ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · VMWARE VSPHERE

VMware vSphere monitoring, cluster by cluster.

How ClearWatch reads vCenter and ESXi with a read-only account, files each cluster under its client, and alerts on hosts, datastores and alarms.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO VMWARE VSPHERE: VCENTER SERVER AND ESXI

EXECUTIVE SUMMARY

vCenter knows everything. It tells whoever is looking.

vCenter Server is where a vSphere environment is run, and its alarms are read inside the vSphere Client, one vCenter at a time. When one vCenter runs clusters for several sites or several clients, nothing in it says which client a host belongs to, and a disconnected host or a filling datastore waits for someone to log in.

ClearWatch reads vCenter, or a standalone ESXi host, through a ClearBridge with a read-only vSphere account. Each cluster is filed under a client and location you choose, its ESXi hosts and virtual machines become devices there, and a lost host, a low datastore or a new red alarm raises an alert on the right device.

KEY TAKEAWAYS

- **Nothing installed, nothing written:** a read-only account over the vSphere API.
- **Filed per cluster:** each cluster maps to a client and location; an unmapped one is held.
- **Hosts and VMs become devices:** each ESXi host carries its own alarms, and VMs follow their host.
- **Changes, not history:** the first read is a baseline, so day one pages nobody about last year.

IN THIS BRIEF

01 **The challenge** — What the vSphere Client leaves to you — 2
02 **How ClearWatch connects** — ClearBridge, account, certificate — 2
03 **Clusters and clients** — The vSphere panel, cluster filing — 4
04 **Hosts and virtual machines** — Topology, host and VM pages — 5
05 **Checks and alerts** — What raises an alert, and where — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs and IT teams who run VMware vSphere, whether one standalone ESXi host or a vCenter managing clusters across several sites or clients.

AT A GLANCE

READ BY	ACCESS	FILING	ALERTS
A ClearBridge	**Read-only**	**Per cluster**	**Red, not yellow**
Over the vSphere API on port 443, every five minutes.	A vSphere account; the certificate is pinned on first use.	To a client and location; held until someone maps it.	Lost hosts, datastores under 10% free, red alarms.

01 THE CHALLENGE

vCenter sees every host. Nobody sees vCenter.

The vSphere Client is a complete console for one environment: hosts, datastores, virtual machines and a long list of alarms, red and yellow. It answers whoever has it open. An MSP or an IT team with several vCenters, or one vCenter whose clusters serve different sites or clients, has to open each one and know from memory which cluster belongs to whom. A host that stops responding overnight is in the inventory, marked, and unread.

THE QUESTION	VSPHERE CLIENT ALONE	CLEARWATCH
Is every ESXi host connected?	The host list, per vCenter	A host that leaves **connected** raises an alert on that host's own device
Which client is this cluster?	Folder and cluster names	Each cluster **mapped to a client and location**; an unmapped one is held
Is a datastore filling?	The datastore view, per vCenter	Fullest first on the panel; **under 10% free** or inaccessible alerts
Which alarms matter?	Every red and yellow alarm, in one list	A **new red alarm** alerts; yellow is shown and pages nobody
Where are the VMs?	The vCenter inventory	VMs become **devices under their host's client**, with VMware Tools state
Every vSphere environment at once?	One vSphere Client per vCenter	**One Hypervisors dashboard**, beside Proxmox VE and Hyper-V

The first collection is a baseline

Adding a vCenter with a six-month-old yellow alarm and a host in maintenance must not page anybody about the last six months. So the first collection only records the current state, and the panel shows it. From then on, ClearWatch compares each collection with the one before and alerts on what **changed**.

02 HOW CLEARWATCH CONNECTS

Through a ClearBridge, with a read-only account

vCenter and ESXi do not run the ClearWatch agent, so a ClearBridge reads them: the agent on any machine on the same network. Nothing is installed on a host, nothing is written to vSphere, and nothing is opened to the internet.

