

# HIFIS: VO FEDERATION FOR EFSS

Andreas Klotz and Björn Schießle

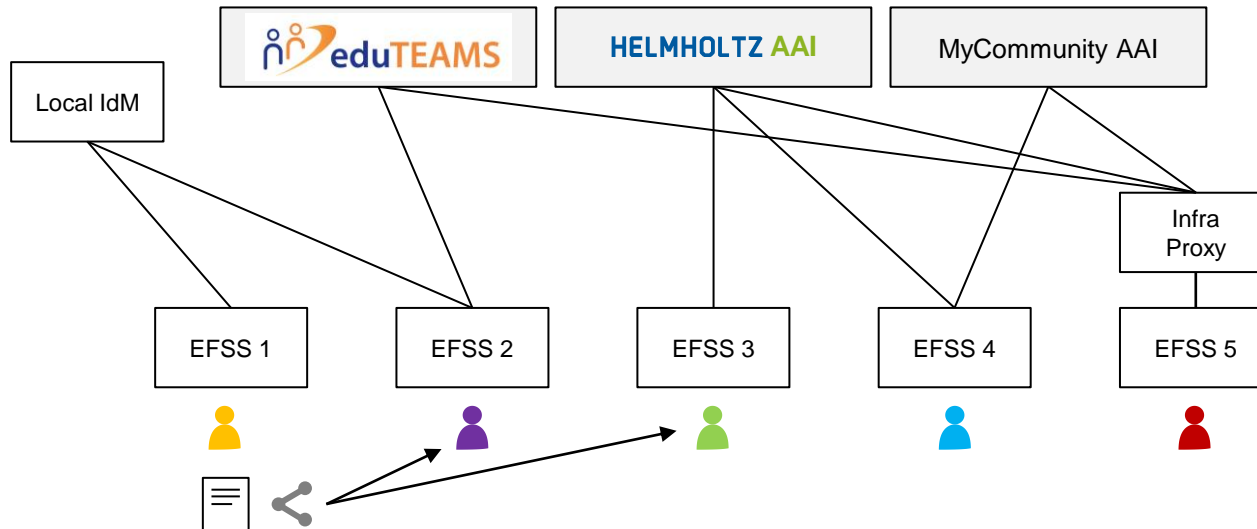
On behalf of HIFIS and Nextcloud

March 7th 2023, CS3 Barcelona

- Virtual Organisation (VO) = Community AAI **managed** group of any size
- Federated shares with VOs instead of individual users

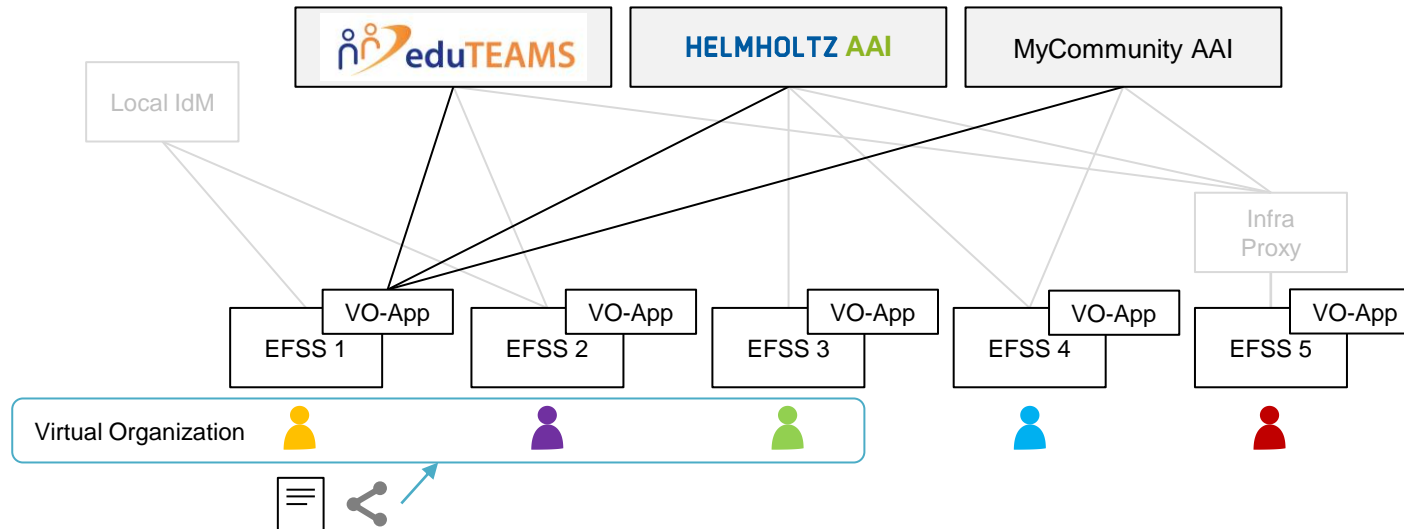


- Introducing new Federated Group Share type for OCM
- Focus on data protection and data sovereignty



# VO FEDERATION

## Minimally intrusive



**Demo!**

## Federated Group Share for OCM – Goals

---

**Add real federated group sharing where both groups and users can be distributed across multiple Nextcloud instances.**

Based on OCM and what we already have:

- New share type „federated group share“
- Utilize the already available remote group share
- Keep all existing improvements like a flat re-shares
- Generic/Extensible approach to support other back-ends in the future, e.g. Global Scale

### Prerequisites

- Nextcloud need to know all Nextcloud servers it should federate with
- Nextcloud should know all Community AAI server
- Introduce new (optional) share type for „federated group shares“
- The admin settings interface from the VO-App will allow the admin to configure all known Nextcloud servers and Community AAI's
  - A plugin system should be used to connect the VO-App information with Nextcloud in order to allow different sources for this kind of information in the future

## Federated Group Share for OCM

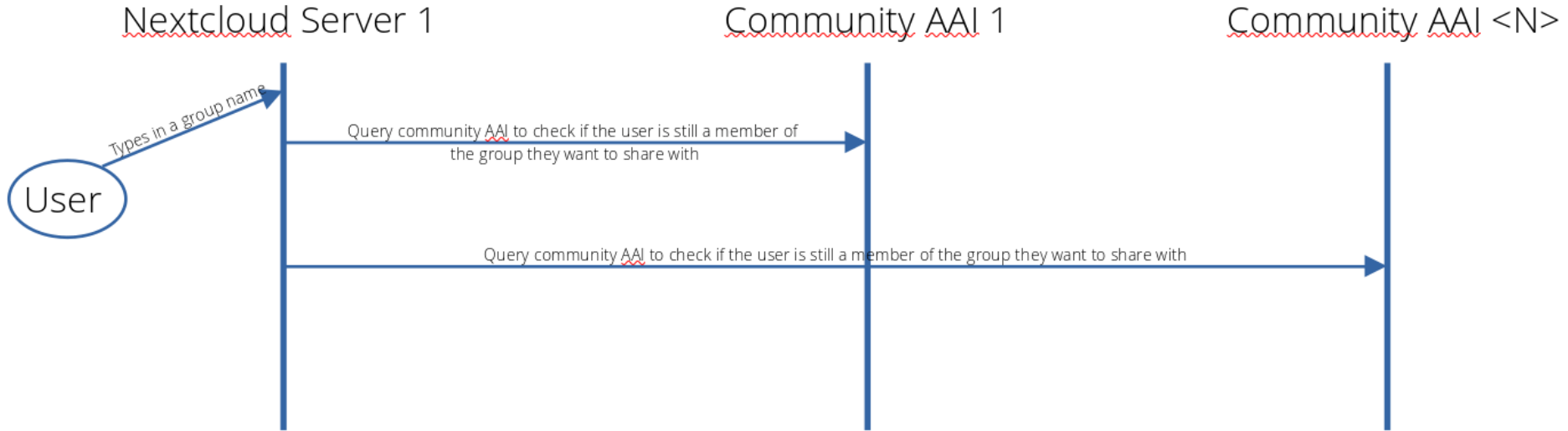
---

### Step 1: Get to know the group Members

- Users are assigned to the right groups and group membership is kept in sync for the individual users
- Community AAI's know all groups across all Nextcloud
  - User connect to their community AAI to find all their groups.
  - Groups get synced regularly from the AAI to Nextcloud
  - Nextcloud should distinguish between local groups and Community-AAI-Groups and indicate the difference to the user
  - Connection to AAI happens by the VO-App which is a plugin to a generic „federated groups API“ which allows to have additional group back-ends later on (e.g. the lookup server from Global Scale)



