



NEXTCLOUD DEPLOYMENT
CLOUD INFRASTRUCTURE PROJECT

Cloud Infrastructure Project – Deploy

Next cloud on AWS

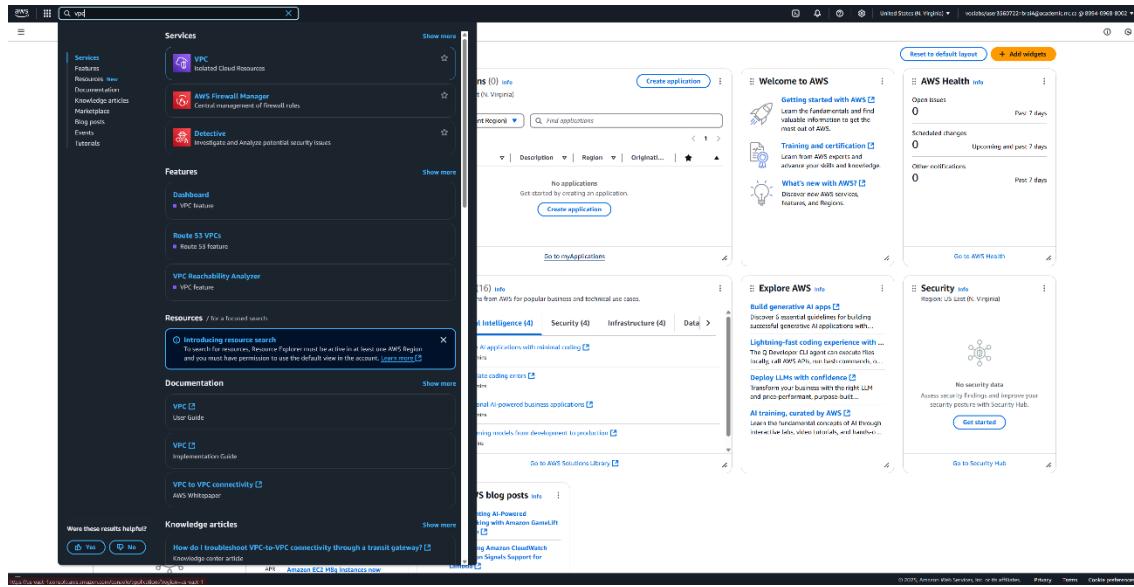
Contents

MILESTONE 1 – VPC & Security Groups	2
Creating a VPC:.....	2
Creating a NextCloud Security Group:	5
Creating an EFS Security Group:.....	7
Customize a NextCloud Security Group:	8
Milestone 2 – S3 & EFS storage – Demonstration	9
Create an elastic file system.....	10
Create S3 Bucket	14
MILESTONE 3 – EC2 Instances & Elastic IP.....	21
Creating EC2 Instance:	21
Allocating Elastic IP to EC2 Instance:	25
Create a duck DNS domain:	28
Create a CloudWatch Monitoring:	28
MILESTONE 4 – Next cloud Demonstration	33
Install Nextcloud:	33
Configure Nextcloud:	37
Creating Amazon machine Image:.....	46
Creating launch template:	47
Creating AWS Backup Plan:	48
Install and Configure desktop client:	49

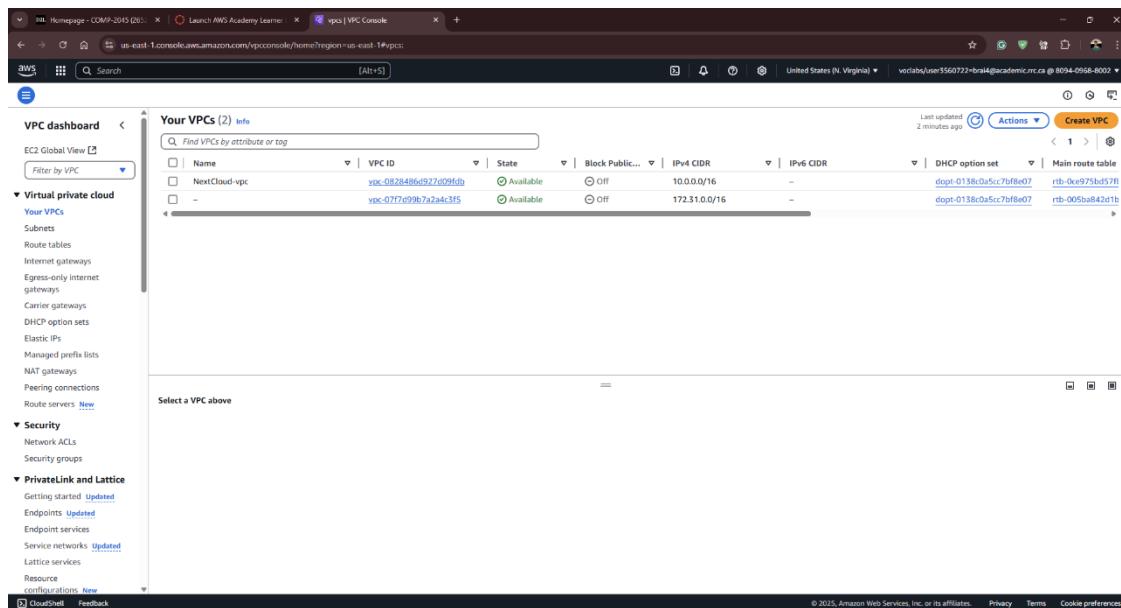
MILESTONE 1 – VPC & Security Groups

Creating a VPC:

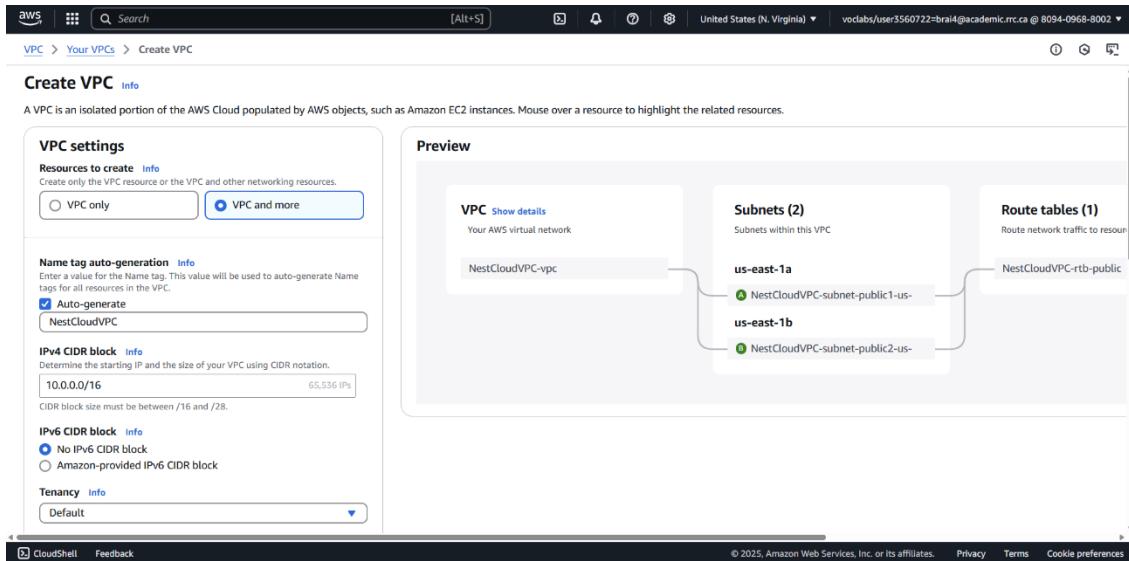
1. In the search box to the right of **Services**, search for and choose **VPC** to open the VPC console.



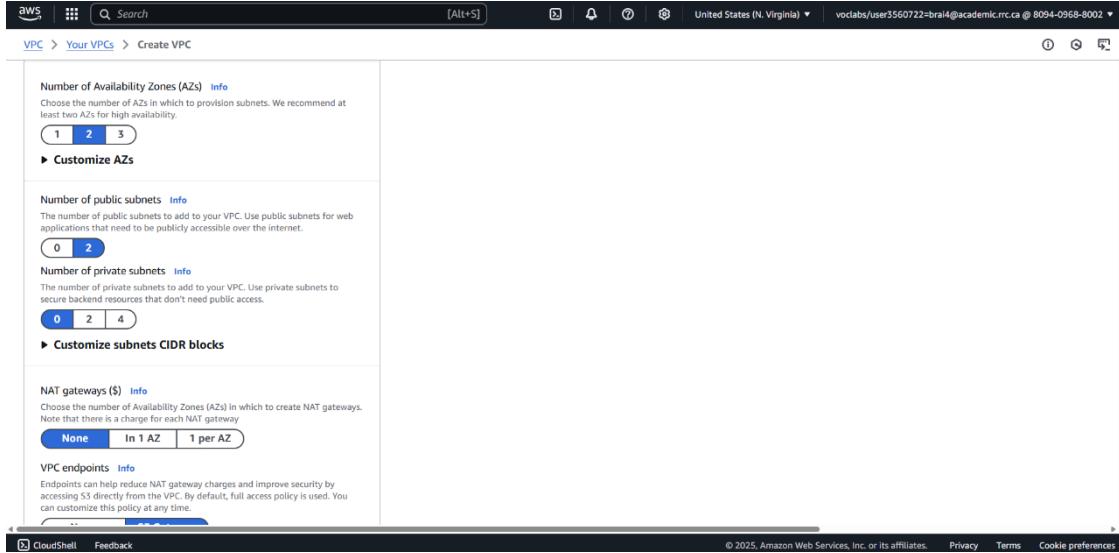
2. Choose the **VPC dashboard** link towards the console's top left.
3. Click on **Your VPC** to see all available VPCs.



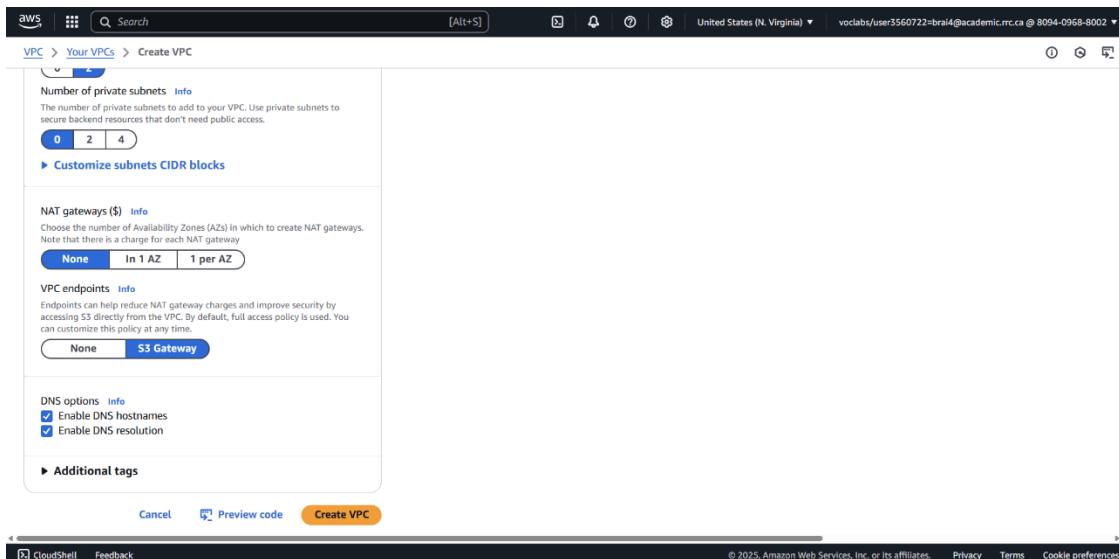
4. Next, choose **Create VPC**.
5. Configure the VPC details in the *VPC settings* panel on the left:
 - a. Choose **VPC and more**.
 - b. Under **Name tag auto-generation**, keep *Auto-generate* selected, however, change the value from project to **NextCloudVPC**.
 - c. Keep the **IPv4 CIDR block** 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**

The screenshot shows the 'Create VPC workflow' page after a successful creation. It displays a list of 17 completed steps under the 'Details' section, each with a green checkmark icon. The steps include creating the VPC, enabling DNS hostnames and resolution, verifying the creation, creating S3 endpoints, creating subnets, creating internet gateways, attaching them to the VPC, creating route tables, associating routes, and verifying route table creation. At the bottom right is a 'View VPC' button.

