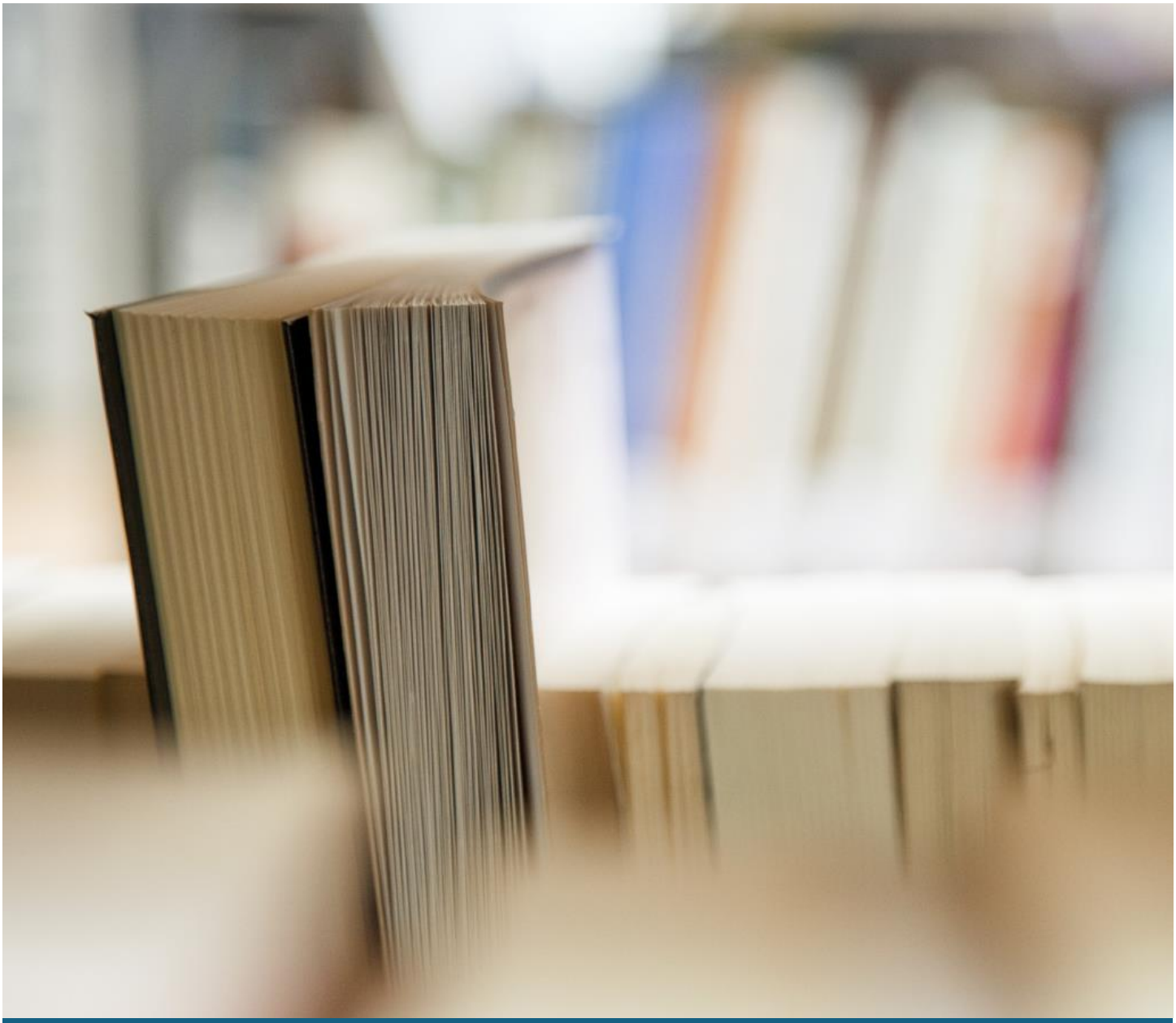


NEXTCLOUD DEPLOYMENT

CLOUD INFRASTRUCTURE PROJECT

Harshdeep Singh Virk

4/24/25

Group: 9

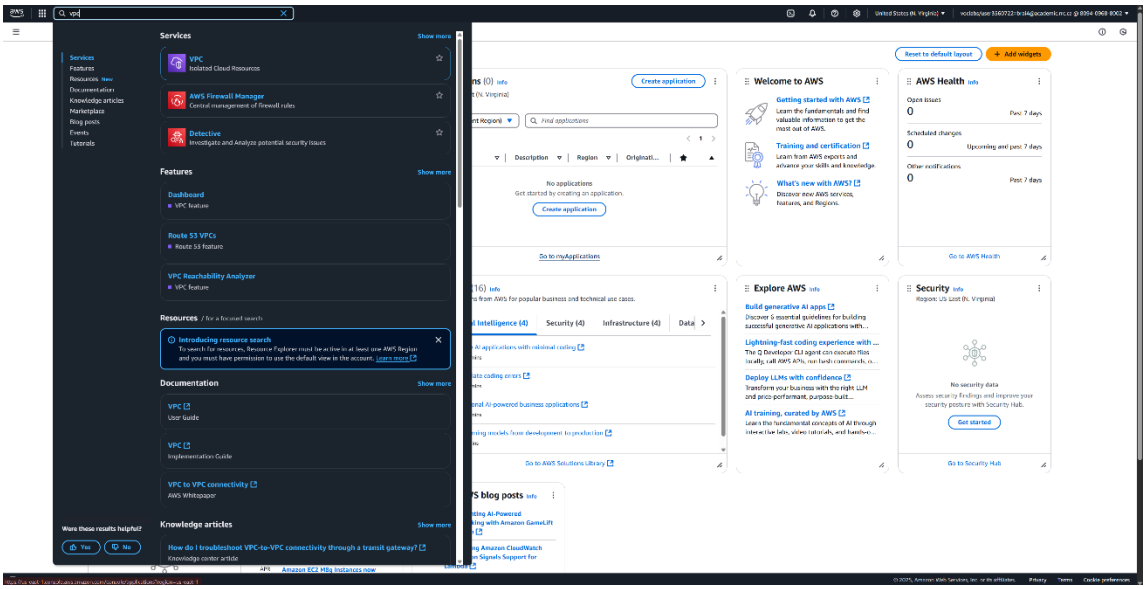
Cloud Infrastructure Project – Deploy Next cloud on AWS

Contents

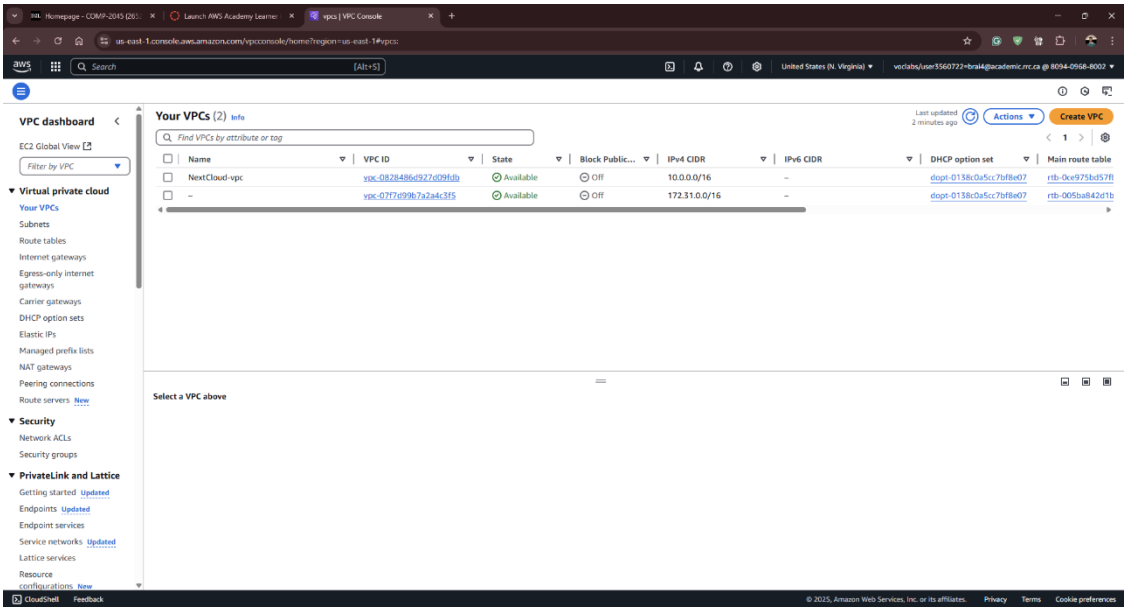
MILESTONE 1 – VPC & Security Groups

Creating a VPC:

1. In the search box to the right of **Services**, search for and choose **VPC** to open the VPC console.

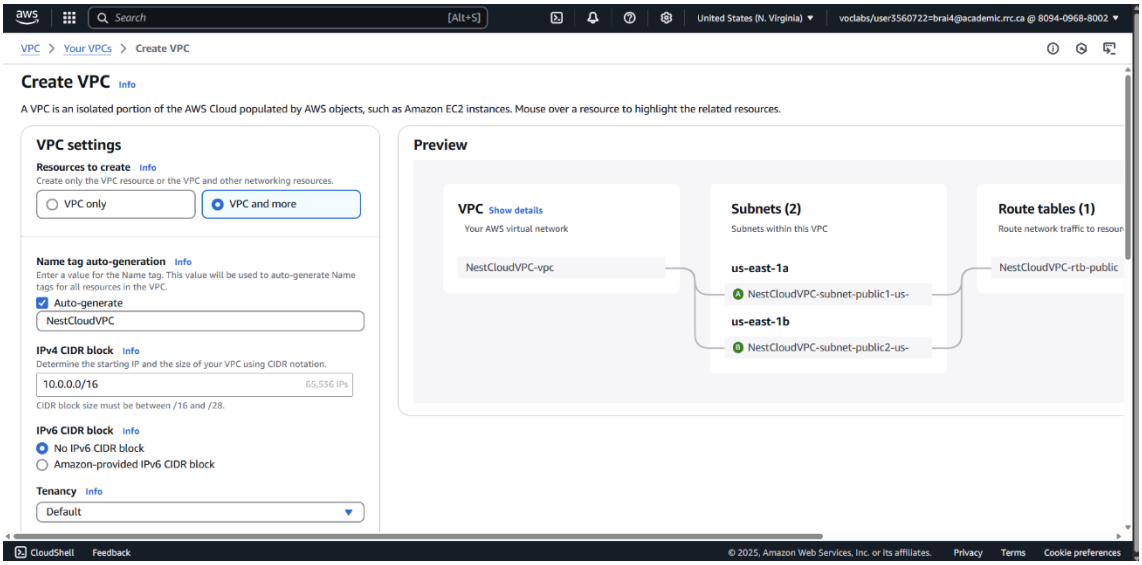


2. Choose the **VPC dashboard** link towards the console's top left.
3. Click on **Your VPC** to see all available VPCs.

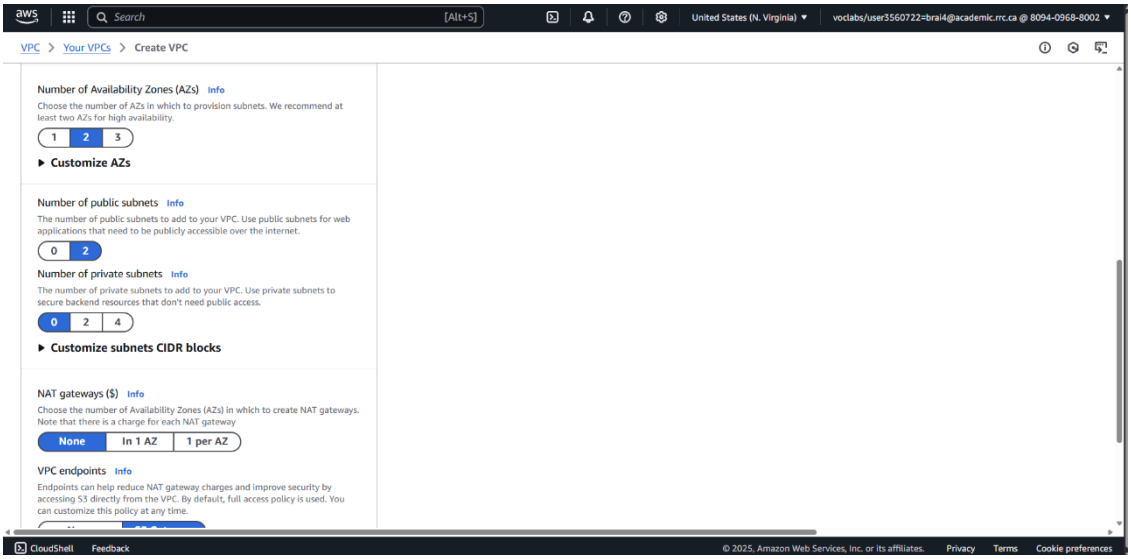


4. Next, choose **Create VPC**.

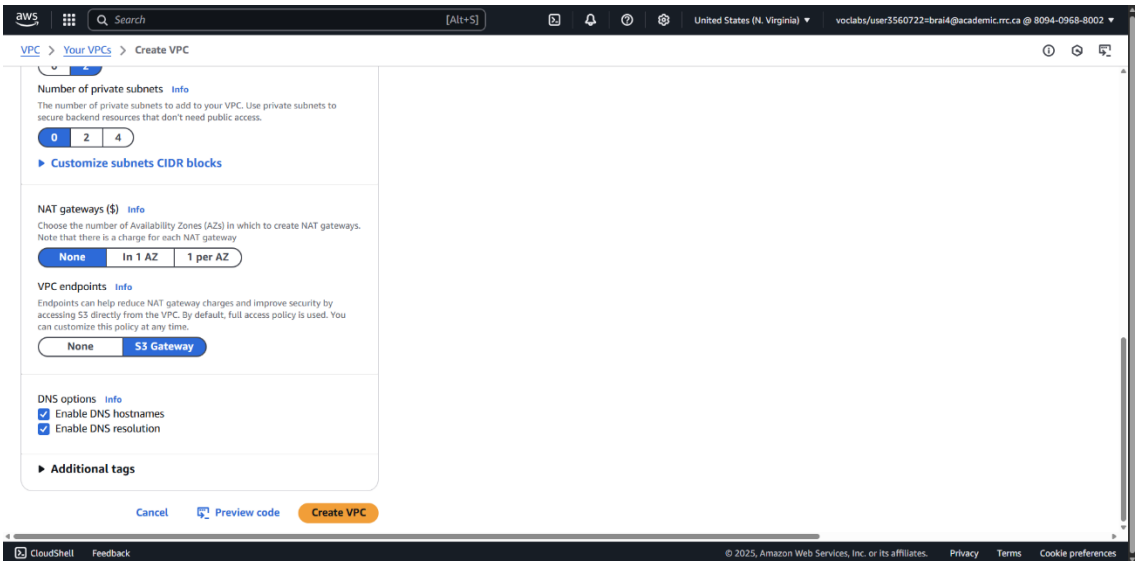
5. Configure the VPC details in the *VPC settings* panel on the left:
    a. Choose **VPC and more**.
    b. Under **Name tag auto-generation**, keep *Auto-generate* selected, however, change the value from project to `NextColudVPC`.
    c. Keep the **IPv4 CIDR block** set to 10.0.0.0/16



    d. Keep the **Number of Availability Zones**, as it is 2.
    e. For the **Number of *public* subnets**, change the **2** settings.
    f. For the **Number of *private* subnets**, change the **0** setting.
    g. Do not make any changes in the **Customize subnets CIDR blocks** section

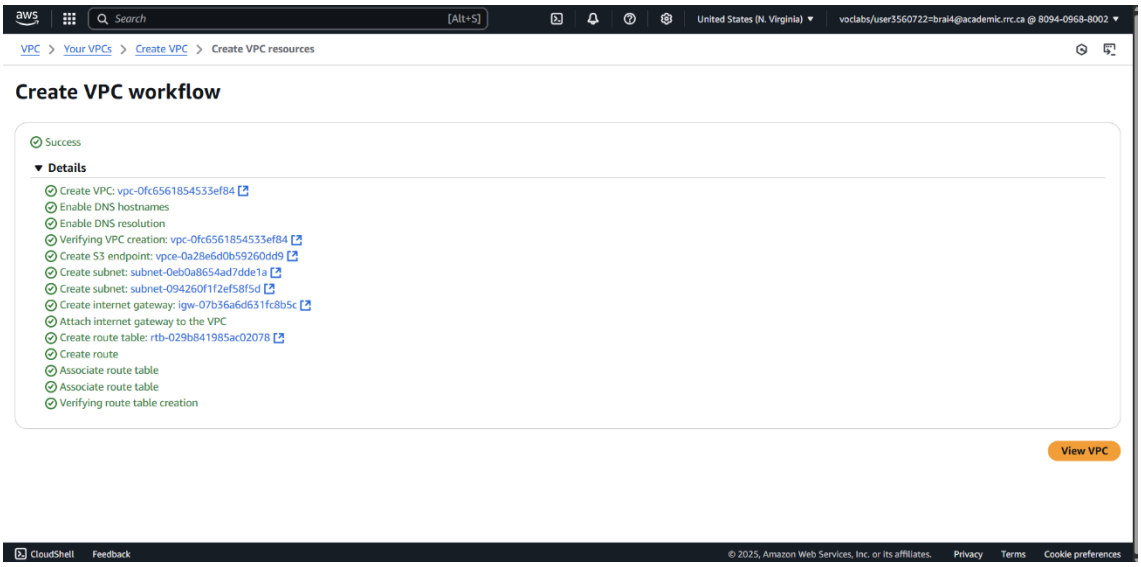


h. Set **NAT gateways** to **None**.
i. Set **VPC endpoints** to **S3 Gateway**.
j. Keep both **DNS hostnames** and **DNS resolution** *enabled*.

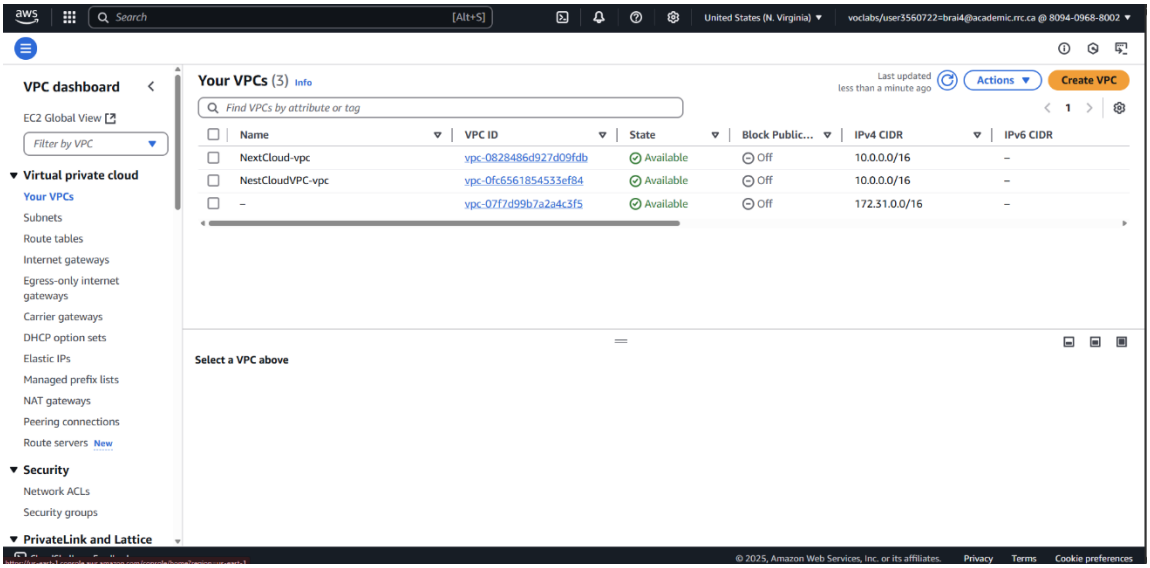


k. Next, choose **Create VPC**

6. In the *Preview* panel on the right, confirm the settings you have configured.
   a. Once it is complete, choose **View VPC**

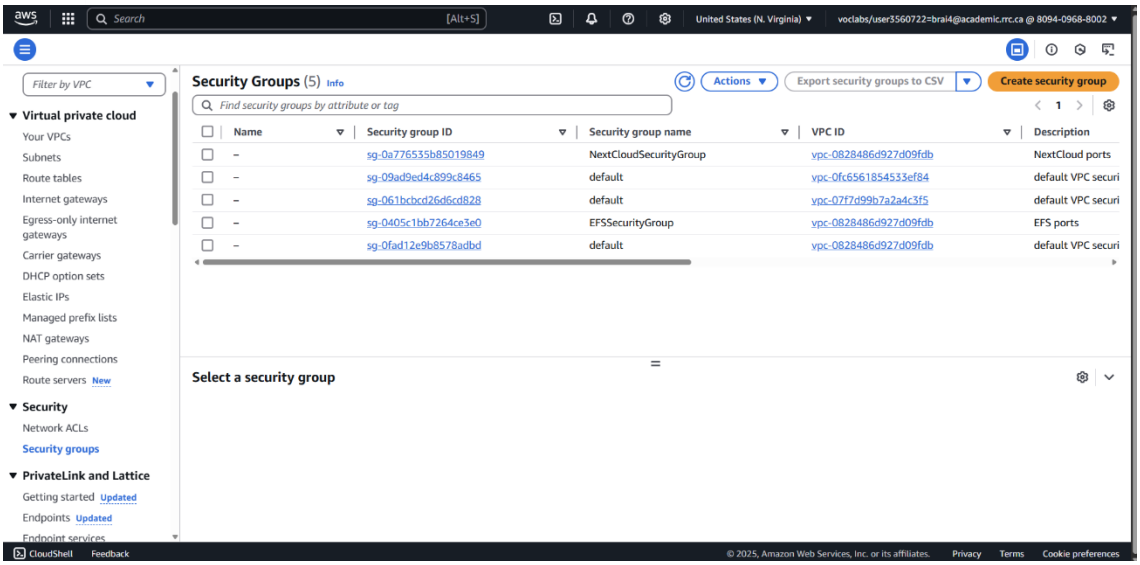


7. Your VPC is created successfully. You can confirm by clicking on Your VPC from the VPC Dashboard on the left panel.

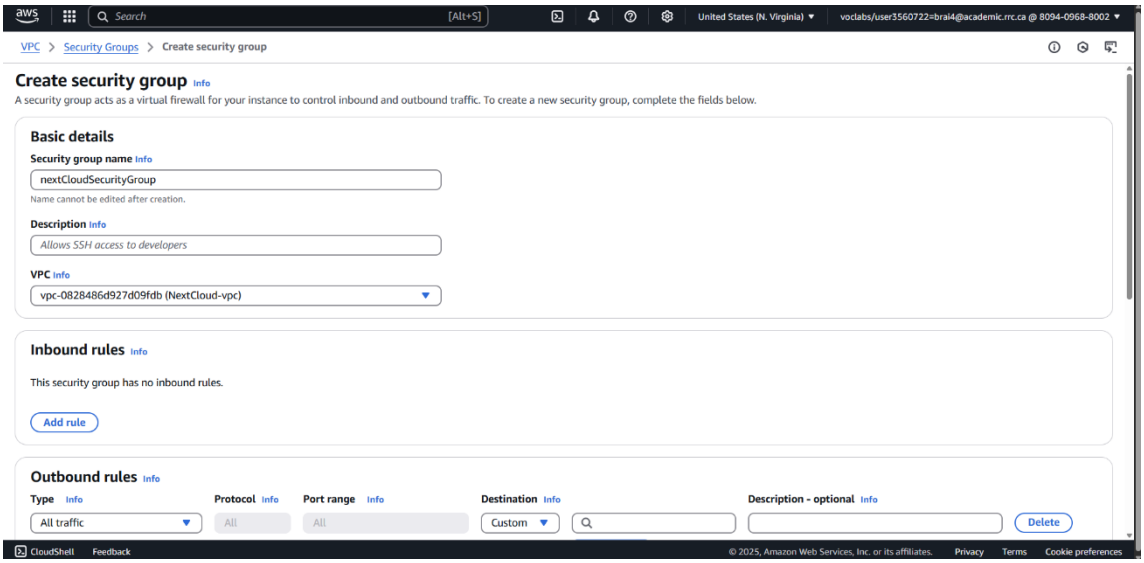


Creating a NextCloud Security Group:

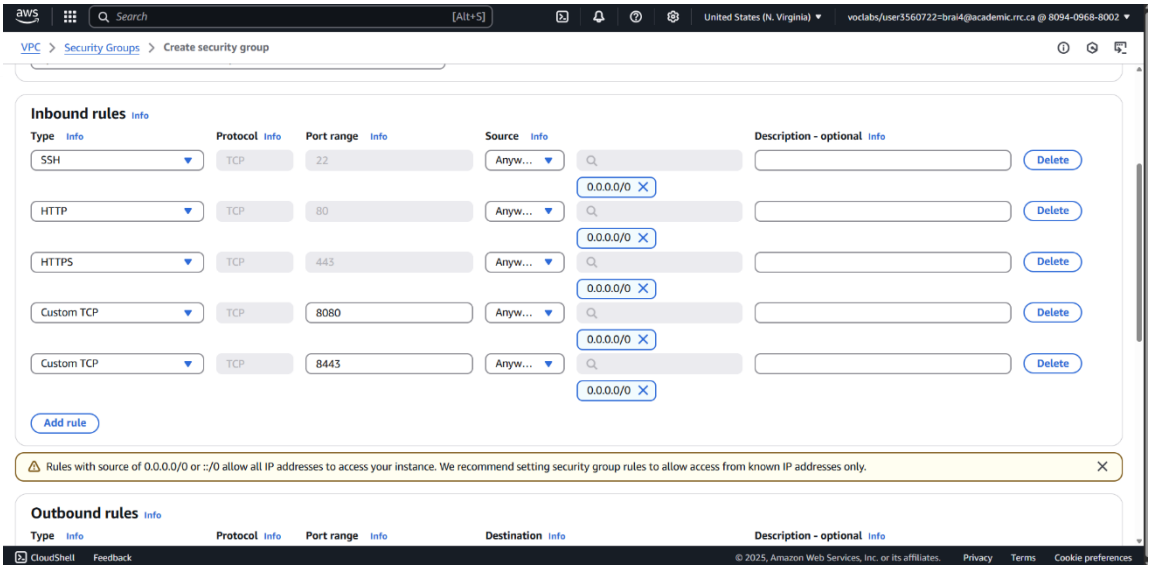
1. In the left navigation pane scroll down, and choose **Security groups**.
2. To create a new security group, click the **Create security group** button on the page's top.



