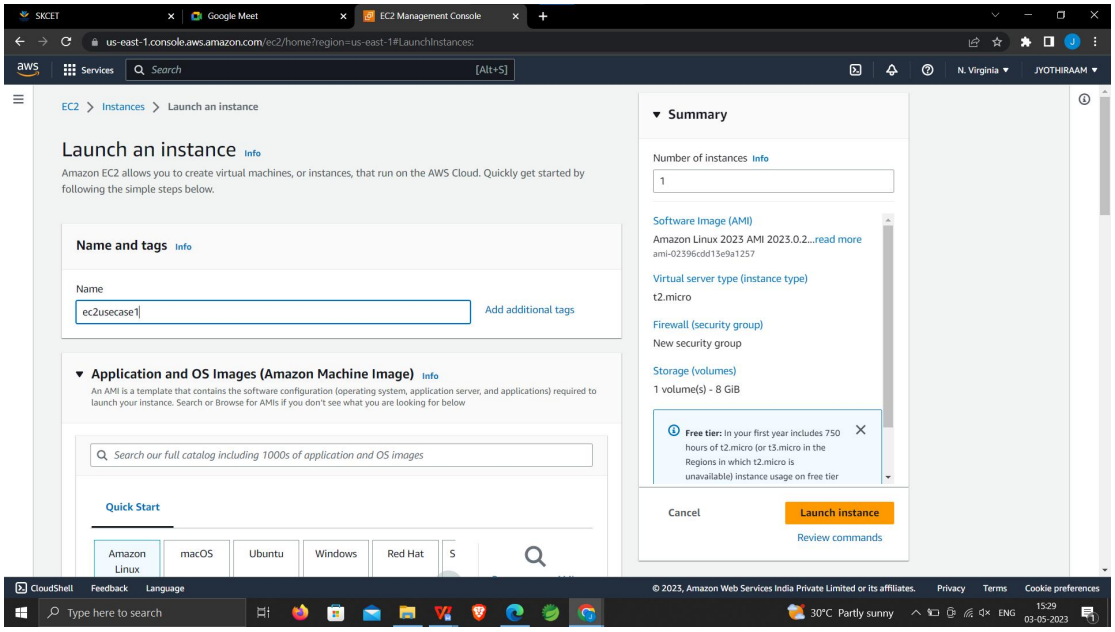
AWS(Amazon Web Service)
CC-1

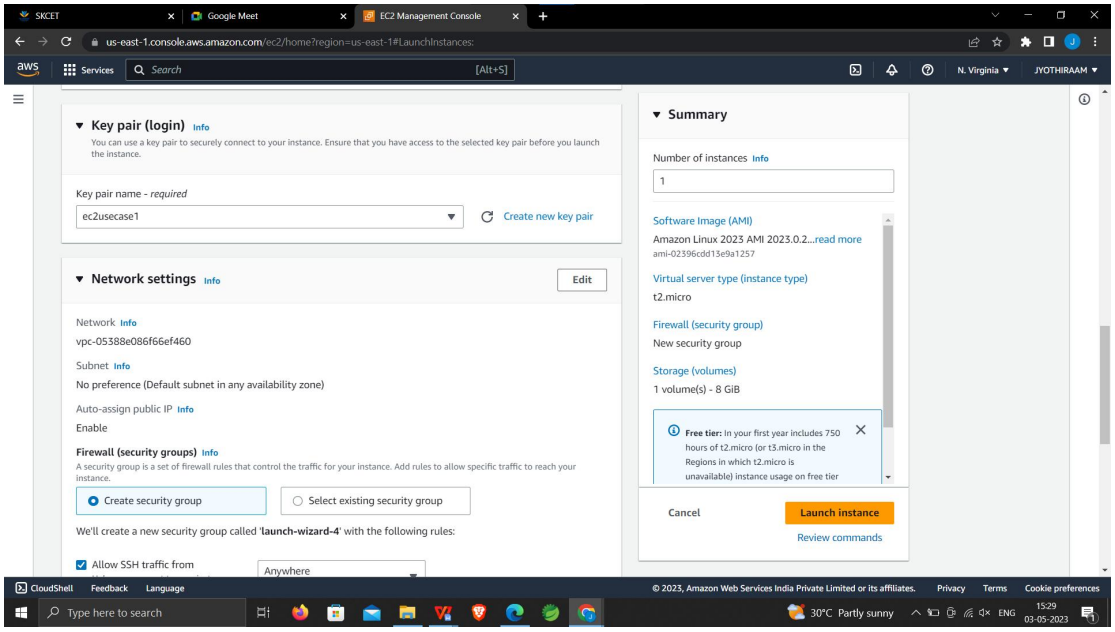
JYOTHIRAAM S R
727721EUIT061
IT-A

EC2:

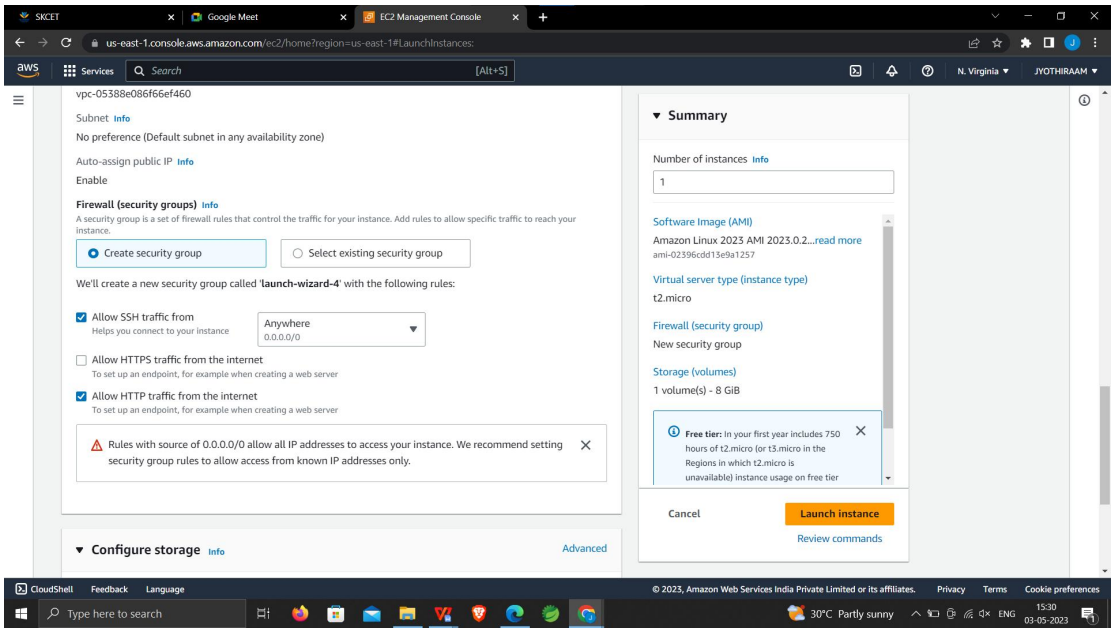
1.



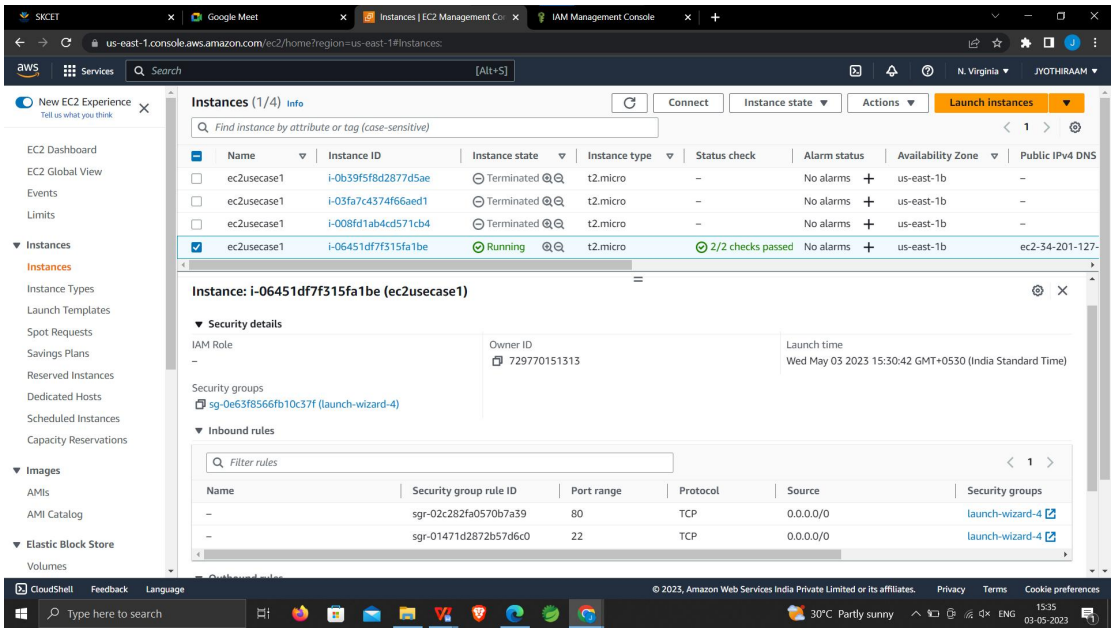
2.



3,4.