YOUR NETWORK
vCenter Server or ESXi
Answers the vSphere API on port 443, the same API for a vCenter and a single host.

→

YOUR NETWORK
ClearBridge
Reads hosts, clusters, datastores, VMs and alarms every five minutes, and pins the certificate.

→

CLEARWATCH
Panel, devices, alerts
Files each cluster, makes hosts and VMs devices, and alerts on what changed.

02 HOW CLEARWATCH CONNECTS, CONTINUED

Add it as a hypervisor, then give it a vSphere check

A vCenter, or a standalone ESXi host, is added from Hypervisors as a device with the platform **VMware ESXi** 1 . ESXi cannot run the agent, so the window asks which ClearBridge watches it 2 . That ClearBridge decides the client and location the device is added under, and it starts with a ping right away.

On the new device's ClearBridge Check card, a **vSphere (ESXi or vCenter)** check is then added with the address, the port (443 unless you changed it) and a vSphere account 3 . It reads the hosts, datastores, virtual machines and alarms every five minutes.

YOU PROVIDE	WHY
A read-only vSphere account	Saved as a **vSphere account (ESXi or vCenter)** credential, username and password, sealed in ClearWatch. ClearWatch sees exactly what the account can see.
The address	As the ClearBridge reaches it. A private address is fine.
A ClearBridge	Any machine on that network running the ClearWatch agent.

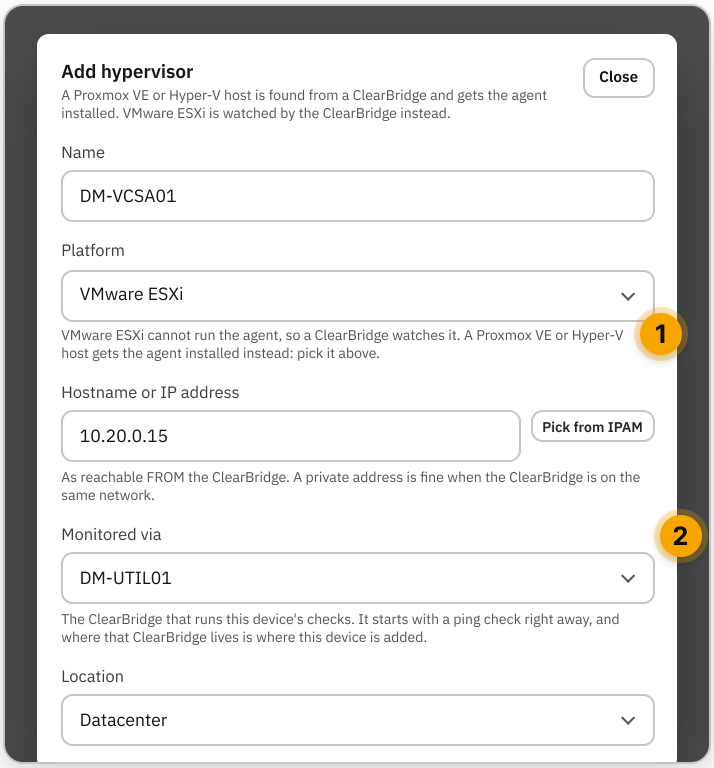


FIGURE 1 Adding a vCenter from Hypervisors, rebuilt from the ClearWatch console with demo data.

