

Proxmox VE

Proxmox VE

Purpose

Proxmox VE is the primary hypervisor for the Bytek homelab.

Proxmox hosts and manages:

- Virtual machines.
- Linux containers.
- Virtual networking.
- Proxmox firewall rules.
- LVM-thin storage.
- VM and LXC snapshots.
- Scheduled backups.
- Backup restoration.
- Physical-device passthrough.
- Emergency guest consoles.

Proxmox is a critical management system and must remain accessible independently of Pi-hole, Traefik, and Authentik.

Service Information

Setting	Value
Private hostname	pve.bytek.ca
Private IP address	192.168.2.254

Web interface port	TCP 8006
SSH port	TCP 22
Access scope	Home LAN or trusted VPN
Normal authentication	Authentik OIDC
Emergency authentication	root@pam
General DNS resolver	9.9.9.9
Backup storage	pve-backup
Primary VM storage	local-lvm
Large-data storage	user-data

Management interface:

[Open Proxmox VE](#)

Access Policy

The Proxmox management interface must remain private.

Approved access paths include:

- A workstation on the home LAN.
- A trusted remote-access VPN.
- The Proxmox physical console.
- A deliberately configured emergency SSH tunnel.

The following access methods are prohibited:

- Public WHC DNS record for pve.bytek.ca.
- Bell router forwarding of TCP 8006.
- VPS forwarding of TCP 8006.
- Public Traefik routing to Proxmox.
- Direct internet exposure of SSH.

Pi-hole resolves pve.bytek.ca directly to 192.168.2.254.

DNS Design

The Proxmox host intentionally uses Quad9 at 9.9.9.9 instead of Pi-hole.

This prevents the hypervisor from depending on a guest VM or LXC for its own DNS service.

The DNS behavior differs depending on the requester:

Requester	Hostname	Result
LAN workstation using Pi-hole	pve.bytek.ca	192.168.2.254
Proxmox using Quad9	portal.bytek.ca	38.29.213.101
LAN workstation using Pi-hole	portal.bytek.ca	192.168.2.182

Proxmox may therefore reach Authentik through the public VPS, WireGuard, and Traefik path.

If that path becomes unreliable for OIDC, a single static entry can map portal.bytek.ca to 192.168.2.182 in the Proxmox /etc/hosts file without changing the general DNS resolver.

Browser DNS Requirement

The private hostname pve.bytek.ca exists only in Pi-hole.

Firefox-based browsers such as Zen may bypass Pi-hole when enhanced DNS protection or DNS over HTTPS is forced.

Recommended browser configuration:

- **DNS over HTTPS:** Off or Default Protection.
- **Proxy:** No proxy or system proxy settings.
- **VPN:** Must allow access to the home LAN.

If the private hostname does not load but the IP address works, verify browser DNS protection before changing Proxmox.

Useful Windows checks:

- Resolve-DnsName pve.bytek.ca
- nslookup pve.bytek.ca 192.168.2.65

- `Test-NetConnection pve.bytek.ca -Port 8006`
- `Clear-DnsClientCache`
- `ipconfig /flushdns`

Expected results:

- `pve.bytek.ca` resolves to `192.168.2.254`.
- TCP port 8006 is reachable.

Authentication Model

Normal Authentication

Normal administration uses native OpenID Connect with Authentik.

OIDC Setting	Value
Realm	authentik
Issuer	<code>https://portal.bytek.ca/application/o/proxmox/</code>
Username claim	username
Scopes	email profile
Automatically create users	Enabled
Default realm	Optional after validation

The matching Authentik provider requires:

- **Application slug:** proxmox
- **Client type:** Confidential
- **Subject mode:** User UUID
- **Signing key:** Selected
- **Encryption key:** None
- **Authorization redirect:** `https://pve.bytek.ca:8006`

Required Authentik bindings:

- Group bytek-admin.
- Policy Allow bytek.ca users.

- Policy engine mode `ALL`.

A user must satisfy both the group and policy requirements.

Authentik Scope Mappings

The Proxmox Authentik provider must include the following selected scope mappings:

- `openid`
- `email`
- `profile`

Missing scope mappings can allow the browser authorization step to succeed while causing Proxmox to fail at the Authentik userinfo endpoint.

A previously observed failure was:

- OpenID authentication failure.
- Failed to contact the userinfo endpoint.
- Proxmox returned authentication failure 401.

Selecting the expected mappings in the Authentik provider resolved the authentication flow.

Authentication and Authorization Are Separate

Successful Authentik authentication creates the Proxmox user but does not grant access to VMs, containers, nodes, or storage.

A newly created OIDC user may initially see an empty interface.

The user requires an explicit Proxmox access-control entry.

For the primary administrator:

Permission Setting	Value
Path	/
Role	Administrator
Propagate	Enabled
User	Authentik-created Proxmox user

The username normally ends with the realm:

- Example: brygagl@authentik

Do not accidentally grant the permission to the PAM version of the username.

Break-Glass Authentication

The local Proxmox PAM account must remain available.

Setting	Value
Account	root@pam
Authentication source	Proxmox host PAM
Purpose	Emergency recovery
Password storage	Password manager
Removal permitted	No

Never:

- Delete root@pam.
- Disable the PAM realm.
- Make Authentik the only possible administrative login.
- Depend on public ingress for emergency Proxmox access.

The root@pam account should be tested periodically in a private browser session.

Web Service Health

The Proxmox web interface is provided by `pveproxy`.

Check service state with:

```
systemctl is-active pveproxy
```

Expected result:

- `active`

Check the listener with:

```
ss -lntp | grep ':8006'
```

Expected result:

- A listener on TCP port 8006.
- `pveproxy` and worker processes appear.

Test locally with:

```
curl -k https://127.0.0.1:8006/
```

A `501 method HEAD not available` response from a command using `curl -I` does not indicate an outage. That response confirms the HTTPS service was reached, but the endpoint does not support the HTTP HEAD method.

Network Validation

Test from another LAN VM:

```
nc -zv -w 5 192.168.2.254 8006
```

A successful result confirms TCP reachability.

Test HTTPS by IP:

```
curl -k https://192.168.2.254:8006/
```

Test HTTPS by private hostname:

```
curl -k https://pve.bytek.ca:8006/
```

If the hostname fails but the IP works, investigate DNS rather than `pveproxy`.

OIDC Validation

Verify that Proxmox can retrieve Authentik discovery information:

```
curl -fsS https://portal.bytek.ca/application/o/proxmox/.well-known/openid-configuration
```

The response should contain OIDC metadata such as:

- Issuer.
- Authorization endpoint.
- Token endpoint.
- Userinfo endpoint.
- JWKS endpoint.

A request to the userinfo endpoint without a bearer token should return an authentication error.

That response is expected and proves the endpoint is reachable.

OIDC Troubleshooting

Review recent Proxmox authentication logs with:

```
journalctl -u pvedaemon --since "10 minutes ago" --no-pager
```

Look for terms such as:

- OpenID.
- Userinfo.
- Token.
- Claim.
- Signature.
- Issuer.

- Authentication.

Authentication Failure 401

Possible causes include:

- Incorrect client ID.
- Incorrect client secret.
- Missing Authentik scope mappings.
- Incorrect redirect URI.
- Missing signing key.
- Token encryption enabled.
- Userinfo endpoint failure.
- Browser callback hostname mismatch.

Failed to Contact Userinfo Endpoint

Check:

1. Authentik readiness.
2. OIDC discovery.
3. The userinfo endpoint.
4. Selected Authentik `email` and `profile` mappings.
5. Proxmox realm scopes.
6. VPS and WireGuard connectivity.
7. Traefik routing.

Login Works but No VMs Appear

The OIDC user has not been assigned a Proxmox ACL.

Assign the required role at `/` with propagation enabled.

Private Hostname Does Not Resolve

Check:

1. Pi-hole record.
 2. Workstation DNS server.
 3. Browser DNS over HTTPS.
 4. Active VPN.
 5. Browser proxy.
 6. Windows DNS cache.
-

Firewall Policy

Proxmox TCP port 8006 should accept traffic only from approved management sources.

Potential management sources include:

- Home LAN.
- Reserved administrative workstation.
- Future WireGuard remote-access gateway.
- Emergency SSH tunnel endpoint.

Do not create an internet-wide accept rule for TCP 8006.

SSH should use:

- Key-based authentication.
 - No root password login over SSH where hardening permits.
 - LAN or trusted VPN access.
 - Firewall restrictions.
-

Storage Attached to Proxmox

Storage ID	Type	Primary Role
local	Directory	ISOs, templates, and selected local content
local-lvm	LVM-thin	VM and LXC operating-system disks
user-data	LVM-thin	Large application and user-data disks
pve-backup	Directory on ext4	VZDump backup files

Review storage state using:

```
pvesm status
```

All required storage should show as active.

Backup System

Proxmox uses its built-in scheduled backup system.

Backups are written to:

- **Storage ID:** pve-backup
- **Mount point:** /mnt/pve/pve-backup
- **Physical disk:** Dedicated internal 4 TB HDD

The general job uses:

- Snapshot mode.
- ZSTD compression.
- A retention policy.
- Selection of production VMs and LXC.

The backup mount uses mount-point validation to prevent writing backup data to the Proxmox root filesystem if the HDD is unavailable.

Snapshots

Snapshots are used only for short-term rollback.

Appropriate snapshot cases include:

- Before Authentik changes.
- Before Traefik changes.
- Before operating-system upgrades.
- Before enabling GPU passthrough.

- Before risky application changes.

Snapshots are not backups.

Delete snapshots after the associated change has been validated.

Long-lived snapshots consume thin-pool capacity and increase storage risk.

Planned GPU Passthrough

The RTX 2060 is planned for a dedicated Plex VM.

Before passthrough:

1. Confirm VT-d and IOMMU.
2. Identify GPU and audio PCI functions.
3. Review the IOMMU group.
4. Confirm the group contains no critical host devices.
5. Create a Proxmox backup.
6. Preserve console recovery.
7. Use a Q35 and OVMF Plex VM.
8. Attach all required RTX 2060 functions.
9. Keep the GPU non-primary for the headless Plex VM.

A VM with passed-through hardware cannot use normal live migration.

Proxmox Recovery

If Authentik authentication fails:

1. Open the Proxmox login page.
2. Select the PAM realm.
3. Sign in as `root@pam`.
4. Verify Authentik readiness.
5. Verify the Authentik Proxmox provider.

6. Verify selected scope mappings.
7. Verify the Proxmox realm.
8. Review `pvedaemon` logs.
9. Verify the OIDC user ACL.
10. Retest from a private browser session.

If the web interface fails:

1. Access the Proxmox console or SSH.
2. Verify the Proxmox IP address.
3. Verify `pveproxy`.
4. Verify TCP port 8006.
5. Review firewall rules.
6. Verify storage.
7. Restart `pveproxy` only if the service is unhealthy.

If the system disk fails:

1. Preserve the user-data NVMe and backup HDD.
2. Reinstall Proxmox on replacement system storage.
3. Restore networking and storage definitions.
4. Reconnect `user-data`.
5. Remount `pve-backup`.
6. Restore guests from backup.
7. Recreate the Authentik realm.
8. Verify `root@pam`.
9. Test OIDC only after local management works.

Validation Checklist

- Proxmox owns `192.168.2.254`.
- Pi-hole resolves `pve.bytek.ca` to `192.168.2.254`.
- Zen or Firefox does not force public DNS for the private hostname.
- TCP port 8006 is reachable from the administrative workstation.
- `pveproxy` is active.
- `root@pam` login works.

- Authentik OIDC login works.
 - Authentik user has an explicit Proxmox ACL.
 - `local-lvm` is active.
 - `user-data` is active.
 - `pve-backup` is active.
 - Backup jobs complete successfully.
 - The backup HDD is mounted before scheduled jobs run.
 - No Proxmox management port is exposed publicly.
-

Document Control

- **Owner:** Bryan Gagne-Plante
 - **Private hostname:** `pve.bytek.ca`
 - **Private address:** `192.168.2.254`
 - **Normal authentication:** Authentik OIDC
 - **Emergency authentication:** `root@pam`
 - **General DNS resolver:** `9.9.9.9`
 - **Last verified:** YYYY-MM-DD
 - **Last backup test:** YYYY-MM-DD
 - **Last restore test:** YYYY-MM-DD
 - **OIDC recovery tested:** Yes / No
 - **Known limitations:** Single Proxmox host and no current high-availability cluster
-

Revision #2

Created 2026-08-17 14:49:40 UTC by Bryan Gagne-Plante

Updated 2026-08-17 15:30:23 UTC by Bryan Gagne-Plante