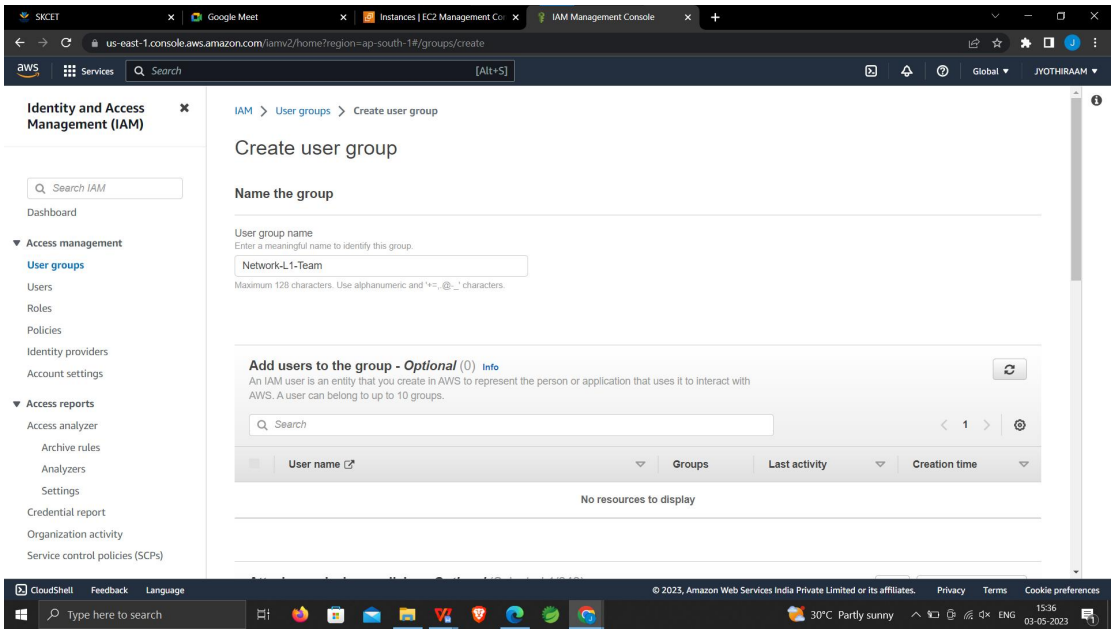


EC2 Created:

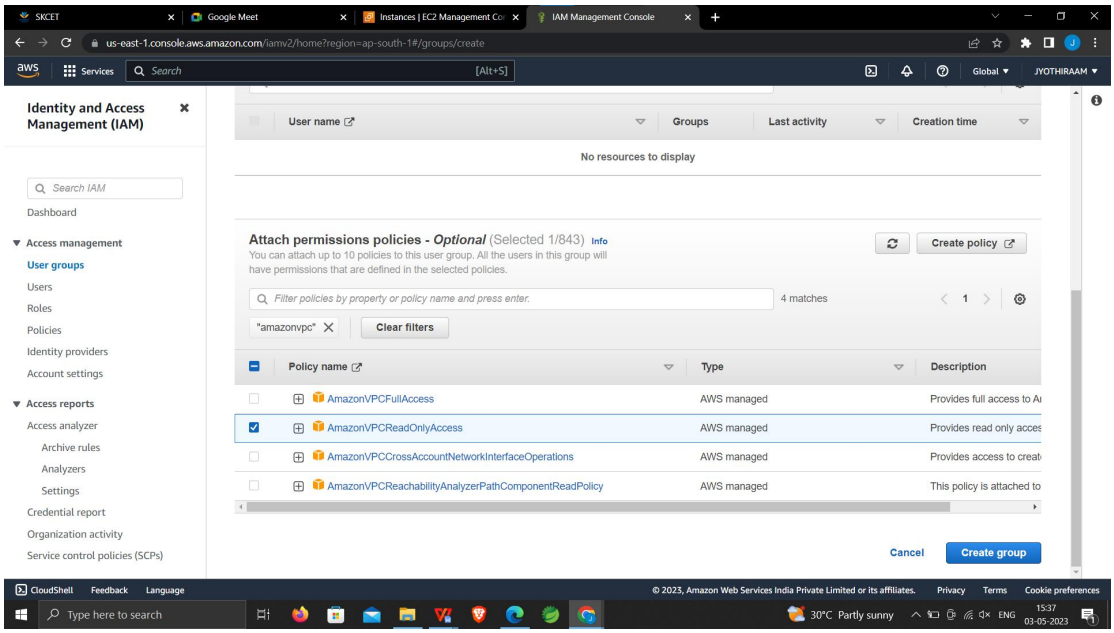


IAM:

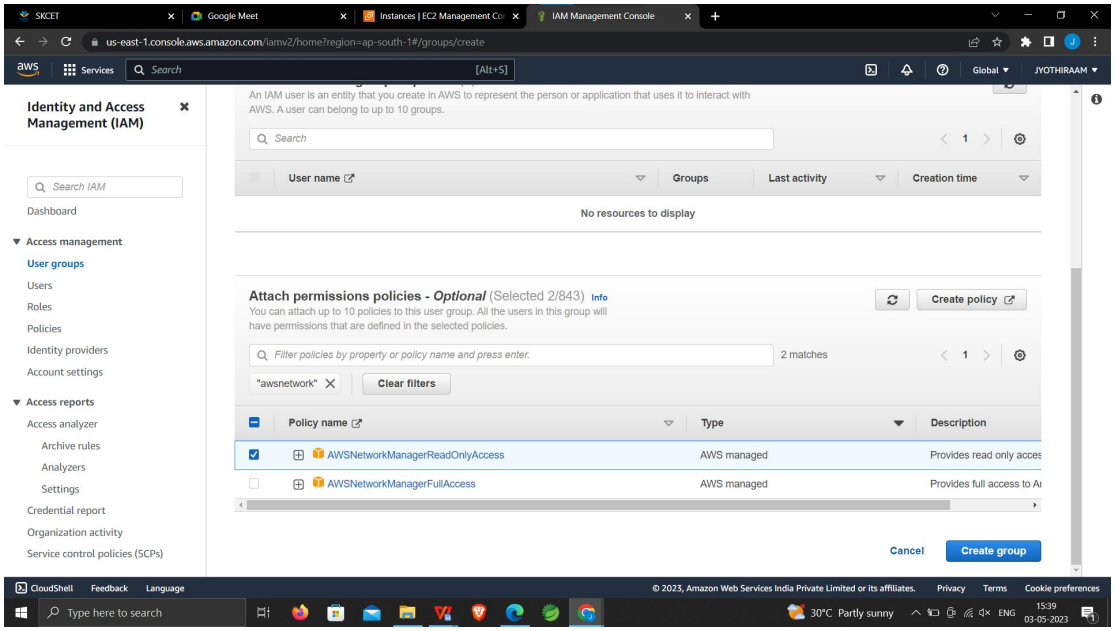
1.


SKCET
Google Meet
Instances | EC2 Management Co
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/create
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Network-L1-Team
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (0) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.
Search
1
User name
Groups
Last activity
Creation time
No resources to display
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
30°C Partly sunny
ENG
15:36
03-05-2023

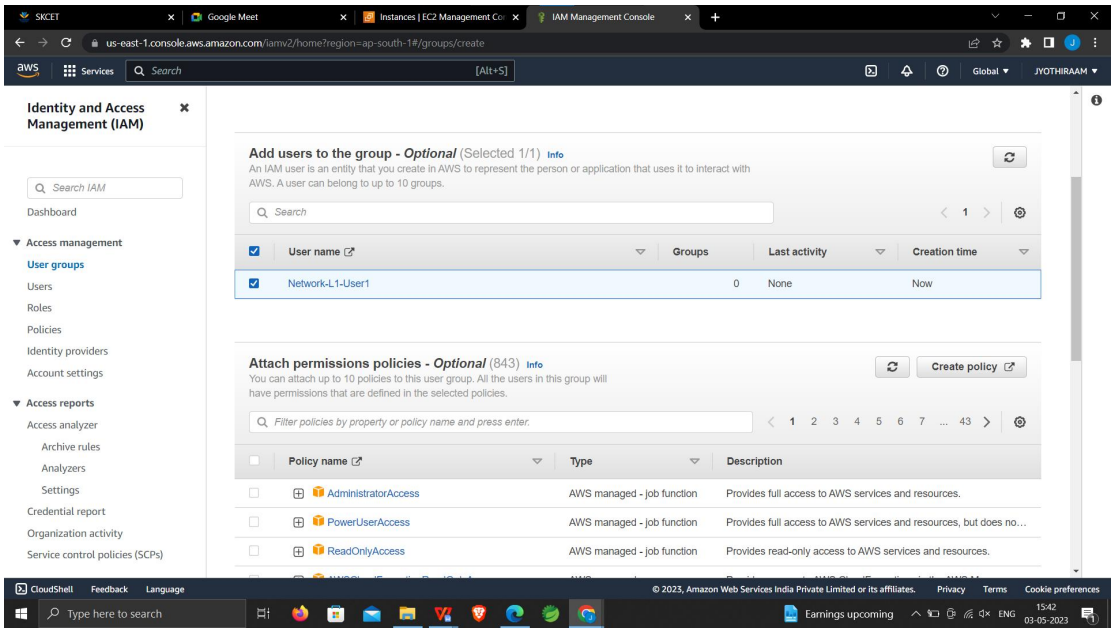
2.


