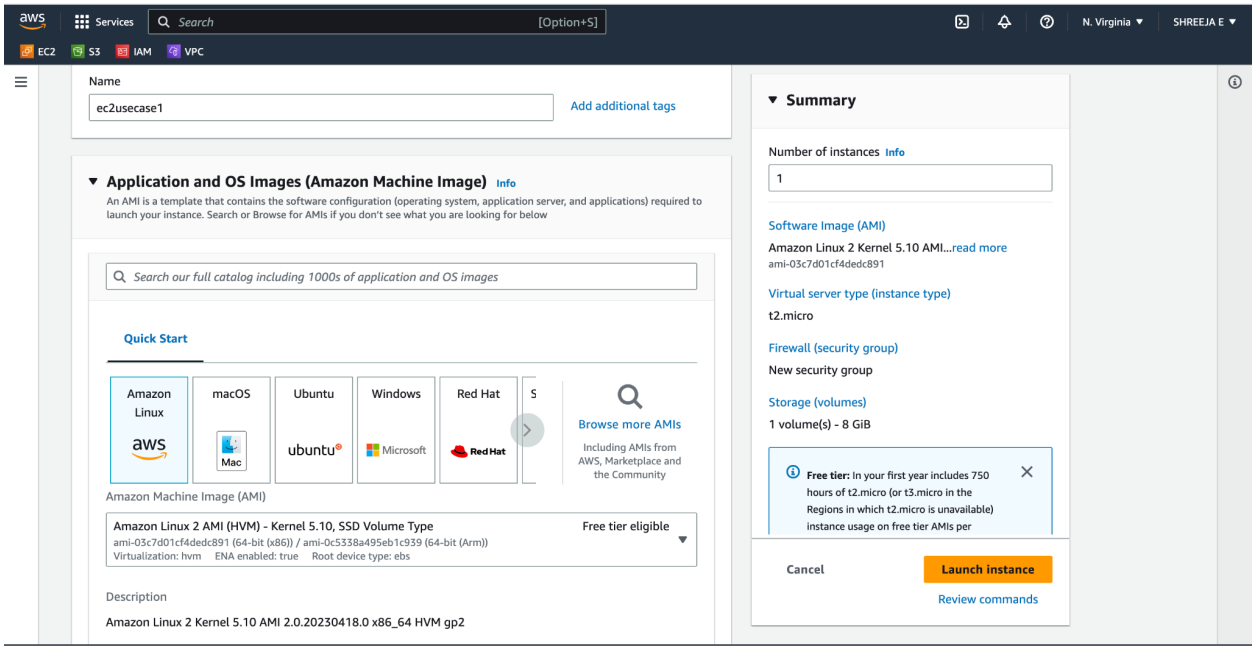
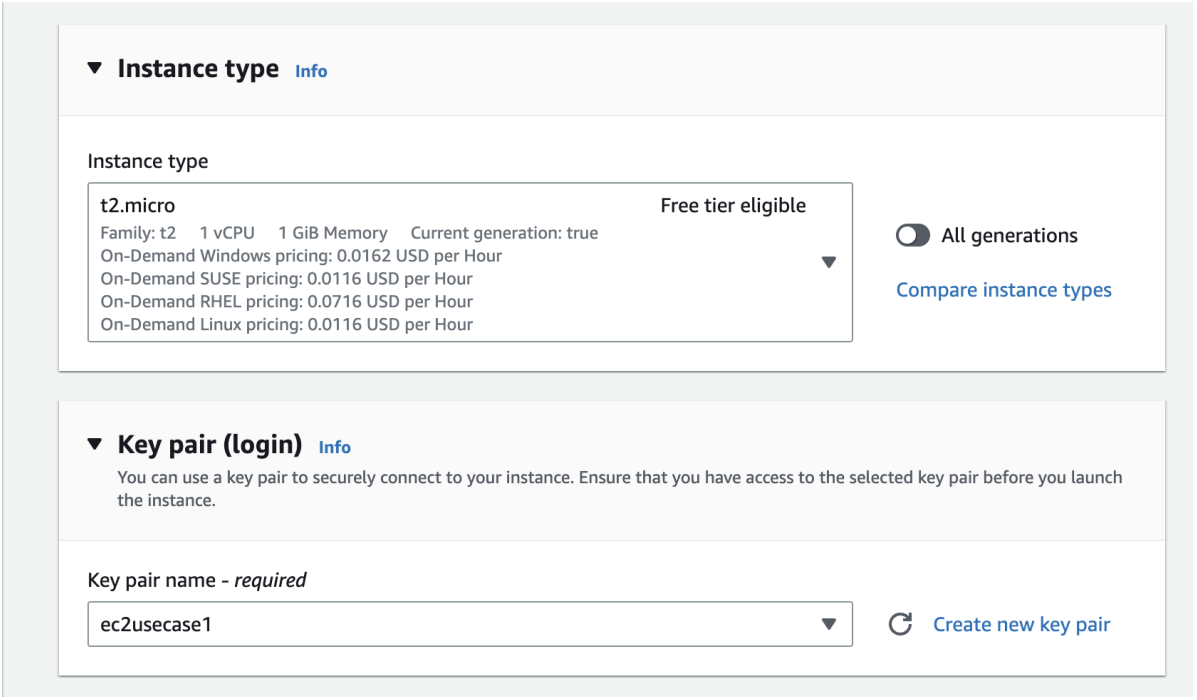
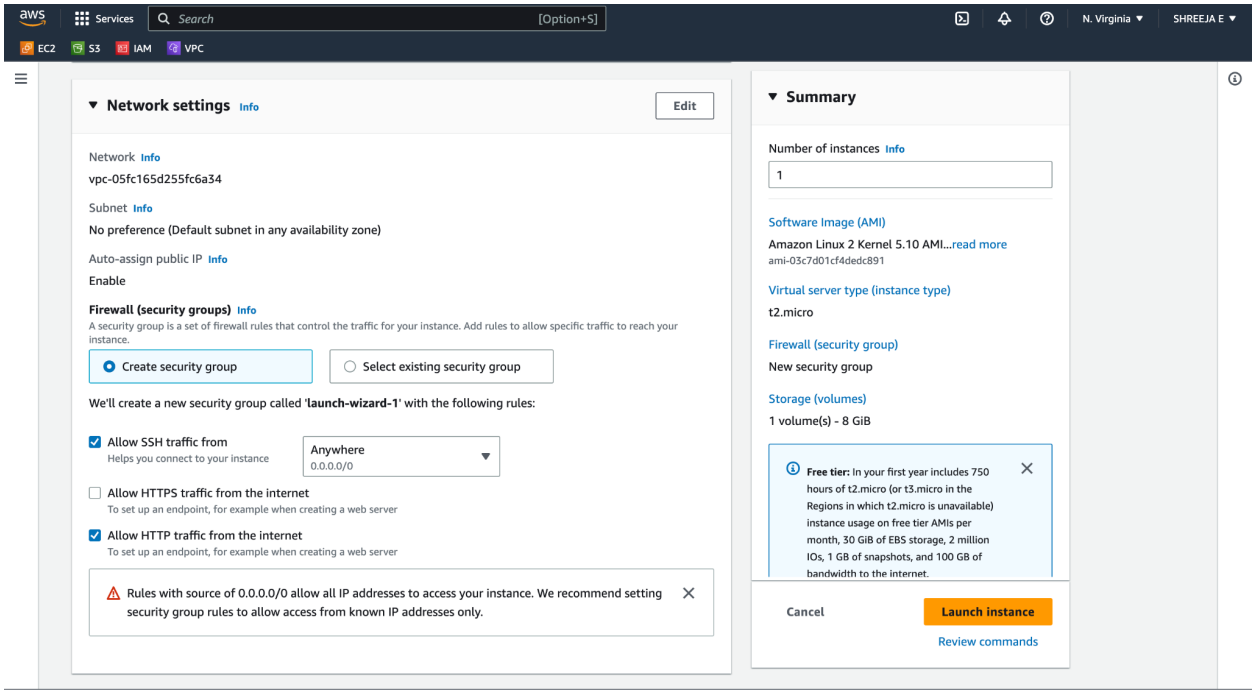
SHREEJA E
727721EUIT147

