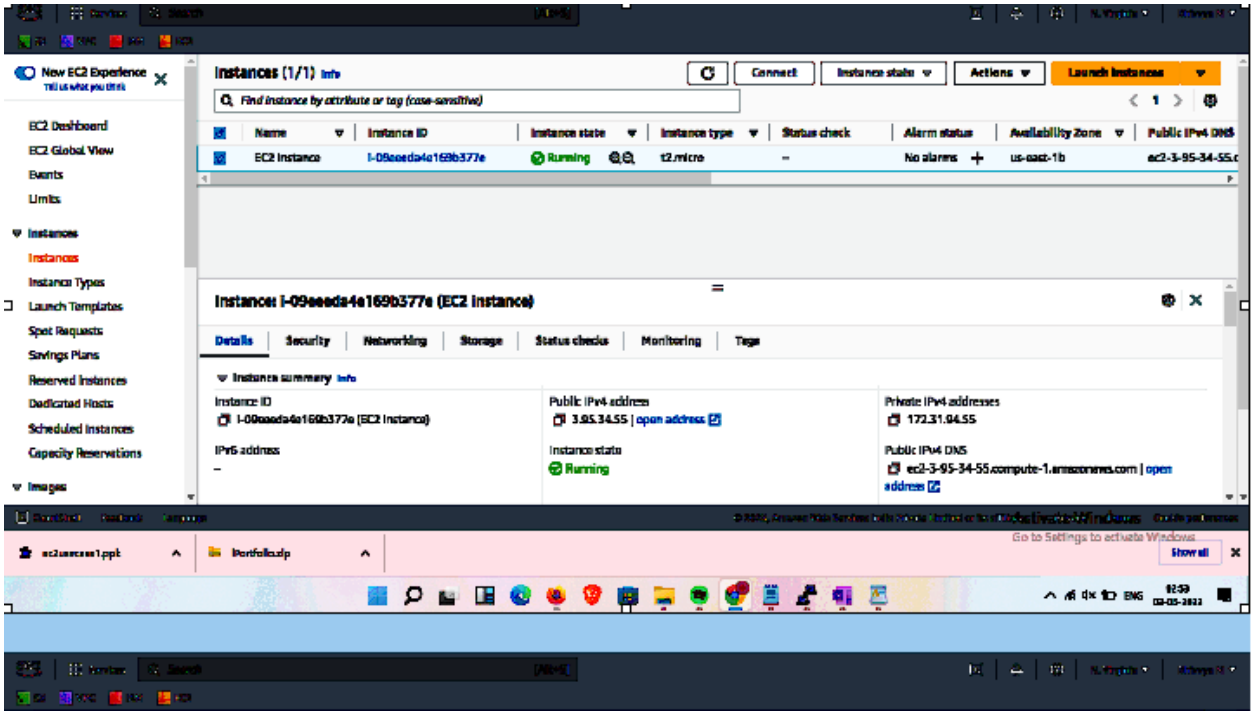
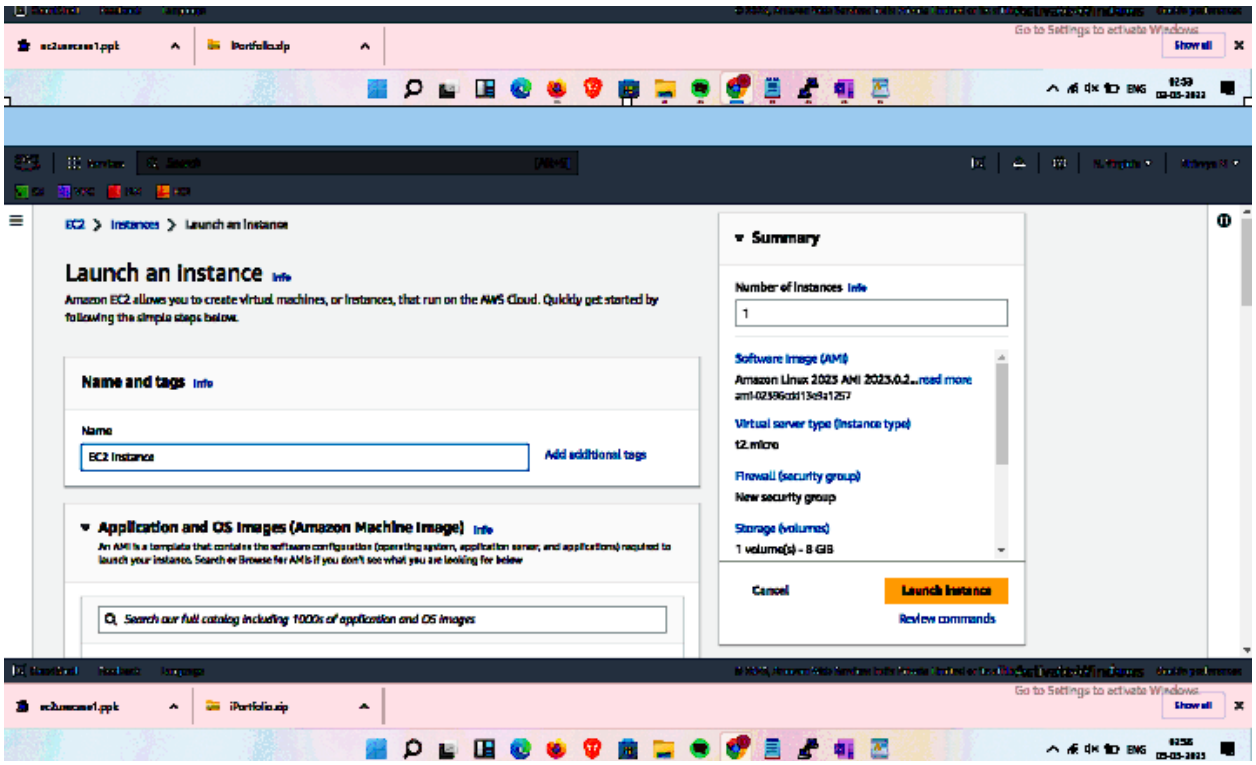
