

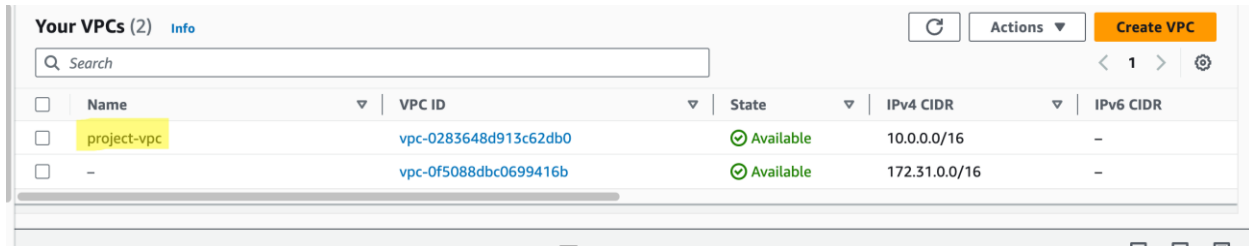
## Webserver

### Table of Contents

<b>VPC Creation .....</b>	<b>2</b>
<i>NextCloud Security Group Creation.....</i>	<i>3</i>
<b>EFS Storage and S3 bucket creation .....</b>	<b>4</b>
<i>Step 1: Create EFS Storage .....</i>	<i>4</i>
<i>Step 2: Create an S3 Bucket.....</i>	<i>5</i>
<i>Step 3: S3 Policy Generation.....</i>	<i>6</i>
<i>Step 4: S3 Lifecycle Rule Configuration .....</i>	<i>7</i>
<b>Creation of EC2 .....</b>	<b>7</b>
<b>Creation of elastic IP .....</b>	<b>9</b>
<i>Create a Duck DNS domain .....</i>	<i>9</i>
<i>Configure CloudWatch Monitoring .....</i>	<i>10</i>
<b>Install NextCloud.....</b>	<b>10</b>
<b>Configure Nextcloud .....</b>	<b>13</b>
<i>Backup Setup.....</i>	<i>13</i>
<i>Log In to Nextcloud .....</i>	<i>14</i>
Enable External Storage Support .....	15
Security Scan .....	15
S3 bucket set up on nextcloud .....	17
<i>NextCloud New User Creation.....</i>	<i>19</i>
<b>Create Image &amp; Launch Template .....</b>	<b>20</b>
<i>Create Launch Template.....</i>	<i>21</i>
<b>Create AWS Backup Plan .....</b>	<b>22</b>
<b>Install and Configure Desktop Client.....</b>	<b>24</b>
<b>Install &amp; Configure Mobile Client.....</b>	<b>28</b>

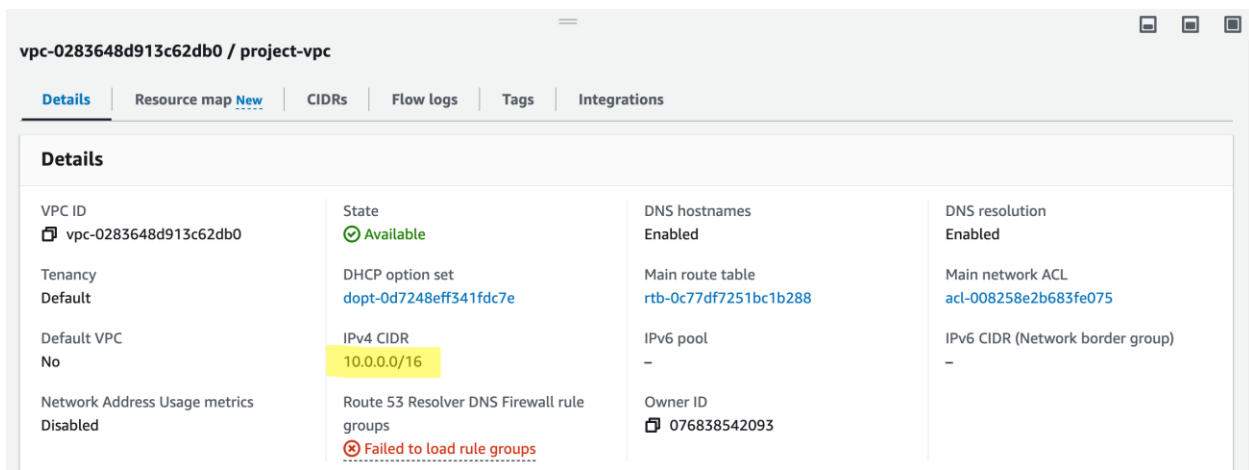
## VPC Creation

New VPC is created by name = project-~~vpc~~



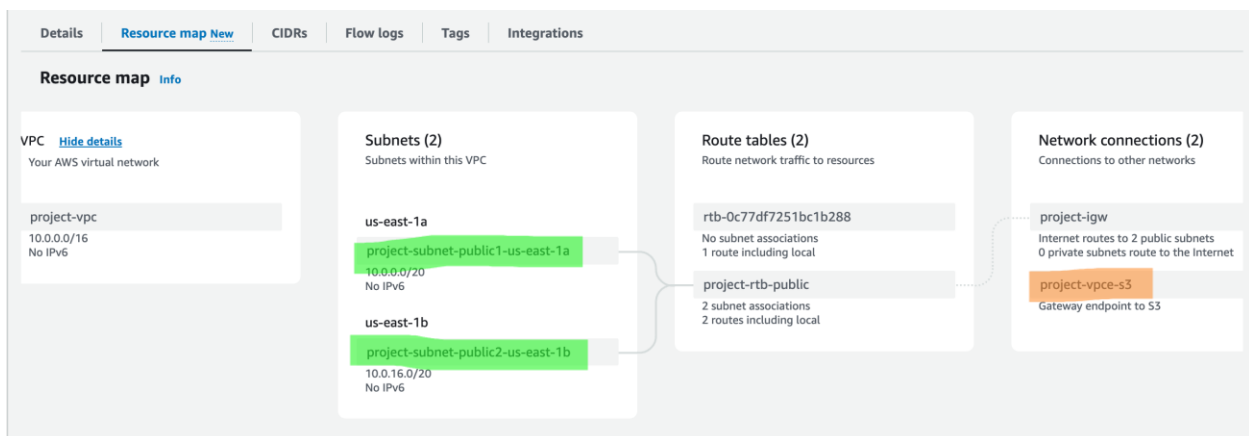
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
project-vpc	vpc-0283648d913c62db0	Available	10.0.0.0/16	-
-	vpc-0f5088dbc0699416b	Available	172.31.0.0/16	-

The IPv4 range for this VPC is 10.0.0.0/16



Details	Resource map	CIDRs	Flow logs	Tags	Integrations
<b>Details</b>					
VPC ID vpc-0283648d913c62db0	State Available	DNS hostnames Enabled	DNS resolution Enabled		
Tenancy Default	DHCP option set dopt-0d7248eff341fdc7e	Main route table rtb-0c77df7251bc1b288	Main network ACL acl-008258e2b683fe075		
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -		
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 076838542093			

Two Subnets and One S3 Gateway is associated with this VPC Resource Map.



Internet gateways (1/2) Info						Actions	Create internet gateway
Search						< 1 >	
	Name	Internet gateway ID	State	VPC ID	Owner		
<input type="checkbox"/>	-	igw-013bd4f22ad6fb78b	Attached	vpc-0f5088dbc0699416b	076838542093		
<input checked="" type="checkbox"/>	project-igw	igw-05d0c44b2db8bb57c	Attached	vpc-0283648d913c62db0   project-vpc	076838542093		

## NextCloud Security Group Creation

There are two security groups created for **EC2** and **EFS**

Security Groups (2/4) Info								Actions	Export security groups to CSV	Create security group
Filter security groups								< 1 >		
	Name	Security group ID	Security group na...	VPC ID	Description	Owner	Inbound rules count			
<input checked="" type="checkbox"/>	-	sg-0617152ae35715dae	Nextcloud EC2	vpc-0283648d913c62db0	ec2 security group	076838542093	6 Permission entries			
<input checked="" type="checkbox"/>	-	sg-0f61d3378d68a1c99	NextCloud EFS	vpc-0283648d913c62db0	efs group	076838542093	1 Permission entry			
<input type="checkbox"/>	-	sg-082ada59088666fa9	default	vpc-0f5088dbc0699416b	default VPC security group	076838542093	1 Permission entry			
<input type="checkbox"/>	-	sg-034bdac8404c3babb	default	vpc-0283648d913c62db0	default VPC security group	076838542093	1 Permission entry			

## Inbound rules for EC2 as per requirement

sg-0617152ae35715dae - Nextcloud EC2

Actions

Details

Security group name

Nextcloud EC2

Owner

076838542093

Security group ID

sg-0617152ae35715dae

Inbound rules count

6 Permission entries

Description

ec2 security group

Outbound rules count

1 Permission entry

VPC ID

vpc-0283648d913c62db0

Inbound rules

Outbound rules

Tags

Inbound rules (6)

Filter security group rules

Manage tags

Edit inbound rules

< 1 >

	Name	Security group rule...	IP versi...	Type	Protocol	Port range	Source	Description
	-	sgr-043bae413b7b33...	IPv4	Custom TCP	TCP	8080	0.0.0.0/0	-
	-	sgr-051b4f3111922a5...	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
	-	sgr-01aff02aa6c26c1e5	-	NFS	TCP	2049	sg-0617152ae35715d...	-
	-	sgr-0746a60d919ba7...	IPv4	HTTP	TCP	80	0.0.0.0/0	-
	-	sgr-00e8380a1e9ca52e2	IPv4	SSH	TCP	22	0.0.0.0/0	-
	-	sgr-0c52b9b99318d6...	IPv4	Custom TCP	TCP	8443	0.0.0.0/0	-

## Inbound rules for EFS as per requirement

VPC > Security Groups > sg-0f61d3378d68a1c99

sg-0f61d3378d68a1c99 - NextCloud EFS Actions ▾

**Details**

Security group name NextCloud EFS	Security group ID sg-0f61d3378d68a1c99	Description efs group	VPC ID vpc-0283648d913c62db0
Owner 076838542093	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

**Inbound rules (1/1)** Refresh Manage tags Edit inbound rules

Filter security group rules

<input checked="" type="checkbox"/>	Name ▾	Security group rule... ▾	IP versi... ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾	Description
<input checked="" type="checkbox"/>	-	sgr-0b605ef76357f2eed	-	NFS	TCP	2049	sg-0617152ae35715dae / Nextcloud EC2	-





## EFS Storage and S3 bucket creation

### Creating EFS Storage and S3 Bucket for NextCloud

Introduction: This document provides step-by-step instructions for setting up Amazon Elastic File System (EFS) storage and an S3 bucket for use with NextCloud.

