

Einrichtung eines sicheren SSH-Zugangs für Proxmox und LXC

Das Ziel ist es, ein einheitliches, schlüsselbasiertes Authentifizierungsmodell sowohl für den Proxmox-Host als auch für seine Container aufzubauen:

- keine SSH-Root-Anmeldung
- keine Passwortauthentifizierung
- Zugriff nur über einen `admin`-Benutzer mit einem SSH-Schlüssel
- bequemer Zugriff über die SSH-Konfiguration

Dieser Ansatz reduziert die Angriffsfläche und macht alles deutlich einfacher zu verwalten.

Teil 1: Bereite deinen lokalen Rechner vor

Generiere ein SSH-Schlüsselpaar

Falls du noch keins hast:

```
ssh-keygen -t ed25519 -C "admin"
```

Speichere es sicher, zum Beispiel hier:

```
/home/deinname/.ssh/admin_key
```

Optional: Füge den Schlüssel zum Agenten hinzu

Wenn der Schlüssel eine Passphrase hat:

```
ssh-add /home/deinname/.ssh/admin_key
```

Teil 2: Sichere den Proxmox-Host

Erstelle einen Administratorbenutzer

Auf dem Proxmox-Host (über Web-Shell oder SSH):

```
adduser admin
usermod -aG sudo admin
```

Stelle den SSH-Schlüssel bereit

```
ssh-copy-id -i /home/deinname/.ssh/admin_key.pub admin@<Proxmox-Hostname>
```

Teste den Zugriff:

```
ssh -i /home/deinname/.ssh/admin_key admin@<Proxmox-Hostname>
```

Deaktiviere die unsicheren Authentifizierungsmethoden

Bearbeite `/etc/ssh/sshd_config`:

```
PermitRootLogin no
PasswordAuthentication no
ChallengeResponseAuthentication no
PubkeyAuthentication yes
```

Wende die Änderungen an:

```
systemctl restart sshd
```

Der Host akzeptiert jetzt nur noch schlüsselbasierte Anmeldungen für den `admin`-Benutzer.

Teil 3: Sichere deine LXC-Container

Viele Vorlagen erlauben SSH-Zugriff als Root – teilweise sogar mit Passwort. Wende dieselben Sicherheitsmaßnahmen in jedem Container an.

Erstelle einen Administratorbenutzer

Gehe in den Container:

```
pct enter <CTID>
```

Lege den Benutzer an und gib ihm sudo-Rechte:

```
adduser admin  
usermod -aG sudo admin
```

Stelle deinen Schlüssel im Container bereit

Auf deinem lokalen Rechner:

```
ssh-copy-id -i /home/deinname/.ssh/admin_key.pub admin@<lxc-ip-oder-hostname>
```

Teste:

```
ssh admin@<lxc-ip-oder-hostname>
```

Deaktiviere die unsicheren Methoden im Container

Bearbeite `/etc/ssh/sshd_config`:

```
PermitRootLogin no  
PasswordAuthentication no  
ChallengeResponseAuthentication no  
PubkeyAuthentication yes
```

Starte neu:

```
sudo systemctl restart sshd
```

Der Container hat jetzt exakt dieselbe Sicherheitsstufe wie der Host.

Teil 4: Mach dir das Leben mit der lokalen SSH-Konfiguration leichter

Erstelle oder bearbeite die Datei:

```
~/.ssh/config
```

Beispiel-Inhalt:

```
Host proxmox
  HostName <Proxmox-Hostname>
  User admin
  IdentityFile /home/deinname/.ssh/admin_key

Host lxc-admin
  HostName <lxc-ip-oder-hostname>
  User admin
  IdentityFile /home/deinname/.ssh/admin_key
```

Schütze die Datei:

```
chmod 600 ~/.ssh/config
```

Ab jetzt reicht:

```
ssh proxmox
ssh lxc-admin
```

Ergebnis

- Proxmox-Host und alle Container nutzen dieselbe sichere Anmeldemethode.
- Root-Login ist überall deaktiviert.
- Passwort-Authentifizierung ist überall aus.
- Ein einziger Schlüssel + ein einziger Benutzer (`admin`) für den administrativen Zugriff.
- Super einfache Verbindung über sprechende Host-Namen in der SSH-Konfiguration.

Revision #4

Created 2025-11-26 20:42:19 UTC by Carsten

Updated 2026-02-14 14:52:42 UTC by Carsten