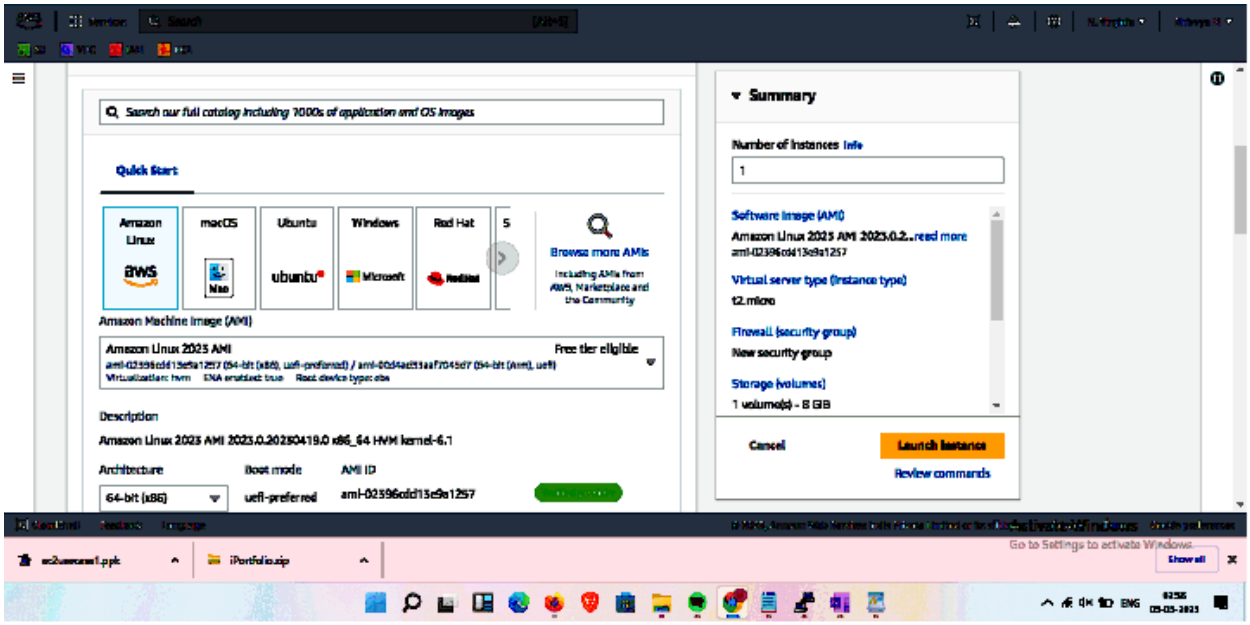
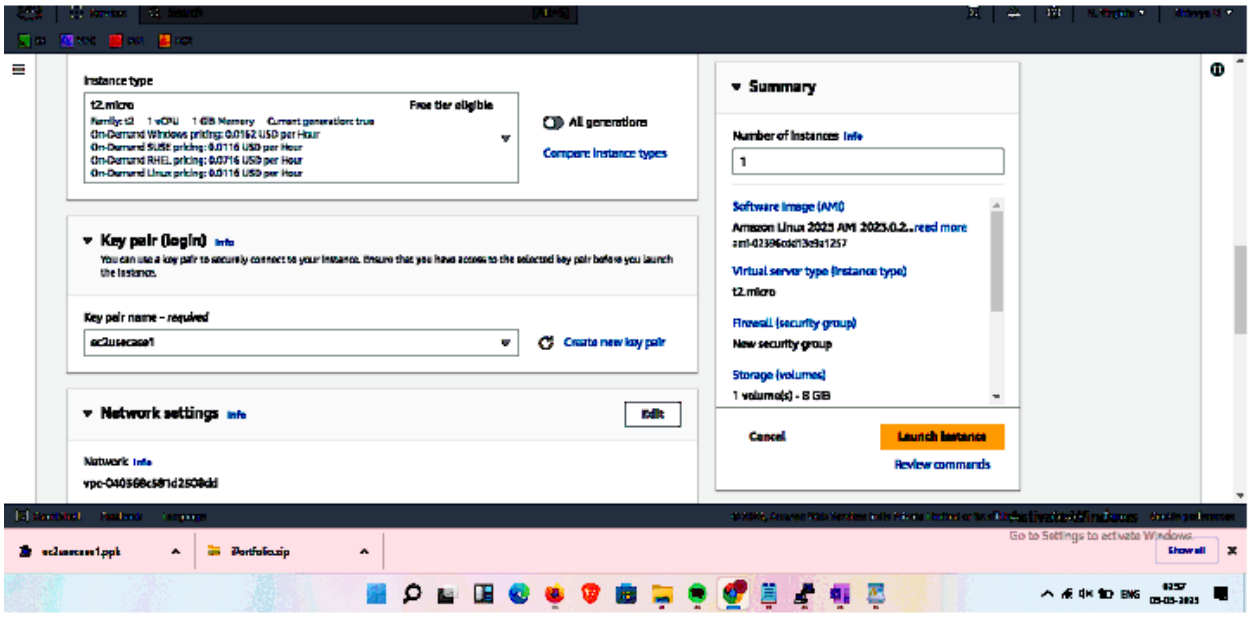
CC - CLOUD COMPUTING
727721EUIT034

