How to Troubleshoot a VMware ESXi Host Disconnected from vCenter

An ESXi host can appear as **Disconnected** or **Not Responding** in vCenter while its virtual machines continue running. The safest approach is to restore management connectivity without unnecessarily rebooting the host or interrupting production workloads.

This guide is written for VMware administrators who have access to vCenter Server and, when required, the ESXi Host Client, ESXi Shell, SSH, or out-of-band server management.

> ***Important:*** *Follow your change-control procedures. Avoid restarting the ESXi host as a first response, especially when production virtual machines are running.*

What you will investigate

Work through the problem in this order:

- Confirm the scope and workload impact.
- Check ESXi and vCenter network connectivity.
- Verify DNS and hostname resolution.
- Check time synchronization and certificates.
- Inspect the `hostd` and `vpxa` management agents.
- Review logs.
- Reconnect the host from vCenter.
- Remove and re-add the host only as a last resort.

This order moves from the least disruptive checks to higher-impact actions.

Step 1: Confirm the host state and workload impact

In vCenter, open the affected host and record:

- Host name and cluster
- Current state: **Disconnected**, **Not Responding**, or another error
- Time of the first alert
- Recent vCenter tasks and events
- Any active HA, DRS, vMotion, backup, or replication operations
- Datastore and network alarms

Next, determine whether the virtual machines are still running:

- Check application availability.
- Confirm the VM power states shown in vCenter.
- Check the ESXi Host Client directly if available.
- Use out-of-band management to verify that the physical host is powered on.

Why this matters

A disconnected host may lose management operations while continuing to run its workloads. Rebooting immediately can turn a management-plane problem into a service outage.

Common mistake

Do not assume that a disconnected host is powered off. Confirm the physical state and the VM impact before taking disruptive action.

Step 2: Test management network connectivity

The ESXi management network must be reachable from vCenter. Test the following from an approved management system:

```
ping <esxi-management-ip>
ping <vcenter-ip-address>
```

If you have access to the ESXi Shell or SSH, inspect the management VMkernel interface:

```
esxcli network ip interface ipv4 get
```

Check that:

- The management VMkernel adapter is up.
- The expected IP address is configured.
- The subnet mask is correct.
- The default gateway is correct.
- The management VLAN is available.
- The physical uplink is connected.
- The switch port is assigned to the correct VLAN.

List the physical network adapters:

```
esxcli network nic list
```

Review the routing table:

```
esxcli network ip route ipv4 list
```

Test connectivity from the ESXi host toward vCenter using the management VMkernel interface where required:

```
vmkping <vcenter-ip-address>
```

How to interpret the result

- **ESXi cannot reach vCenter:** Investigate routing, VLANs, gateways, uplinks, or firewalls.
- **ESXi can reach vCenter but vCenter cannot reach ESXi:** Check return routing, firewall rules, ACLs, and the ESXi management interface.
- **IP connectivity works but the host remains disconnected:** Continue with DNS, services, certificates, and logs.

Common mistake

Testing only from your workstation is not enough. Your workstation may be on a different network path from vCenter.

Step 3: Verify DNS and hostname resolution

vCenter and ESXi should consistently resolve the host name and fully qualified domain name.

From the vCenter environment or an equivalent management system, check:

- Forward lookup of the ESXi FQDN
- Reverse lookup of the ESXi management IP
- Resolution of the vCenter FQDN from ESXi
- Whether the host IP changed recently
- Whether stale or duplicate DNS records exist

Confirm that the name configured in vCenter matches the current ESXi identity. A host may respond to its IP address while still failing vCenter communication because the hostname or reverse DNS record is incorrect.

Example failure pattern

The ESXi host was rebuilt with a new management IP, but vCenter still references the old address. Basic network testing appears inconsistent, and reconnect attempts fail.

Corrective action

Correct the DNS records and routing first. Avoid removing and re-adding the host until you understand whether the identity or address changed.

Common mistake

Changing `/etc/hosts` entries as a quick fix without documenting the change can create a second name-resolution problem later. Prefer correct, centrally managed DNS wherever possible.

Step 4: Check time synchronization and certificates

Large time differences can cause authentication and SSL/TLS failures between ESXi and vCenter.

