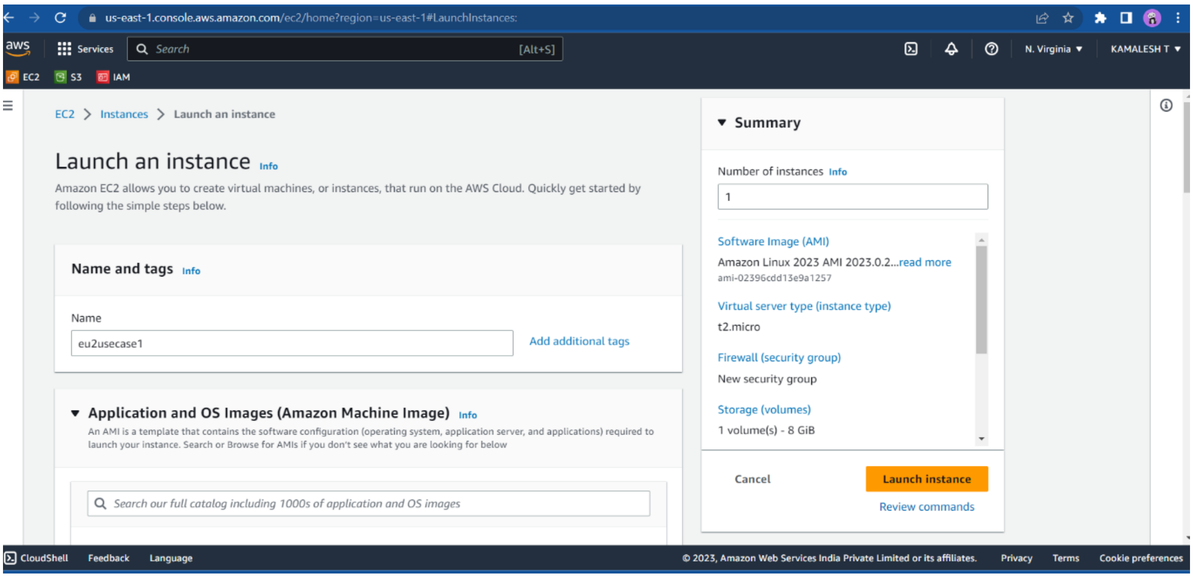
727721EUIT066

KAMALESH T

CODING CONTEST:

QUESTION 1:

Give the Name tag of both EC2 instance & keypair as "ec2usecase1"(Name):


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: eu2usecase1

▼ 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

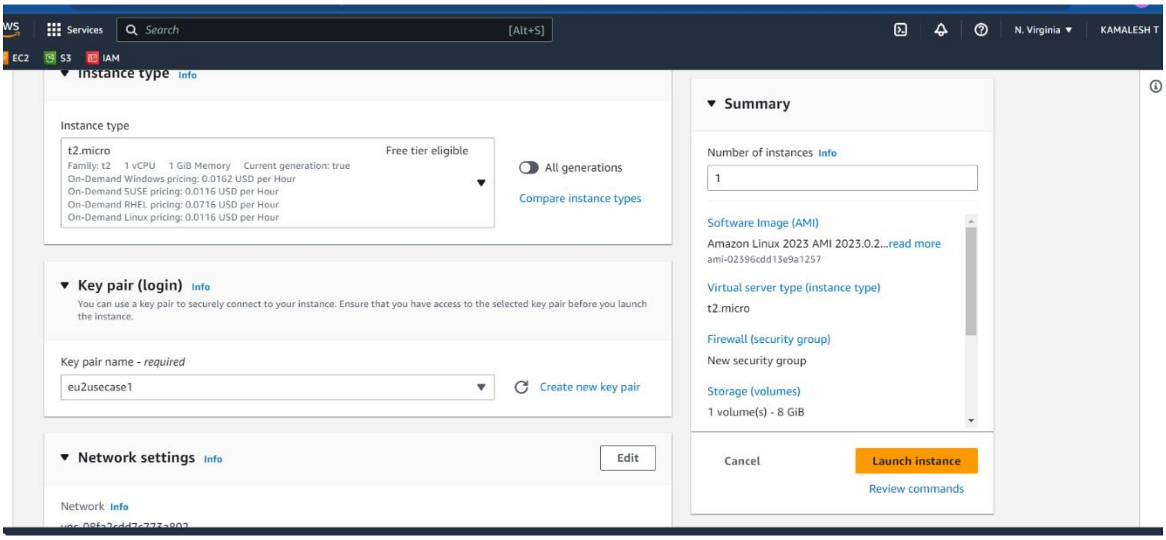
Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-02396cdd13e9a1257

