LOGZILLA DOCUMENTATION

Proxmox VE

Rules, dashboards, and triggers for Proxmox Virtual Environment and integrated Ceph storage

LogZilla App Store · Generated June 17, 2026 · logzilla.ai/docs/logzilla-appstore/proxmox

Overview

Proxmox Virtual Environment (PVE) is an open-source server virtualization platform that manages KVM virtual machines and LXC containers, software-defined storage and networking, clustering, and high availability from a single web interface. PVE clusters are frequently deployed hyper-converged with integrated Ceph distributed storage. Each node is Debian-based and emits standard syslog from its management daemons, cluster stack, firewall, and Ceph services.

App Function

- Parse Proxmox VE management-plane syslog identified by program name (`pvedaemon`, `pveproxy`, `pvestatd`, `pmxcfs`, `corosync`, `pve-ha-lrm`, `pve-ha-crm`, `qmeventd`, `vzdump`, `pvefw-logger`, and related daemons).
- Parse integrated Ceph daemon logs (`ceph-osd`, `ceph-mon`, `ceph-mgr`, `ceph-mds`) and classify storage-health conditions under `Product=Ceph`.
- Extract metadata tags for authentication, task lifecycle (UPID), HA service state, cluster quorum, firewall verdicts, backups, and storage.
- Categorize events with cross-vendor Event Class / Event Type taxonomy and apply the relevant compliance frameworks.
- Strip per-event-unique noise (UPID worker identifiers, Ceph thread ids and timestamps, variable timing values) so repeated events deduplicate.
- Provide dashboards for cluster/HA health, tasks and backups, authentication and firewall activity, and Ceph storage health.
- Alert on quorum loss, cluster link failure, HA fencing, login failures, failed tasks/backups, and Ceph OSD or health failures.

Vendor Documentation

- Proxmox VE Documentation Index (https://pve.proxmox.com/pve-docs/)
- Proxmox VE Administration Guide (https://pve.proxmox.com/pve-docs/pve-admin-guide.html)
- Cluster Manager (pvecm, corosync) (https://pve.proxmox.com/wiki/Cluster_Manager)
- High Availability (https://pve.proxmox.com/wiki/High_Availability)
- Proxmox VE Firewall (https://pve.proxmox.com/wiki/Firewall)
- Deploy Hyper-Converged Ceph Cluster (https://pve.proxmox.com/wiki/Deploy_Hyper-Converged_Ceph_Cluster)

Device Configuration

Proxmox VE 8 logs to the systemd journal by default. To forward logs to LogZilla, install and configure `rsyslog` on each node to relay the journal over the network. No dedicated LogZilla port is required: each Proxmox daemon sets a unique syslog program name, so the app identifies events by program name without a dedicated port.

Install rsyslog on each Proxmox node (if not already present):

```
apt-get update && apt-get install -y rsyslog
```

Create `/etc/rsyslog.d/99-logzilla.conf` and forward all facilities to the LogZilla server, replacing `LOGZILLA_IP` with the server address:

```
module(load="imjournal" StateFile="imjournal.state")

*.* action(
  type="omfwd"
  target="LOGZILLA_IP"
  port="514"
  protocol="tcp"
  template="RSYSLOG_SyslogProtocol23Format"
  action.resumeRetryCount="-1"
  queue.type="LinkedList"
  queue.size="50000"
)
```

Restart rsyslog:

```
systemctl restart rsyslog
```

Repeat on every node in the cluster.

Firewall packet logs (`pvefw-logger`) are written to `/var/log/pve-firewall.log` and are not sent to syslog by default. To capture the firewall verdicts described below, configure the node to also forward that file (for example with an rsyslog `imfile` input) or raise the firewall log level under **Datacenter -> Firewall -> Options**.

Verification

Trigger a recognizable event (for example, log in to the Proxmox web UI or start a VM) and confirm events arrive in LogZilla with `Vendor` set to `Proxmox`.

Incoming Log Format

Proxmox emits standard syslog with the daemon as the program (tag) field:

```
<program>[<pid>]: <message>
```

- **program** - Proxmox daemon name (`pvedaemon`, `corosync`, `pve-ha-lrm`, `ceph-osd`, ...)