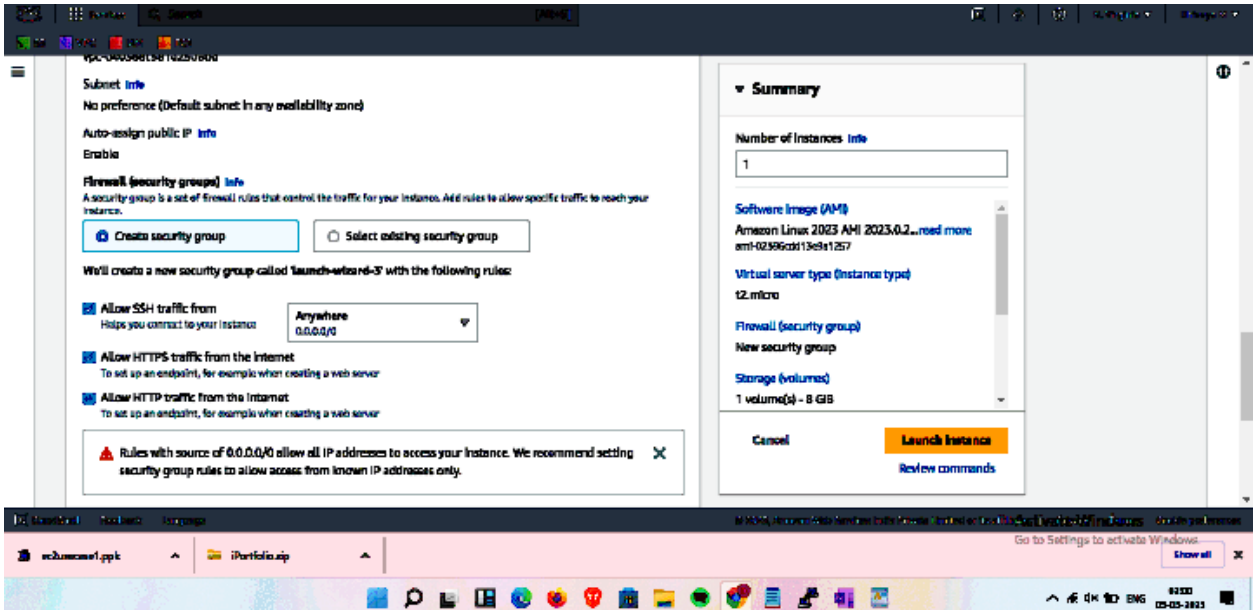
DHIVYA M
1.