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

The screenshot shows the 'Your VPCs (3) Info' page in the VPC dashboard. It lists three VPCs: 'NextCloud-vpc', 'NestCloudVPC-vpc', and a third unnamed entry. The table includes columns for Name, VPC ID, State, Block Public..., IPv4 CIDR, and IPv6 CIDR. All VPCs are listed as 'Available'. The 'Actions' dropdown menu is open at the top right. The left sidebar shows navigation options like VPC dashboard, EC2 Global View, Virtual private cloud, Security, and PrivateLink and Lattice.

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
NextCloud-vpc	vpc-0828486d927d09fdb	Available	Off	10.0.0.0/16	-
NestCloudVPC-vpc	vpc-0fc6561854533ef84	Available	Off	10.0.0.0/16	-
-	vpc-07f7d99b7a2a4c3f5	Available	Off	172.31.0.0/16	-

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.

The screenshot shows the AWS VPC Security Groups page. On the left, there's a navigation sidebar with sections like Virtual private cloud, Security, and PrivateLink and Lattice. The main area displays a table of security groups with columns for Name, Security group ID, Security group name, VPC ID, and Description. The table contains five rows:

Name	Security group ID	Security group name	VPC ID	Description
sg-0a776535b85019849		NextCloudSecurityGroup	vpc-0828486d927d09fdb	NextCloud ports
sg-09a09ed4c899c8465		default	vpc-0fc6561854533cf84	default VPC securi
sg-061bcbd26d6cd828		default	vpc-07f7d99b7a2a4c3f5	default VPC securi
sg-0405c1bb7264ce3e0		EFSecurityGroup	vpc-0828486d927d09fdb	EFS ports
sg-0fad12e9b8578adbd		default	vpc-0828486d927d09fdb	default VPC securi

Below the table, there's a section titled "Select a security group".

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.

The screenshot shows the "Create security group" page. The "Basic details" section has "Security group name" set to "nextCloudSecurityGroup" and "Description" set to "Allows SSH access to developers". The "VPC Info" section has "VPC" set to "vpc-0828486d927d09fdb (NextCloud-vpc)". The "Outbound rules" section has "Type" set to "All traffic", "Protocol" set to "All", "Port range" set to "All", and "Destination" set to "Custom".

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 NextCloudSecurity Group from the Dropdown Box.

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
EFSecurityGroup
Name cannot be edited after creation.

Description Info
Allows SSH access to developers

VPC Info
vpc-0828486d927d09fdb (NextCloud-vpc)

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional
NFS	TCP	2049	Custom	sg-0a776535b8501984 sg-0a776535b85019849

Add rule

Outbound rules Info

Type	Protocol	Port range	Destination	Description - optional
CloudShell	Feedback			

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

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0a776535b85019849	NextCloudSecurityGroup	vpc-0828486d927d09fdb	NextCloud ports
-	sg-09ad9ed4899c8465	default	vpc-0fc6561854533ef84	default VPC securi
-	sg-061bc02f26d6cd828	default	vpc-0fffd99b7a2a4c3f5	default VPC securi
-	sg-0405c1bb7264ce3e0	EFSecurityGroup	vpc-0828486d927d09fdb	EFS ports
-	sg-0fad12e9b8578adbd	default	vpc-0828486d927d09fdb	default VPC securi

3. Click on the **Add rule** button.
4. Add an inbound rule for NFS (2049). Select the source as custom and select EFSecurity Group from the Dropdown Box.

The screenshot shows the 'Edit inbound rules' page in the AWS VPC console. It lists six security group rules under the 'Inbound rules' section. Each rule includes columns for Security group rule ID, Type, Protocol, Port range, Source, and Description - optional.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0d8d2275bd0bb2c46	Custom TCP	TCP	8443	Custom	Q 0.0.0.0/0
sgr-0142ef88b529ea754	HTTP	TCP	80	Custom	Q 0.0.0.0/0
sgr-0ff61aaeeeaeff1c6	SSH	TCP	22	Custom	Q 0.0.0.0/0
sgr-05e2092e8aaa7af65	NFS	TCP	2049	Custom	Q sg-0405c1bb7264ce5e0
sgr-095ae8131a2f1a0df	HTTPS	TCP	443	Custom	Q 0.0.0.0/0
sgr-0bf57626c2b7a0b93	Custom TCP	TCP	8080	Custom	Q 0.0.0.0/0

[Add rule](#)

https://us-east-1.console.aws.amazon.com/vpc/SecurityGroups?region=us-east-1

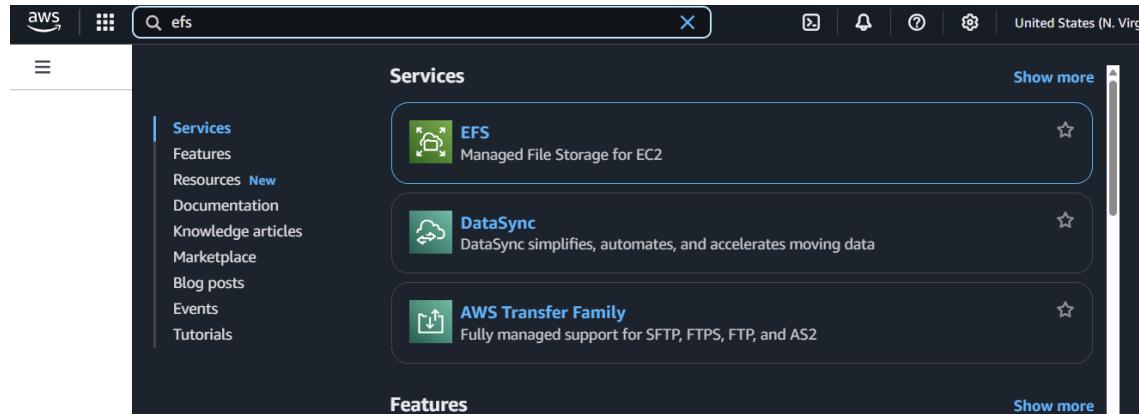
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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.

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.

Create file system

Create a file system with the recommended settings shown below by choosing Create file system. To view all settings or to customize your file system, choose Customize. [Learn more](#)

Name - optional
Name your file system.

Name can include letters, numbers, and +-=_. symbols, up to 256 characters.

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system.

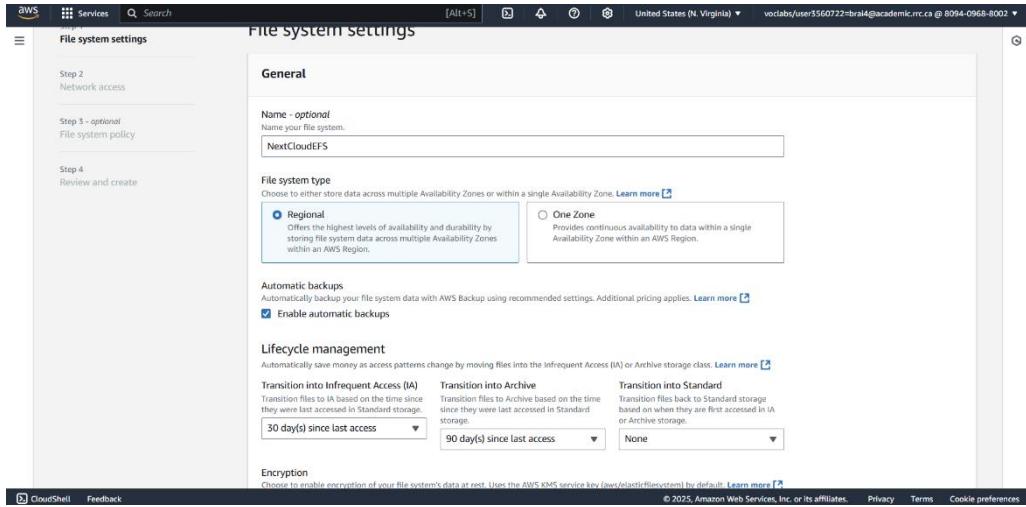
NextCloud-vpc

Recommended settings
Your file system is created with the following recommended settings unless you choose to customize the file system. You will be charged for storage and throughput. We recommend reviewing pricing for these features using the [AWS Pricing Calculator](#).

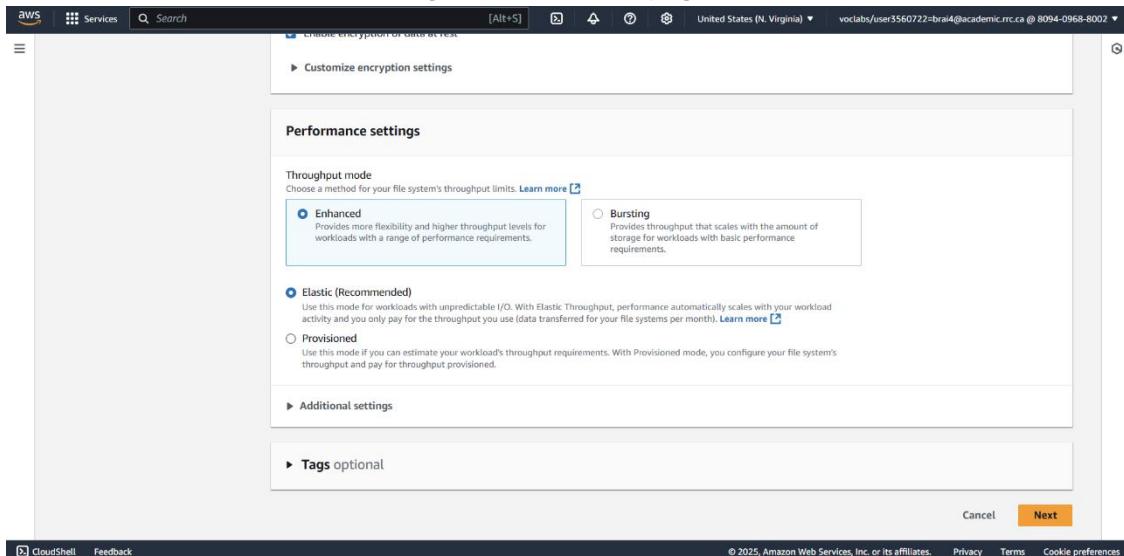
Setting	Value	Editable after creation
Throughput mode Learn more	Elastic	Yes
Transition into Infrequent Access (IA)	30 day(s) since last access	Yes
Transition into Archive	90 day(s) since last access	Yes

[Cancel](#) [Customize](#) **Create file system**

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.

Virtual Private Cloud (VPC) [Learn more](#)
Choose the VPC where you want EC2 instances to connect to your file system.
vpc-0828486d927d09fdb
NextCloud-vpc

Mount targets

Availability zone	Subnet ID	IP address	Security groups
us-east-1a	subnet-0a23f3f4a6...	Automatic	Choose security gro... sg-0fad12e9b8578adbd default
us-east-1b	subnet-04a524a67...	Automatic	Choose security gro... sg-0fad12e9b8578adbd default

Add mount target

Cancel Previous Next

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.

Amazon EFS > File systems > Create

File system policy - optional

Policy options

Select one or more of these common policy options, or create a custom policy using the editor. [Learn more](#)

- Prevent root access by default*
- Enforce read-only access by default*
- Prevent anonymous access
- Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

Grant additional permissions

Policy editor (JSON)

Clear

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel Previous Next

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

The screenshot shows the 'Review and create' step of the AWS EFS 'File system settings' creation wizard. On the left, a sidebar lists steps: Step 1 (File system settings), Step 2 (Network access), Step 3 (optional File system policy), and Step 4 (Review and create). The main area displays the 'File system' configuration:

Field	Value	Is editable?
Name	NextCloudEFS	Yes
Performance mode	General Purpose	No
Throughput mode	Elastic	Yes
Encrypted	Yes	No
KMS Key ID	-	No
Lifecycle management	Transition into Infrequent Access (IA): 30 day(s) since last access Transition into Archive: 90 day(s) since last access Transition into Standard: None	Yes
Automatic backups	Yes	Yes
VPC ID	vpc-0828486d927d09fdb (NextCloud-vpc)	Yes
Availability Zone	Regional	No

At the bottom right of the main area are 'Edit' and 'Create' buttons.

The screenshot shows the 'Step 2: Network access' and 'Step 3: File system policy' sections of the EFS creation wizard.