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

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



▼ Instance type Info

Instance type:
t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

▼ 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*: eu2usecase1

▼ Network settings Info

Network Info

▼ Summary

Number of instances Info: 1

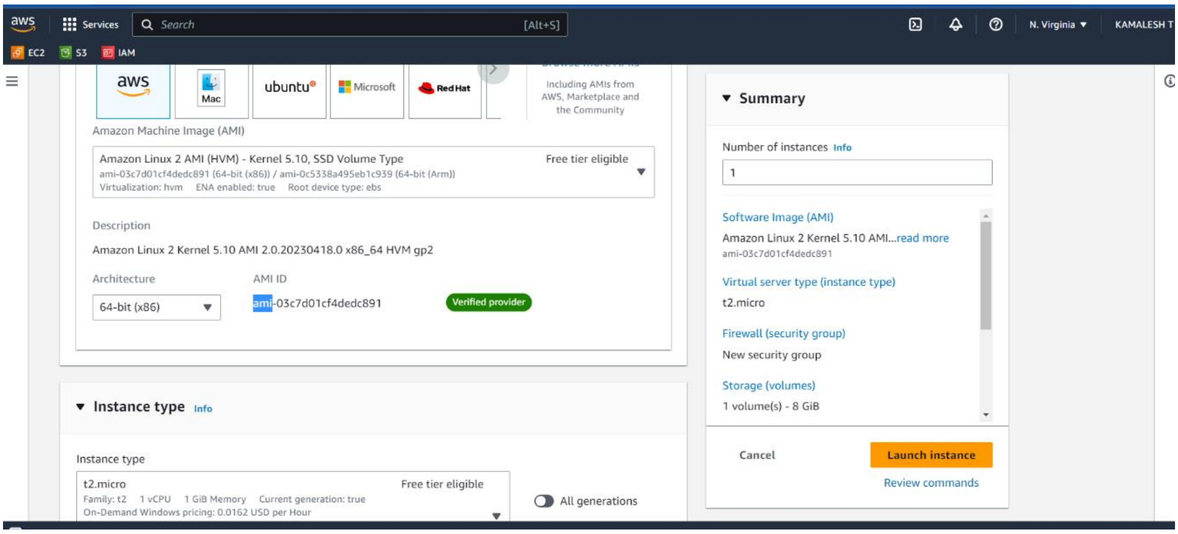
Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-02396cdd13e9a1257

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

EC2 instance AMI should be "Amazon Linux 2".



Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
ami-03c7d01cf4dedc891 (64-bit (x86)) / ami-0c5338a495eb1c939 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20230418.0 x86_64 HVM gp2

Architecture: 64-bit (x86)

AMI ID: ami-03c7d01cf4dedc891 — Verified provider

▼ Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour

All generations

▼ Summary

Number of instances Info: 1

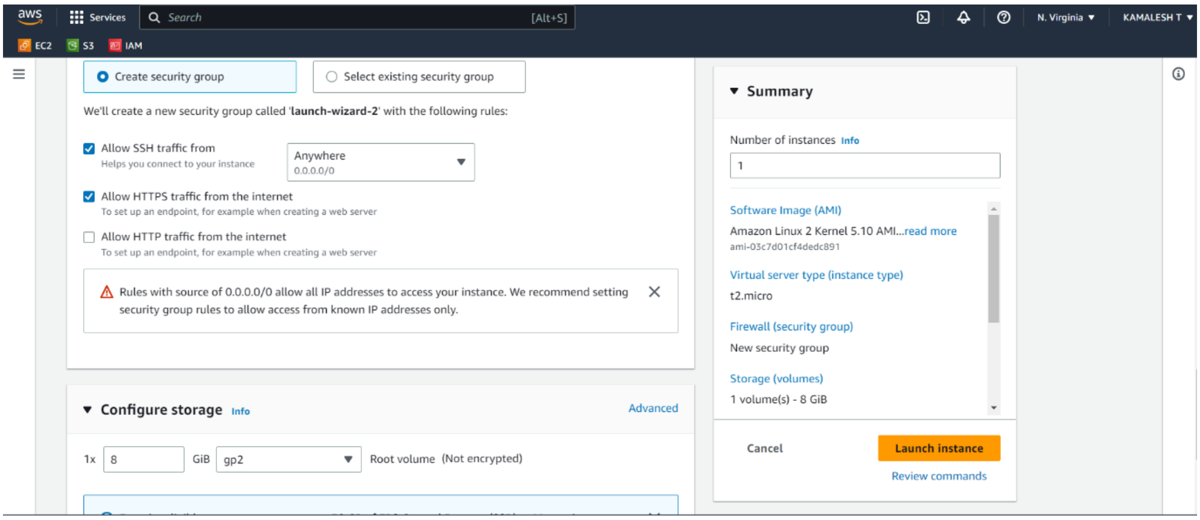
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-03c7d01cf4dedc891