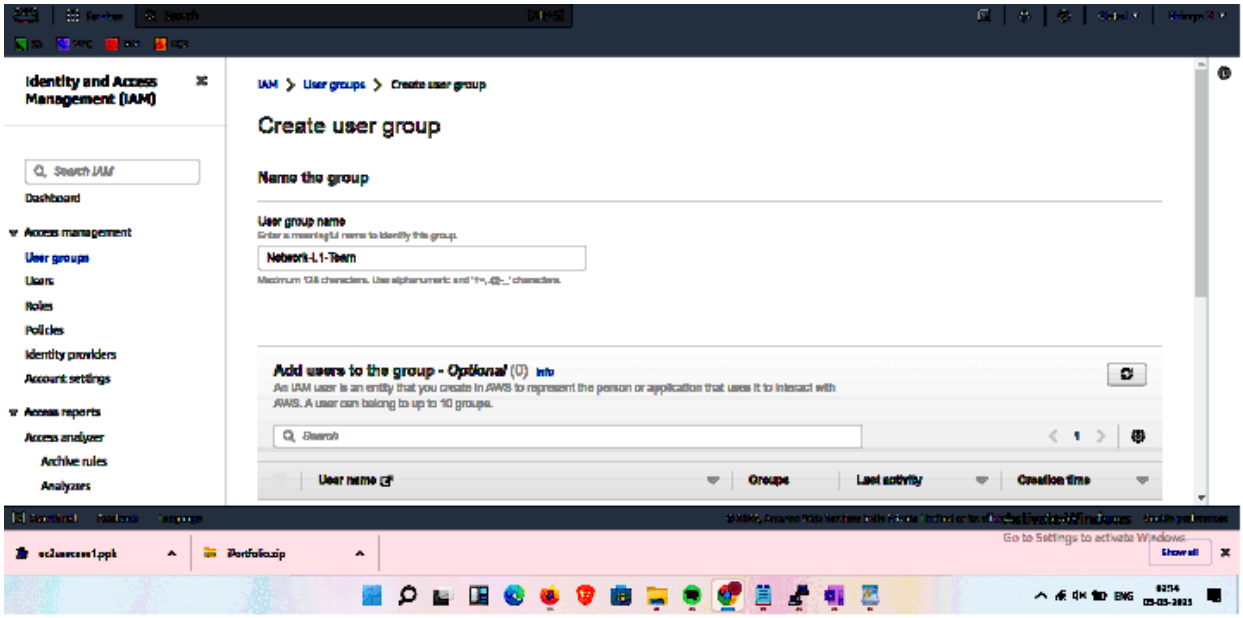


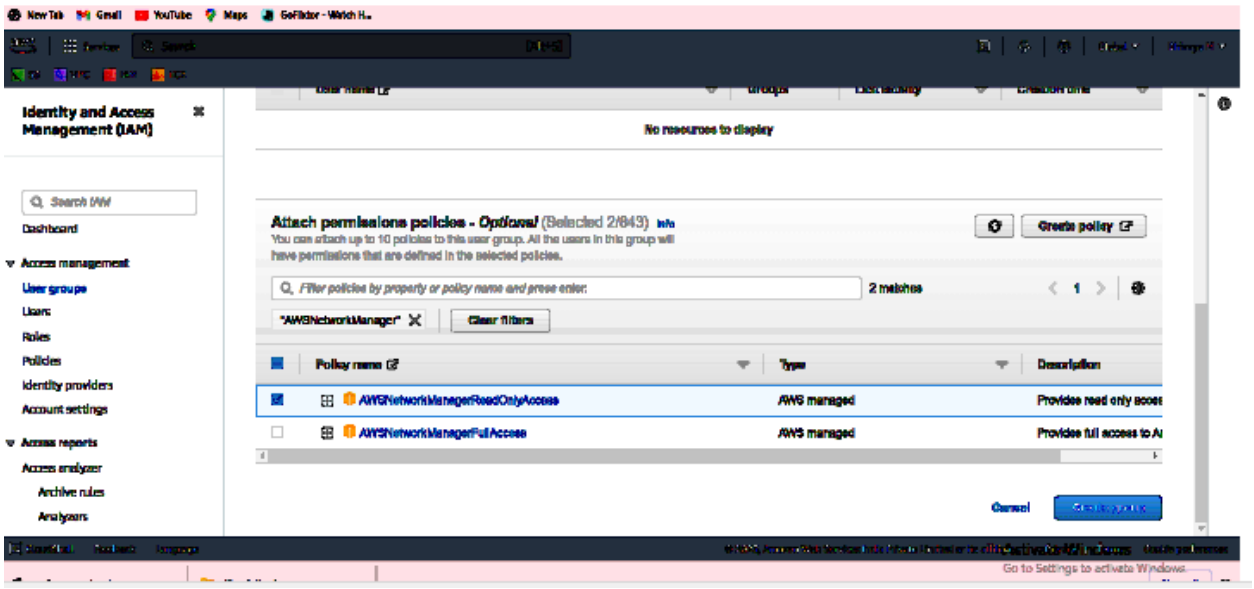

Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 AMI
Free tier eligible
Description
Amazon Linux 2023 AMI 2023.0.20230419.0 x86_64 HVM kernel-6.1
Architecture
Boot mode
AMI ID
64-bit (x86)
uefi-preferred
ami-02596cdd13e9a1257
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.0.2..read more
ami-02596cdd13e9a1257
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
ec2usecase1.ppk
iPortfolio.zip
Go to Settings to activate Windows.
Show all
ENG
03-05-2023

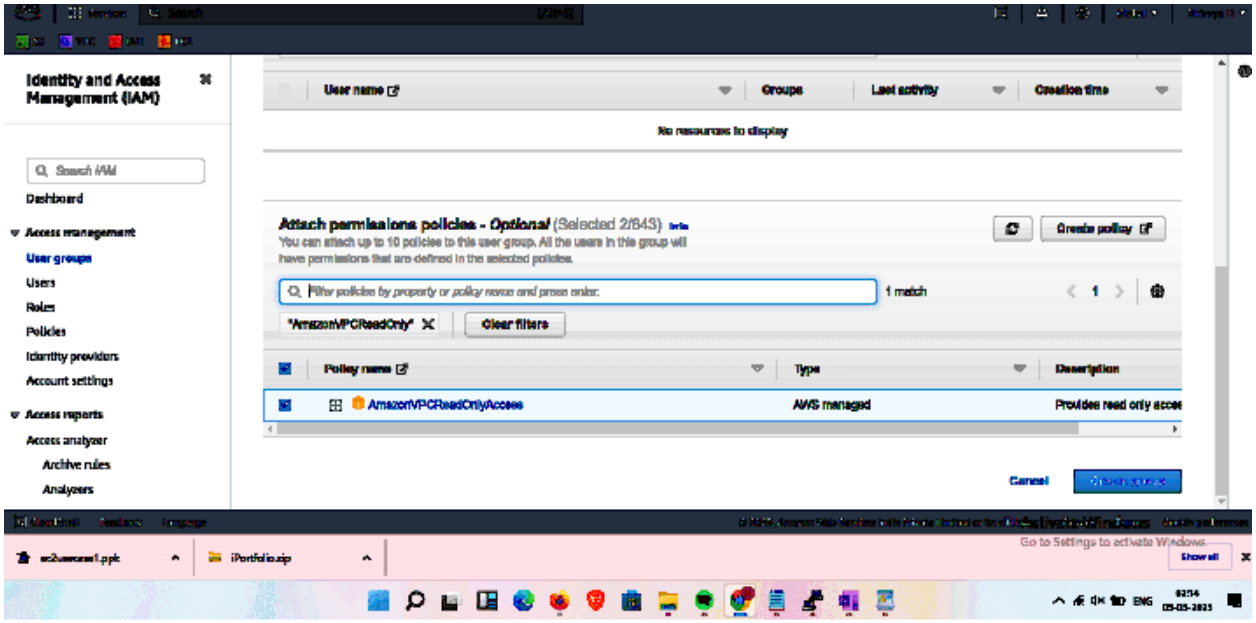

Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour
All generations
Compare instance types
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-040568c5811d2508dd
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.0.2..read more
ami-02596cdd13e9a1257
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
ec2usecase1.ppk
iPortfolio.zip
Go to Settings to activate Windows.
Show all
ENG
03-05-2023