Step 2: Network access

Mount targets

Availability zone	Subnet	IP address	Security groups
us-east-1a	subnet-0a23f3f4a65f01fc0	-	sg-0fad12e9b8578adbd
us-east-1b	subnet-04a524a6745647869	-	sg-0fad12e9b8578adbd

Step 3: File system policy

File system policy

A small table with one row is visible, showing index 1.

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.

The screenshot shows the AWS Elastic File System (EFS) console. The left sidebar has 'File systems' and 'Access points' under 'Elastic File System'. The main area shows a table titled 'File systems (1)'. The table has columns: Name, File system ID, Encrypted, Total size, Size in Standard, Size in IA, Size in Archive, and Provisioned Throughput (MiB/s). One row is listed: 'NextCloudFS' with File system ID 'fs-0c4a7c248d244aae1', Encrypted checked, Total size 102.00 KiB, and others 0 Bytes. A 'Create file system' button is at the top right.

Create S3 Bucket

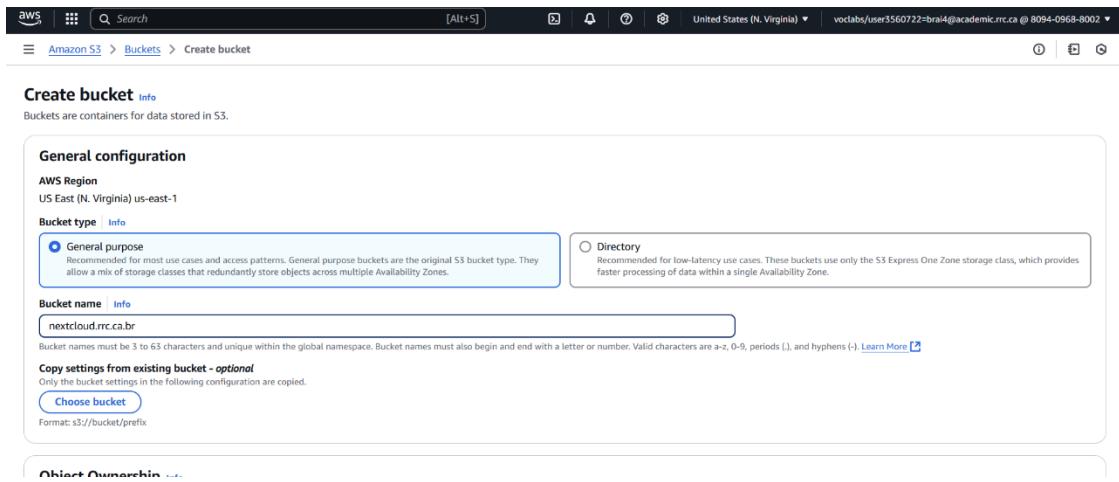
1. Click on services navigate the cursor to the search bar and look for S3.

The screenshot shows the AWS search results for 's3'. The search bar at the top has 's3'. Below it, the 'Services' section lists 'S3 Scalable Storage in the Cloud' and 'S3 Glacier Archive Storage in the Cloud'. There is also a link to 'Amazon S3 Family'.

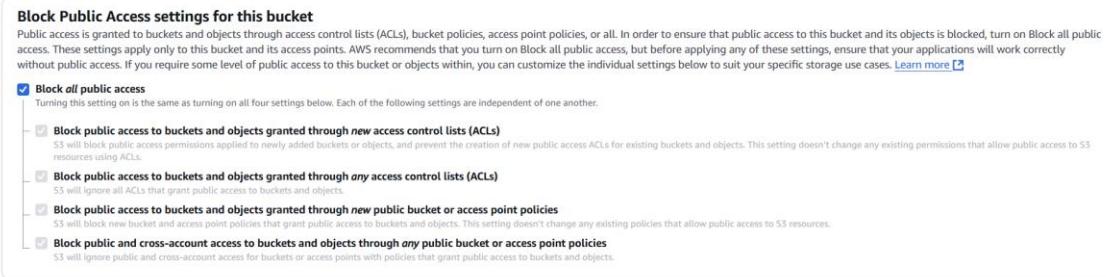
2. Click on the first link as shown in the picture. Navigate the cursor to CREATE BUCKET.

The screenshot shows the Amazon S3 console. The left sidebar has 'General purpose buckets', 'Directory buckets', 'Table buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. The main area shows a table titled 'General purpose buckets (1)'. The table has columns: ARN, Copy ARN, Empty, Delete, and Create bucket. One row is listed: 'arn:aws:s3:::NextCloudFS'. A 'View Storage Lens dashboard' button is at the top right.

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



- We will leave the other setting to default.



- From the BUCKET VERSIONING tab, make it ENABLE.

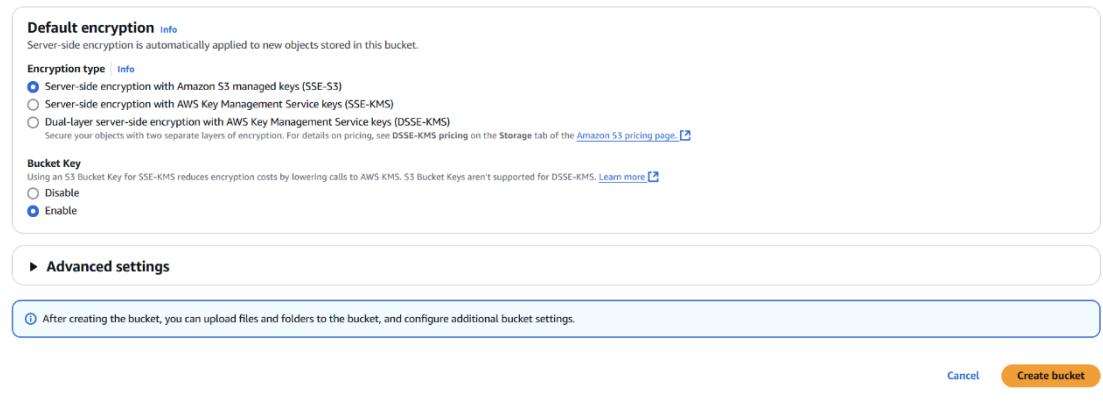
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to pre-can easily recover from both unintended user actions and application failures. [Learn more](#)

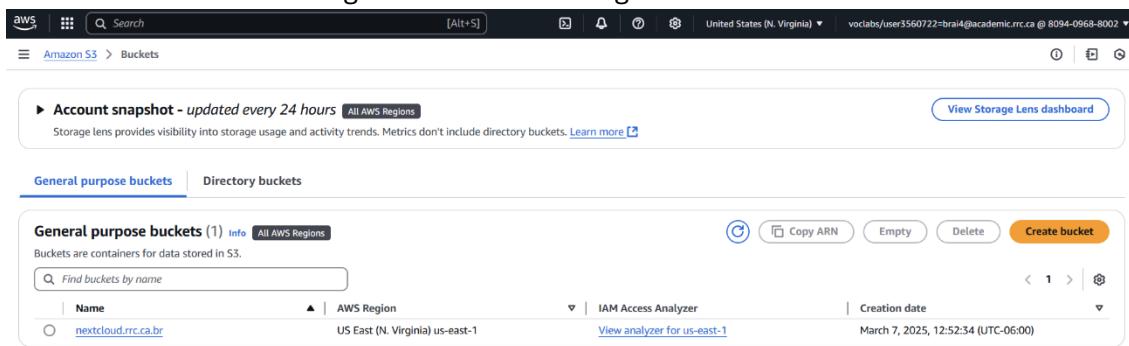
Bucket Versioning

- Disable
- Enable

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



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



8. If you are able to do 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.

nextcloud_rrc.ca.br [Info](#)

Objects | Metadata | Properties | **Permissions** | Metrics | Management | Access Points

Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access
 On
► Individual Block Public Access settings for this bucket

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.

IAM > Dashboard

IAM Dashboard [Info](#)

IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	21	6	0

What's new [View all](#)

- AWS IAM announces support for encrypted SAML assertions. *3 months ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *3 months ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *4 months ago*
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. *5 months ago*

AWS Account

Account ID [809409688002](#)
Account Alias [Create](#)
Sign-in URL for IAM users in this account [https://809409688002.signin.aws.amazon.com/console](#)

Tools [View](#)
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information [View](#)
Security best practices in IAM
IAM documentation

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

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for Identity and Access Management (IAM), Access management, and Access reports. The main content area displays a table titled 'Roles (1/21)'. The table has columns for Role name, Trusted entities, and Last activity. One role, 'LabRole', is selected and highlighted in blue. Other roles listed include AWSServiceRoleForTrustedAdvisor, c145905a377823319184088e1w80940968800-LambdaSLRRole-KGJ3EqgPWCIJL, EMR_AutoScaling_DefaultRole, EMR_DefaultRole, EMR_EC2_DefaultRole, EMR_Notebooks_DefaultRole, myRedshiftRole, RedshiftRole, RoleForLambdaModLabRole, vocareum, and vocareum-eventbridge.

15. In the lab role page copy the ARN.

The screenshot shows the AWS LabRole page. The left sidebar is identical to the previous screenshot. The main content area shows the 'LabRole' details. A green box highlights the 'ARN copied' message above the ARN field. The ARN is shown as arn:aws:iam::809409688002:role/LabRole. Below this, there are sections for Summary, Permissions, Trust relationships, Tags, Last Accessed, and Revoke sessions. The Permissions section shows 7 managed policies attached to the role.

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

The screenshot shows the 'Edit bucket policy' page in the AWS Management Console. The URL is [Amazon S3 > Buckets > nextcloud.rrc.ca.br > Edit bucket policy](#). The policy editor interface includes tabs for 'Bucket policy' (selected), 'Policy examples', and 'Policy generator'. The policy document is displayed in a code editor:

```

1 * {
2   "Version": "2012-10-17",
3   "Id": "Policy1741373763524",
4   "Statement": [
5     {
6       "Sid": "Stmt1741373763524",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": "ARN:aws:iam:809409688002:role/LabRole",
10      "Resource": "arn:aws:s3:::nextcloud.rrc.ca.br"
11    }
12  ]
13 }
14
15

```

On the right side, there are sections for 'Edit statement' (with ID Stmt1741373763524), 'Add actions' (with 'Choose a service' dropdown), and a sidebar with categories like 'Included' (S3), 'Available' (AI Operations, AMP).

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.

The screenshot shows the 'Add new statement' section of the AWS IAM Policy Generator. The JSON document is as follows:

```

+ Add new statement
JSON Ln 7, Col 14
Security: 0 Errors: 0 Warnings: 0 Suggestions: 0
Preview external access
You need permissions
User: arn:aws:sts::809409688002:assumed-role/voclabs/user3560722=brai4@academic.rrc.ca is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:809409688002:*
Diagnose with Amazon Q
Cancel Save changes

```

A red box highlights the error message: 'User: arn:aws:sts::809409688002:assumed-role/voclabs/user3560722=brai4@academic.rrc.ca is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:809409688002:*'.