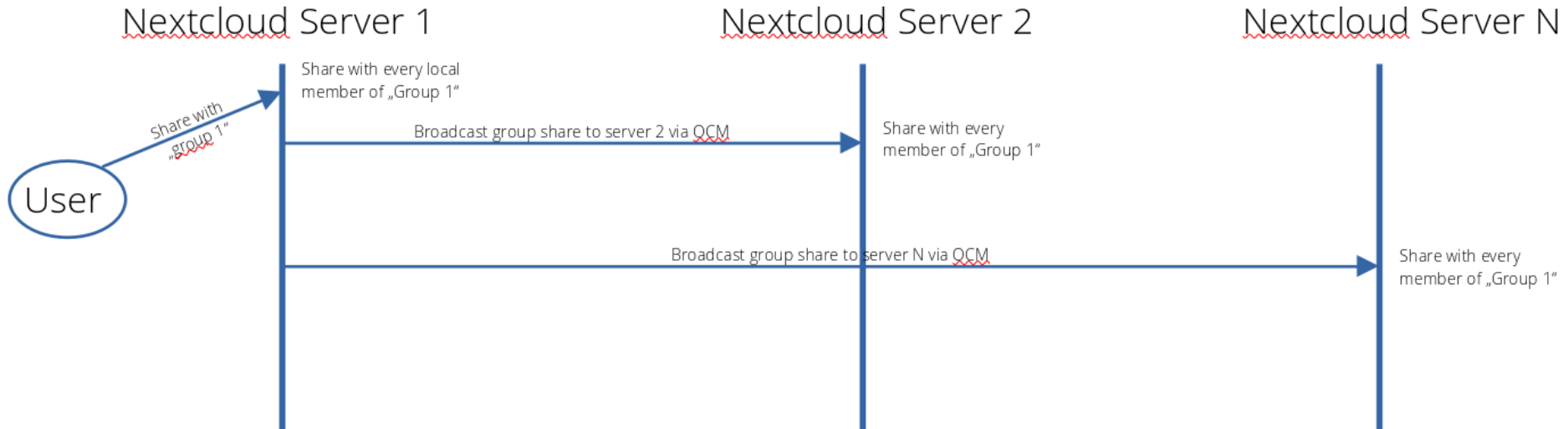
## Federated Group Share for OCM – Check Group Membership



### Notes:

- Auto completion based on the synced groups from the Community AAI
- Before share is initiated we check with the Community AAI if the user is still a member of the group they want to share with

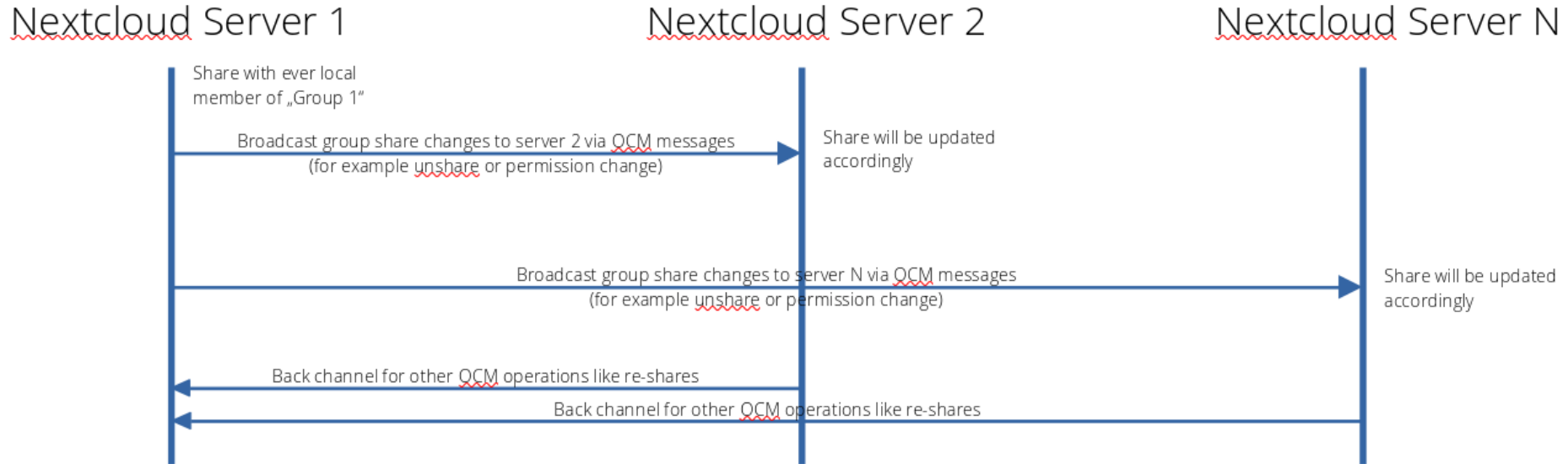
## Federated Group Share for OCM – Broadcast Group Share



### Notes:

- Based on the already existing OCM group sharing available in Nextcloud
- Once accepted, share gets mounted via webdav
- Regularly check if the user is still a member of the group, otherwise remove access by removing the user from the locally synced group

## Federated Group Share for OCM – Broadcast Group Share Changes



### Notes:

- Used existing OCM Notification-requests
- Comes with all (Nextcloud-specific) optimizations like flat re-shares

**Demo!**

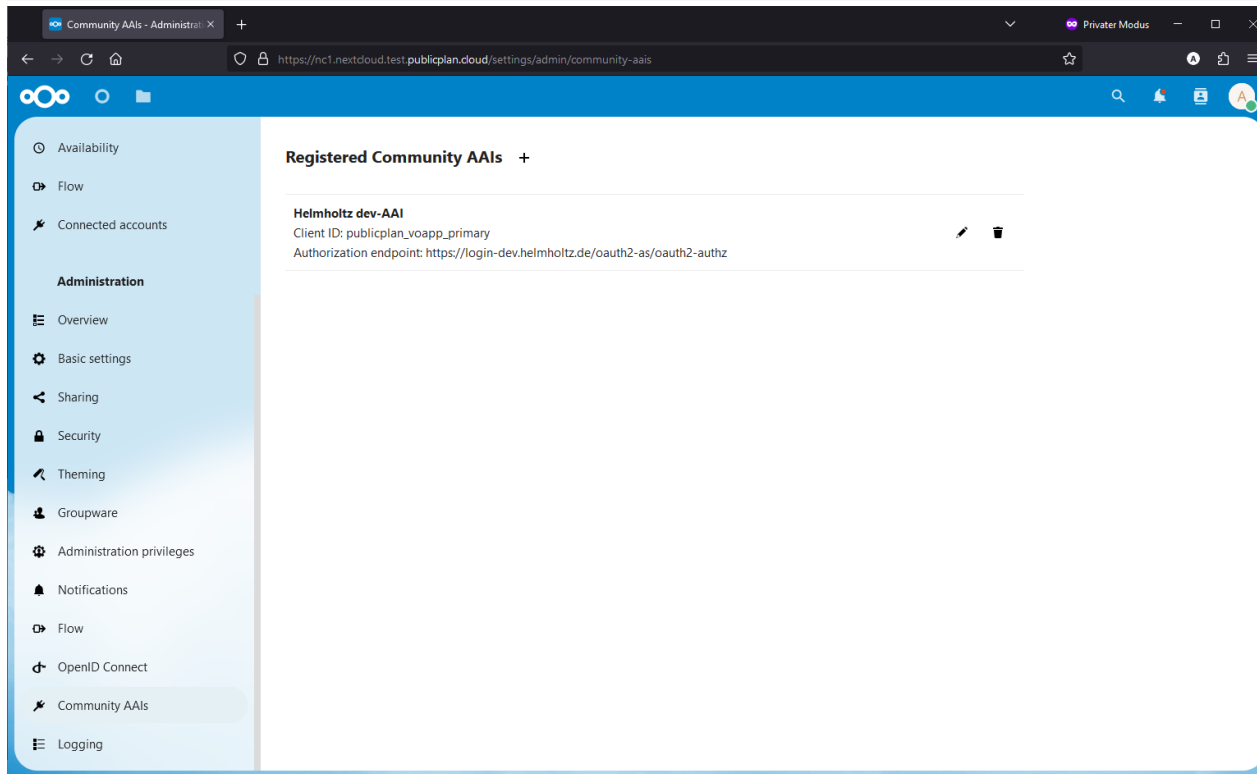
- „VO Folders“, a group based folder which will be automatically mounted for remote VO members
- SCIM lookup of VO members to directly share with them
- Automatically linking account if instance authenticates with Community AAI via OIDC
- Individual group avatars
- IETF standardisation

