LOGZILLA DOCUMENTATION

Vmware Vsphere

LogZilla App Store application: Vmware Vsphere

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/vmware-vsphere

Overview

VMware vSphere is a virtualization and cloud computing platform that enables organizations to create, run, and manage virtual machines (VMs) and cloud-based services. It provides a complete virtualization infrastructure, including virtualized computing, networking, storage, and security resources.

vSphere enables multiple operating systems and applications to run on a single physical server or cluster of servers, allowing organizations to consolidate IT infrastructure and reduce hardware costs. Key features include High Availability (HA), Distributed Resource Scheduler (DRS), and Fault Tolerance (FT) for increased reliability and availability of virtualized applications.

App Function

- Parse VMware vSphere syslog messages from ESXi, vCenter, and vSAN
- Extract user from RFC 5424 structured data for audit trails
- Classify events by type (auth, ha, storage, system)
- Identify ESXi problems from vobd daemon
- Track HA cluster state changes
- Provide dashboards for infrastructure monitoring

Vendor Documentation

- VMware vSphere (https://techdocs.broadcom.com/us/en/vmware-cis/vsphere.html)

Device Configuration

VMware events require a dedicated syslog port in LogZilla to enable RFC 5424 structured data parsing. The dedicated port tags incoming events with a `source_type` that routes them to the VMware parsing rule. Configure LogZilla first, then configure the VMware devices.

LogZilla Configuration

Navigate to **Settings > System > Application Ports**
Set **VMware syslog port** to a dedicated port (e.g., `5522`)
Click **Save**
The syslog and parser services reload automatically. Both TCP and UDP listeners are enabled on the configured port.

ESXi Host Configuration

Configure each ESXi host to send syslog via TCP using RFC 5424 format:

Log into the ESXi host via SSH or console
Configure syslog destination with TCP and RFC 5424 formatter:

```
esxcli system syslog config set \
  --loghost="tcp://LOGZILLA_IP:1514?formatter=RFC_5424"
esxcli system syslog reload
```

Verify configuration:

```
esxcli system syslog config get
```

The firewall automatically opens for non-default ports. For port 514, enable the syslog ruleset:

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
```

vCenter Appliance Configuration

Configure vCenter to forward syslog to LogZilla:

Log into the vCenter Appliance Management Interface (VAMI) at `https://vcenter:5480`
Navigate to **Syslog > Configuration**
Click **Configure** and add a new remote syslog destination:

- **Server**: LogZilla IP address
- **Port**: 1514 (or configured port)
- **Protocol**: TCP

Select log levels to forward (recommend: info and above)
Click **Save**

Verification

Generate test events by logging into vCenter or performing a VM operation, then verify events appear in LogZilla with programs like `Hostd`, `vpxd`, or `vmkernel`.

Incoming Log Format

VMware vSphere uses RFC 5424 syslog format with structured data:

```
process[pid]: severity process[pid] [Originator@6876 sub=SUBSYSTEM opID=OPID user=USER] message
```

- **process** - VMware daemon name (Hostd, vpxd, vmkernel, Fdm, vobd, etc.)
- **pid** - Process ID
- **Originator@6876** - VMware structured data block (SD-ID 6876 is VMware's IANA PEN)
- **sub** - Internal subsystem
- **opID** - Operation ID for request tracing
- **user** - Username performing the operation
- **message** - Event description

Supported Programs

Program	Service	Description
`Hostd`	ESXi	Host daemon
`vmkernel`	ESXi	Kernel messages
`vmkwarning`	ESXi	Kernel warnings
`Vpxa`	ESXi	vCenter agent
`vobd`	ESXi	Observer daemon (problems)
`Fdm`	ESXi	Fault Domain Manager (HA)
`vpxd`	vCenter	vCenter daemon
`vcenter-server`	vCenter	vCenter appliance
`vsan`	vSAN	vSAN services

Event Class Values

The `Event Class` tag enables cross-vendor dashboards and filtering:

Value	Description
`auth`	Authentication events (login, logout, password)

Value	Description
`ha`	High availability and failover events
`storage`	Storage events (VMFS, NFS, iSCSI, SCSI)
`network`	Network events (vMotion, portgroup, vSwitch)
`security`	Security events (alarms, audits)
`system`	General system events

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`VMware`	Vendor identifier
`Product`	`vSphere`	Product identifier
`Event Class`	`storage`	Cross-vendor event classification
`VMware Service`	`ESXi`	Service type: ESXi, vCenter, vSAN
`VMware Problem`	`clock.correction.adjtime.sync`	ESXi problem type from vobd
`VMware HA State`	`Master`	HA cluster state
`User`	`vpxuser`	Username from RFC 5424 structured data
`SrcIP`	`192.168.1.100`	Source IP from auth events

Log Examples

Hostd Event

```
info hostd[2101836] [Originator@6876 sub=Libs opID=62a3c433 user=vpxuser]
SlowRefresh: path /vmfs/volumes/65aec72d-3e2d2f46-79e2-0025b5320a0f
```

vmkernel Event

```
cpu39:2097544)StorageDevice: 7059: End path evaluation for device
naa.600a098038314372395d564664487a57
```

FDM HA Event

```
info fdm[2100462] [Originator@6876 sub=Cluster opID=SWI-10d63af1]
hostId=host-6031 state=Slave master=host-6047 isolated=false
```

vobd Problem Event

```
[ClockCorrelator] 697517624666us: [esx.problem.clock.correction.adjtime.sync]
system clock synchronized to upstream time servers
```

Dashboards

Two Event Class-aligned dashboards provide focused views for different analyst roles:

Dashboard	Event Class	Purpose
`VMware vSphere: Security`	`auth`	User activity, login tracking, source IPs
`VMware vSphere: System`	`system`, `ha`, `storage`	HA state, problems, errors

Triggers

Trigger	Description
`VMware: HA State Change`	HA cluster Master/Slave transitions
`VMware: Storage Error`	Storage events with severity error or worse
`VMware: ESXi Problem Detected`	vobd hardware/driver issues
`VMware: Kernel Warning`	vmkwarning kernel-level issues

Trigger	Description
`VMware: Critical System Error`	Severity 0-2 on any VMware event
`VMware: User Login Tracked`	Auth events with user (audit trail, no notification)
`VMware: Privileged User Login`	root or administrator@vsphere.local access