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

The screenshot shows the AWS S3 console with the following details:

- Left sidebar:** Shows navigation options like General purpose buckets, Storage Lens, and Feature spotlight.
- Top bar:** Shows the AWS logo, search bar, and account information: United States (N. Virginia) and vocabs/user5560722-brai4@academic.rrc.ca @ 8094-0968-8002.
- Bucket Overview:** The bucket name is 'nextcloud.rrc.ca.br'.
- Management Tab:** Selected tab.
- Lifecycle Configuration:**
 - Default minimum object size for transitions:** All storage classes 128K.
 - Lifecycle rules (1):**

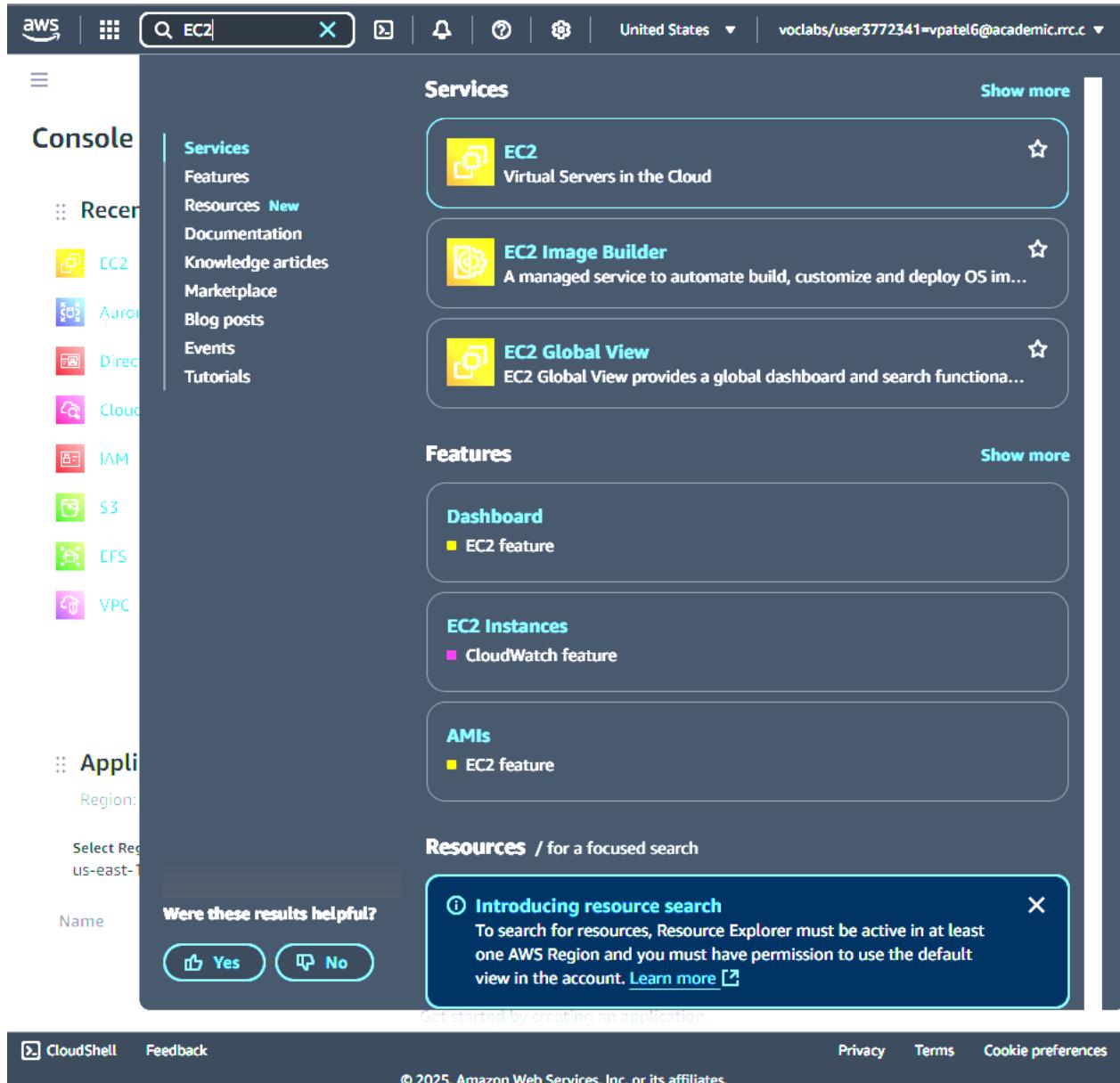
Lifecycle rule name	Status	Scope	Current version action	Noncurrent version action	Expired object action	Incomplete multi-part upload action
today-intelligentTieringRule	Enabled	Entire bucket	Transition to Intelligent	-	-	-
 - Replication rules (0):** No replication rules are present.
- Bottom right:** Copyright notice: © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

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**.



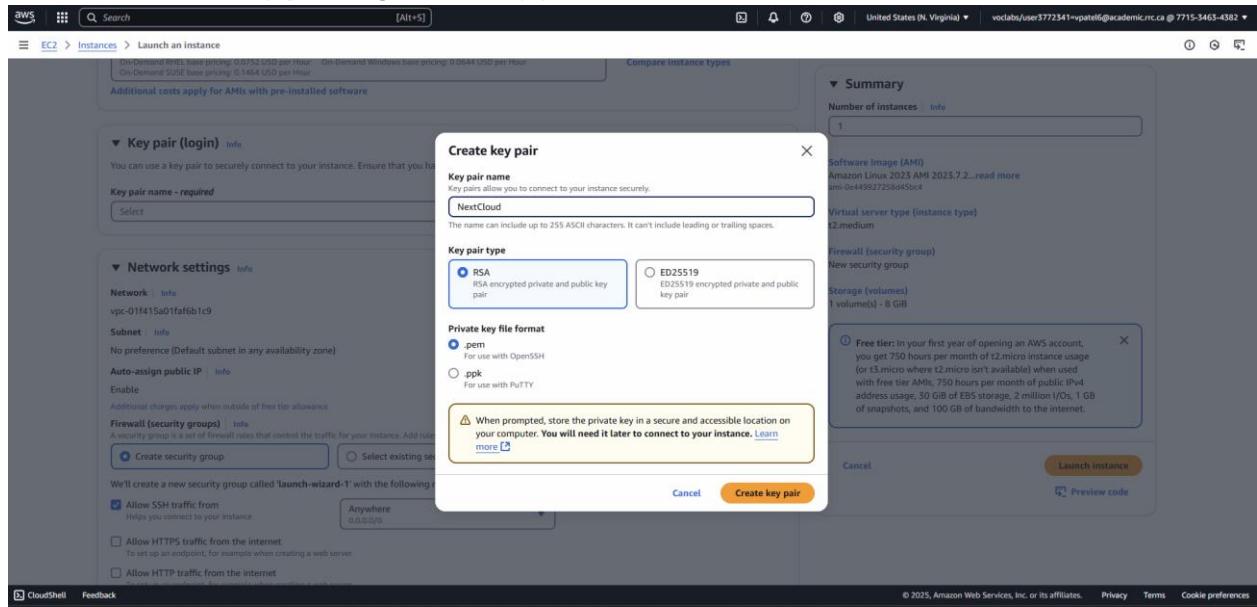
2. Choose the **instances** menu and select **Launch instance**.

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**.

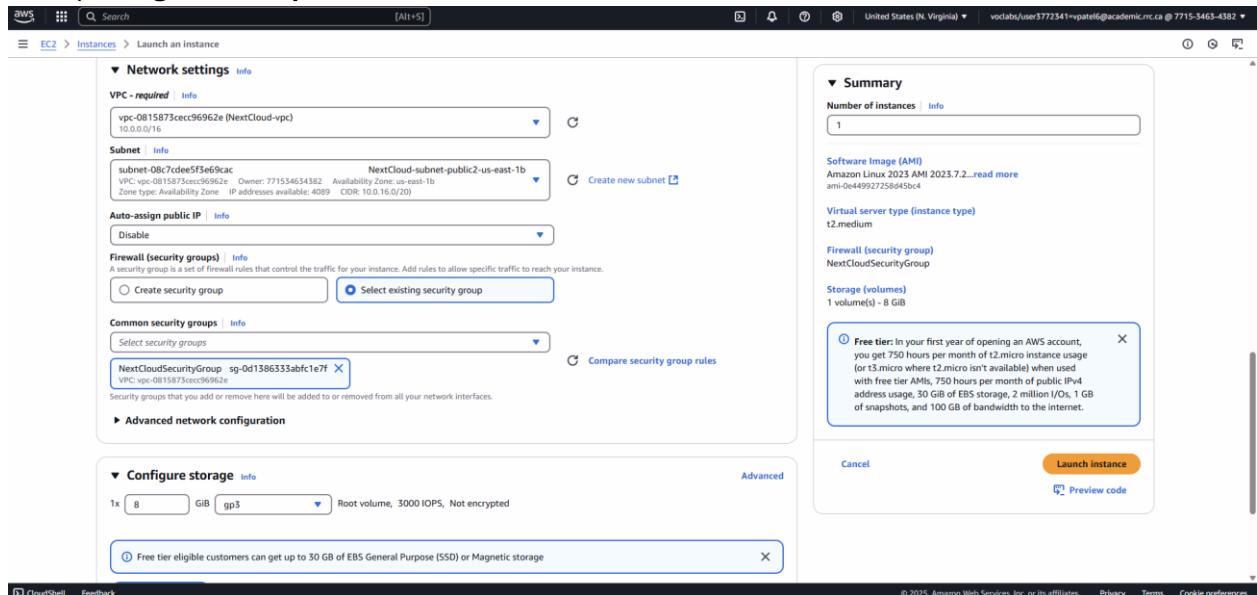
12. For **VPC**, select **NextCloud VPC**.

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.

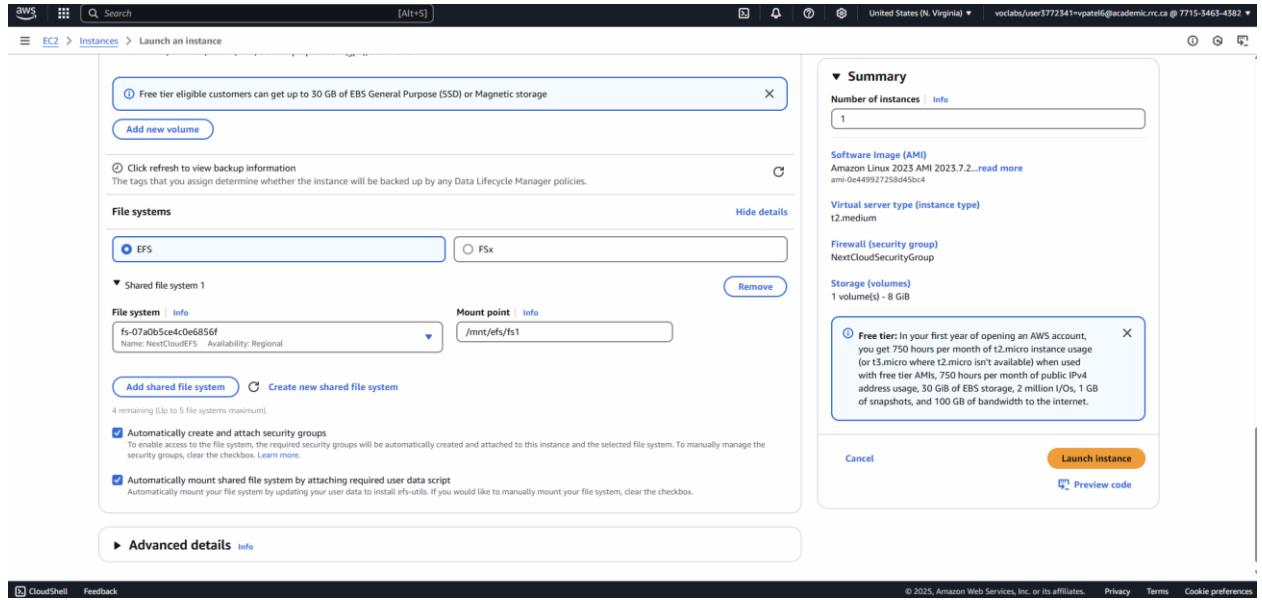


16. In the **Configure storage** section, keep the default settings.

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**.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2, Dashboard, EC2 Global View, Events, Instances (selected), Images, Elastic Block Store, Network & Security, and more. The main area displays 'Instances (1) Info' with a table showing one instance: NextCloud (Instance ID: i-0d9d48a9aa3f4e80b, State: Running, Type: t2.medium). There are buttons for Launch instances, Connect, Instance state, Actions, and a search bar.

	Name	Instance ID	Instance state	Instance type
<input type="checkbox"/>	NextCloud	i-0d9d48a9aa3f4e80b	Running	t2.medium

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.

Elastic IP address settings

Public IPv4 address pool

- Amazon's pool of IPv4 addresses
- Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
- Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)
- Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group

us-east-1

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tag

Actions

[Allocate](#)

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

Elastic IP addresses (1/1)

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associate
3.231.178.149	Public IP	eipalloc-0c499e604b8baa0f9	-	-	Associate

3.231.178.149

Summary

Associated instance ID

Allocation ID

Scope

Reverse DNS record

Private IP address

Actions

[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.

Elastic IP address: 3.231.178.149

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance
 Network interface

Reassociation
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.
 Allow this Elastic IP address to be reassigned

Associate

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

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address
3.231.178.149	3.231.178.149	Public IP	eipalloc-0c499e604b8ba0f9	-	i-0d9d48a9aa3f4e80b	10.0.21.244

Summary

Allocated IPv4 address 3.231.178.149	Type Public IP	Allocation ID eipalloc-0c499e604b8ba0f9	Reverse DNS record -
Association ID eipassoc-0c29c7c8f94781307	Scope VPC	Associated instance ID i-0d9d48a9aa3f4e80b	Private IP address 10.0.21.244
Network interface ID eni-0954d19aa1700144f	Network interface owner account ID 77154654382	Public DNS ec2-3-231-178-149.compute-1.amazonaws.com	NAT Gateway ID -
Address pool Amazon	Network border group us-east-1		

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.

