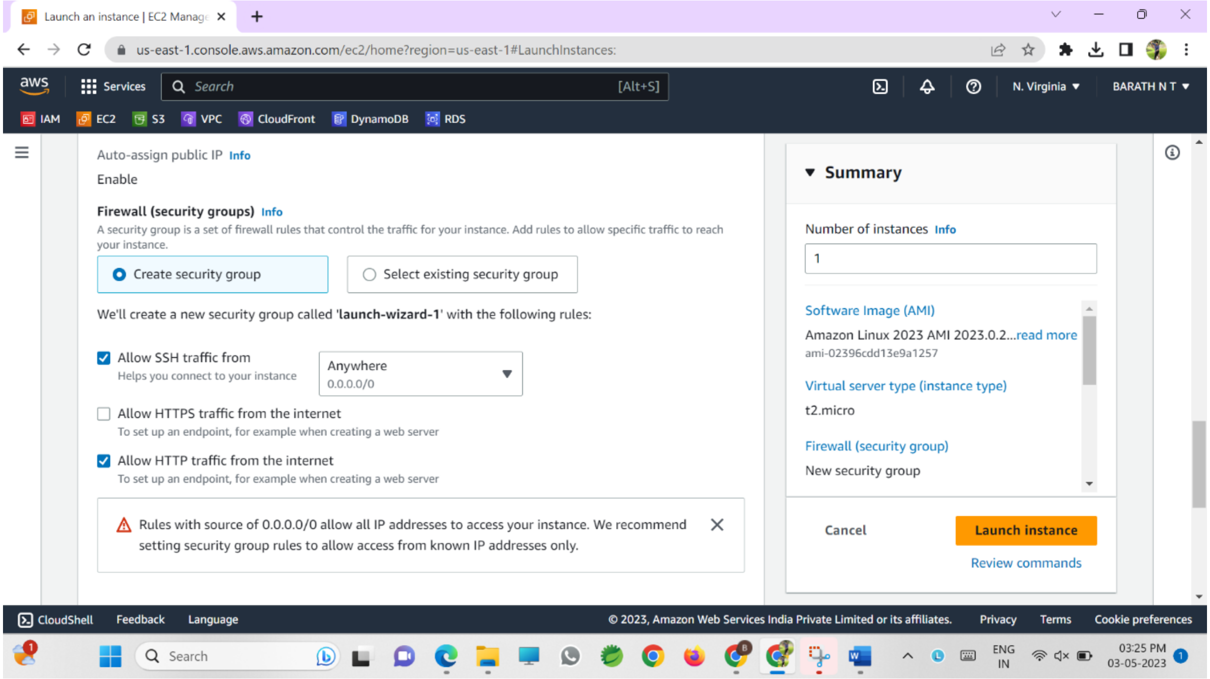
Firewall (security group)

New security group

Cancel

Launch instance

Review commands


Launch an instance | EC2 Manage
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search
[Alt+S]
N. Virginia
BARATH N T
IAM
EC2
S3
VPC
CloudFront
DynamoDB
RDS
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
03:25 PM
03-05-2023

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0

Helps you connect to your instance

□ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2...read more

ami-02396cdd13e9a1257

Virtual server type (instance type)

t2.micro

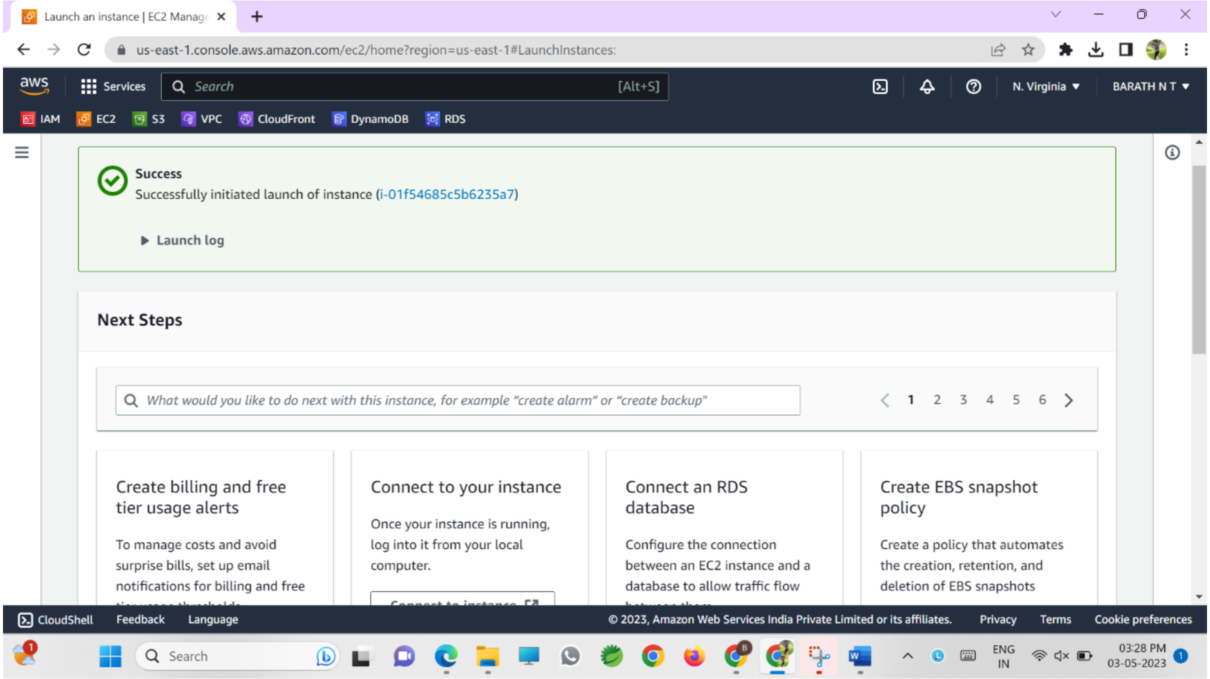
Firewall (security group)

