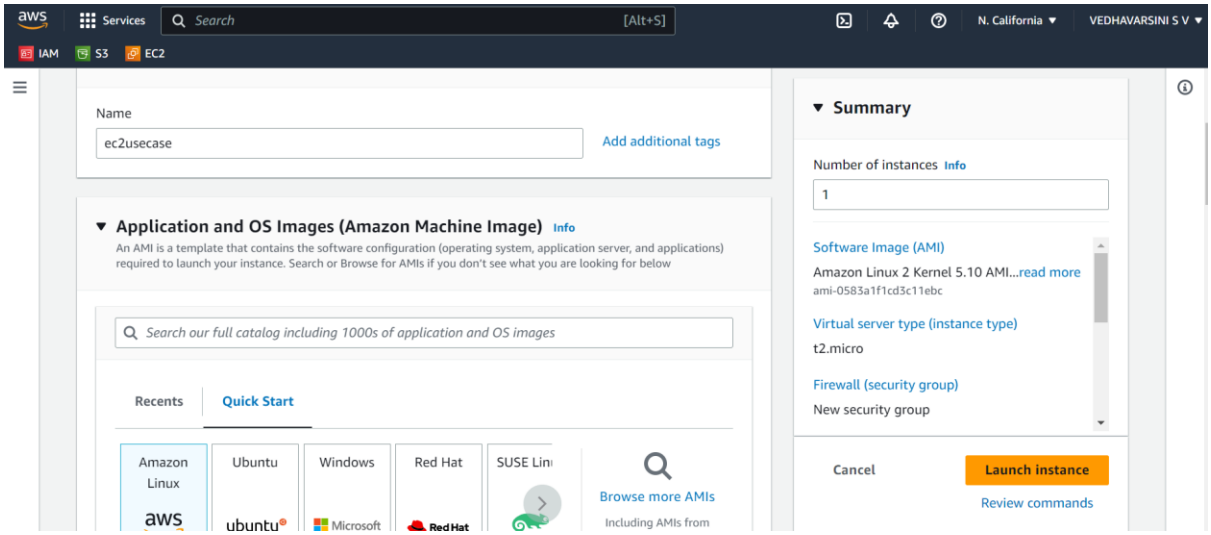
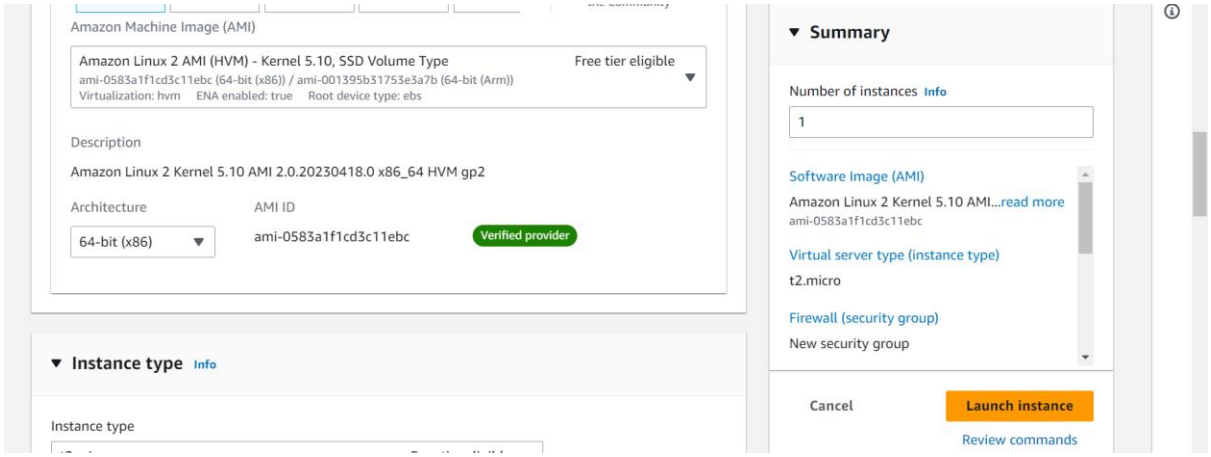
VEDHAVARSINI S V