---

## SPARE SLIDES

# VO FEDERATION

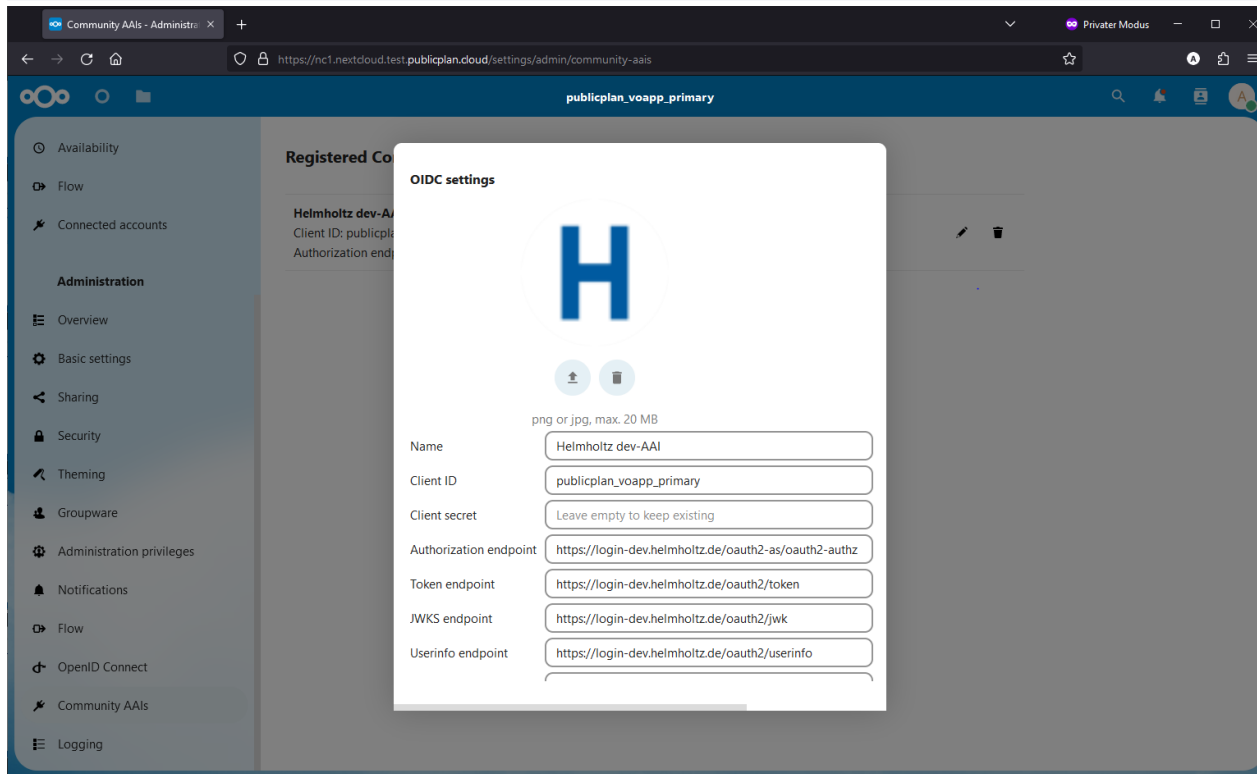
## Demo Screenshots



The screenshot shows a web browser window with the URL `https://nc1.nextcloud.test.publicplan.cloud/settings/admin/community-aas`. The page title is "Community AAs - Administration". The left sidebar contains a navigation menu with the following items: Availability, Flow, Connected accounts, Administration (expanded), Overview, Basic settings, Sharing, Security, Theming, Groupware, Administration privileges, Notifications, Flow, OpenID Connect, Community AAs (highlighted), and Logging. The main content area is titled "Registered Community AAs +". It displays a single entry for "Helmholtz dev-AAI" with the following details: Client ID: `publicplan_voapp_primary` and Authorization endpoint: `https://login-dev.helmholtz.de/oauth2-as/oauth2-Authz`. There are edit and delete icons to the right of the entry.

# VO FEDERATION

## Demo Screenshots



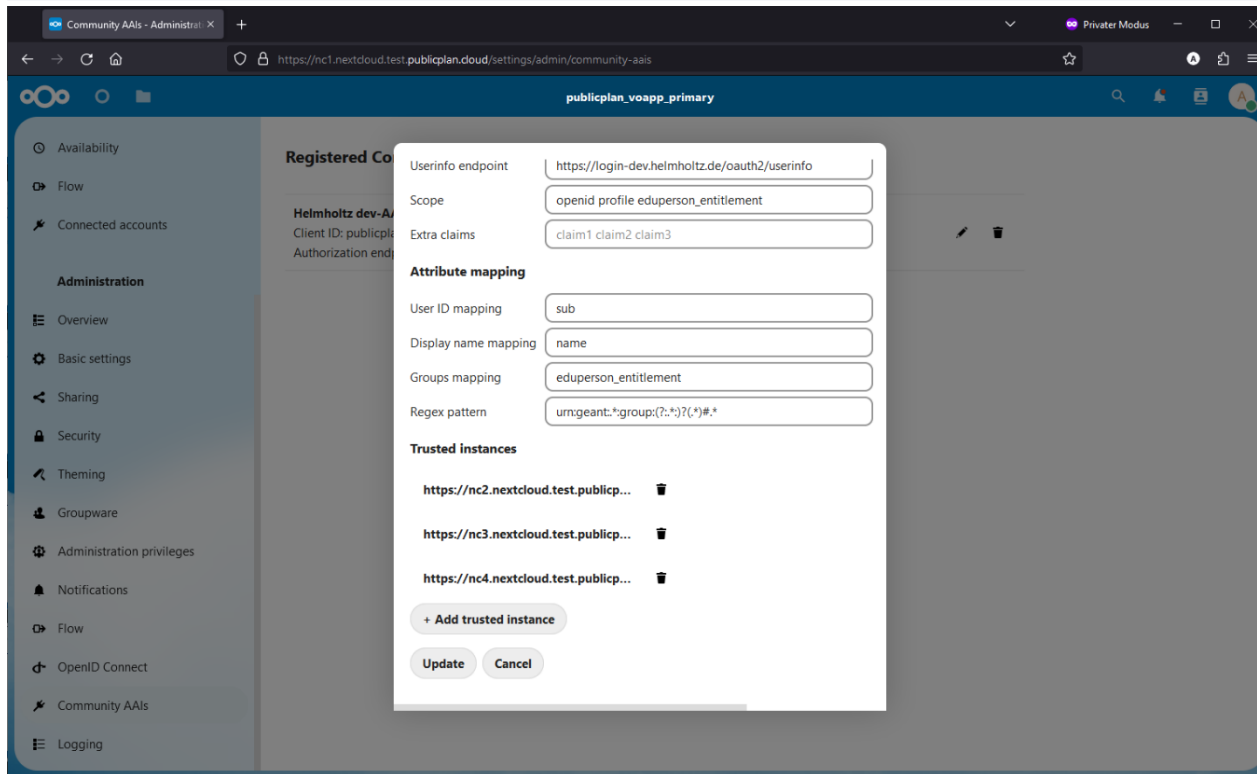
The screenshot shows a web browser window displaying the administration interface for 'publicplan\_voapp\_primary'. A modal window titled 'OIDC settings' is open, showing the configuration for a registered client named 'Helmholtz dev-AAI'. The client ID is 'publicplan\_voapp\_primary'. The settings include the following endpoints:

Field	Value
Name	Helmholtz dev-AAI
Client ID	publicplan_voapp_primary
Client secret	Leave empty to keep existing
Authorization endpoint	https://login-dev.helmholtz.de/oauth2-as/oauth2-Authz
Token endpoint	https://login-dev.helmholtz.de/oauth2/token
JWKS endpoint	https://login-dev.helmholtz.de/oauth2/jwk
Userinfo endpoint	https://login-dev.helmholtz.de/oauth2/userinfo