New security group

Cancel

Launch instance

Review commands



Launch an instance | EC2 Manag
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search
[Alt+S]
N. Virginia
BARATH N T
IAM
EC2
S3
VPC
CloudFront
DynamoDB
RDS
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
03:28 PM
03-05-2023

Success

Successfully initiated launch of instance (i-01f54685c5b6235a7)

▶ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

1 2 3 4 5 6

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free

Connect to your instance

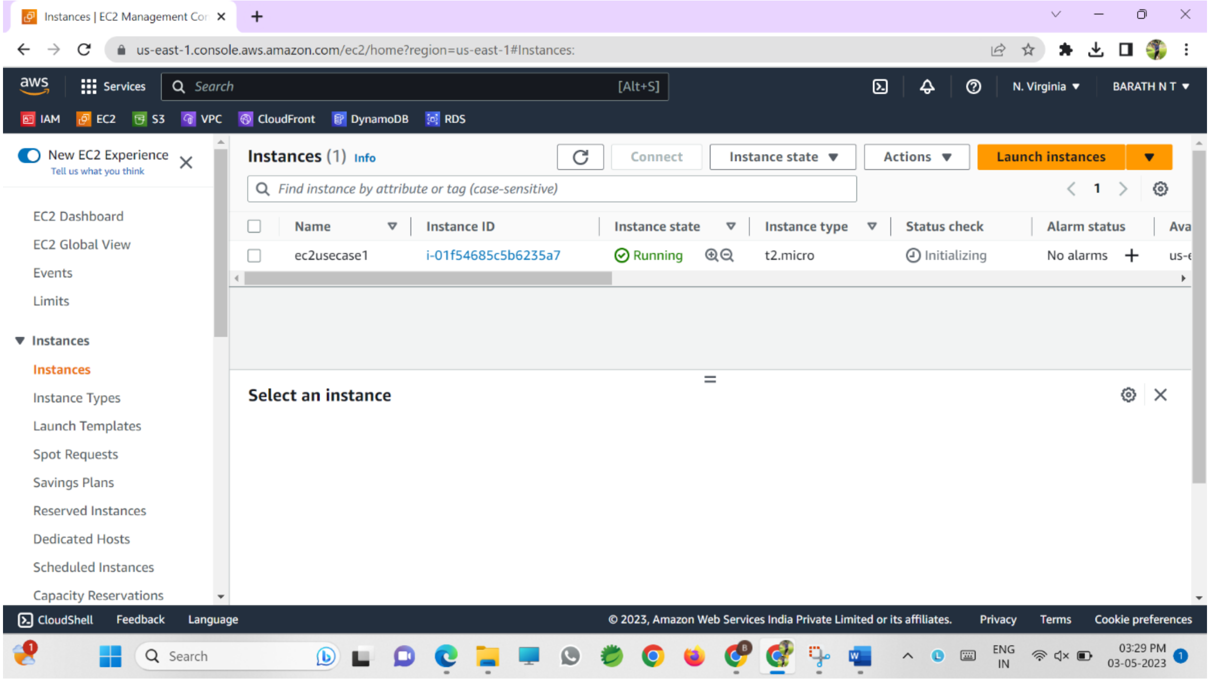
Once your instance is running, log into it from your local computer.