SKCET
Google Meet
Instances | EC2 Management Co
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/create
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
User name
Groups
Last activity
Creation time
No resources to display
Attach permissions policies - Optional (Selected 1/843) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Create policy
Filter policies by property or policy name and press enter.
4 matches
1
"amazonvpc"
Clear filters
Policy name
Type
Description
AmazonVPCFullAccess
AWS managed
Provides full access to A
AmazonVPCReadOnlyAccess
AWS managed
Provides read only acces
AmazonVPCCrossAccountNetworkInterfaceOperations
AWS managed
Provides access to creat
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
AWS managed
This policy is attached to
Cancel
Create group
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
30°C Partly sunny
ENG
15:37
03-05-2023

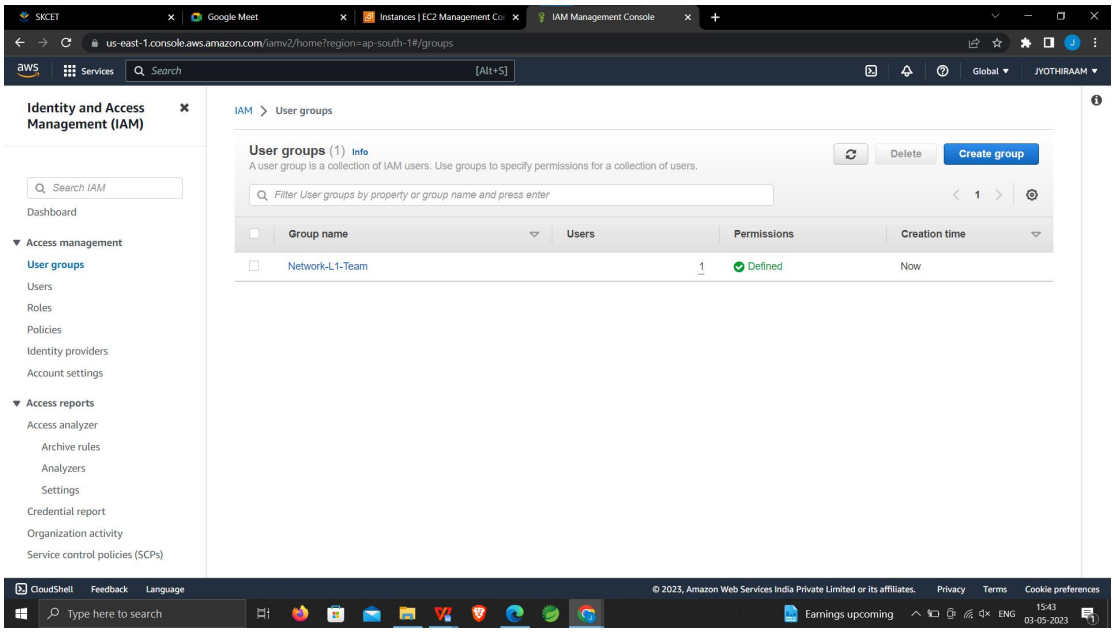
3.


SKCET
Google Meet
Instances | EC2 Management Co
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/create
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.
User name
Groups
Last activity
Creation time
No resources to display
Attach permissions policies - Optional (Selected 2/843) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Create policy
Filter policies by property or policy name and press enter.
2 matches
"awsnetwork"
Clear filters
Policy name
Type
Description
AWSNetworkManagerReadOnlyAccess
AWS managed
Provides read only acces
AWSNetworkManagerFullAccess
AWS managed
Provides full access to A
Cancel
Create group
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
30°C Partly sunny
ENG
15:39
03-05-2023

4.