3. In the Create security group page, Enter a name and description for the security group.
4. Select the appropriate VPC from the dropdown box. We need to select NextcloudVPC which was created earlier.



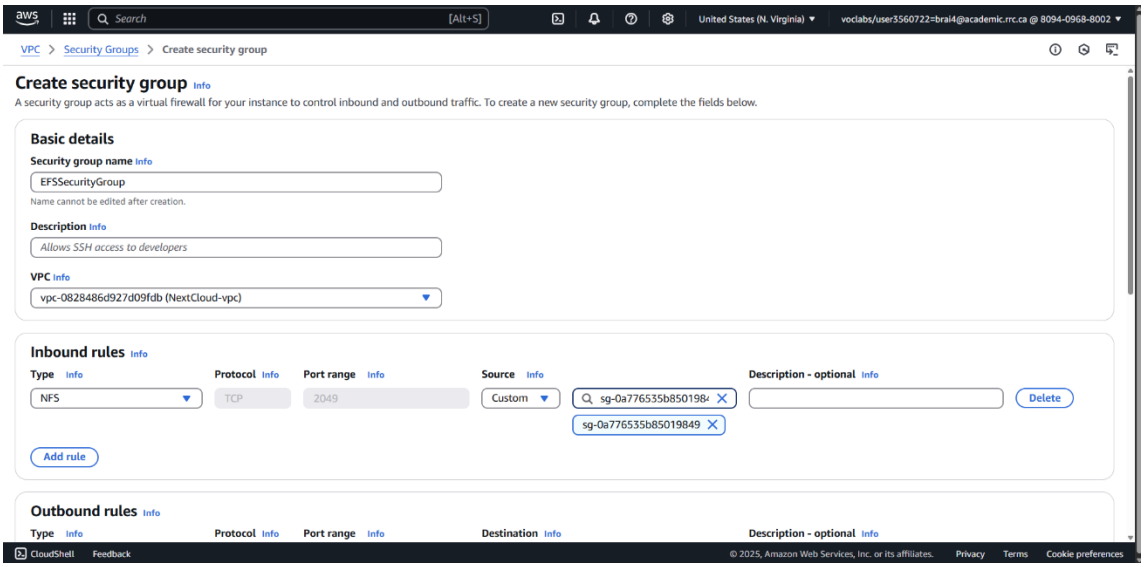
5. Add inbound rules for the following ports: SSH (22), HTTP (80), HTTPS(443), Custom TCP(8080), and Custom TCP (8443). Make sure you select the source as anywhere from IPV4 (0.0.0.0/0).



6. Keep “Outbound Rules” as default.
7. Scroll to the bottom of the page and choose **Create Security Group**

Creating an EFS Security Group:

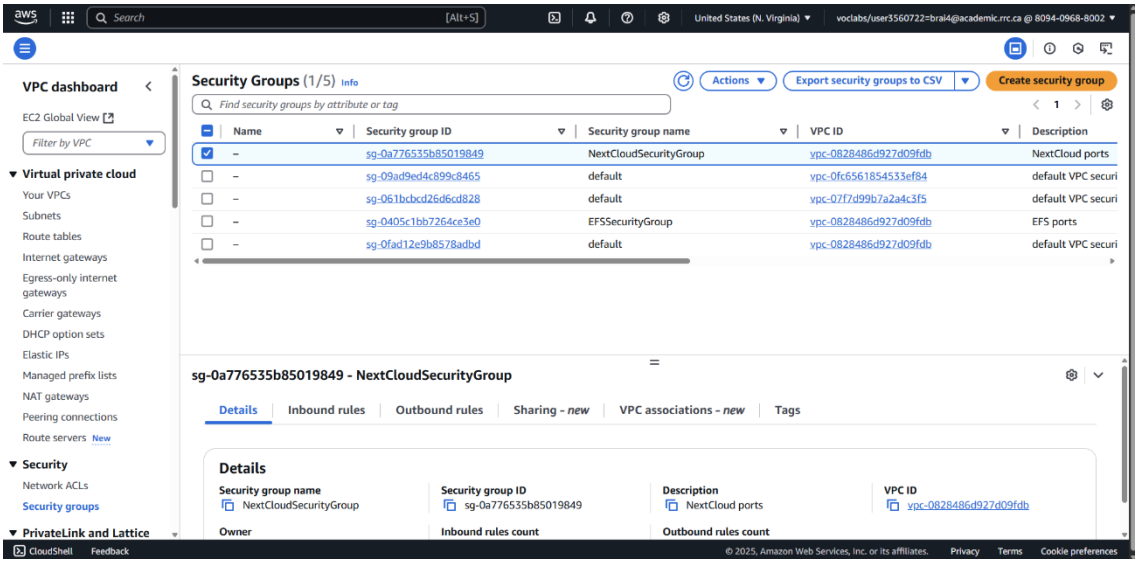
1. in the left navigation pane scroll down, and choose **Security groups**.
2. To create a new security group, click the **Create security group** button on the page's top.
3. In the Create security group page, Enter a name and description for the security group.
4. Select the appropriate VPC from the dropdown box. We need to select NextcloudVPC which was created earlier.
5. Add an inbound rule for NFS (2049). Select the source as custom and select NextClodSecurity Group from the Dropdown Box.



8. Keep **Outbound Rules** as default.
9. Scroll to the bottom of the page and choose **Create Security group**

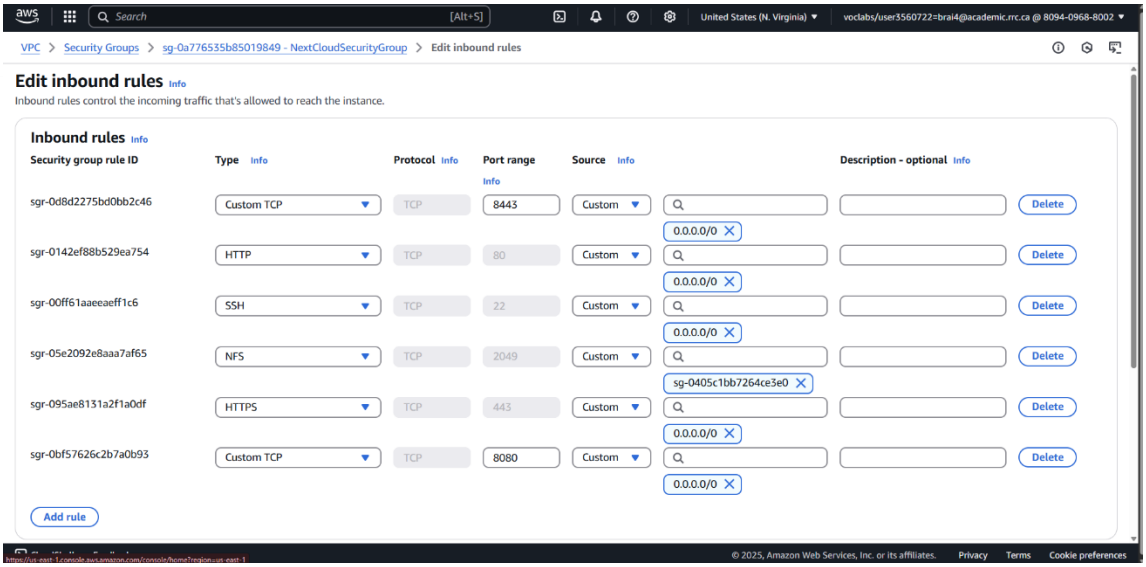
Customize a NextCloud Security Group:

1. Click on “NextClodSecurityGroup” From Security Groups
2. Click on **Edit inbound rule**



3. Click on the **Add rule** button.

4. Add an inbound rule for NFS (2049). Select the source as custom and select EFSSecurity Group from the Dropdown Box.

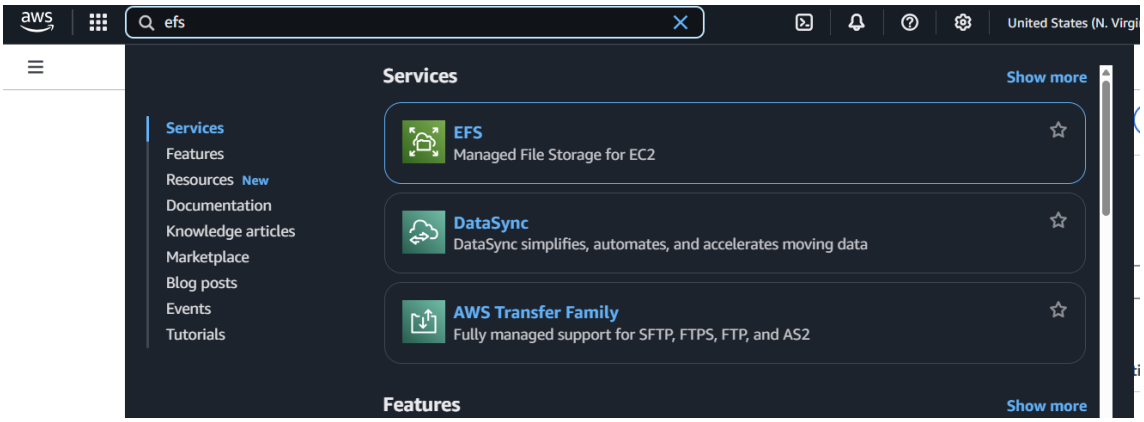


You successfully created security groups and VPC.

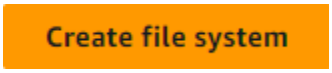
Milestone 2 – S3 & EFS storage – Demonstration

Create an elastic file system

1. Click on services and navigate the cursor to the search bar and look for EFS.

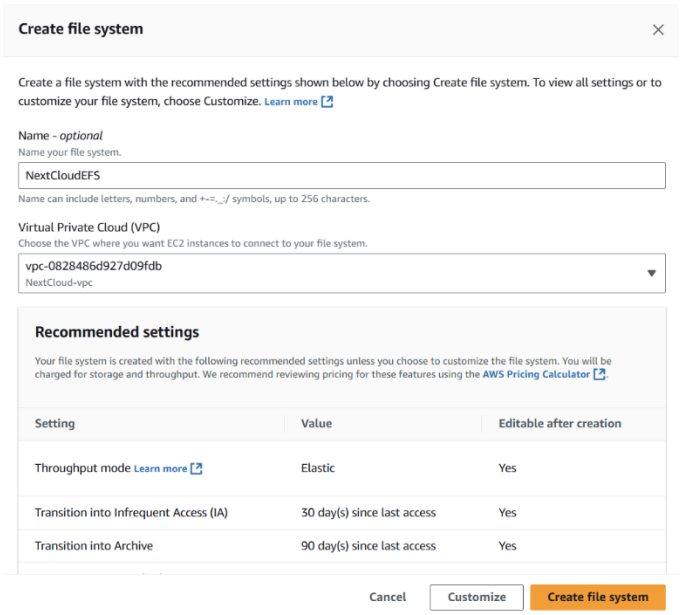


2. You will see the EFS dashboard and click on Create file system.

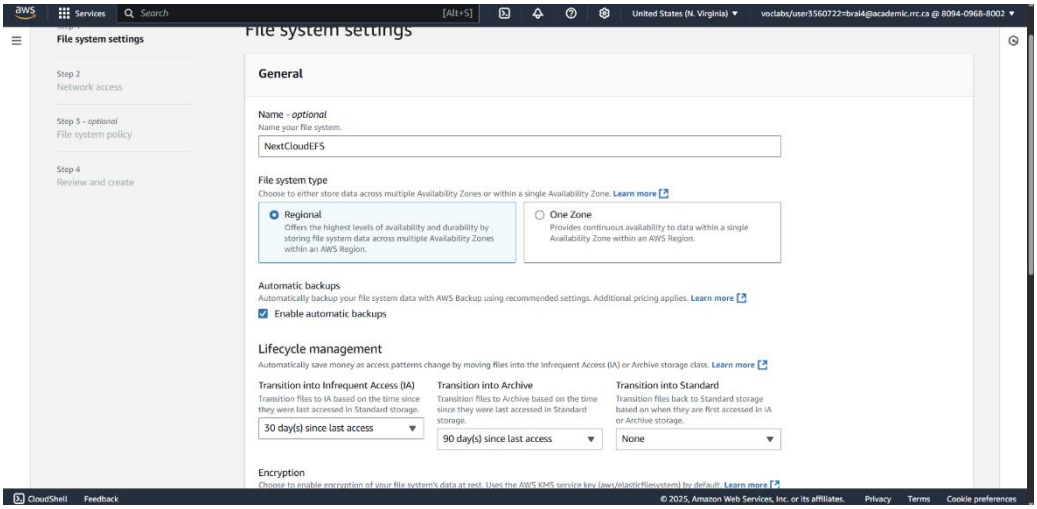


3. Name your file system according to your need and select your project VPC (Virtual Private Cloud).

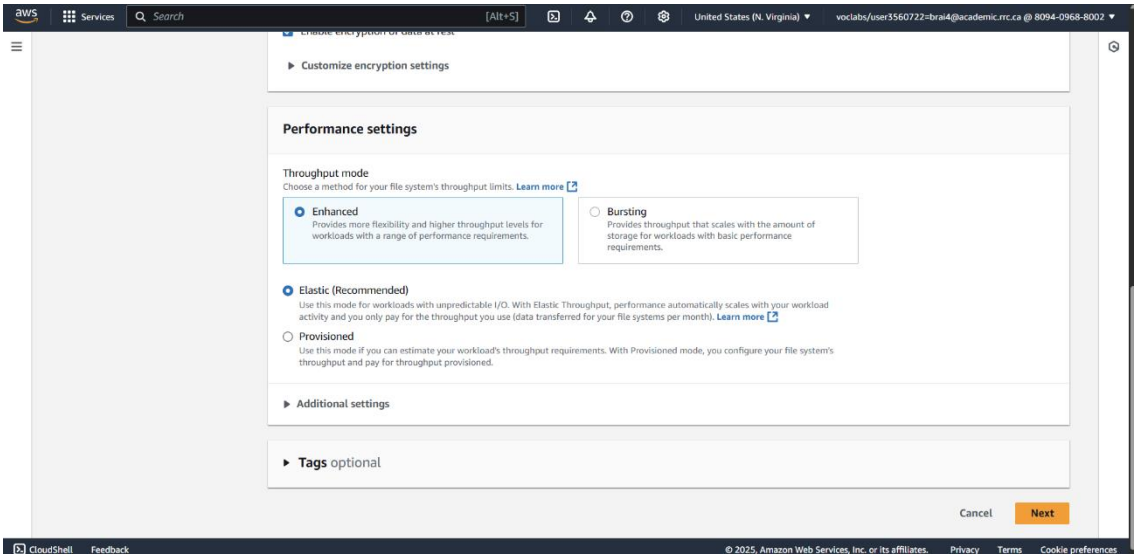
4. Click on Customize for more customization.



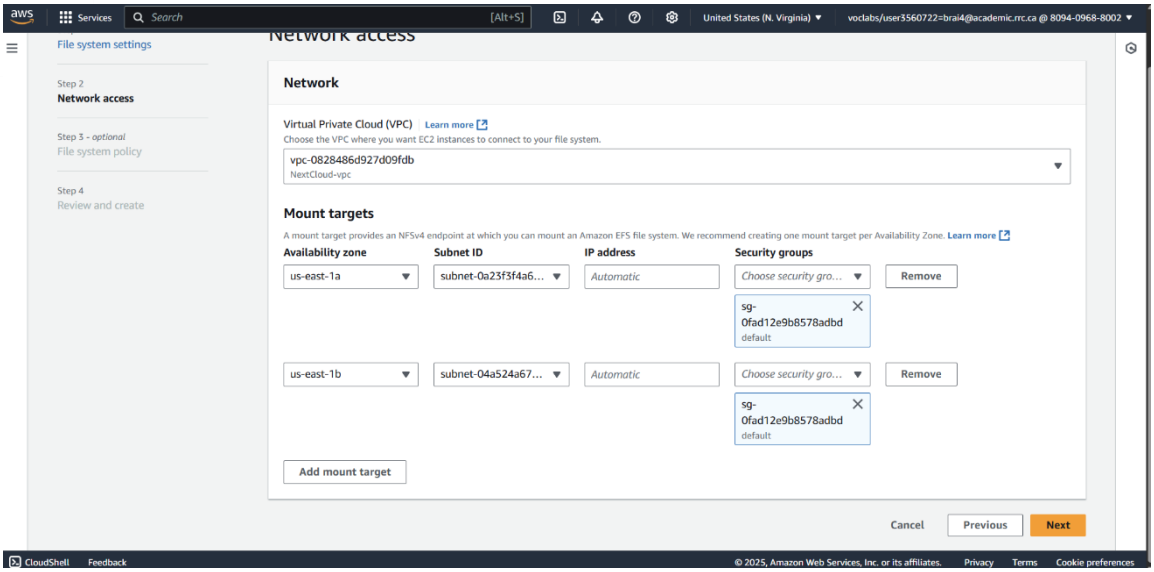
5. When you click Customize, you will see file system settings. In the General and lifecycle management tab, we don't need to make any changes, leave them default.



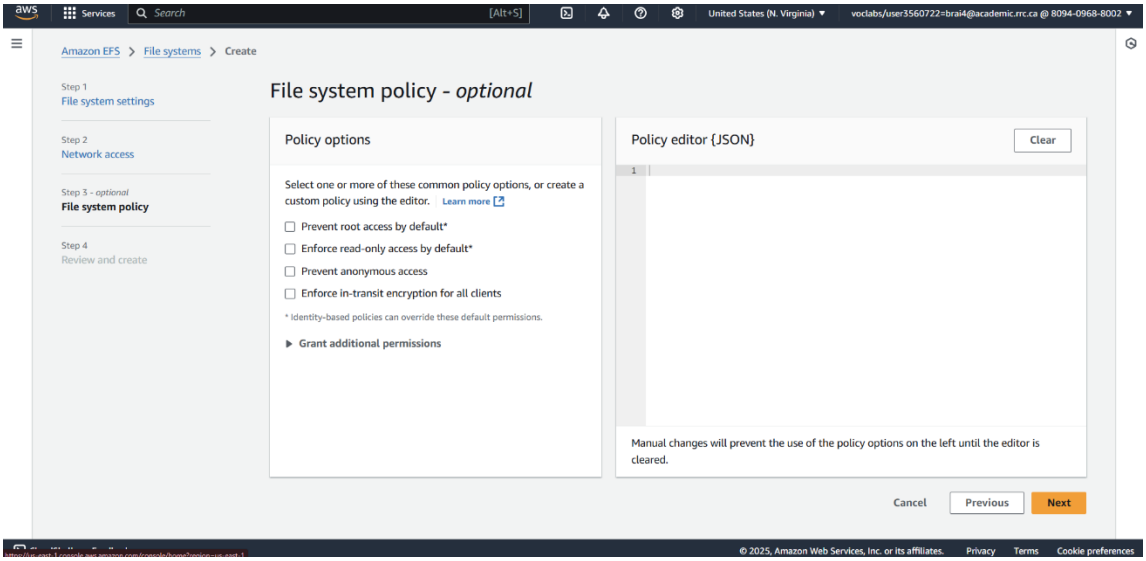
6. Click on Next from the right bottom of the page.



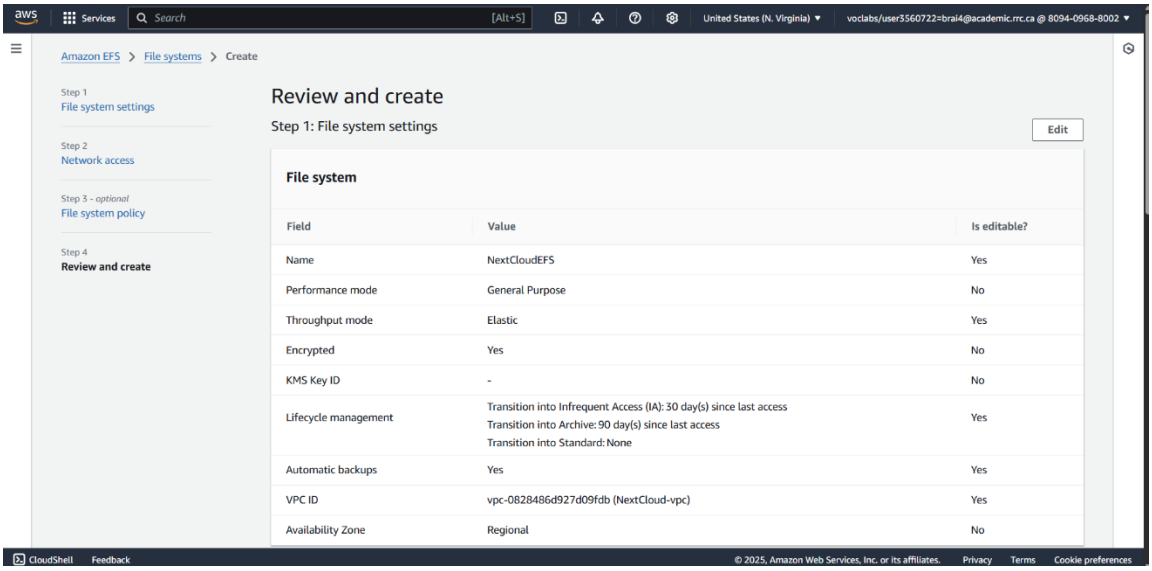
7. We will see the Network access page. From the network tab, We need to change the security group. For this project purpose, we will choose EFS SECURITY GROUP for both availability zones.

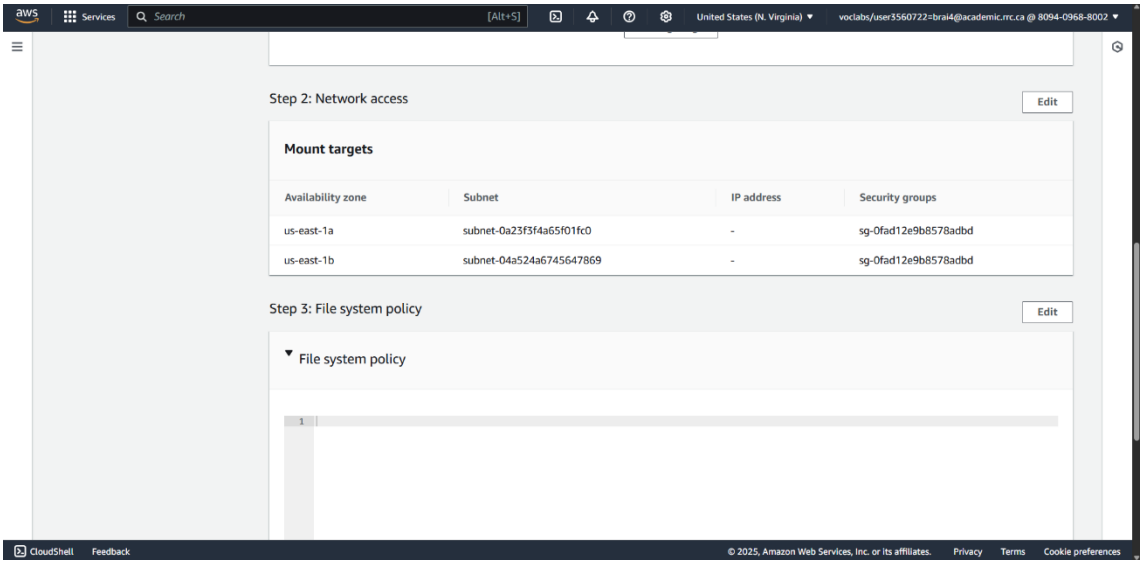


8. After making changes in both zones, click on NEXT from the bottom right corner.
9. We can leave the default setting for File system policy and Click on NEXT.