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots



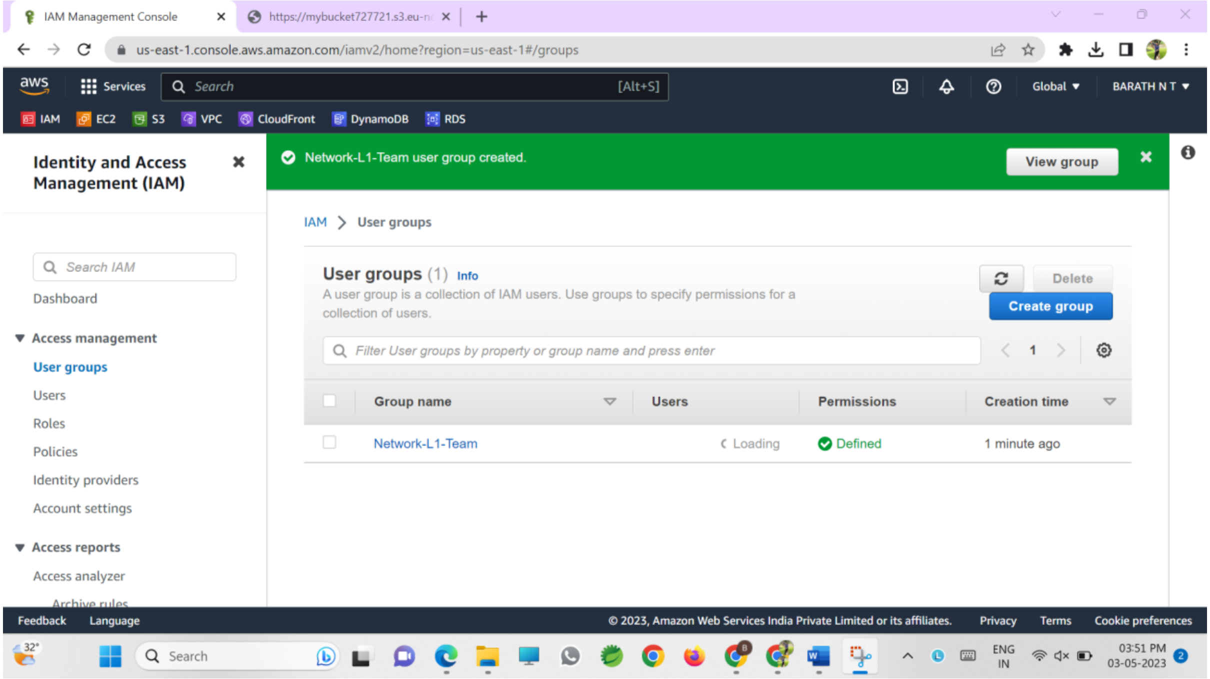
Instances (1) Info

Find instance by attribute or tag (case-sensitive)

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Ava
□	ec2usecase1	i-01f54685c5b6235a7	Running	t2.micro	Initializing	No alarms	us-e

Select an instance

2.Create an IAM group called ‘Network-L1-Team’…



us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups

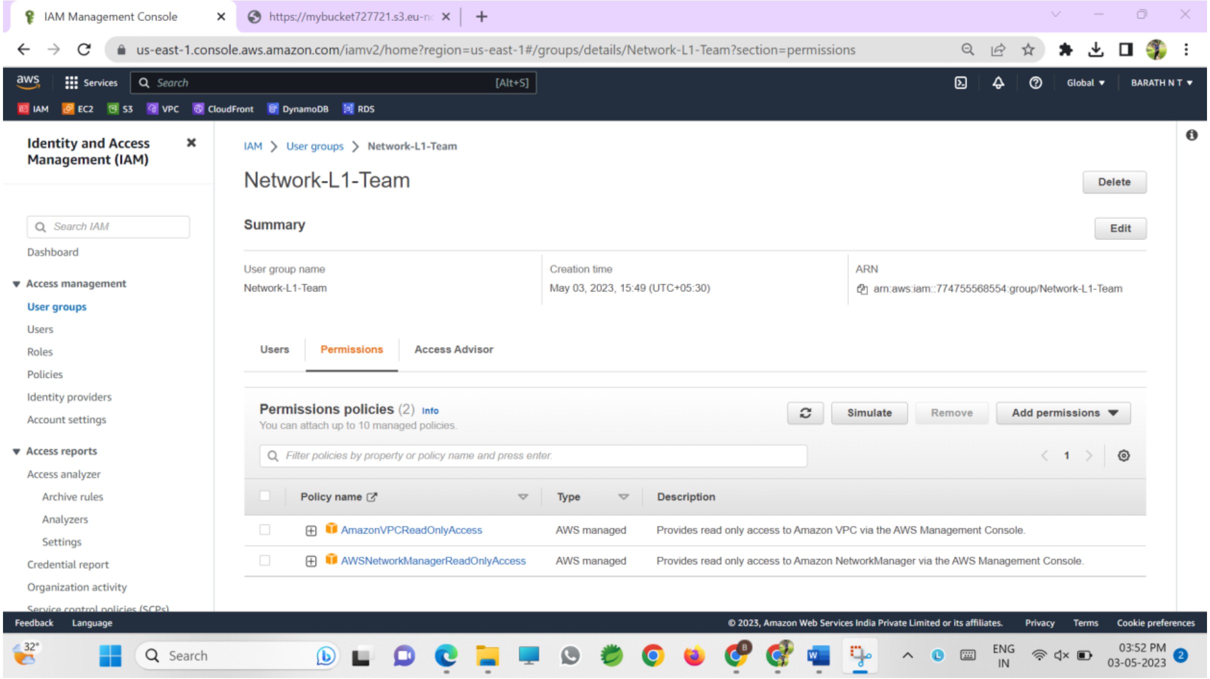
Network-L1-Team user group created.

IAM > User groups

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
Network-L1-Team	Loading	✓ Defined	1 minute ago



us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/Network-L1-Team?section=permissions