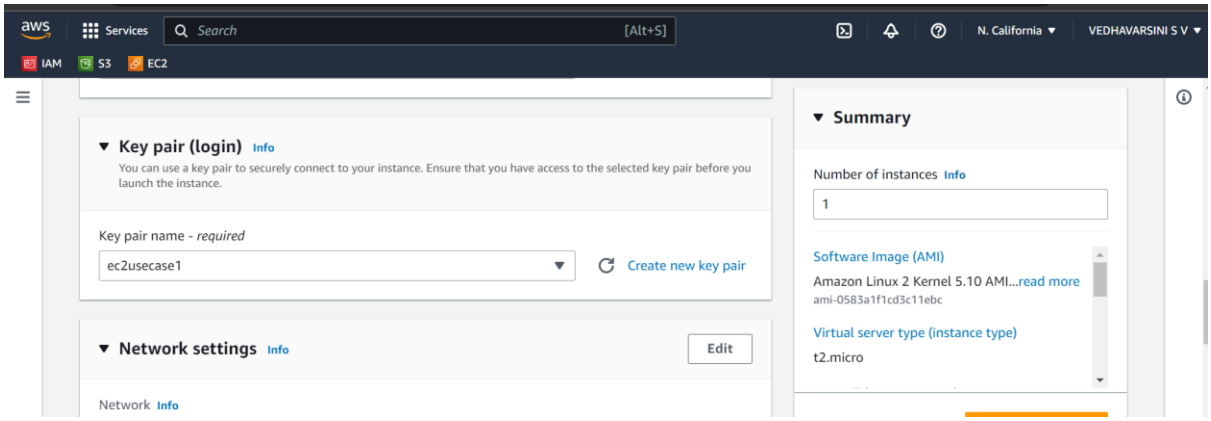
727721EUIT175

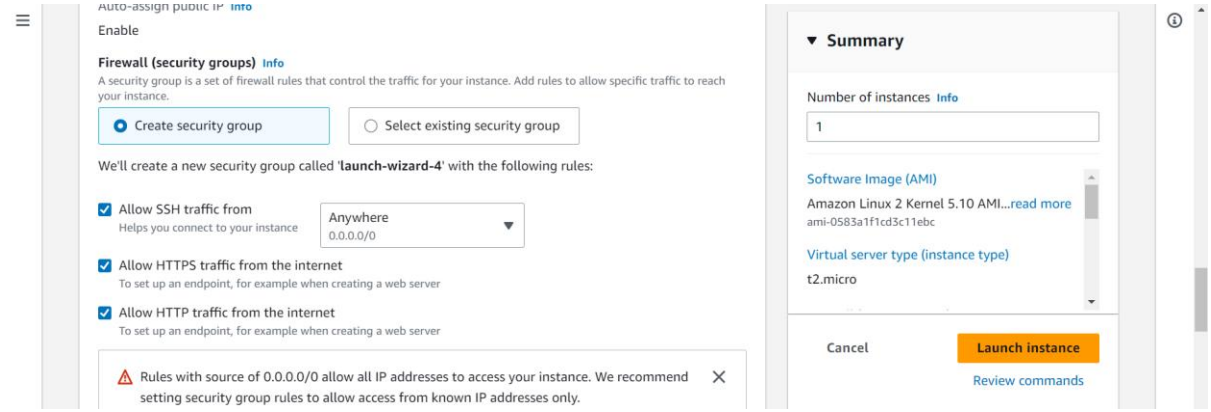
CC1

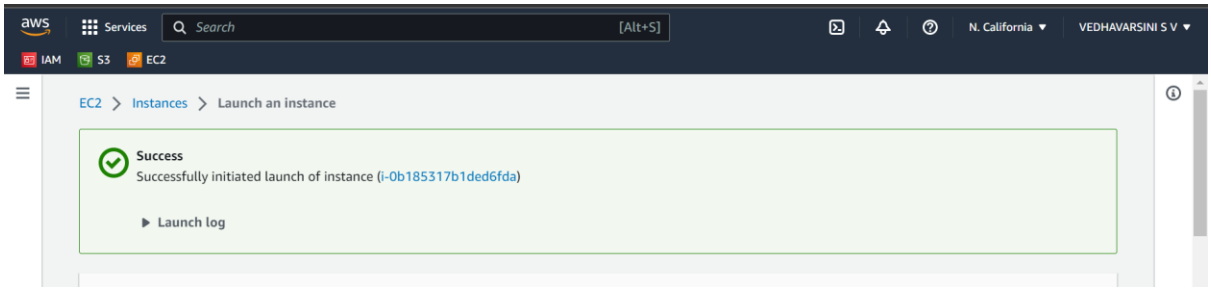
1.