The screenshot shows the Duck DNS homepage. At the top, there's a navigation bar with links for 'Duck DNS', 'spec', 'about', 'why', 'install', 'faqs', and 'logout'. To the right, it says 'logged in with vrajapatel0912@gmail.com |||'. Below the navigation is a large yellow rubber duck icon. To its right, account details are displayed: 'account vrajapatel0912@gmail.com', 'type free', 'token fb849d09-8000-4655-aa9a-124995a34270', 'token generated 1 month ago', and 'created date 10 Mar 2025, 16:05:27'. Below this is a table titled 'domains' with one entry:

domain	current ip	ipv6	changed
nextcloudrrckuchbhi	3.231.178.149	update ip	update ipv6 1 month ago

Below the table, there's a note: 'This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.' At the bottom, there are links for 'Donate', 'Bitcoin' (with a QR code), 'patreon', 'Terms of Use', and 'Privacy Statement'.

Create a CloudWatch Monitoring:

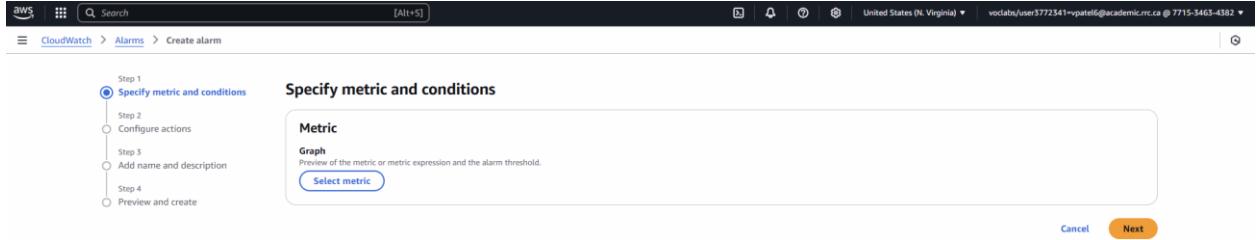
1. In the **AWS Management Console** choose **Services**, choose **Computer** and then choose **CloudWatch**.

The screenshot shows the AWS CloudWatch homepage. On the left, there's a sidebar with links for Services, Favorites and Dashboards, AI Operations, Alarms, Logs, Metrics, X-Ray traces, Events, Application Signals, Network Monitoring, Insights, Settings, Telemetry config, Getting Started, and What's new. The main content area has sections for Services (CloudWatch, Athena, Amazon EventBridge), Features (Create a SFTP server, CloudWatch dashboard, Data sources), and Resources (Introducing resource search). A message at the bottom asks if the results were helpful, with 'Yes' and 'No' buttons. At the bottom right, there are links for Documentation, Configure Application Insights, and a feedback button.

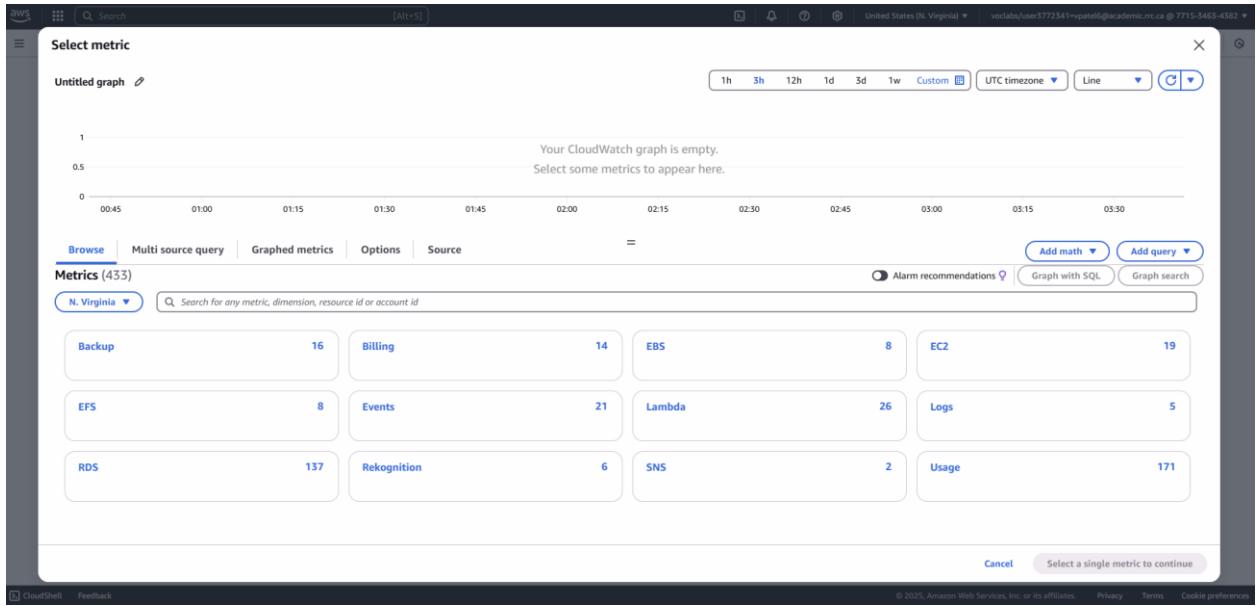
2. Select alarms on the left-hand menu, the click **Create alarm**.

The screenshot shows the AWS CloudWatch Alarms page. The left sidebar includes links for CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms (with a count of 0), All alarms, Billing, Logs, Metrics, X-Ray traces, Events, Application Signals, Network Monitoring, and Insights. The main area displays a table titled 'Alarms (1)' with one entry: 'NextCloudMonitoring' (OK, last updated 2025-04-25 03:33:17, condition: StatusCheckFailed >= 1 for 1 datapoints within 5 minutes, actions: Actions enabled Warning). There are filters for Hide Auto Scaling alarms, Clear selection, Create composite alarm, Actions, and a 'Create alarm' button. Navigation controls for pages 1 and 2 are also present.

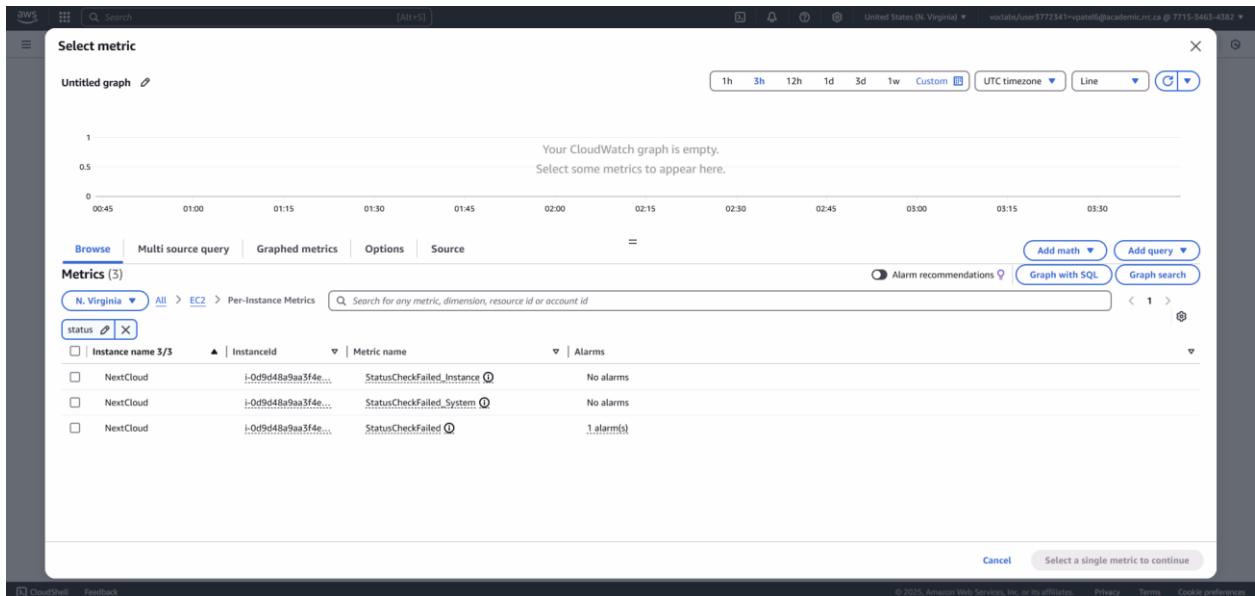
3. Click on **Select metric**



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.

The screenshot shows the 'Configure actions' step of the CloudWatch Create alarm wizard. On the left, a vertical navigation bar lists four steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). Step 2 is currently selected and highlighted in blue.

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN to notify other accounts

Send a notification to...

Q NextCloudHealth X

Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Email (endpoints)
Topic has no endpoints - View in SNS Console

Add notification

Lambda action

Add Lambda action

Auto Scaling action

10. Click **next**.

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

The screenshot shows the 'Add name and description' step of the CloudWatch Create alarm wizard. On the left, the same vertical navigation bar is present, with Step 3 (Add name and description) now highlighted in blue.

Add name and description

Name and description

Alarm name
NextCloudMonitor

Alarm description - optional [View formatting guidelines](#)

Edit | Preview

This is an H1
*double asterisks will produce strong character**
This is [an example][https://example.com/] inline link.

Up to 1024 characters (0/1024)

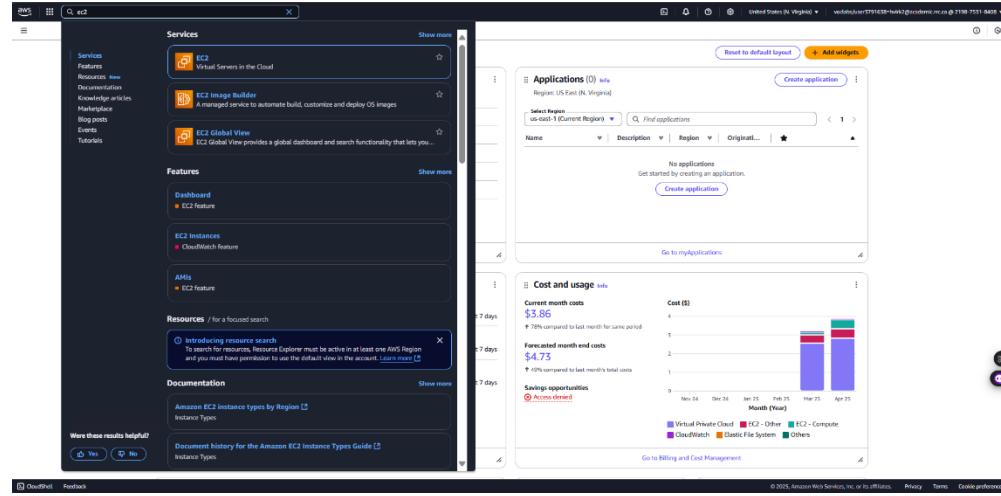
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel Previous Next

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.

