

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	docs.bytek.ca
Deployment directory	/opt/bookstack
Application container	bookstack
Database container	bookstack-db
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	base64
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	bookstack
Provider type	OAuth2/OpenID Connect
Client type	Confidential
Subject mode	User UUID
Issuer	https://portal.bytek.ca/application/o/bookstack/
Callback	https://docs.bytek.ca/oidc/callback
Required group	bytek-users
Required policy	Allow bytek.ca users
Policy engine	ALL
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
-

Revision #2

Created 2026-08-17 14:52:18 UTC by Bryan Gagne-Plante

Updated 2026-08-18 00:41:41 UTC by Bryan Gagne-Plante