IAM > User groups > Network-L1-Team

Network-L1-Team

Summary

User group name: Network-L1-Team

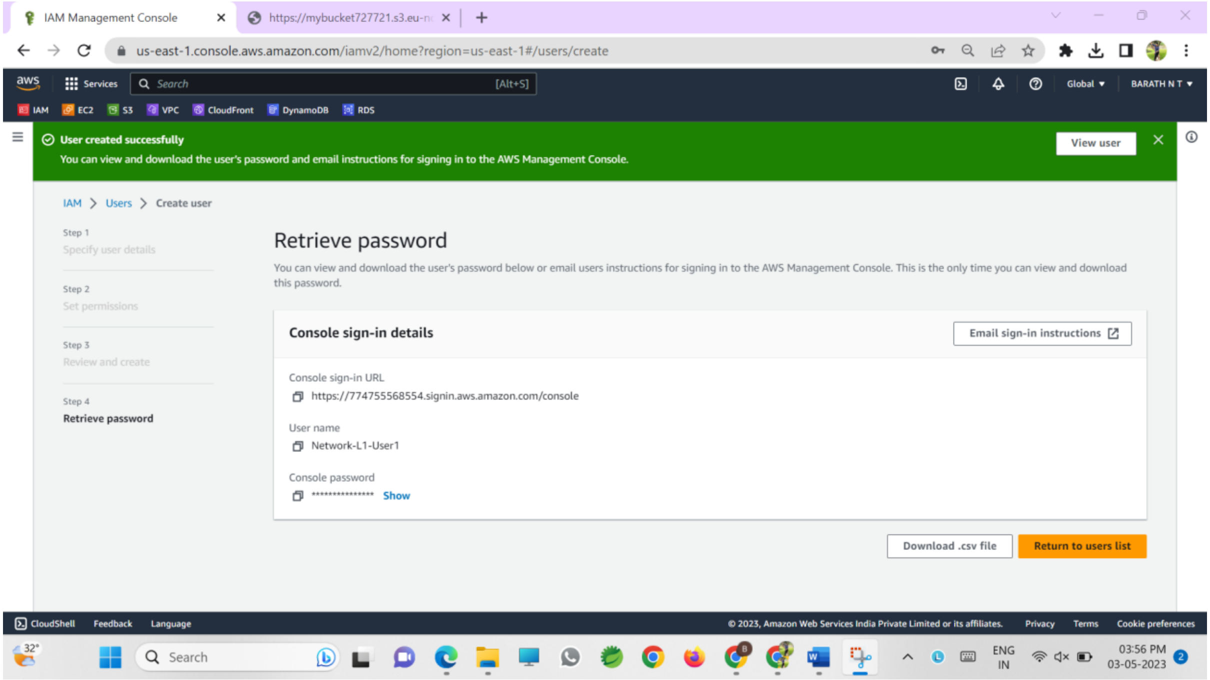
Creation time: May 03, 2023, 15:49 (UTC+05:30)

ARN: arn:aws:iam::774755568554:group/Network-L1-Team

Permissions policies (2) Info

You can attach up to 10 managed policies.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console.
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon NetworkManager via the AWS Management Console.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

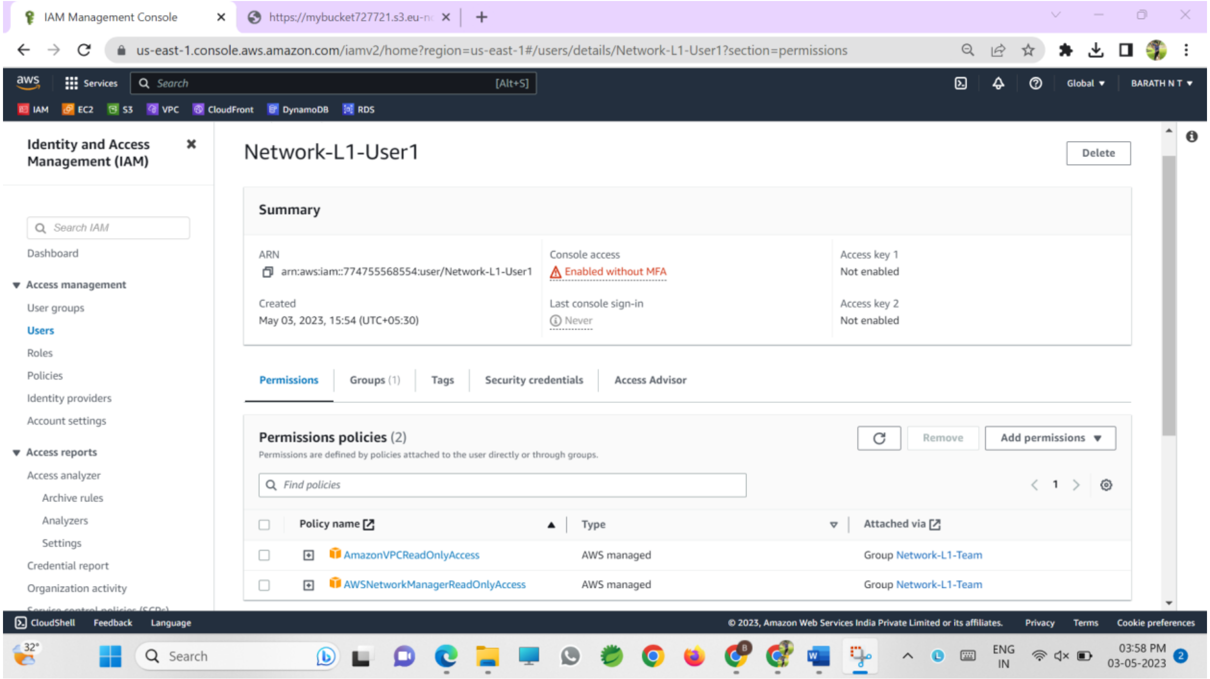
Console sign-in details

Console sign-in URL
https://774755568554.signin.aws.amazon.com/console

User name
Network-L1-User1

Console password
*************** Show

© 2023, Amazon Web Services India Private Limited or its affiliates.