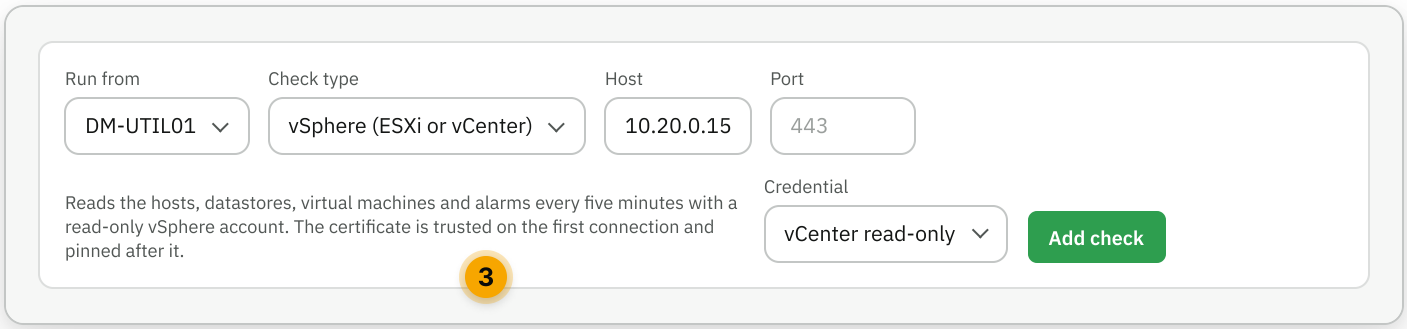


FIGURE 2 The add row at the foot of the device's ClearBridge Check card.

The certificate, pinned on first use

vCenter and ESXi usually carry a self-signed certificate, so the first collection trusts the certificate it meets and pins its SHA-256 fingerprint. After that any other certificate is refused, and the check goes down naming both fingerprints.

A collection can never replace a pin. After a real certificate renewal, a person with the right to change monitoring presses **Forget certificate**, and the action is logged.

One check for vCenter and ESXi

- vCenter and a standalone ESXi host answer the same vSphere API, so one check type reads both. The panel says which it found: **vCenter Server** or **Standalone ESXi**.
- The account only reads. ClearWatch has no power, snapshot or console control for a VMware VM, so it never needs more.
- The check is up when a collection succeeds. It is down when the address cannot be reached, the login is refused or the certificate changed, and its detail says which.

03 CLUSTERS AND CLIENTS

One vCenter, each cluster filed where it belongs

The first collection puts a vSphere panel on the vCenter's page: four tiles, the clusters and where each is filed, then every ESXi host. Here an MSP's vCenter runs clusters for two clients and a lab.