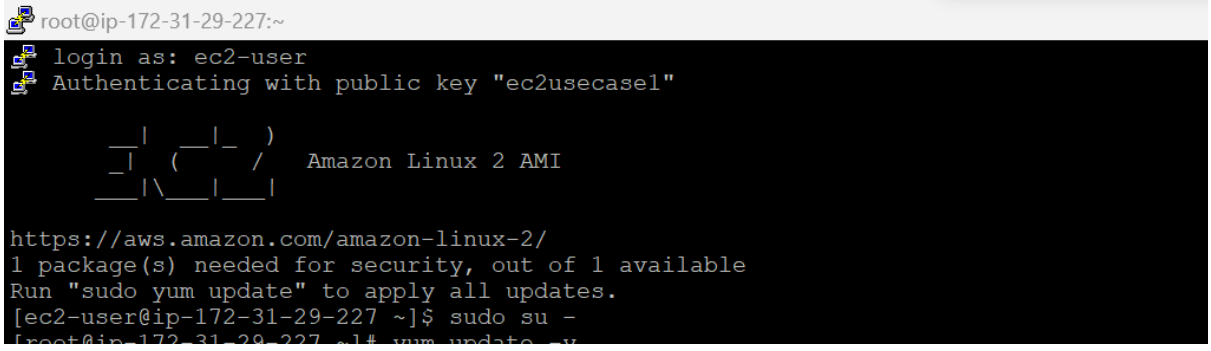




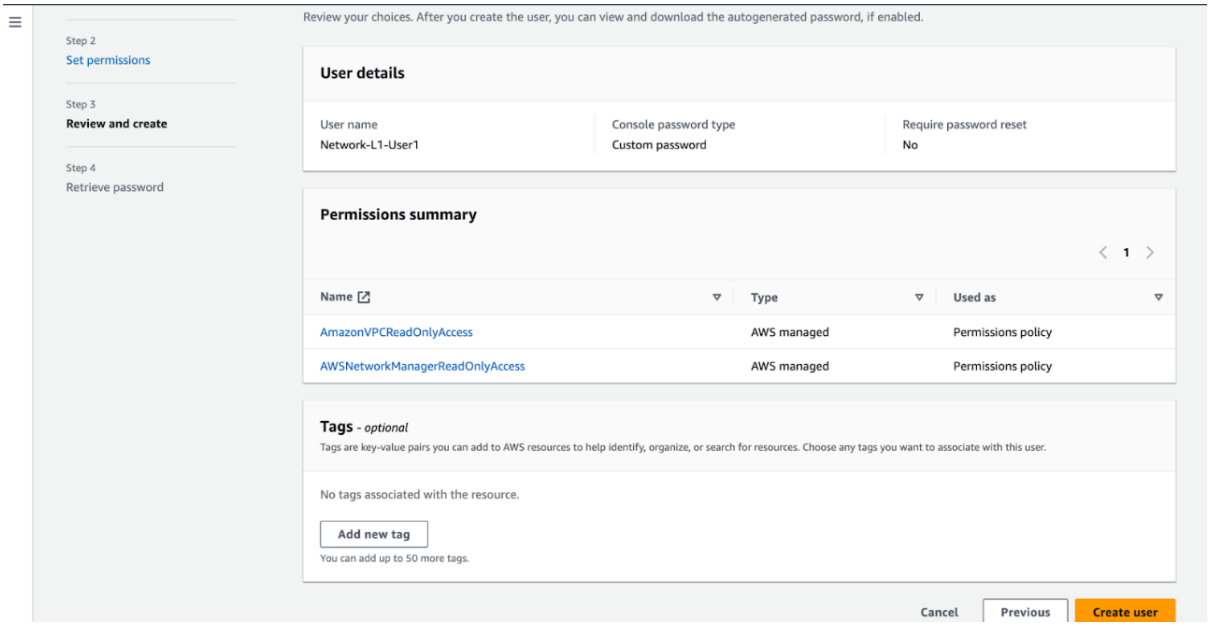

aws
Services
Search
[Alt+S]
N. California
VEDHAVARSINI S V
IAM
S3
EC2
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
ec2usecase1
Create new key pair
Network settings Info
Edit
Network Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0583a1f1cd3c11ebc