Network-L1-User1

Summary

ARN arn:aws:iam::774755568554:user/Network-L1-User1	Console access Enabled without MFA	Access key 1 Not enabled
Created May 03, 2023, 15:54 (UTC+05:30)	Last console sign-in Never	Access key 2 Not enabled

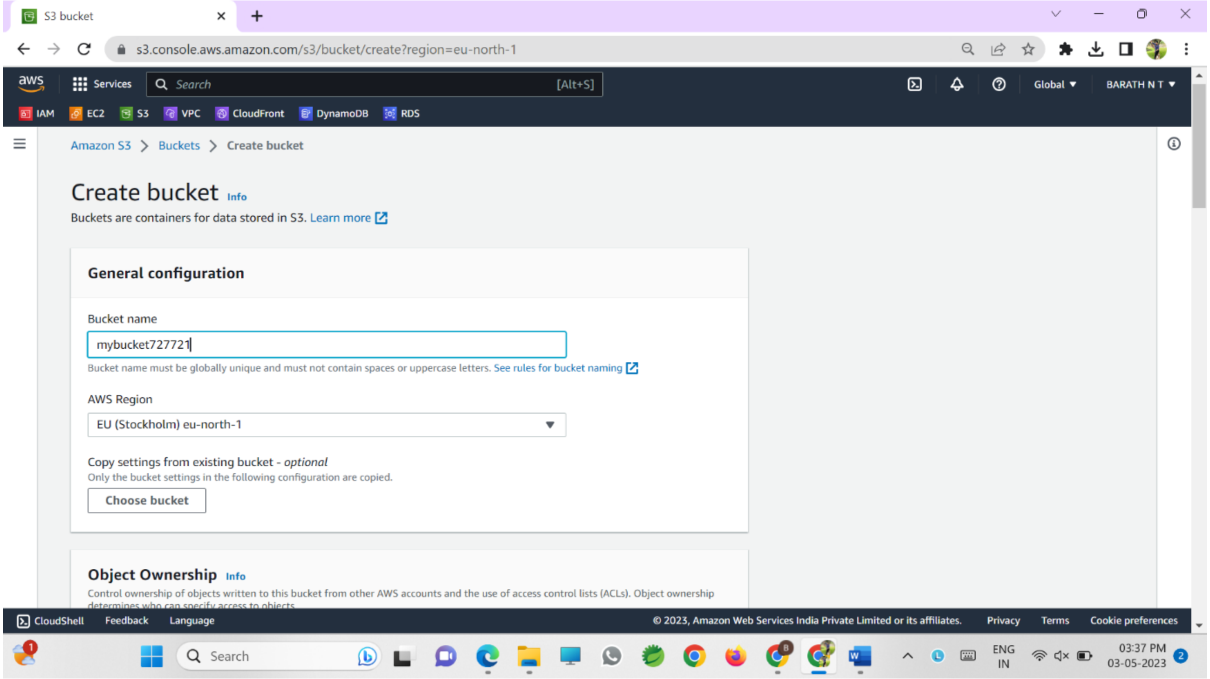
Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonVPCReadOnlyAccess	AWS managed	Group Network-L1-Team
AWSNetworkManagerReadOnlyAccess	AWS managed	Group Network-L1-Team

© 2023, Amazon Web Services India Private Limited or its affiliates.

3.Create a S3 bucket for the following requirements.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

mybucket727721

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

EU (Stockholm) eu-north-1

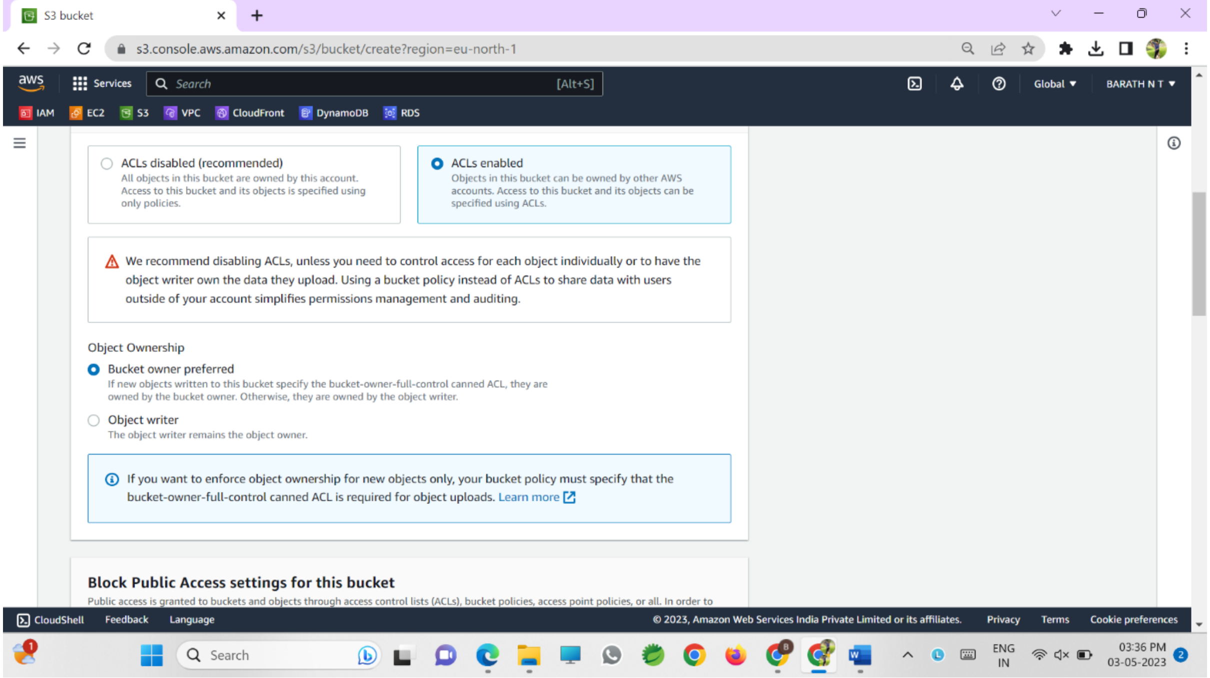
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.