# VO FEDERATION

## Demo Screenshots

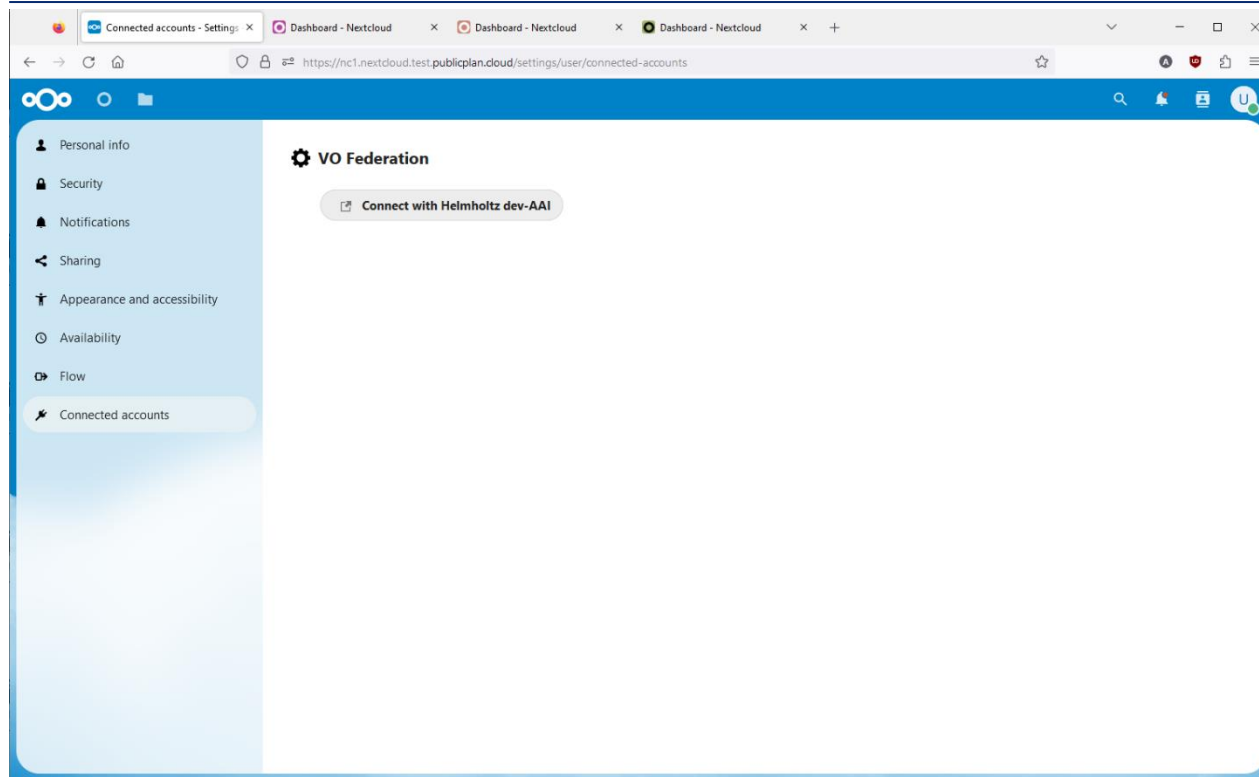


The screenshot shows the Nextcloud Administration interface for a community AAI. The main content area displays the configuration for a registered OpenID Connect application named "Helmholtz dev-A". A modal dialog is open for editing the application settings. The dialog contains the following fields and sections:

- Userinfo endpoint:**
- Scope:**
- Extra claims:**
- Attribute mapping:**
  - User ID mapping:**
  - Display name mapping:**
  - Groups mapping:**
  - Regex pattern:**
- Trusted instances:**
  - <https://nc2.nextcloud.test.publicplan.dcloud> 
  - <https://nc3.nextcloud.test.publicplan.dcloud> 
  - <https://nc4.nextcloud.test.publicplan.dcloud> 
- Buttons:**

# VO FEDERATION

## Demo Screenshots



Connected accounts - Settings | Dashboard - Nextcloud | Dashboard - Nextcloud | Dashboard - Nextcloud

https://nc1.nextcloud.test.publicplan.cloud/settings/user/connected-accounts

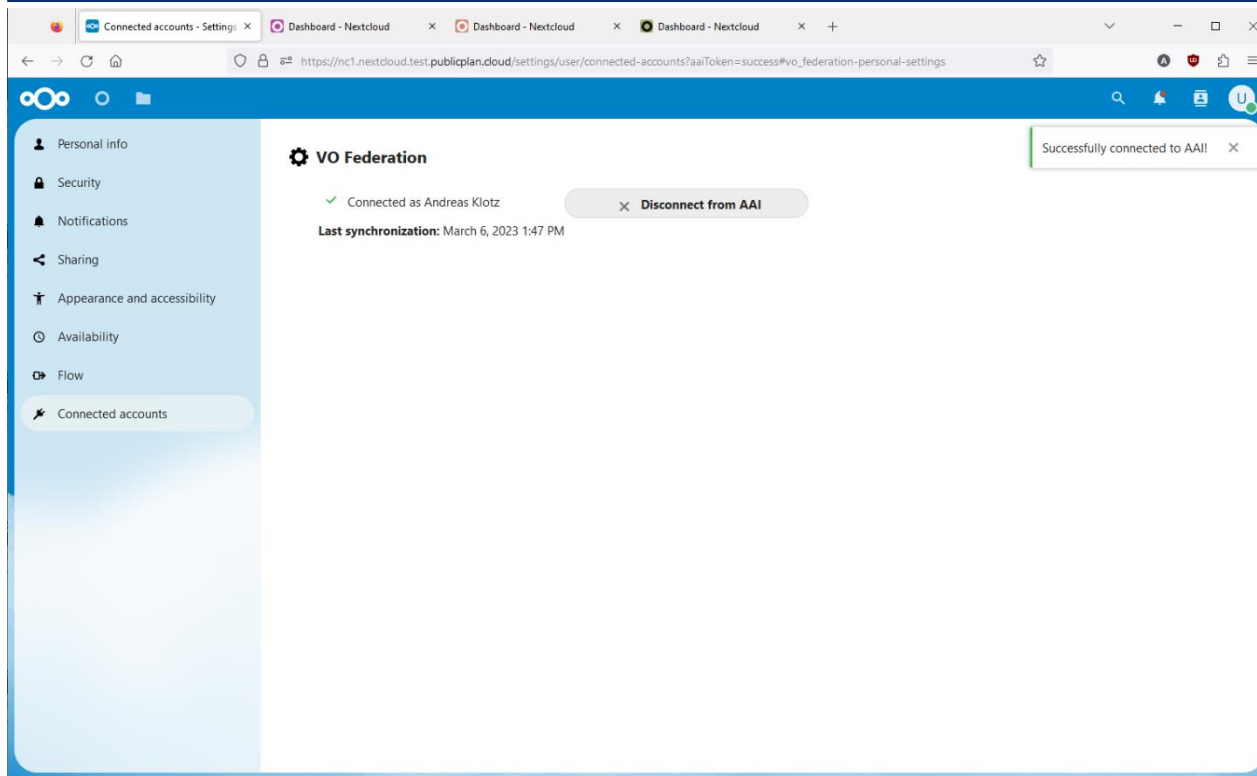
- Personal info
- Security
- Notifications
- Sharing
- Appearance and accessibility
- Availability
- Flow
- Connected accounts

### VO Federation

Connect with Helmholtz dev-AAI

# VO FEDERATION

## Demo Screenshots



Connected accounts - Settings | Dashboard - Nextcloud | Dashboard - Nextcloud | Dashboard - Nextcloud

https://nc1.nextcloud.test.publicplan.cloud/settings/user/connected-accounts?aaToken=success#vo\_federation-personal-settings

Personal info  
Security  
Notifications  
Sharing  
Appearance and accessibility  
Availability  
Flow  
Connected accounts