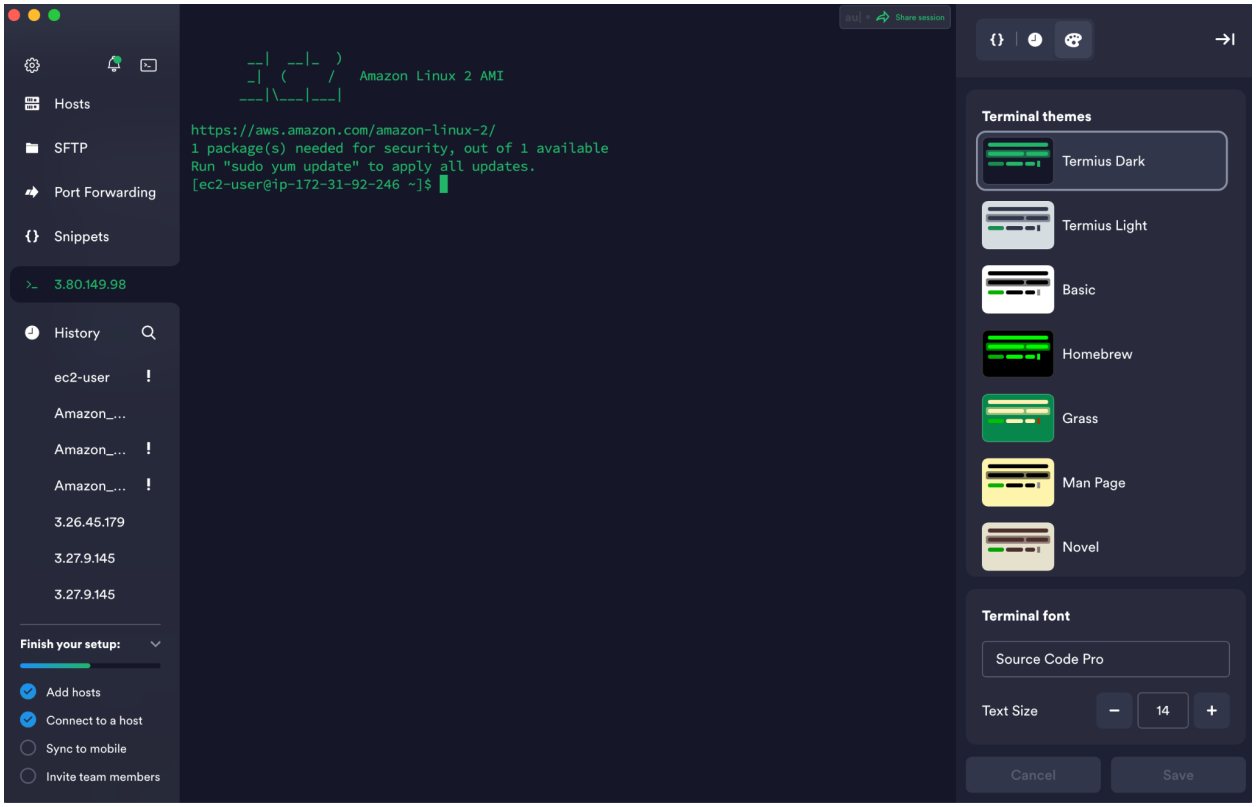
CC1

1

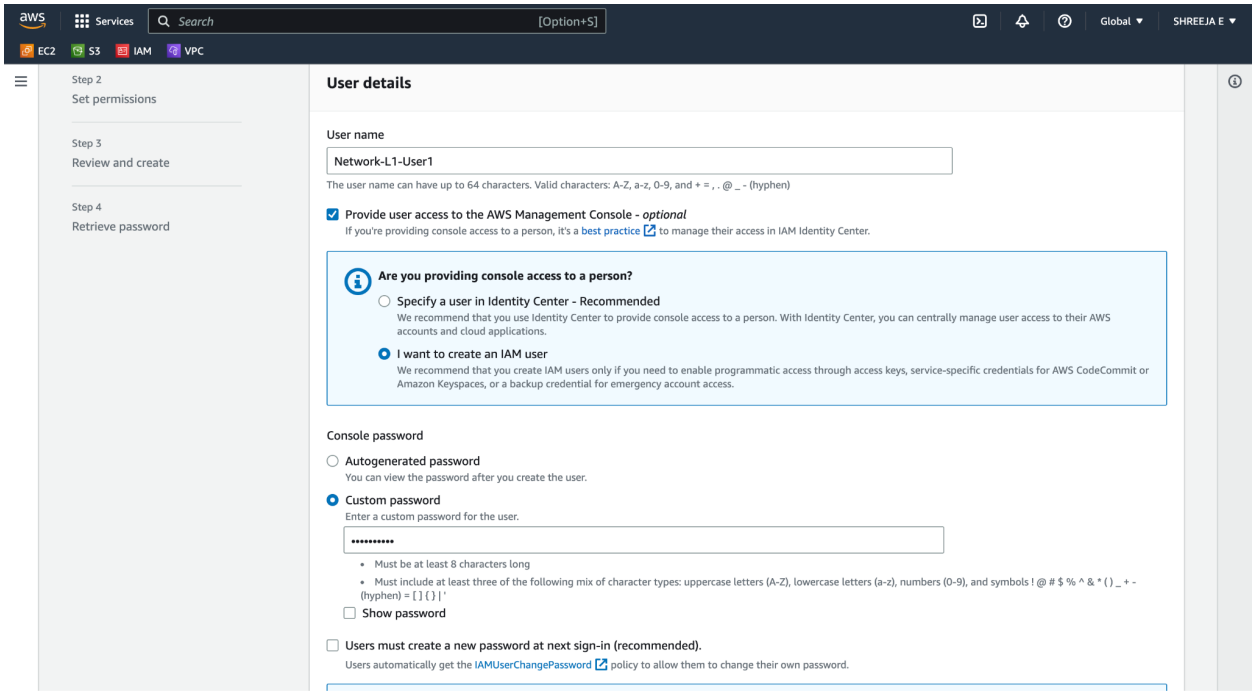


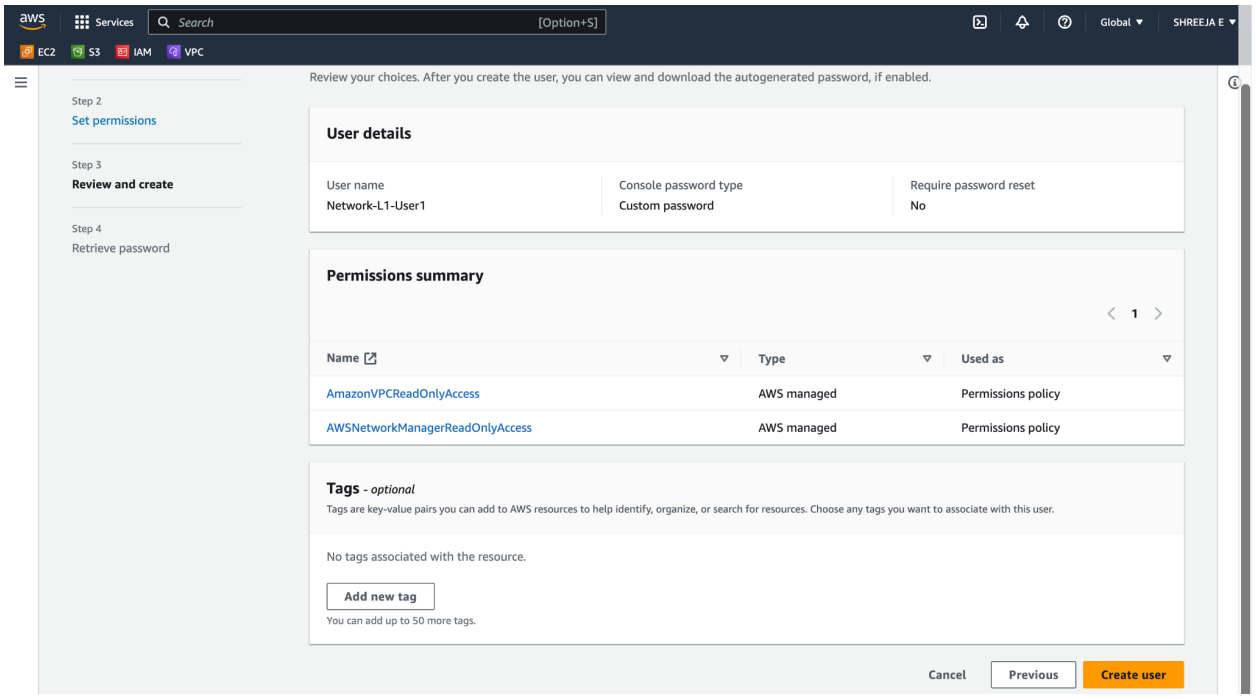


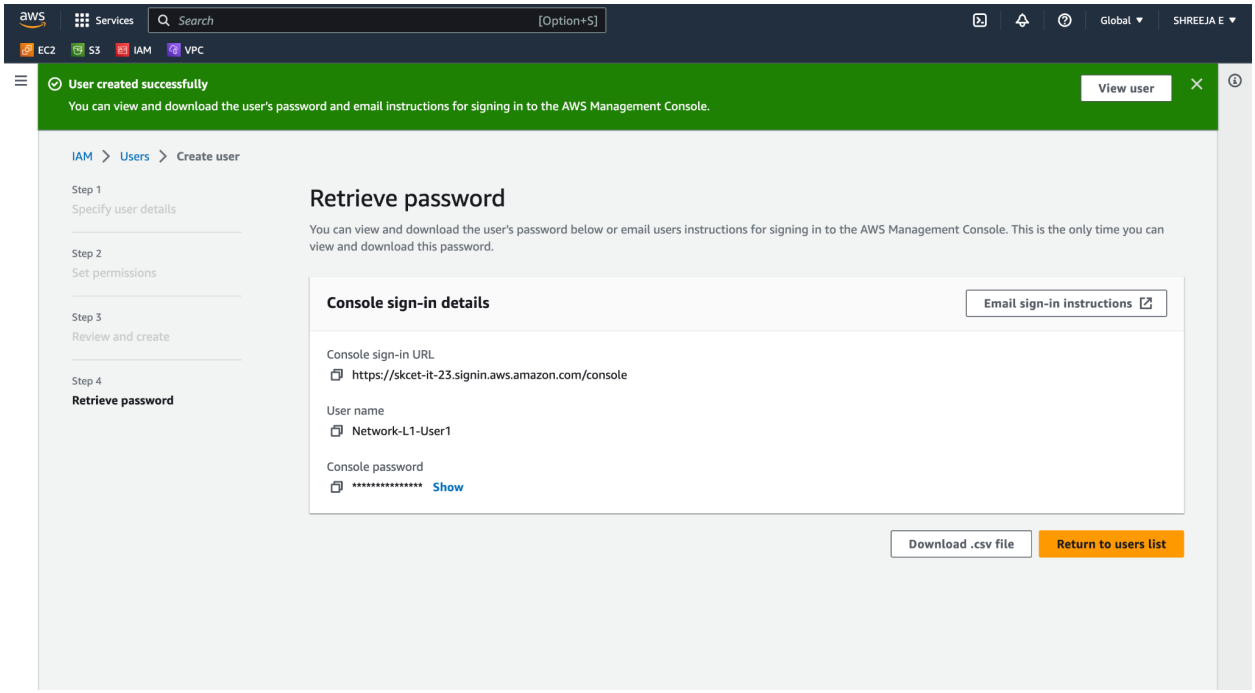

aws
Services
Search
[Option+S]
EC2
S3
IAM
VPC
N. Virginia
SHREEJA E
Network settings Info
Edit
Network Info
vpc-05fc165d255fc6a34
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall 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-1' 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 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
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands

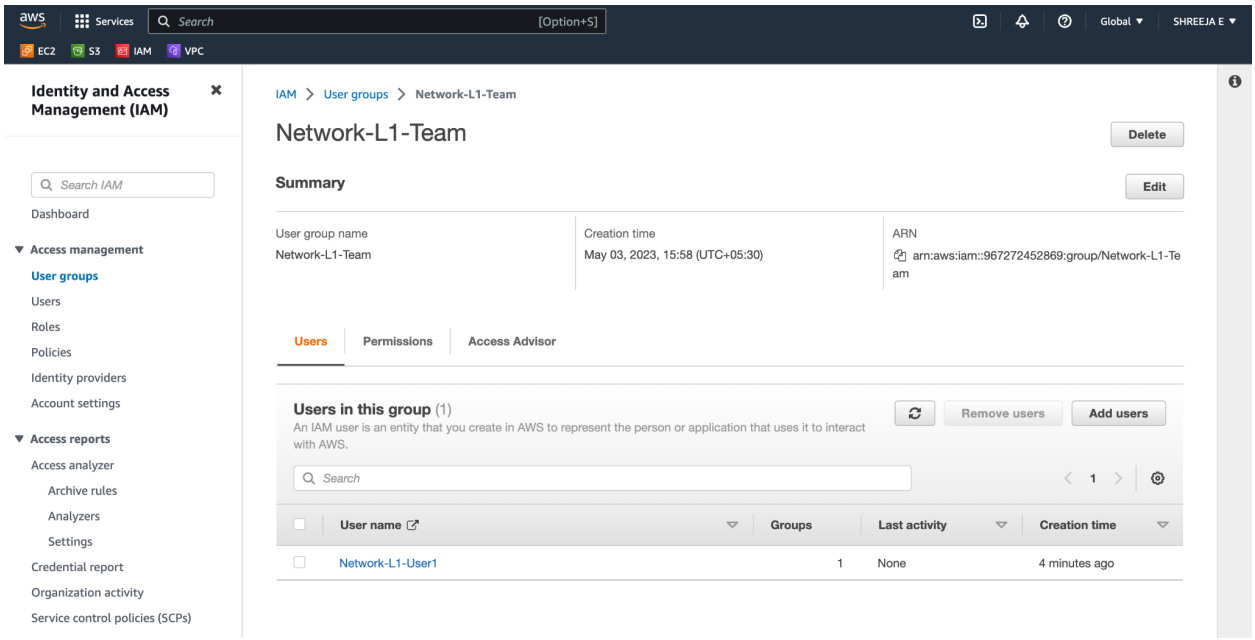

Hosts
SFTP
Port Forwarding
Snippets
3.80.149.98
History
ec2-user
Amazon_...
Amazon_...
Amazon_...
3.26.45.179
3.27.9.145
3.27.9.145
Finish your setup:
Add hosts
Connect to a host
Sync to mobile
Invite team members
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-92-246 ~]$
Terminal themes
Termius Dark
Termius Light
Basic
Homebrew
Grass
Man Page
Novel
Terminal font
Source Code Pro
Text Size
14
Cancel
Save

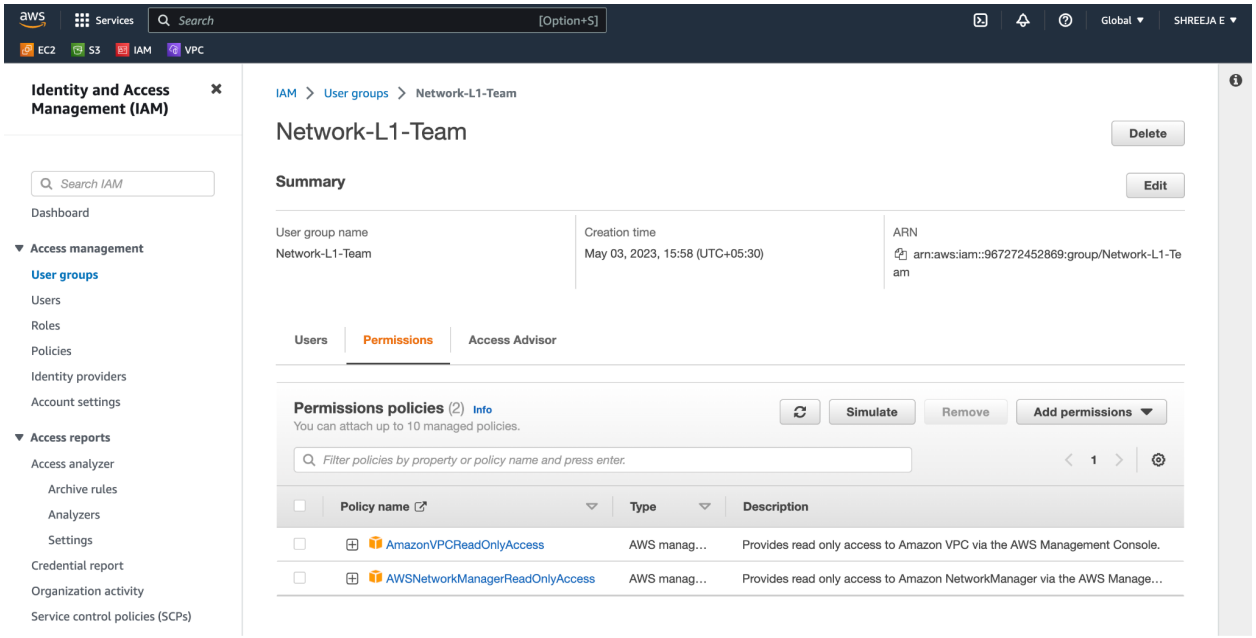
2


aws
Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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.