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Allow SSH traffic for taking puttyremote connection



● Create security group ○ Select existing security group

We'll create a new security group called 'launch-wizard-2' 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.

▼ Configure storage Info — Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

▼ Summary

Number of instances Info: 1

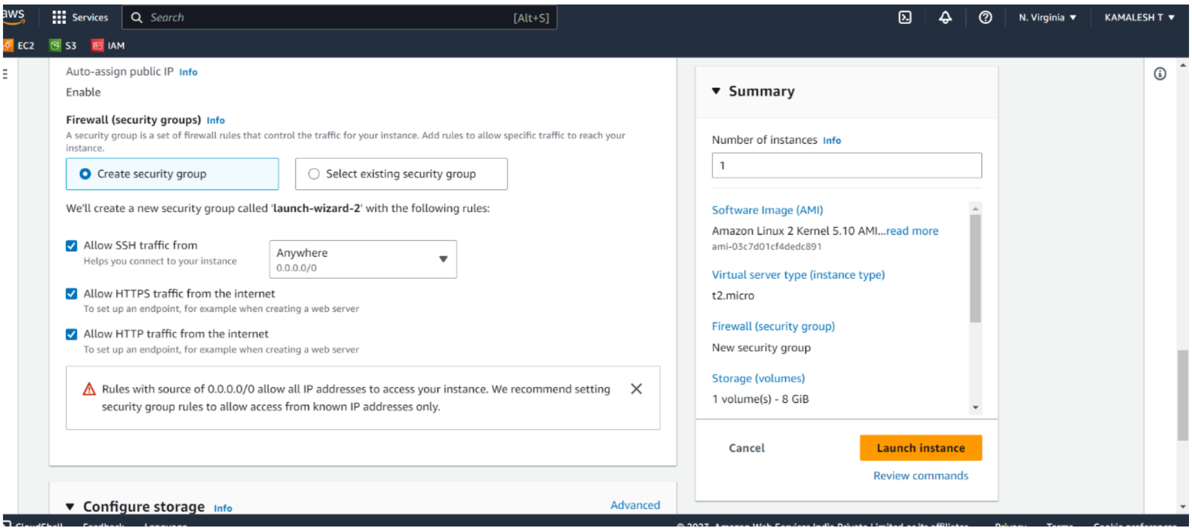
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-03c7d01cf4dedc891

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Allow HTTP traffic from the internet for reaching website requests



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-2' 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.

▼ Configure storage Info — Advanced

▼ Summary

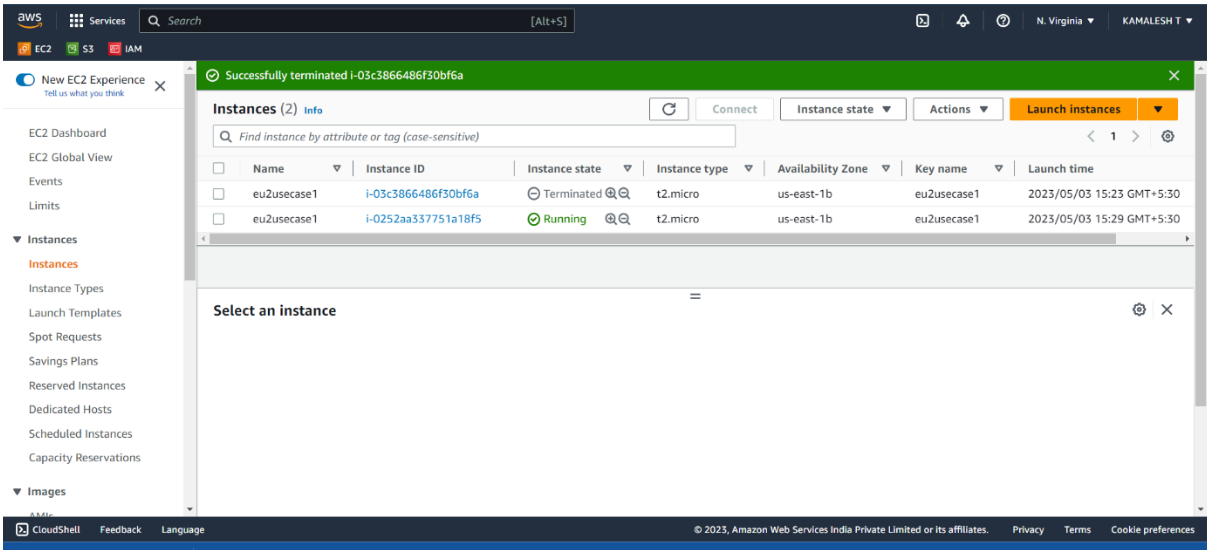
Number of instances Info: 1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-03c7d01cf4dedc891