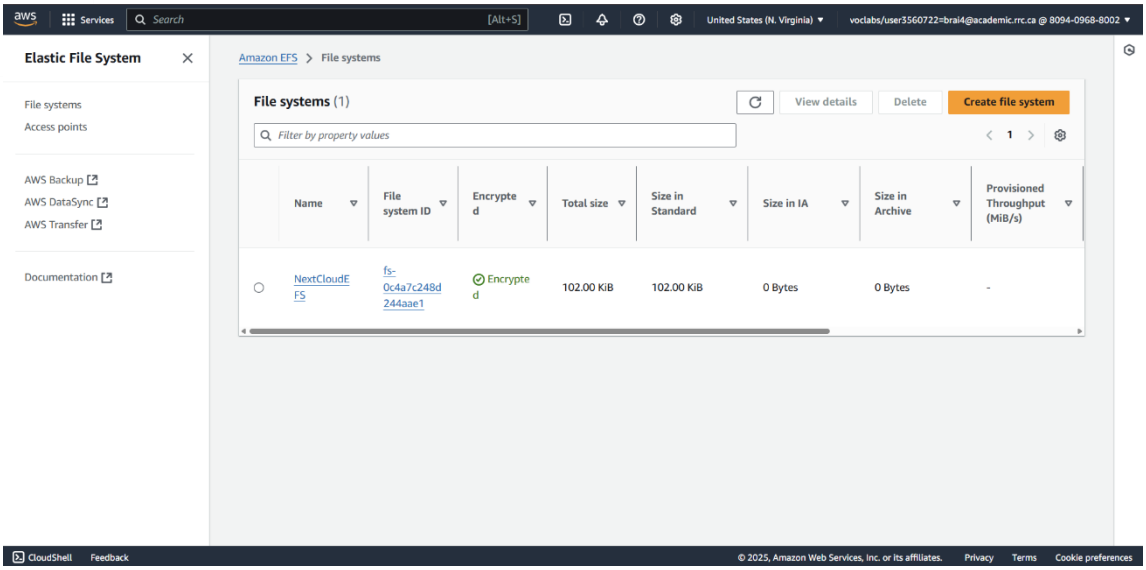
10. From the REVIEW page we will have a chance to make final changes before we create EFS Storage.





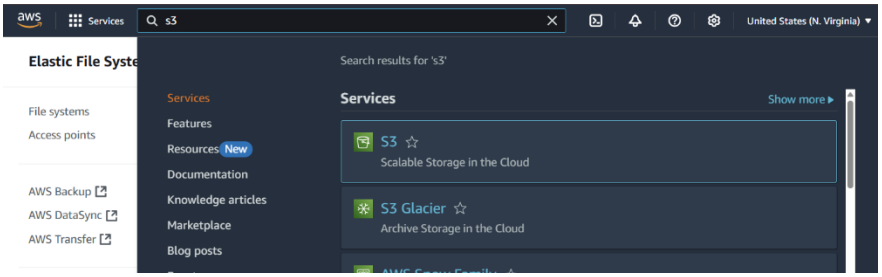
11. Once reviewed all the changes click on CREATE.

12. Once click on the CREATE tab, we will see the NEXTCLOUDEFS with the success message.

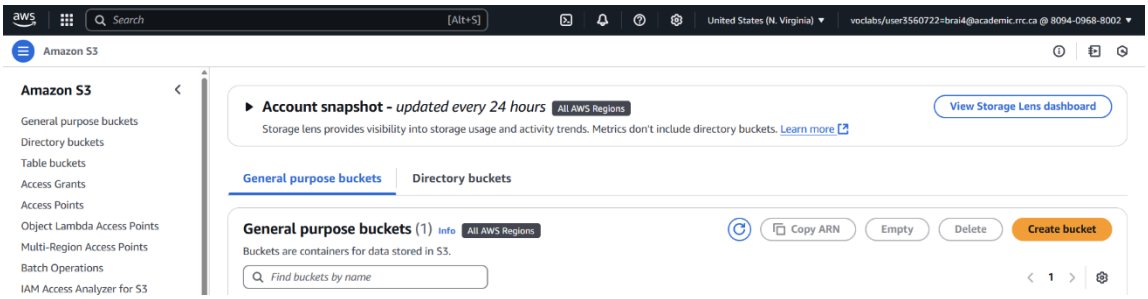


Create S3 Bucket

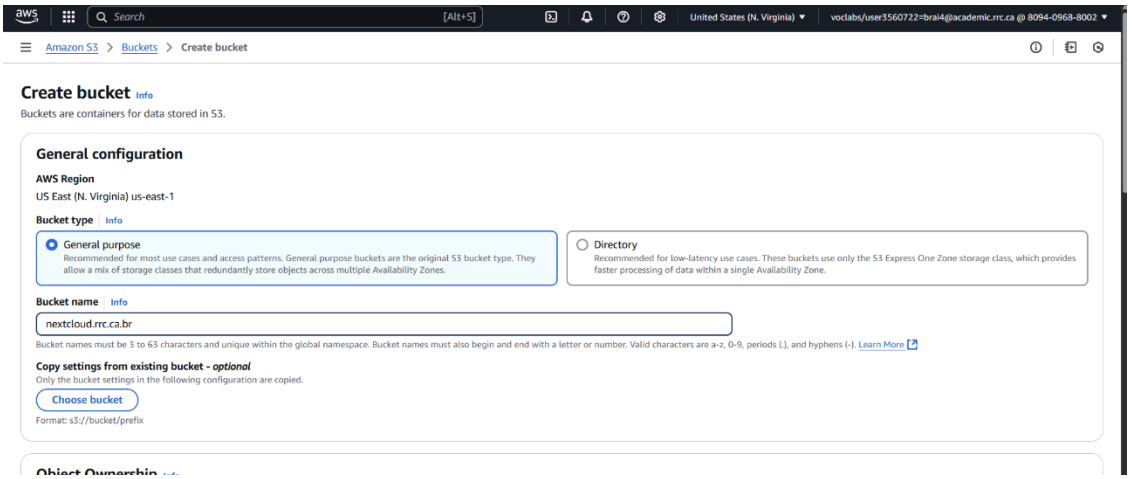
1. Click on services navigate the cursor to the search bar and look for S3.



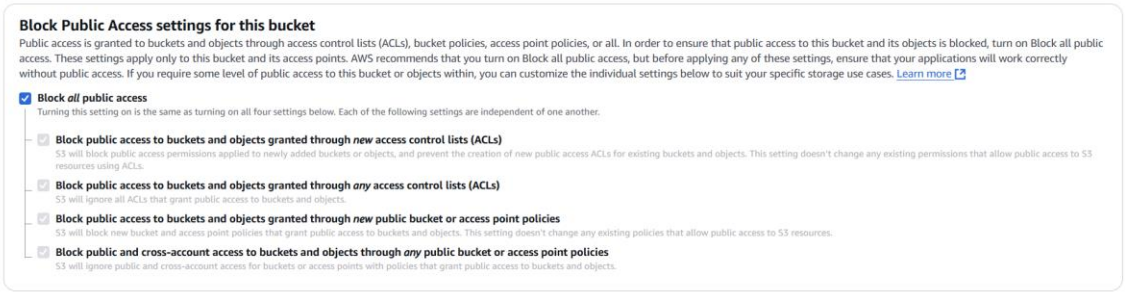
2. Click on the first link as shown in the picture. Navigate the cursor to CREATE BUCKET.



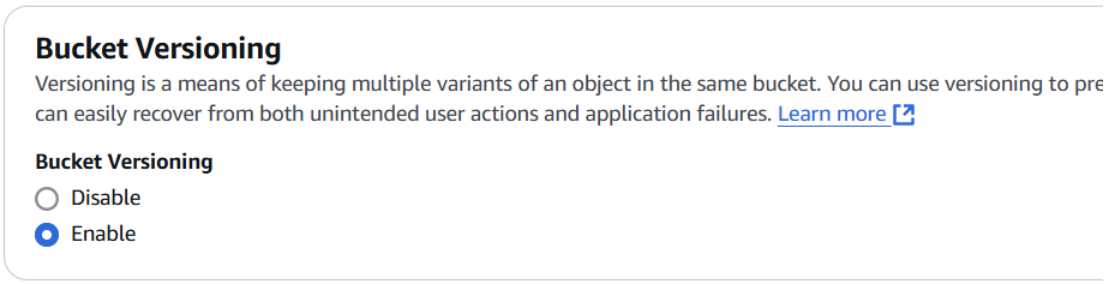
3. From the bucket name column, We will insert a globally unique name for the bucket.



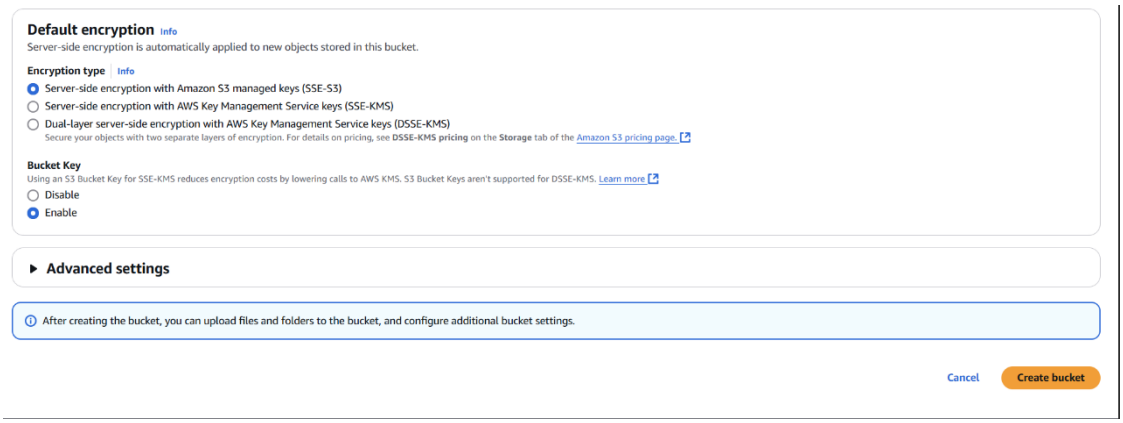
4. We will leave the other setting to default.



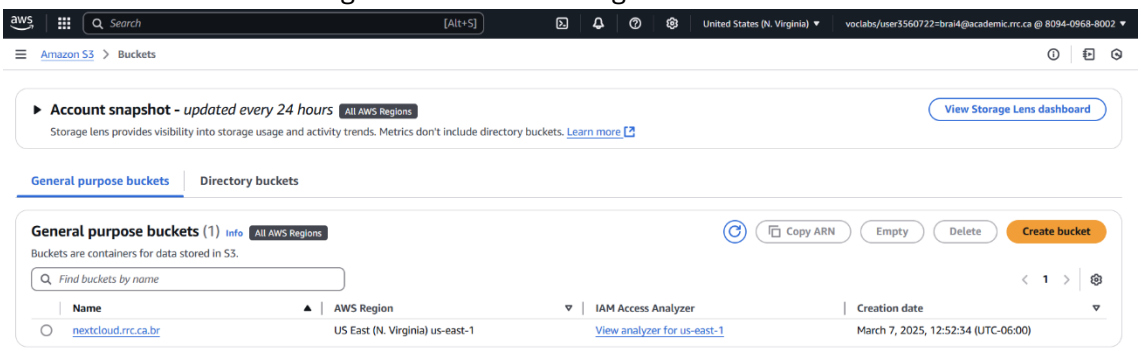
5. From the BUCKET VERSIONING tab, make it ENABLE.



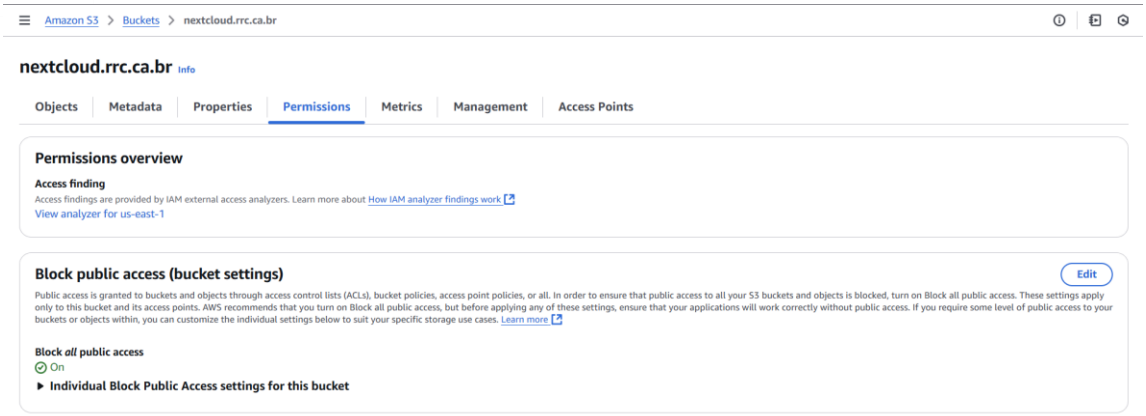
6. From the bottom of the page click on CREATE.



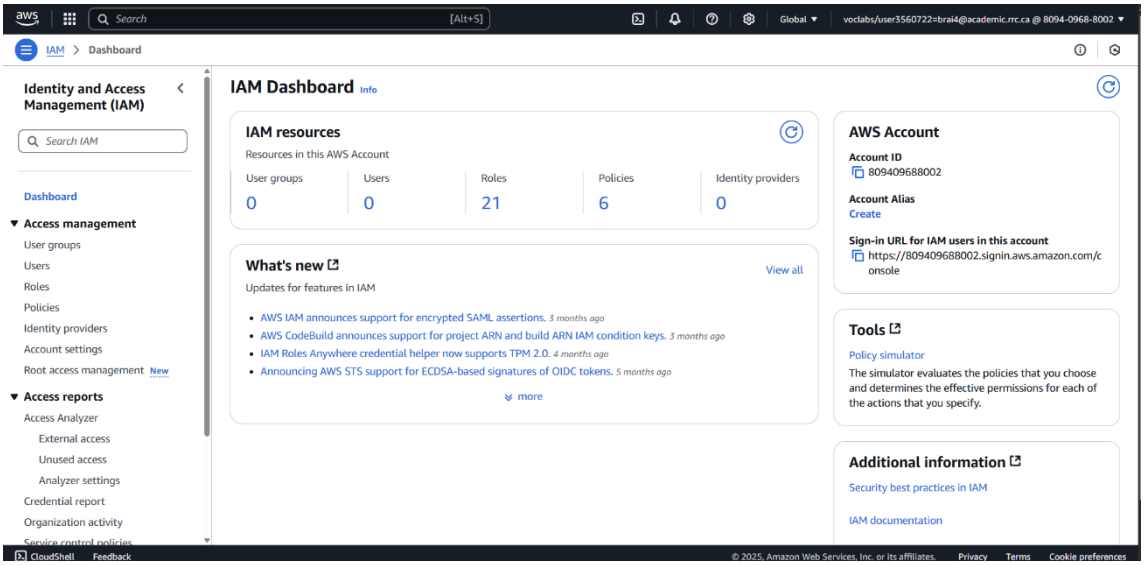
7. We will the bucket with a green success message.



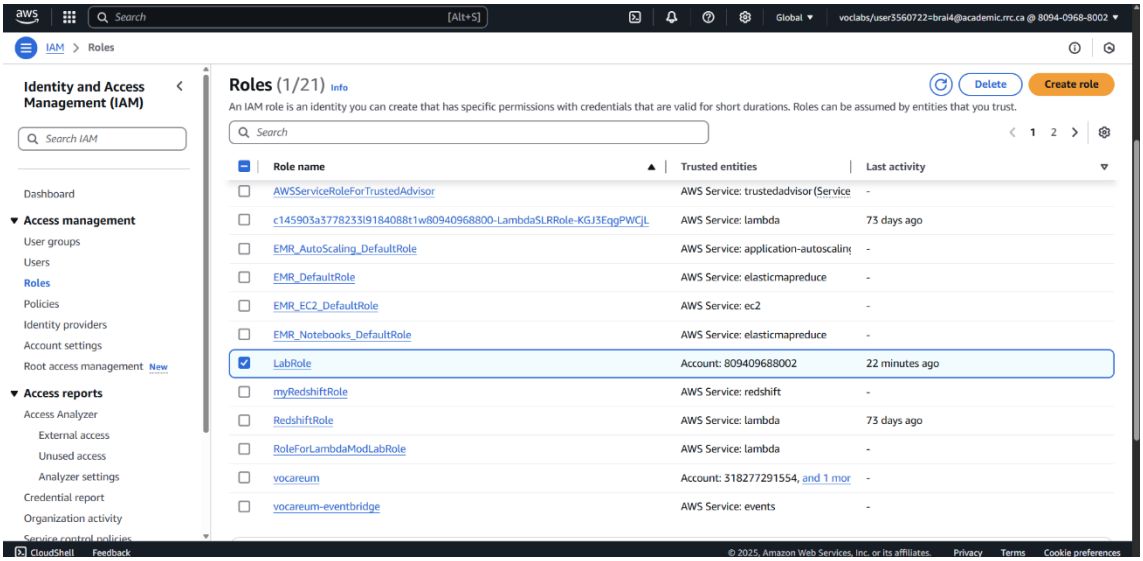
8. If you are able this, that means you have successfully made a bucket. From General Purpose Buckets, Click on the bucket name.
9. You will be able to access the options as shown in the picture below, Click on the Permissions Tab from the options.



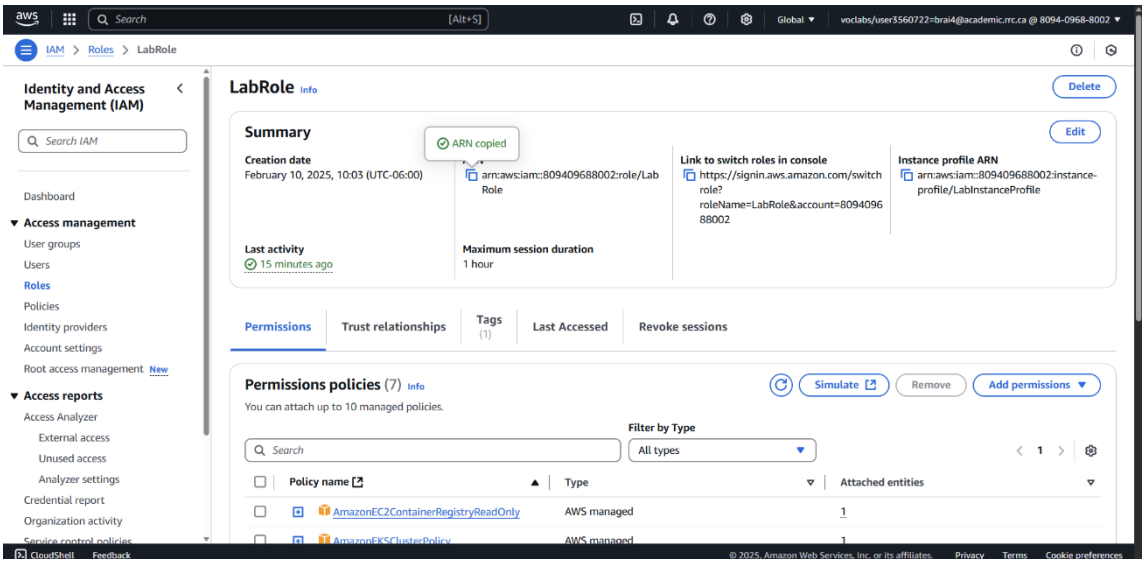
10. Verify that block all public access is ON.
11. From the same page, click on the EDIT option from the BUCKET POLICY tab.
12. Click on the SERVICE option from the left side of the screen and search IAM, open a new Brower page.
13. After viewing the IAM page click on ROLES Option from the left side of the screen in ACCESS MANAGEMENT.



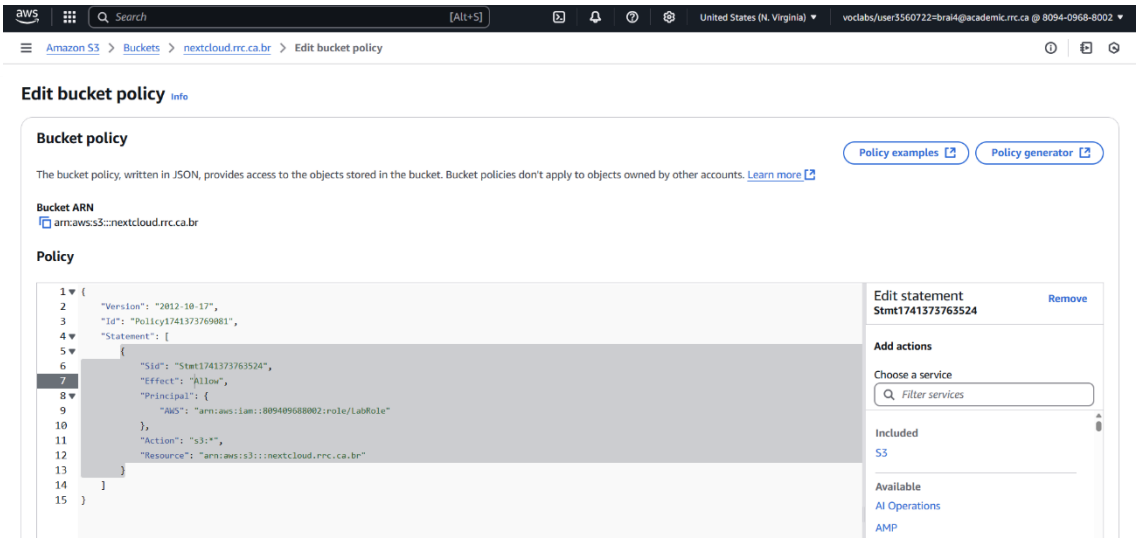
14. Once click on the ROLES Option, you will be able to see the page shown below. SELECT LABROLE.



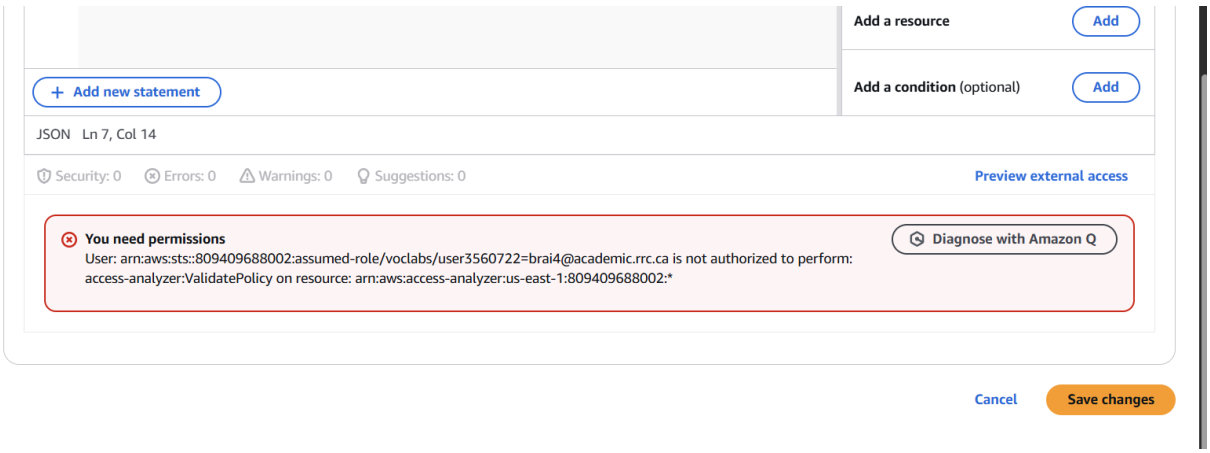
15. In the lab role page copy the ARN.