Are you providing console access to a person?
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in (recommended).
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

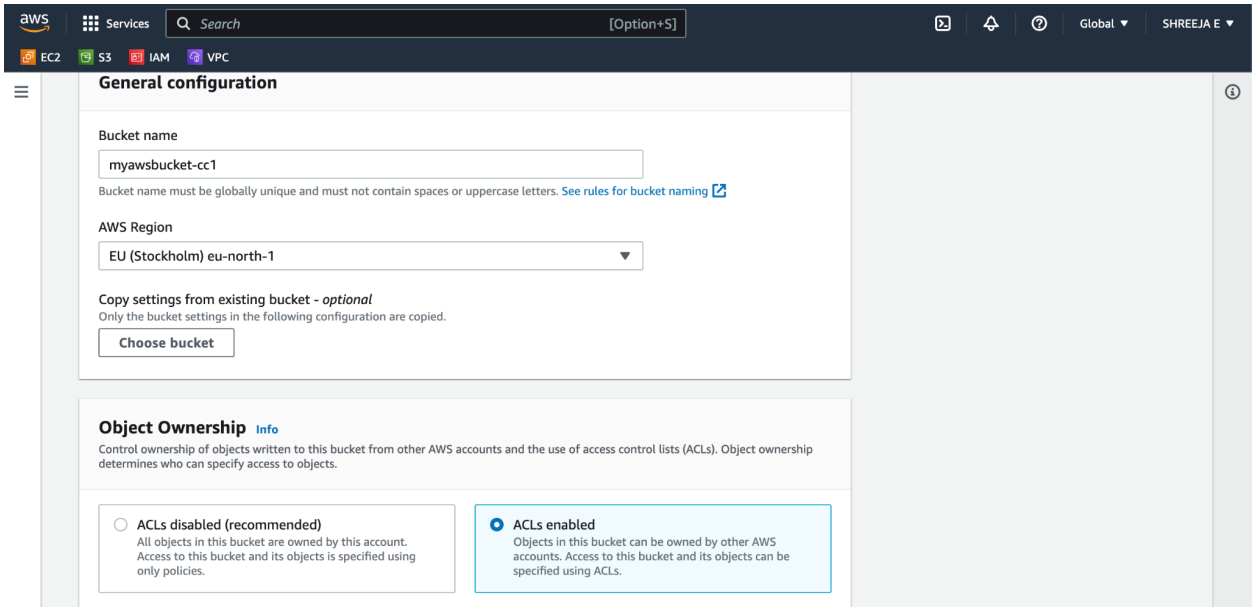

aws
Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Network-L1-User1
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonVPCReadOnlyAccess
AWS managed
Permissions policy
AWSNetworkManagerReadOnlyAccess
AWS managed
Permissions policy
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user

