

Disaster Recovery Checklist

Purpose

This checklist provides a concise response plan for major Bytek homelab failures.

The objective is to restore core infrastructure before application services.

Avoid making several unrelated configuration changes simultaneously.

Initial Assessment

Before changing configuration:

1. Determine whether the problem affects one service or the entire environment.
2. Check electrical power.
3. Check the Proxmox host.
4. Check the home network.
5. Check internet connectivity.
6. Check Pi-hole.
7. Check WireGuard.
8. Check Traefik.
9. Check Authentik.
10. Check application VMs.
11. Review Uptime Kuma.
12. Record the observed symptoms.

Do not rely only on browser errors.

Test direct IPs and backend ports where possible.

Complete Proxmox Host Failure

1. Confirm server power.
2. Check the physical console.
3. Confirm the firmware detects all storage devices.
4. Confirm the Proxmox system NVMe.
5. Confirm the user-data NVMe.
6. Confirm the backup HDD.
7. Attempt normal Proxmox boot.
8. Review boot messages.
9. Confirm network bridge configuration.
10. Confirm `pveproxy`.
11. Confirm TCP 8006.
12. Use `root@pam`.

If the system NVMe failed:

1. Replace the failed system storage.
 2. Install Proxmox.
 3. Restore network configuration.
 4. Restore storage configuration.
 5. Reconnect `user-data`.
 6. Remount `pve-backup`.
 7. Restore VMs and LXC.
 8. Verify local authentication.
 9. Restore the Authentik Proxmox realm.
 10. Test OIDC only after local access works.
-

Pi-hole Failure

1. Open Proxmox using `192.168.2.254`.
2. Confirm the Pi-hole LXC is running.
3. Open the LXC console.
4. Confirm address `192.168.2.65`.
5. Confirm TCP port 53.

6. Confirm UDP port 53.
7. Confirm local DNS records.
8. Confirm public upstream resolution.
9. Review Pi-hole logs.
10. Restore from backup if necessary.

During the outage, access services using private IP addresses where supported.

Do not make Pi-hole recovery depend on Authentik.

WireGuard Failure

1. Confirm the WireGuard gateway guest.
2. Confirm address `192.168.2.64`.
3. Confirm the WireGuard interface.
4. Confirm the VPS peer.
5. Confirm the latest handshake.
6. Confirm transfer counters.
7. Confirm IPv4 forwarding.
8. Confirm firewall rules.
9. Confirm NAT rules.
10. Test Traefik connectivity from the tunnel.
11. Test a public hostname externally.

If the keys are lost or compromised, rotate the affected peer key pair and update the opposite peer.

Public VPS Failure

1. Open the provider console.
2. Confirm the VPS is running.
3. Confirm public IP `38.29.213.101`.
4. Confirm SSH service.
5. Confirm firewall rules.

6. Confirm WireGuard.
7. Confirm TCP 443.
8. Confirm forwarding to the home tunnel.
9. Confirm disk space.
10. Review system logs.

LAN access should continue through Pi-hole and Traefik while the VPS is unavailable.

Traefik Failure

1. Confirm the Traefik VM owns `192.168.2.182`.
2. Confirm Docker.
3. Confirm the Traefik container.
4. Confirm TCP 443.
5. Confirm container DNS.
6. Review Traefik logs.
7. Check recently changed dynamic YAML.
8. Search for tabs.
9. Test the direct application backend.
10. Restore the previous dynamic file if necessary.
11. Confirm certificate state.
12. Do not delete `acme.json`.

If all applications fail simultaneously but direct backends work, prioritize Traefik, Pi-hole, and certificates.

Authentik Failure

1. Sign into Proxmox using `root@pam`.
2. Confirm the Authentik VM owns `192.168.2.162`.
3. Confirm Docker.
4. Confirm PostgreSQL.
5. Confirm Redis.

6. Confirm Authentik server.
7. Confirm Authentik worker.
8. Test direct readiness.
9. Test routed readiness.
10. Review Authentik logs.
11. Review Traefik.
12. Restore Authentik from backup if necessary.

Use application break-glass access during recovery:

Application	Recovery Method
Proxmox	<code>root@pam</code>
Nextcloud	Local administrator
BookStack	Switch to standard authentication
Uptime Kuma	Restore local authentication
Traefik	Basic Auth or restore known-good route

Nextcloud Failure

1. Confirm VM address `192.168.2.100`.
2. Confirm the 500 GB data disk.
3. Confirm `/mnt/nextcloud-data`.
4. Confirm free disk space.
5. Confirm Docker.
6. Open AIO management by private IP.
7. Confirm PostgreSQL.
8. Confirm Redis.
9. Confirm Nextcloud.
10. Confirm Apache.
11. Confirm TCP 11000.
12. Confirm Traefik.
13. Use the local administrator if OIDC fails.
14. Restore both virtual disks if recovery is required.

Do not start normal Nextcloud operation if the data mount is missing.

Vikunja Failure

1. Confirm VM address `192.168.2.121`.
 2. Confirm Docker.
 3. Confirm PostgreSQL.
 4. Confirm the Vikunja container.
 5. Confirm TCP 3456.
 6. Test `/health`.
 7. Run the Vikunja doctor command.
 8. Check attachment permissions.
 9. Check Traefik.
 10. Check Authentik after application health is restored.
-

BookStack Failure

1. Confirm the BookStack VM.
2. Confirm the current private IP.
3. Confirm Docker.
4. Confirm MariaDB.
5. Confirm the BookStack container.
6. Confirm TCP 6875.
7. Review the Laravel log.
8. Confirm `APP_URL`.
9. Confirm the application key.
10. Confirm Traefik.
11. Switch to standard authentication if OIDC blocks access.
12. Restore the VM if application data is damaged.