- **pid** - Process ID
- **message** - Daemon-specific event text

Task workers embed a Unique Process ID (UPID) describing the operation:

```
UPID:<node>:<pid>:<pstart>:<starttime>:<type>:<id>:<user>:
```

The `<type>` (for example `qmstart`, `vzdump`, `qmdestroy`), guest `<id>`, and `<user>` are extracted; the volatile hex fields are removed to aid deduplication.

Ceph daemons prefix each line with an ISO 8601 timestamp and thread id:

```
<ISO8601 timestamp> <thread-id> <level> <entity> <message>
```

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Proxmox`	Always `Proxmox`
`Product`	`VE`	`VE` for the management plane, `Ceph` for storage
`Event Class`	`HA`	Cross-vendor class (Auth, Config, HA, Security, System)
`Event Type`	`High Availability`	Cross-vendor event type
`Action`	`quorum lost`	Auth result, firewall verdict, or cluster action
`User`	`root@pam`	Realm-qualified user for a login or task (HC)
`PVE Realm`	`pam`	Authentication realm (`pam`, `pve`, `pbs`, `ad`, `ldap`)
`PVE Task Type`	`qmstart`	Task (UPID) operation
`PVE Task Status`	`OK`	Result of a completed task (`OK` or `Error`)
`PVE VMID`	`100`	Guest ID; `0` denotes the host firewall
`PVE HA State`	`fence`	HA service or manager state

Tag Name	Example	Description
PVE Storage	cephpool	Datastore in a storage activation or mount error
SrcIP	198.51.100.23	Source IP, login rhost or firewall SRC (HC)
DstIP	192.0.2.10	Firewall destination IP (HC)
DstPort	ssh	Firewall destination port (named service)
Protocol	TCP	Firewall protocol
Ceph Event	OSD Marked Down	Classified Ceph health condition
Ceph OSD	5	Ceph OSD numeric ID

Log Examples

Web Authentication Failure

```
pvedaemon[12345]: authentication failure; rhost=::ffff:198.51.100.23 user=admin@pve
msg=Authentication failure
```

VM Start Task

```
pvedaemon[12345]: <root@pam> end task UPID:pve1:001A2B3C:0A1B2C3D:65000000:qmstart:100:root@pam: OK
```

HA Service Fenced

```
pve-ha-crm[2900]: service 'vm:101': state changed from 'started' to 'fence'
```

Cluster Quorum Lost

```
pmxcfs[2345]: [status] notice: node lost quorum
```

Corosync Link Down

```
corosync[1936]: [KNET ] link: host: 2 link: 0 is down
```

Firewall Packet Dropped

```
pvefw-logger[1234]: 0 6 PVEFW-HOST-IN 13/Jun/2025:10:15:42 +0000 DROP: IN=vmbr0 OUT= SRC=203.0.113.5
DST=192.0.2.10 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=12345 PROTO=TCP SPT=44321 DPT=22
```

Backup Finished

```
vzdump[5678]: INFO: Finished Backup of VM 100 (00:05:46)
```

Ceph OSD Heartbeat Failure

```
ceph-osd[3210]: 2024-10-08T17:42:58.892-0400 7a13a6950840 -1 osd.5 19 heartbeat_check: no reply from
192.0.2.7:6802 osd.7
```

Ceph Health Error

```
ceph-mon[2100]: 2024-10-08T18:10:00.000-0400 7a1300000002 -1 mon.pve1@0(leader) e9 cluster [ERR]
Health check failed: Reduced data availability: 4 pgs inactive (PG_AVAILABILITY)
```

Dashboards

- **Proxmox: Cluster & HA** - quorum, corosync links, HA service states, and fencing across the cluster.
- **Proxmox: Tasks & Backups** - VM/container task volume, failures, backup results, and configuration changes.
- **Proxmox: Authentication & Firewall** - web login success/failure and firewall verdicts with top sources and ports.
- **Proxmox: Ceph Storage Health** - OSD heartbeat failures, slow ops, OSDs marked down, and cluster health warnings/errors.

Triggers

Trigger	Description
`Proxmox: Cluster quorum lost`	A node lost cluster quorum
`Proxmox: Cluster link down`	A corosync cluster link went down
`Proxmox: HA service fenced`	An HA service transitioned to the fence state
`Proxmox: Web authentication failure`	A Proxmox web/API login failed
`Proxmox: Task or backup failure`	A task worker or backup job ended in error
`Proxmox: Ceph OSD down or failed`	A Ceph OSD was marked down or reported failed
`Proxmox: Ceph health error`	Ceph reported a HEALTH_ERR condition