Virtual server type (instance type)
t2.micro

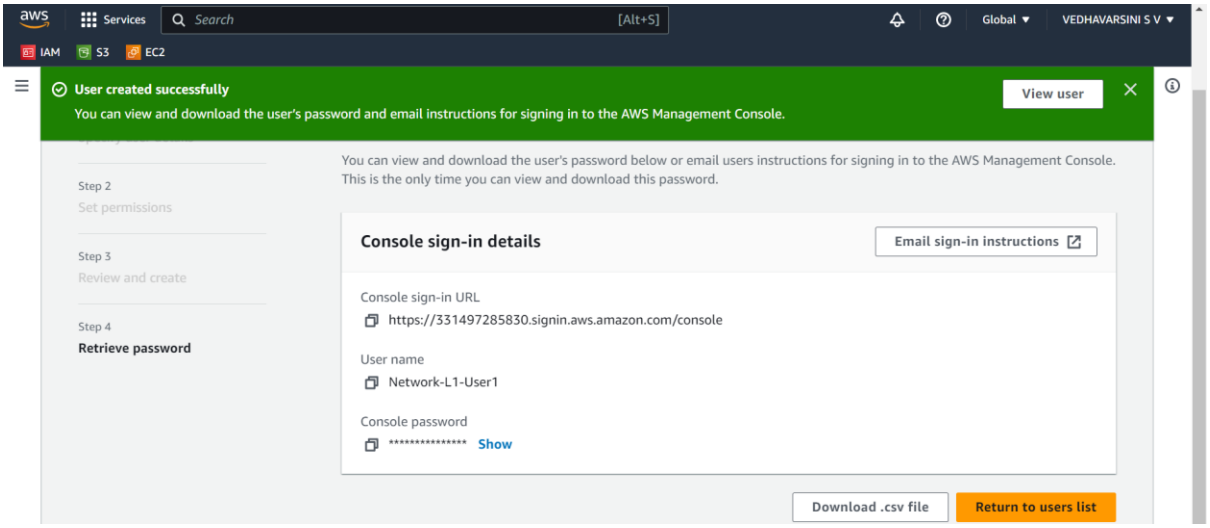

Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-4' 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-0583a1f1cd3c11ebc
Virtual server type (instance type)
t2.micro
Cancel
Launch instance
Review commands