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB



Successfully terminated i-03c3866486f30bf6a

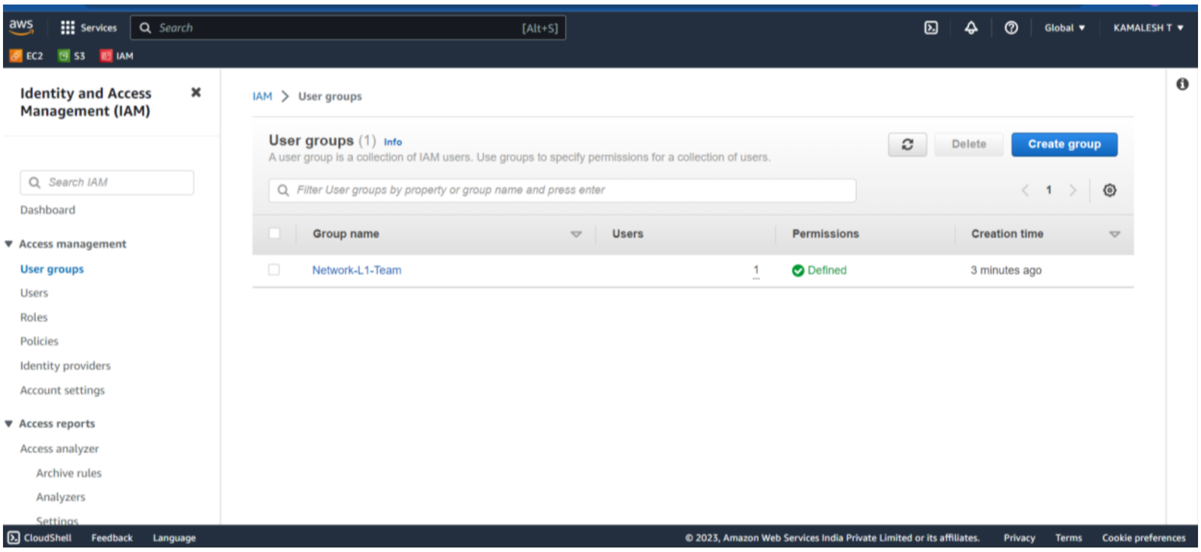
Instances (2) Info

Name	Instance ID	Instance state	Instance type	Availability Zone	Key name	Launch time
eu2usecase1	i-03c3866486f30bf6a	Terminated	t2.micro	us-east-1b	eu2usecase1	2023/05/03 15:23 GMT+5:30
eu2usecase1	i-0252aa337751a18f5	Running	t2.micro	us-east-1b	eu2usecase1	2023/05/03 15:29 GMT+5:30

Select an instance

QUESTION 2:

The name of the IAM group should be 'Network-L1-Team'.