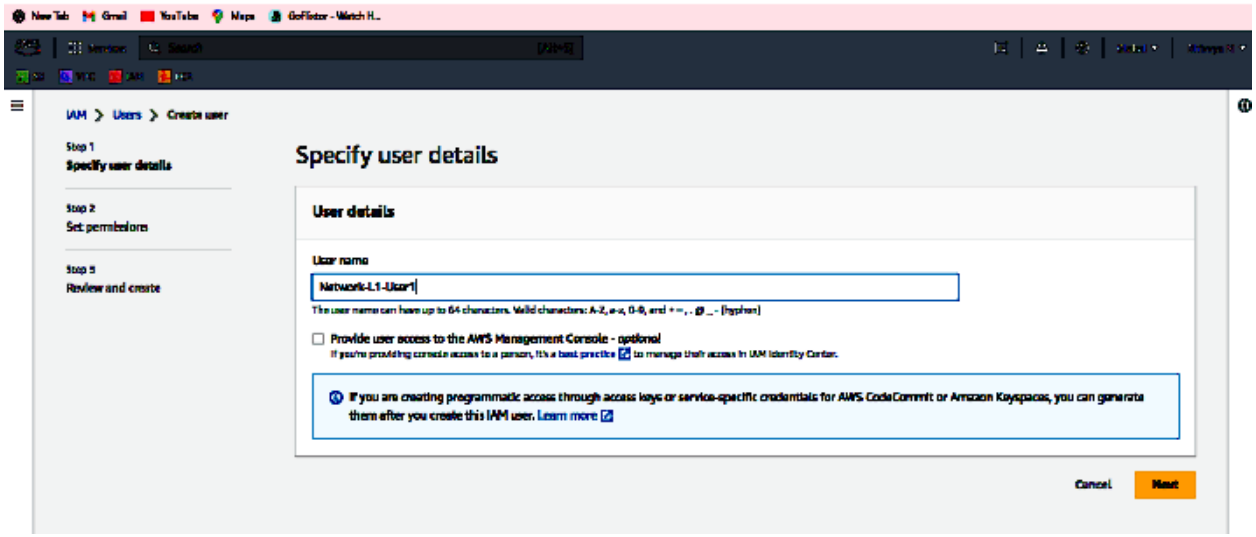

Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-3' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
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
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
iPortfolio.zip
Go to Settings to activate Windows.
Show all
ENG

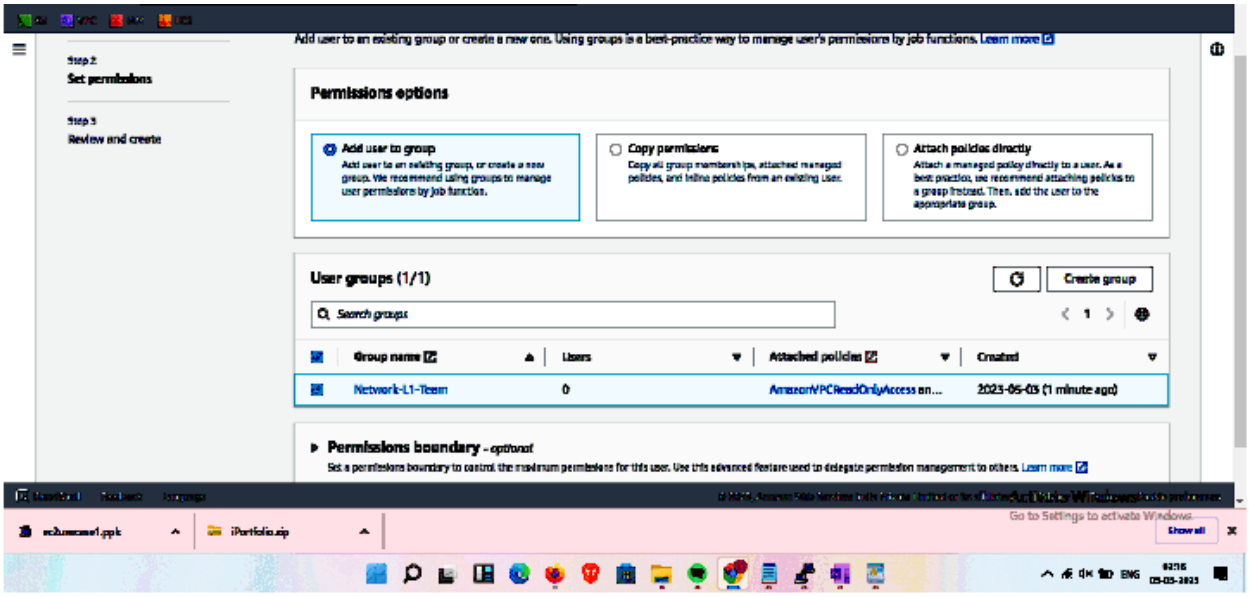
2.

