

Nextcloud AIO

Purpose

Nextcloud AIO provides private file storage, synchronization, sharing, productivity, and collaboration services for the Bytek environment.

Nextcloud currently supports or is intended to support:

- Personal file storage.
- Shared folders.
- File synchronization across computers and mobile devices.
- Public and private file sharing.
- Calendar synchronization.
- Contact synchronization.
- Tasks and notes.
- Browser-based document editing.
- Simultaneous document collaboration.
- Authentik single sign-on.
- Desktop and mobile Nextcloud clients.
- WebDAV, CalDAV, and CardDAV access.
- Optional photo, communication, and productivity applications.

Nextcloud runs as an isolated application VM and uses Nextcloud All-in-One to manage its containers.

Service Information

Setting	Value
Service name	Nextcloud AIO
Private IP address	192.168.2.100

Public hostname	cloud.bytek.ca
AIO management port	TCP 8080
Traefik backend port	TCP 11000
Deployment directory	/opt/nextcloud-aio
Operating-system disk	64 GB
User-data disk	500 GB
User-data mount	/mnt/nextcloud-data
Nextcloud data directory	/mnt/nextcloud-data/ncdata
Reverse proxy	Traefik
Authentication	Authentik OIDC
Office integration	AIO-managed Collabora CODE
Time zone	America/Toronto
Backup coverage	Proxmox OS and data-disk backup
Proxmox VM ID	Confirm current VM ID

User application:

[Open Nextcloud](#)

AIO management address:

https://192.168.2.100:8080/

Architecture Role

Nextcloud is the central user-file and collaboration platform.

Nextcloud is separate from:

- BookStack documentation.
- Vikunja task management.
- Authentik identity management.
- Traefik HTTPS routing.
- Uptime Kuma monitoring.
- Proxmox infrastructure management.

This separation limits the effect of an application failure and allows Nextcloud storage to grow independently from the infrastructure VMs.

Container Architecture

Nextcloud AIO manages the application stack.

Core containers include equivalents of:

- AIO master container.
- Apache and Caddy.
- Nextcloud.
- PostgreSQL.
- Redis.
- Notify Push.
- Domain validation during initial setup.

Optional containers may include:

- Collabora Online.
- ClamAV.
- Full-text search.
- Imaginary.
- Nextcloud Talk.
- Talk recording.
- HaRP.
- Whiteboard.
- Community containers.

Optional containers should be added one at a time and tested before enabling another.

Public Request Flow

When an external user opens Nextcloud:

1. The browser opens `ccloud.bytek.ca`.
 2. WHC public DNS resolves the hostname to `38.29.213.101`.
 3. The public VPS accepts the HTTPS connection.
 4. The VPS forwards the traffic through WireGuard.
 5. The home WireGuard gateway forwards the request to Traefik.
 6. Traefik receives the request for `ccloud.bytek.ca`.
 7. Traefik forwards the request to `192.168.2.100` on TCP port 11000.
 8. The AIO Apache container serves Nextcloud.
-

Internal Request Flow

When a LAN user opens Nextcloud:

1. The client queries Pi-hole.
2. Pi-hole resolves `ccloud.bytek.ca` to `192.168.2.182`.
3. The client connects directly to Traefik.
4. Traefik forwards the request to `192.168.2.100:11000`.
5. Nextcloud serves the request.

Internal clients use the same HTTPS hostname as external clients.

Traefik Route

The Nextcloud Traefik router uses:

Setting	Value
Hostname rule	<code>ccloud.bytek.ca</code>
Entry point	<code>websecure</code>
Certificate resolver	<code>letsencrypt</code>
Backend protocol	HTTP
Backend destination	<code>192.168.2.100:11000</code>
Host-header forwarding	Enabled
Authentik ForwardAuth	Disabled

Do not attach Authentik ForwardAuth to the Nextcloud Traefik router.

Nextcloud requires direct access for:

- Desktop clients.
- Mobile clients.
- WebDAV.
- CalDAV.
- CardDAV.
- Application passwords.
- Public shares.
- Federation.
- Synchronization APIs.

Nextcloud performs user authentication through its native OIDC integration.

AIO Management Interface

The AIO management interface is available only by private IP:

```
https://192.168.2.100:8080/
```

The management interface uses its own certificate, so a browser warning may appear.

Always use the private IP for AIO management.

Do not use:

- `ccloud.bytek.ca:8080`
- A public WHC record.
- A Traefik public router.
- VPS forwarding.
- Public router forwarding.
- Authentik ForwardAuth.

The AIO management interface controls:

- Container startup and shutdown.

- Updates.
- Optional containers.
- Backup settings.
- AIO passphrase.
- Application version selection.
- Time-zone settings.
- Container logs.

Restricted Ports

The following ports must not be exposed publicly:

Port	Purpose
TCP 8080	AIO management
TCP 11000	AIO Apache backend
TCP 8443	AIO-managed certificate interface, not used in this reverse-proxy design
TCP 9000	Internal AIO service
Docker socket	Container management

Only Traefik should reach TCP port 11000 during normal operation.

LAN administrators may reach TCP port 8080.

Storage Architecture

Nextcloud uses separate virtual disks for the operating system and user data.

Operating-System Disk

Setting	Value
Nominal size	64 GB

Proxmox storage	local-lvm
Root filesystem	ext4
Purpose	Debian, Docker, AIO configuration, and system files

User-Data Disk

Setting	Value
Nominal size	500 GB
Proxmox storage	user-data
Guest device	/dev/sda1 at the time of configuration
Filesystem	ext4
Filesystem label	nextcloud-data
Mount point	/mnt/nextcloud-data
Nextcloud data path	/mnt/nextcloud-data/ncdata
Mount options	Defaults and noatime

The operating-system disk appeared as /dev/sdb, while the 500 GB data disk appeared as /dev/sda during initial configuration.

Linux device names may change, so the permanent mount uses the filesystem UUID rather than /dev/sda1.

Data-Disk Validation

Confirm the data disk is mounted using:

```
findmnt /mnt/nextcloud-data
```

Confirm available capacity using:

```
df -h /mnt/nextcloud-data
```

Confirm the filesystem using:

```
lsblk -o NAME,SIZE,FSTYPE,LABEL,UUID,MOUNTPOINTS
```

Confirm the data directory exists using:

```
sudo ls -ld /mnt/nextcloud-data/ncdata
```

The Nextcloud containers should not be started if the expected data filesystem is missing.

Starting the application with an unmounted data path could cause data to be written to the operating-system disk instead.

Filesystem Mount

The data filesystem is mounted through `/etc/fstab` using its UUID.

The mount point is:

```
/mnt/nextcloud-data
```

The intended behavior is:

- The disk mounts automatically at boot.
- The mount fails visibly if the filesystem is unavailable.
- The path remains consistent even if Linux device letters change.
- Nextcloud AIO always receives the same data location.

Review the mount after every storage or boot issue.

AIO Data Directory

The AIO deployment uses:

- **Nextcloud data directory:** `/mnt/nextcloud-data/ncdata`

The directory should remain on the 500 GB user-data disk.

Do not move the directory manually while Nextcloud containers are running.

Do not directly edit files inside the Nextcloud data directory using normal filesystem tools unless following a documented recovery process.

Nextcloud tracks files through its database and filesystem metadata.

Files manually copied into the data directory may not appear correctly until an application-level rescan is performed.

Authentication

Nextcloud uses native OpenID Connect through Authentik.

The installed Nextcloud application is:

- **OpenID Connect user backend**
- **Application ID:** `user_oidc`

Do not install another OIDC login application alongside it unless a migration is deliberately planned.

Avoid enabling overlapping authentication applications such as:

- OpenID Connect Login.
- Social Login.
- OpenID Connect SSO by Gluu.
- OIDC Identity Provider.

The OIDC Identity Provider application serves the opposite role by making Nextcloud an identity provider.

Authentik OIDC Configuration

Setting	Value
Authentik application name	Nextcloud
Application slug	<code>nextcloud</code>
Provider type	OAuth2/OpenID Connect
Client type	Confidential
Subject mode	User UUID

Signing key	Selected
Encryption key	None
Authorization callback	<code>https://cloud.bytek.ca/apps/user_oidc/code</code>
Required group	<code>bytek-users</code>
Required policy	<code>Allow bytek.ca users</code>
Policy engine	<code>ALL</code>

Normal users must:

- Belong to `bytek-users`.
- Pass the `Allow bytek.ca users` policy.

Do not attach `bytek-admin` as another required `ALL` binding for normal Nextcloud access.

Administrators who need Nextcloud should also belong to `bytek-users`.

Nextcloud OIDC Settings

Setting	Value
Provider identifier	<code>authentik</code>
Discovery endpoint	Authentik discovery URL for application slug <code>nextcloud</code>
Scopes	<code>openid email profile</code>
User ID mapping	<code>sub</code>
Display-name mapping	<code>name</code>
Email mapping	<code>email</code>

The OIDC discovery endpoint must be reachable from inside the Nextcloud application container.

The client ID and client secret must match the Authentik Nextcloud provider.

Do not place the client secret in BookStack.

OIDC Login Flow

1. The user opens `cloud.bytek.ca`.
2. Nextcloud offers Authentik login.
3. The browser is redirected to `portal.bytek.ca`.
4. Authentik requests authentication and MFA.
5. Authentik evaluates the `bytek-users` group.
6. Authentik evaluates the Bytek email policy.
7. Authentik redirects to the Nextcloud callback.
8. Nextcloud validates the OIDC response.
9. Nextcloud creates or matches the user.
10. The user enters Nextcloud.

Nextcloud application permissions remain controlled inside Nextcloud.

Local Break-Glass Administrator

The local Nextcloud administrator must remain available.

The local account provides recovery when:

- Authentik is unavailable.
- Pi-hole is unavailable.
- OIDC is misconfigured.
- Authentik policies deny access.
- The user OIDC application fails.
- A signing or discovery problem occurs.

The direct local-login path is:

[Open the Nextcloud Local Login](#)

The local administrator password must:

- Be unique.
- Be stored in the password manager.
- Differ from the Authentik password.
- Be rotated if exposed.
- Be tested periodically.

A local Nextcloud second factor may be enabled for the break-glass account if recovery codes are stored securely.

Trusted Proxy

Nextcloud must trust Traefik as its reverse proxy.

Expected trusted proxy:

- 192.168.2.182

Review using:

```
sudo docker exec --user www-data nextcloud-aio-nextcloud php occ config:system:get trusted_proxies
```

The output should include Traefik's current private address.

If Traefik's IP changes, update:

- Nextcloud trusted proxies.
- Traefik route.
- Pi-hole records if required.
- Proxmox firewall rules.
- Uptime Kuma monitors.
- Documentation.

HTTPS Detection

Nextcloud must generate HTTPS URLs when accessed through Traefik.

If Nextcloud generates HTTP links, investigate:

- Trusted proxy.
- Forwarded protocol headers.
- `overwriteprotocol`.
- `overwrite.cli.url`.
- `APP_URL` equivalent settings.

- Traefik host-header forwarding.

The expected external URL is:

```
https://cloud.bytek.ca
```

Do not set the external URL to the private IP or TCP port 11000.

Office Integration

Nextcloud uses the AIO-managed Collabora Online container.

This component provides browser-based document editing and simultaneous collaboration.

The Nextcloud Office application connects Nextcloud to the AIO-managed Collabora CODE server.

Do not also install the separate Built-in CODE Server application.

Using both would create competing office backends and complicate troubleshooting.

Office Dictionaries

Configured dictionaries:

- `en_US`
- `fr_FR`

These provide:

- English, United States.
- French, France.

Canadian French would normally use `fr_CA`, but the AIO interface should be checked before adding a locale not listed as supported.

Locale values are separated by spaces.

Office Validation

To validate collaborative editing:

1. Sign in as the first Nextcloud user.
2. Create or upload an office document.
3. Open the document in the browser editor.
4. Share the document with a second user.
5. Open a private browser session.
6. Sign in as the second user.
7. Open the same document.
8. Make an edit from each session.
9. Confirm both sessions see updates.
10. Confirm the file is saved in Nextcloud.

If a document does not open:

- Check the AIO Collabora container.
 - Check Nextcloud Office settings.
 - Check Nextcloud logs.
 - Check Traefik.
 - Check browser console errors.
 - Check the Collabora container log.
-

Enabled Applications

Recommended core applications include:

- Files.
- OpenID Connect user backend.
- Nextcloud Office.
- Calendar.
- Contacts.
- Tasks.
- Notes.

Applications that may be added later include:

- Team Folders.
- Deck.
- Forms.
- Collectives.
- Memories.
- Imaginary.
- Talk.
- Mail.
- Whiteboard.

Add applications only when there is a clear use case.

Every additional application becomes part of:

- Update testing.
 - Backup scope.
 - Database growth.
 - Background processing.
 - Compatibility testing.
 - Recovery procedures.
-

Team Folders

Team Folders may be used for administrator-managed shared storage.

Use Team Folders instead of placing every shared resource inside one user's personal files.

Possible shared folders include:

- Shared Documents.
- Family Photos.
- Game Project.
- Common Resources.
- Collaboration Files.

Team Folder permissions should use stable Nextcloud users and groups after OIDC account provisioning has been tested.

Optional AIO Containers

Collabora

Enabled for browser-based document editing.

Imaginary

May be enabled later for expanded preview support.

Possible preview formats include:

- HEIC.
- HEIF.
- PDF.
- SVG.
- TIFF.
- WebP.

Review compatibility before enabling server-side encryption.

ClamAV

May be enabled later for antivirus scanning.

ClamAV requires additional memory and may affect upload processing.

Full-Text Search

May be enabled later when enough content exists to justify indexing.

Initial indexing can consume significant resources and affect availability.

Nextcloud Talk

May be enabled later.

Talk requires deliberate network configuration, including TCP and UDP port 3478 for TURN functionality.

Do not enable Talk before designing the complete VPS, WireGuard, firewall, and guest-port path.

HaRP

May be enabled if a future ExApp requires it.

Do not enable it without a specific application requirement.

Docker Socket Proxy

Do not enable the deprecated Docker Socket Proxy when HaRP is the supported alternative for the intended application.

Community Containers

AIO Community Containers are not official core Nextcloud containers.

Community containers may:

- Have independent maintenance.
- Introduce additional dependencies.
- Become incompatible.
- Require additional ports.
- Expand backup size.
- Complicate AIO updates.

Do not enable community containers merely because they are available.

Plex was considered as an AIO Community Container but rejected in favor of a dedicated Plex VM.

Reasons include:

- GPU isolation.
- Service separation.

- Backup control.
 - Network separation.
 - Avoiding dependency between Plex and Nextcloud.
 - Keeping the media library outside the Nextcloud VM.
-

Time Zone

Nextcloud AIO uses:

- `America/Toronto`

The Debian host should also use:

- `America/Toronto`

Verify the host using:

```
timedatectl
```

Expected properties:

- Correct local time.
- Correct UTC time.
- System clock synchronized.
- NTP active.
- RTC stored in UTC.

The AIO time-zone setting and Debian host time zone are separate settings.

Email Configuration

Nextcloud should use SMTP for:

- User notifications.
- Shares.
- Security events.

- Password-related messages.
- Calendar invitations.
- Administrative alerts.

WHC SMTP settings should be obtained from:

- cPanel.
- Email Accounts.
- Connect Devices.
- Manual configuration.

Typical secure combinations include:

Port	Encryption
587	STARTTLS
465	SSL/TLS

The full mailbox address is normally used as the SMTP username.

Use the mailbox password, not the cPanel password.

Do not store the SMTP password in BookStack.

Email Troubleshooting

If Nextcloud cannot send email:

1. Confirm the mailbox credentials in WHC webmail.
2. Confirm the exact WHC SMTP hostname.
3. Confirm the selected port and encryption match.
4. Test DNS from the Nextcloud VM.
5. Test TCP reachability from the VM.
6. Test TCP reachability from the Nextcloud container.
7. Test STARTTLS using OpenSSL if using port 587.
8. Review the Nextcloud log.
9. Review cPanel Email Track Delivery.
10. Contact WHC support only after collecting the exact error.

If no attempt appears in cPanel Track Delivery, the message may not have reached the WHC mail server.

Application Administration Overview

Review the Nextcloud administration overview after installation and updates.

Common warnings may include:

- Missing default phone region.
- Email server not configured.
- Maintenance window.
- Missing database indexes.
- Mimetype migrations.
- Background-job configuration.
- Proxy-header issues.
- HTTPS URL detection.
- App compatibility warnings.

Use the exact warning text from the installed Nextcloud version before running administrative commands.

Do not copy commands from unrelated versions without reviewing the current warning.

Default Phone Region

For Canadian phone numbers, use:

-

This helps Nextcloud interpret local phone-number formats.

Review the current value using the Nextcloud system configuration.

Container Management

Nextcloud AIO containers should be managed through the AIO interface whenever practical.

AIO management address:

```
https://192.168.2.100:8080/
```

Use the AIO interface for:

- Starting containers.
- Stopping containers.
- Updating containers.
- Adding optional containers.
- Removing optional containers.
- Reviewing container logs.
- Changing the AIO configuration.

Do not manually recreate AIO-generated application containers unless following an AIO-specific recovery procedure.

Docker Compose Management

The master container deployment is stored under:

```
/opt/nextcloud-aio
```

Move to the directory using:

```
cd /opt/nextcloud-aio
```

Validate Compose using:

```
sudo docker compose config --quiet
```

Check the master container using:

```
sudo docker compose ps
```

View master-container logs using:

```
sudo docker logs nextcloud-aio-mastercontainer --tail 100
```

Container-level settings in the master Compose definition require recreation of the master container.

AIO-managed child containers remain controlled through AIO.

Container Health

List containers using:

```
sudo docker ps --format='table {{.Names}}\t{{.Status}}\t{{.Ports}}'
```

Expected core containers include equivalents of:

- nextcloud-aio-mastercontainer
- nextcloud-aio-database
- nextcloud-aio-redis
- nextcloud-aio-nextcloud
- nextcloud-aio-apache
- nextcloud-aio-notify-push
- Collabora container when enabled

A running container may still be unhealthy.

Review the status and relevant application endpoint.

Backend Validation

Confirm TCP port 11000 from the Nextcloud VM using:

```
curl -I http://127.0.0.1:11000/
```

Confirm from the Traefik VM using:

```
curl -I http://192.168.2.100:11000/
```

A redirect or Nextcloud response confirms the HTTP backend is reachable.

A timeout indicates a firewall or routing issue.

A connection refusal indicates that the VM was reached but no service is listening.

Public Validation

Validate the public hostname using:

[Open Nextcloud](#)

Expected behavior:

- Valid Let's Encrypt certificate.
- Redirect to the Nextcloud login page when unauthenticated.
- Secure session cookies.
- HTTPS links.
- Authentik login option.

A browser cache previously caused a Firefox TLS error while Edge worked.

Before changing Traefik or certificates, test:

- Another browser.
 - Private mode.
 - Browser DNS cache.
 - Browser socket cache.
 - DNS over HTTPS.
 - Operating-system DNS.
-

Monitoring

Recommended Uptime Kuma monitors include:

Monitor	Target
---------	--------

Nextcloud VM	Ping <code>192.168.2.100</code>
Nextcloud AIO Apache	TCP <code>192.168.2.100:11000</code>
Nextcloud Through Traefik	<code>https://cloud.bytek.ca/status.php</code>
Nextcloud certificate	<code>cloud.bytek.ca</code>
AIO management	Optional private monitor on TCP 8080

Expected routed status:

- HTTP 200.

The Nextcloud VM firewall must allow Uptime Kuma if direct monitoring is used.

Firewall Policy

AIO Management

Allow TCP port 8080 only from approved LAN or VPN management sources.

AIO Apache Backend

Allow TCP port 11000 from:

- Traefik at `192.168.2.182`.
- Uptime Kuma at `192.168.2.115` only if direct backend monitoring is used.

SSH

Allow SSH only from approved LAN or VPN administration sources.

Public Exposure

Do not publicly forward:

- TCP 8080.
 - TCP 11000.
 - TCP 8443.
 - Docker ports.
 - Database ports.
 - Redis ports.
-

Backup Architecture

The AIO Borg backup location is currently not configured.

This is intentional because the currently available local destinations are not sufficiently separate from the live data or existing Proxmox backup.

Current backup protection consists of:

- Proxmox backup of the 64 GB operating-system disk.
- Proxmox backup of the 500 GB data disk.
- Backup archive stored on the dedicated 4 TB HDD.

An AIO Borg repository placed on the same Nextcloud data disk would not protect against failure of that disk.

It would also cause the Proxmox backup to contain both live data and an embedded Borg backup copy.

Future AIO Backup

A future AIO Borg repository should use:

- Another physical computer.
- A remote Borg server.
- A dedicated storage device not included in the Nextcloud VM.
- A trusted remote host.
- A dedicated future backup platform.

A remote AIO backup would add an application-aware recovery method alongside Proxmox's whole-VM backup.

The separate location is more important than simply enabling the backup field.

Proxmox Backup Coverage

Both Nextcloud virtual disks must be included in the Proxmox backup.

Review the VM configuration using:

```
qm config <NEXTCLOUD_VMID>
```

Confirm the operating-system disk and data disk do not contain:

- `backup=0`

The initial consistent baseline may use a stopped backup.

Routine backups may use snapshot mode if brief application downtime is undesirable.

Restore Testing

A Nextcloud restore test must avoid creating a duplicate live instance.

Recommended procedure:

1. Restore the backup under a new VM ID.
2. Disconnect the restored VM network adapter.
3. Start the VM using the Proxmox console.
4. Confirm the operating-system disk.
5. Confirm the data disk.
6. Confirm `/mnt/nextcloud-data`.
7. Confirm Docker.
8. Confirm the AIO containers.
9. Confirm user files exist.
10. Shut down and delete the restored test VM.

Do not connect the restored clone to the production LAN while the live Nextcloud VM is active.

Data Growth

Monitor Nextcloud growth using:

```
df -h /mnt/nextcloud-data
```

Review directory usage using:

```
sudo du -sh /mnt/nextcloud-data/ncdata
```

Monitor the Proxmox `user-data` thin pool using:

```
pvesm status
```

Also review LVM-thin data and metadata utilization.

Storage monitoring must account for:

- User uploads.
- File versions.
- Deleted-file retention.
- Application data.
- Previews.
- Office files.
- Shared folders.
- Future photo libraries.

Security Considerations

- Nextcloud is available only through HTTPS.
- Traefik is explicitly trusted.
- AIO management remains private.
- The local administrator is preserved.
- Normal users authenticate through Authentik.

- MFA is handled by Authentik.
 - Public registration is reviewed.
 - Application installation is controlled.
 - Optional containers are added deliberately.
 - Backend ports remain private.
 - SMTP credentials remain secret.
 - Proxmox backups cover both disks.
 - File sharing settings are reviewed.
 - Administrative roles are assigned intentionally.
-

Common Failure Scenarios

AIO Management Loads but Nextcloud Does Not

Check:

- AIO child containers.
- Apache container.
- TCP port 11000.
- Traefik route.
- Nextcloud application log.
- Database and Redis.

Direct Backend Works but Public Hostname Fails

Check:

- Pi-hole.
- Traefik router.
- Certificate.
- Public DNS.

- VPS.
- WireGuard.
- Browser cache.

Public Hostname Works but OIDC Fails

Check:

- Authentik readiness.
- OIDC discovery.
- Client ID and secret.
- Redirect URI.
- Scope mappings.
- Container DNS.
- Authentik policies.
- Nextcloud log.

Discovery Endpoint Not Reachable

Check DNS inside the Nextcloud container.

Use:

```
sudo docker exec nextcloud-aio-nextcloud getent hosts portal.bytek.ca
```

No output indicates container DNS failure.

After confirming Pi-hole, restart the AIO containers or Docker as appropriate.

User Is Denied by Authentik

Check the Nextcloud Authentik application bindings.

Expected requirements:

- `bytek-users`
- `Allow bytek.ca users`

Do not require `bytek-admin` for all Nextcloud users.

Wrong Time Display

Confirm:

- Debian host time zone is `America/Toronto`.
- AIO time zone is `America/Toronto`.
- UTC clock is synchronized.
- NTP is active.

Data Disk Missing

Do not start normal application use until the data disk is mounted.

Check:

- `lsblk`
 - `findmnt`
 - `/etc/fstab`
 - Filesystem UUID
 - Proxmox virtual disk
-

Power-Failure Recovery

After a power interruption:

1. Confirm Proxmox.
2. Confirm Pi-hole.
3. Confirm the WireGuard gateway.
4. Confirm Authentik.
5. Confirm Traefik.
6. Confirm the Nextcloud VM owns `192.168.2.100`.
7. Confirm the user-data disk.
8. Confirm `/mnt/nextcloud-data`.
9. Confirm Docker.
10. Open AIO management by private IP.
11. Confirm the AIO master container.

12. Confirm PostgreSQL.
13. Confirm Redis.
14. Confirm Nextcloud.
15. Confirm Apache.
16. Confirm Collabora.
17. Test TCP port 11000.
18. Test `cloud.bytek.ca`.
19. Test Authentik login.
20. Test a file download.

If container DNS remains broken after Pi-hole recovery, restart the affected containers in a controlled manner.

Recovery Procedure

If the Nextcloud application is unavailable:

1. Use the Proxmox console or SSH.
2. Confirm the VM address.
3. Confirm the data-disk mount.
4. Confirm free disk space.
5. Confirm Docker.
6. Open the AIO interface.
7. Review container states.
8. Review master-container logs.
9. Review the failing child-container log.
10. Test the local backend.
11. Test the Traefik route.
12. Test the public route.
13. Use the local administrator if Authentik is unavailable.
14. Restore only after identifying the failure.

If the data disk is damaged:

1. Stop the AIO containers.
2. Avoid writing to the damaged filesystem.

3. Review filesystem and device health.
 4. Identify the latest valid Proxmox backup.
 5. Restore both the OS and data disks.
 6. Test the restored VM offline.
 7. Reconnect only after validation.
-

Validation Checklist

- Nextcloud VM owns `192.168.2.100`.
 - Operating-system disk is available.
 - User-data disk is mounted at `/mnt/nextcloud-data`.
 - Nextcloud data directory exists.
 - Docker is active.
 - AIO master container is healthy.
 - PostgreSQL is running.
 - Redis is running.
 - Nextcloud is running.
 - Apache is running on TCP 11000.
 - Collabora is running.
 - Traefik can reach TCP 11000.
 - `ccloud.bytek.ca` has a valid certificate.
 - Authentik login works.
 - Local administrator login works.
 - File upload works.
 - File download works.
 - Collaborative editing works.
 - SMTP test works.
 - Uptime Kuma reports healthy.
 - Both VM disks are included in backup.
 - Offline restore test has been completed.
 - AIO management is not publicly exposed.
-

Document Control

- **Owner:** Bryan Gagne-Plante
- **Private address:** 192.168.2.100
- **Public hostname:** cloud.bytek.ca
- **AIO management port:** TCP 8080
- **Traefik backend port:** TCP 11000
- **Deployment directory:** /opt/nextcloud-aio
- **Operating-system disk:** 64 GB on local-lvm
- **User-data disk:** 500 GB on user-data
- **Data mount:** /mnt/nextcloud-data
- **Data directory:** /mnt/nextcloud-data/ncdata
- **Authentication:** Authentik OIDC
- **OIDC application:** OpenID Connect user backend
- **Office integration:** AIO-managed Collabora
- **AIO backup repository:** Not configured
- **Proxmox VM ID:** Confirm current VM ID
- **Last verified:** YYYY-MM-DD
- **Last OIDC test:** YYYY-MM-DD
- **Last collaborative-editing test:** YYYY-MM-DD
- **Last SMTP test:** YYYY-MM-DD
- **Last backup test:** YYYY-MM-DD
- **Last restore test:** YYYY-MM-DD
- **Known limitations:** No separate remote AIO Borg repository and no offsite backup copy

Revision #2

Created 2026-08-17 14:51:22 UTC by Bryan Gagne-Plante

Updated 2026-08-18 00:36:25 UTC by Bryan Gagne-Plante