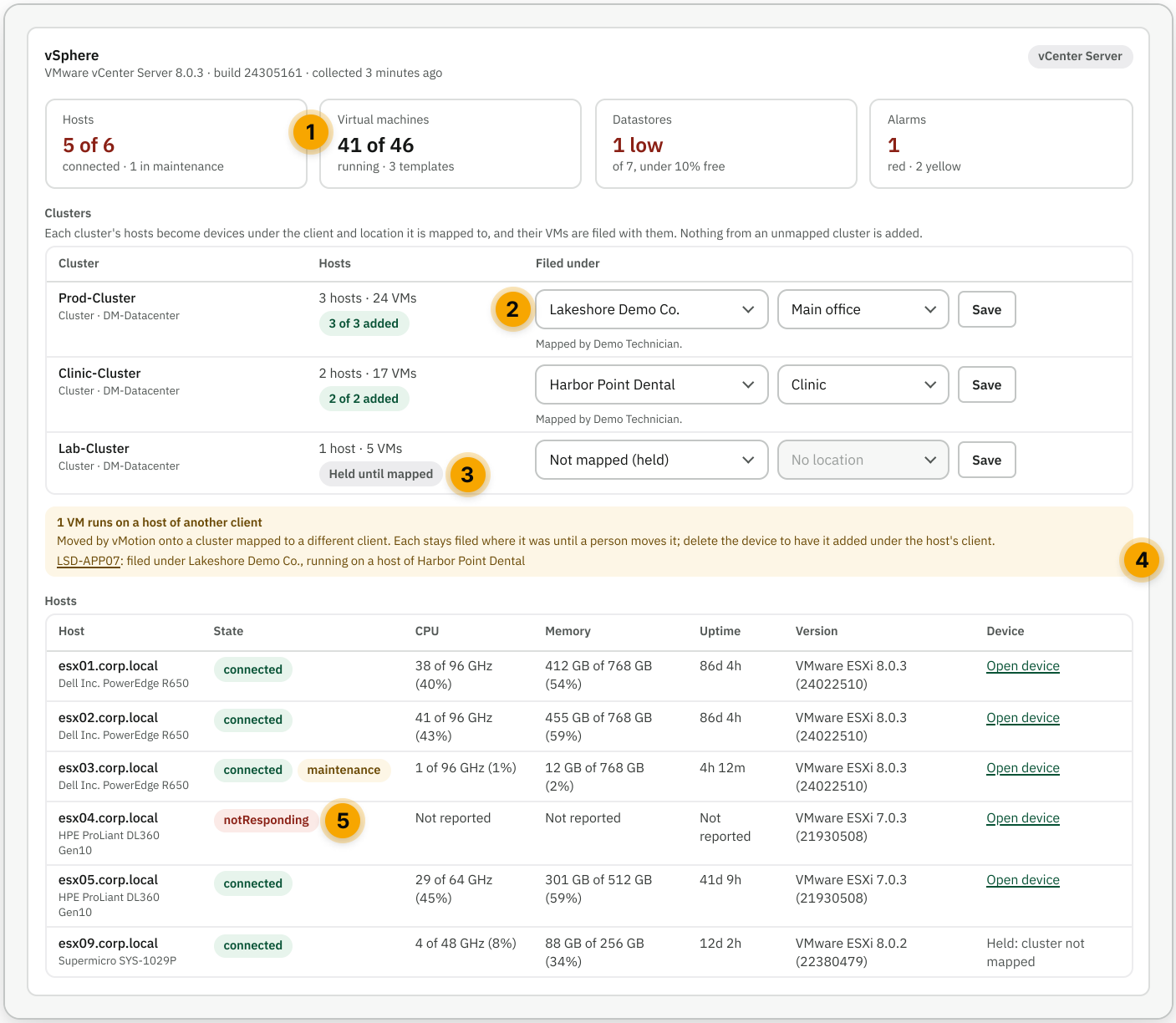


FIGURE 3 The vSphere panel on a vCenter's page: tiles, Clusters and Hosts.

The tiles count hosts connected, VMs running, low datastores and red alarms 1 . A host that is not connected turns the count red. vSphere's own words are shown as they arrived.

Each cluster gets a client and an optional location 2 , from the vCenter's own organization and those below it. Its hosts become devices there at once. An unmapped cluster is **held** 3 : nothing from it is added.

A VM moved by vMotion onto another client's cluster keeps its client and is flagged 4 : its license, checks and history never move without a person. Each host shows its state 5 and links to its device.

04 HOSTS AND VIRTUAL MACHINES

The environment as it is built, every VM a device

On the Hypervisors dashboard a vCenter is drawn like a Proxmox VE cluster: each ESXi host with its VMs inside, datastores underneath.

