Specific Terms and Conditions – Management Proxmox VE

Updated: June 10, 2025

1.0 General

This agreement governs the relationship between ServeTheWorld AS (STW) and the Customer. The purpose of this document is to define the specific terms and conditions applicable to the basic operations of the Proxmox VE server. These terms are in addition to STW's General Terms and Conditions, available on the company's website, currently available at https://stw.no/en-us/legal/

In case of conflict between the two, the specific terms outlined here shall take precedence over the general terms.

Any matters not defined in the specific terms fall under the General Terms and Conditions.

2.0 90-Day Money-Back Guarantee

If the Customer is not satisfied after using the service for up to 90 days and decides to terminate the service, the entire amount paid will be refunded.

3.0 Scope of Service

Basic operations include daily management, maintenance, and monitoring of one or more Proxmox VE nodes, including the underlying Debian operating system. Servers can be customer-owned, rented from the provider as a separate service, or rented from a third party chosen by the customer. The provider is responsible for keeping Proxmox VE components (like pve-kernel, pve-manager, and qemu-kvm) and Debian packages in the standard installation up to date.

4.0 Operation and Updating of Proxmox VE

To qualify for basic operations, the node must run a Proxmox VE major version still supported with security updates by Proxmox GmbH. The service includes access to the enterprise repository via a Proxmox community subscription. The provider follows its own maintenance plan and installs updates as soon as they are deemed stable. If updates affect virtual guests—such as changes to drivers or agents—it is the customer's responsibility to manage the consequences. Customers may request to postpone updates, but they assume the risk for any resulting issues.

5.0 Monitoring

The provider continuously monitors various aspects of the server environment, including availability via ping or SSH, Proxmox cluster status through Corosync and Quorum, and resource usage such as CPU, memory, and storage in ZFS, LVM, or Ceph pools. Monitoring is conducted using modular tests adapted to the specific environment.

6.0 System Access

The customer must ensure the provider has root or sudo access via SSH, preferably through a dedicated user, and ensure necessary firewall and ACL rules are configured for monitoring and administration. In the event of hardware failure, access to IP-KVM, iDRAC, or iLO must also be granted. If the provider loses the necessary access to fulfill its operational responsibilities, the responsibility is temporarily suspended until access is restored. The customer's payment obligation remains unaffected, and any additional costs incurred may be invoiced.

7.0 Responsibility During Monitoring Disruptions

If the monitoring system suffers technical failures, the provider is obligated to restore functionality as soon as the issue is detected. During any downtime, alerts are not considered delivered, and the provider is not liable for incidents that go undetected in this period.

8.0 Service Limitations

The service does not include configuration or operation of virtual guests, container templates, or software running inside the guests. It also excludes third-party software not found in Proxmox's or Debian’s official APT repositories, and does not include customizations beyond the standard Proxmox platform functionality.

9.0 Maintenance Window

All planned security updates and patches are typically performed during regular business hours, defined as 08:00 to 16:00 CET. If the customer prefers updates outside this window, this must be agreed upon in writing. Virtual machines are migrated between servers as needed to allow maintenance without downtime.

10.0 Cluster Capacity Requirements

To maintain proper Proxmox cluster operation, it must always be possible to take down at least one node for maintenance without affecting the availability of virtual guests. The customer is responsible for ensuring sufficient capacity, either by adding nodes/resources or reducing usage (e.g., by limiting CPU/RAM overcommitment, reducing the number of VMs, or lowering disk usage). If the recommended capacity is not followed, the provider disclaims responsibility for any service interruptions due to resource shortages.

11.0 CEPH Storage

When Ceph is used as a distributed storage solution in the cluster, the provider is responsible for installation, operation, and monitoring of all Ceph components, including OSD, MON, MDS, and RGW. These components are subject to the same operational, updating, and monitoring terms as the rest of the server environment.

12.0 Backup

Basic operations do not include backup of virtual guests or data. The customer must implement and manage an external backup solution, such as Proxmox Backup Server, Veeam, or similar. Alternatively, the customer may order backup as an add-on service provided by the vendor.

13.0 Liability

Under no circumstances can the customer claim compensation exceeding the amount paid for the service in the last 12 months from the time the issue was reported. Compensation does not cover indirect losses, including lost profits, consequential damages, or other incidental losses. Claims must be submitted without undue delay. STW is not liable in cases of Force Majeure.