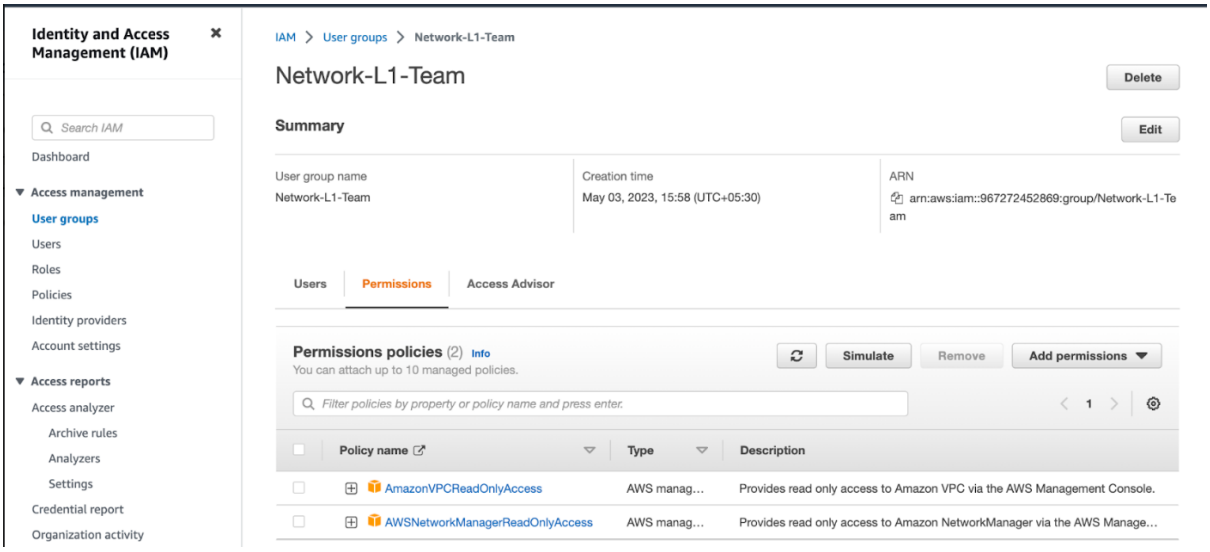

aws
Services
Search
[Alt+S]
N. California
VEDHAVARSINI S V
IAM
S3
EC2
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0b185317b1ded6fda)
Launch log


root@ip-172-31-29-227:~
login as: ec2-user
Authenticating with public key "ec2usecase1"
__| __|_)
_| (/ 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-172-31-29-227 ~]$ sudo su -

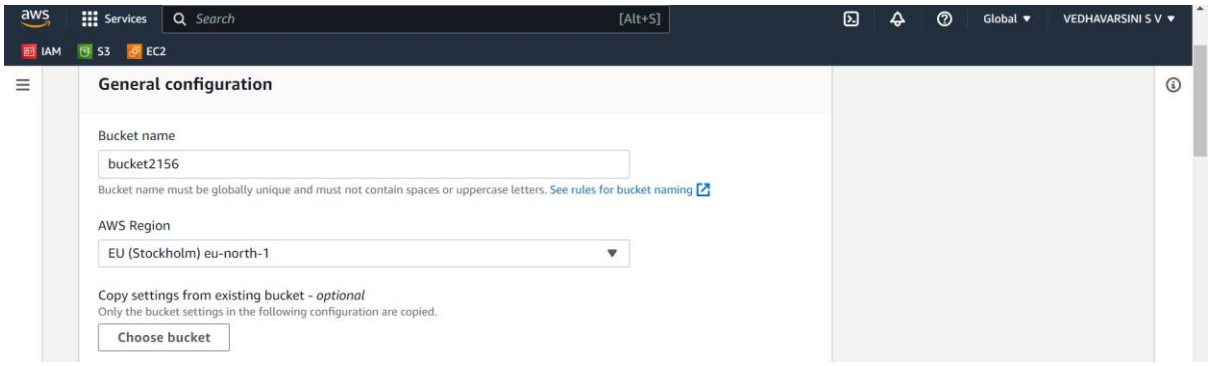
2.