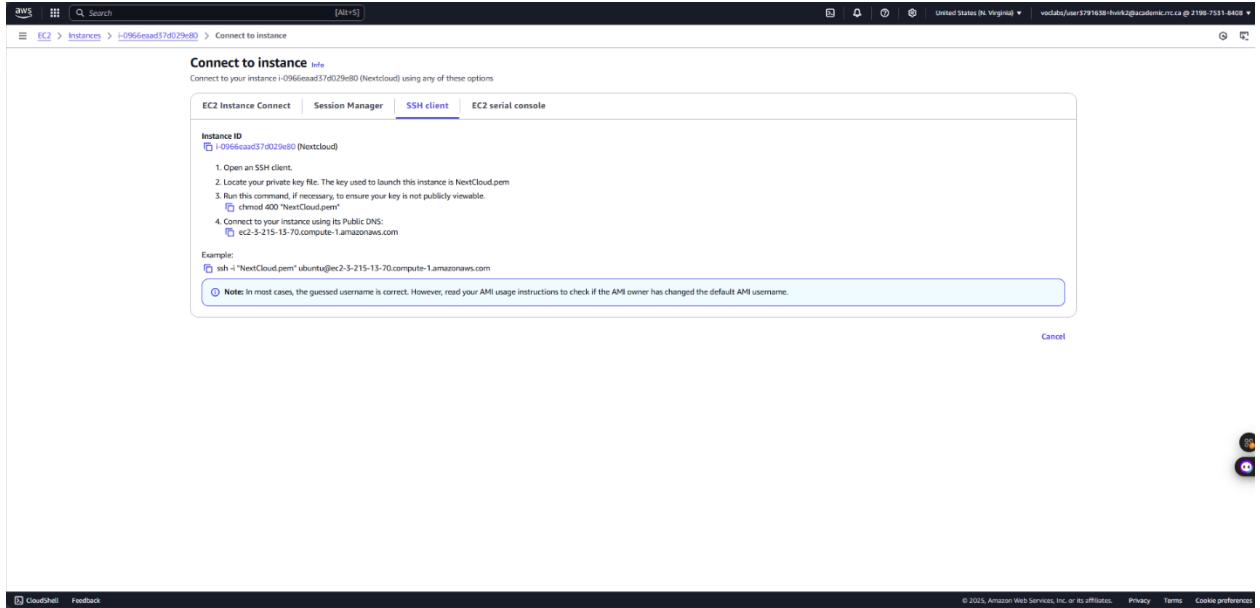


The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main area displays a table titled 'Instances (1) Info' with one row. The row details are: Name (Nextcloud), Instance ID (i-0966ead37d029e80), Instance state (Running), Instance type (t2.medium), Status check (Initializing), Availability Zone (us-east-1b), Public IPv4 DNS (ec2-3-215-15-70.compute-1.amazonaws.com), Public IPv4 (3.215.15.70), Elastic IP (3.215.15.70), IPv6 IPs (disabled), Monitoring (disabled), and Security (NextCloud). Below the table, a dropdown menu says 'Select an instance'.

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

The screenshot shows the AWS EC2 Instance summary page for the instance i-0966ead37d029e80. The summary card contains various details: Instance ID (i-0966ead37d029e80), Public IPv4 address (3.215.15.70), Instance state (Running), Private IP DNS name (ip-10-0-26-203.ec2.internal), Instance type (t2.medium), VPC ID (vpc-09788fa10fb237c72), Subnet ID (subnet-049ea078ee1a20a6c), Instance ARN (arn:aws:ec2:us-east-1:219875318408:instance/i-0966ead37d029e80), IAM Role (LambdaRole), and Auto Scaling Group name (Managed). The 'Details' tab is selected, showing sections for Instance details, Monitoring, Networking, Storage, and Tags. The 'Monitoring' section indicates it is disabled. The 'Networking' section shows the instance has a private IP of 10.0.26.203 and is connected to a subnet in the us-east-1b availability zone. The 'Storage' section shows the instance is using an EBS volume. The 'Tags' section is empty. The 'Platform details' section indicates the instance is a Linux/UNIX server. The 'Termination protection' is set to 'Disabled'. The 'AMI location' is listed as 'amazon/ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20250115'. The 'Lifecycle' is set to 'normal'. The 'Stop/hibernate behavior' is 'Disabled'. The 'State transition reason' is also 'Disabled'. The 'Connect' button is located in the top right corner of the summary card.

4. For connect to the instance, select the SSH client and copy the “**ssh -l "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.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\harsh> cd downloads
PS C:\Users\harsh\downloads> ssh -i "NextCloud.pem" ubuntu@ec2-3-215-13-70.compute-1.amazonaws.com

```

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.

```

ubuntu@ip-10-0-26-203: ~ + ~
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Apr 24 17:40:53 2025 from 142.161.138.216
ubuntu@ip-10-0-26-203:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND           CREATED          STATUS          NAMES
PORTS

```

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

```

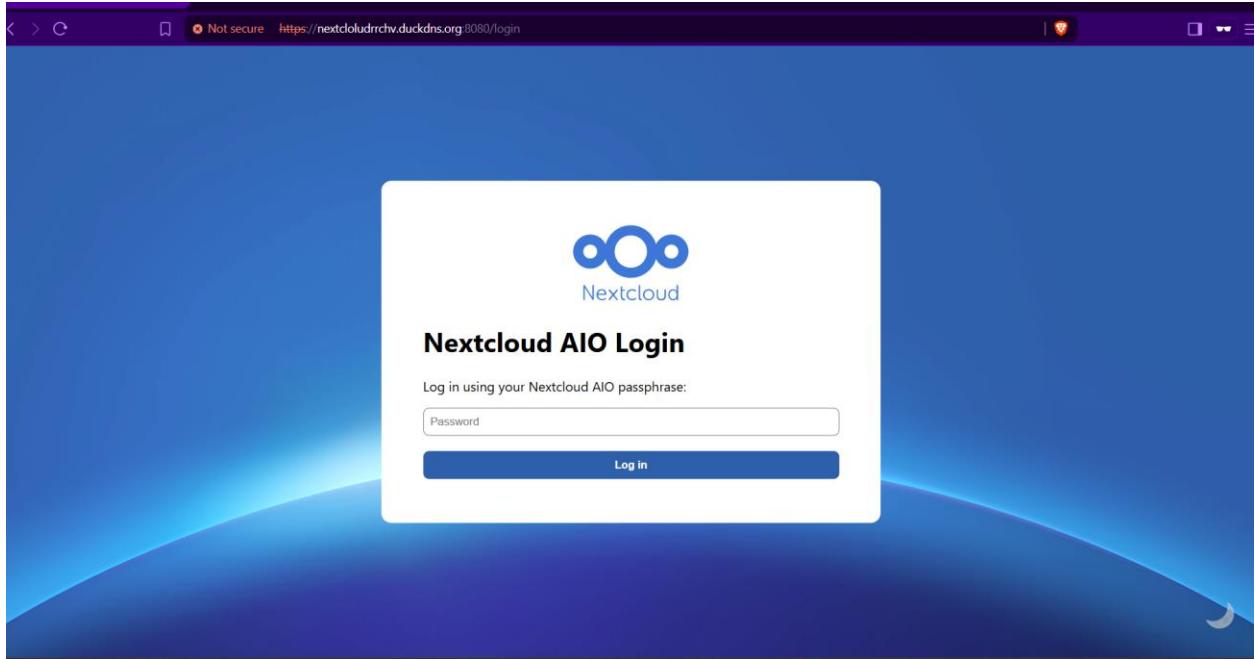
# For Linux and without a web server or reverse proxy (like Apache, Nginx,
Cloudflare Tunnel and else) already in place:
sudo docker run \
--init \
--sig-proxy=false \
--name nextcloud-aio-mastercontainer \
--restart always \
--publish 80:80 \
--publish 8080:8080 \
--publish 8443:8443 \
--volume nextcloud_aio_mastercontainer:/mnt/docker-aio-config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

Please note: Make sure to save your changes by clicking **Save changes** below the list of optional containers. The changes will not be auto-saved.

- ClamAV (Antivirus backend for Nextcloud, only supported on x64, needs ~1GB additional RAM)
- Collabora (Nextcloud Office)
- Fulltextsearch (needs ~1GB additional RAM. **Please note:** the initial indexing can take a long time during which Nextcloud will be unavailable)
- Imaginary (for previews of heic, heif, illustrator, pdf, svg, tiff and webp. Imaginary is currently [incompatible with server-side-encryption](#))
- Nextcloud Talk (needs ports 3478/TCP and 3478/UDP open/forwarded in your firewall/router)
- Nextcloud Talk Recording-server (needs Nextcloud Talk being enabled and ~1GB additional RAM ~2 additional vCPUs)
- Docker Socket Proxy (needed for [Nextcloud App API](#))
- Whiteboard

Save changes

Minimal system requirements: When any optional container is enabled, at least 2GB RAM, a dual-core CPU and 40GB system storage are required. When enabling ClamAV, Nextcloud Talk Recording-server or Fulltextsearch, at least 3GB RAM are required. For Talk Recording-server additional 2 vCPUs are required. When

Changes.

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

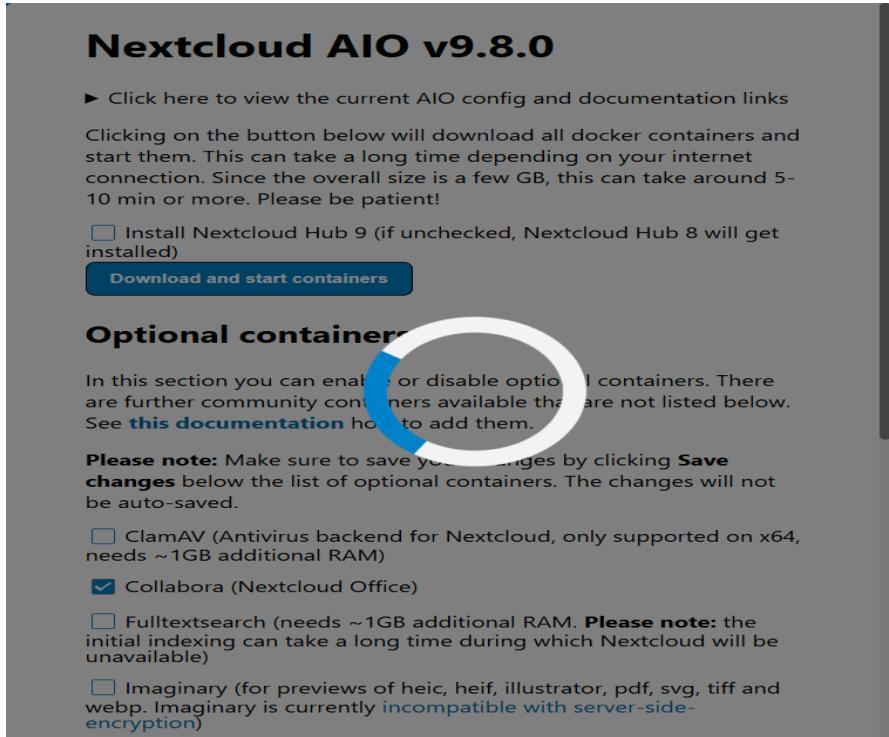
Timezone change

To get the correct time values for certain Nextcloud features, set the timezone for Nextcloud to the one that your users mainly use. Please note that this setting does not apply to the mastercontainer and any backup option.

You can configure the timezone for Nextcloud below:

You need to make sure that the timezone that you enter is valid. An example is **Europe/Berlin**. You can get valid values by looking at the 'TZ identifier' column of this list: [click here](#). The default is **Etc/UTC** if nothing is entered.

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



Nextcloud AIO v9.8.0

- ▶ Click here to view the current AIO config and documentation links

Clicking on the button below will download all docker containers and start them. This can take a long time depending on your internet connection. Since the overall size is a few GB, this can take around 5-10 min or more. Please be patient!