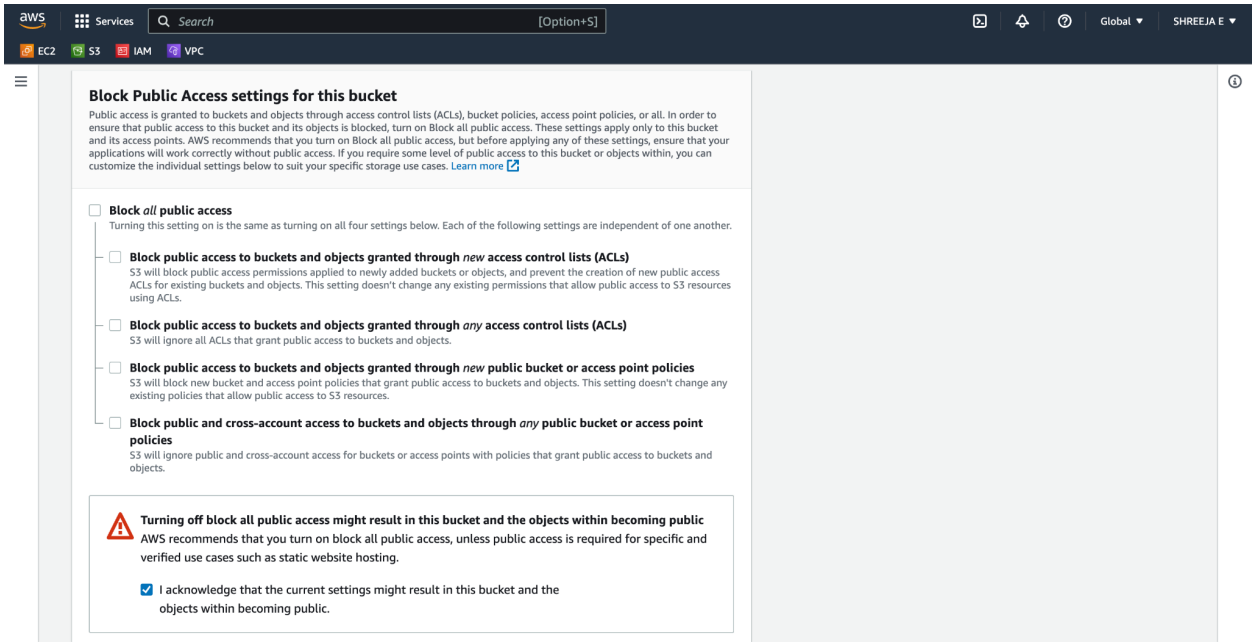

Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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
Email sign-in instructions
Console sign-in URL
https://skcet-it-23.signin.aws.amazon.com/console
User name
Network-L1-User1
Console password
********** Show
Download .csv file
Return to users list