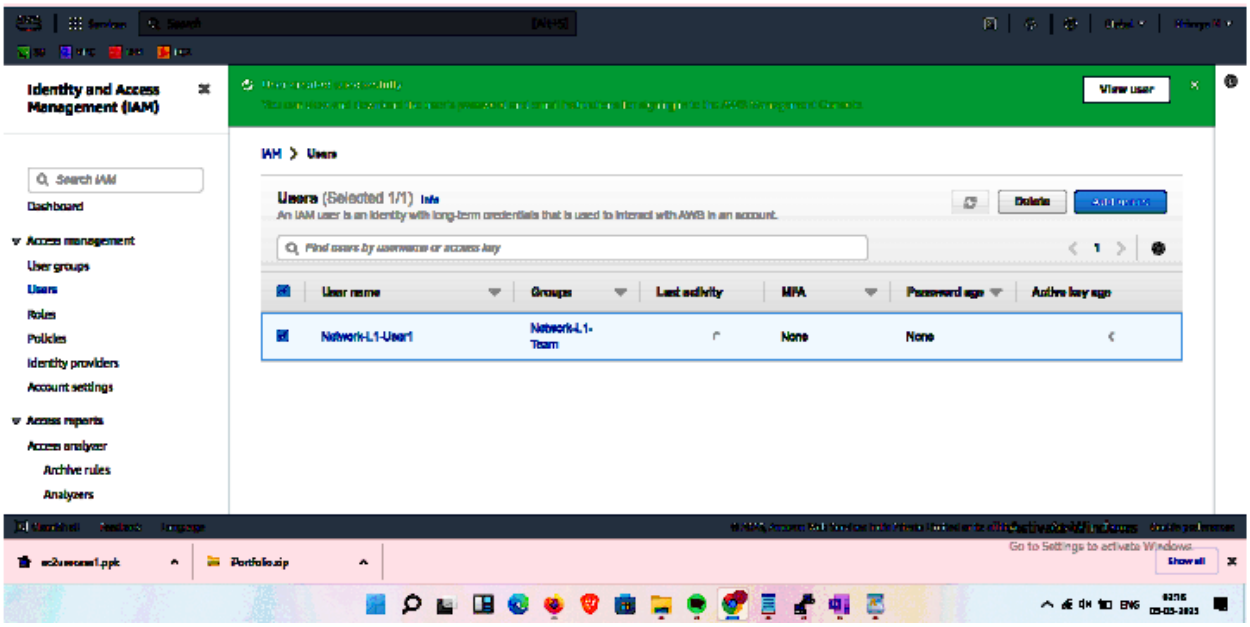

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Network-L1-Team
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
User name
Groups
Last activity
Creation time
Go to Settings to activate Windows.
Show all


New Tab
Gmail
YouTube
Maps
GoFlicker - Watch H...
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
No resources to display
Attach permissions policies - Optional (Selected 2/643) 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
"AWSNetworkManager"
Clear filters
Policy name
Type
Description
AWSNetworkManagerReadOnlyAccess
AWS managed
Provides read only acces
AWSNetworkManagerFullAccess
AWS managed
Provides full access to A
Cancel
Go to Settings to activate Windows.