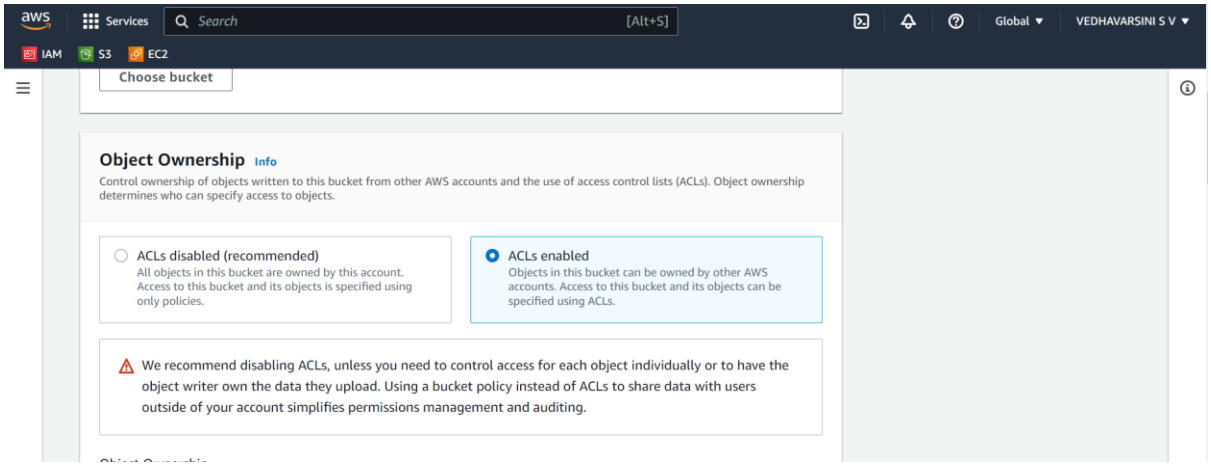

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
Network-L1-User1
Console password type
Custom password
Require password reset
No
Permissions 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

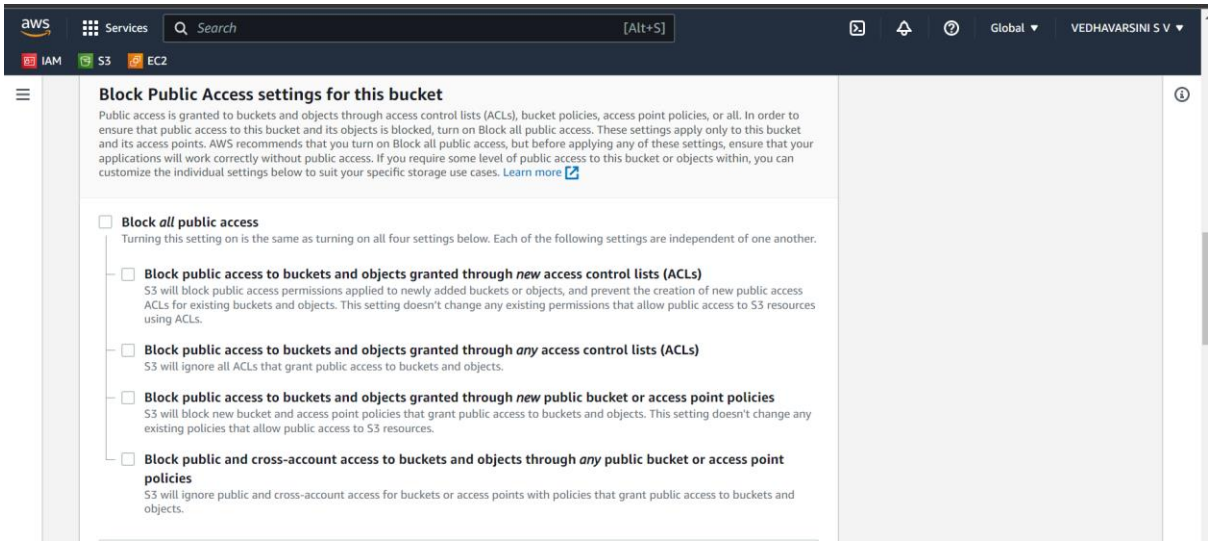

Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://331497285830.signin.aws.amazon.com/console
User name
Network-L1-User1
Console password
Show
Download .csv file
Return to users list

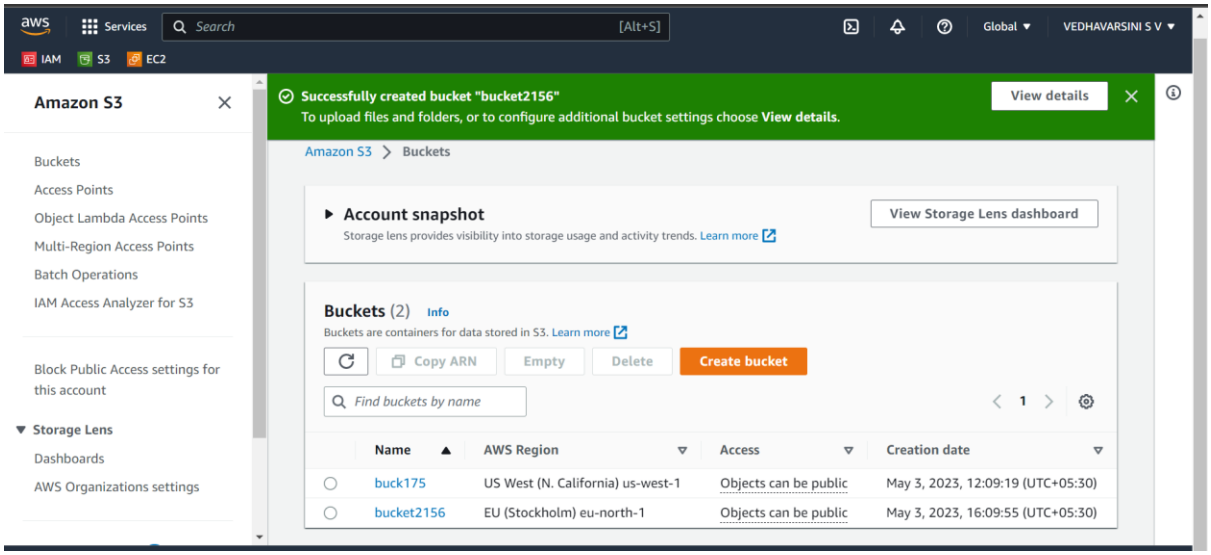

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
IAM > User groups > Network-L1-Team
Network-L1-Team
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.
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...

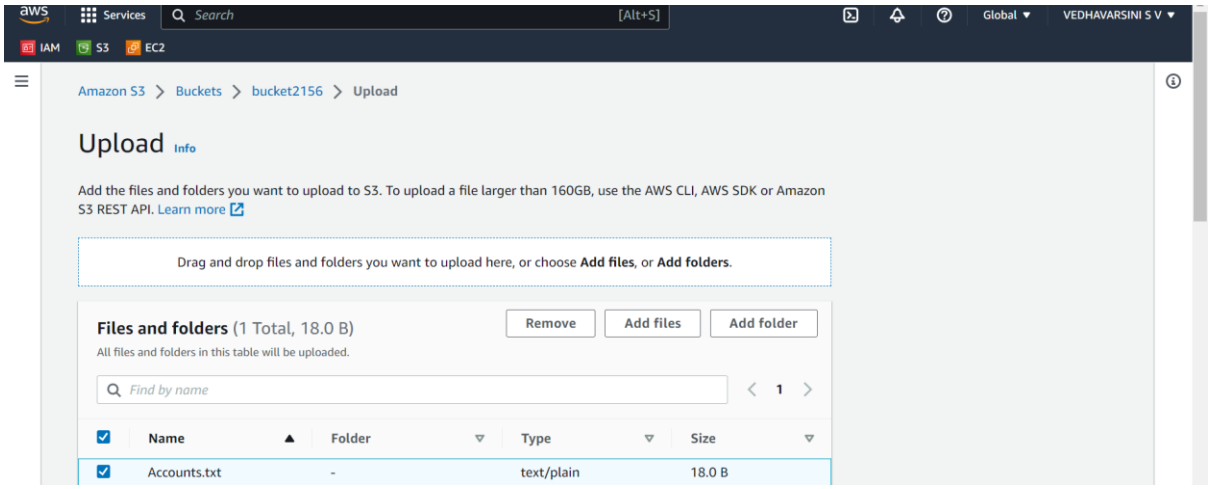
3.