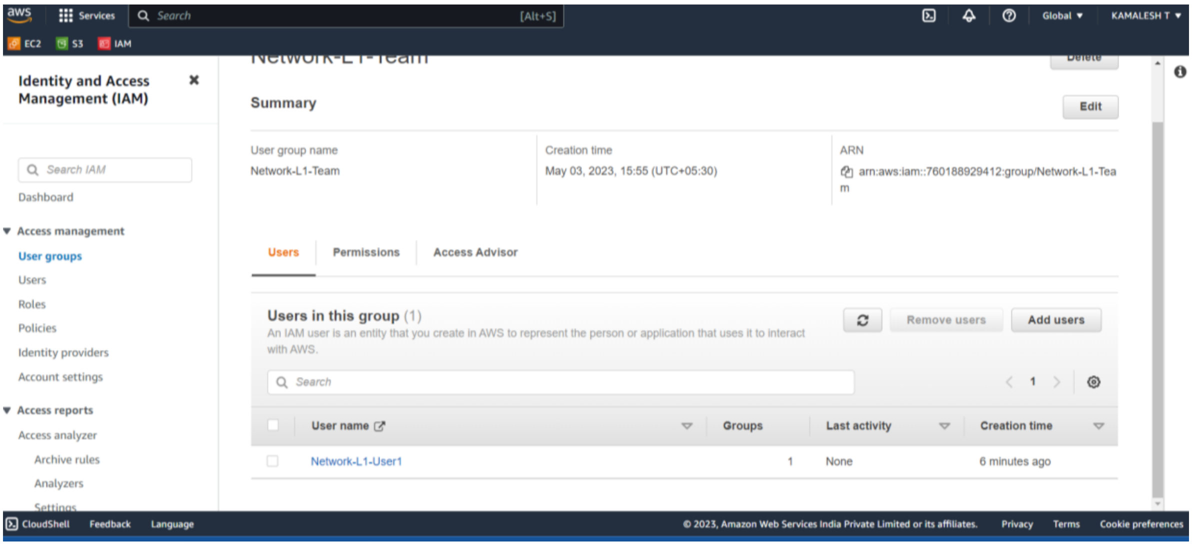


User groups (1) Info

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	1	Defined	3 minutes ago

The name of the IAM user should be 'Network-L1-User1'



Network-L1-Team

Summary

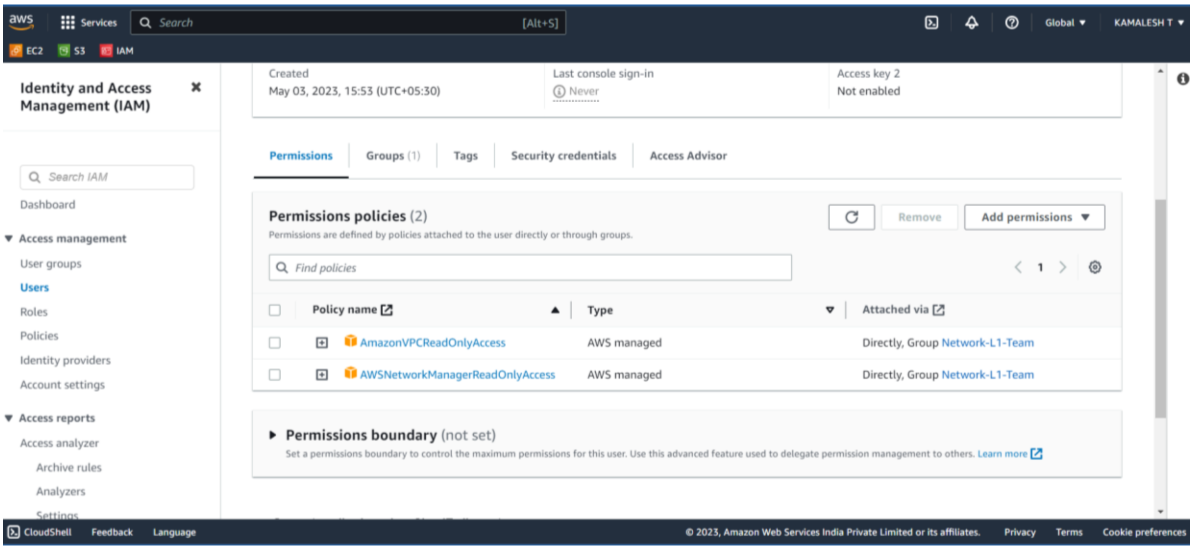
User group name	Creation time	ARN
Network-L1-Team	May 03, 2023, 15:55 (UTC+05:30)	arn:aws:iam::760188929412:group/Network-L1-Team

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	Network-L1-User1	1	None	6 minutes ago

'AmazonVPCReadOnlyAccess' policy should be attached.