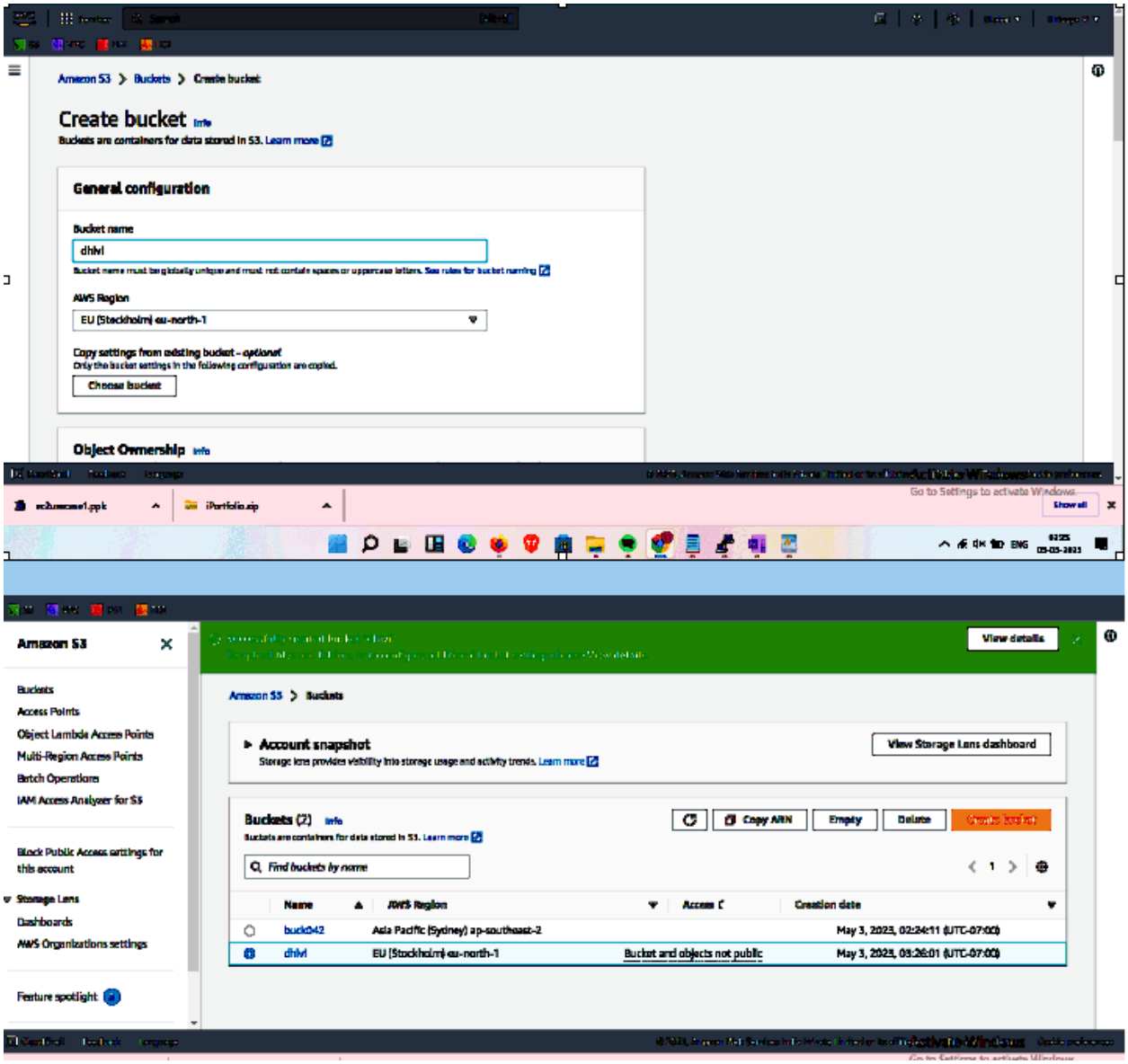

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
User name
Groups
Last activity
Creation time
No resources to display
Attach permissions policies - Optional (Selected 2/843)
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 match
"AmazonVPCReadOnly"
Clear filters
Policy name
Type
Description
AmazonVPCReadOnlyAccess
AWS managed
Provides read only acces
Cancel
Go to Settings to activate Windows.
Show all

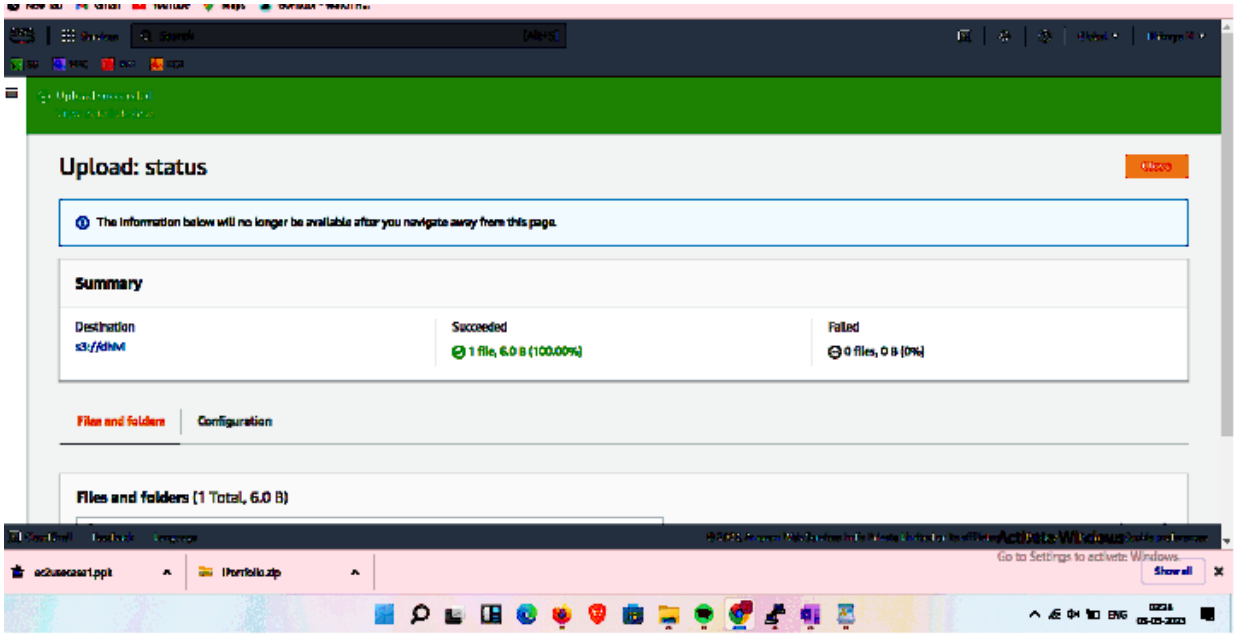

New Tab
Gmail
YouTube
Maps
GoFloter - Watch H...
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Network-L1-User1
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next