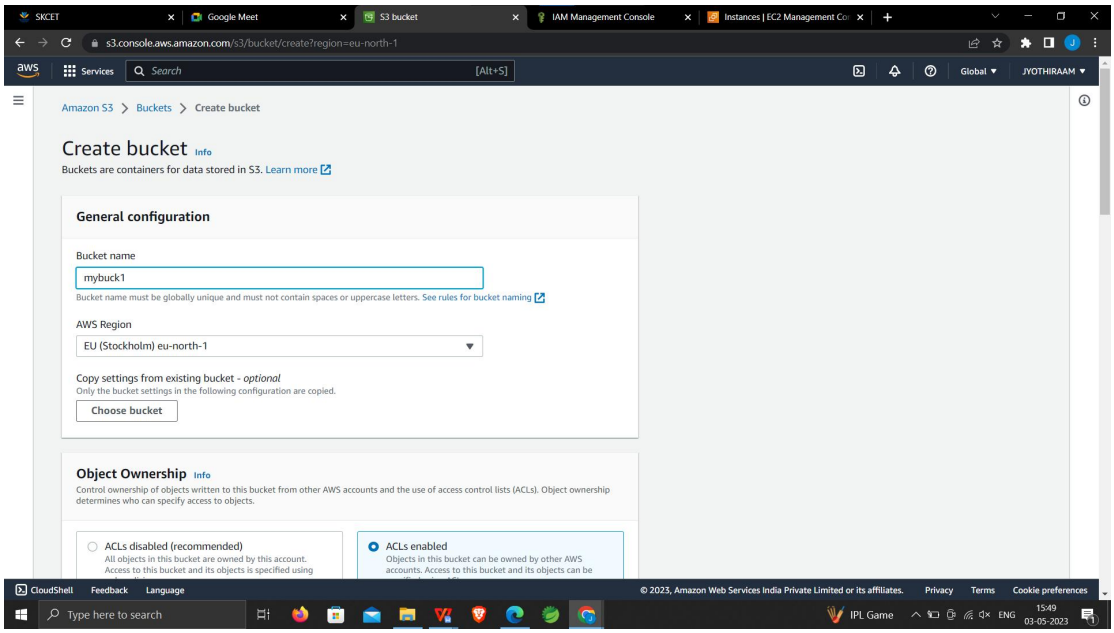

SKCET
Google Meet
Instances | EC2 Management Co
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/create
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Add users to the group - Optional (Selected 1/1) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.
User name
Groups
Last activity
Creation time
Network-L1-User1
0
None
Now
Attach permissions policies - Optional (843) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Create policy
Filter policies by property or policy name and press enter.
1 2 3 4 5 6 7 ... 43
Policy name
Type
Description
AdministratorAccess
AWS managed - job function
Provides full access to AWS services and resources.
PowerUserAccess
AWS managed - job function
Provides full access to AWS services and resources, but does no...
ReadOnlyAccess
AWS managed - job function
Provides read-only access to AWS services and resources.
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Earnings upcoming
ENG
15:42
03-05-2023

IAM Group Created:

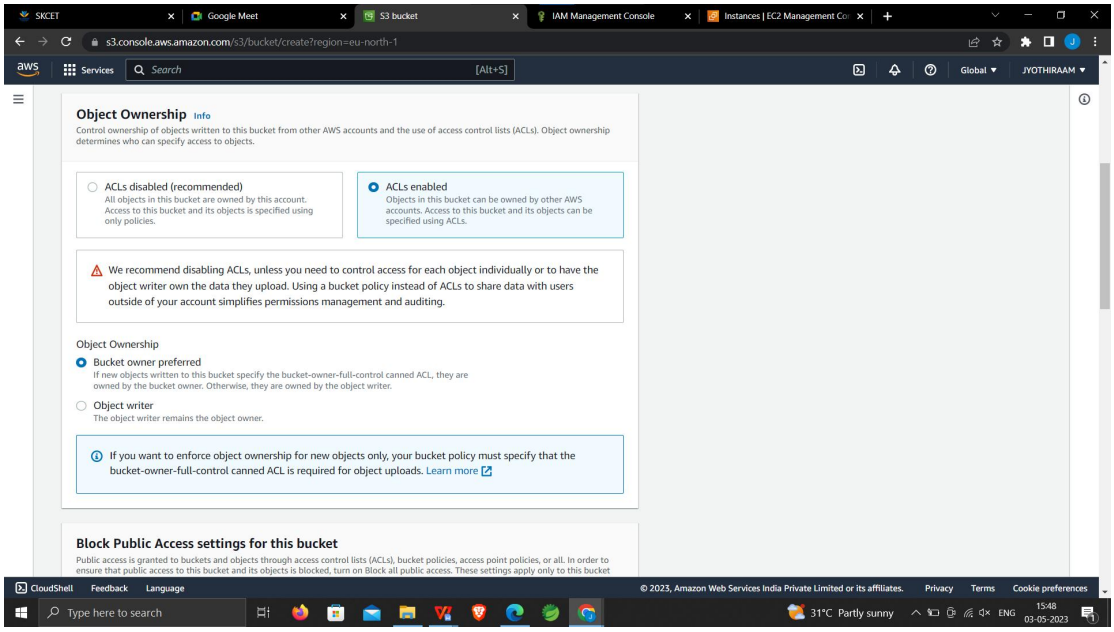


S3:

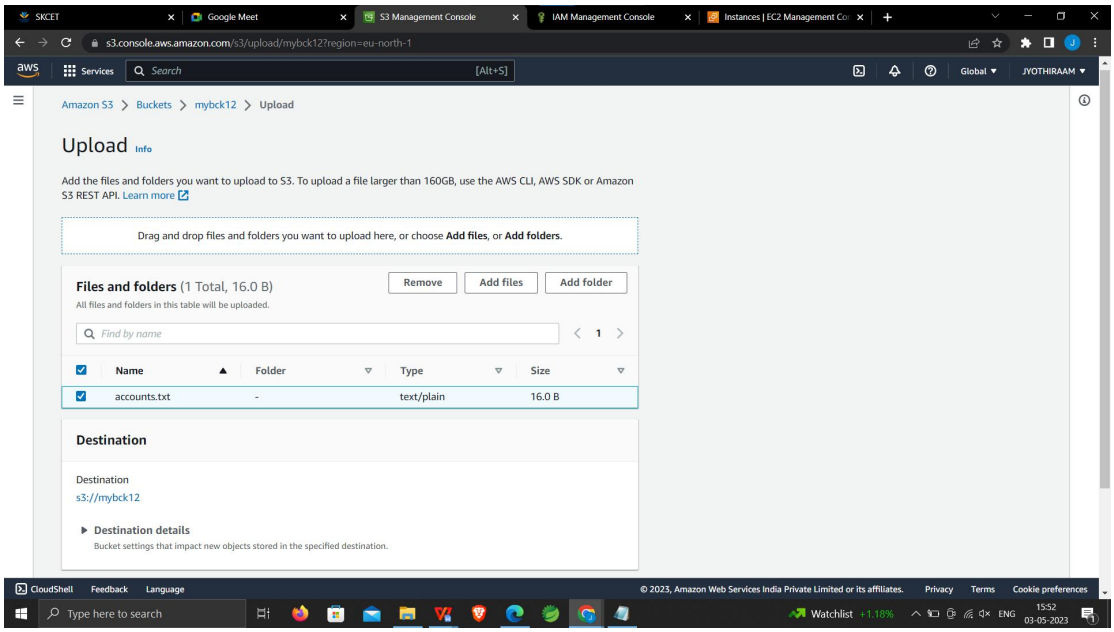
1.