### VO Federation

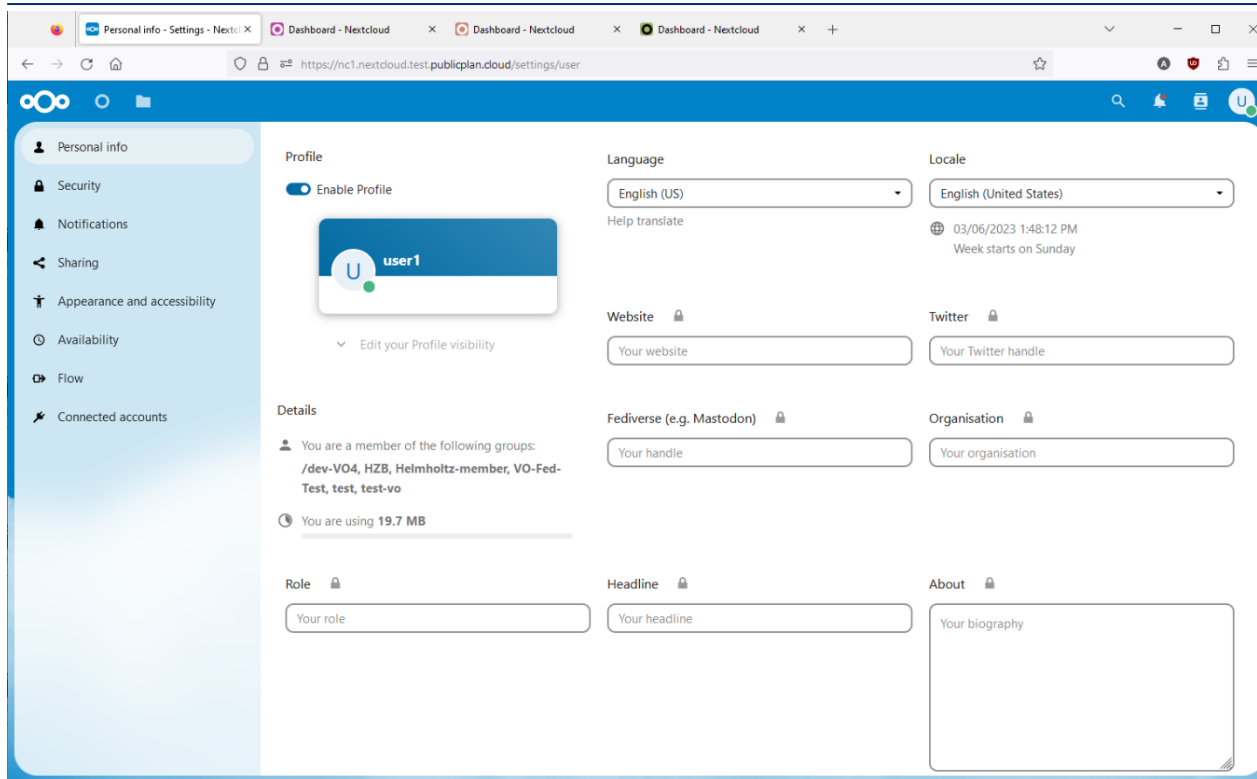
✓ Connected as Andreas Klotz [Disconnect from AAI](#)

Last synchronization: March 6, 2023 1:47 PM

Successfully connected to AAI!

# VO FEDERATION

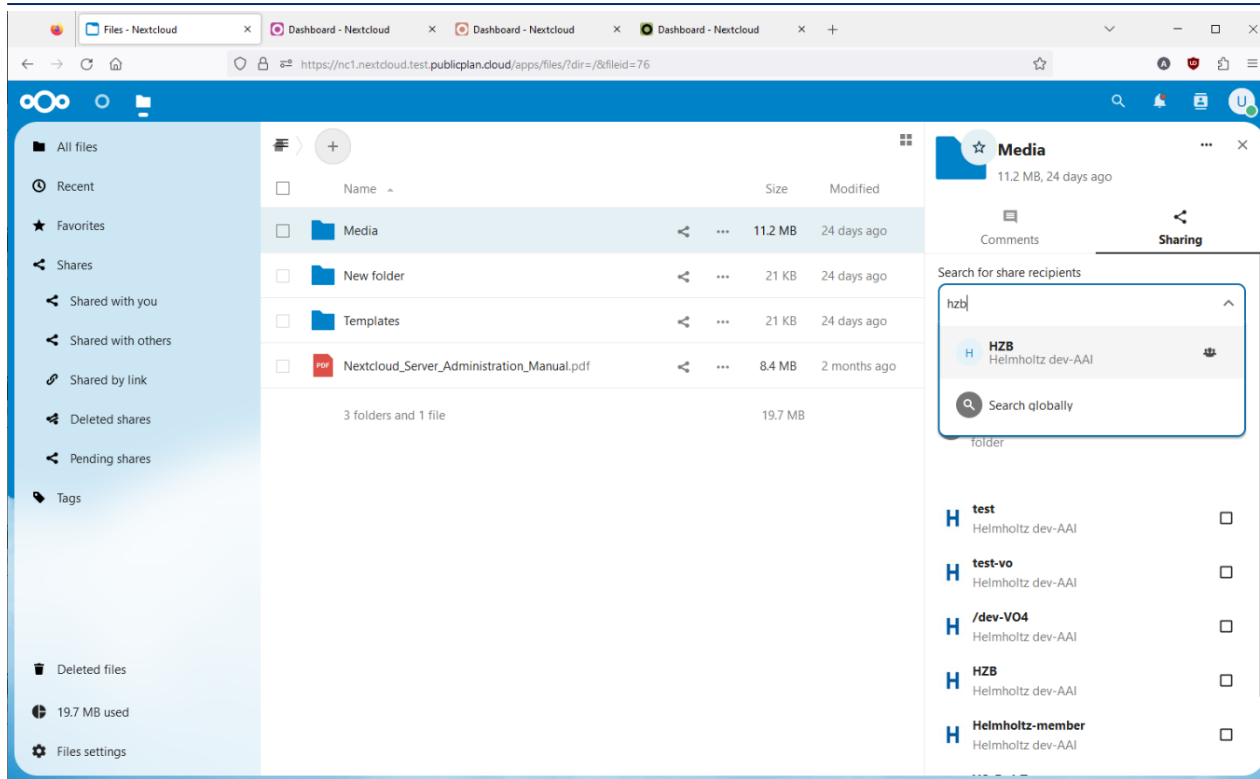
## Demo Screenshots



The screenshot shows a web browser window with multiple tabs. The active tab is titled "Personal info - Settings - Nextcloud" and the address bar shows the URL "https://nc1.nextcloud.test.publicplan.cloud/settings/user". The page content is a user profile settings interface with a blue header and a light blue sidebar on the left. The sidebar contains menu items: Personal info (selected), Security, Notifications, Sharing, Appearance and accessibility, Availability, Flow, and Connected accounts. The main content area is divided into several sections: Profile, Language, Locale, Website, Twitter, Details, Fediverse (e.g. Mastodon), Organisation, Role, Headline, and About. The Profile section includes an "Enable Profile" toggle (checked), a profile picture placeholder for "user1", and a link to "Edit your Profile visibility". The Language section has a dropdown menu set to "English (US)" and a "Help translate" link. The Locale section shows a date "03/06/2023 1:48:12 PM" and "Week starts on Sunday". The Website and Twitter sections each have a text input field for "Your website" and "Your Twitter handle" respectively. The Details section shows group membership: "/dev-VO4, HZB, Helmholtz-member, VO-Fed-Test, test, test-vo" and storage usage: "You are using 19.7 MB". The Fediverse and Organisation sections have text input fields for "Your handle" and "Your organisation". The Role, Headline, and About sections have text input fields for "Your role", "Your headline", and "Your biography".

