

03 - Applications

- [Nextcloud AIO](#)
- [Vikunja](#)
- [BookStack](#)

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	ccloud.bytek.ca

AIO management port	TCP 8080
Traefik backend port	TCP 11000
Deployment directory	<code>/opt/nextcloud-aio</code>
Operating-system disk	64 GB
User-data disk	500 GB
User-data mount	<code>/mnt/nextcloud-data</code>
Nextcloud data directory	<code>/mnt/nextcloud-data/ncdata</code>
Reverse proxy	Traefik
Authentication	Authentik OIDC
Office integration	AIO-managed Collabora CODE
Time zone	<code>America/Toronto</code>
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 `cloud.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 `cloud.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 `cloud.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>cloud.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:

- `cloud.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	<code>local-lvm</code>
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	Allow bytek.ca users
Policy engine	ALL

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	authentik
Discovery endpoint	Authentik discovery URL for application slug nextcloud
Scopes	openid email profile
User ID mapping	sub
Display-name mapping	name
Email mapping	email

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 ccloud.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 `ccloud.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.
 - `cloud.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

Vikunja

Purpose

Vikunja provides project and task management for the two-person video game project.

The service is used for:

- Project planning.
- Kanban boards.
- Backlogs.
- Task assignment.
- Due dates.
- Priorities.
- Labels.
- Subtasks.
- Milestone planning.
- Tracking bugs, features, art, audio, and release work.

Service Information

Setting	Value
Service name	Vikunja
Private IP address	192.168.2.121
Backend port	TCP 3456
Public hostname	projects.bytek.ca
Deployment directory	/opt/vikunja
Application container	vikunja
Database container	vikunja-db
Database	PostgreSQL
Reverse proxy	Traefik

Authentication	Authentik OIDC
Container user	UID 1000 and GID 1000
Backup coverage	Proxmox scheduled backup
Proxmox VM ID	Confirm current VM ID

Application:

[Open Vikunja](#)

Components

The deployment contains two main containers:

Container	Purpose
vikunja	Application API and web interface
vikunja-db	PostgreSQL database

The application and database communicate through a private Docker network.

PostgreSQL is not exposed publicly.

Persistent Data

Path	Purpose
/opt/vikunja/files	Uploaded task attachments
/opt/vikunja/postgres	PostgreSQL data
/opt/vikunja/config.yml	Vikunja configuration
/opt/vikunja/.env	Database password and service secrets
/opt/vikunja/compose.yml	Docker Compose configuration

The `.env` and `config.yml` files contain sensitive values and must not be copied into BookStack.

Request Flow

Internal Access

1. The client resolves `projects.bytek.ca` through Pi-hole.
2. Pi-hole returns Traefik at `192.168.2.182`.
3. Traefik receives the HTTPS request.
4. Traefik forwards the request to `192.168.2.121:3456`.
5. Vikunja responds.

External Access

1. WHC DNS resolves `projects.bytek.ca` to `38.29.213.101`.
 2. The VPS receives the HTTPS request.
 3. Traffic travels through WireGuard.
 4. The WireGuard gateway forwards the request to Traefik.
 5. Traefik forwards the request to `192.168.2.121:3456`.
-

Traefik Configuration

Setting	Value
Hostname rule	<code>projects.bytek.ca</code>
Entry point	<code>websecure</code>
Certificate resolver	<code>letsencrypt</code>
Backend	<code>http://192.168.2.121:3456</code>
Host-header forwarding	Enabled
Authentik ForwardAuth	Disabled

Vikunja uses native OIDC. Do not attach Authentik ForwardAuth to the Traefik router.

DNS

Public DNS

WHC resolves:

- `projects.bytek.ca` to `38.29.213.101`

Internal DNS

Pi-hole resolves:

- `projects.bytek.ca` to `192.168.2.182`

The Vikunja backend IP is not published in DNS.

Authentication

Vikunja uses native Authentik OpenID Connect.

Setting	Value
Authentik application	Vikunja
Application slug	<code>vikunja</code>
Provider type	OAuth2/OpenID Connect
Client type	Confidential
Subject mode	User UUID
Callback	<code>https://projects.bytek.ca/auth/openid/authentik</code>
Scopes	<code>openid profile email</code>
Required group	<code>bytek-users</code>
Required policy	<code>Allow bytek.ca users</code>
Policy engine	<code>ALL</code>

A user must:

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

Local Authentication

Local authentication remains available as a recovery method.

Local authentication should not be disabled until:

- Authentik login works for both project members.
 - OIDC account provisioning has been tested.
 - Proxmox backups have succeeded.
 - A restore has been tested.
 - Local recovery credentials are stored securely.
-

Container Runtime Identity

The Vikunja container runs as:

- **UID:** 1000
- **GID:** 1000

The attachment directory should have:

- **Owner:** `1000:1000`
- **Mode:** `0755`
- **Writable:** Yes

The container is explicitly configured to run as user `1000:1000`.

Permission Validation

Run the Vikunja diagnostic command:

```
sudo docker exec vikunja /app/vikunja/vikunja doctor
```

The file-storage section should report:

- Directory exists.
- Directory owner is 1000:1000.
- Ownership matches.
- Directory is writable.
- Disk space is available.

Check the container identity using:

```
sudo docker exec vikunja id
```

Expected identity:

- UID 1000.
 - GID 1000.
-

Docker Management

Move to the deployment directory:

```
cd /opt/vikunja
```

Validate Compose:

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

Check container state:

```
sudo docker compose ps
```

View recent logs:

```
sudo docker compose logs --tail 100 vikunja db
```

Apply normal configuration changes:

```
sudo docker compose up -d
```

Recreate only the application container:

```
sudo docker compose up -d --force-recreate vikunja
```

Pull updated images and apply them:

```
sudo docker compose pull && sudo docker compose up -d
```

Do not use `docker compose down -v`.

The `-v` option can remove Docker-managed volumes.

Health Endpoint

Vikunja provides a health endpoint at:

- `/health`

Direct health URL:

```
http://192.168.2.121:3456/health
```

Routed health URL:

[Open Vikunja Health](#)

Expected result:

- HTTP 200.

Use the health endpoint rather than the interactive login page for monitoring.

Direct Validation

From the Vikunja VM:

```
curl -i http://127.0.0.1:3456/health
```

From the Traefik VM:

```
curl -i http://192.168.2.121:3456/health
```

From the Uptime Kuma VM:

```
curl -i http://192.168.2.121:3456/health
```

All three tests should return HTTP 200.

Firewall Requirements

The Vikunja VM should permit:

Source	Port	Purpose
Home LAN or administrative workstation	TCP 22	SSH administration
192.168.2.182	TCP 3456	Traefik backend access
192.168.2.115	TCP 3456	Uptime Kuma direct monitor
192.168.2.115	ICMP	Optional ping monitor

TCP port 3456 must not be exposed publicly through the router or VPS.

Monitoring

Monitor	Type	Target
Vikunja VM	Ping	192.168.2.121
Vikunja Backend Direct	HTTP	http://192.168.2.121:3456/health
Vikunja Through Traefik	HTTPS	https://projects.bytek.ca/health
Vikunja Certificate	Certificate	projects.bytek.ca

Expected health status:

- HTTP 200.

If the VM monitor fails but the HTTP monitors succeed, ICMP is probably blocked.

Database Backup

The PostgreSQL database can be exported using:

```
sudo docker compose exec -T db pg_dump -U vikunja vikunja > vikunja-backup.sql
```

Verify that the file was created:

```
ls -lh vikunja-backup.sql
```

Database dumps contain application data and must be protected.

Do not leave old unencrypted dumps accumulating on the VM.

Proxmox Backup

The Vikunja VM is included in the scheduled Proxmox backup job.

The backup protects:

- Debian.
- Docker.
- PostgreSQL data.
- Attachments.
- Vikunja configuration.
- OIDC configuration.
- Compose file.
- Environment file.

A stopped baseline backup may be created after a known-good configuration.

Routine backups may use snapshot mode.

Project Structure

The current recommended structure is:

Main Project

- Game

Subprojects

- Game Design
- Programming
- Art and Animation
- Audio
- Levels and Content
- QA and Bugs
- Release
- Marketing

Workflow Columns

- Ideas
- Backlog
- Ready
- In Progress
- Review or Playtest
- Blocked
- Done

Suggested Labels

- Feature
- Bug
- Design
- Code
- Art
- Audio
- Level
- Balancing

- Performance
 - Playtest
 - Release Blocker
 - Nice to Have
-

Common Failures

Vikunja Is Reachable Directly but Not Through the Hostname

Check:

- Pi-hole record.
- Traefik router.
- Traefik backend IP.
- Certificate.
- Proxmox firewall.
- Traefik logs.

Health Endpoint Is Unreachable

Check:

- Docker service.
- Vikunja container.
- PostgreSQL container.
- TCP port 3456.
- Guest firewall.
- Application logs.

Authentik Login Does Not Appear

Check:

- OIDC configuration in `config.yml`.

- Configuration-file mount.
- Client ID and secret.
- Authentik discovery URL.
- Callback URI.
- Vikunja logs.
- Container DNS.

Authentik Returns Permission Denied

Check:

- User membership in `bytek-users`.
- Allow `bytek.ca-users` policy result.
- No unintended `bytek-admin` binding.
- Policy engine mode is `ALL`.

Attachments Fail

Check:

- `/opt/vikunja/files`.
- Owner `1000:1000`.
- Directory is writable.
- Container user is `1000:1000`.
- Disk space.
- Vikunja doctor output.

Database Is Unavailable

Check:

- `vikunja-db` container.
 - PostgreSQL health check.
 - Database credentials.
 - Docker network.
 - Free disk space.
 - PostgreSQL logs.
-

Power-Failure Recovery

1. Confirm Proxmox is running.
2. Confirm Pi-hole.
3. Confirm Authentik.
4. Confirm Traefik.
5. Confirm the Vikunja VM owns `192.168.2.121`.
6. Confirm Docker is active.
7. Confirm the PostgreSQL container.
8. Confirm the Vikunja container.
9. Test the direct health endpoint.
10. Test the routed health endpoint.
11. Test Authentik login.
12. Test project and task access.

If OIDC fails after startup, verify DNS from the Vikunja VM before changing credentials.

Recovery Procedure

If Vikunja is unavailable:

1. Confirm the VM is running.
2. Confirm the VM address.
3. Confirm available disk space.
4. Confirm Docker.
5. Confirm PostgreSQL.
6. Confirm the Vikunja container.
7. Review logs.
8. Test `/health`.
9. Run Vikunja doctor.
10. Test Traefik.
11. Test Authentik only after application health is restored.

If the VM must be restored:

1. Restore the current backup under a temporary VM ID.
 2. Disconnect the restored VM network adapter.
 3. Confirm Docker.
 4. Confirm PostgreSQL.
 5. Confirm attachments.
 6. Confirm configuration files.
 7. Shut down the failed production VM.
 8. Assign the expected network identity.
 9. Start the restored VM.
 10. Confirm 192.168.2.121.
 11. Test direct health.
 12. Test routed health.
 13. Test OIDC.
-

Validation Checklist

- Vikunja VM owns 192.168.2.121.
 - Docker is active.
 - PostgreSQL is healthy.
 - Vikunja container is running.
 - TCP port 3456 responds.
 - /health returns HTTP 200.
 - Attachment directory is writable.
 - Container runs as 1000:1000.
 - Traefik routes projects.bytek.ca.
 - Certificate is valid.
 - Authentik login works.
 - Both project members can sign in.
 - Task assignment works.
 - Attachment upload and download work.
 - Uptime Kuma monitors are healthy.
 - Proxmox backup includes the VM.
 - Database export has been tested.
 - Offline restore has been tested.
-

Document Control

- **Owner:** Bryan Gagne-Plante
- **Private address:** 192.168.2.121
- **Backend port:** TCP 3456
- **Public hostname:** projects.bytek.ca
- **Deployment directory:** /opt/vikunja
- **Database:** PostgreSQL
- **Authentication:** Authentik OIDC
- **Required group:** bytek-users
- **Container identity:** 1000:1000
- **Proxmox VM ID:** Confirm current VM ID
- **Last verified:** YYYY-MM-DD
- **Last OIDC test:** YYYY-MM-DD
- **Last attachment test:** YYYY-MM-DD
- **Last database-export test:** YYYY-MM-DD
- **Last restore test:** YYYY-MM-DD
- **Known limitation:** Vikunja availability depends on one application VM and its local PostgreSQL container

BookStack

Purpose

BookStack is the documentation platform for the Bytek homelab.

BookStack stores:

- Architecture documentation.
- Service configuration references.
- Installation notes.
- Operational procedures.
- Backup and restore instructions.
- Disaster-recovery procedures.
- Troubleshooting notes.

Service Information

Setting	Value
Service name	BookStack
Private IP address	Confirm current IP
Backend port	TCP 6875
Public hostname	<code>docs.bytek.ca</code>
Deployment directory	<code>/opt/bookstack</code>
Application container	<code>bookstack</code>
Database container	<code>bookstack-db</code>
Database	MariaDB
Reverse proxy	Traefik
Authentication	Authentik OIDC
Backup coverage	Proxmox scheduled backup
Proxmox VM ID	Confirm current VM ID

Application:

[Open BookStack](#)

Components

Container	Purpose
bookstack	BookStack application and web interface
bookstack-db	MariaDB database

MariaDB is connected to BookStack through a private Docker network.

The database is not publicly exposed.

Persistent Data

Path	Purpose
/opt/bookstack/app	BookStack configuration, uploads, logs, and application data
/opt/bookstack/database	MariaDB data
/opt/bookstack/.env	Passwords, application key, and OIDC credentials
/opt/bookstack/compose.yml	Docker Compose configuration

The `.env` file must not be copied into BookStack.

The application key, database password, OIDC secret, and other credentials must remain in the password manager or encrypted backup.

Request Flow

Internal Access

1. The client resolves `docs.bytek.ca` through Pi-hole.
2. Pi-hole returns Traefik at `192.168.2.182`.
3. Traefik receives the HTTPS request.
4. Traefik forwards the request to the BookStack VM on TCP port 6875.
5. BookStack responds.

External Access

1. WHC DNS resolves `docs.bytek.ca` to `38.29.213.101`.
 2. The VPS receives the HTTPS request.
 3. Traffic travels through WireGuard.
 4. The WireGuard gateway forwards the request to Traefik.
 5. Traefik forwards the request to BookStack.
-

Traefik Configuration

Setting	Value
Hostname rule	<code>docs.bytek.ca</code>
Entry point	<code>websecure</code>
Certificate resolver	<code>letsencrypt</code>
Backend	BookStack private IP on TCP 6875
Host-header forwarding	Enabled
Authentik ForwardAuth	Disabled

BookStack uses native OIDC.

Do not attach Authentik ForwardAuth to the BookStack router.

Application URL

The BookStack application URL must be exactly:

```
https://docs.bytek.ca
```

The earlier provisional hostname `wiki.bytek.ca` must not remain in:

- BookStack `APP_URL`.
- Traefik configuration.
- Authentik redirect URIs.
- Authentik post-logout URIs.
- Pi-hole.
- WHC DNS.
- Browser bookmarks.

Search the deployment for the old hostname using:

```
grep -RFn 'wiki.bytek.ca' /opt/bookstack 2>/dev/null
```

Application Key

BookStack uses a Laravel application key for encryption.

The key must:

- Begin with `base64:`.
- Decode to 32 bytes.
- Remain unchanged after BookStack contains real data.
- Be preserved with backups.
- Remain secret.

An invalid key previously caused this application error:

- Unsupported cipher or incorrect key length.

After BookStack contains real data, do not regenerate the application key.

Changing the key may make encrypted data unreadable.

Application-Key Validation

A valid key should report:

Property	Expected Value
Prefix	<code>base64</code>
Total length	51 characters
Decoded length	32 bytes

The application key itself must not be printed into documentation.

Authentication

BookStack uses native Authentik OpenID Connect.

Setting	Value
Authentik application	BookStack
Application slug	<code>bookstack</code>
Provider type	OAuth2/OpenID Connect
Client type	Confidential
Subject mode	User UUID
Issuer	<code>https://portal.bytek.ca/application/o/bookstack/</code>
Callback	<code>https://docs.bytek.ca/oidc/callback</code>
Required group	<code>bytek-users</code>
Required policy	<code>Allow bytek.ca users</code>
Policy engine	<code>ALL</code>
Signing key	RSA key selected
Encryption key	None

A user must:

- Belong to `bytek-users`.

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

OIDC Token Requirements

BookStack accepts signed OIDC tokens but the Authentik provider encryption key must remain empty.

A previously selected encryption key caused BookStack to report:

- ID token validation failure.
- Could not parse a valid payload from the token.

The working Authentik configuration is:

- **Signing key:** Selected.
 - **Encryption key:** None.
-

Account Model

Local Break-Glass Administrator

BookStack has a dedicated local administrator for recovery.

The local account should use:

- A dedicated administrative email address.
- A unique password.
- The BookStack Admin role.
- Credentials stored in the password manager.

The local account must not use the same email address as the normal Authentik account.

Normal Authentik Account

The normal daily account uses:

- Authentik authentication.
- Authentik MFA.
- The user's normal email address.
- BookStack roles assigned inside BookStack.

BookStack identifies the OIDC account through the `sub` claim, not email alone.

Authentication Modes

OIDC Mode

Normal operation uses:

- `AUTH_METHOD` set to `oidc`.
- `AUTH_AUTO_INITIATE` set to false during initial validation.

Standard Mode

Emergency local authentication uses:

- `AUTH_METHOD` set to `standard`.
- `AUTH_AUTO_INITIATE` set to false.

BookStack cannot normally provide standard and OIDC login simultaneously through the same authentication mode.

Switching authentication modes requires recreating the BookStack container.

Local Authentication Recovery

If Authentik is unavailable or OIDC is broken:

1. Keep the current BookStack VM running.
2. Edit `/opt/bookstack/compose.yml`.

3. Change `AUTH_METHOD` from `oidc` to `standard`.
4. Validate the Compose file.
5. Recreate only the BookStack application container.
6. Sign in using the local break-glass administrator.
7. Repair the Authentik integration.
8. Change `AUTH_METHOD` back to `oidc`.
9. Recreate the BookStack container again.
10. Test OIDC in a private browser window.

Apply the change using:

```
sudo docker compose up -d --force-recreate bookstack
```

MariaDB does not need to be recreated for an authentication-setting change.

Docker Management

Move to the deployment directory:

```
cd /opt/bookstack
```

Validate Compose:

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

Check container state:

```
sudo docker compose ps
```

View BookStack logs:

```
sudo docker compose logs --tail 100 bookstack
```

View database logs:

```
sudo docker compose logs --tail 100 database
```

Apply normal changes:

```
sudo docker compose up -d
```

Recreate only BookStack:

```
sudo docker compose up -d --force-recreate bookstack
```

Pull updated images:

```
sudo docker compose pull
```

Do not use `docker compose down -v`.

Application Logs

The BookStack application log is stored at:

```
/opt/bookstack/app/log/bookstack/laravel.log
```

Review recent entries using:

```
sudo tail -n 100 /opt/bookstack/app/log/bookstack/laravel.log
```

Review OIDC-related entries using:

```
sudo grep -iE 'oidc|token|payload|signature|issuer|jwks|error|exception' /opt/bookstack/app/log/bookstack/laravel.log | tail -n 100
```

Focus on entries with the current timestamp.

Old failures remain in the log after the problem is fixed.

Firewall Requirements

The BookStack VM should permit:

Source	Port	Purpose
Approved LAN administrator	TCP 22	SSH
192.168.2.182	TCP 6875	Traefik backend
192.168.2.115	TCP 6875	Uptime Kuma direct monitoring
192.168.2.115	ICMP	Optional ping monitor

TCP port 6875 must not be exposed publicly.

MariaDB must not be exposed outside the private Docker network.

Monitoring

Monitor	Type	Target
BookStack VM	Ping	BookStack private IP
BookStack Backend Direct	HTTP	BookStack private IP on TCP 6875
BookStack Through Traefik	HTTPS	<code>https://docs.bytek.ca/login</code>
BookStack Certificate	Certificate	<code>docs.bytek.ca</code>

The login endpoint may return a redirect.

Configure the monitor to accept expected status codes from 200 through 399.

Backup

The BookStack VM is included in the Proxmox scheduled backup job.

The backup protects:

- BookStack application configuration.
- MariaDB data.
- Uploaded images.
- Attachments.
- Themes.
- Application logs.
- Docker Compose configuration.
- Environment file.
- Application key.
- OIDC configuration.

The application key and database must be restored together.

Database Export

A logical MariaDB dump can supplement the Proxmox VM backup.

Run the dump from `/opt/bookstack`.

Use the MariaDB credentials stored in the deployment environment.

The resulting export contains BookStack data and must be protected.

Do not leave old unencrypted database exports accumulating on the VM.

Update Procedure

Before updating BookStack:

1. Confirm the current Proxmox backup completed successfully.
2. Review available disk space.
3. Create a short-term Proxmox snapshot if desired.
4. Record the current container image.
5. Pull the updated images.
6. Recreate the containers.
7. Review BookStack logs.
8. Test the login page.
9. Test Authentik login.
10. Open an existing page.
11. Edit and save a test page.
12. Test an attachment.
13. Remove the temporary snapshot after validation.

Use:

```
sudo docker compose pull && sudo docker compose up -d
```

Common Failures

Generic “An Error Occurred” Page

Review the Laravel log.

Possible causes include:

- Invalid application key.
- Database unavailable.
- OIDC configuration error.
- Filesystem permissions.
- Incorrect application URL.

Unsupported Cipher or Incorrect Key Length

The application key is missing, truncated, malformed, or not passed into the container.

Confirm:

- The `.env` variable exists.
- Compose references the correct variable.
- The value begins with `base64:`.
- The decoded key length is 32 bytes.
- The BookStack container was recreated after the change.

OIDC Token Cannot Be Parsed

Confirm:

- Authentik signing key is selected.
- Authentik encryption key is empty.
- The issuer is correct.
- A fresh private browser session is used.

Email Address Already Taken

The local administrator and Authentik user are attempting to use the same email address.

Use:

- A dedicated email for the local break-glass administrator.
- The normal personal email for the Authentik user.

OIDC Redirect Fails

Confirm:

- `APP_URL` is `https://docs.bytek.ca`.
- Authentik callback is `https://docs.bytek.ca/oidc/callback`.
- No configuration still uses `wiki.bytek.ca`.
- Client ID and secret match.
- Authentik discovery is reachable.
- Browser cookies are accepted.

CSRF Cookie Not Set

Check:

- New private browser session.
- Browser cookie blocking.
- Request Host header.
- Request Origin header.
- Traefik host-header forwarding.
- Stale Authentik cookies.
- VPN or browser proxy.

Database Unavailable

Check:

- `bookstack-db` or database Compose service.
- MariaDB logs.
- Database credentials.
- Docker network.
- Persistent database directory.

- Available disk space.
-

Power-Failure Recovery

1. Confirm Proxmox.
2. Confirm Pi-hole.
3. Confirm Authentik.
4. Confirm Traefik.
5. Confirm the BookStack VM owns its reserved IP.
6. Confirm Docker.
7. Confirm MariaDB.
8. Confirm the BookStack container.
9. Test the direct backend.
10. Test `docs.bytek.ca`.
11. Test Authentik login.
12. Open an existing documentation page.

If OIDC fails but BookStack is otherwise healthy, switch temporarily to standard authentication rather than rebuilding the application.

Recovery Procedure

If BookStack is unavailable:

1. Confirm the VM is running.
2. Confirm the VM's private IP.
3. Confirm available disk space.
4. Confirm Docker.
5. Confirm MariaDB.
6. Confirm the BookStack container.
7. Review the Laravel log.
8. Verify `APP_URL`.
9. Verify the application key.
10. Test the direct backend.
11. Test Traefik.

12. Test OIDC only after the application is healthy.

If the VM must be restored:

1. Restore the latest backup under a temporary VM ID.
 2. Disconnect the restored VM network adapter.
 3. Confirm Docker.
 4. Confirm MariaDB.
 5. Confirm BookStack data.
 6. Confirm the application key.
 7. Confirm attachments and pages.
 8. Shut down the failed production VM.
 9. Assign the expected network identity.
 10. Start the restored VM.
 11. Test direct access.
 12. Test Traefik.
 13. Test Authentik login.
-

Validation Checklist

- BookStack VM owns its reserved address.
- Docker is active.
- MariaDB is running.
- BookStack container is running.
- TCP port 6875 responds.
- `APP_URL` is `https://docs.bytek.ca`.
- Application key is valid.
- Traefik routing works.
- Let's Encrypt certificate is valid.
- Authentik OIDC works.
- Authentik encryption key is empty.
- Local break-glass account works in standard mode.
- Local and OIDC accounts use separate email addresses.
- Existing pages open.
- Page editing works.
- Attachment upload works.

- Uptime Kuma monitors are healthy.
 - Proxmox backup includes the VM.
 - Database export has been tested.
 - Offline restore has been tested.
-

Document Control

- **Owner:** Bryan Gagne-Plante
- **Private address:** Confirm current BookStack IP
- **Backend port:** TCP 6875
- **Public hostname:** docs.bytek.ca
- **Deployment directory:** /opt/bookstack
- **Database:** MariaDB
- **Authentication:** Authentik OIDC
- **Required group:** bytek-users
- **Break-glass authentication:** BookStack standard authentication
- **Proxmox VM ID:** Confirm current VM ID
- **Last verified:** YYYY-MM-DD
- **Last OIDC test:** YYYY-MM-DD
- **Last local-login test:** YYYY-MM-DD
- **Last page-editing test:** YYYY-MM-DD
- **Last database-export test:** YYYY-MM-DD
- **Last restore test:** YYYY-MM-DD
- **Known limitation:** BookStack availability depends on one application VM and its local MariaDB container