The application key and database must be restored together.

Uptime Kuma Failure

1. Confirm VM address `192.168.2.115`.
2. Confirm Docker.
3. Confirm the Uptime Kuma container.
4. Confirm persistent data.
5. Confirm embedded database health.
6. Confirm container DNS.
7. Test TCP 3001.
8. Confirm Traefik.
9. Confirm Authentik Proxy Provider.
10. Restore local authentication if proxy access fails.

The absence of monitoring does not necessarily mean every monitored system is down.

Backup HDD Failure

1. Confirm `/dev/sda`.
2. Confirm `/dev/sda1`.
3. Confirm filesystem UUID.
4. Confirm `/etc/fstab`.
5. Confirm `/mnt/pve/pve-backup`.
6. Confirm Proxmox storage state.
7. Review SMART health.
8. Stop scheduled backups if the filesystem is unsafe.
9. Replace the backup HDD if necessary.
10. Create a fresh backup set immediately after replacement.

Do not allow backups to write into an unmounted directory on the root filesystem.

User-Data NVMe Failure

Expected impact includes Nextcloud user data and any other data disks stored on `user-data`.

Response:

1. Stop affected guests.
 2. Avoid further writes.
 3. Confirm the physical NVMe.
 4. Review NVMe health.
 5. Confirm the `lvm1` volume group.
 6. Confirm the `data` thin pool.
 7. Identify the latest valid backups.
 8. Replace the failed storage if required.
 9. Recreate the `user-data` storage.
 10. Restore affected data disks.
 11. Validate guests offline.
 12. Return services to production.
-

Authentication Lockout

Proxmox

Use `root@pam`.

Nextcloud

Use the local administrator and direct local-login path.

BookStack

Set `AUTH_METHOD` to `standard`, recreate the BookStack container, and use the local administrator.

Uptime Kuma

Restore the direct Traefik route, allow temporary private access, and re-enable local authentication.

Traefik Dashboard

Restore the previous dashboard YAML or use retained Basic Auth.

Authentik

Use the local Authentik administrator or restore Authentik from backup.

Restore Validation

Before replacing production with a restored guest:

1. Restore under a temporary guest ID.
 2. Disconnect the network adapter.
 3. Start through the Proxmox console.
 4. Confirm operating-system boot.
 5. Confirm all intended disks.
 6. Confirm mount points.
 7. Confirm Docker.
 8. Confirm database.
 9. Confirm application data.
 10. Confirm configuration and secrets.
 11. Shut down the test clone.
 12. Schedule the production cutover.
 13. Shut down the failed production guest.
 14. Assign the expected network identity to the restored guest.
 15. Start the restored guest.
 16. Test direct backend access.
 17. Test Traefik.
 18. Test Authentik.
 19. Test external access.
 20. Update documentation.
-

Emergency Credentials

The password manager must contain:

- Proxmox `root@pam` password.
- Authentik administrator credentials.
- Nextcloud local administrator credentials.
- BookStack break-glass administrator credentials.
- Uptime Kuma administrator credentials.
- Traefik Basic Auth credentials.
- VPS SSH private key.
- Home-infrastructure SSH keys.
- WireGuard configuration and recovery keys.
- WHC cPanel credentials.
- SMTP credentials.
- Database recovery credentials where required.

Do not store the actual credential values in BookStack.

BookStack should record only the credential purpose and storage location.

Recovery Priority

Restore services in this order:

1. Proxmox VE.
2. Storage pools.
3. Pi-hole.
4. WireGuard Gateway.
5. Authentik database and Authentik.
6. Traefik.
7. Uptime Kuma.
8. Nextcloud.
9. Vikunja.
10. BookStack.

Incident Record

After a significant incident, record:

- Date and time.
- Affected services.
- Initial symptoms.
- Root cause.
- Recovery actions.
- Backup used.
- Data loss, if any.
- Configuration changes.
- Monitoring gaps.
- Preventive actions.
- Documentation changes.

Do not include passwords, tokens, private keys, or session cookies.

Final Recovery Checklist

- Proxmox management works.
- Required storage is active.
- Backup HDD is mounted.
- Pi-hole resolves internal and public names.
- WireGuard handshake exists.
- VPS ingress works.
- Authentik readiness returns HTTP 200.
- Traefik routes load.
- Certificates are valid.
- Uptime Kuma is healthy.
- Nextcloud data disk is mounted.

- Nextcloud file access works.
 - Vikunja health returns HTTP 200.
 - BookStack documentation opens.
 - OIDC works.
 - Local break-glass accounts work.
 - Public access works externally.
 - New backup completes successfully.
 - Documentation is updated.
-

Document Control

- **Owner:** Bryan Gagne-Plante
 - **Primary recovery platform:** Proxmox VE
 - **Primary backup storage:** pve-backup
 - **Backup mount:** /mnt/pve/pve-backup
 - **Offsite backup:** Not configured
 - **Last verified:** YYYY-MM-DD
 - **Last disaster-recovery exercise:** YYYY-MM-DD
 - **Last full restore test:** YYYY-MM-DD
 - **Last authentication-recovery test:** YYYY-MM-DD
 - **Last backup-HDD review:** YYYY-MM-DD
 - **Known limitations:** One Proxmox host, one local backup disk, and no offsite recovery copy
-

Revision #3

Created 2026-08-17 14:52:55 UTC by Bryan Gagne-Plante

Updated 2026-08-18 00:46:50 UTC by Bryan Gagne-Plante