SKCET
Google Meet
S3 bucket
IAM Management Console
Instances | EC2 Management Co
s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
mybuck1
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
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
IPL Game
ENG
15:49
03-05-2023

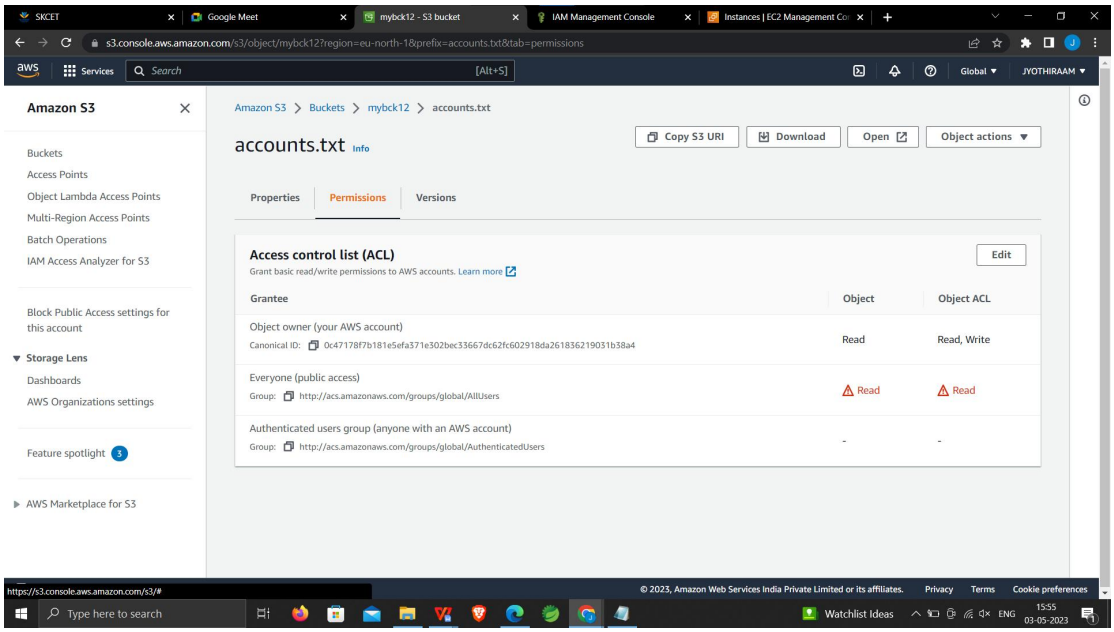
2.


SKCET
Google Meet
S3 bucket
IAM Management Console
Instances | EC2 Management Co
s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
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 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
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
31°C Partly sunny
ENG
15:48
03-05-2023