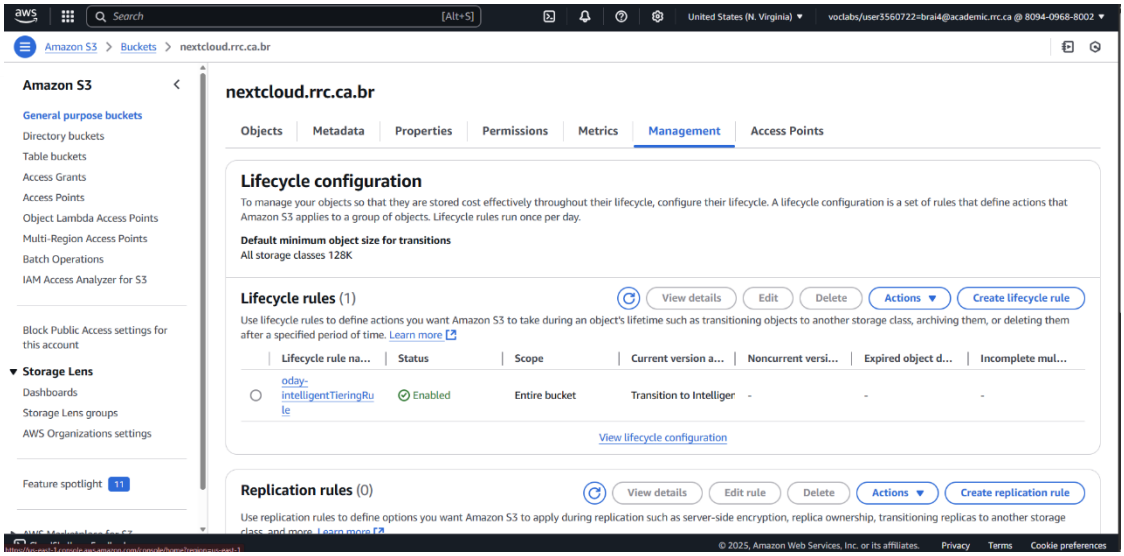
16. Now we need to go back to the S3 page. Click on Policy Generator from the right side of the page.



17. In AWS policy generator. Choose the S3 BUCKET POLICY from the type of the policies.
18. In the Principal column paste the ARN from the IAM management console.
19. For ACTIONS, select all actions.
20. In Amazon resource name (ARN), paste ARN from S3 bucket policy tab.
21. Click on ADD STATEMENT.
22. From the bottom of the page you will see a button named Generate Policy. Click on it.
23. Copy the policy JSON Document.
24. Go back to the edit bucket policy and paste the JSON document.
25. Click on the save changes from the right side of the page.



26. Navigate to the S3 dashboard, select buckets, and select your bucket.
27. Click the Management tab, then click Create lifecycle run.

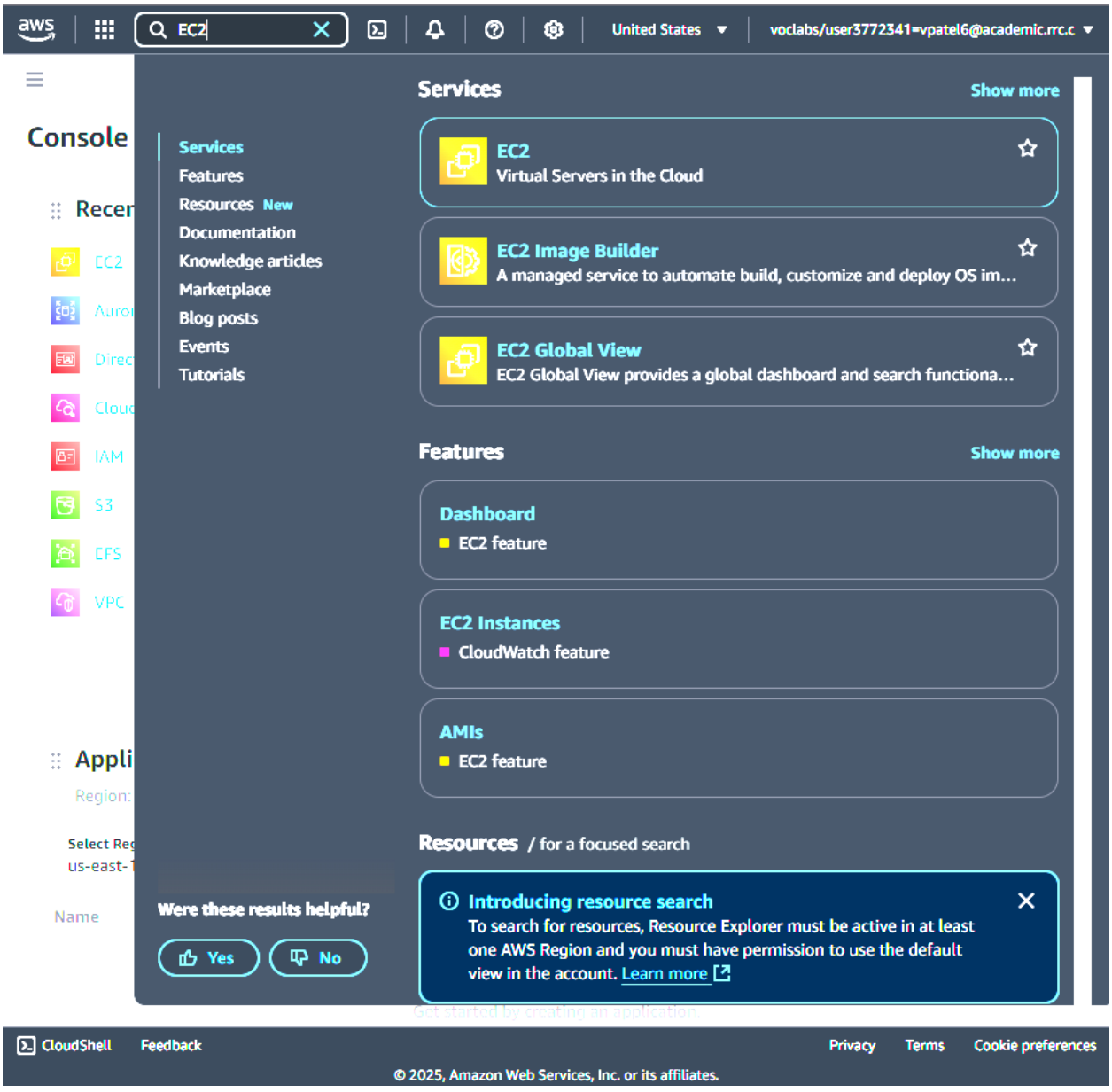


28. Change the name of the lifecycle rule from the name option.
29. Click on the acknowledgment option from the box.
30. Under lifecycle rule actions, check the Transition current versions of objects between storage classes
31. Select Intelligent-Tiering and enter 0 days in the transition fields.
32. Click Create rule

MILESTONE 3 – EC2 Instances & Elastic IP

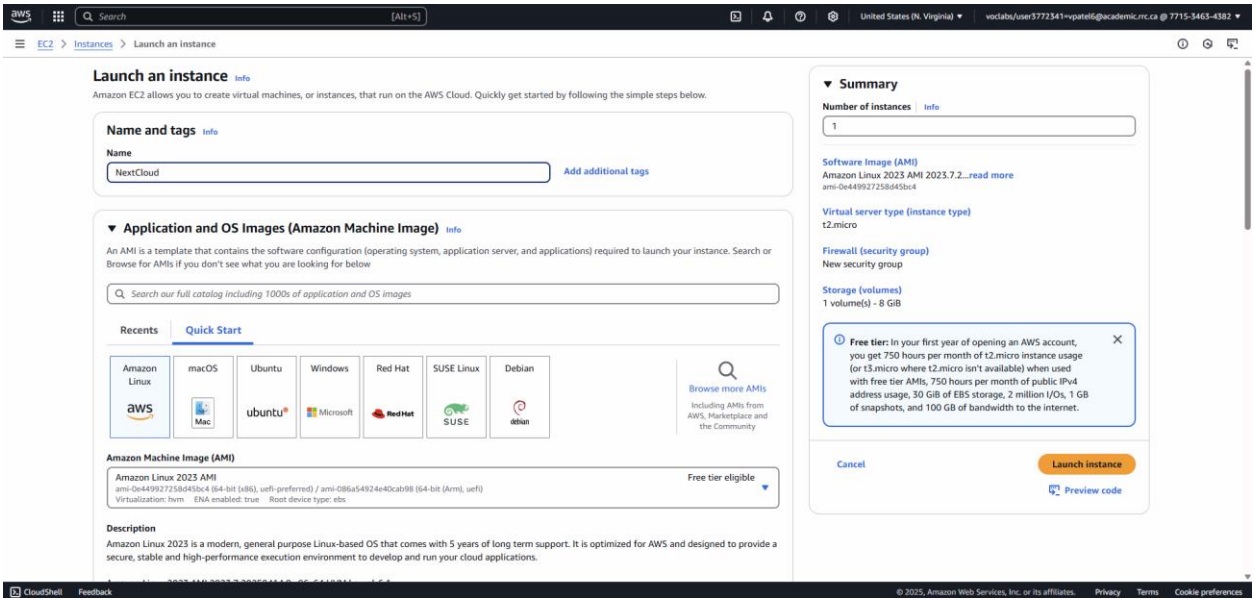
Creating EC2 Instance:

1. In the **AWS Management Console** choose **Services**, choose **Compute** and then choose **EC2**.

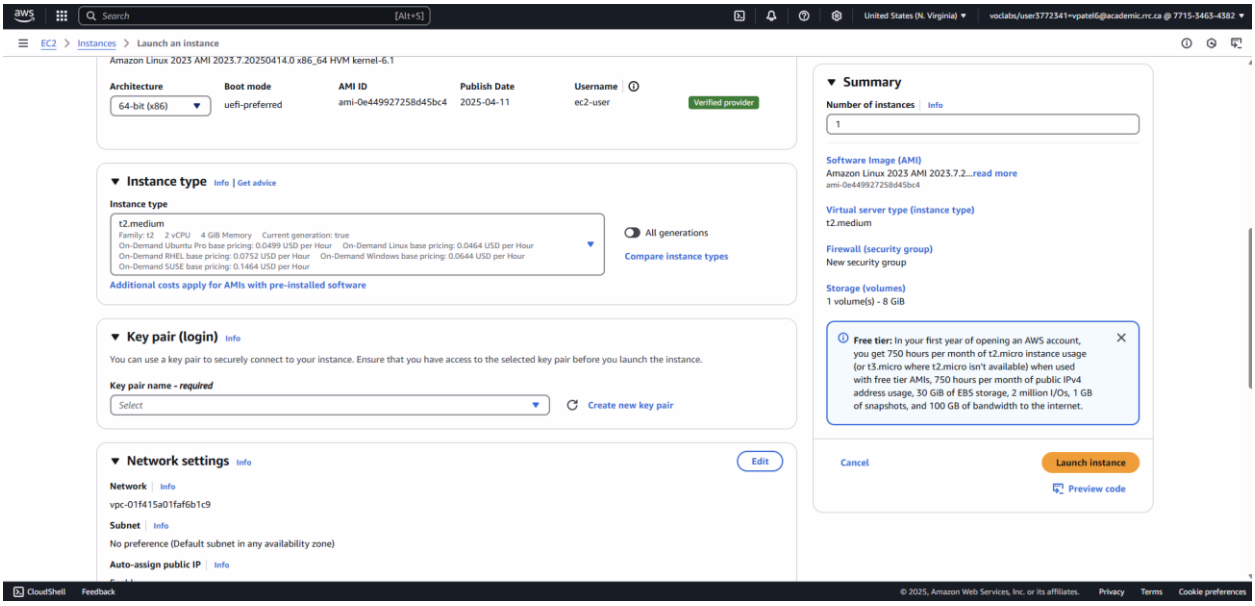


2. Choose the **instances** menu and select **Launch instance**.

3. Give the instance the name NextCloud.
4. In the list of available *Quick Start* AMIs, choose **Ubuntu** AMI.
5. Also keep the default **Ubuntu server 24.04 lTS AMI** selected

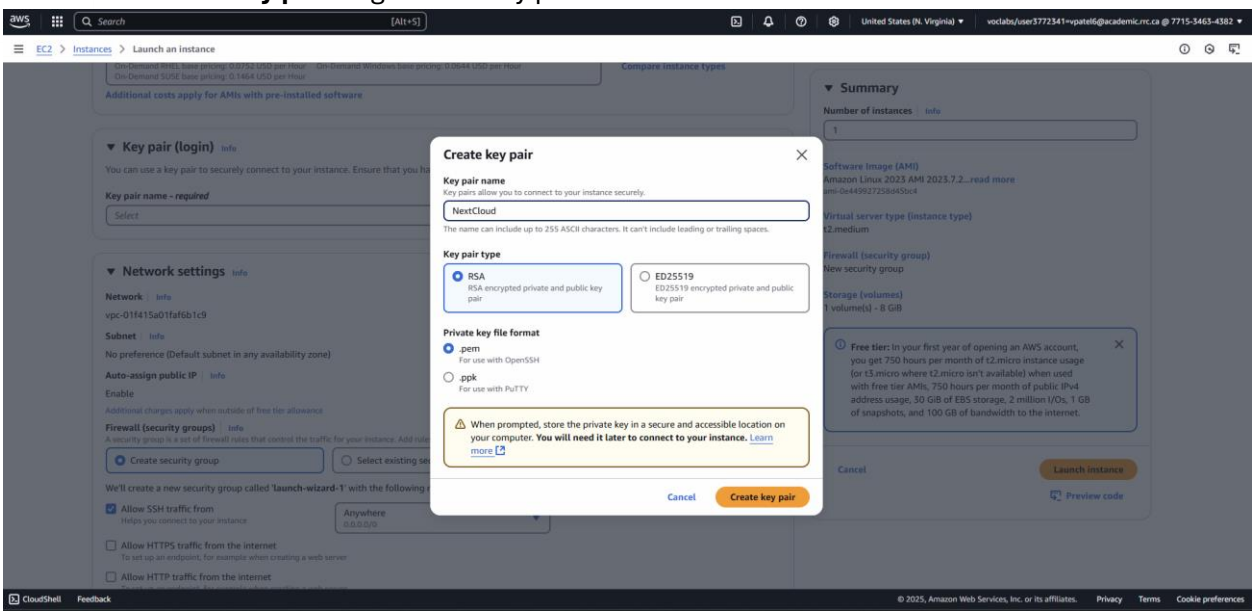


6. In the *Instance type* panel, choose the **t2.medium**.
7. For **Key pair name - *required***, choose **to create new key pair.**

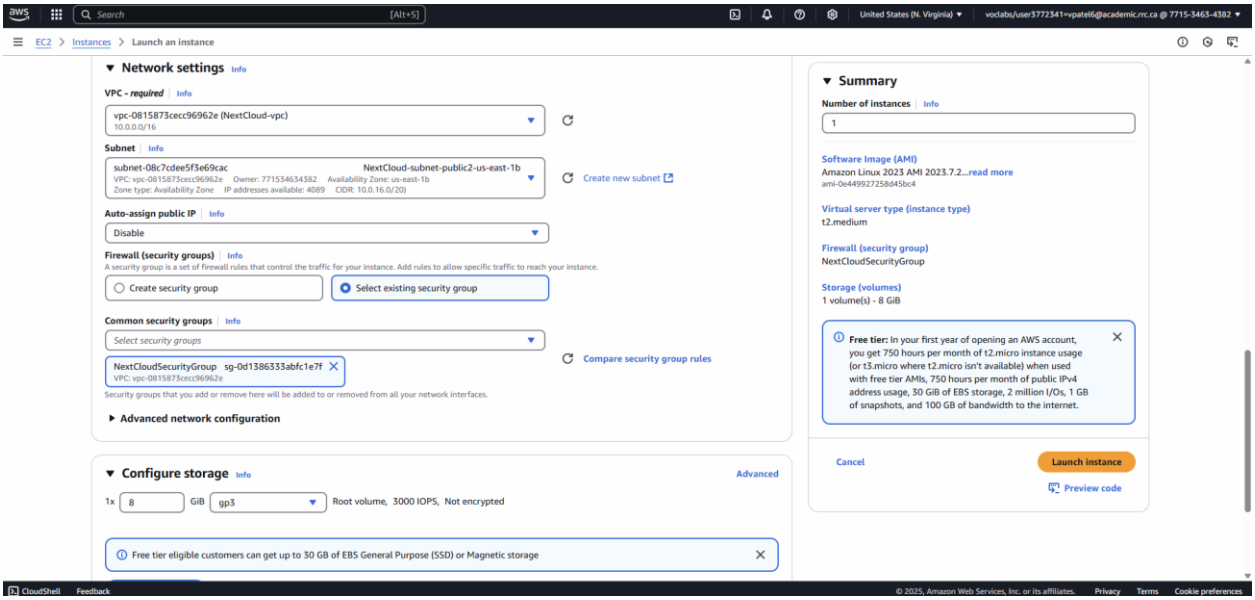


8. It will be redirected to a small screen. In the key pair name section, enter NextCloud.
9. Keep the rest setting as default.

10. Click on **Create key pair** to generate key pair.

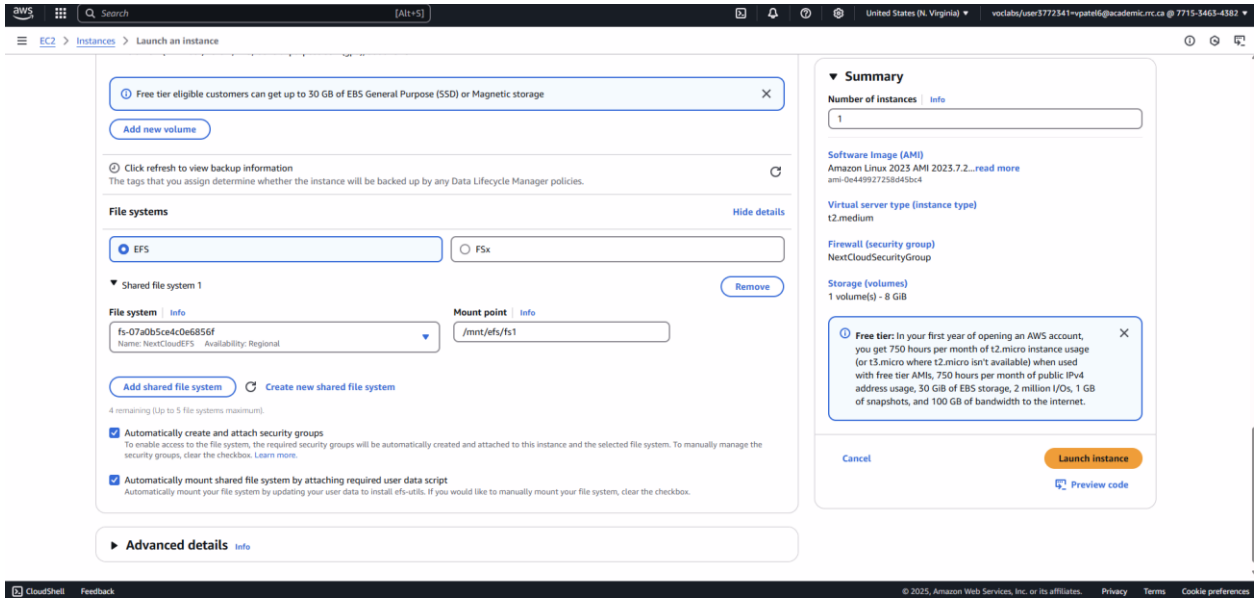


11. Next to Network settings, choose **Edit**.
12. For **VPC**, select **NextCloud VPC**.
13. Keep the default subnet **PublicSubnet1**.
14. Under **Firewall (security groups)**, choose **Select(existing) security group** and configure:
    a. Choose nextCloud Security group in common security groups.
15. Keep **assign default public IP** to disable.

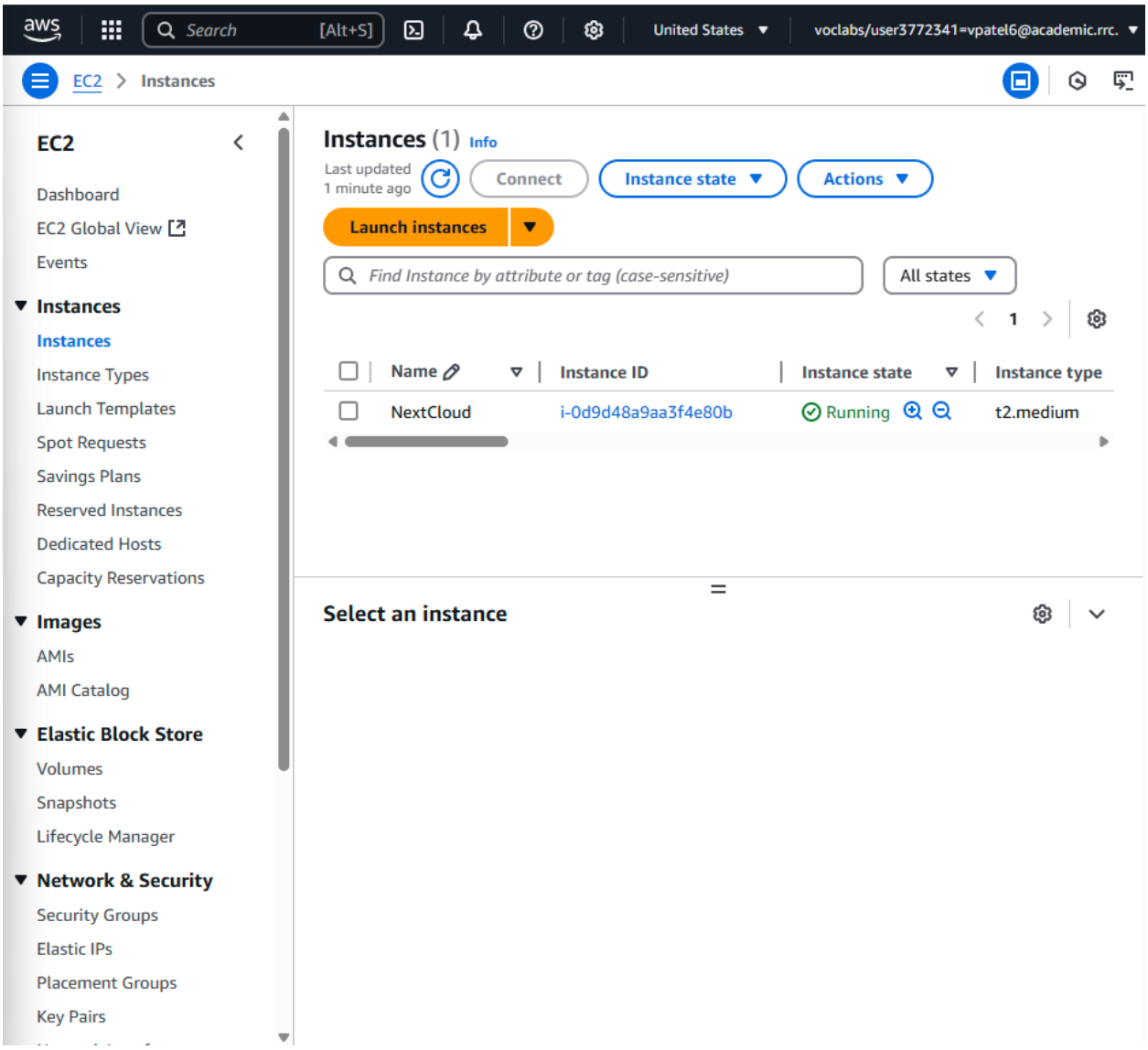


16. In the *Configure storage* section, keep the default settings.
17. Expand **File Systems**
    a. Keep **EFS** selected.

b. Choose **NextCloudEFS** for the file system.
c. Uncheck Automatically **detect and assign security groups** checkbox.
d. Keep the rest setting as default.