Created	Last console sign-in	Access key 2
May 03, 2023, 15:53 (UTC+05:30)	Never	Not enabled

Permissions policies (2)

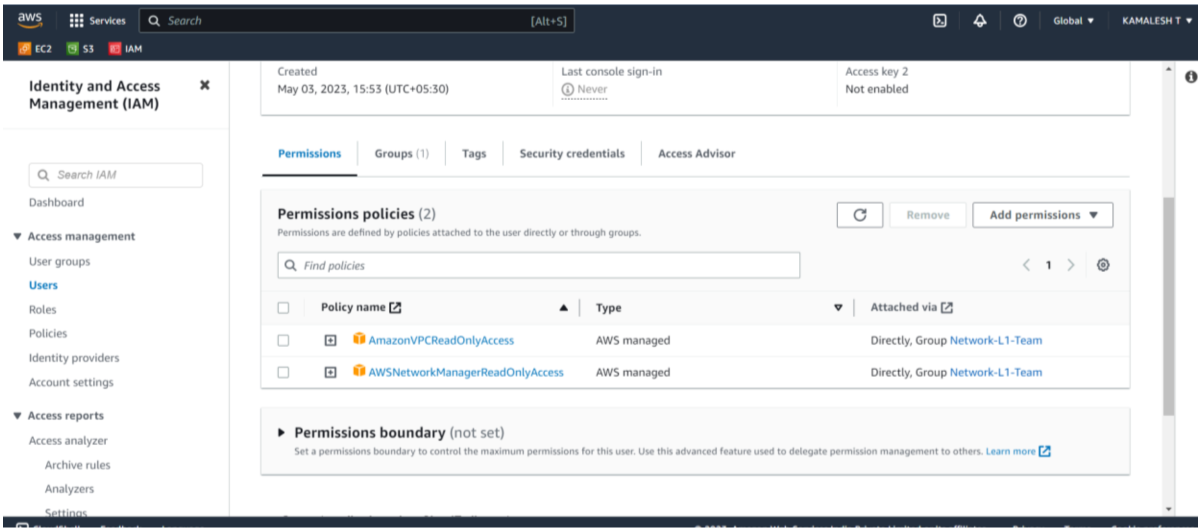
Permissions are defined by policies attached to the user directly or through groups.

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

▶ Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

'AWSNetworkManagerReadOnlyAccess' policy should be attached


Created	Last console sign-in	Access key 2
May 03, 2023, 15:53 (UTC+05:30)	Never	Not enabled

Permissions policies (2)

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

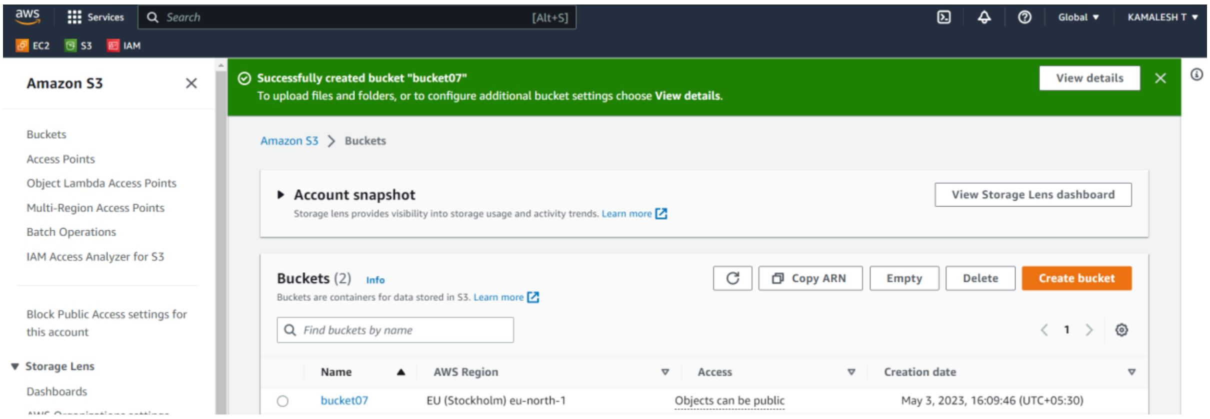
□	Policy name	Type	Attached via
□	AmazonVPCReadOnlyAccess	AWS managed	Directly, Group Network-L1-Team
□	AWSNetworkManagerReadOnlyAccess	AWS managed	Directly, Group Network-L1-Team

▶ Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

QUESTION3:

Create a new S3 bucket in the region of "Stockholm"