# VO FEDERATION

## Demo Screenshots



The screenshot shows a web browser window displaying the Nextcloud file sharing interface. The browser's address bar shows the URL: `https://nc1.nextcloud.test.publicplan.cloud/apps/files/?dir=/&fileid=76`. The interface features a blue header with navigation icons and a search bar. On the left, a sidebar lists navigation options: All files, Recent, Favorites, Shares, Shared with you, Shared with others, Shared by link, Deleted shares, Pending shares, and Tags. At the bottom of the sidebar, it shows 'Deleted files', '19.7 MB used', and 'Files settings'. The main content area displays a file list with columns for Name, Size, and Modified. The files listed are:

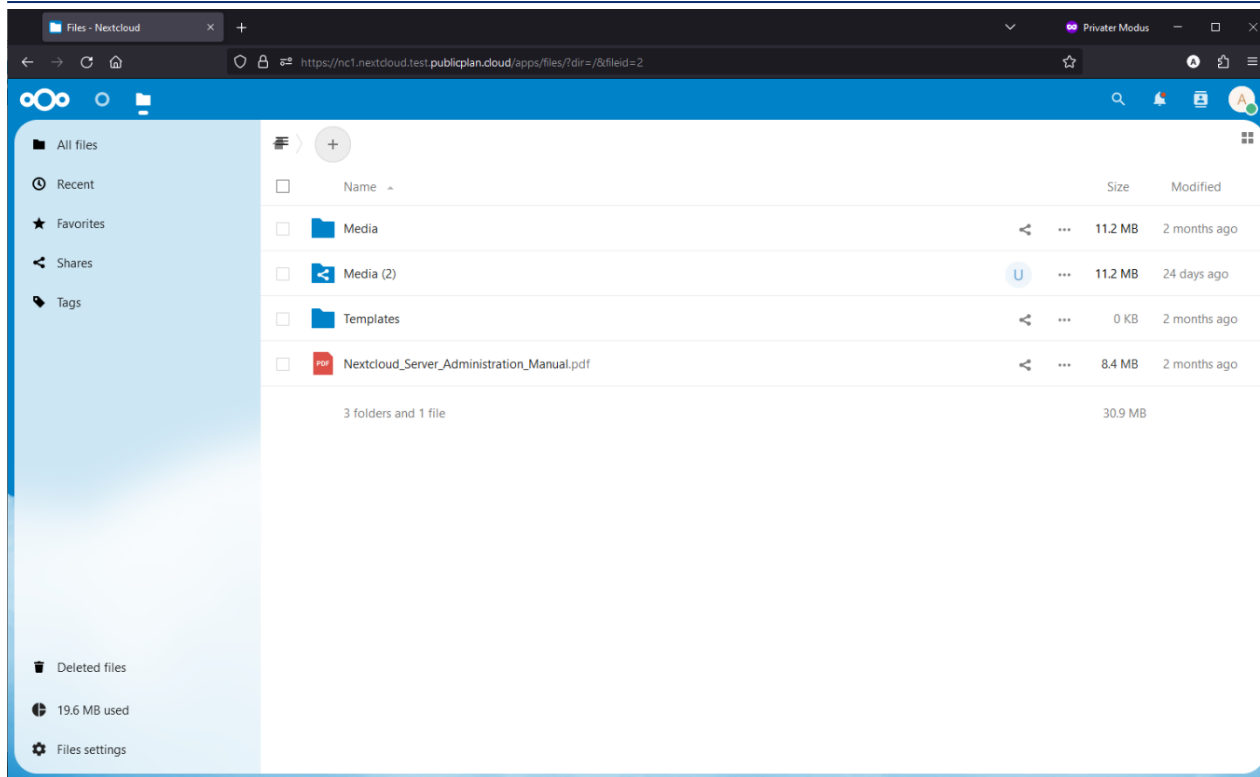
Name	Size	Modified
Media	11.2 MB	24 days ago
New folder	21 KB	24 days ago
Templates	21 KB	24 days ago
Nextcloud_Server_Administration_Manual.pdf	8.4 MB	2 months ago
3 folders and 1 file		19.7 MB

On the right side, a 'Media' share dialog is open, showing '11.2 MB, 24 days ago'. It includes a search bar for share recipients, which is currently displaying 'hzb'. Below the search bar, a list of recipients is shown, each with a checkbox:

- HZB** (Helmholtz dev-AAI)
- test** (Helmholtz dev-AAI)
- test-vo** (Helmholtz dev-AAI)
- /dev-VO4** (Helmholtz dev-AAI)
- HZB** (Helmholtz dev-AAI)
- Helmholtz-member** (Helmholtz dev-AAI)

# VO FEDERATION

## Demo Screenshots

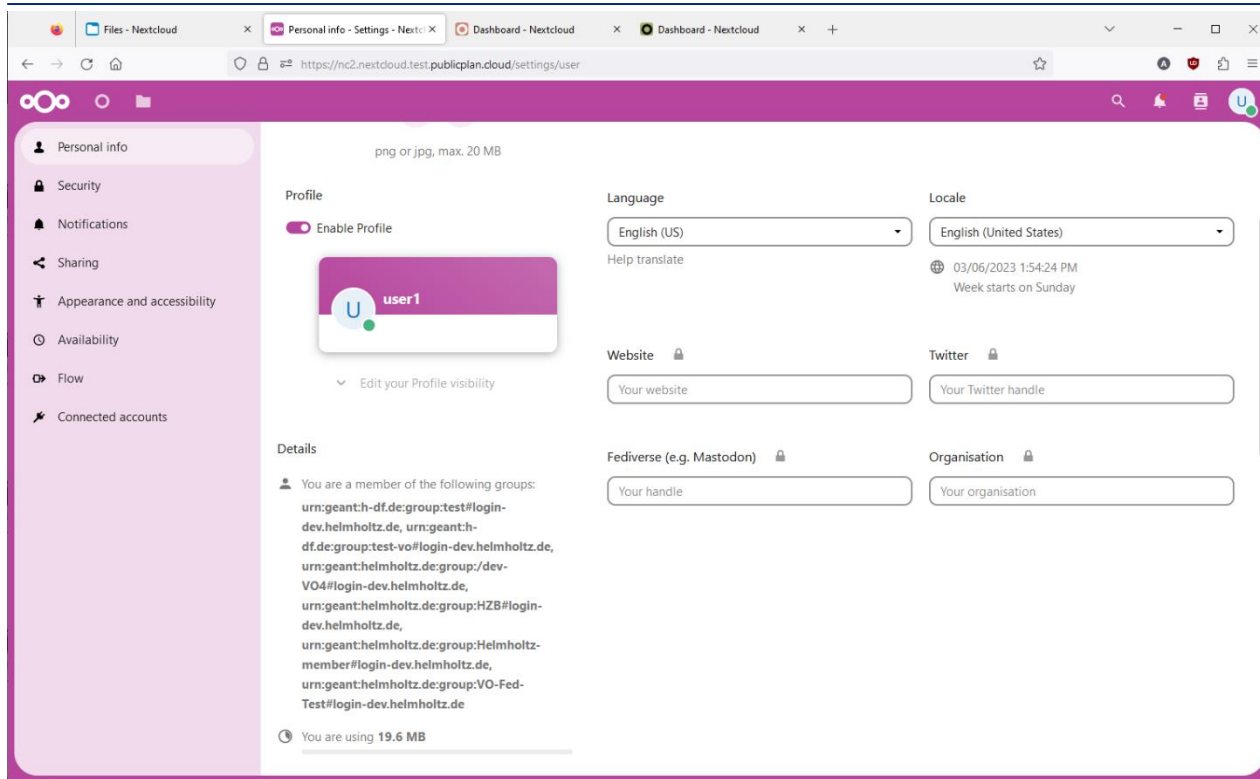


The screenshot shows the Nextcloud Files web interface in a browser window. The browser address bar displays the URL: `https://nc1.nextcloud.test.publiplan.cloud/apps/files/?dir=/&fileid=2`. The interface features a left sidebar with navigation options: All files, Recent, Favorites, Shares, Tags, Deleted files, 19.6 MB used, and Files settings. The main content area shows a file list with columns for Name, Size, and Modified. The list includes folders 'Media', 'Media (2)', and 'Templates', and a file 'Nextcloud\_Server\_Administration\_Manual.pdf'. A summary row indicates '3 folders and 1 file' with a total size of '30.9 MB'. The browser window title is 'Files - Nextcloud' and the user is logged in as 'Privater Modus'.

Name	Size	Modified
Media	11.2 MB	2 months ago
Media (2)	11.2 MB	24 days ago
Templates	0 KB	2 months ago
Nextcloud_Server_Administration_Manual.pdf	8.4 MB	2 months ago
3 folders and 1 file		30.9 MB

# VO FEDERATION

## Demo Screenshots



Files - Nextcloud x Personal info - Settings - Nextcloud x Dashboard - Nextcloud x Dashboard - Nextcloud x +

https://nc2.nextcloud.test.publicplan.cloud/settings/user

Personal info

Security

Notifications

Sharing

Appearance and accessibility

Availability

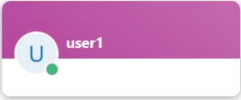
Flow

Connected accounts

png or jpg, max. 20 MB

Profile

Enable Profile



user1

Edit your Profile visibility

Language

English (US)

Help translate

Locale

English (United States)

03/06/2023 1:54:24 PM

Week starts on Sunday

Website

Your website

Twitter

Your Twitter handle

Fediverse (e.g. Mastodon)

Your handle

Organisation

Your organisation

Details

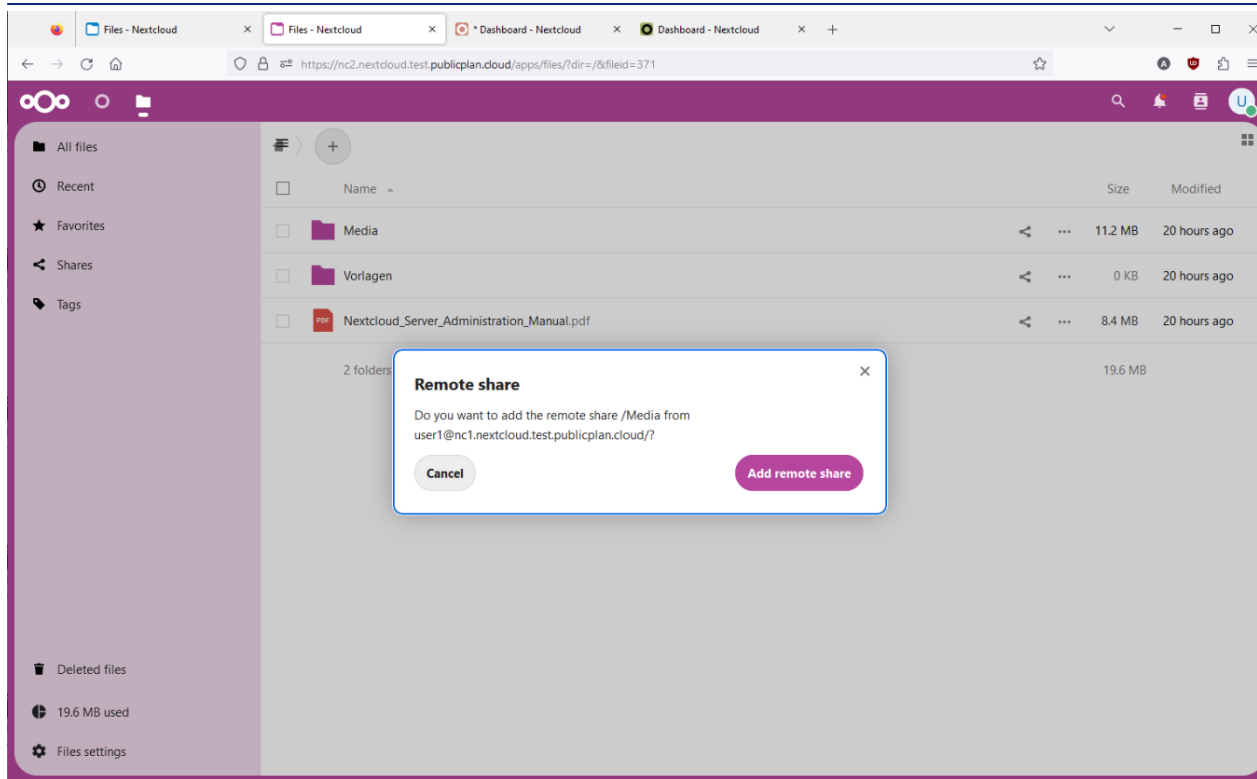
You are a member of the following groups:

- urn:geant:h-df.de:group:test#login-dev.helmholtz.de, urn:geant:h-df.de:group:test-vo#login-dev.helmholtz.de,
- urn:geant:helmholtz.de:group:/dev-VO4#login-dev.helmholtz.de,
- urn:geant:helmholtz.de:group:H2B#login-dev.helmholtz.de,
- urn:geant:helmholtz.de:group:Helmholtz-member#login-dev.helmholtz.de,
- urn:geant:helmholtz.de:group:VO-Fed-Test#login-dev.helmholtz.de

You are using 19.6 MB

# VO FEDERATION

## Demo Screenshots



The screenshot shows the Nextcloud file manager interface. The browser address bar displays the URL: `https://nc2.nextcloud.test.publicplan.cloud/apps/files/?dir=/&fileid=371`. The interface includes a sidebar with navigation options: All files, Recent, Favorites, Shares, Tags, Deleted files, 19.6 MB used, and Files settings. The main content area shows a file list with columns for Name, Size, and Modified. The files listed are:

Name	Size	Modified
Media	11.2 MB	20 hours ago
Vorlagen	0 KB	20 hours ago
Nextcloud_Server_Administration_Manual.pdf	8.4 MB	20 hours ago
2 folders	19.6 MB	

A modal dialog box titled "Remote share" is displayed in the foreground. It contains the following text:

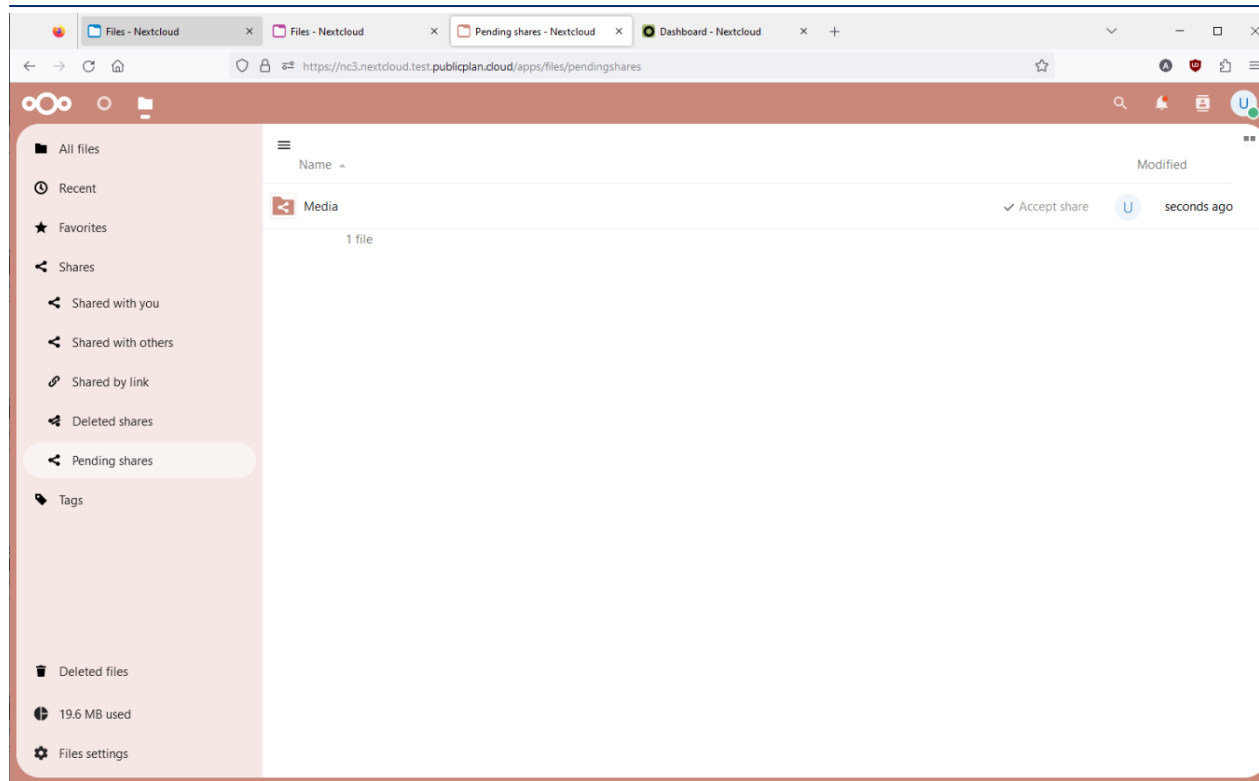
Do you want to add the remote share /Media from user1@nc1.nextcloud.test.publicplan.cloud/?

The dialog has two buttons: "Cancel" and "Add remote share".



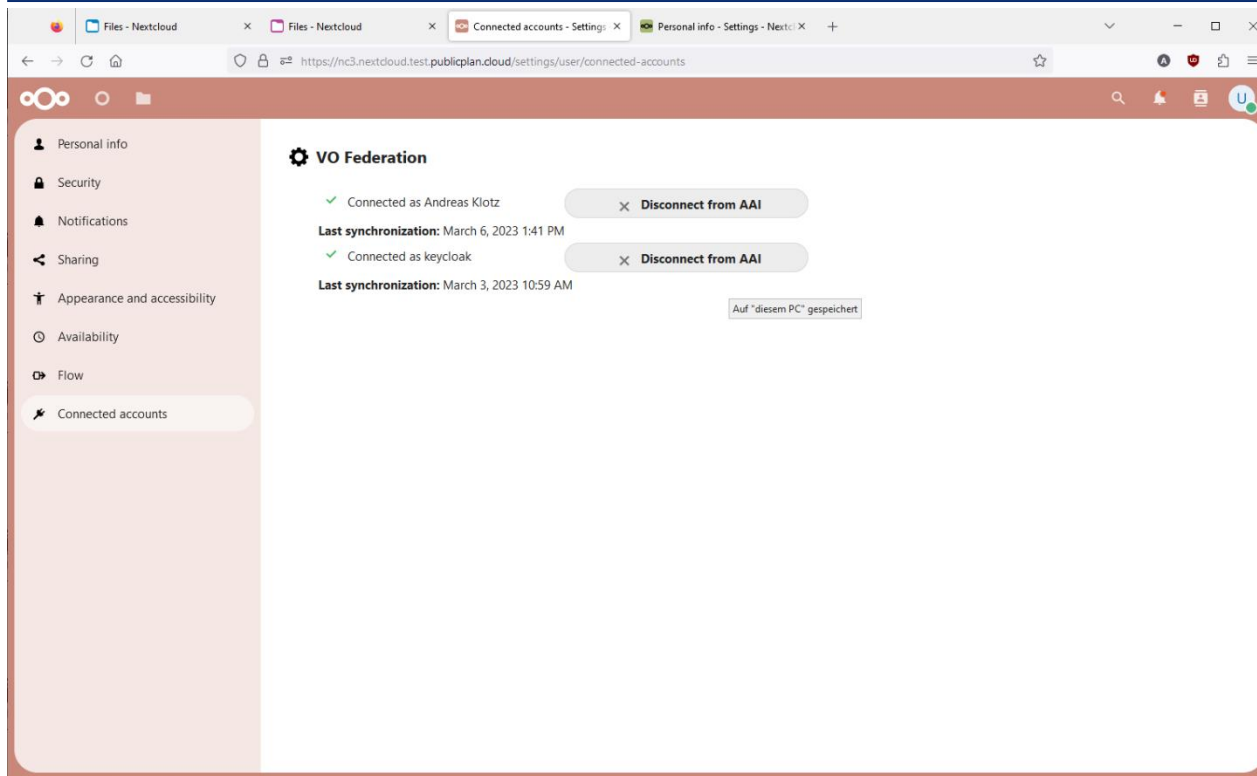
# VO FEDERATION

## Demo Screenshots



# VO FEDERATION

## Demo Screenshots



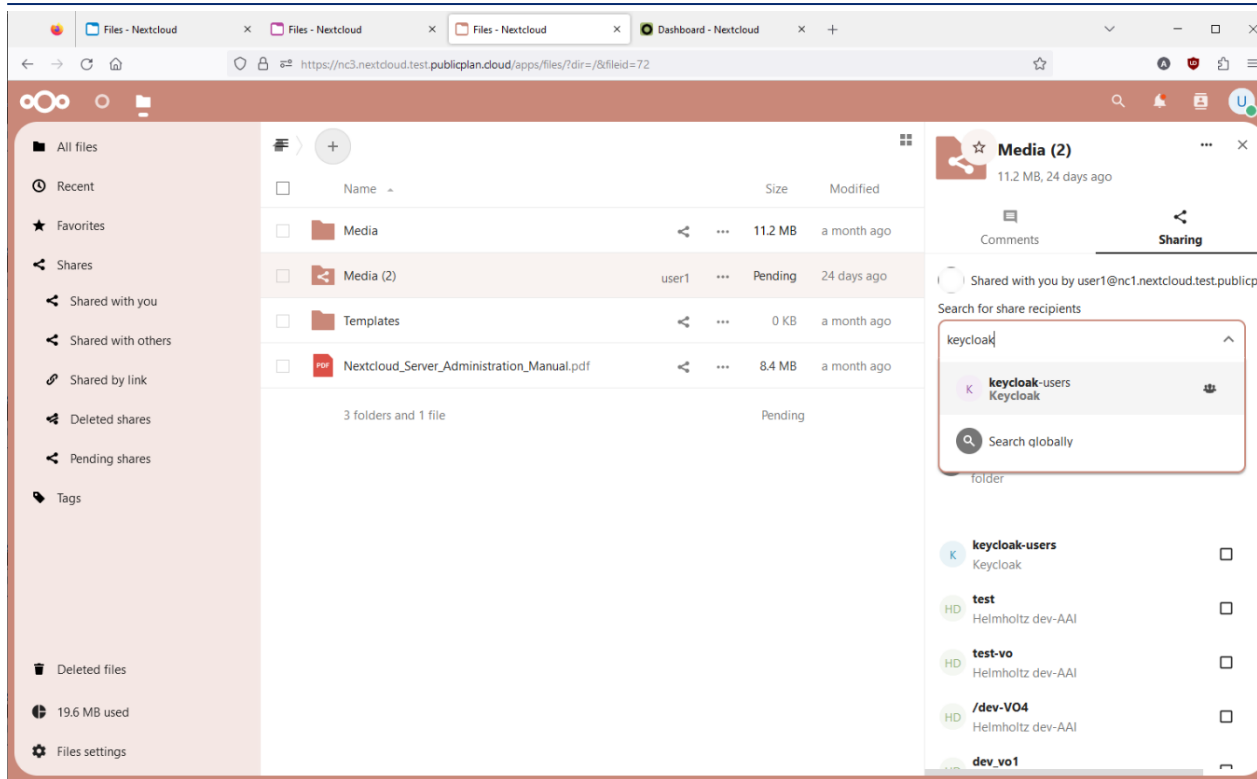
The screenshot shows a web browser window with the URL `https://nc3.nextcloud.test.publicplan.cloud/settings/user/connected-accounts`. The page displays the 'VO Federation' settings. On the left, a sidebar menu includes 'Personal info', 'Security', 'Notifications', 'Sharing', 'Appearance and accessibility', 'Availability', 'Flow', and 'Connected accounts'. The main content area is titled 'VO Federation' and shows two connected accounts:

- Connected as Andreas Klotz (with a 'Disconnect from AAI' button) and a last synchronization time of March 6, 2023 1:41 PM.
- Connected as keycloak (with a 'Disconnect from AAI' button) and a last synchronization time of March 3, 2023 10:59 AM.

A small tooltip at the bottom right of the page reads 'Auf "diesem PC" gespeichert'.

# VO FEDERATION

## Demo Screenshots



The screenshot shows a web browser window displaying the Nextcloud file sharing interface. The browser's address bar shows the URL: `https://nc3.nextcloud.test.publicplan.cloud/apps/files/?dir=/&fileid=72`. The interface includes a sidebar on the left with navigation options like 'All files', 'Recent', 'Favorites', 'Shares', and 'Tags'. The main content area displays a file list with columns for 'Name', 'Size', and 'Modified'. The list includes folders 'Media' (11.2 MB, a month ago) and 'Media (2)' (Pending, 24 days ago), and a file 'Nextcloud\_Server\_Administration\_Manual.pdf' (8.4 MB, a month ago). A sharing dialog is open on the right for the 'Media (2)' folder, showing it is shared with 'user1@nc1.nextcloud.test.publicplan.cloud'. The dialog includes a search bar for share recipients, with 'keycloak' entered. A dropdown menu shows search results for 'keycloak-users' (Keycloak) and other users like 'test', 'test-vo', and 'dev-vo1'. The 'keycloak-users' entry is highlighted.

Name	Size	Modified
Media	11.2 MB	a month ago
Media (2)	Pending	24 days ago
Templates	0 KB	a month ago
Nextcloud_Server_Administration_Manual.pdf	8.4 MB	a month ago

3 folders and 1 file Pending

Media (2) 11.2 MB, 24 days ago

Shared with you by user1@nc1.nextcloud.test.publicplan.cloud

Search for share recipients

keycloak

- keycloak-users Keycloak
- test Helmholtz dev-AAI
- test-vo Helmholtz dev-AAI
- /dev-VO4 Helmholtz dev-AAI
- dev\_vo1