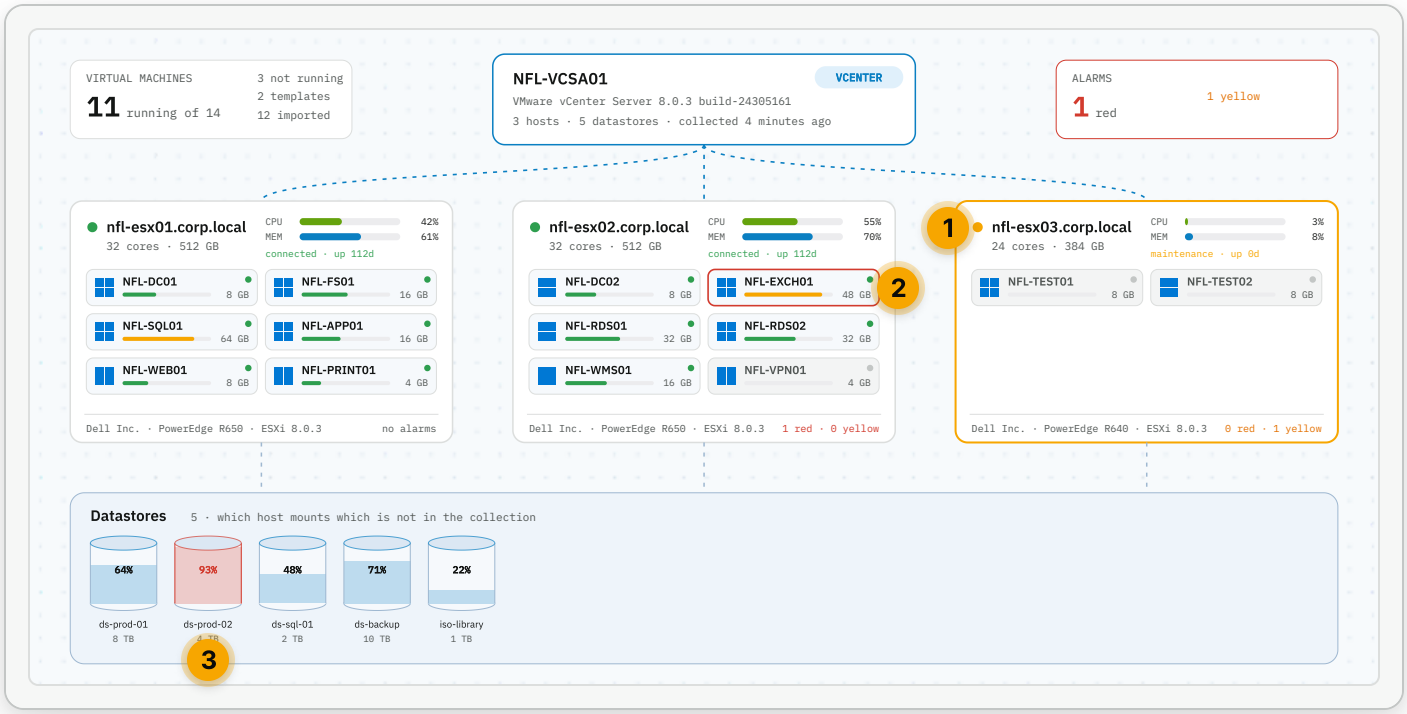


FIGURE 4 A vCenter on the Hypervisors dashboard. Operating system marks are simplified.

Each host shows CPU, memory and its state: amber in maintenance 1 , red when not connected. Maintenance never excuses a lost host.

Each VM shows its power, active memory and size; one with a red alarm is outlined in red 2 . Templates are counted, not drawn.

Datastores show how full they are, red under 10% free or when not accessible 3 . They are drawn as one shared layer.

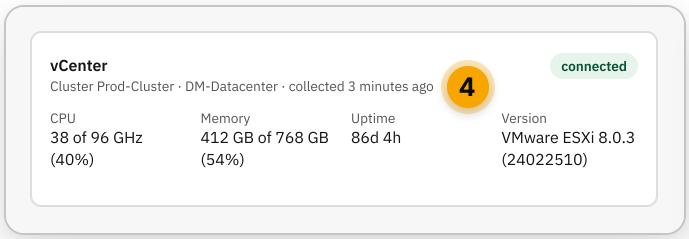


FIGURE 5 The vCenter card on esx01's own page, under Lakeshore Demo Co.

Each ESXi host is a licensed device in its cluster's client and location, with its own slice of what vCenter reports 4 . A client sees its own hosts and never the rest of the vCenter. vCenter is the host's heartbeat: it reads offline after three missed collections, like any device.

A host already in ClearWatch is adopted, not added twice.