Check:

- Current time on the ESXi host
- Current time on vCenter Server
- NTP configuration and reachability
- Certificate expiration dates
- Certificate or trust errors in vCenter events
- Whether either system was restored from an old backup or snapshot

Look for errors containing terms such as:

- `SSL`
- `certificate`
- `handshake`
- `trust`
- `authentication`
- `clock skew`

Why this matters

A network ping can succeed even when the vCenter-to-ESXi session cannot be established because certificate validation or time-based authentication fails.

Common mistake

Regenerating certificates before correcting time synchronization can cause further trust problems. Fix the clock and identify the exact certificate error first.

Step 5: Check the ESXi management agents

The two key ESXi agents involved in vCenter communication are:

- `hostd` - provides the main ESXi host management service.
- `vpxa` - enables communication between the ESXi host and vCenter.

Use the ESXi Host Client, ESXi Shell, or your approved management method to check their status. If an agent is stopped, unresponsive, or repeatedly failing, review logs before restarting it.

Safe recovery sequence

- Confirm that network connectivity is working.
- Check the status of `hostd` and `vpxa`.
- Review recent errors in their logs.
- Confirm no critical host operation is in progress.
- Restart the affected management agent according to your operational procedure.
- Allow time for the service to initialize.
- Attempt to reconnect the host in vCenter.
- Verify VM, datastore, network, HA, and DRS status.

Restarting management agents is different from rebooting the ESXi host. It is generally less disruptive to running virtual machines, but it can temporarily interrupt management operations and should still follow your change process.

Common mistake

Restarting all management services immediately without recording the original error removes useful diagnostic evidence. Capture the error and relevant log timestamps first.

Step 6: Review ESXi and vCenter logs

Review logs around the time the host disconnected.

Useful ESXi logs include:

- `hostd.log`
- `vpxa.log`
- `vmkernel.log`

Also review:

- vCenter tasks and events
- ESXi hardware health events
- Physical switch logs
- Firewall or ACL logs
- Backup and monitoring logs

Search for:

- `connection failed`
- `timeout`

- `agent unreachable`
- `no route`
- SSL
- `certificate`
- `authentication`
- `handshake`

Compare timestamps between vCenter and ESXi. If the first ESXi error appears before the vCenter alarm, the ESXi or network logs may reveal the original cause.

Example interpretation

- Repeated connection timeouts suggest network, firewall, or resource problems.
- SSL or certificate errors suggest time, identity, or trust issues.
- Agent startup failures suggest an ESXi management-service or system-resource problem.
- Storage or filesystem errors may indicate that the host cannot reliably write its management state.

Common mistake

Reading only the latest log line can be misleading. Examine the first error and the events immediately before it.

Step 7: Reconnect the host from vCenter

Once network, DNS, time, certificate, and management-agent checks are satisfactory:

- Select the affected host in vCenter.
- Start the **Reconnect** action.
- Enter valid ESXi administrator credentials if prompted.
- Review any certificate warning carefully.
- Wait for the task to complete.
- Confirm the host status changes to **Connected**.

After reconnection, validate:

- Host alarms
- Datastore accessibility
- VM power states
- VM network connectivity
- HA status
- DRS status
- vMotion availability

- Backup access
- Monitoring status

Common mistake

A successful reconnect does not automatically mean the incident is fully resolved. Check for the underlying cause and confirm that related services have recovered.

Step 8: If reconnect fails

Use the error message to select the next path.

Network error

Check VLAN assignment, switch ports, uplinks, routing, gateways, MTU settings where relevant, and firewall rules.

DNS error

Correct forward and reverse DNS records, then retry the connection after confirming resolution from both sides.

Authentication error

Verify the ESXi administrator account, password, lockout state, and any recent identity changes.

SSL or certificate error

Correct time synchronization, inspect certificate validity, and follow the approved certificate-management process.

Host resource or storage error

Check datastore capacity, system partitions, hardware health, and filesystem errors. Do not delete snapshots or files without confirming their role and ownership.

Host was rebuilt or restored

Confirm whether the existing host identity should be preserved, whether it has been added elsewhere, and whether the host configuration needs to be restored before attempting reconnection.

Step 9: Remove and re-add the host only as a last resort

Removing a host from vCenter can affect cluster membership, HA, DRS, networking, datastore presentation, and inventory relationships. Use this step only after documenting the cause and completing the necessary approvals.

Before removal:

- Back up the ESXi host configuration.
- Confirm datastore visibility.
- Document port groups and VMkernel networking.
- Check HA and DRS configuration.
- Confirm no critical vMotion, backup, or replication task is active.
- Confirm VM registration and power state.
- Record the host's inventory location and cluster membership.