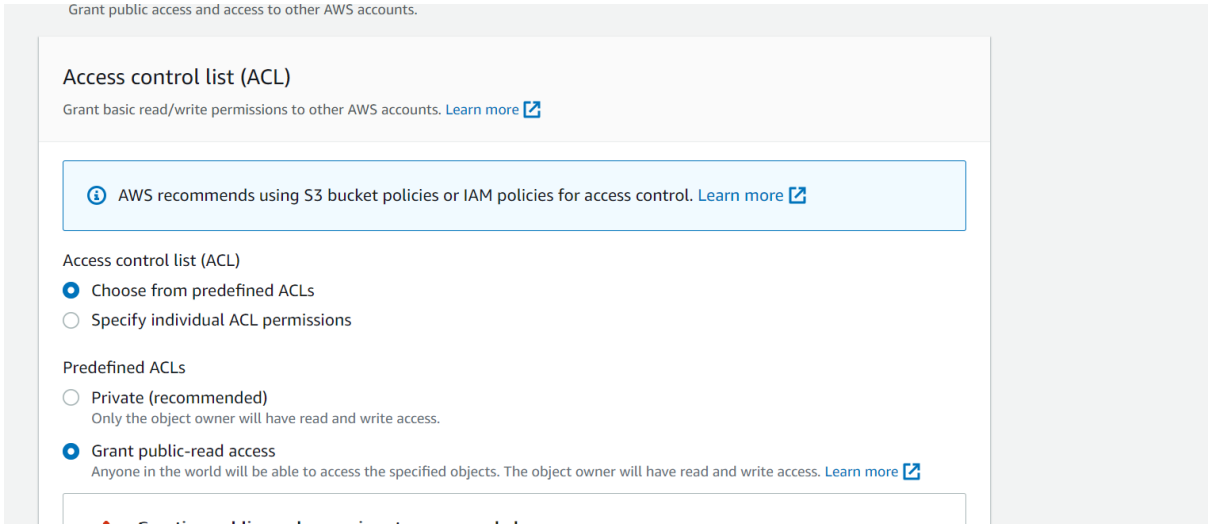

aws
Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
General configuration
Bucket name
bucket2156
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
EU (Stockholm) eu-north-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket

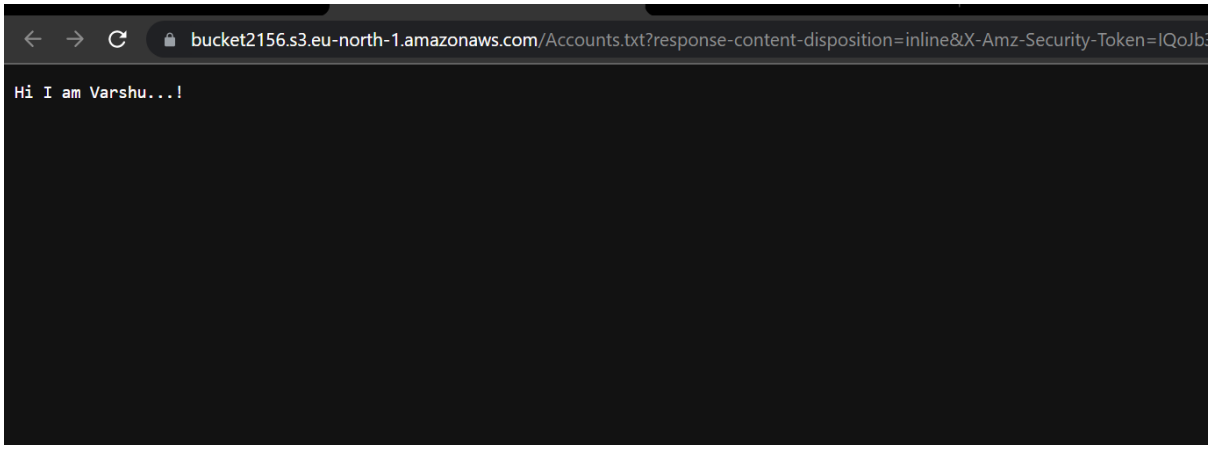

aws
Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
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.


aws
Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
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.


Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
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
Successfully created bucket "bucket2156"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (2) 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
buck175
US West (N. California) us-west-1
Objects can be public
May 3, 2023, 12:09:19 (UTC+05:30)
bucket2156
EU (Stockholm) eu-north-1
Objects can be public
May 3, 2023, 16:09:55 (UTC+05:30)


Services
Search
[Alt+S]
Global
VEDHAVARSINI S V
IAM
S3
EC2
Amazon S3 > Buckets > bucket2156 > 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, 18.0 B)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
Accounts.txt
-
text/plain
18.0 B


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


bucket2156.s3.eu-north-1.amazonaws.com/Accounts.txt?response-content-disposition=inline&X-Amz-Security-Token=IQoJb
Hi I am Varshu...!