#### Step 1: Create EFS Storage

1. In the AWS (Amazon Web Services) Management Console, navigate to "Elastic File System."
2. Click "Create file system."
3. Choose the previously created VPC from the dropdown.
4. Use the existing security group for access.
5. Complete the EFS setup.

[Option+S]     N. Virginia voclabs/user2734257=Muhammad\_Abdullah @ 0768-3854-2093

Amazon EFS > File systems > fs-0b695d905491568c1

## ProjectEFS (fs-0b695d905491568c1) Delete Attach

General Edit

Performance mode  
General Purpose  
  
Throughput mode  
Elastic  
  
Lifecycle management  
Transition into IA: 30 day(s) since last access  
Transition out of IA: None  
  
Availability zone  
Standard

Automatic backups  
Enabled  
  
Encrypted  
7da6d969-b57e-4a80-9eb1-482c1441c9a9 (aws/elasticfilesystem)  
  
File system state  
Available  
  
DNS name  
fs-0b695d905491568c1.efs.us-east-1.amazonaws.com

Availability zone ▲	Mount target ID ▼	Subnet ID ▼	Mount target state ▼	IP address ▼	Network interface ID ▼	Security groups ▼
us-east-1a	fsmt-027468e7682ee80f8	subnet-01beaa32724bb2fa0	<span>Available</span>	10.0.5.0	eni-0a9744f54e07c4b66	sg-0f61d3378d68a1c99 (NextCloud EFS), sg-0617152ae35715dae (Nextcloud EC2)
us-east-1b	fsmt-0d997b8b66910359c	subnet-0a7b81cd0af05e82e	<span>Available</span>	10.0.20.22	eni-097243551e810bbd3	sg-0f61d3378d68a1c99 (NextCloud EFS), sg-0617152ae35715dae (Nextcloud EC2)

## Step 2: Create an S3 Bucket


1. Navigate to "S3" in the AWS Management Console.
2. Click "Create bucket."
3. Choose the same AWS region as your Nextcloud EC2 instance.
4. Enable bucket versioning.
5. Leave all other settings at their defaults.
6. Click "Create bucket."
7. Confirm that the bucket is NOT public.

Amazon S3 > Buckets > projects3bucketabd

## projects3bucketabd [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

### Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)  arn:aws:s3::projects3bucketabd	Creation date October 10, 2023, 14:19:59 (UTC-05:00)
---	--	---

### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

[Edit](#)

**Bucket Versioning**  
**Enabled**


Multi-factor authentication (MFA) delete  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

**Disabled**

### 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

### Step 3: S3 Policy Generation

1. In the S3 bucket's properties, navigate to the "Permissions" tab.
2. Click on "Bucket Policy" and use the Policy Generator.
3. Create a policy to allow "LabRole" full access to the bucket.

### Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Edit
Delete

**Public access is blocked because Block Public Access settings are turned on for this bucket**  
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LabRoleFullAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::076838542093:role/LabRole"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::projects3bucketabd",
        "arn:aws:s3:::projects3bucketabd/*"
      ]
    }
  ]
}
```

Copy

## Step 4: S3 Lifecycle Rule Configuration

1. In the S3 bucket's properties, navigate to the "Management" tab.
2. Click on "Lifecycle."
3. Create a lifecycle rule that moves ALL files to the intelligent-tiering storage class after 0 days.

### Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

View details
Edit
Delete
Actions
Create lifecycle rule

Find lifecycle rules by name

	Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
<input type="radio"/>	rule 1	Enabled	Entire bucket	Transition to Intelligent-Tiering	-	-	-

## Creation of EC2

Create an EC2 instance with the following specifications:

- Ubuntu server 22.04LTS;
- t2.medium;
- Use previously made VPC and Security group
- 8GB EBS storage

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

Ubuntu WebServer

[Add additional tags](#)

### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

#### Quick Start

Amazon Linux  
aws

macOS  
Mac

Ubuntu  
ubuntu

Windows  
Microsoft

Red Hat  
Red Hat

SUSE Li  
SUS

Browse more AMIs  
Including AMIs from AWS, Marketplace and the Community

Number of instances [Info](#)

1

#### Software Image (AMI)

Canonical, Ubuntu, 20.04 LTS, ...[read more](#)  
ami-06aa3f7caf3a30282

#### Virtual server type (instance type)

t2.medium

#### Firewall (security group)

2 security groups

#### Storage (volumes)

1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. ×

[Cancel](#)

[Launch instance](#)

[Review commands](#)

- Mount the previously created EFS volume into /mnt/efs
  - Enable: automatically mount the file system.
  - Disable: automatically create and attach security groups

## File systems

[Hide details](#)

☒ EFS

☐ FSx

### ▼ Shared file system 1

[Remove](#)

File system [Info](#)

fs-00a7ce45c82af158f

Name: starSectorEFS Availability: Regional

Mount point [Info](#)

/mnt/efs

[Add shared file system](#)

[Create new shared file system](#)

4 remaining (Up to 5 file systems maximum).

☐ Automatically create and attach security groups

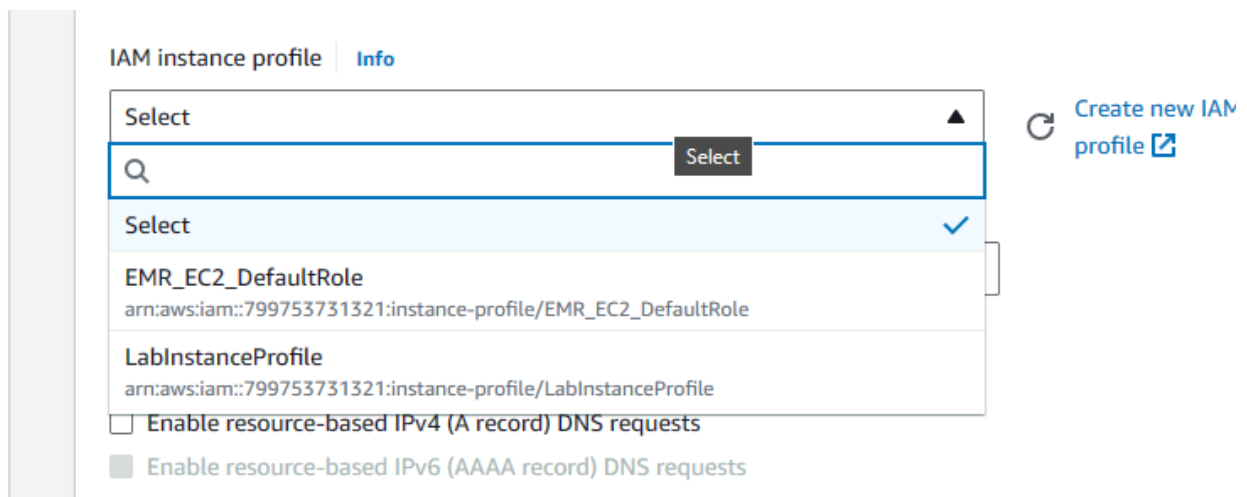
To enable access to the file system, the required security groups will be automatically created and attached to this instance and the selected file system. To manually manage the security groups, clear the checkbox. [Learn more.](#)

☒ Automatically mount shared file system by attaching required user data script

Automatically mount your file system by updating your user data to install efs-utils. If you would like to manually mount your file system, clear the checkbox.

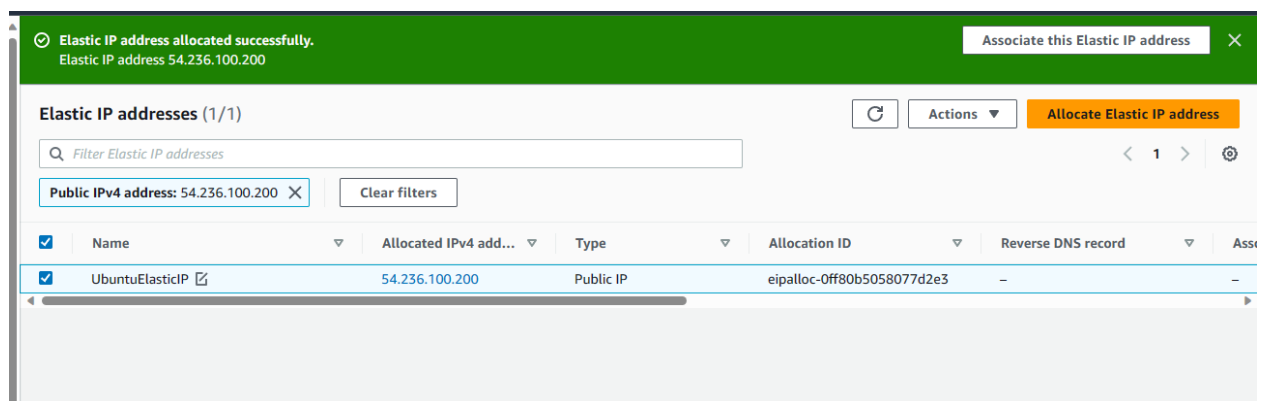
- Add the LabInstance role so the instance can connect to S3 and other services





## Creation of elastic IP\_\_

Elastic IP created and associated



## Create a Duck DNS domain

Go to <https://www.duckdns.org/>

Elastic IP to point 54.236.100.200

Domain: <https://starsector.duckdns.org>

success: ip address for **starsector.duckdns.org** updated to **54.236.100.200**

domains 1/5

http://

sub domain

.duckdns.org

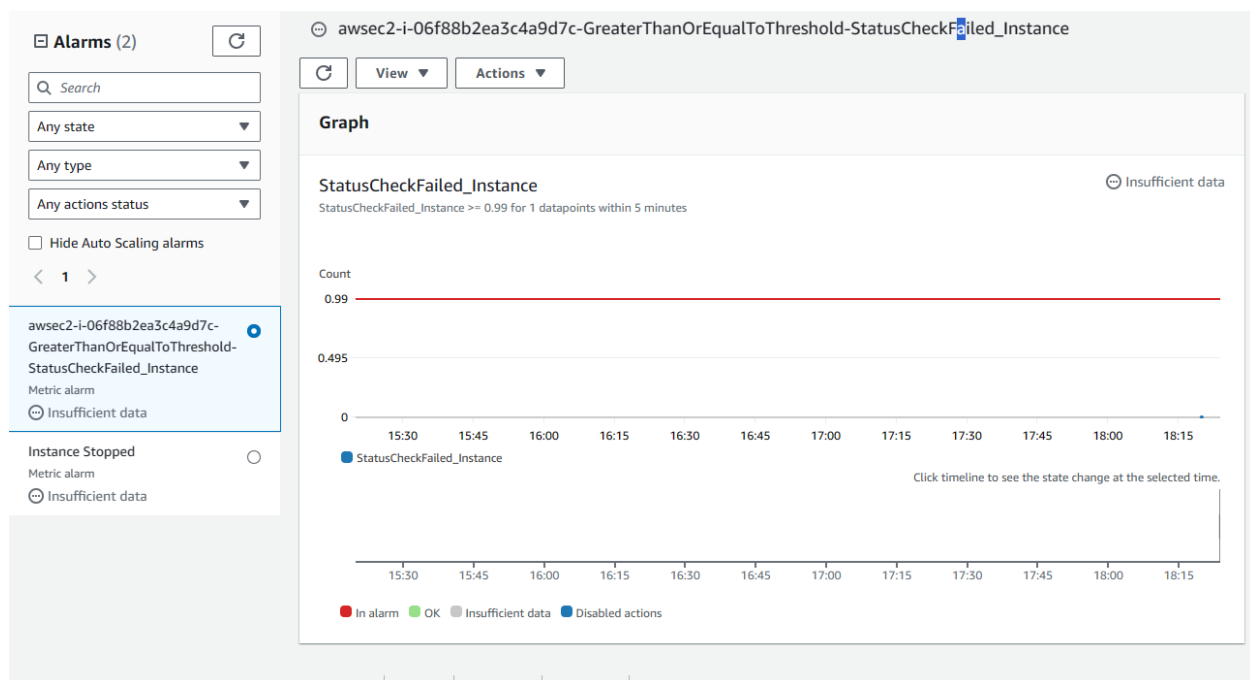
add domain

domain	current ip	ipv6	changed
starsector	54.236.100.200 <div>update ip</div>	ipv6 address <div>update ipv6</div>	0 seconds ago <div>delete domain</div>

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

## Configure CloudWatch Monitoring

Create a new CloudWatch task monitoring NextCloud ec2 instance; Done by creating an alarm to check if the instance fails status checks



## Install NextCloud

Login via ssh with the following command:

```
ssh -i "C:\Users\adeko\OneDrive - Red River College Polytech\Cloud Infrastructure\phoenix.pem" ubuntu@54.236.100.200
```

```

@ 54.236.100.200
ssh: connect to host port 22: Connection refused
PS C:\Users\adeko> ssh -i "C:\Users\adeko\OneDrive - Red River College Polytech\Cloud Infrastructure\phoenix.pem" ubuntu
@54.236.100.200
The authenticity of host '54.236.100.200 (54.236.100.200)' can't be established.
ED25519 key fingerprint is SHA256:s6sZ11/5gCIH13yAa43Fj/263xh/rCOPM1sqC8xoZXU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.236.100.200' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Nov 15 18:27:36 UTC 2023

System load:  0.080078125      Processes:            112
Usage of /:   20.7% of 7.57GB   Users logged in:     0
Memory usage: 6%              IPv4 address for eth0: 10.0.27.241
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

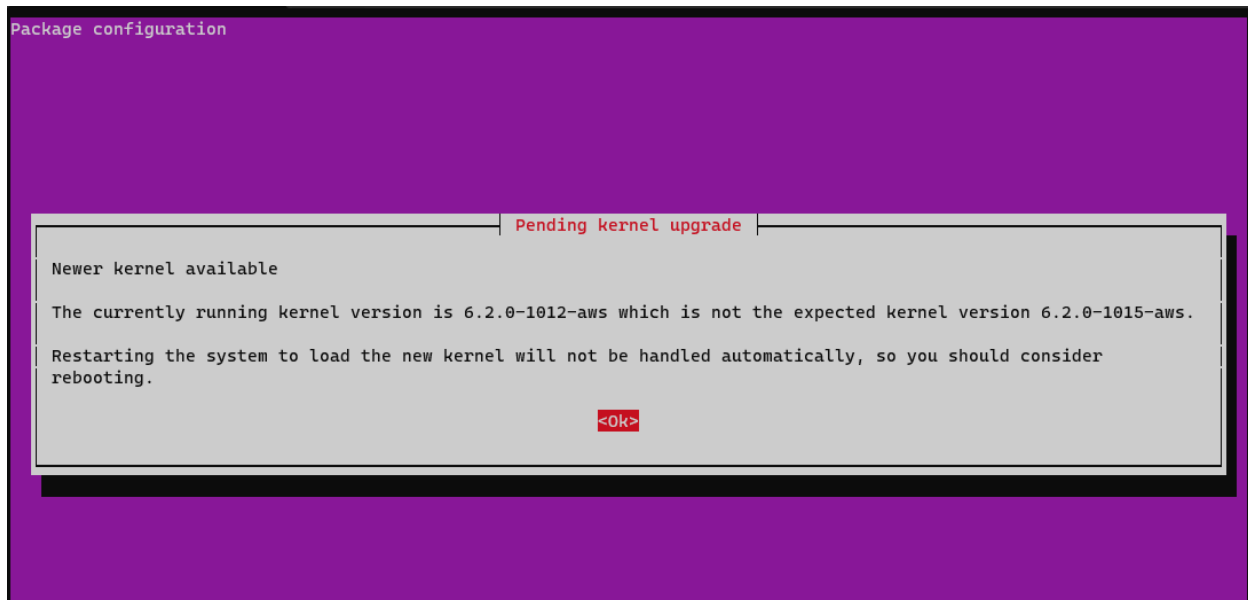
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

```

1

Perform updates using the following code:

- *sudo apt update*
- *sudo apt dist-upgrade*



Install docker.io from repositories using the command: *sudo apt install docker.io*

Create a folder called docker folder In your EFS mount and other necessary folders:

- */mnt/efs/docker*
- */mnt/efs/docker/nextcloud\_aio\_apache*

- `/mnt/efs/docker/nextcloud_aio_collabora_fonts`
- `/mnt/efs/docker/nextcloud_aio_database`
- `/mnt/efs/docker/nextcloud_aio_database_dump`
- `/mnt/efs/docker/nextcloud_aio_mastercontainer`
- `/mnt/efs/docker/nextcloud_aio_nextcloud`
- `/mnt/efs/docker/nextcloud_aio_nextcloud_data`
- `/mnt/efs/docker/nextcloud_aio_redis`
- `/mnt/efs/backup`

Manually ADD docker volumes for each of the folders created

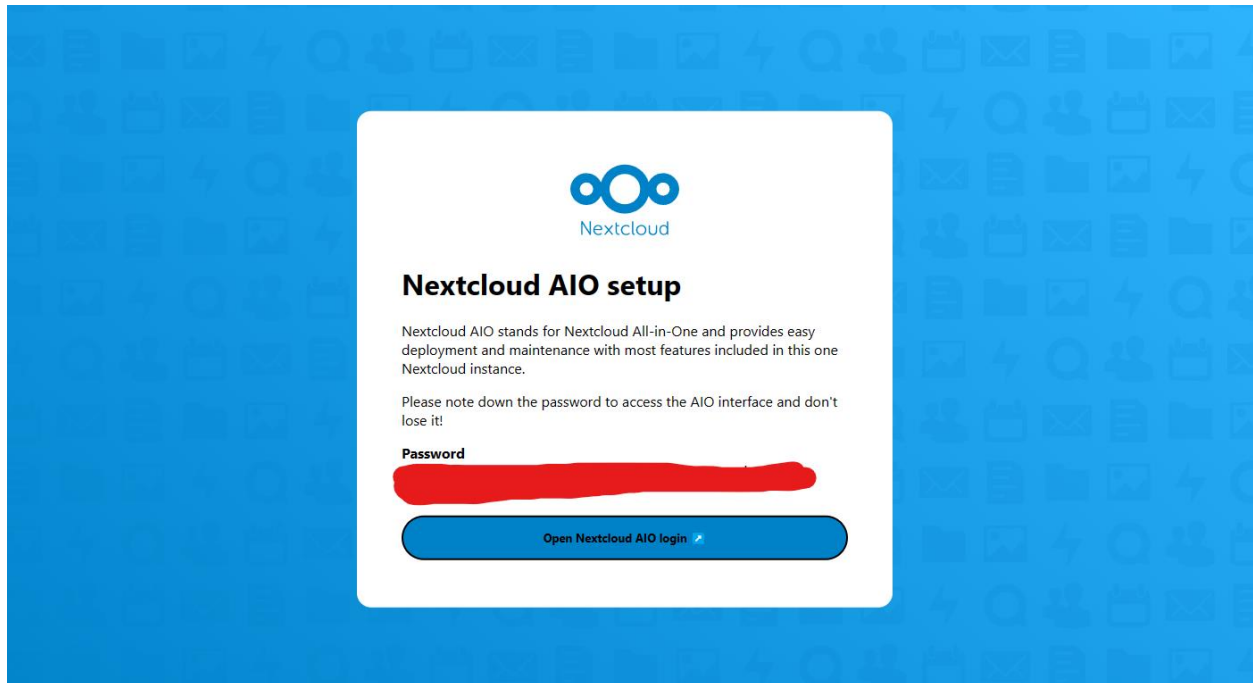
- `sudo docker volume create --driver local --name nextcloud_aio_apache -o device=/mnt/efs/docker/nextcloud_aio_apache -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_collabora_fonts -o device=/mnt/efs/docker/nextcloud_aio_collabora_fonts -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_database -o device=/mnt/efs/docker/nextcloud_aio_database -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_database_dump -o device=/mnt/efs/docker/nextcloud_aio_database_dump -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_mastercontainer -o device=/mnt/efs/docker/nextcloud_aio_mastercontainer -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_nextcloud -o device=/mnt/efs/docker/nextcloud_aio_nextcloud -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_nextcloud_data -o device=/mnt/efs/docker/nextcloud_aio_nextcloud_data -o type=none -o o=bind`
- `sudo docker volume create --driver local --name nextcloud_aio_redis -o device=/mnt/efs/docker/nextcloud_aio_redis -o type=none -o o=bind`
- `sudo docker volume create --driver local --name backup -o device=/mnt/efs/backup -o type=none -o o=bind`

Run the command to install NextCloud