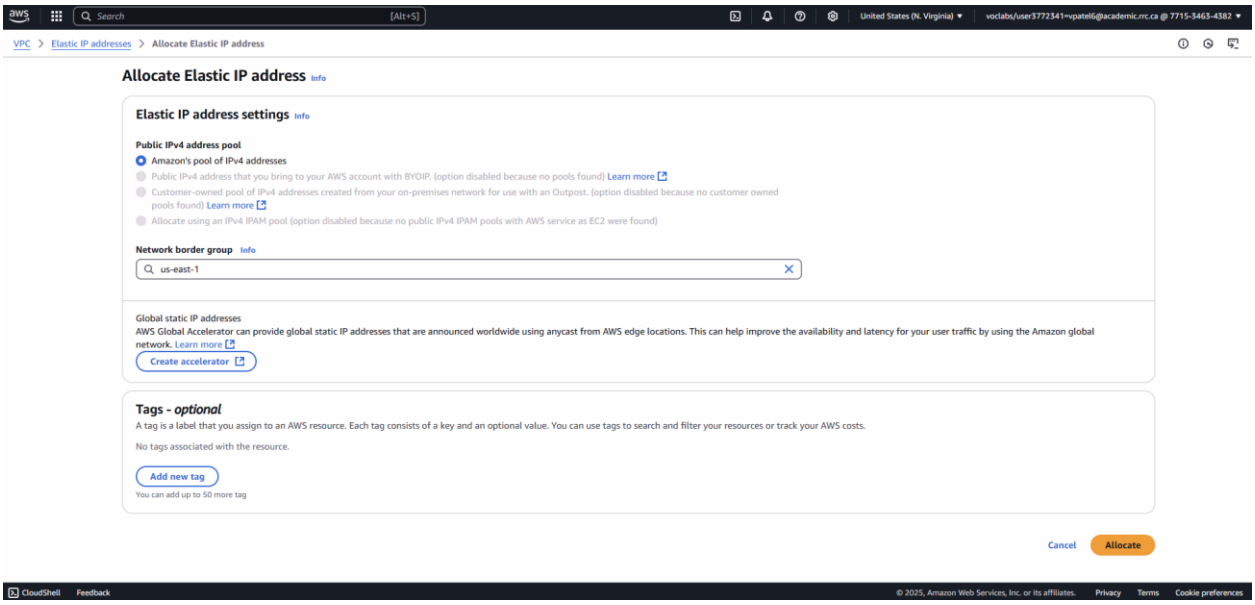


18. Expand **the Advance details** tab.
19. Choose LabInstanceProfile for IAM instance profile.
20. At the bottom of the Summary panel choose **Launch instance.**
21. Choose **View all instances.**

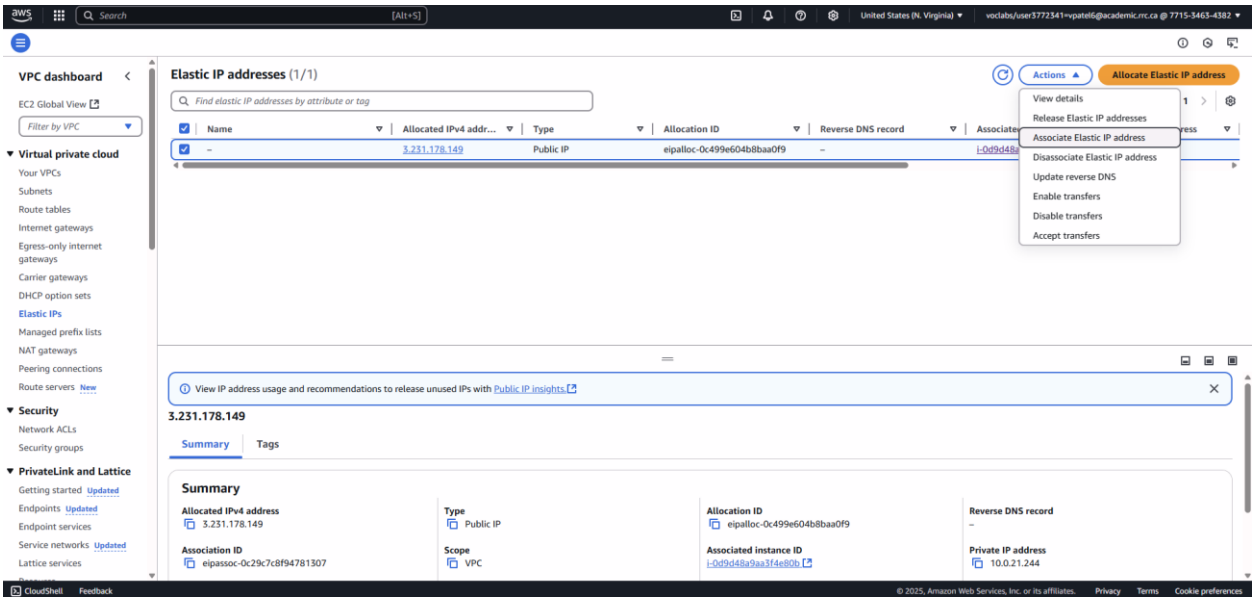


Allocating Elastic IP to EC2 Instance:

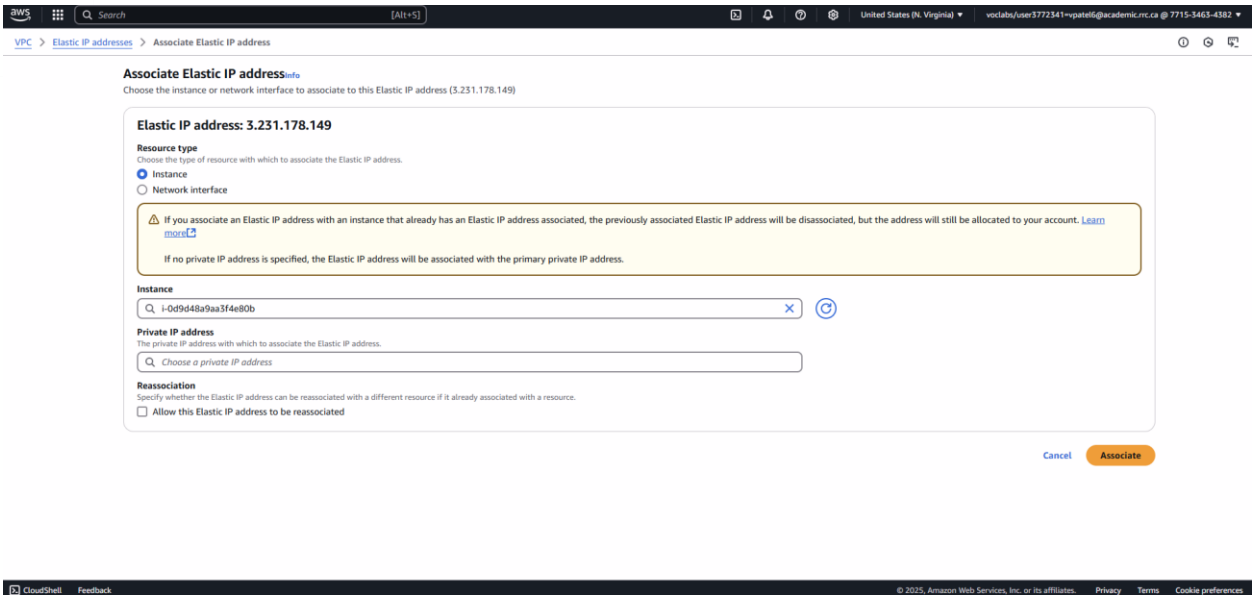
1. In the left-hand side navigation, go to **Elastic IPs.**
2. Click the **Allocate Elastic IP address** button.
3. Leave all the settings as default and click the **Allocate** button.



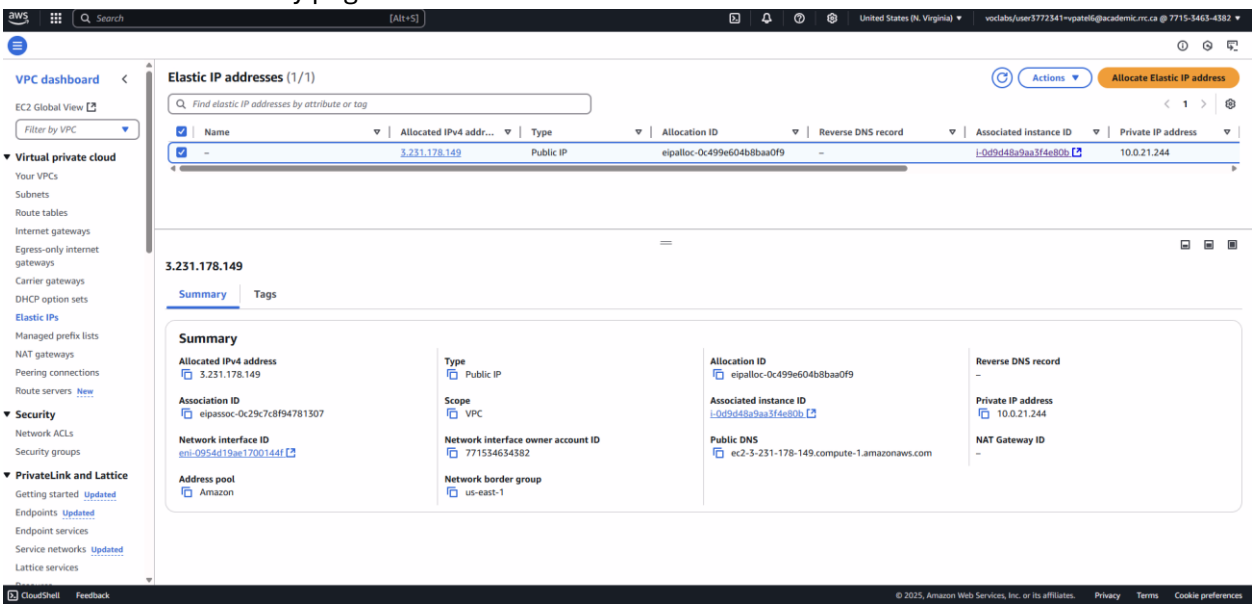
4. Select the newly created Elastic IP.
5. Click **Action** at the top right of the page, then select **Associate Elastic IP address**.



6. Choose the nextCloud EC2 instance.
7. Keep the rest of the setting as default.
8. Click the "Associate" button to complete the process.

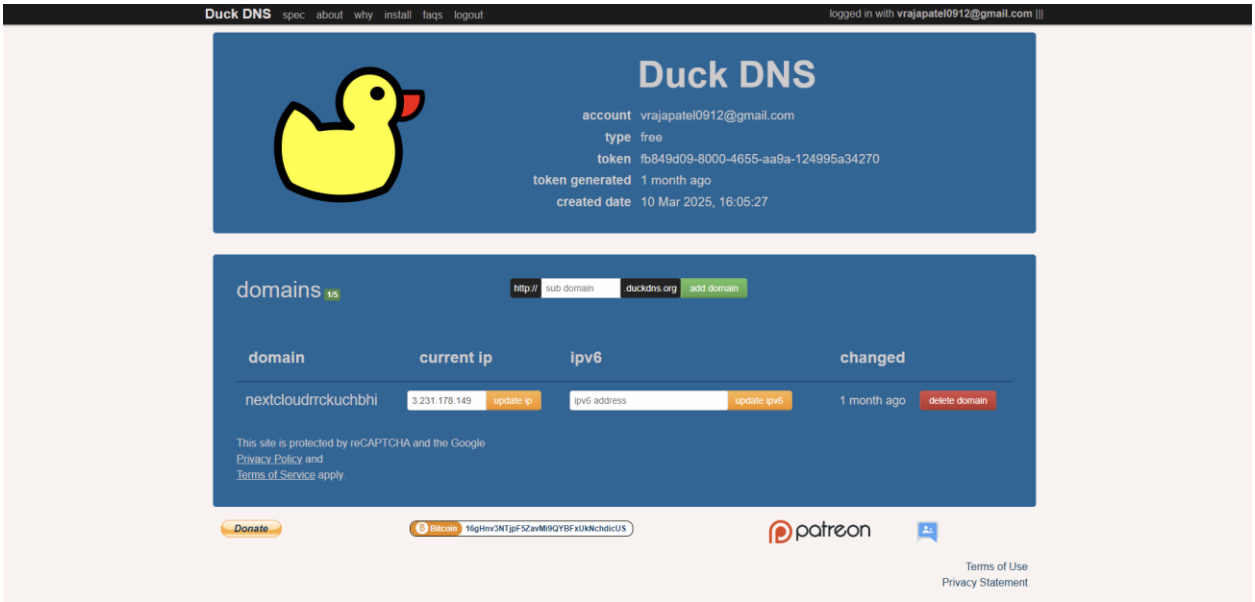


9. Now, our EC2 instance has been assigned a public IP address, which will be displayed on the instance summary page.



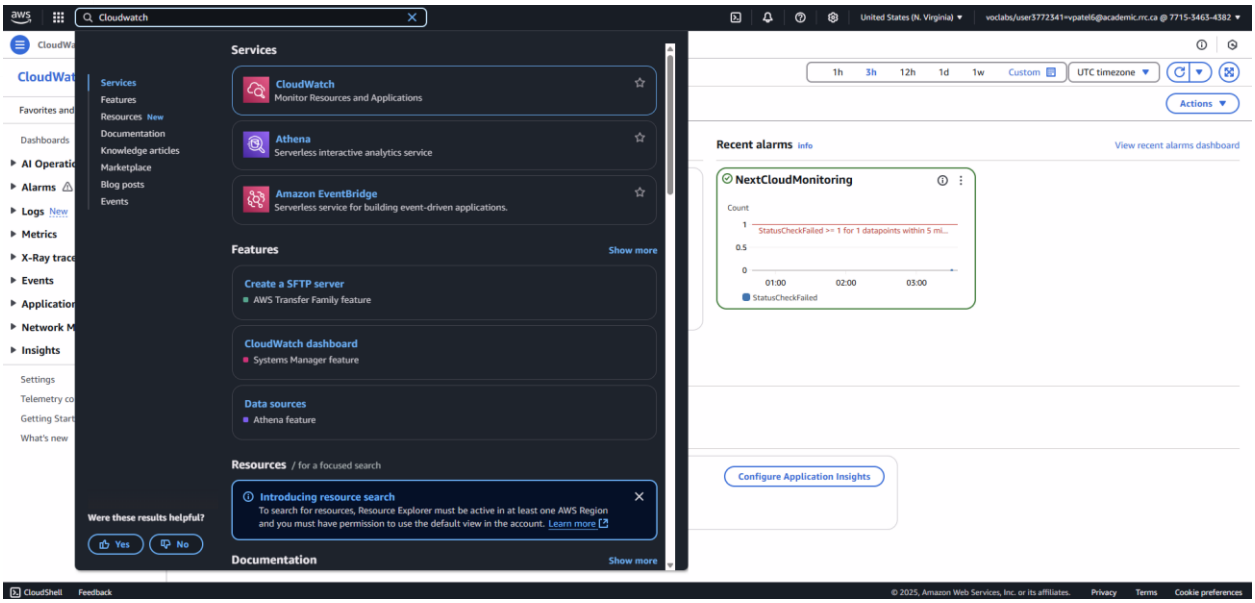
Create a duck DNS domain:

1. Sign in to duckdns.org
2. Create a unique domain and click add domain
3. Enter your elastic IP and click update ip.

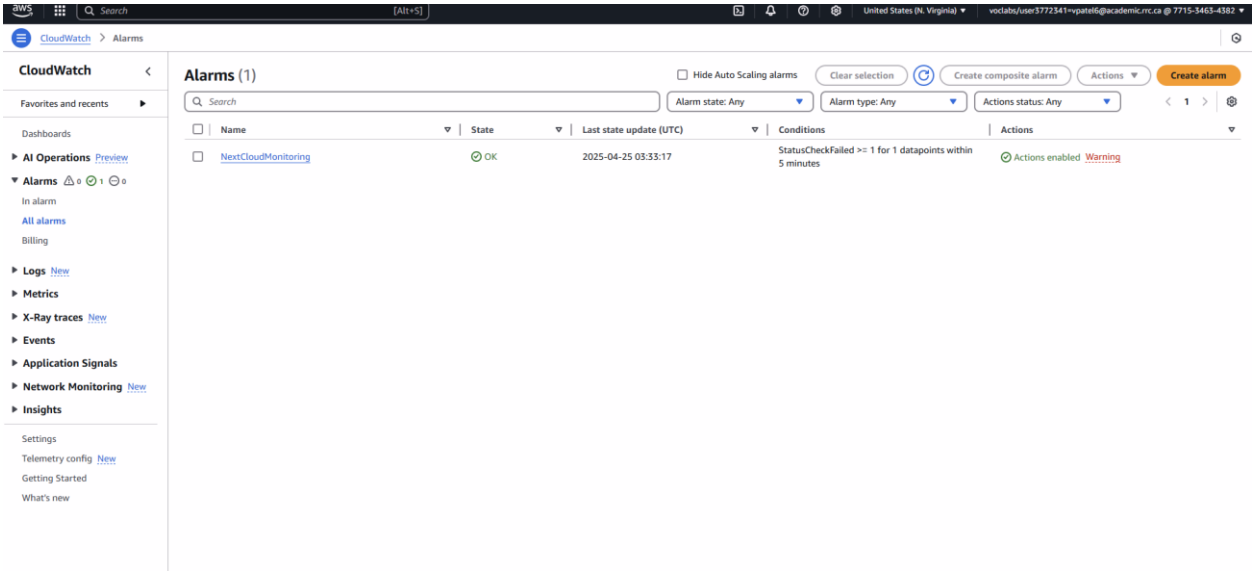


Create a CloudWatch Monitoring:

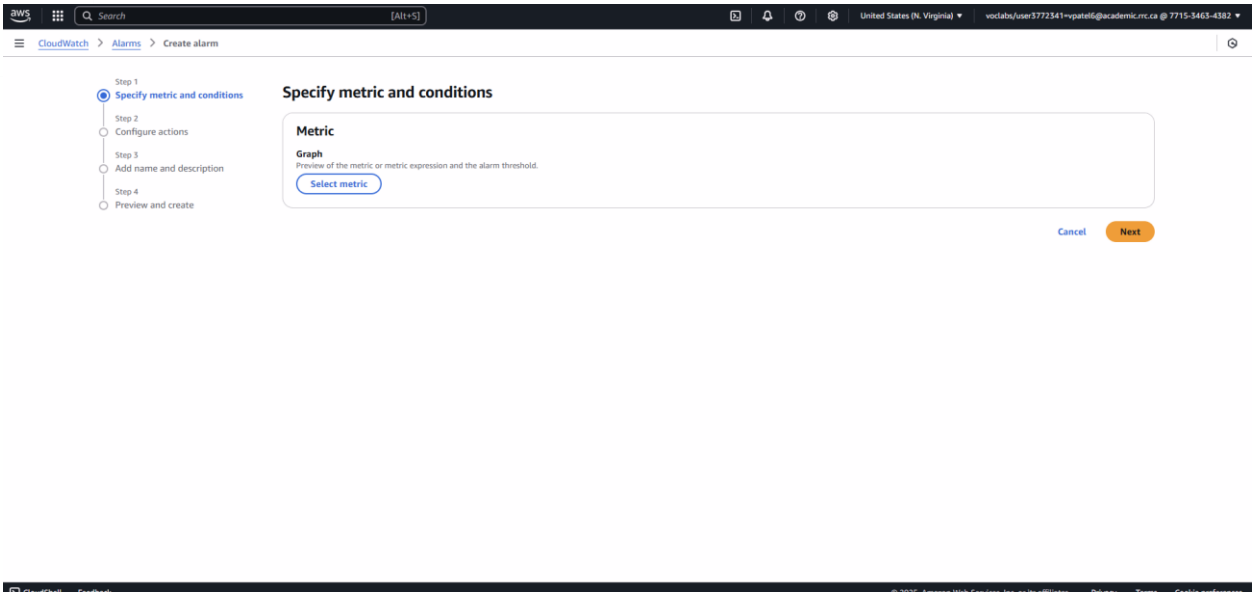
1. In the **AWS Management Console** choose **Services**, choose **Computer** and then choose **CloudWatch**.



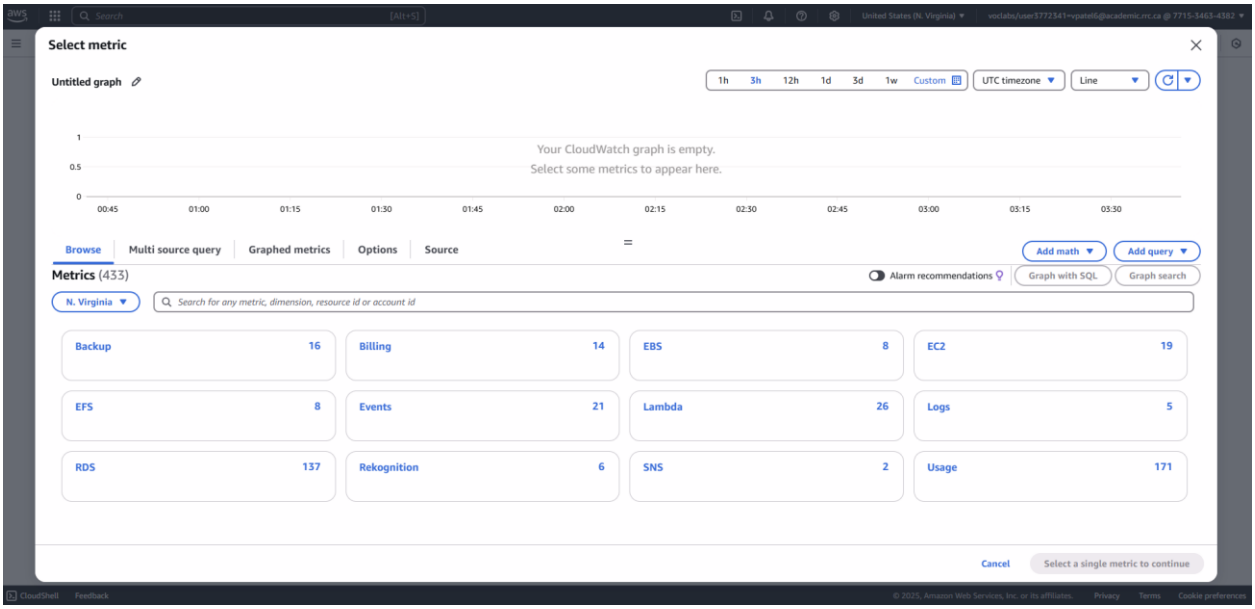
2. Select alarms on the left-hand menu, the click **Create alarm**.



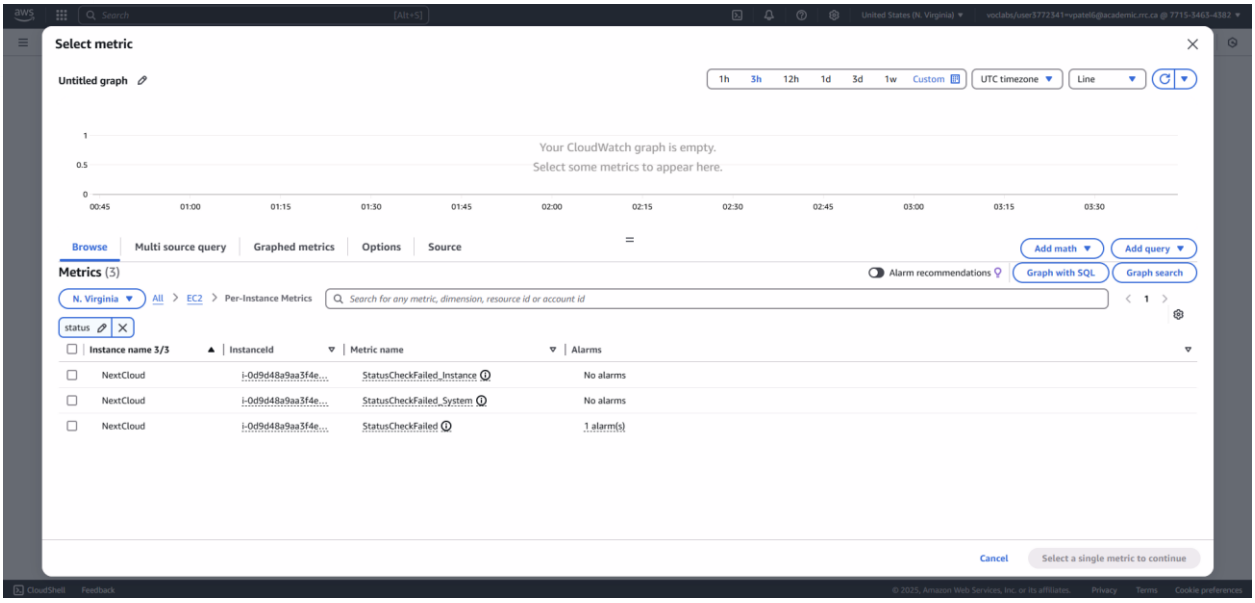
3. Click on **Select metric**



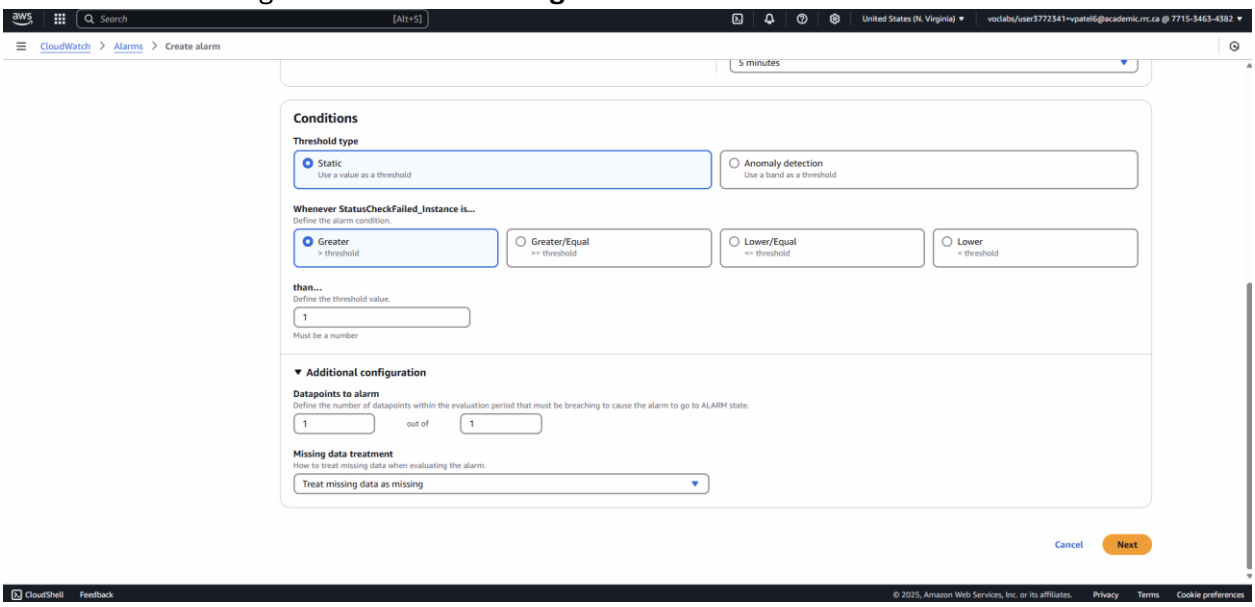
4. Select the EC2 button near the bottom-right. Click Per-Instance Metrics.



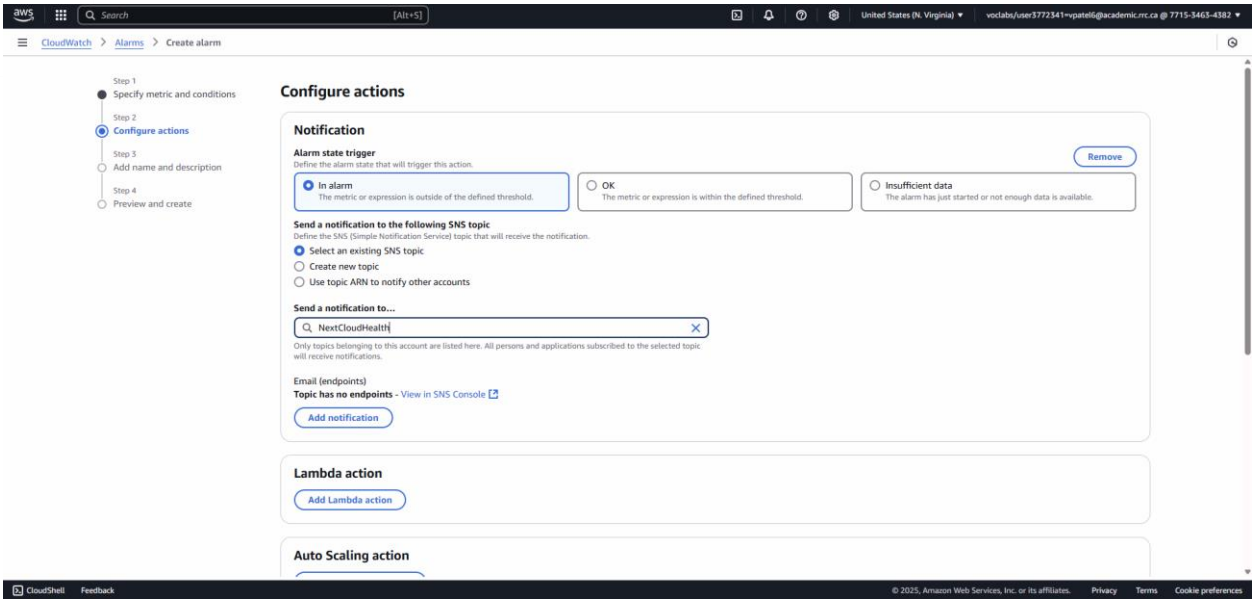
5. Scroll and find the StatusCheckFailed_Instance metric. Then click on **Select metric**.



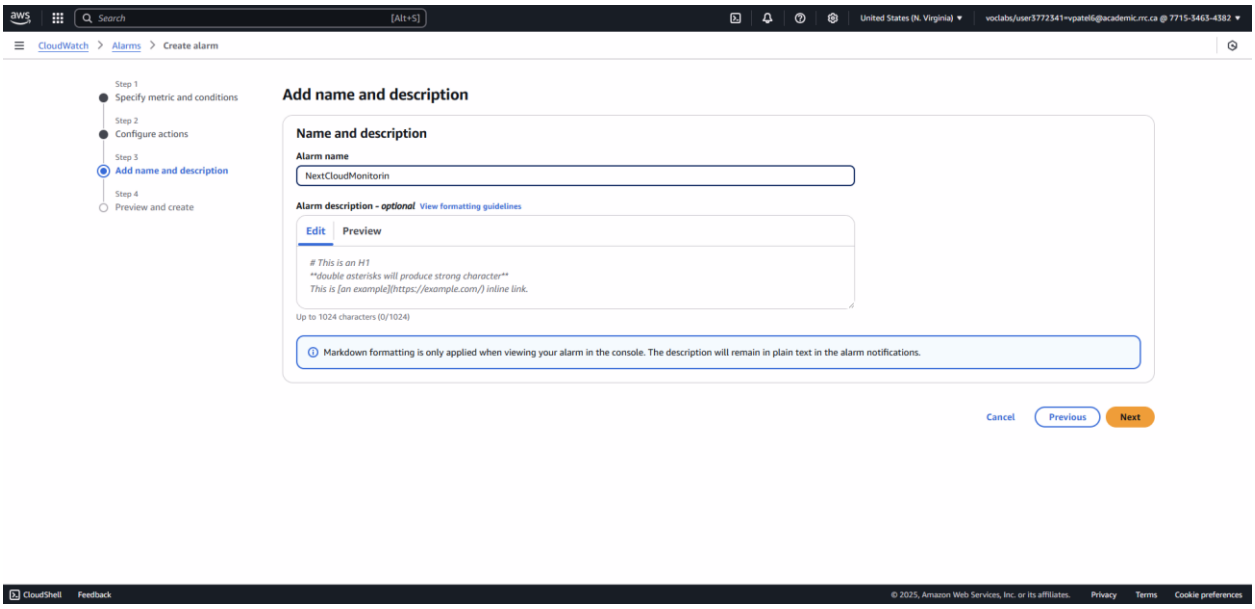
6. Under conditions, select static as the threshold type. Set it to Greater than 1.
7. Select treat missing data as bad in **missing data treatment** section.



8. On the next page, choose **in alarm**. Select **Create a new topic**, and enter a name for the topic.
9. Enter your email address that you wish to receive the alarm. Click create topic.



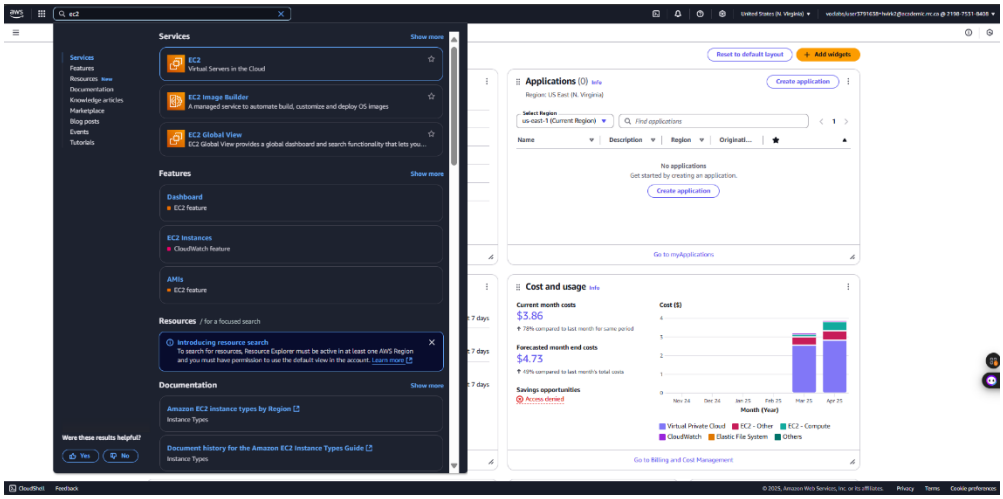
10. Click **next**.
11. Name the alarm as NextCloudMonitoring.
12. Click **next**, confirm the summary,
13. Click **Create alarm** to create an alarm.

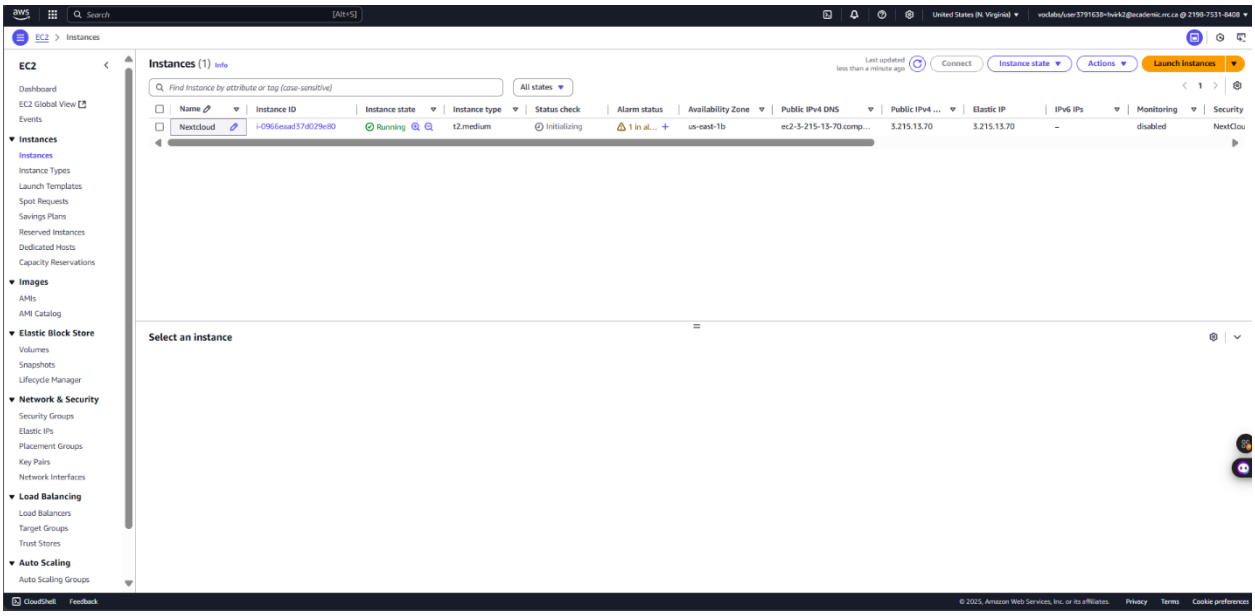


MILESTONE 4 – Next cloud Demonstration

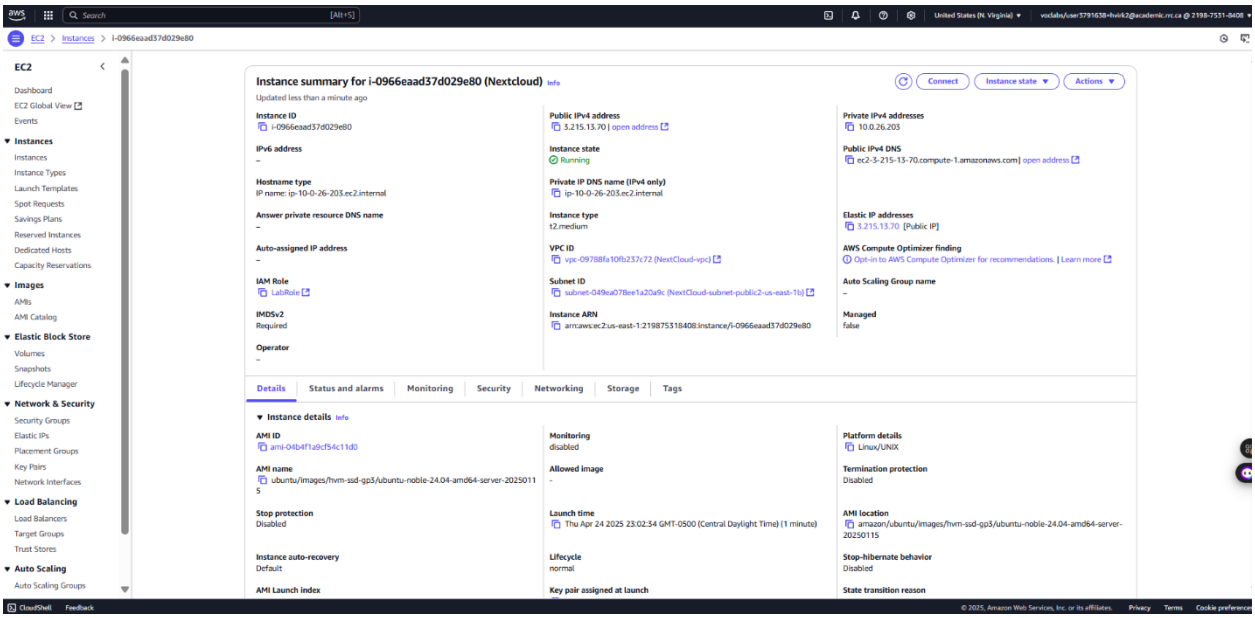
Install Nextcloud:

1. Click on **services**, navigate the cursor to the search bar, and look for **EC2**.
2. Click on instances on the left of the panel and select the **Nextcloud** instances after the passing status check.

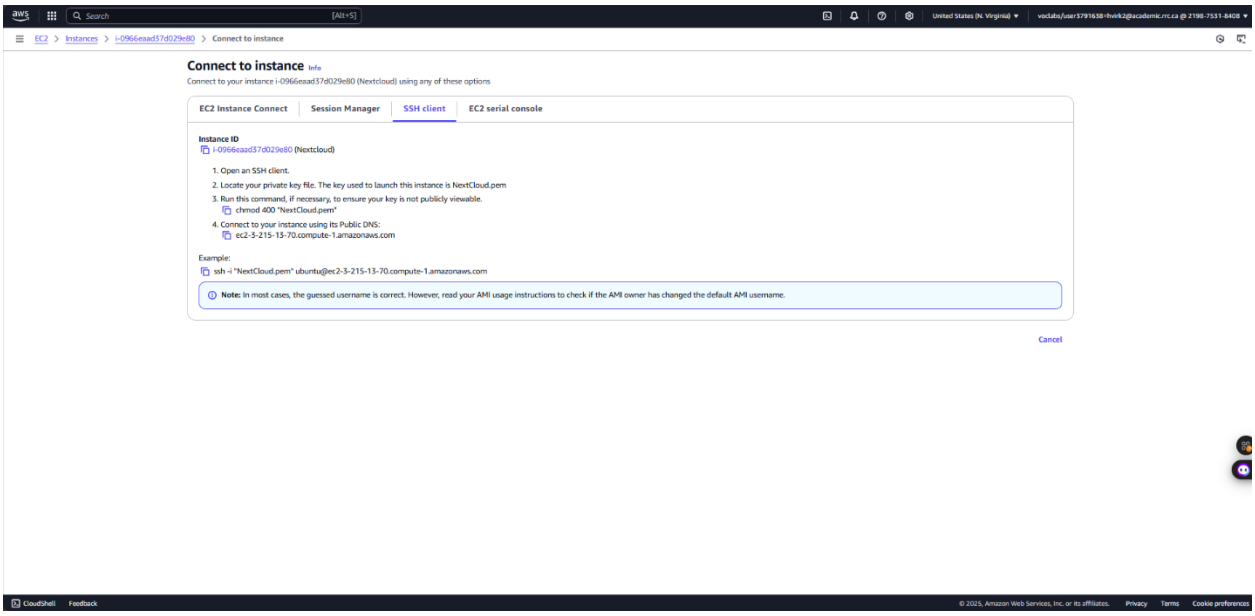




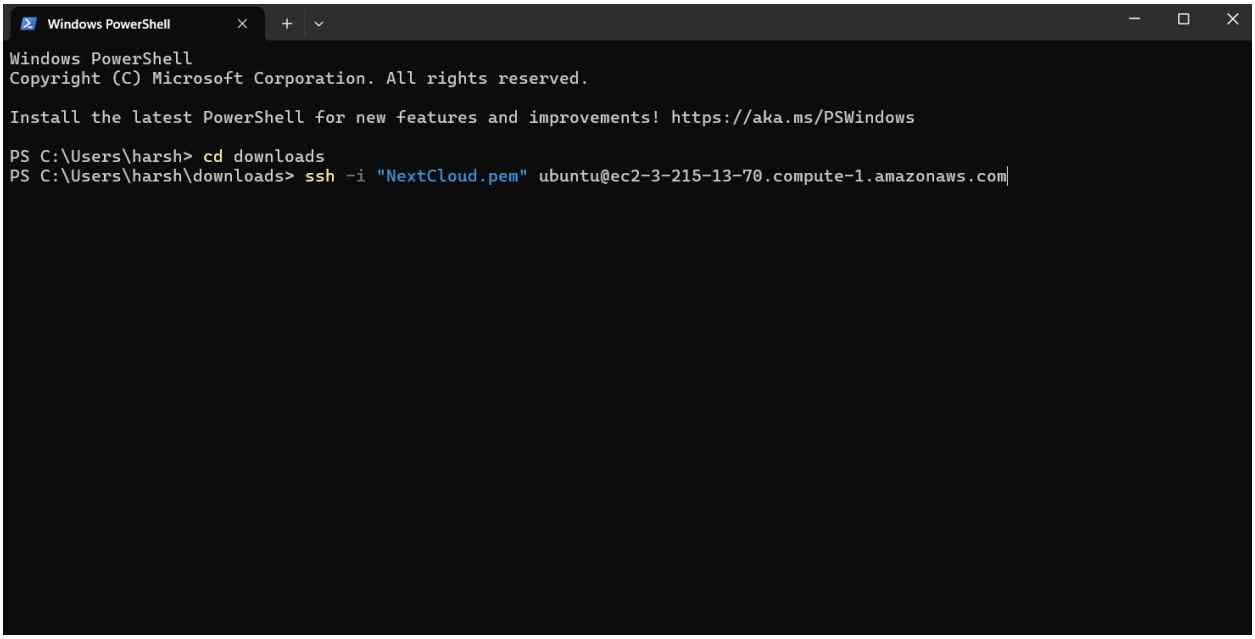
3. Click on the **connect** option.



4. For connect to the instance, select the SSH client and copy the "**ssh -I "Nextcloud.pem" ubuntu@ec2-44-205-176-197.compute-1.amazonaws.com**" command.

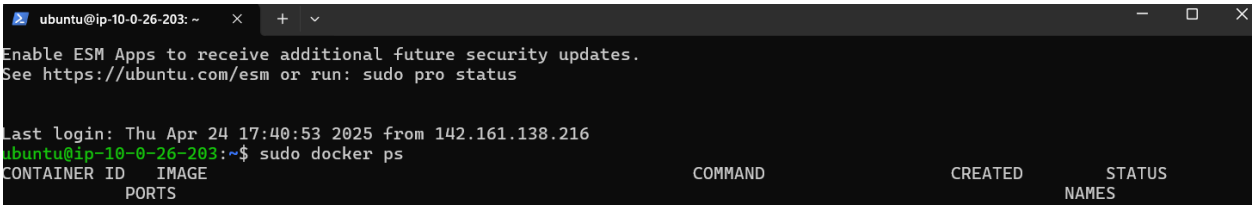


5. Open the command prompt on your computer where we download the Nextcloud.pem file in milestone 3 and paste the ssh command.



6. Login to the instance via ssh or admin console
7. Type **sudo apt update**
8. Type **sudo apt dist-upgrade** and press **“Y”**
9. Type **sudo apt install docker.io** and press **“Y”**

10. Type **sudo apt install -y nfs-common**
11. Type **df-h** to confirm the mount.



12. Type

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_apache

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_collabora_fonts

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_database

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_database_dump

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_mastercontainer

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_nextcloud

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_nextcloud_data

sudo mkdir -p /mnt/efs/docker/nextcloud_aio_redis

sudo mkdir -p /mnt/efs/backup

13. Change the name and path properties for each directory we just created.

Sudo docker volume create --driver local --name nextcloud_aio_apache \ -o device=/mnt/efs/docker/nextcloud_aio_apache \ -o type=none -o o=bind

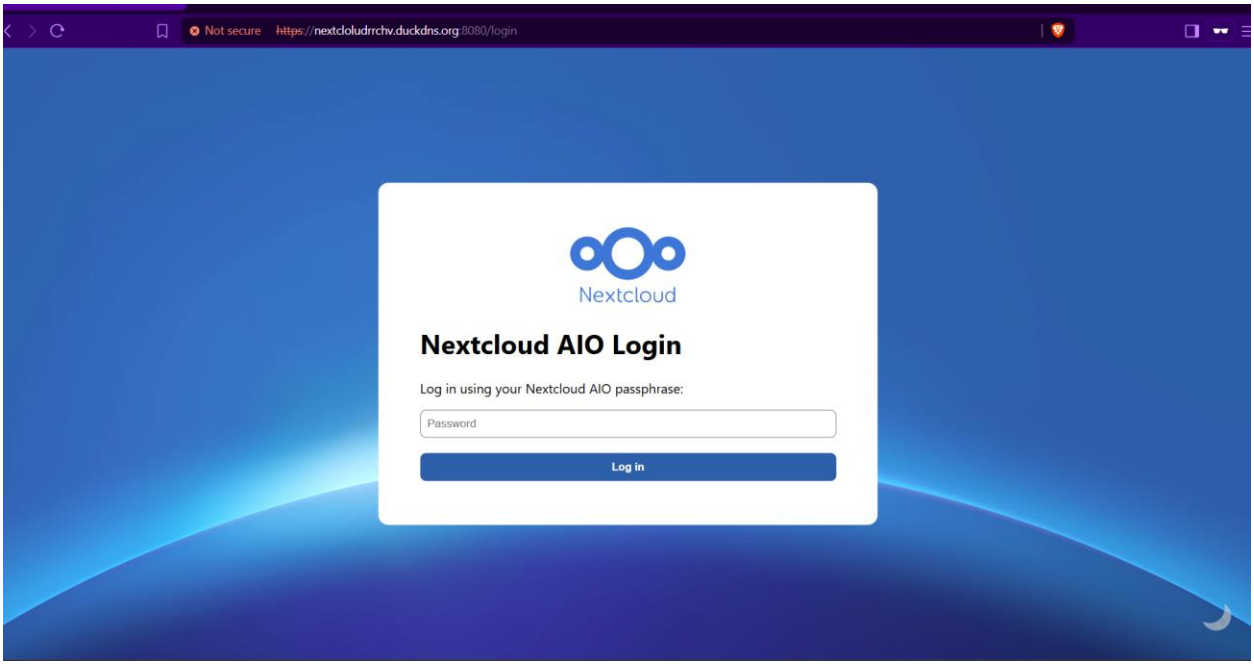
14. **Type sudo docker volume** ls to confirm they've been created.
15. Run this script

```
# For Linux and without a web server or reverse proxy (like Apache, Nginx,
Cloudflare Tunnel and else) already in place:
sudo docker run \
--init \
--sig-proxy=false \
--name nextcloud-aio-mastercontainer \
--restart always \
--publish 80:80 \
--publish 8080:8080 \
--publish 8443:8443 \
--volume nextcloud_aio_mastercontainer:/mnt/docker-aio-config \
--volume /var/run/docker.sock:/var/run/docker.sock:ro \
```

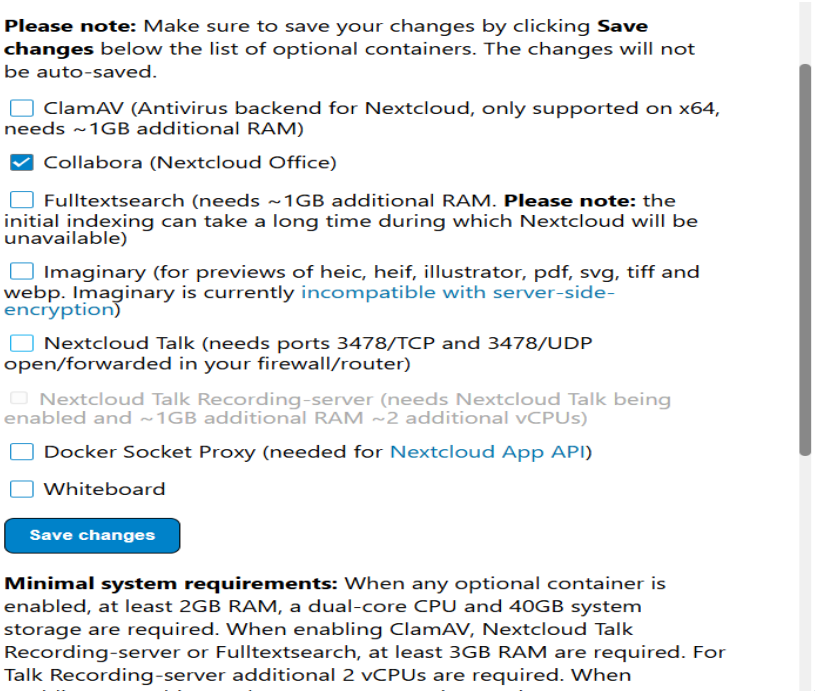
```
nextcloud/all-in-one:latest
```

Configure Nextcloud:

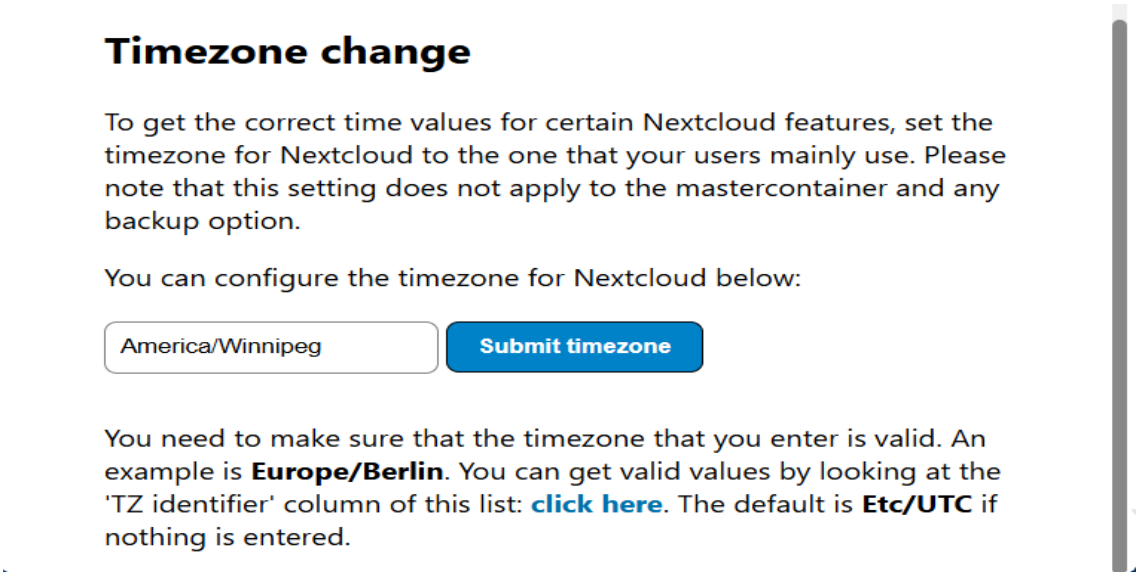
1. Open the browser and search your **Duckdns domain** which we created in milestone 3.
2. Copy the passphrase and click the **open Nextcloud AIO login link**.
3. Paste the passphrase and click on **login**.