Install Nextcloud Hub 9 (if unchecked, Nextcloud Hub 8 will get installed)

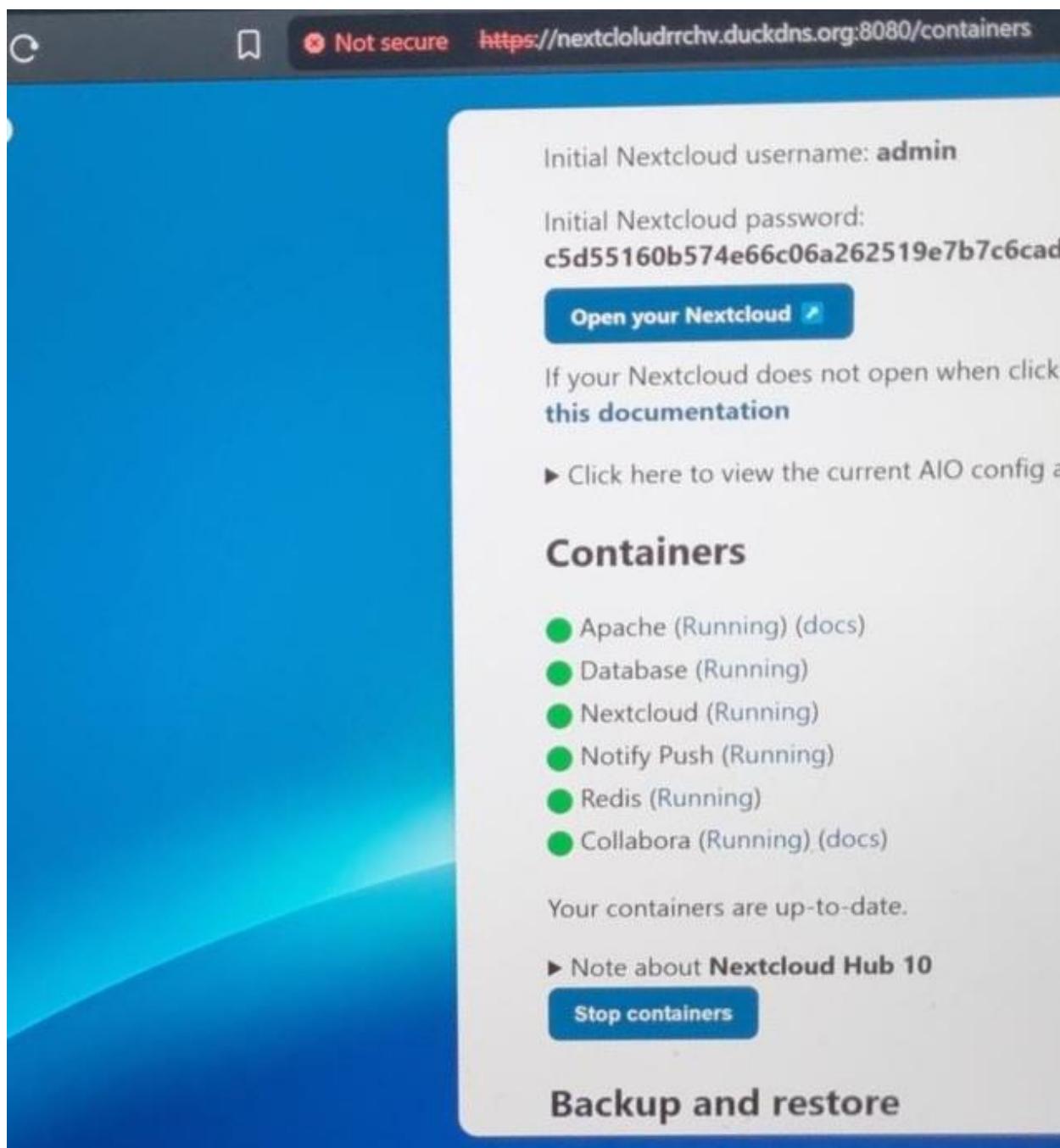
Optional containers

In this section you can enable or disable optional containers. There are further community containers available that are not listed below. See [this documentation](#) how to add them.

Please note: Make sure to save your changes by clicking **Save changes** below the list of optional containers. The changes will not be auto-saved.

- ClamAV (Antivirus backend for Nextcloud, only supported on x64, needs ~1GB additional RAM)
- Collabora (Nextcloud Office)
- Fulltextsearch (needs ~1GB additional RAM. **Please note:** the initial indexing can take a long time during which Nextcloud will be unavailable)
- Imaginary (for previews of heic, heif, illustrator, pdf, svg, tiff and webp. Imaginary is currently [incompatible with server-side-encryption](#))

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](#)

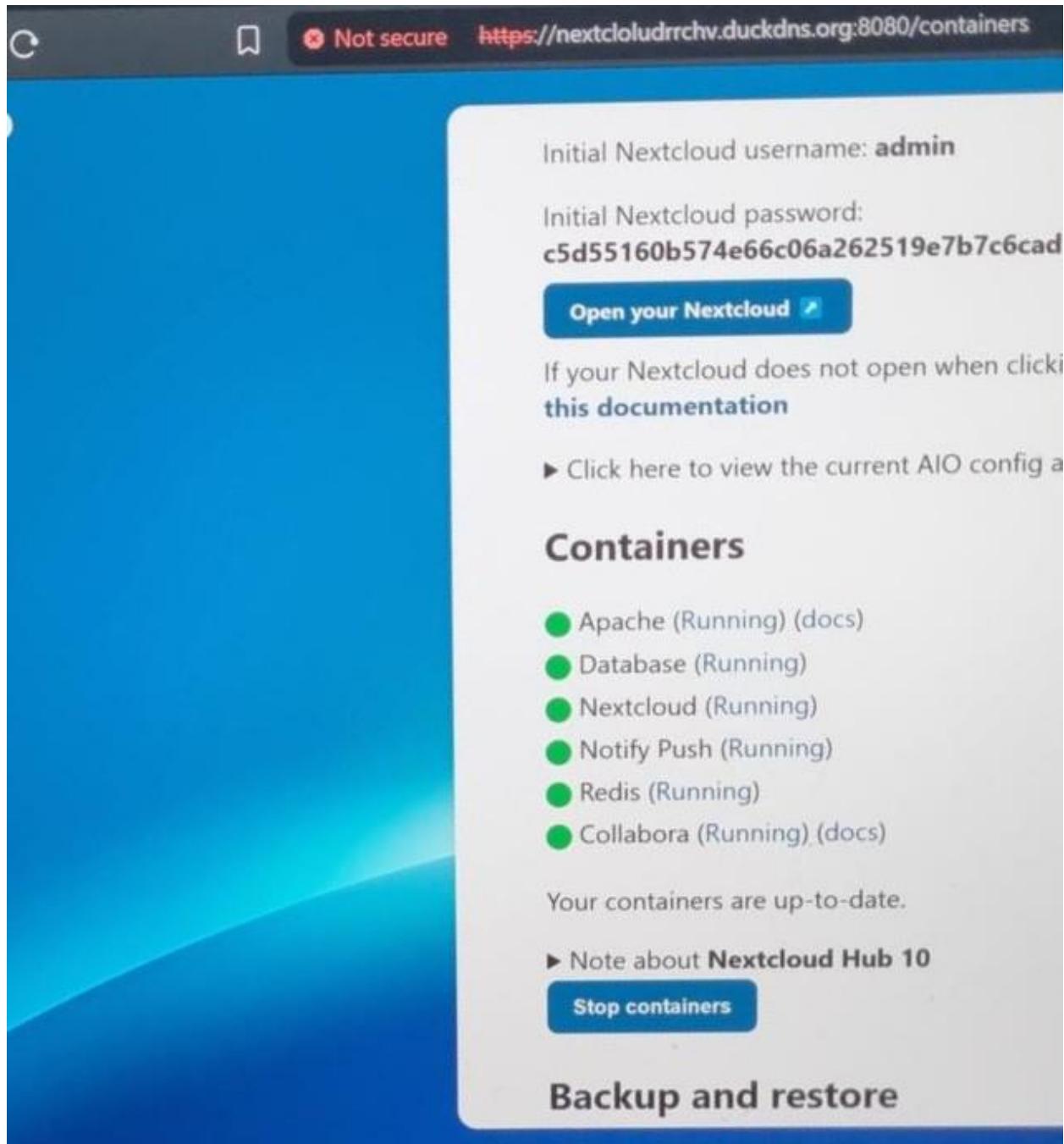
The folder path that you enter must start with **/** and must **not** end with **/**.

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.

Nextcloud AIO v9.8.0

You are running the **latest** channel. ([Logs](#))

- ▶ Click here to reveal the initial Nextcloud credentials

[Open your Nextcloud ↗](#)

- ▶ Click here to view the current AIO config and documentation links

Containers

- Apache ([Running](#))
- Database ([Running](#))
- Nextcloud ([Running](#))
- Notify Push ([Running](#))
- Redis ([Running](#))
- Collabora ([Running](#))

Your containers are up-to-date.

[View All Container Status ↗](#)

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.

Rating <https://nextcloudrchv.duckdns.org>

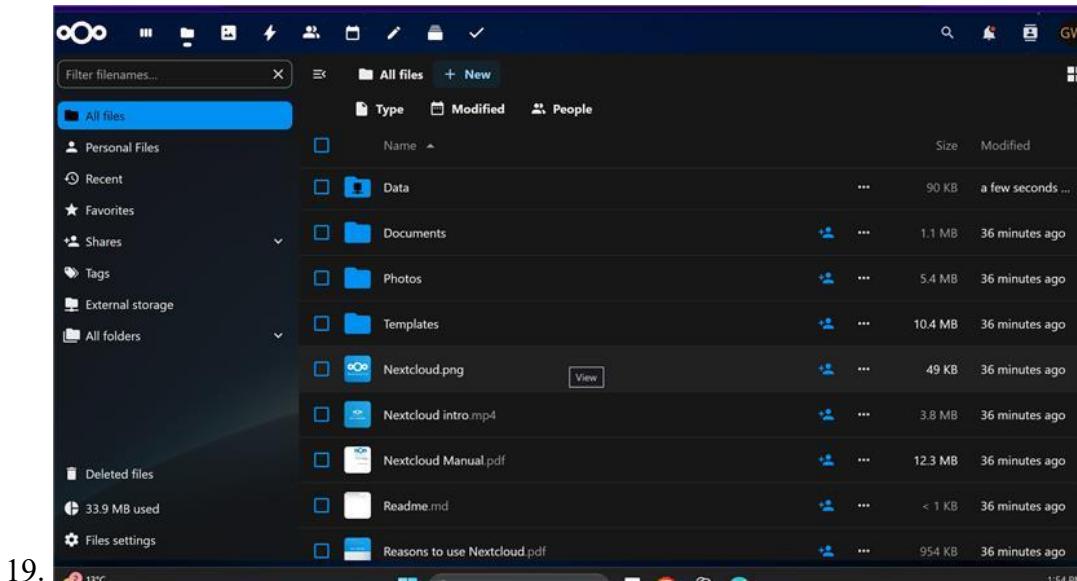
A+

Running Nextcloud 30.0.10

- ✓ Latest patch level
- ✓ Major version still supported

Scanned at 2025-04-24 18:09:55 [Trigger re-scan](#)

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**.

New account X

Account name (required) —
Group

Display name —
Group Work

Either password or email is required

Password —
Group@11223344 (Q)

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

23.

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.

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID i-0966ead37d027e0f0 (Nextcloud)

Image name Maximum 127 characters. Can't be modified after creation.

Image description - optional Maximum 255 characters.

Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/sda1	Create new snapshot from v...	16	EBS General Purpose SSD	3000	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add volume

During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Tag image and snapshots together
Tag the image and the snapshots with the same tag.

Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Create image

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

Amazon Machine Images (AMIs) (1) Info

Owned by me

Name	AMI name	AMI ID	Source	Owner	Visibility	Status	Creation date	Platform	Root
NextcloudAMI	ami-090c224654d2dd71a	21987518408/NextcloudAMI	21987518408	Private	Available	2025/04/24 13:23 GMT-5	Linux/UNIX	ebs	

Select an AMI

Creating launch template:

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

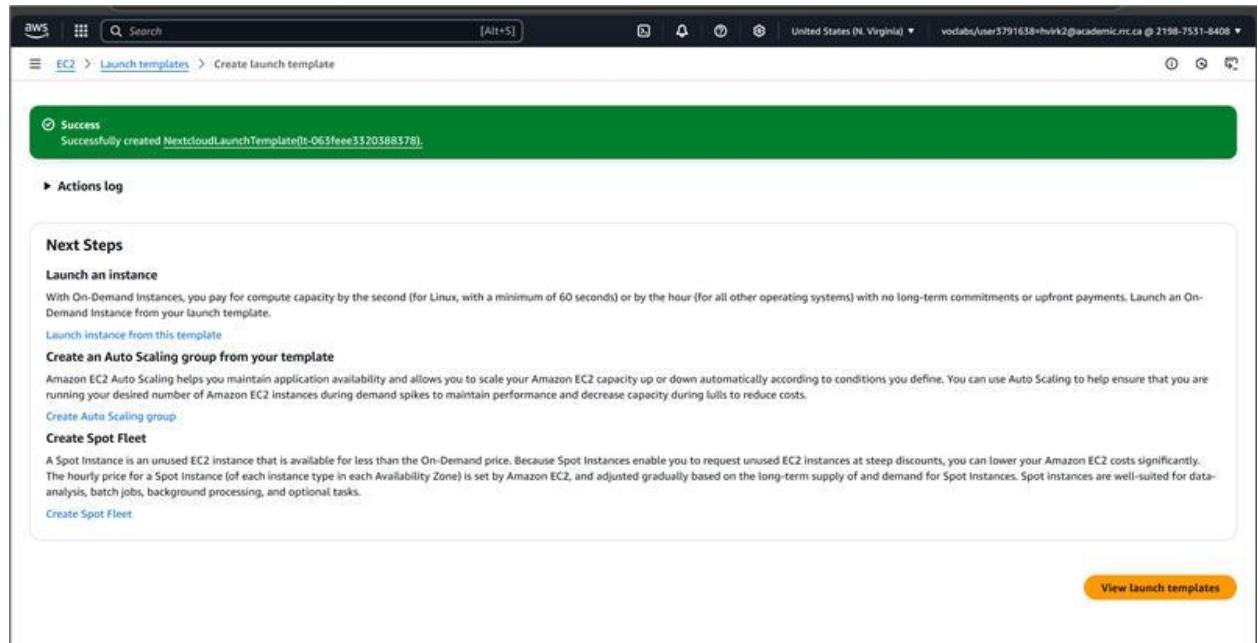
The screenshot shows the 'Create launch template' wizard on the AWS Management Console. The current step is 'Launch template name and description'. The 'Launch template name - required' field contains 'NextcloudLaunchTemplate'. The 'Template version description' field contains 'A prod webserver for MyApp'. Under 'Auto Scaling guidance', there is a checkbox 'Select this if you intend to use this template with EC2 Auto Scaling'. Below the main form, there are sections for 'Template tags' and 'Source template'. On the right side, there is a summary panel with the following details:

- Software Image (AMI):** NextcloudAMI ami-09062246d4d2dd71a
- Virtual server type (instance type):** t2.medium
- Firewall (security group):** nextCloudSecurityGroup
- Storage (volumes):** 1 volume(s) - 16 GiB
- Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

At the bottom right of the wizard, there are 'Cancel' and 'Create launch template' buttons.