```
# 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
```

You should be able to open browser and put in <https://elasticIP:8080>

Allows you to set up nextcloud.



Note the password

## Configure Nextcloud

Make sure collabora is checked and others are unchecked

Set your backup location as `/mnt/efs/backup` NOTE: This should have been created previously

Change the time zone: America/Winnipeg

Wait until all the containers are GREEN Note: Might take a while

Note the Admin username and password, NOTE: do not lose this

## Backup Setup

Enter your backup path "`/mnt/efs/backup`" and create a backup; NOTE: this would stop containers do not be alarmed.

Note the backup encryption key;

## Nextcloud AIO v7.6.2

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

● Backup container is currently running. ([Logs](#))

### Containers

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

Your containers are up-to-date.

Restore or Backup currently running. Cannot start the containers until that's done.

## Log In to Nextcloud

Click on the link that says open your nextcloud

## Nextcloud AIO v7.6.2

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.

[Stop containers](#)

### Backup and restore

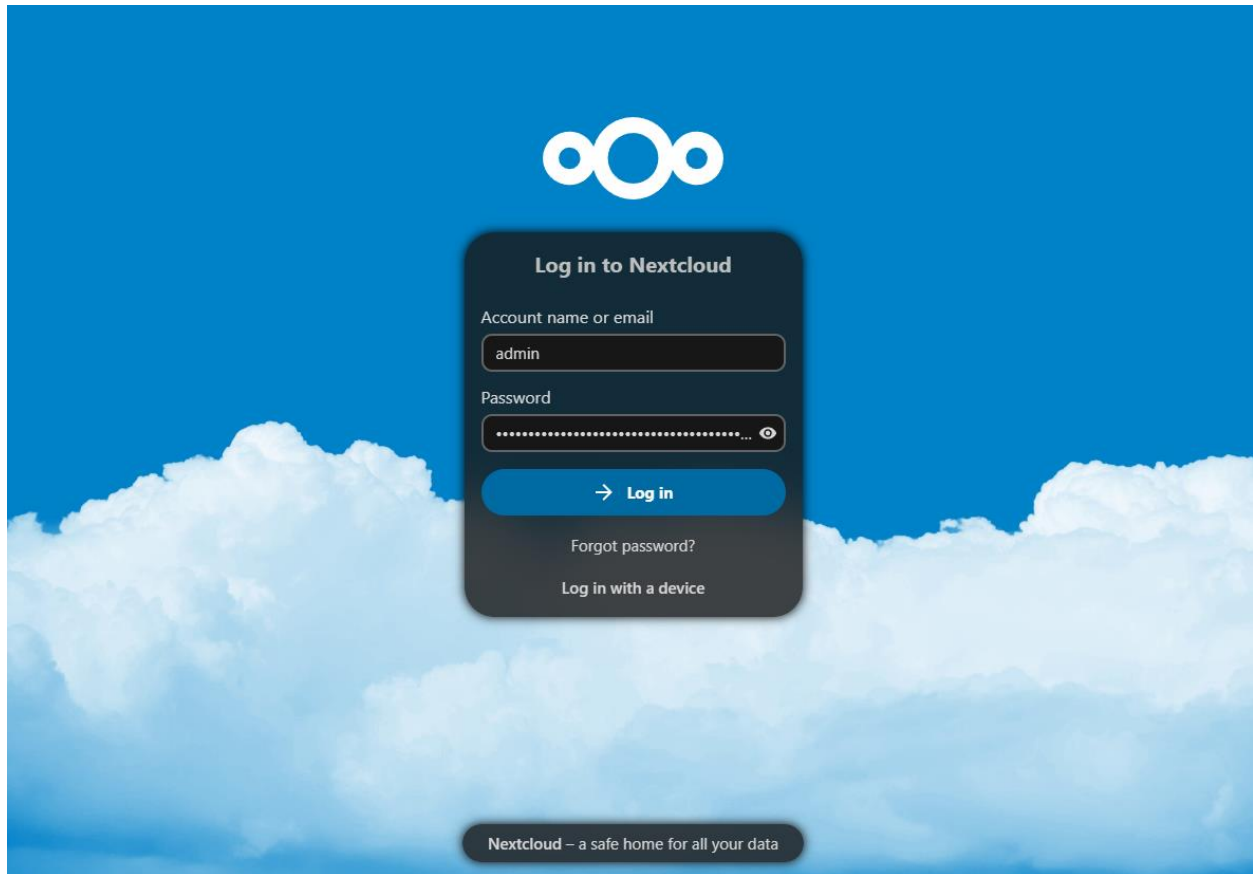
#### Backup information

This is your encryption password for backups:

**04538a16b3515f6cfd5df9cd8960883e738df37354daf9ef**

Please save it at a safe place since you won't be able to restore from

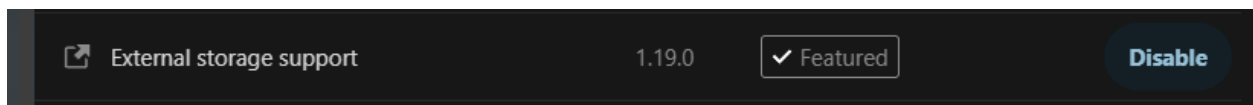
Then log in with your credentials as seen in the following picture



### Enable External Storage Support

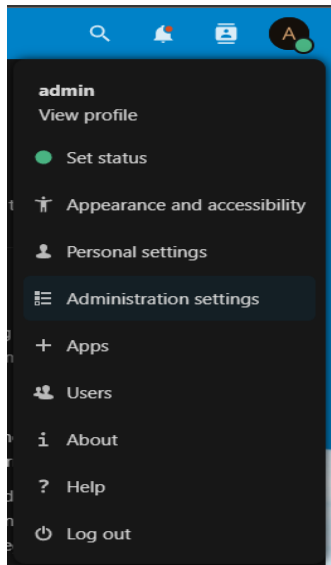
This done by clicking on your profile icon and selecting Apps

In the list you should see the external storage support with an option to enable.



### Security Scan

Click on your profile and select Administration Settings



Click the security scan link which will take you to:

## Nextcloud All-in-One

Open Nextcloud AIO Interface

Click here for more infos on this feature (e.g. also on how to change the link in the button)

### Security & setup warnings

It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information.

There are some warnings regarding your setup.

- You have not set or verified your email server configuration, yet. Please head over to the [Basic settings](#) in order to set them. Afterwards, use the "Send email" button below the form to verify your settings.