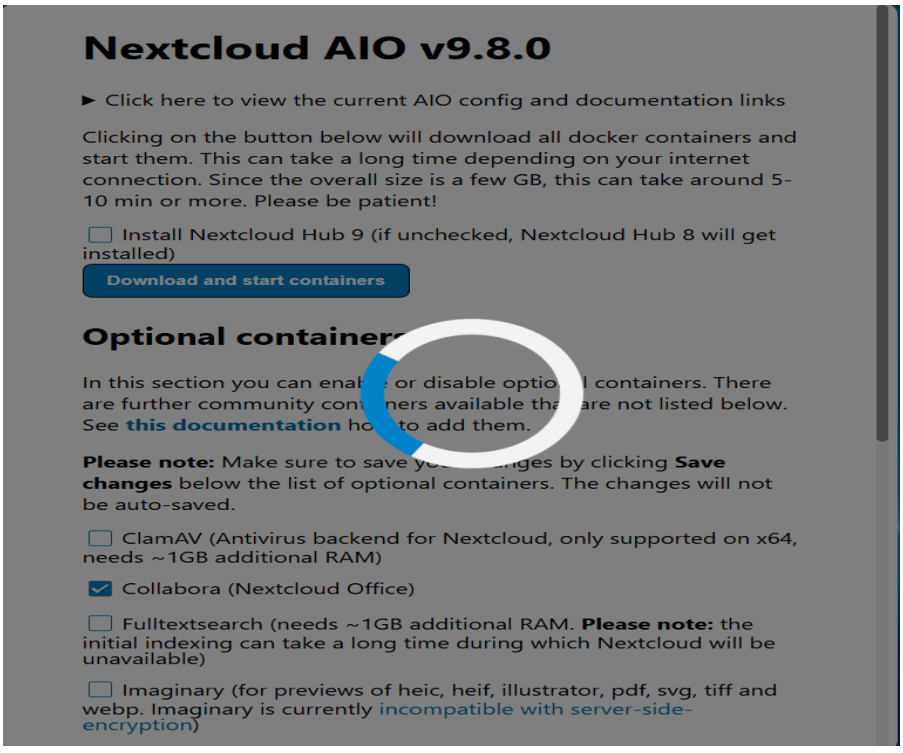
4. Enter your **duckdsn domain** information and click on **submit domain.**
5. Disable everything but select **the Collabora (Nextcloud office)** option and click **Save Changes.**



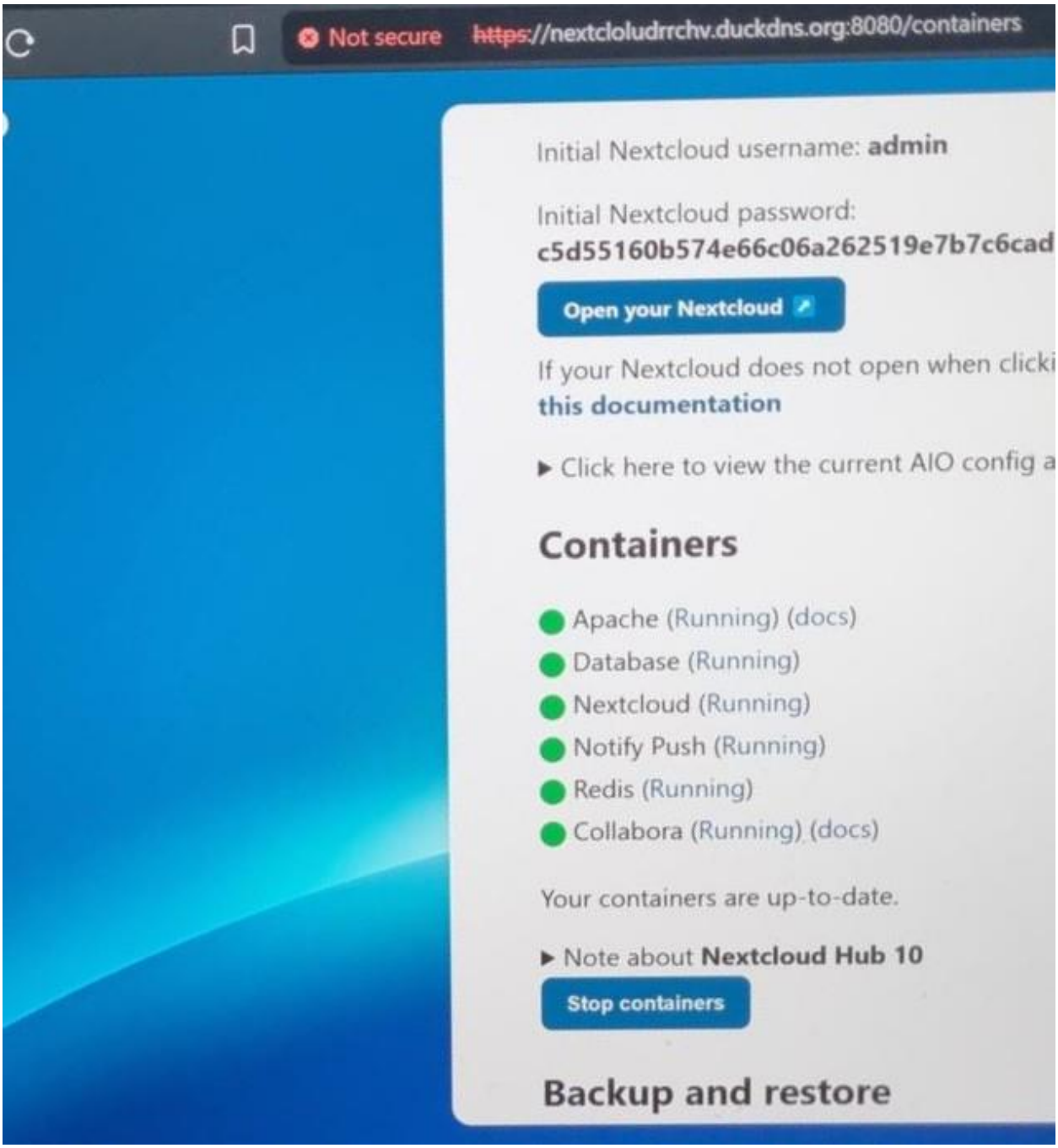
6. Ensure the time zone is set to **America/Winnipeg** and click **submit time zone**.



7. After scrolling up, click **Download and start Containers**.



8. Wait for the containers to all turn green. Refresh if you must.



9. Enter **/mnt/efs/backup** under the backup and restore option and submit it.

Containers

- Apache (Running)
- Database (Running)
- Nextcloud (Running)
- Notify Push (Running)
- Redis (Running)
- Collabora (Running)

Your containers are up-to-date.

▶ Note about **Nextcloud Hub 9**

Stop containers

Backup and restore

Please enter the directory path below where backups will be created on the host system. It's best to choose a location on a separate drive and not on your root drive.

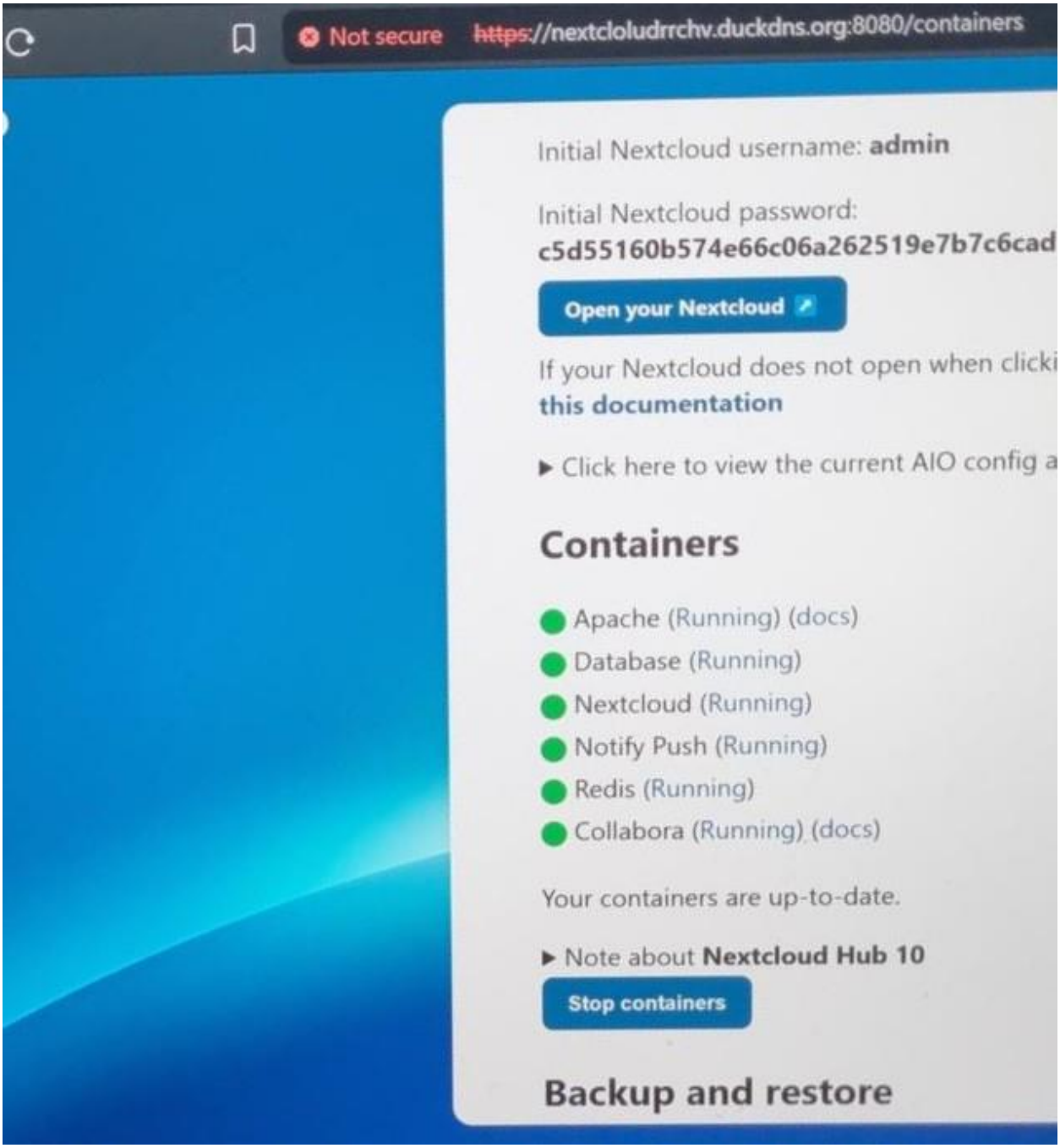
/mnt/efs/backup **Submit backup location**

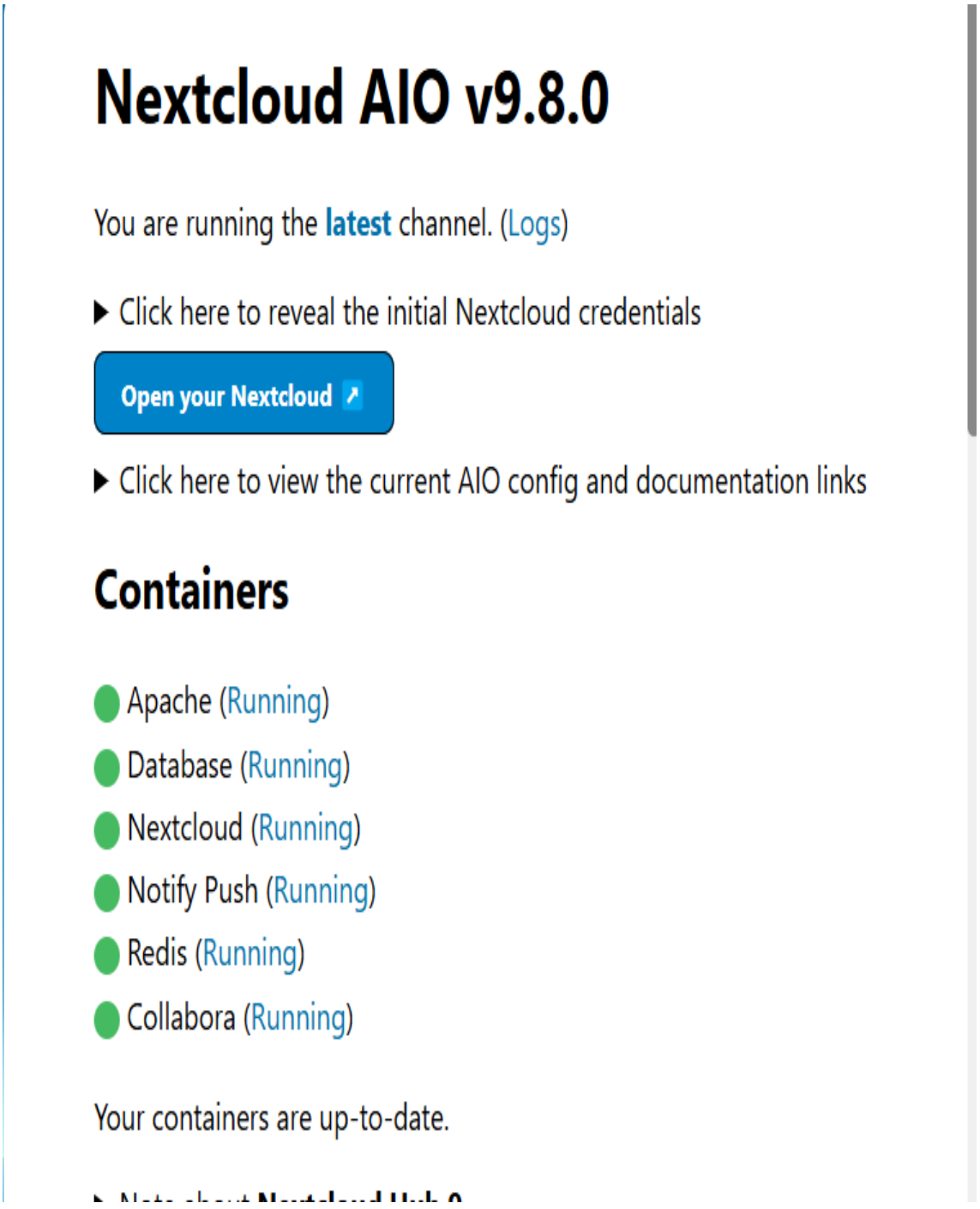
The folder path that you enter must start with **/** and must **not** end with **/**.

An example for Linux is **/mnt/backup**.

On Synology it could be **/volume1/docker/nextcloud/backup**.

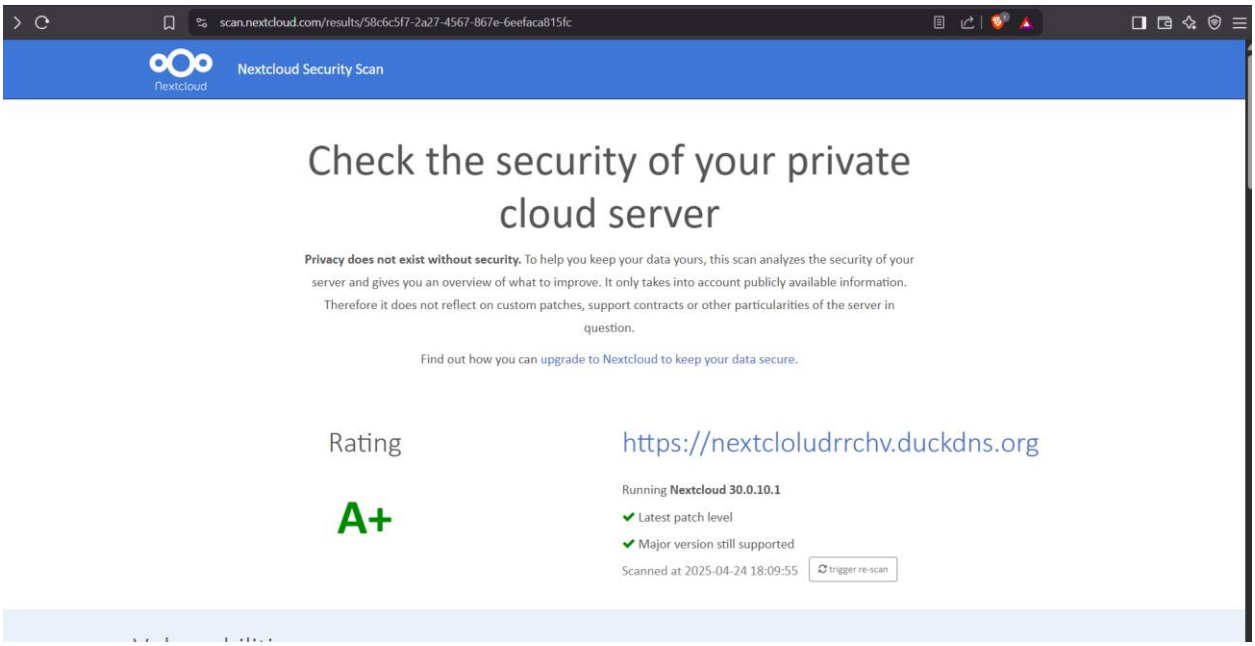
For macOS it may be **/var/backup**.

10. Click the link to open your **Nextcloud link**.
11. 

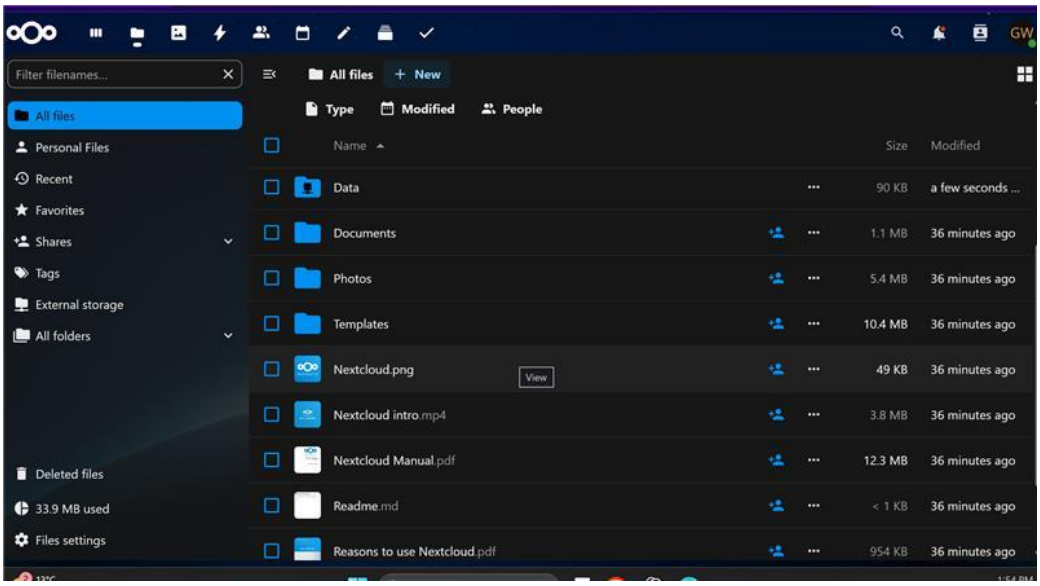


12. Enter the **username or email address** and **password** to login to the next cloud.

13. Select your **app** option on the left of the panel and enable **external support.**
14. Return to the top-right icon menu and click **Administration settings**.
15. Click the **security scan link**.
16. Enter your **duckdns domain** to check the security of your private Nextcloud server.

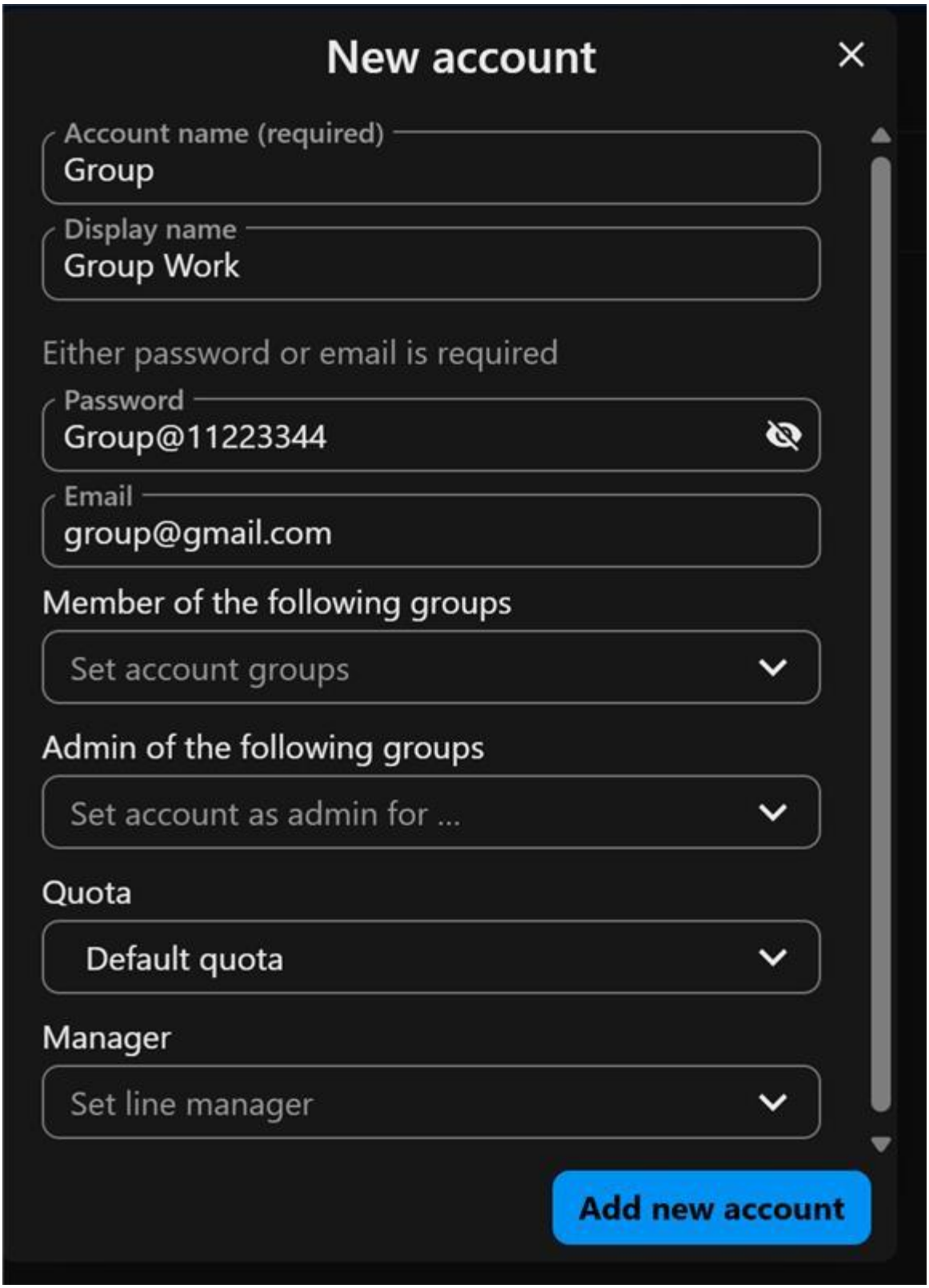


17. Click **external storage**, and create a folder named **"Data"** Enter your **S3 bucket** details leaving the hostname and port empty. **"None"** for authentication. Enable SSL. **Save** your settings.
18. At the top bar, click files and drop a file in the Data folder. The object should appear in your S3 bucket.