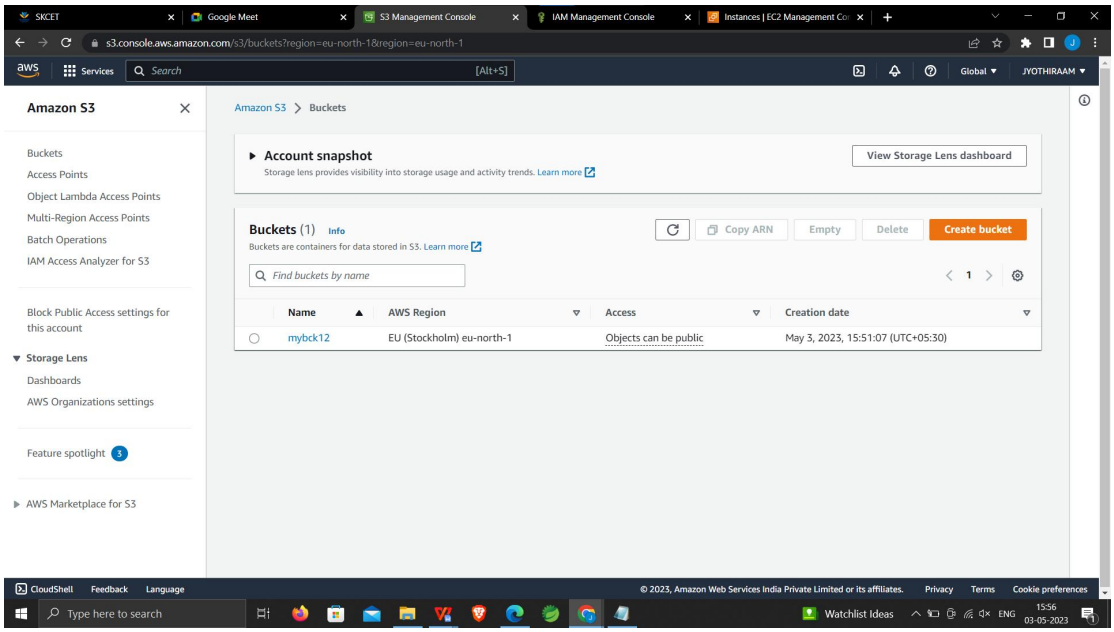
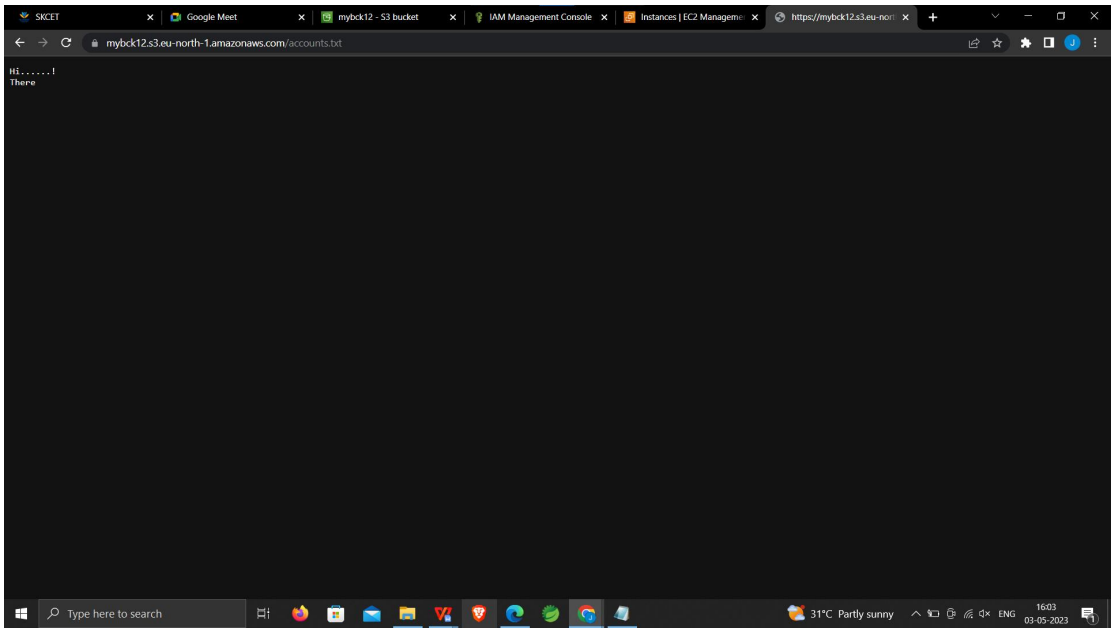
3.


SKCET
Google Meet
S3 Management Console
IAM Management Console
Instances | EC2 Management Co
s3.console.aws.amazon.com/s3/upload/mybck12?region=eu-north-1
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
Amazon S3 > Buckets > mybck12 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.
Files and folders (1 Total, 16.0 B)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1
Name
Folder
Type
Size
accounts.txt
-
text/plain
16.0 B
Destination
Destination
s3://mybck12
Destination details
Bucket settings that impact new objects stored in the specified destination.
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Watchlist +1.18%
ENG
15:52
03-05-2023

4.


SKCET
Google Meet
mybck12 - S3 bucket
IAM Management Console
Instances | EC2 Management Co
s3.console.aws.amazon.com/s3/object/mybck12?region=eu-north-1&prefix=accounts.txt&tab=permissions
aws
Services
Search
[Alt+S]
Global
JYOTHIRAAM
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
AWS Marketplace for S3
Amazon S3 > Buckets > mybck12 > accounts.txt
accounts.txt Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Access control list (ACL)
Grant basic read/write permissions to AWS accounts. Learn more
Edit
Grantee
Object
Object ACL
Object owner (your AWS account)
Canonical ID: 0c47178f7b181e5efa371e302bec33667dc62fc602918da261836219031b38a4
Read
Read, Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
Read
Read
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
https://s3.console.aws.amazon.com/s3/#
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Watchlist Ideas
ENG
15:55
03-05-2023

S3 Bucket Created:



Object is publicly visible: