Knowledge Base

Aktive technische Knowledge-Base-Einträge aus Obsidian.

- NTP auf dem Proxmox-Cluster
- UEFI Secure Boot Zertifikate 2023 (Proxmox EFI-Disk)

NTP auf dem Proxmox-Cluster

NTP auf dem Proxmox-Cluster

> **abstract:** Zweck Auf allen Cluster-Nodes eine **deterministische Zeitsynchronisation** mit chrony einrichten. Eine stabil laufende Zeit ist im Proxmox-Cluster zwingend: abweichende Uhrzeiten können zu Corosync-Problemen, Zertifikatsfehlern (VNC-Konsole, API) und missverständlichen Log-Zeiten führen.

Grundlagen

- Proxmox VE installiert chrony als Standard-NTP-Daemon und sieht eine laufende Zeitsynchronisation als wichtig an.
- Cluster-Knoten werden nicht zwingend selbst als NTP-Server voneinander genutzt; alle Nodes synchronisieren gegen dieselben, verlässlichen Quellen.
- Empfehlung: eine interne, autoritative Quelle (z. B. Firewall/Router mit NTP-Dienst) mit `prefer`, plus öffentliche Fallback-Server (Swiss NTP Pool) mit `iburst`.
- Debian-Defaults (`pool 2.debian.pool.ntp.org`) und DHCP-abhängige Quellen (`sourcedir /run/chrony-dhcp`) bewusst deaktivieren, damit die Zeitquelle deterministisch ist.

Umstellung Schritt für Schritt

1. Konfiguration anpassen:

```
nano /etc/chrony/chrony.conf
```

2. Dienst neu starten:

```
systemctl restart chrony
```

3. Synchronisation prüfen:

```
chronyc sources -v
```

Erwartung: mindestens eine Quelle mit Status `^*` (aktiv) bzw. `^+` (Kandidat), z. B.:

```
^* 192.0.2.1
^+ ch.pool.ntp.org
```

Konfigurationsvorlage

Auf **jedem** Proxmox-Node identisch setzen (primäre interne Quelle durch die echte Management-Adresse ersetzen):

```
## Welcome to the chrony configuration file. See chrony.conf(5) for more
## information about usable directives.

## Include configuration files found in /etc/chrony/conf.d.
confdir /etc/chrony/conf.d

## === Proxmox Cluster NTP Configuration ===

## Primary NTP - Firewall (LAN / MGMT), interne Adresse eintragen
server <NTP-SERVER-LAN-IP> iburst prefer

## Fallback - Swiss NTP Pool
server ch.pool.ntp.org iburst

## --- Disabled defaults for deterministic cluster time ---
## pool 2.debian.pool.ntp.org iburst
## sourcedir /run/chrony-dhcp
## sourcedir /etc/chrony/sources.d
```

> **warning:** > Vor der Umsetzung prüfen, dass die interne NTP-Quelle (Firewall/Router) tatsächlich NTP-Anfragen beantwortet (`chronyc sources -v` muss `^*` zeigen) und dass NTP auf dem MGMT-Netz nicht per Firewall geblockt ist.

Verifikation Cluster-weit

```
pvecm status                # Cluster gesund?
for h in <node1> <node2>; do ssh $h chronyc tracking; done
```

`chronyc tracking` muss auf allen Nodes dieselbe Referenz/Stratum zeigen.

Quellen

- Proxmox VE Administration Guide – Time Synchronization: https://pve.proxmox.com/pve-docs/pve-admin-guide.html#_time_synchronization
- chrony-Dokumentation (`chrony.conf(5)`): https://chrony-project.org/doc/latest/chrony.conf.html
- Swiss NTP Pool: https://www.pool.ntp.org/zone/ch

Quelle: Obsidian `Knowledge Base/Proxmox/NTP Proxmox Cluster.md` · Stand: 2026-10-12 · Automatisiert publiziert durch Hermes.

UEFI Secure Boot Zertifikate 2023 (Proxmox EFI-Disk)

UEFI Secure Boot Zertifikate 2023 (Proxmox EFI-Disk)

> **abstract:** Problem EFI-Disk ohne `ms-cert=2023k`-Marker: die UEFI-2023-Zertifikate von Microsoft sind nicht eingespielt. Die originalen UEFI-2011-Zertifikate laufen **Juni 2026** ab. Die 2023-Zertifikate werden für Secure-Boot-Updates von Windows und gängigen Linux-Distributionen benötigt.

Hintergrund

- Die Firmware bootet nur Bootloader, deren Signaturzertifikate auf der EFI-Disk hinterlegt sind. Eine EFI-Disk mit nur den 2011-Zertifikaten **verwirft** mit den 2023-Zertifikaten signierte Bootloader.
- Seit `pve-edk2-firmware >= 4.2025.05-1` enthalten neu erstellte EFI-Disk **beide** Zertifikatsätze (2011 + 2023) und tragen den Marker `ms-cert=2023k` in der VM-Konfiguration.
- Für EFI-Disks, die **vor** dieser Version erstellt wurden, müssen die Zertifikate nachgerüstet werden.
- Marker `ms-cert=2023` / `ms-cert=2023w` bedeuten **unvollständige** Enrollment — im Start-Task-Log wird gewarnt; auch hier die Enrollment-Prozedur anwenden.

Lösung

In der Proxmox-Web-UI (VM kann laufen):

1. EFI-Disk in der Hardware-Ansicht auswählen → `Disk Action > Enroll Updated Certificates`.
2. Alternativ denselben Effekt über den API-Endpoint `/nodes/{node}/qemu/{vmid}/config` erreichen; die Enrollment greift beim nächsten Start der VM.

CLI (VM muss heruntergefahren sein):

```
qm enroll-efi-keys <VMID>
```

Windows mit BitLocker

Vor der Enrollment bei jedem BitLocker-Laufwerk in PowerShell (als Administrator):

```
manage-bde -protectors -disable C:
```

Wichtig für **jedes** BitLocker-Laufwerk; sonst verlangt der nächste Boot den BitLocker-Wiederherstellungsschlüssel. Für das Windows-Update und das Signieren des Bootloaders mit den 2023-Zertifikaten die Microsoft-Support-Artikel zu CVE-2023-24932 (Enterprise-Deployment-Guidance) beachten.

Verifikation

```
qm config <VMID> | grep ms-cert
## erwartet: ms-cert: 2023k
```

Quellen

- Proxmox VE Administration Guide – Secure Boot Certificate Expiration: https://pve.proxmox.com/pve-docs/chapter-qm.html
- Proxmox VE `qm(1)` Manpage – `qm enroll-efi-keys`: https://pve.proxmox.com/pve-docs/qm.1.html
- Microsoft – Windows Secure Boot certificate expiration and CA updates: https://support.microsoft.com/en-us/topic/windows-secure-boot-certificate-expiration-and-ca-updates-7ff40d33-95dc-4c3c-8725-a9b95457578e

---

Quelle: Obsidian `Knowledge Base/Proxmox/UEFI Secure Boot Zertifikate 2023.md` · Stand: 2026-10-12 · Automatisiert publiziert durch Hermes.