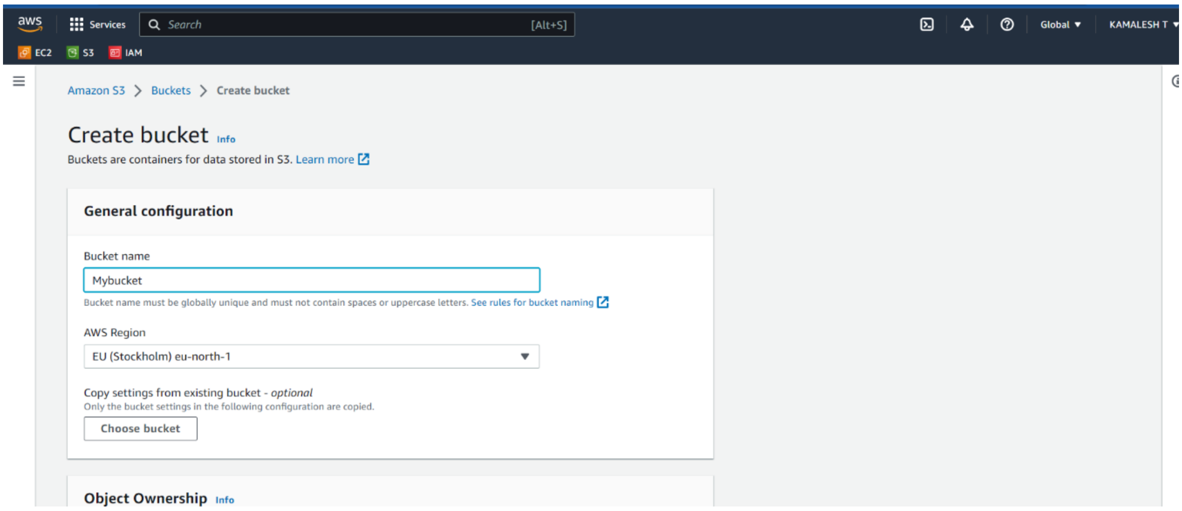


Successfully created bucket "bucket07"
To upload files and folders, or to configure additional bucket settings choose **View details**.

▸ **Account snapshot**
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (2)
Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region	Access	Creation date
○	bucket07	EU (Stockholm) eu-north-1	Objects can be public	May 3, 2023, 16:09:46 (UTC+05:30)



Create bucket
Buckets are containers for data stored in S3. Learn more

General configuration

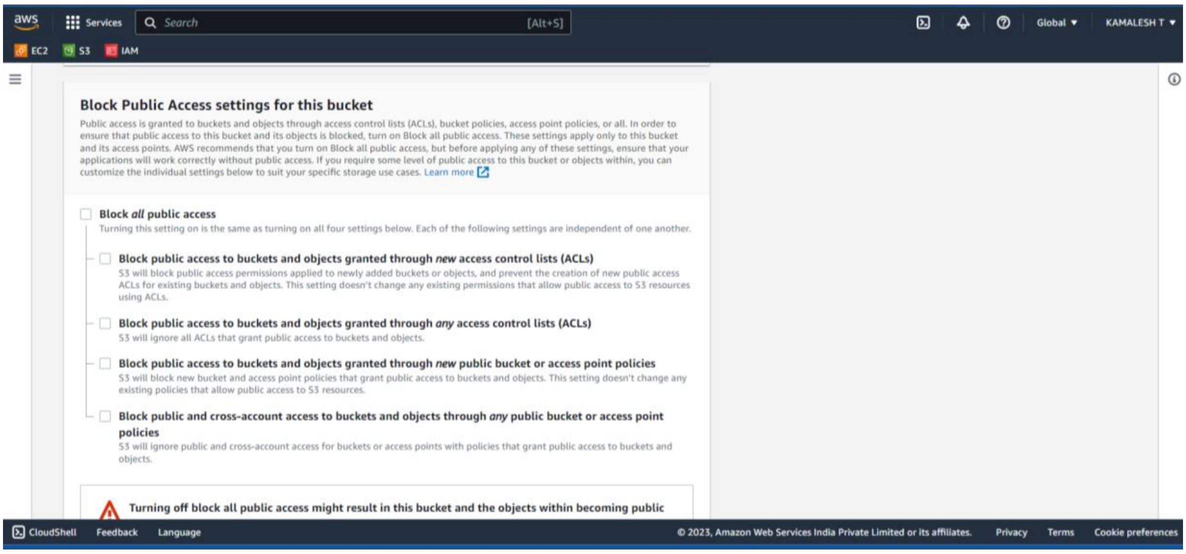
Bucket name
Mybucket
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region
EU (Stockholm) eu-north-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Object Ownership