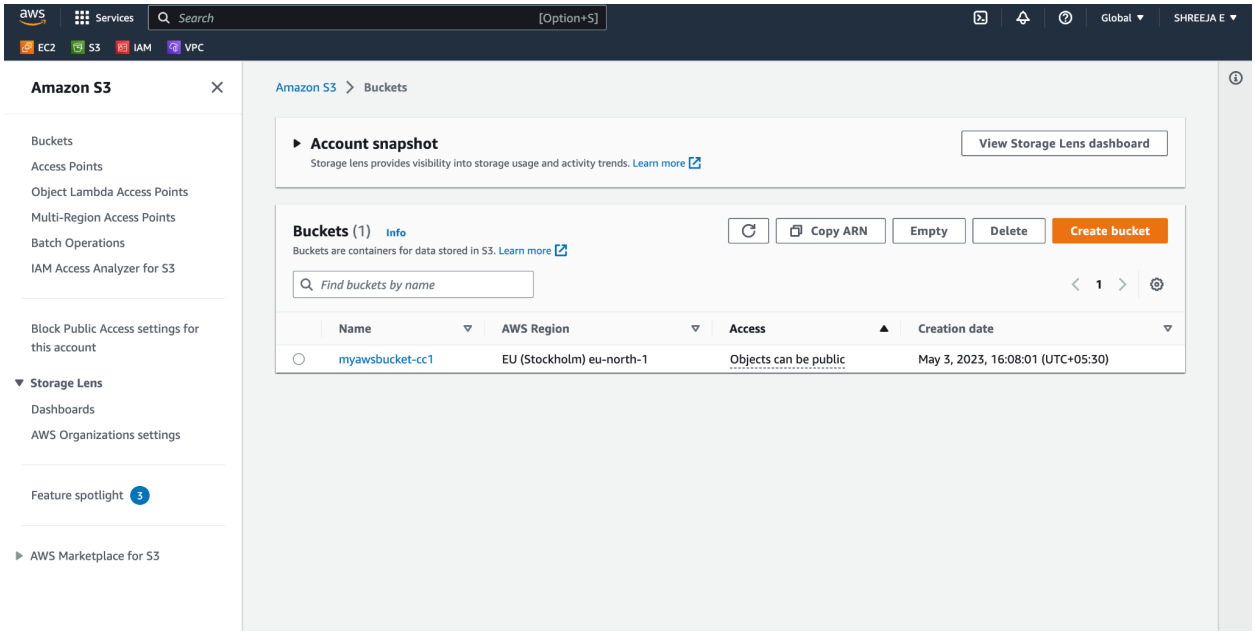

Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Network-L1-Team
Network-L1-Team
Delete
Summary
Edit
User group name
Network-L1-Team
Creation time
May 03, 2023, 15:58 (UTC+05:30)
ARN
arn:aws:iam::967272452869:group/Network-L1-Team
Users
Permissions
Access Advisor
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.
Remove users
Add users
Search
1
User name
Groups
Last activity
Creation time
Network-L1-User1
1
None
4 minutes ago

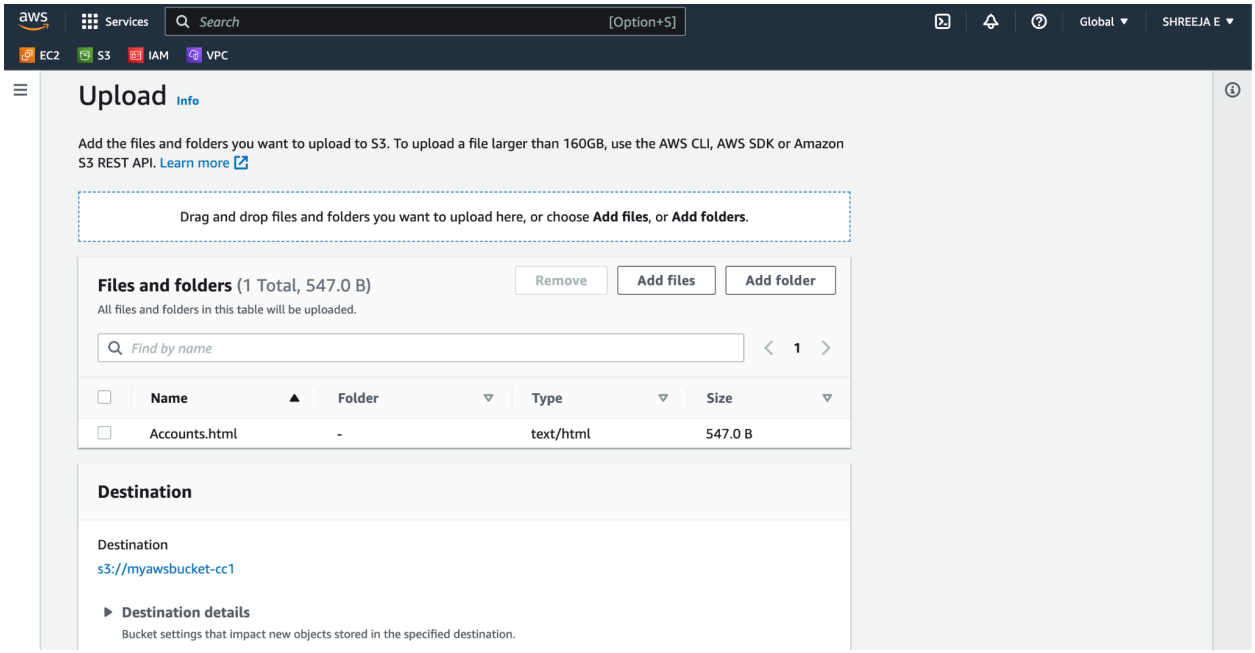

aws
Services
Search
[Option+S]
EC2
S3
IAM
VPC
Global
SHREEJA E
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Network-L1-Team
Network-L1-Team
Delete
Summary
Edit
User group name
Network-L1-Team
Creation time
May 03, 2023, 15:58 (UTC+05:30)
ARN
arn:aws:iam::967272452869:group/Network-L1-Team
Users
Permissions
Access Advisor
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter policies by property or policy name and press enter.
1
Policy name
Type
Description
AmazonVPCReadOnlyAccess
AWS manag...
Provides read only access to Amazon VPC via the AWS Management Console.
AWSNetworkManagerReadOnlyAccess
AWS manag...
Provides read only access to Amazon NetworkManager via the AWS Manage...

