

UniFi on Proxmox: Setup and Recovery Decision Guide

When to host the UniFi Network Application on Proxmox, how to size and protect the VM, and when a UniFi Console is the better pick.

Updated **2026-10-29** · Full guide: www.mrplanb.com/blog/should-you-run-the-ubiquiti-unifi-network-application-on-proxmox

Running UniFi on Proxmox works well when you already operate dependable virtualization and only need UniFi Network management. Use a dedicated Debian or Ubuntu VM with a fixed IP, keep both UniFi and Proxmox backups, and test the restore. Choose a CloudKey or other UniFi Console when you want the simplest vendor-supported setup.

2 GB

minimum memory in Ubiquiti's published UniFi OS Server requirements

2 vCPU

starting point for a small network, with 2 to 4 GB RAM

20–40 GB

suggested storage for a small deployment

2

backup types to keep: UniFi backup and Proxmox VM backup

Setup checklist

A dedicated Linux VM is the safer default. Do not install UniFi on the Proxmox host.

- ☐ Use a Debian 13 or Ubuntu 24.04 (or later) VM, not LXC and not the Proxmox host.
- ☐ Start with 2 vCPUs, 2 to 4 GB RAM and 20 to 40 GB of storage for a small network.
- ☐ Give the VM a fixed or reserved IP address.
- ☐ Attach it to a trusted management network through a Proxmox bridge.
- ☐ Make sure it can reach every UniFi device it manages (routing, firewall rules, Layer 3 adoption if needed).
- ☐ Document the address, routes and adoption method for restore day.
- ☐ Keep a management path to Proxmox that does not depend on the UniFi VM.

VM, LXC or CloudKey?

	Linux VM	LXC	UniFi Console / CloudKey
Fit	Safer default	Possible, less clear	Simplest vendor-supported
Kernel	Own kernel, separate from host	Shares host kernel	Dedicated hardware
Main risk	You maintain Linux and backups	Questions on services, nesting, compatibility	Another box to buy
Backups and updates	Yours to run	Yours to run	Automated, integrated
Other UniFi apps (Protect, Access, Talk, Connect)	Need compatible hosting	Need compatible hosting	Supported on the hardware

Back up both layers

UniFi backup

Network backup files hold settings and device configuration and restore into another compatible UniFi host.

Proxmox VM backup

Protects the whole VM: OS, software and database. Fastest way to restore the full guest.

Off-box copy

Keep at least one copy outside the Proxmox server and outside the storage holding the UniFi VM.

Restore test

Confirm devices reconnect to the restored application. Until then the plan is incomplete.

Update and migrate safely

- 1 Take a UniFi Network backup before any update or migration.
- 2 Create a Proxmox backup before a major update.
- 3 Update Proxmox, the guest OS and UniFi in separate maintenance windows.
- 4 For migration, update the new host, download a backup from the old application, stop or remove the old system, then restore on the new host.
- 5 Check that devices show online. Layer 3 setups may need the inform address changed.
- 6 Never run two active copies, and never clone an active UniFi VM as a standby.

If the UniFi VM goes down

- Adopted access points and switches generally keep their last applied configuration and traffic continues.
- You temporarily lose central monitoring, configuration changes, alerts and some management functions.
- It gets more serious if the VM also serves guest portals or you need it to diagnose another network problem.
- Proxmox HA can restart the VM on another node, but it is not instant: the VM, OS and UniFi services must all start.
- Every recovery node needs access to the same management VLANs and routed networks.
- For many small businesses, reliable backups and a documented restore process may be enough.

Sources and notes: Ubiquiti UniFi OS Server and Network Application self-hosting guidance, as summarized on the page · Proxmox VE networking and HA documentation, as summarized on the page