CHECKLIST

# VMware vSphere Hardening Checklist: Reducing Attack Surface in Virtualization

A practical, vendor-neutral checklist for reducing vSphere attack surface by hardening management access, services, network exposure, logging, and operational workflows without disrupting production.

## VMware vSphere Hardening Checklist

Purpose: Reduce the attack surface of a vSphere environment while preserving production operations.

How to use this checklist:

- Review each section against your current environment.
- Mark items as Done, Needs work, or Not applicable.
- Capture exceptions with an owner, expiration date, and compensating control.
- Re-check the baseline after every major change.

---

## 1) Management access and identity

- [ ] Administrative access is limited to named user accounts; shared admin accounts are not used.
- [ ] Privileged access is separated from everyday user access.
- [ ] All administrative accounts are backed by a controlled identity source.
- [ ] Multi-factor authentication is enabled wherever supported and operationally feasible.

- [ ] Privileged roles are assigned using least-privilege principles.
- [ ] Default accounts have been disabled, renamed, or otherwise protected where supported.
- [ ] Emergency access accounts are documented, secured, and tested.
- [ ] Administrative access paths are logged and reviewed.
- [ ] Account lifecycle processes remove access promptly when staff change roles or leave.
- [ ] Service accounts used by automation, backup, or monitoring are separate from human accounts.

Notes:

- Document who owns each privileged account.
- Avoid using the same credentials for admin, automation, and vendor support access.

---

## 2) Management plane exposure

- [ ] vSphere management interfaces are reachable only from approved administrative networks.
- [ ] Management access is blocked from user VLANs and guest networks.
- [ ] Direct access from broad enterprise networks is restricted unless explicitly required.
- [ ] Jump hosts or administration zones are used where appropriate.
- [ ] Firewall rules for management access are narrowly scoped to required sources and destinations.
- [ ] Temporary access rules have expiration dates and are removed after use.
- [ ] Remote troubleshooting paths are documented and reviewed.
- [ ] Internet exposure of any management component has been eliminated.
- [ ] Network paths to hosts and management components are validated from an attacker?s point of view.
- [ ] Management access changes are included in change control.

Validation checks:

- [ ] Attempt to reach management interfaces from unauthorized segments and confirm access is denied.
- [ ] Confirm only approved jump hosts can access management services.

---

## 3) Host and service minimization

- [ ] Only required services are enabled on hosts and management components.
- [ ] Legacy or unused remote access methods are disabled.
- [ ] Unnecessary extensions, integrations, or plugins are removed or disabled.
- [ ] Services enabled for troubleshooting are disabled when the maintenance window ends.
- [ ] Backup, monitoring, and patching integrations are documented so they can be preserved during hardening.
- [ ] Any protocol that is not required for daily operations has been removed from the steady-state configuration.
- [ ] Default service settings have been reviewed for exposure.
- [ ] Configuration drift is monitored so disabled services do not reappear.

Before disabling anything, confirm:

- [ ] Which tools depend on the service.
- [ ] Whether a maintenance workflow requires it.
- [ ] Whether a vendor or backup process still uses it.

---

## 4) Network segmentation and lateral movement resistance

- [ ] Management, storage, vMotion, backup, and workload networks are separated according to design.
- [ ] Control-plane traffic is not mixed with general user traffic without a documented reason.

- [ ] Host-to-host and host-to-management traffic paths are limited to what is required.
- [ ] Administrative services are not exposed across unnecessary routed networks.
- [ ] Network ACLs or firewall rules prevent lateral movement into management components.
- [ ] Segmentation assumptions are tested after changes.
- [ ] Monitoring confirms that only expected systems can talk to management interfaces.

Good practice:

- Keep the management plane small, explicit, and auditable.
- Do not rely on ?security by obscurity? or hidden network paths.

---

## 5) Logging, alerting, and auditability

- [ ] Authentication events are logged centrally.
- [ ] Administrative actions are logged and retained according to policy.
- [ ] Failed logins, privilege changes, and service enablement events generate alerts.
- [ ] Logs are protected from tampering and unauthorized deletion.
- [ ] Time synchronization is consistent across hosts and management systems.
- [ ] Log retention is long enough to support investigation and change review.
- [ ] Security and operations teams know where to find audit logs.
- [ ] Alert thresholds are tuned to detect suspicious activity without excessive noise.

Review questions:

- [ ] Can you identify who accessed management systems last week?
- [ ] Can you see when a service was enabled or a rule was changed?
- [ ] Can you trace access from source system to action taken?

---

## 6) Backup, monitoring, and support workflows

- [ ] Backup appliances and monitoring systems use least-privilege credentials.
- [ ] Support workflows are documented and limited to approved routes.
- [ ] Vendor access, if needed, is controlled, time-bound, and audited.
- [ ] Recovery procedures do not require permanent broad access.
- [ ] Maintenance exceptions are documented and expire automatically or by review.
- [ ] Operational workflows are tested to ensure hardening did not break production tasks.
- [ ] The team knows how to perform critical operations without opening broad access.

Check for common hidden exposure:

- [ ] Old backup credentials still working somewhere.
- [ ] Monitoring systems with more access than they need.
- [ ] ?Temporary? firewall or firewall-like exceptions that became permanent.
- [ ] Support accounts that are active outside maintenance windows.

---

## 7) Configuration baseline and drift control

- [ ] A hardened baseline is documented for the environment.
- [ ] The baseline identifies required, conditional, and unnecessary exposures.
- [ ] Changes are compared against the baseline before deployment.
- [ ] Post-change validation confirms the attack surface did not expand.
- [ ] Configuration drift is checked on a recurring schedule.
- [ ] Exceptions are recorded with justification, owner, and review date.
- [ ] Hardening actions are reversible if production impact is discovered.
- [ ] The current state is versioned or otherwise tracked.

Suggested baseline categories:

- Identity and privilege
- Management network access
- Enabled services and protocols

- Logging and alerting
- Backup and support paths
- Exception handling

---

## 8) Quick validation test

Use this quick test after hardening changes:

- [ ] Can the management plane be reached from a non-administrative network?
- [ ] Are only approved admin paths able to connect?
- [ ] Are unnecessary services still disabled after reboot, patching, or maintenance?
- [ ] Do logs show expected administrative activity and access sources?
- [ ] Are privileged accounts minimized and individually owned?
- [ ] Are temporary exceptions removed on schedule?
- [ ] Do backup, monitoring, and recovery workflows still function?
- [ ] Has the team documented what changed and why?

If any answer is no or unclear, treat it as a hardening gap.

---

## 9) Exception record template

Use this template for any hardening exception:

- Exception ID: _____
- Date opened: _____
- Owner: _____
- System or service affected: _____
- Reason for exception: _____
- Risk accepted by: _____

- Compensating control: _____
- Expiration or review date: _____
- Status: _____
- Notes: _____

---

## 10) Final readiness check

Before declaring the environment hardened, confirm:

- [ ] The control plane is smaller than the threat model requires.
- [ ] Only necessary administrative paths remain.
- [ ] Remaining paths are protected by segmentation and least privilege.
- [ ] Logging and alerting are working.
- [ ] Operational workflows still function.
- [ ] Exceptions are documented and reviewed.
- [ ] The baseline has been recorded for future drift detection.

---

## Outcome

A hardened vSphere environment does not eliminate risk, but it reduces the number of viable attack paths and makes the remaining ones easier to defend, monitor, and audit.

Related reading:

- Hardening VMware vSphere ESXi against unauthorized access
- VM encryption in vSphere: how to secure sensitive workloads