○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

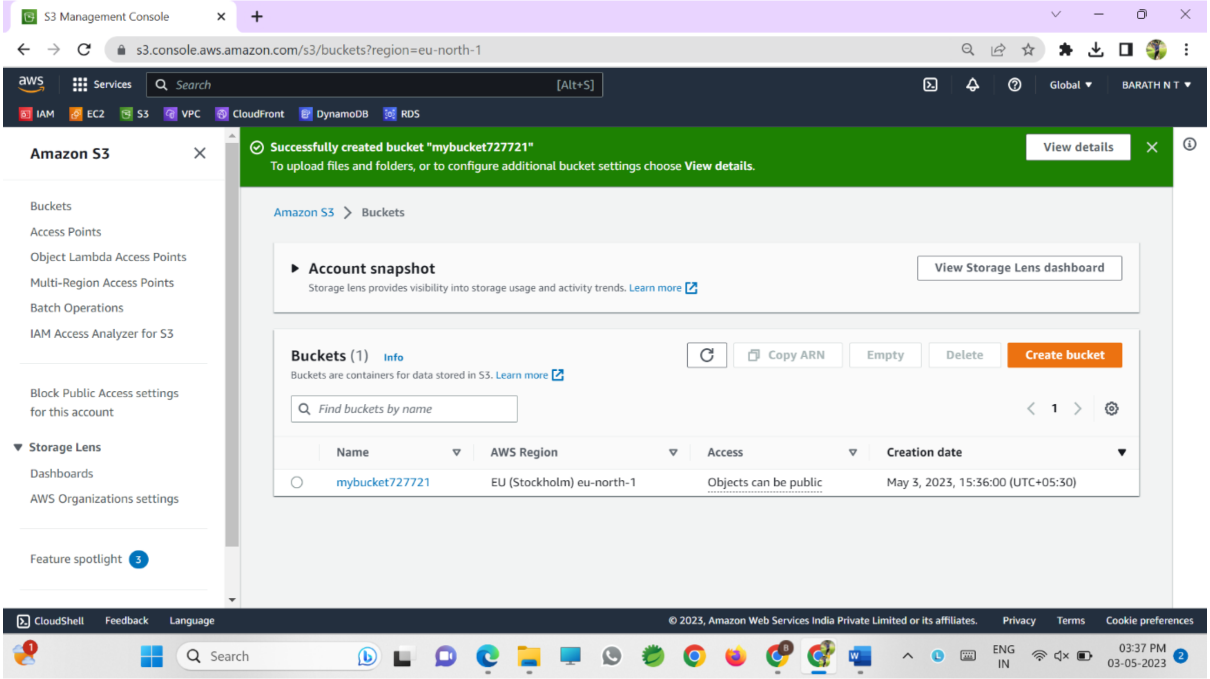
● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to



S3 Management Console
s3.console.aws.amazon.com/s3/buckets?region=eu-north-1
Services
Search [Alt+S]
Global
BARATH N T
IAM EC2 S3 VPC CloudFront DynamoDB RDS
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3

Successfully created bucket "mybucket727721"

To upload files and folders, or to configure additional bucket settings choose **View details**.

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

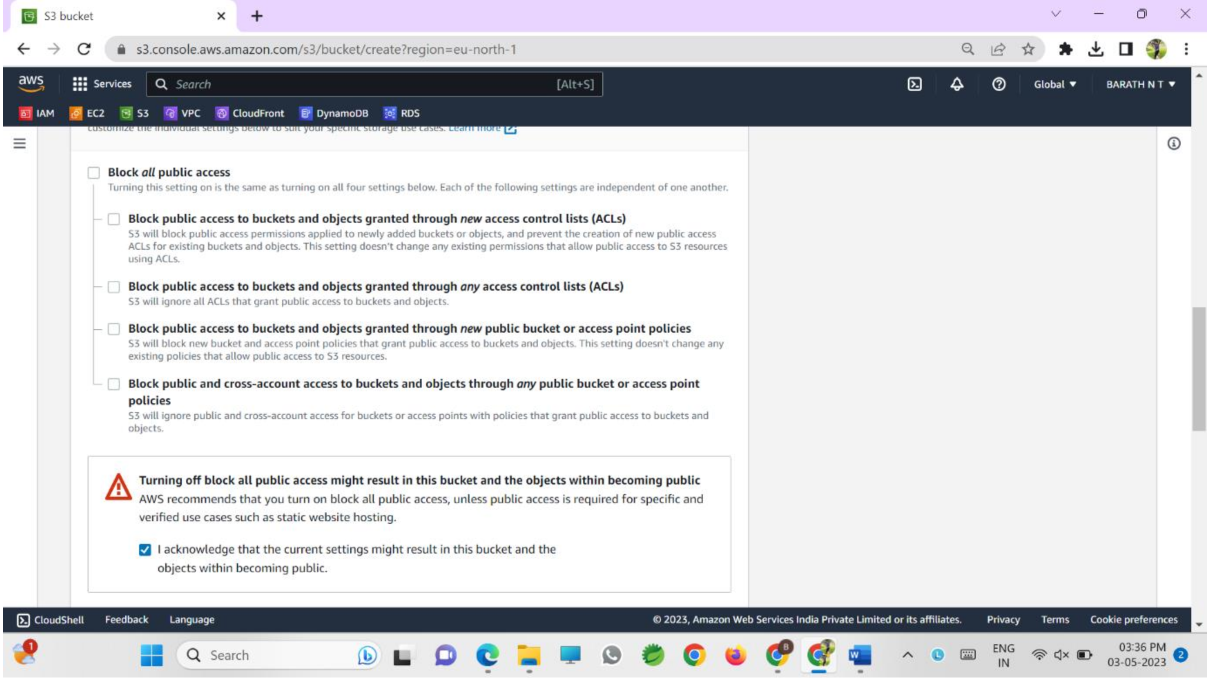
Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Copy ARN
Empty
Delete
Create bucket
Find buckets by name