After re-adding:

- Reapply or verify host configuration.
- Confirm networking and datastores.
- Verify HA, DRS, vMotion, monitoring, and backups.
- Review alarms and events.
- Document the final root cause and corrective action.

Step 10: Prevent recurrence

Implement the following controls:

- Reliable forward and reverse DNS
- Consistent NTP configuration
- Monitoring for `hostd` and `vpxa`
- Alerts for management-network failures
- Capacity alerts for datastores and ESXi system partitions
- Regular ESXi configuration backups
- Documented management VLANs, gateways, and uplinks
- Working out-of-band server access
- Change tracking for vCenter, DNS, firewalls, and switching
- Tested recovery procedures for host and vCenter failures

Final diagnostic order

When an ESXi host is disconnected from vCenter, use this sequence:

> ***Confirm workload impact*** → ***test network*** → ***verify DNS*** → ***check time and certificates*** → ***inspect*** `hostd` ***and*** `vpxa` → ***review logs*** → ***reconnect from vCenter*** → ***remove and re-add only if justified.***

This approach reduces unnecessary disruption while preserving the evidence needed to identify the root cause.

Quick reference checklist

- Confirm the physical host is powered on.
- Confirm whether production VMs are affected.
- Test vCenter-to-ESXi connectivity.
- Verify the management VMkernel interface.
- Check VLAN, uplinks, gateway, and firewall rules.
- Verify forward and reverse DNS.
- Check time synchronization and certificates.
- Inspect `hostd` and `vpxa`.
- Review `hostd.log`, `vpxa.log`, and `vmkernel.log`.
- Reconnect the host from vCenter.
- Validate HA, DRS, datastores, networking, backups, and monitoring.
- Document the root cause and preventive action.

VMware ESXi Host Disconnected from vCenter

Incident Troubleshooting Checklist

Use this runbook when an ESXi host appears as *Disconnected* or *Not Responding* in vCenter Server.

> ***Safety note:*** *Confirm the impact of every action in your environment and follow your change-control process. Do not reboot the host as a first response if production virtual machines are running.*

---

1. Record the incident

- ■ Date and time of the first alert: _____
- ■ ESXi host name: _____
- ■ ESXi management IP address: _____
- ■ vCenter Server name: _____
- ■ vCenter version: _____
- ■ ESXi version/build: _____
- ■ Cluster name: _____
- ■ Error shown in vCenter: _____
- ■ Recent changes, reboots, patches, DNS changes, or network work:

_____

_____

2. Confirm workload impact

- ■ Are the virtual machines still powered on?
- ■ Can users access the affected applications?
- ■ Are there active HA, DRS, vMotion, backup, or replication operations?
- ■ Is the host responding through the ESXi Host Client?
- ■ Is out-of-band management available through the server hardware console?
- ■ Has anyone already restarted the host or management services?

Current workload impact:

_____

3. Check host availability and management networking

- Confirm the physical host is powered on.
- Ping the ESXi management IP from an approved management system.
- Test connectivity from vCenter to the ESXi management IP.
- Confirm the management VLAN is available.
- Check the physical switch port and uplink status.
- Confirm the ESXi management VMkernel adapter is up.
- Verify the management IP, subnet mask, and default gateway.
- Check for duplicate IP addresses.
- Check firewall rules between vCenter and ESXi.
- Confirm required management ports are not blocked.

Optional ESXi checks

Run only when you have authorized console, SSH, or ESXi Shell access:

```
esxcli network ip interface ipv4 get
esxcli network nic list
esxcli network ip route ipv4 list
vmkping <vcenter-ip-address>
```

Network findings:

---

4. Verify DNS and hostname resolution

- Resolve the ESXi hostname from the vCenter environment.
- Resolve the ESXi FQDN from the vCenter environment.
- Perform reverse DNS lookup for the ESXi management IP.
- Confirm the ESXi hostname and FQDN have not changed.
- Confirm vCenter is using the correct ESXi name or IP.
- Check for stale or duplicate DNS records.
- Review recent DNS or domain-controller changes.

DNS results:

---

5. Check time synchronization and certificates

- Compare the ESXi system time with the vCenter Server time.
- Verify NTP is configured and reachable.
- Check whether the ESXi host certificate has expired.