- Your installation has no default phone region set. This is required to validate phone numbers in the profile settings without a country code. To allow numbers without a country code, please add "default\_phone\_region" with the respective [ISO 3166-1 code](#) of the region to your config file.

Please double check the [installation guides](#) , and check for any errors or warnings in the [log](#).

Check the security of your Nextcloud over [our security scan](#) .

### Version

Nextcloud Hub 6 (27.1.3)

Put In your domain to check the security for the server





# Check the security of your private Nextcloud server

**Privacy does not exist without security.** To help you keep your data yours, this scan analyzes the security of your server and gives you an overview of what to improve.



URL  Scan

## Notes

The Scan should show like so:

# Check the security of your private cloud server

**Privacy does not exist without security.** To help you keep your data yours, this scan analyzes the security of your server and gives you an overview of what to improve. It only takes into account publicly available information. Therefore it does not reflect on custom patches, support contracts or other particularities of the server in question.

Find out how you can [upgrade to Nextcloud to keep your data secure](#).

## Rating

A+



<https://phoenixfirst.duckdns.org>

Running **Nextcloud 27.1.3.2**

✓ Latest patch level

✓ Major version still supported

Scanned at 2023-11-14 18:38:29

[trigger re-scan](#)

## Vulnerabilities

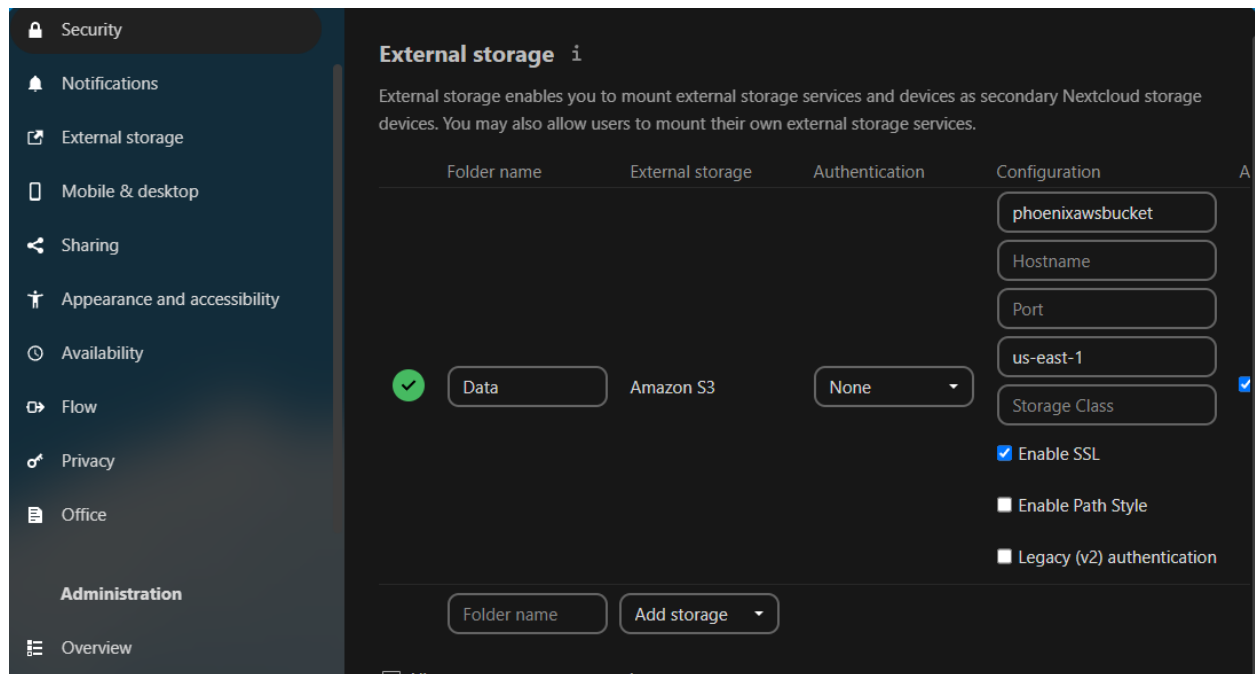
Learn more about [our security efforts](#).

S3 bucket set up on nextcloud

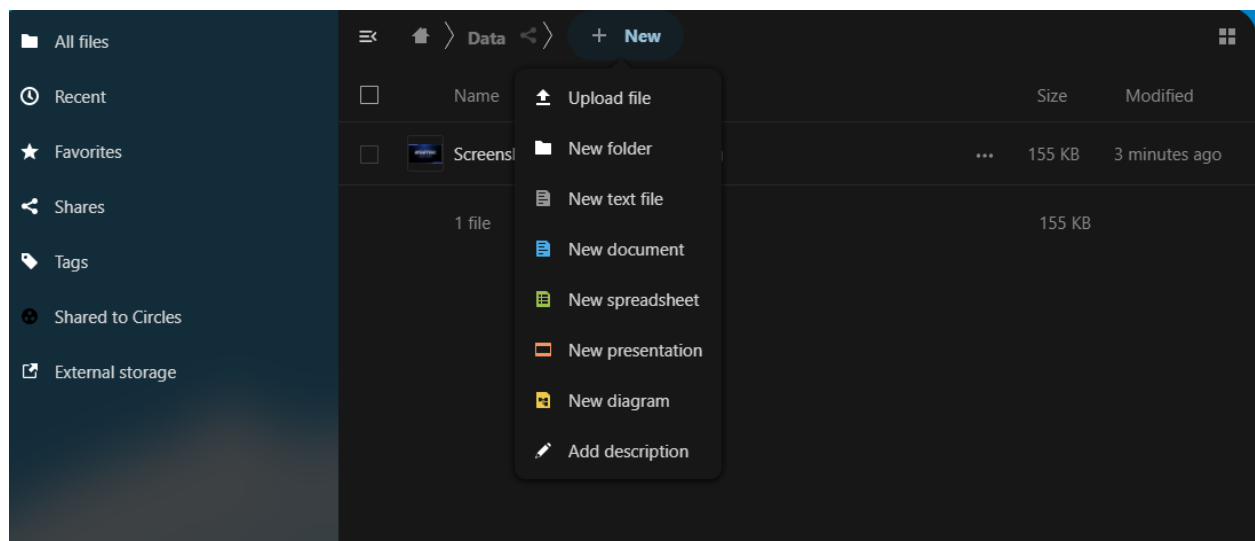
Add Shared Folder "Data" to the external storage settings

This should connect to your AWS S3 bucket

Add your bucket name and region, Authentication was set to none.



Go to the Data folder and upload a test file;



Verify that it has been added to your S3 bucket

[Amazon S3](#) > [Buckets](#) > phoenixawsbucket

## phoenixawsbucket [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)


### Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#)

[Actions](#) [Create folder](#) [Upload](#)

☐ Show versions < 1 > ⚙




<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
<input type="checkbox"/>	 <a href="#">Screenshot</a> <a href="#">2023-10-23</a> <a href="#">163117.png</a>	png	November 14, 2023, 13:03:06 (UTC-06:00)	154.6 KB	Standard

## NextCloud New User Creation

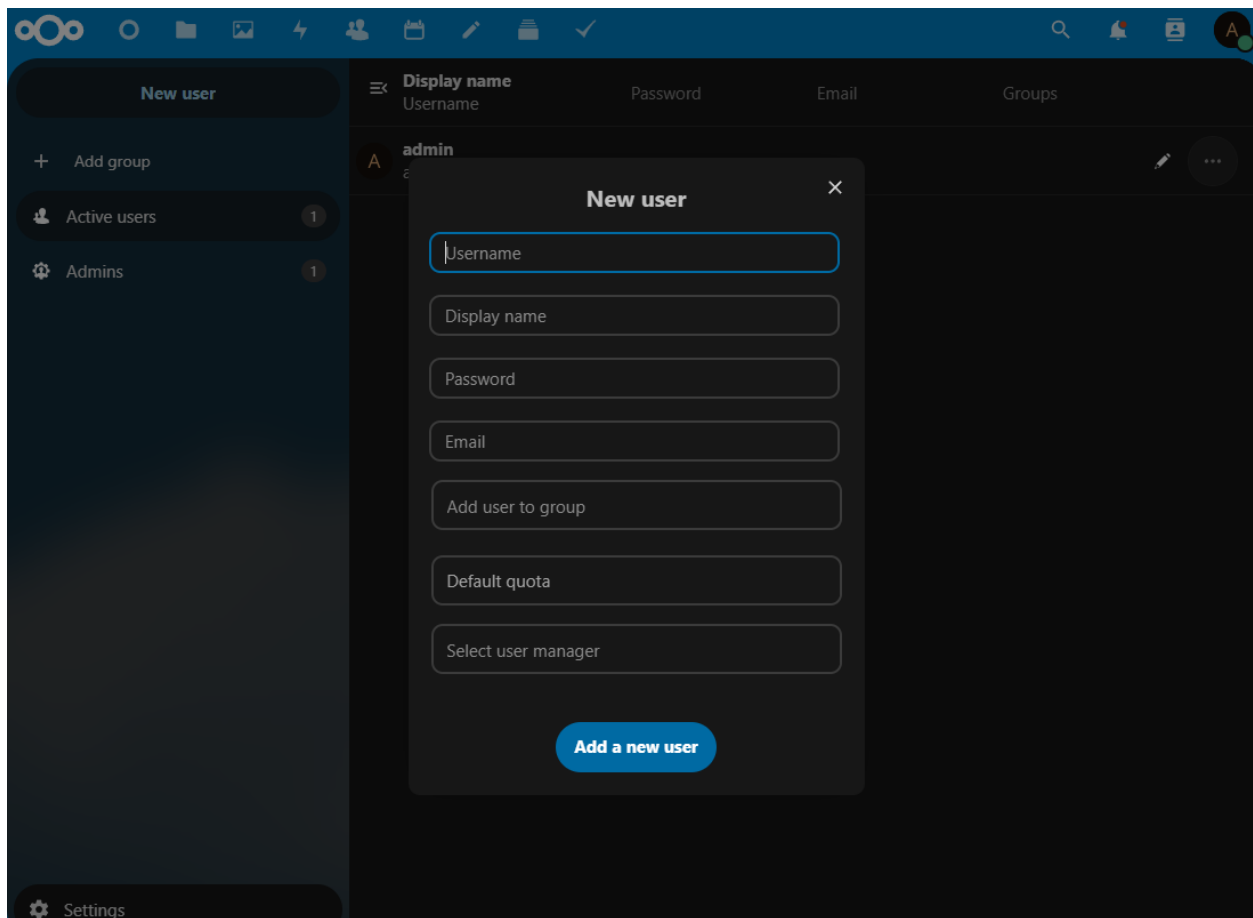
Create a new User by going to the user tab and selecting the option new user

**New user**

[+ Add group](#)

Display name	Username	Password	Email	Groups	Quota	Manager
 admin	admin			admin	Unlimited (35.8 MB used)	 

Fill the information for a new test user



## Create Image & Launch Template

Create an Amazon Machine Image from the instance

Select the instance -> Actions -> Image and templates -> create image

## 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-0ac7b8b9ac703ac53 (UbuntuWebServer)


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

Image description - optional  
  
Maximum 255 characters

No reboot  
☐ Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fr...	8	EBS General Purpose S...	100		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

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

Hit create Image after filling the information

## Create Launch Template

Select Launch Template from the left side menu -> create launch template

[EC2](#) > [Launch templates](#) > Create launch template

## Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

**Launch template name and description**

Launch template name - *required*  
  
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '\*', '@'.

Template version description  
  
Max 255 chars

Auto Scaling guidance [info](#)  
Select this if you intend to use this template with EC2 Auto Scaling  
☐ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags  
▶ Source template


▼ **Summary**

[Software Image \(AMI\)](#)  
-

[Virtual server type \(instance type\)](#)  
-

[Firewall \(security group\)](#)  
-

[Storage \(volumes\)](#)  
-

 **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

×

Launch template contents

Choose “My AMIs” and then choose the previously created Nextcloud AMI.

- Instance type: t2.medium
- Key pair: choose a previously created one.
- Choose the previously created security group (remove any others).

- Under advanced details:
- Choose the “LabInstanceProfile” under IAM instance profile.

You can use this launch template to quickly launch a new fully operational Nextcloud instance, assuming you setup persistent shared storage. Once it’s running, you just need to point your elastic IP at the new instance and everything should work correctly within a few minutes.

## Create AWS Backup Plan

Search services for AWS backup

-select create a backup plan

The screenshot shows the AWS Backup console interface. At the top, it says 'Storage and Data Management'. The main heading is 'AWS Backup' with the subtext 'Centrally manage and automate backups across AWS services'. Below this, it says 'Define backup plans, schedule backups, automate backup retention management, centrally monitor backup activity, and restore backups.' On the right, there's a 'Create a backup plan' section with a description: 'Build a backup plan from scratch or start based on an existing plan.' and a 'Create backup plan' button. Below this, there's a 'Pricing' section stating: 'With AWS Backup, you pay only for the amount of backup storage you use and the amount of backup data you restore in the month. There is no minimum fee and there are no set-up charges.' and a link to 'AWS Backup pricing guide'. At the bottom, there's a 'Supported Services' section with links for 'Amazon EBS' and 'Amazon EC2'. On the left, there's a 'How it works' section with two columns: 'Create' (Build backup plans that define your backup requirements, including backup schedules, backup retention rules and lifecycle rules.) and 'Assign' (Assign your AWS resources to backup plans using resource tags or AWS resource IDs. Resources assigned to backup plans are then backed up automatically according to the schedule defined in the plan.)

Select start with a template and choose Daily-Monthly-1yr-Retention -> create plan

It should ask to assign resources

## Assign resources [Info](#)

### General

Resource assignment name

Resource assignment name is case sensitive. Must contain from 1 to 50 alphanumeric or '-' '\_' characters.

IAM role [Info](#)

AWS Backup will assume this IAM role when creating and managing recovery points on your behalf.

☐ Default role

If the AWS Backup default role is not present, one will be created for you with the correct permissions.

☒ Choose an IAM role

Role name

### Resource selection [Info](#)

Assign resources to this Backup plan using tags and resource IDs.

#### 1. Define resource selection [Info](#)

Protect all resources or specify resources by type or ID.