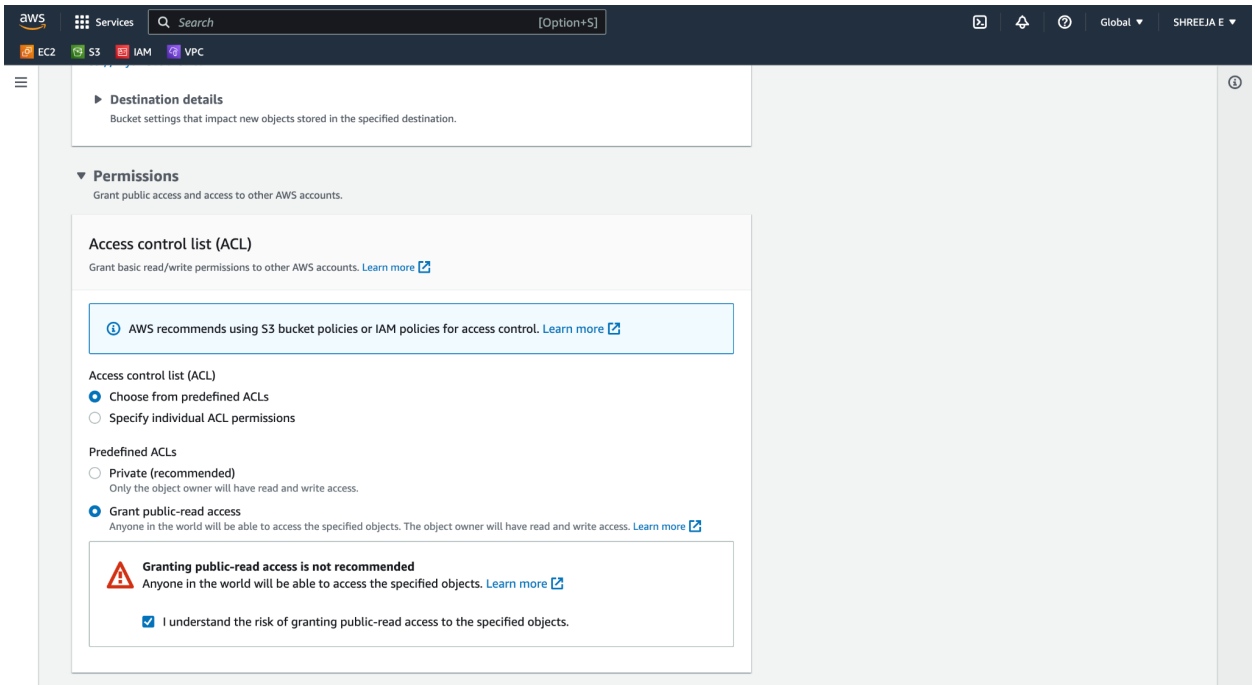
3

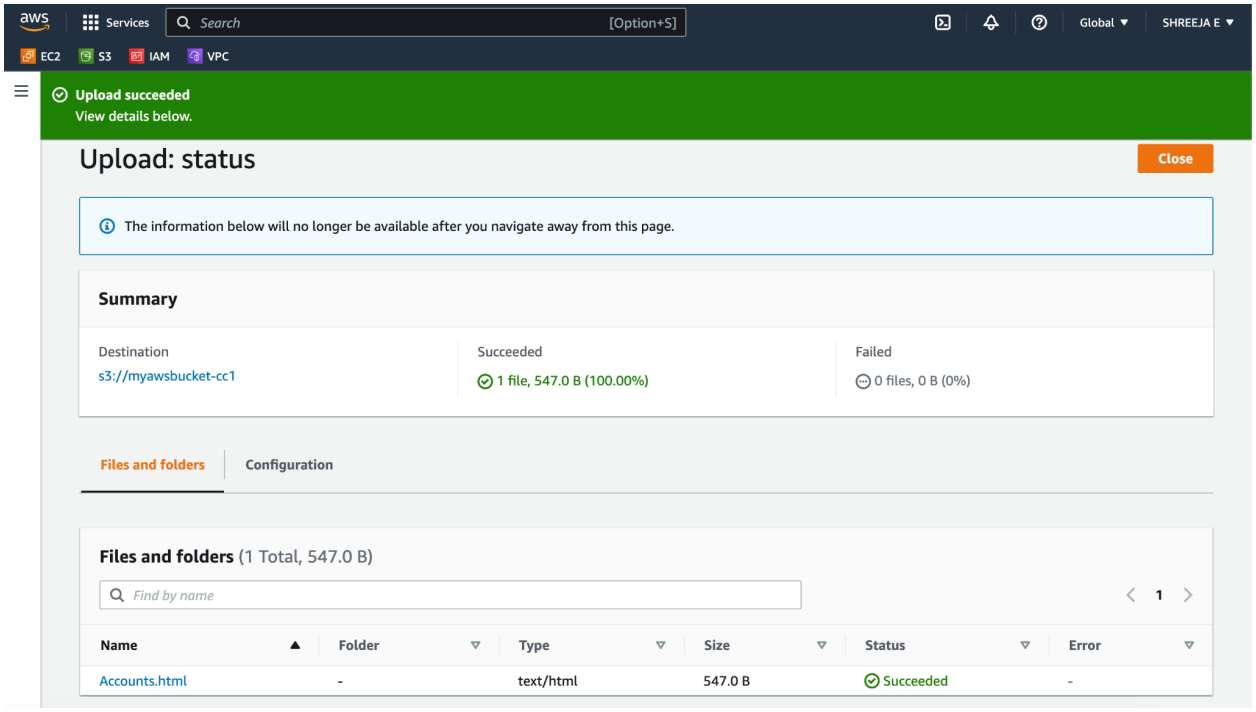

aws
Services
Search
[Option+S]
EC2
S3
IAM
VPC
Global
SHREEJA E
General configuration
Bucket name
myawsbucket-cc1
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
EU (Stockholm) eu-north-1
Copy settings from existing bucket - 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.


Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
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
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.


Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
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
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
1
Name
AWS Region
Access
Creation date
myawsbucket-cc1
EU (Stockholm) eu-north-1
Objects can be public
May 3, 2023, 16:08:01 (UTC+05:30)


aws
Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
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, 547.0 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.html
-
text/html
547.0 B
Destination
Destination
s3://myawsbucket-cc1
Destination details
Bucket settings that impact new objects stored in the specified destination.


aws
Services
Search
[Option+S]
Global
SHREEJA E
EC2
S3
IAM
VPC
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
AWS recommends using S3 bucket policies or IAM policies for access control. Learn more
Access control list (ACL)
Choose from predefined ACLs
Specify individual ACL permissions
Predefined ACLs
Private (recommended)
Only the object owner will have read and write access.
Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more
Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more
I understand the risk of granting public-read access to the specified objects.



Hai !!!
I am Shreeja .