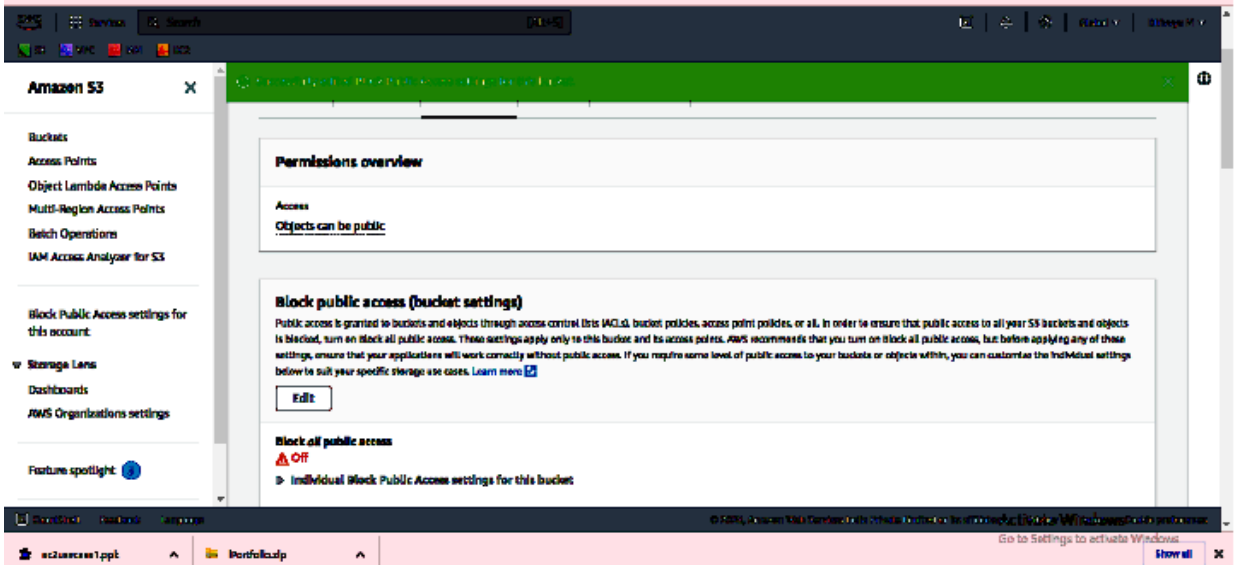

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Step 2
Set permissions
Step 3
Review and create
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
User groups (1/1)
Create group
Search groups
Group name
Users
Attached policies
Created
Network-L1-Team
0
AmazonVPCReadOnlyAccess an...
2023-05-05 (1 minute ago)
Permissions boundary - optional
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
ec2userroot1.ppk
iPortfolio.zip
Go to Settings to activate Windows.
Show all
ENG

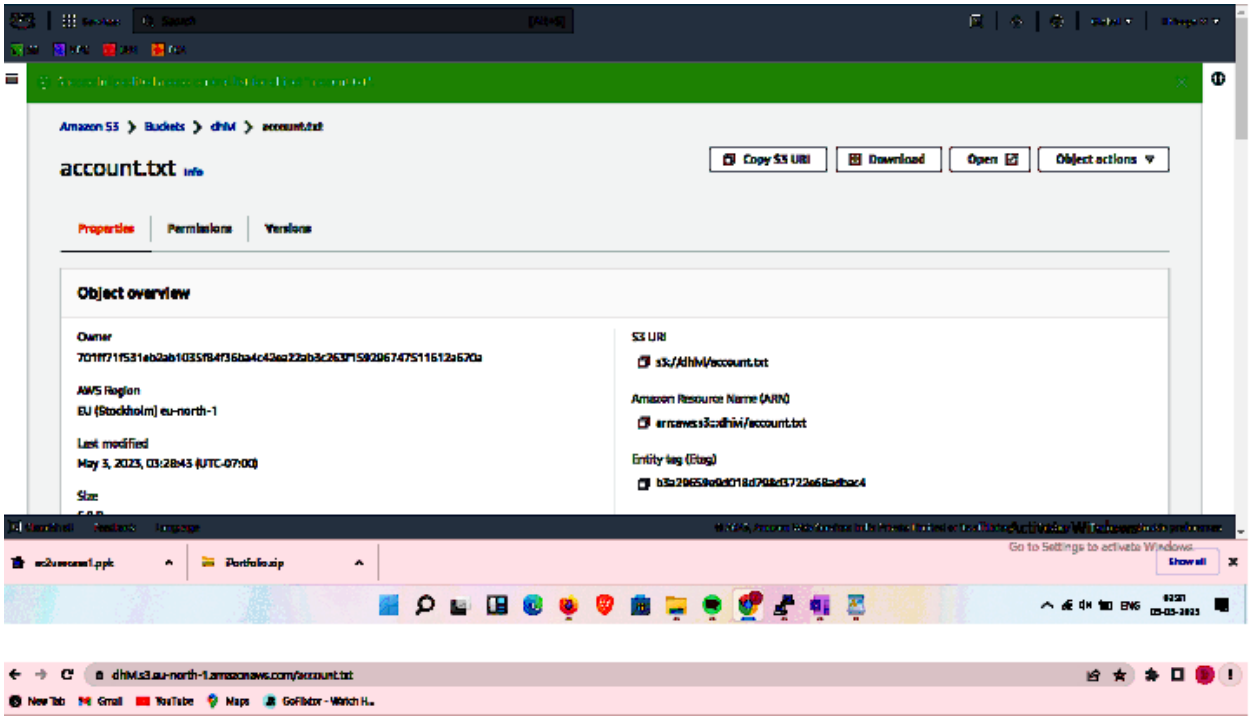

Identity and Access Management (IAM)
View user
IAM > Users
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Users (Selected 1/1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Add users
Find users by username or access key
User name
Groups
Last activity
MFA
Password age
Active key age
Network-L1-User1
Network-L1-Team
None
None
ec2userroot1.ppk
Portfolio.zip
Go to Settings to activate Windows.
Show all
ENG

3.


Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
dhivl
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
Go to Settings to activate Windows.
Show all
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
View details
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (7) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Find buckets by name
Name
AWS Region
Access
Creation date
buck042
Asia Pacific (Sydney) ap-southeast-2
May 3, 2023, 02:24:11 (UTC-07:00)
dhivl
EU (Stockholm) eu-north-1
Bucket and objects not public
May 3, 2023, 03:26:01 (UTC-07:00)


Upload: status
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://dhm
Succeeded
1 file, 6.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 6.0 B)
ec2usecase1.ppt
Portfolio.zip
Show all


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
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
ec2usecase1.ppt
Portfolio.zip
Show all


Amazon S3 > Buckets > dhiv > account.txt
account.txt Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
AWS Region
EU (Stockholm) eu-north-1
Last modified
May 3, 2023, 03:28:43 (UTC-07:00)
Size
S3 URI
s3://dhiv/account.txt
Amazon Resource Name (ARN)
arn:aws:s3:::dhiv/account.txt
Entity tag (Etag)
Portfolio.zip
Show all
Go to Settings to activate Windows.