☒ Include all resource types

Protect all resource types that are enabled in your account.

Select choose an IAM role -> LabRole

Include Specific resources: EBS, EFS, S3

Uncheck all resources and select only your created resources

Resource type	Volume IDs	
EBS	<input type="text" value="Choose resources"/>	<input type="button" value="Remove"/>
	<input type="text" value="vol-0c9fe7fd7a4f6c3ed"/>	
Resource type	File system IDs	
EFS	<input type="text" value="Choose resources"/>	<input type="button" value="Remove"/>
	<input type="text" value="fs-00a7ce45c82af158f"/>	
Resource type	Bucket names	
S3	<input type="text" value="Choose resources"/>	<input type="button" value="Remove"/>
	<input type="text" value="starsector"/>	

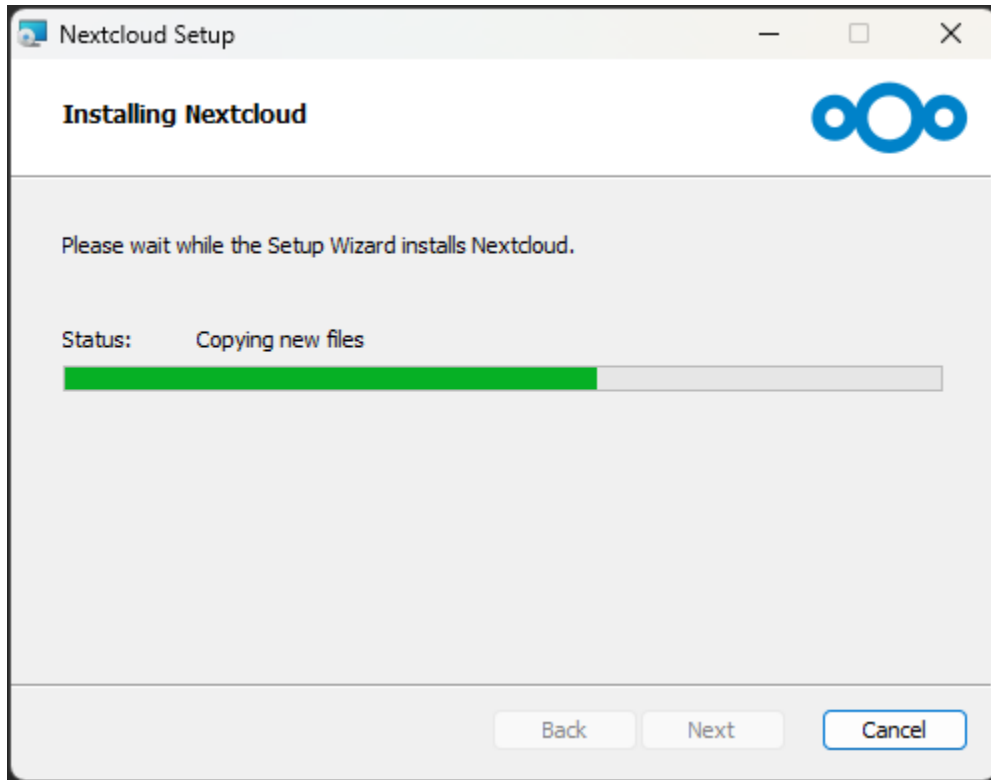
S3 buckets must have versioning enabled. [Learn more](#)

Select Assign resources

## Install and Configure Desktop Client

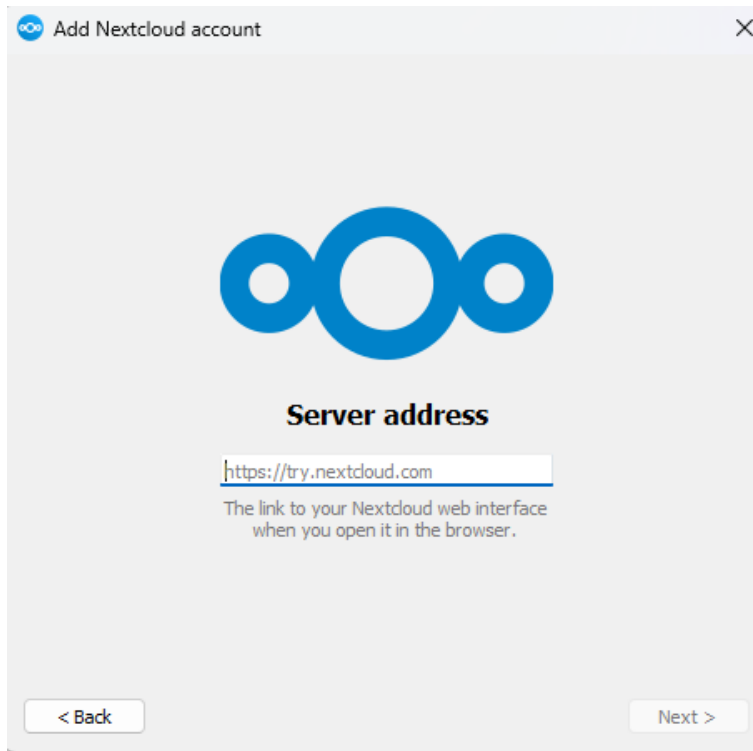
Download the NextCloud client from [NextCloud Download page](#)

Launch and configure with the wizard that pops up

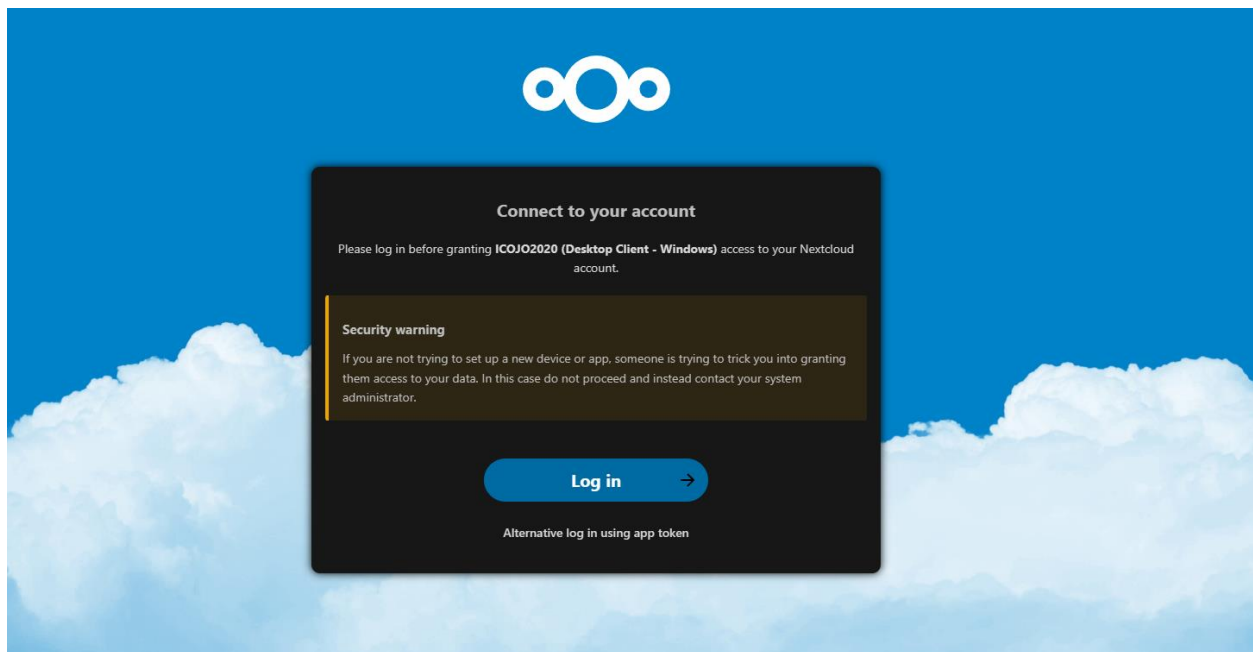


You would need put your nextcloud link that you in a browser in the window below to connect it

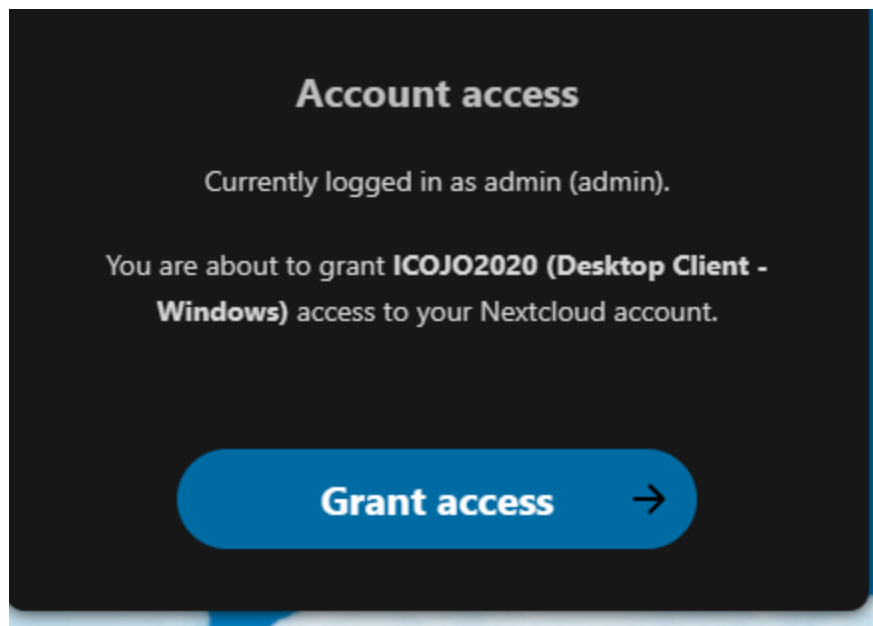




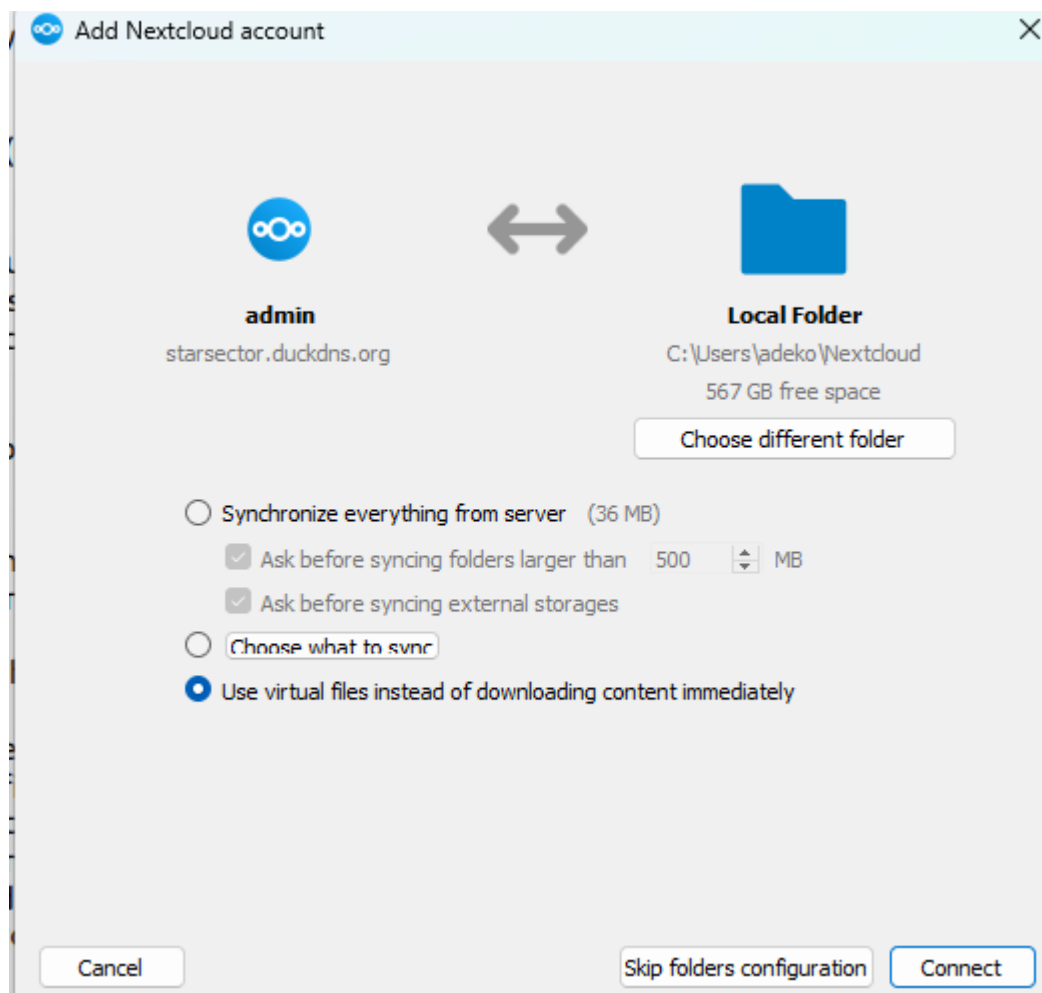
You should get a pop up on your desktop client via the browser



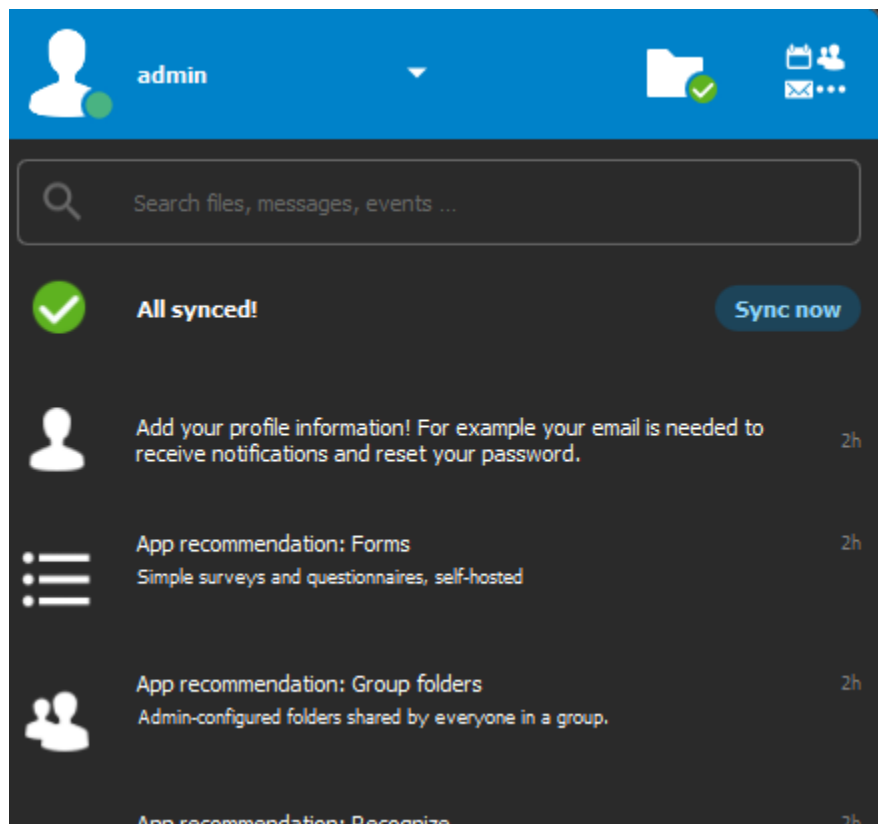
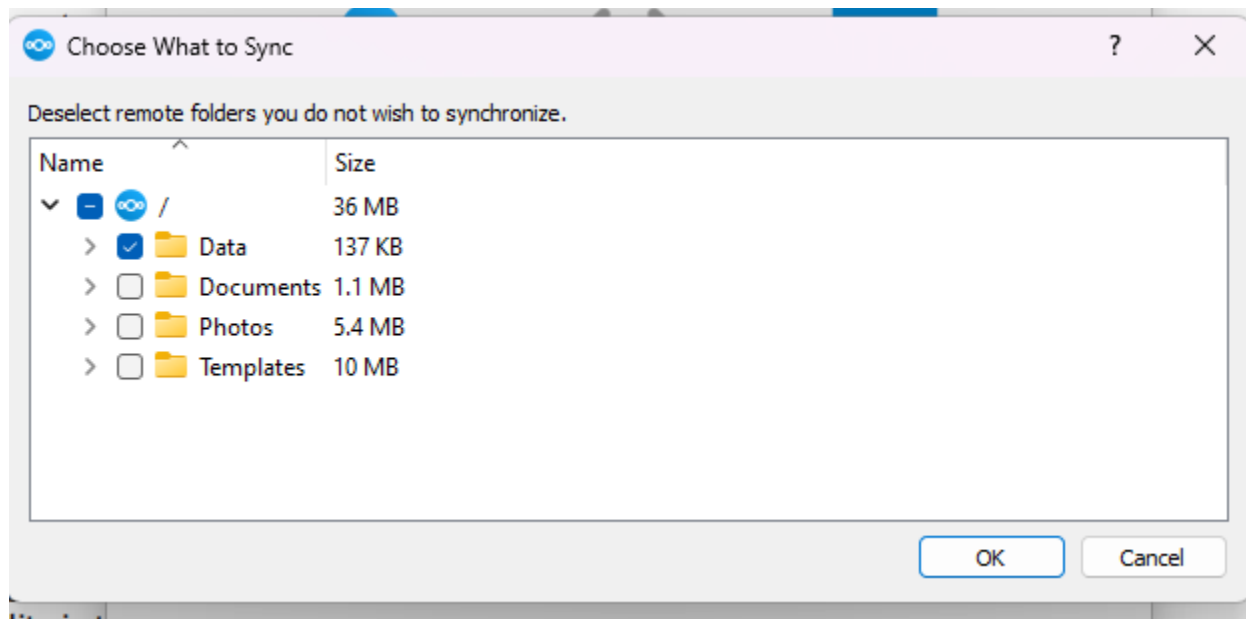
Grant Access



Set up file configurations as you see fit



Select choose what to sync -> make sure you uncheck Data folder because its too large, select others



Test by pasting any files on your folder on your computer and check the browser its should sync automatically

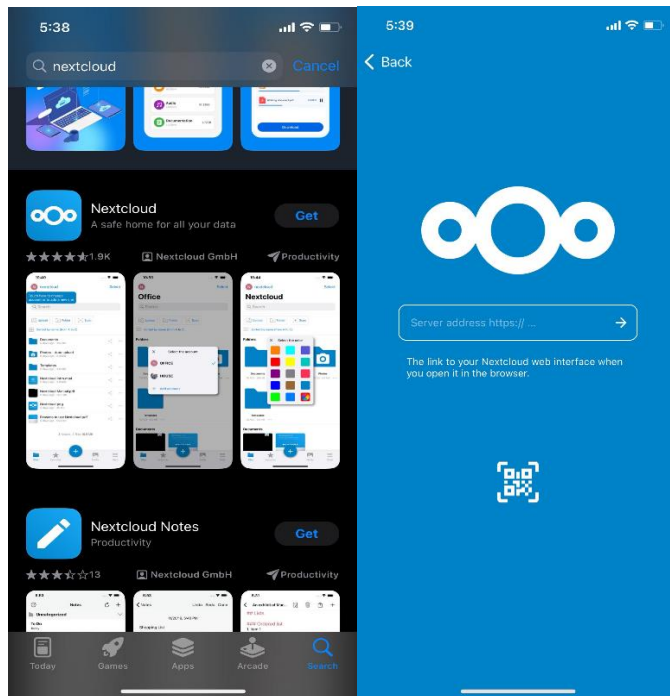


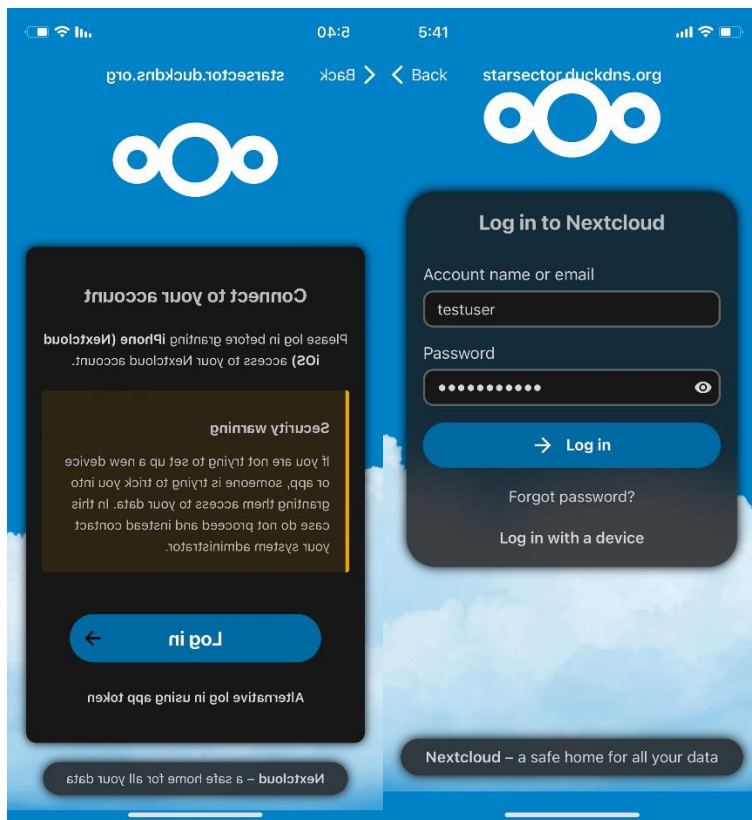


## Install & Configure Mobile Client

Download from the Appstore

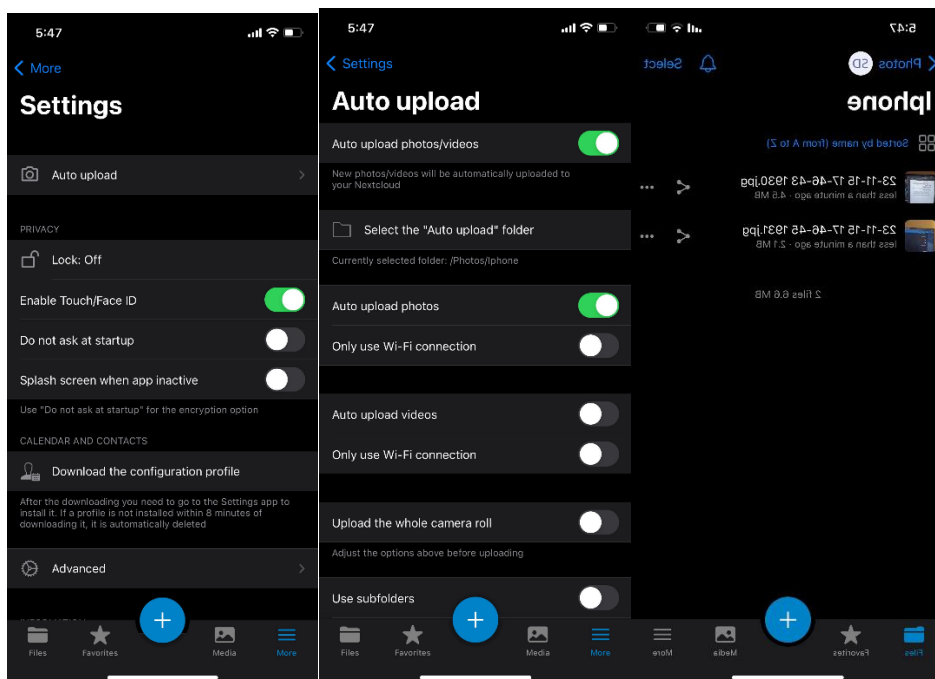
Put in Server information and log in as a User;











Go to Settings and turn on the auto Upload feature for pictures

Take new picture and check the browser to see if the pictures synced.



The test should be confirmed with image similar to the one below

<input type="checkbox"/>	Name ▾			Size	Modified
<input type="checkbox"/>	 23-11-15 17-46-43 1930.jpg			4.5 MB	11 minutes ago
<input type="checkbox"/>	 23-11-15 17-46-45 1931.jpg			2.1 MB	11 minutes ago
2 files				6.6 MB	