19. 

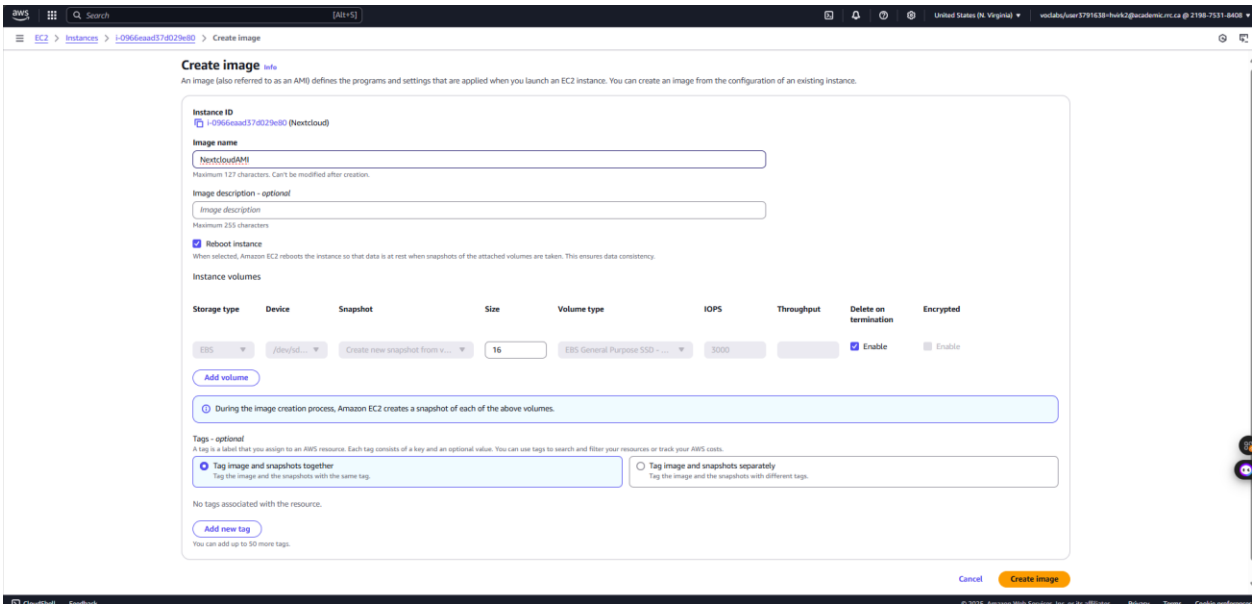
20. Open the data folder and again create the **test folder** name.
21. Select the **users** from the profile option in the left corner.
22. Click on the new account and enter the **username, display, password, and email address**. We can also select the specific group, quota, and manager but it is optional. Click on **Add new user**.

23.

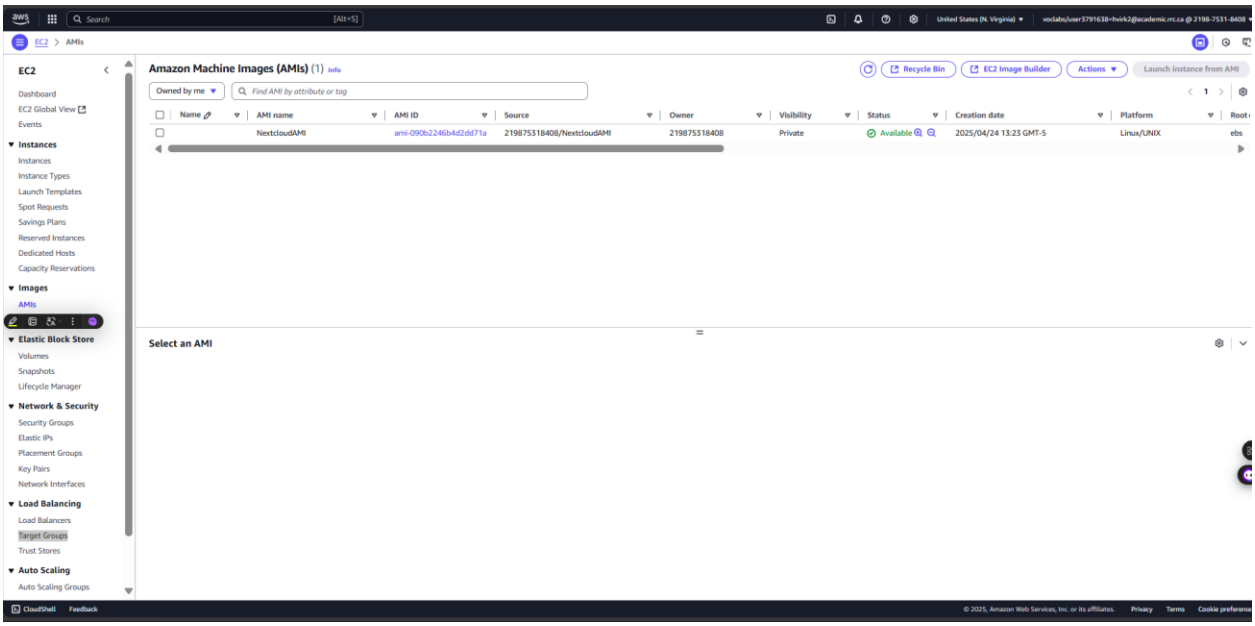

New account
Account name (required)
Group
Display name
Group Work
Either password or email is required
Password
Group@11223344
Email
group@gmail.com
Member of the following groups
Set account groups
Admin of the following groups
Set account as admin for ...
Quota
Default quota
Manager
Set line manager
Add new account

Creating Amazon machine Image:

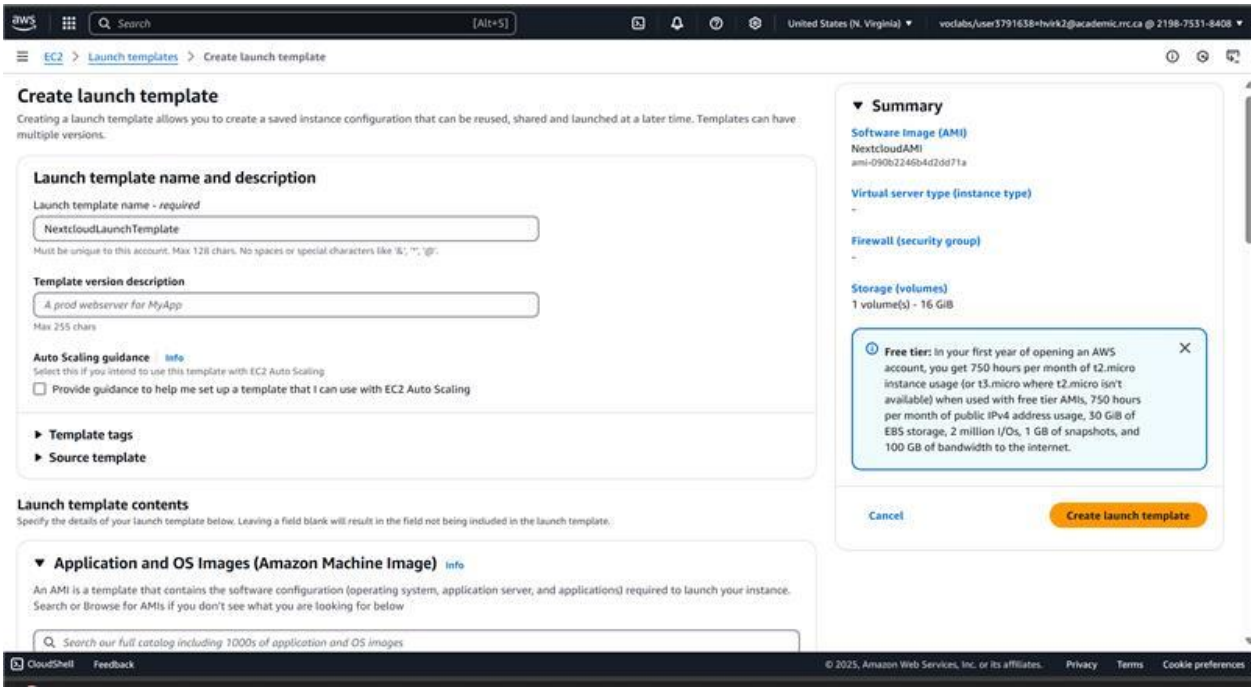
1. In AWS, choose the EC2 instance. Select Images
2. Click on the Create Image button.
3. Enter a name and keep the rest settings as default.
4. Click on the Create Image button.



5. Redirect to image page. Here you can see the created image.

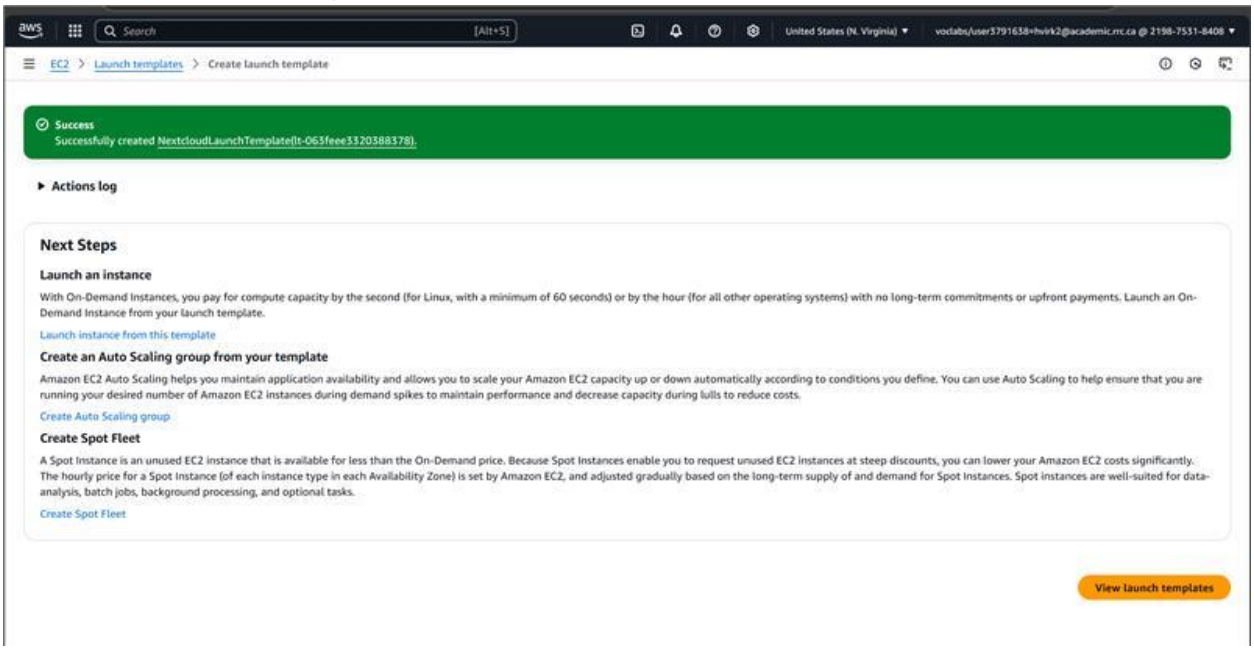


Creating launch template:

1. Select Lunch template from the side bar and then click on create lunch template.
2. Provide NextcloudTemplate name in Name field.
3. Select MyAMIs under AMI section. Make sure that it selects NextCloudAMI.
4. 

5. Select t2.medium instance type.
6. Select nextCloud key pair.
7. Under select existing security group, select nextCloud security group.
8. In network settings, select NextCloud VPC subnet.
9. In Advance details, choose LabInstanceProfile in IAM instance profile.

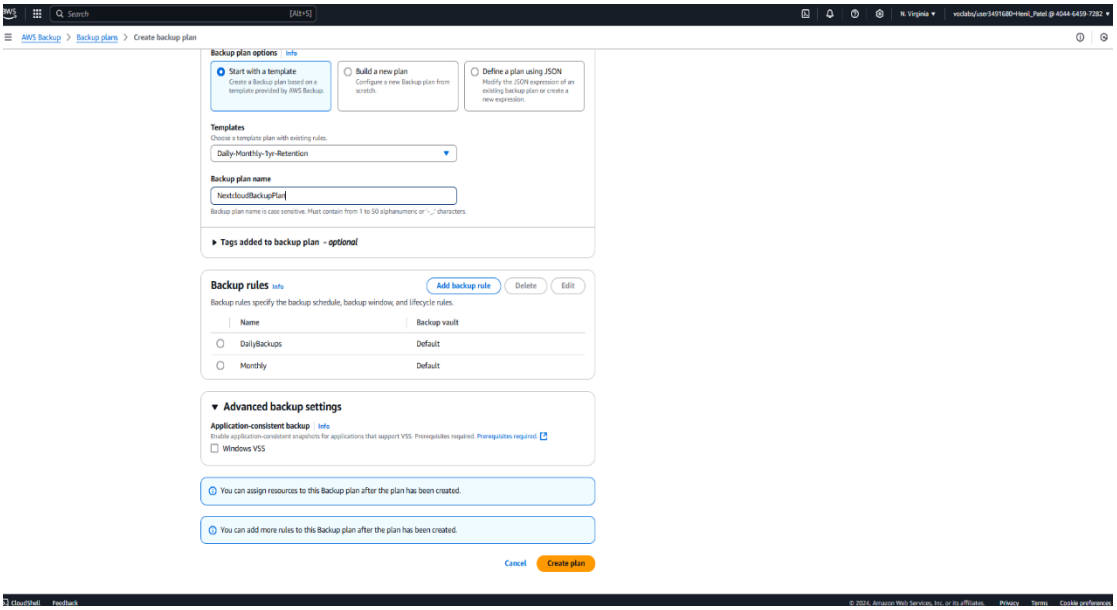
10. Click on Create lunch template.



11.

Creating AWS Backup Plan:

1. In the search bar at the top, type AWS Backup and select it from the search results.
2. Once in the AWS Backup dashboard, click on the “Create backup plan” button.
3. Select Start with a template and enter the backup plan name.
4. Select Daily-Monthly-1Yr-Retention.

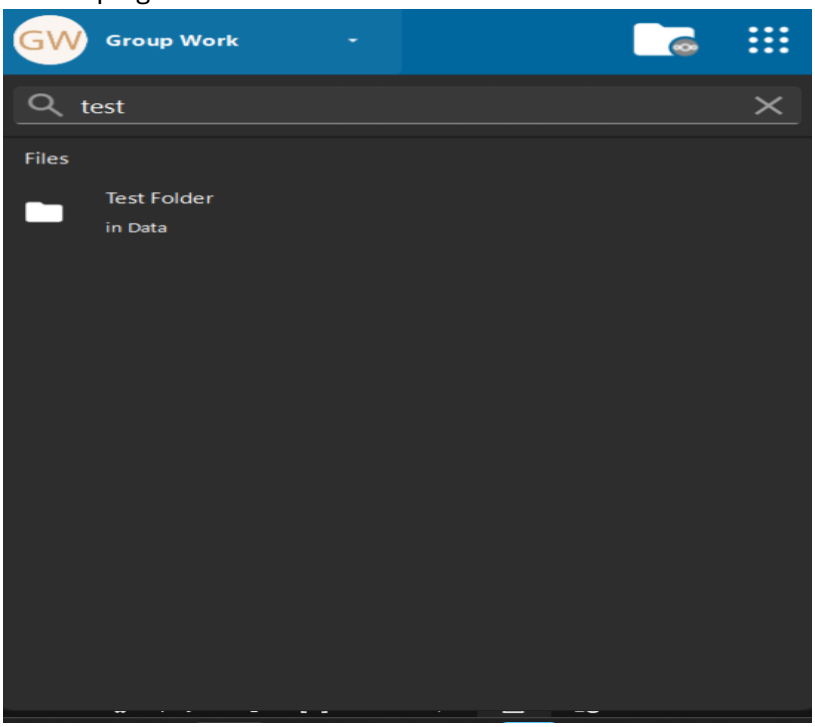


5. Click on the create plan button.

6. On the assign resource page, Select LabRole option for Role name.
7. In the Resource Selection section, Select include specific resource type.
8. From the dropdown menu, select the resource types EBS, EFS, and S3.
9. Click on Assign resources button.

Install and Configure desktop client:

1. Open the browser and navigate to the address https://nextcloud.com/
2. Click on the Download button, you will find clients for Linux, macOS, and Microsoft Windows. Click on the client that matches your local machine's operating system to download the Nextcloud desktop client.
3. Install the Nextcloud client by running the installation file you just downloaded.
4. After completing the installation, the login interface will appear.
5. Click on Log in button.
6. Enter your Nextcloud server address
7. Click on next button. It will redirect to web page.
8. Enter nextCloud user name and password.
9. Click on Grant access when prompted. A message will appear indicating that your client is now connected.
10. Return to the client and click Connect and keep the settings as defualt.
11. Wait for the client to sync the files.
12. To view the shared files on Nextcloud, open the local folder by clicking on the folder icon at the top right of the client.

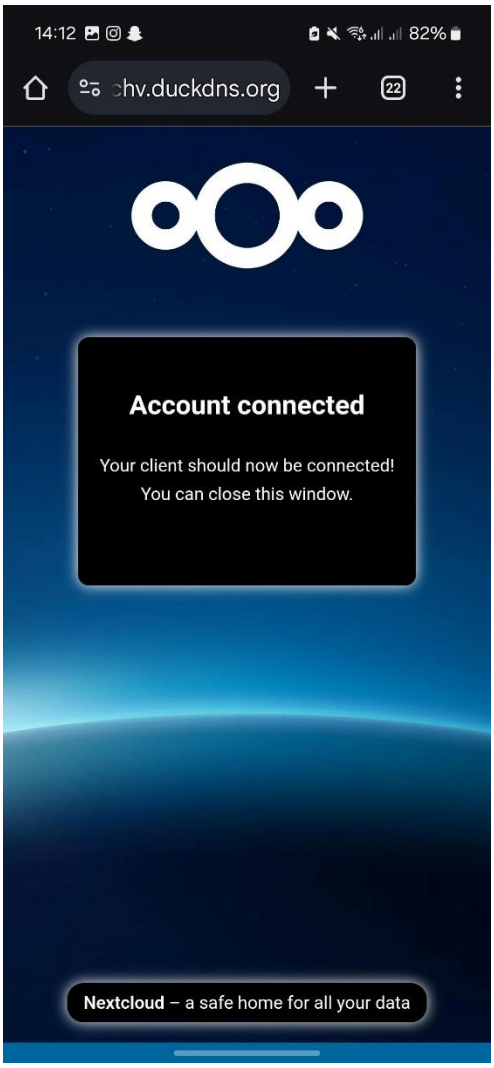


Here you can see all data that stored in different folder on next Cloud.

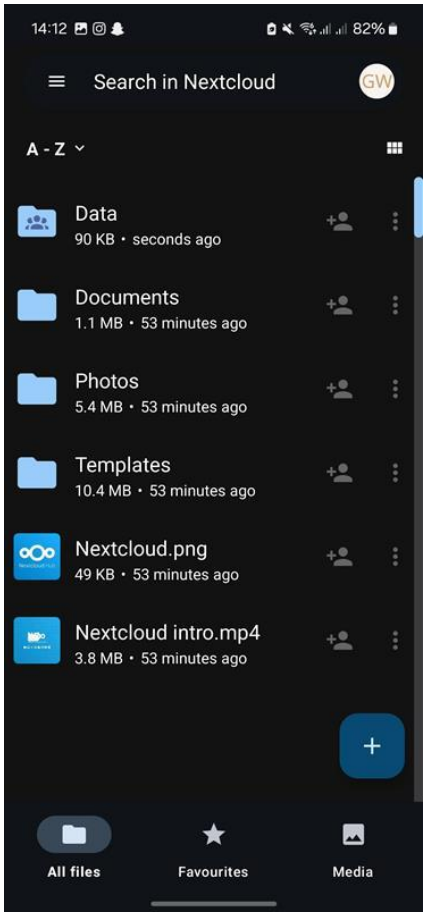
Install and Configure Android client:

1. **Download the App**
   Open the Google Play Store on your Android device and search for **“Nextcloud”**.
   Download and install the official **Nextcloud** mobile app
2. **Launch the App**
   Once installed, open the Nextcloud app.
3. **Enter Server Address**
   On the welcome screen, you’ll be prompted to enter your server address. Type in your Nextcloud server URL
4. **Authenticate via Browser**
   You’ll be redirected to your default browser where you’ll see the **Nextcloud login screen**.
   Enter your account name or email and password.
   Tap **Log in**.

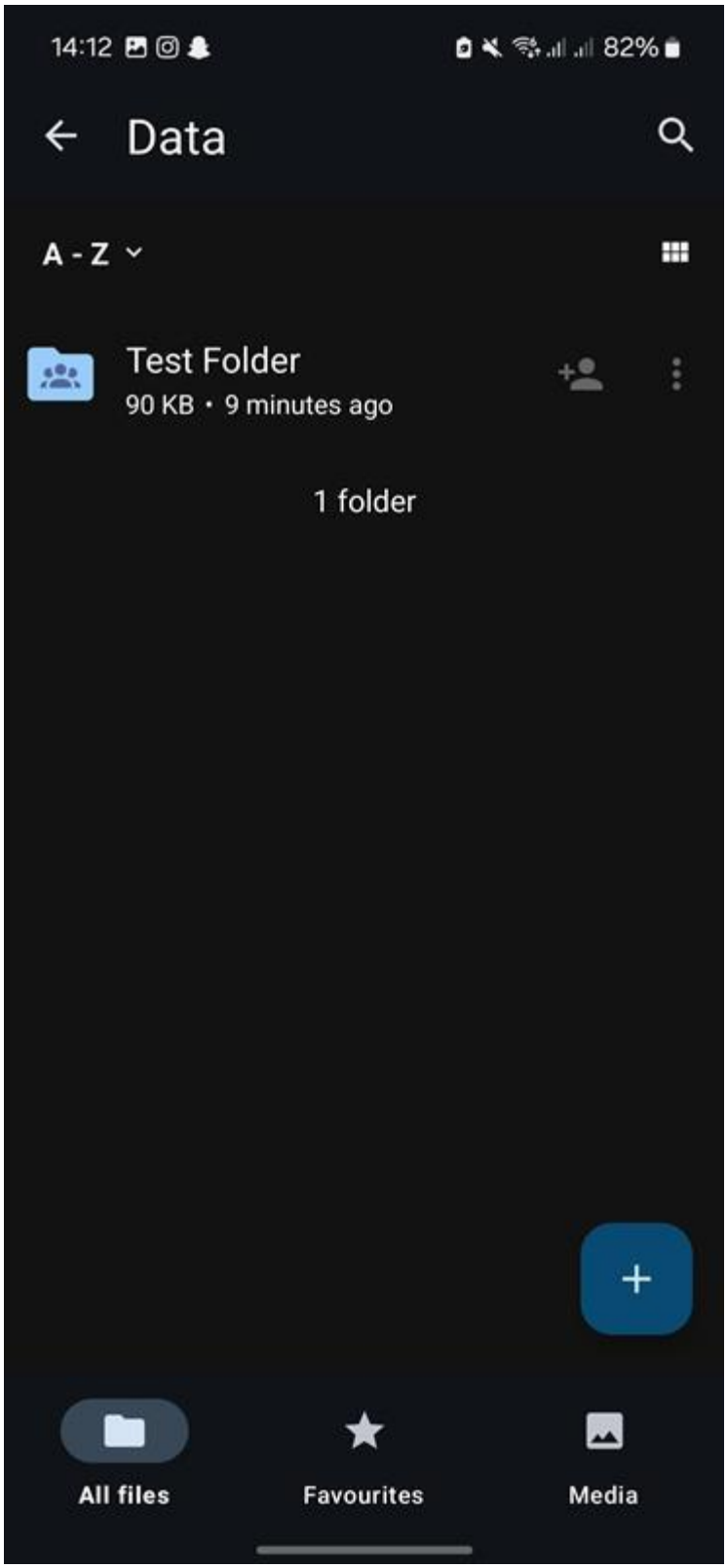
5. **Grant Access**
   Once authenticated, you'll see a message confirming **"Account connected"** (Refer to Screenshot 2). You may now close the browser tab.



6. **Return to App**
   Switch back to the Nextcloud app. It will automatically sync with your account and show you the available folders and files



7. You can now view shared files, such as **Documents**, **Photos**, or any created folders

8. 
14:12
82%
Data
A - Z
Test Folder
90 KB • 9 minutes ago
1 folder
All files
Favourites
Media