	Name	AWS Region	Access	Creation date
○	mybucket727721	EU (Stockholm) eu-north-1	Objects can be public	May 3, 2023, 15:36:00 (UTC+05:30)

CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG IN
03:37 PM
03-05-2023



S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1
Services
Search [Alt+S]
Global
BARATH N T
IAM EC2 S3 VPC CloudFront DynamoDB RDS

Customize the individual settings below to suit your specific storage use cases. Learn more

□ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

□ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

□ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

□ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

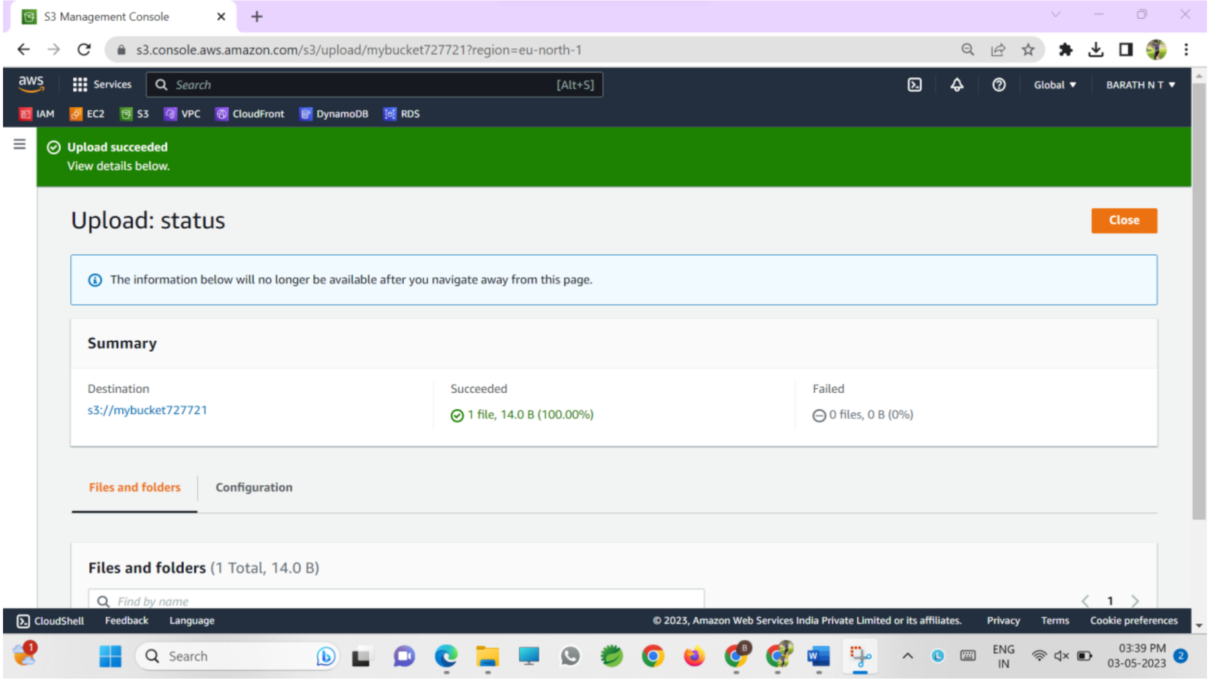
□ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.



Upload succeeded
View details below.