- 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.

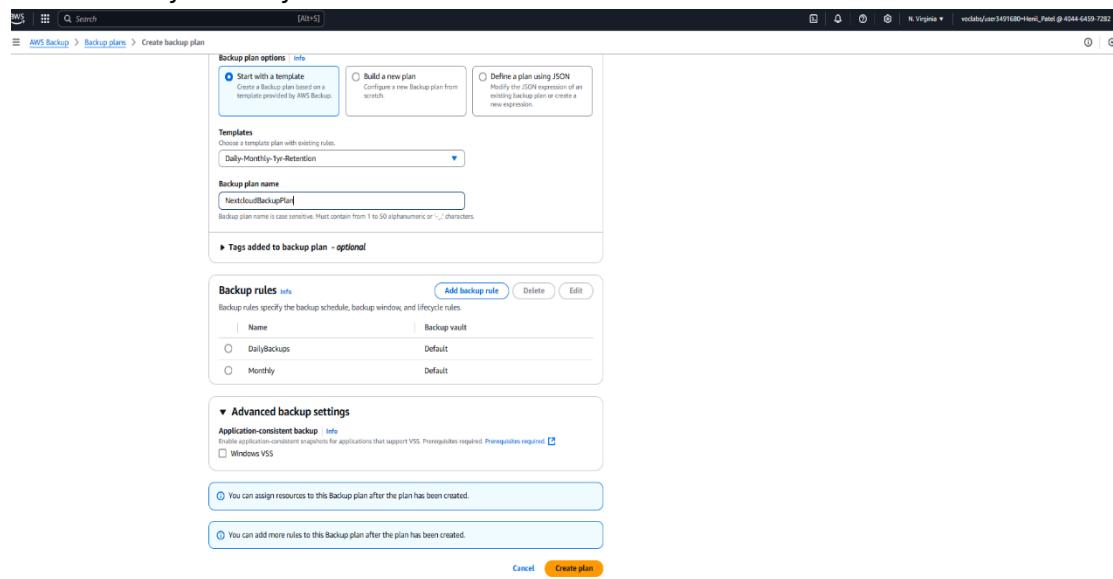
10. Click on Create lunch template.



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.

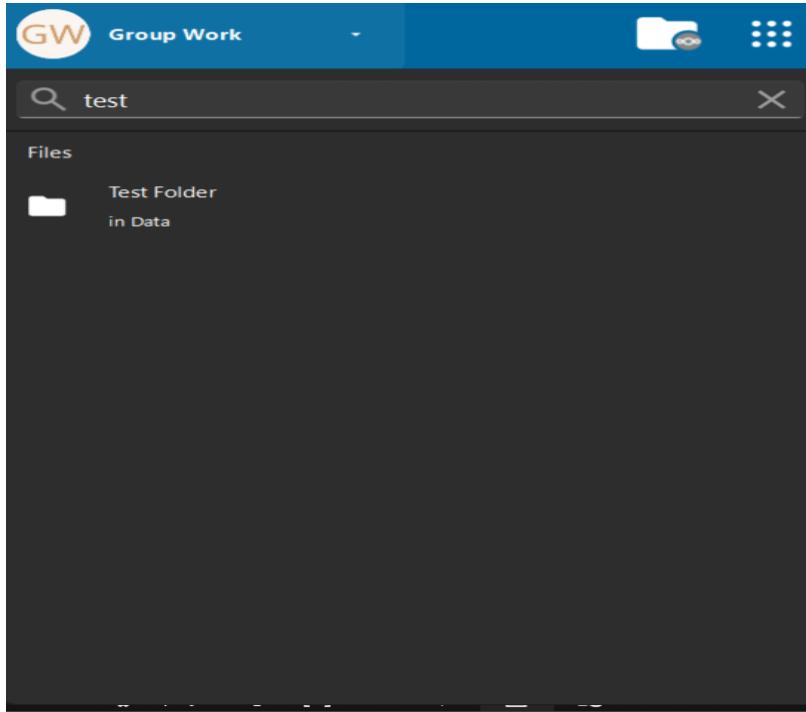


5. Click on the create plan button.

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 default.
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**.

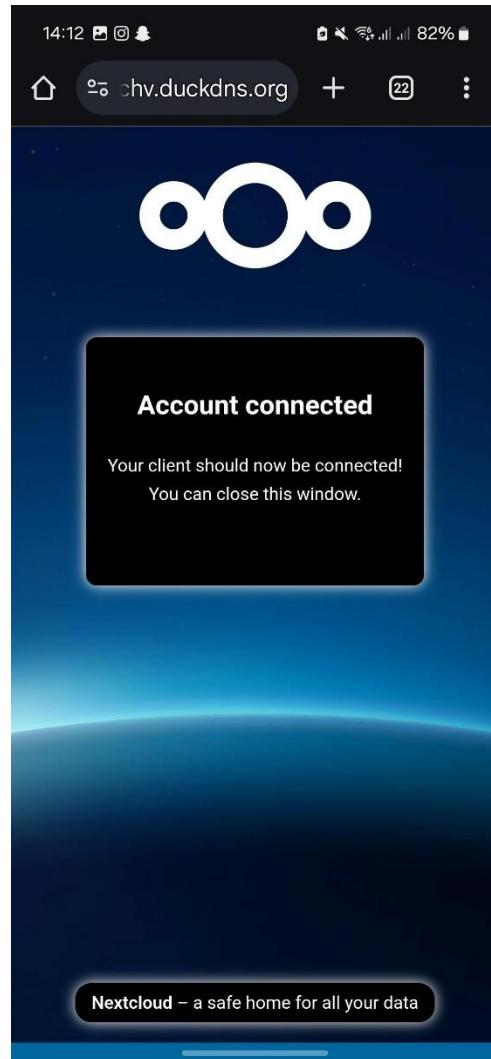
Enter your account name or email and password.

Tap **Log in**.



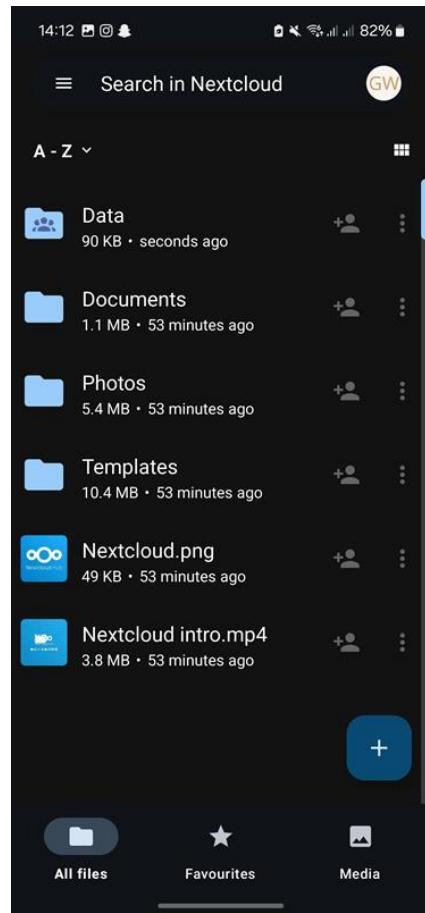
5. Grant Access

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

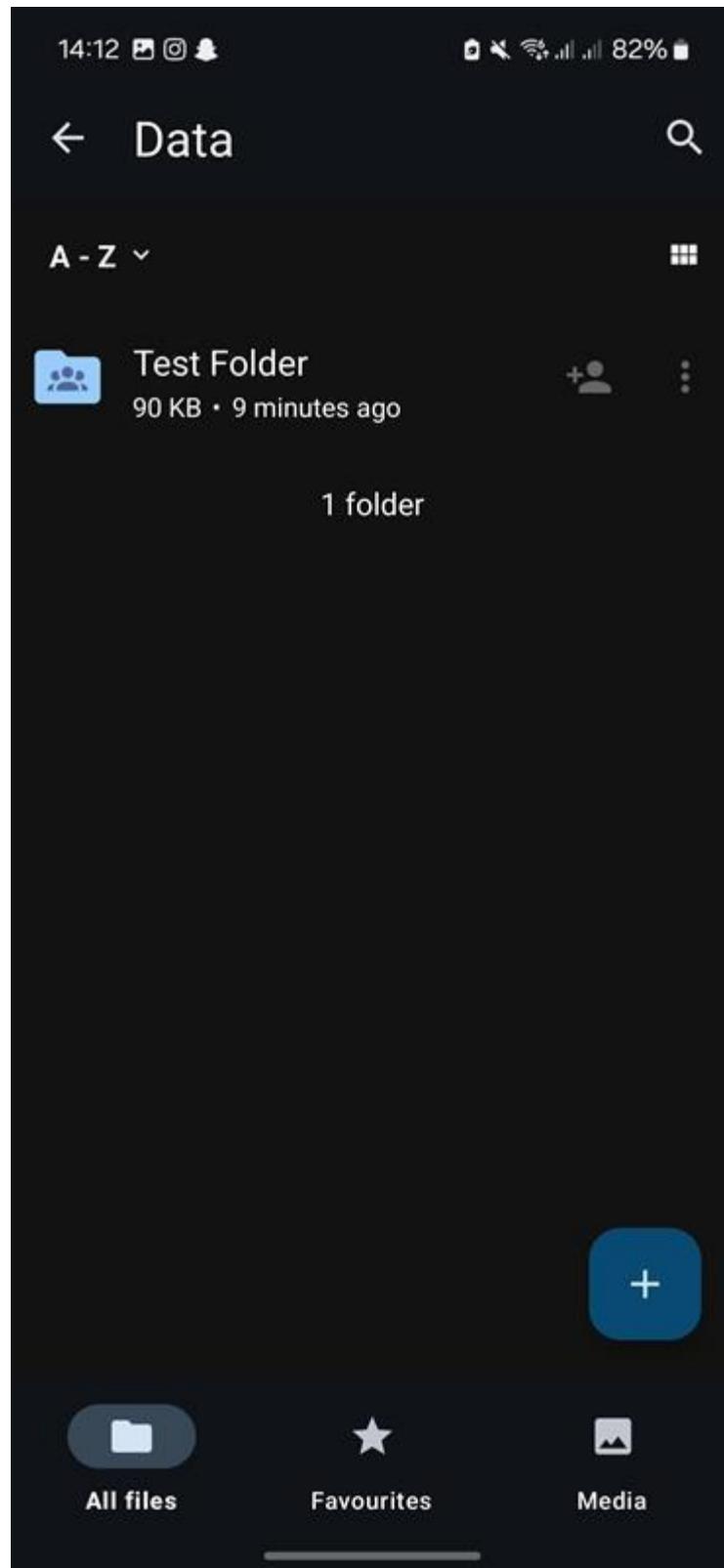


6. Return to App

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.