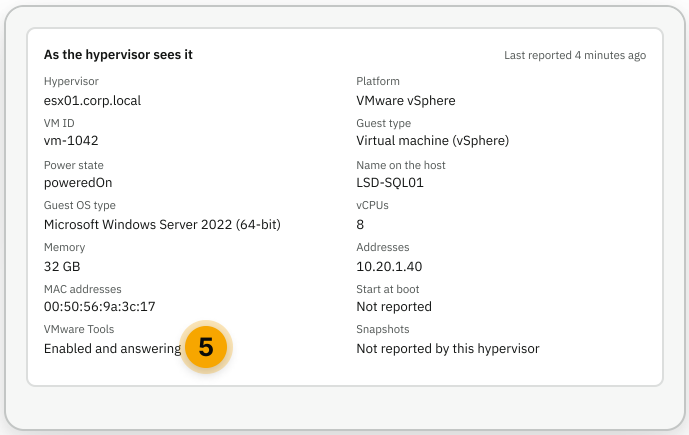


FIGURE 6 A VMware VM's page: what vCenter says about it.

With guest import on, each VM becomes a device filed with its host 5 . It is off unless chosen: each VM uses a license.

05 CHECKS AND ALERTS

What raises an alert, and on which device

After the baseline, each collection is compared with the last. Each change below is filed as **vSphere reported a problem**, an Alert by default. The vSphere check itself is a ClearBridge check like any other, and what its going down means is set on its row.

WHEN	THE ALERT READS	IT CLEARS WHEN
A host leaves connected	vCenter host esx04.corp.local is notResponding	The host is connected again
A datastore drops under 10% free, or goes inaccessible	Datastore ds-prod-02 is 7% free (or: is not accessible)	It has 10% free again, or is accessible
A red alarm appears	vCenter alarm: Host memory usage on esx02.corp.local	vCenter clears the alarm
A hardware sensor turns red or yellow	Sensor Power Supply 2 on esx05.corp.local is yellow	Shown on the panel until it is green
The vSphere check goes down	Unreachable, login refused, or a different certificate	The next collection succeeds

An alert about a host, or a VM on it, lands on **that host's device**, so the client's own people hear about their host. A datastore, or an alarm on the vCenter or a cluster, stays on the vCenter.

Yellow alarms and sensors are listed on the panel 1 and page nobody. Any state vSphere sends that ClearWatch does not know counts as not connected, never as fine. Snoozes and notification policies apply as to any alert.

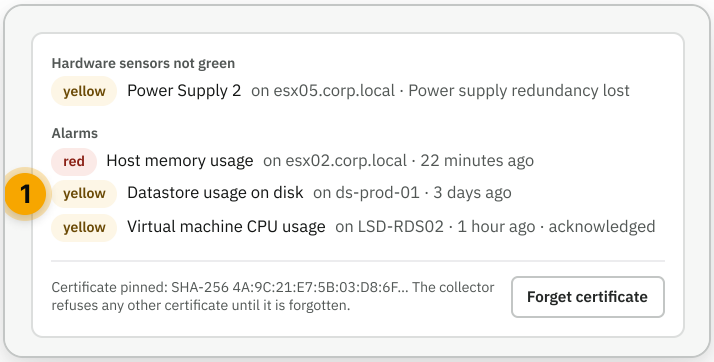


FIGURE 7 The foot of the vSphere panel. All screens are rebuilt with demo data.

06 GOOD TO KNOW

Requirements

- A ClearBridge that reaches vCenter or ESXi on port 443. A VMware-only site can deploy the ClearBridge appliance OVA from the Deployment page.
- A read-only vSphere account that can see the hosts and VMs to be watched.
- Each cluster mapped to a client; each ESXi host and imported VM uses a license.

Limits

- Read-only: no power, snapshot or console control of a VMware VM.
- vSphere reports no VM snapshots to ClearWatch, so snapshot age is not checked for VMware VMs.
- VM figures are vCenter's quick stats; the ClearWatch agent inside a VM reports its own history.
- Read every five minutes.

See every vSphere cluster, client by client.

Start a free trial, or ask us to connect your vCenter with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. VMware, vSphere, vCenter and ESXi are trademarks of Broadcom. Screens show demo data.