- Check for SSL, certificate, or trust errors in vCenter.
- Confirm the host was not restored from an old snapshot or backup.
- Check whether vCenter or the ESXi host was recently replaced.

Time/certificate findings:

---

6. Check ESXi management agents

The main agents involved in vCenter communication are **hostd** and **vpxa**.

- Check whether `hostd` is running.
- Check whether `vpxa` is running.
- Review service errors before restarting anything.
- Confirm the host is not overloaded or out of system resources.
- Check whether a recent task is blocking management operations.
- Restart management agents only according to your operational procedure.
- Wait for the agents to initialize.
- Attempt to reconnect the host from vCenter.
- Confirm that running virtual machines remain healthy.

Management-agent findings:

---

7. Review logs

Review the logs around the time the disconnection began:

- `hostd.log`
- `vpxa.log`
- `vmkernel.log`
- vCenter Server task and event logs
- ESXi hardware health logs
- Network switch logs, if a network fault is suspected

Search for terms such as:

- `connection failed`
- `timeout`
- `SSL`

- `certificate`
- `handshake`
- `authentication`
- `no route`
- `agent unreachable`

Relevant log entries and timestamps:

_____

_____

8. Reconnect the host from vCenter

- Confirm basic network connectivity works.
- Select the affected host in vCenter.
- Start the **Reconnect** action.
- Provide valid ESXi administrator credentials if requested.
- Review any certificate warning carefully.
- Confirm the host returns to a connected state.
- Check datastores and paths.
- Check management and VMkernel networking.
- Check host alarms and vCenter events.
- Confirm virtual machines, HA, DRS, and vMotion status.
- Confirm backup and monitoring systems can see the host again.

Reconnect result:

- Successful
- Failed
- Partially restored

Error message:

_____

9. If reconnect fails, follow the matching path

Network failure

- Investigate VLAN, switch port, uplink, routing, gateway, or firewall issues.
- Confirm the management VMkernel adapter is using the expected network.

DNS failure

- Correct forward and reverse DNS records.
- Confirm hostname and FQDN consistency in vCenter and ESXi.

Service or agent failure

- Review `hostd` and `vpxa` logs.
- Check host resource usage and system partitions.
- Restart agents only after assessing operational risk.

Authentication failure

- Confirm the ESXi administrator account is correct.
- Check for account lockout or password expiration.
- Verify identity and access changes.

SSL or certificate failure

- Verify system time.
- Check certificate validity and trust relationships.
- Follow your approved certificate replacement procedure.

Storage or resource exhaustion

- Check datastore capacity.
- Check ESXi system partitions.
- Check logs for filesystem or hardware errors.
- Avoid deleting files or snapshots without validating their purpose.

10. Consider removing and re-adding the host only as a last resort

Before removing the host from vCenter:

- Confirm the reason is understood or documented.
- Confirm the effect on HA and DRS.
- Confirm the host configuration is backed up.
- Check datastore visibility and VM registration.
- Confirm networking and port groups are documented.
- Confirm no critical vMotion, backup, or replication task is active.
- Obtain the required change approval.

- Document the host’s inventory location and cluster membership.

11. Verify recovery

- Host status is **Connected** in vCenter.
- No new host connection alarms are present.
- Datastores are accessible.
- VM networks are operational.
- HA and DRS are healthy.
- vMotion is available if required.
- Monitoring has returned to normal.
- Backups can access the host.
- No unexpected VM power-state changes occurred.
- Incident timeline and root cause are documented.

12. Prevent a repeat incident

- Configure reliable DNS and reverse DNS.
- Configure and monitor NTP.
- Monitor `hostd` and `vpxa` health.
- Monitor ESXi system partitions and datastores.
- Back up ESXi host configurations.
- Document management VLANs, IPs, gateways, and uplinks.
- Maintain working out-of-band access.
- Alert on repeated vCenter-to-host communication failures.
- Record changes to vCenter, DNS, firewalls, and switching.

Root-cause summary

Most likely root cause:

_____

Evidence:

_____

Corrective action:

_____

Preventive action:

_____

Incident closed by: _____ ***Date:*** _____

Related TechRunbook resources

- VMware ESXi Host Disconnected from vCenter: Troubleshooting Runbook
- VMware vMotion Troubleshooting Checklist
- VMware vSphere HA Admission Control Troubleshooting
- VMware ESXi Time Synchronization and Clock Skew Guide
- VMware Datastore Full Recovery Runbook