Make the bucket accessible to everyone(publicly) via Bucket ACL



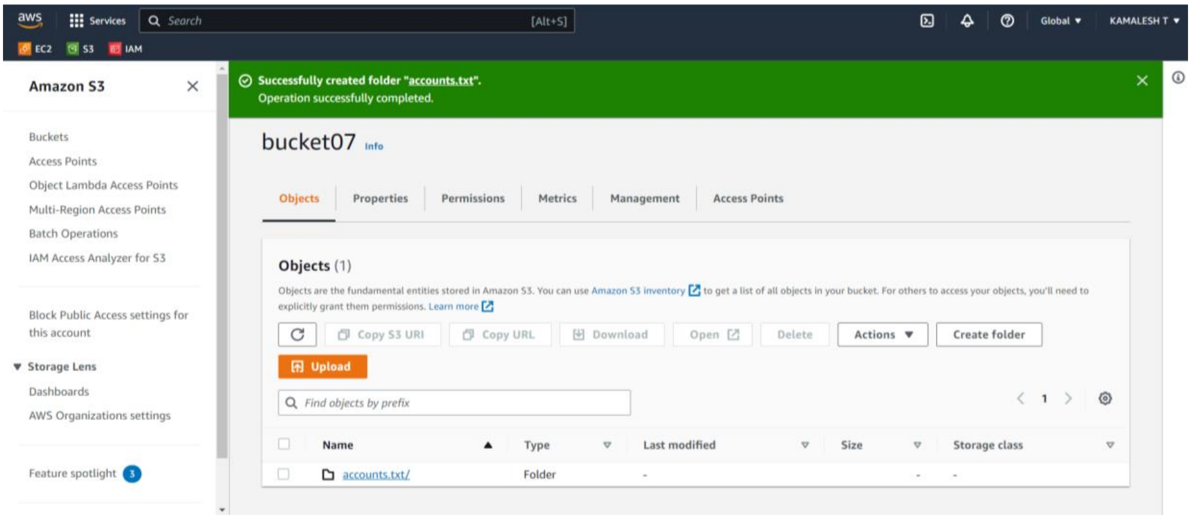
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can 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**

Upload a text file in the name of 'accounts.txt'.



Successfully created folder "accounts.txt".
Operation successfully completed.

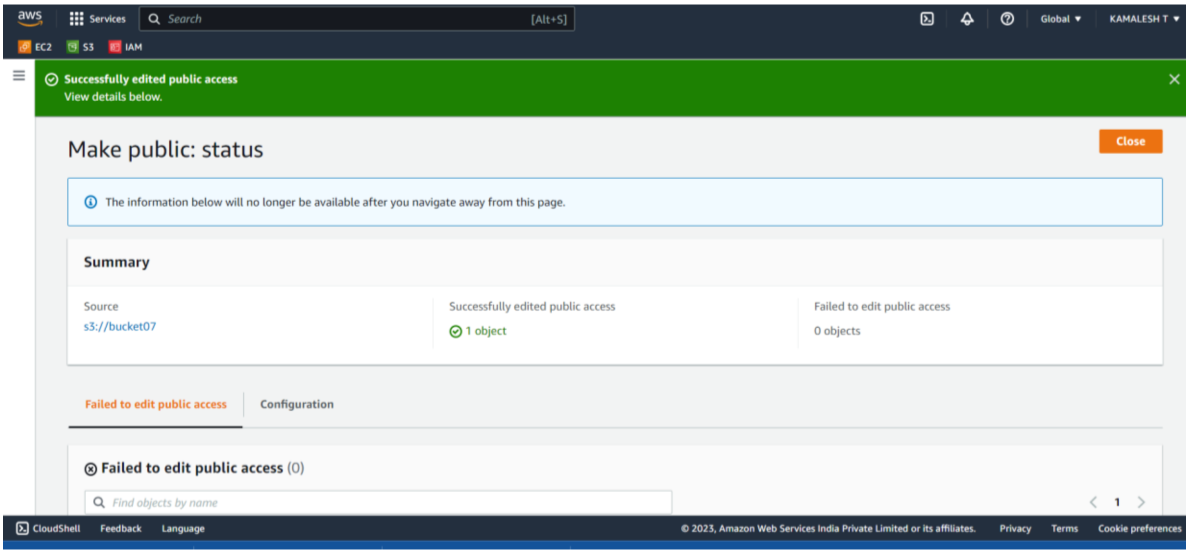
bucket07

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
accounts.txt/	Folder	-	-	-

Make the object 'accounts.txt' file accessible to everyone(publicly)



Successfully edited public access
View details below.

Make public: status

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

Summary

Source	Successfully edited public access	Failed to edit public access
s3://bucket07	1 object	0 objects

Failed to edit public access (0)

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