Upload: status

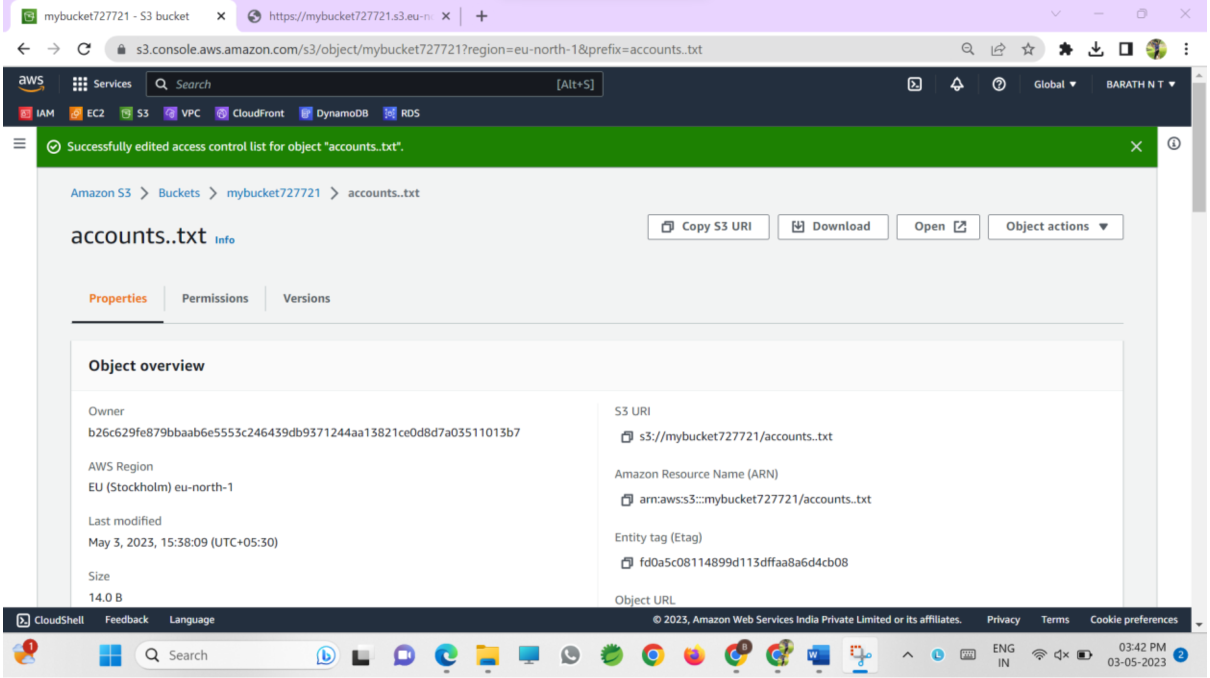
The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://mybucket727721	1 file, 14.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 14.0 B)

© 2023, Amazon Web Services India Private Limited or its affiliates.



Successfully edited access control list for object "accounts..txt".

accounts..txt

Object overview

Owner
b26c629fe879bbaab6e5553c246439db9371244aa13821ce0d8d7a03511013b7

AWS Region
EU (Stockholm) eu-north-1

Last modified
May 3, 2023, 15:38:09 (UTC+05:30)

Size
14.0 B

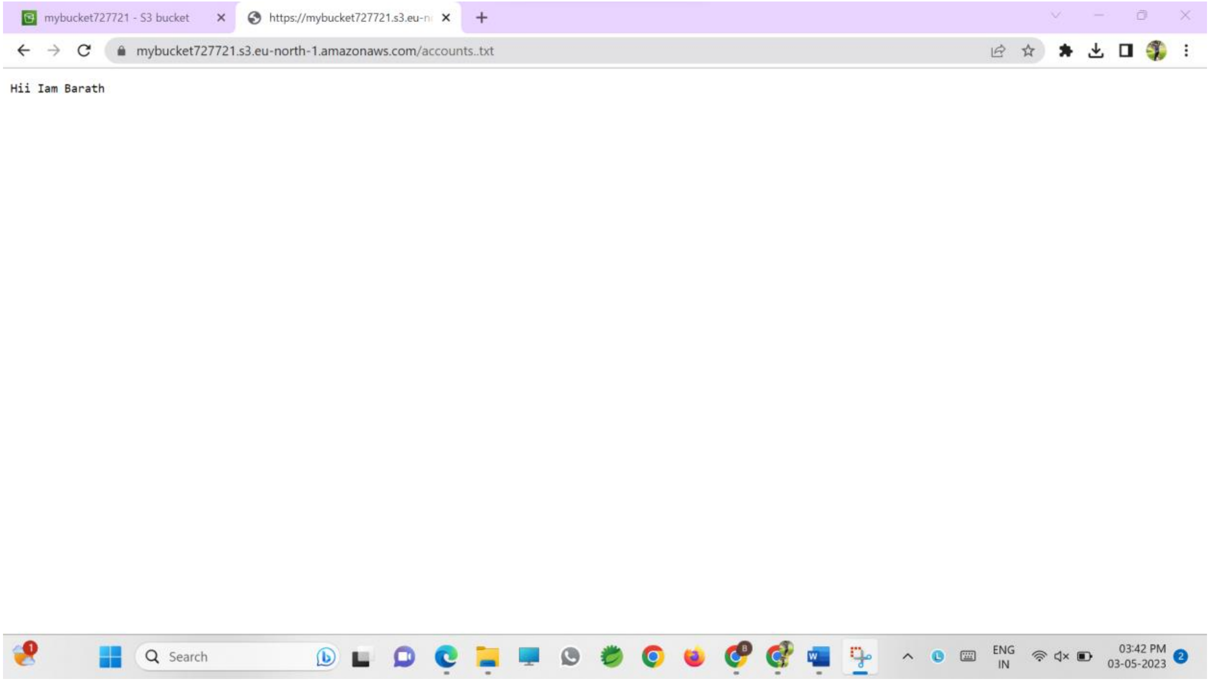
S3 URI
s3://mybucket727721/accounts..txt

Amazon Resource Name (ARN)
arn:aws:s3:::mybucket727721/accounts..txt

Entity tag (Etag)
fd0a5c08114899d113dffaa8a6d4cb08

Object URL

© 2023, Amazon Web Services India Private Limited or its affiliates.



mybucket727721 - S3 bucket
https://mybucket727721.s3.eu-n
mybucket727721.s3.eu-north-1.amazonaws.com/accounts..txt
Search
ENG
IN
03:42 PM
03-05-2023

```
Hii Iam Barath
```