TEMPLATE

ESXi Hardening Validation Template

A practical one-page template for documenting and verifying VMware ESXi hardening controls against unauthorized access before production use.

ESXi Hardening Validation Template

Use this template to document the current state of an ESXi host or cluster, confirm required controls, and record remediation actions before production use.

---

1) Environment details

- Organization / team: _____
- Cluster / host name(s): _____
- vCenter or management domain: _____
- Environment type: ? Lab ? Dev ? Test ? Prod
- Date reviewed: _____
- Reviewer: _____

---

2) Management access paths

Item	Status	Notes

Management interface reachable only from approved administrative networks	? Pass ? Fail ? N/A	_____
Direct access from user or general-purpose subnets blocked	? Pass ? Fail ? N/A	_____
Jump host / bastion required for admin access	? Pass ? Fail ? N/A	_____
Unneeded remote access paths removed	? Pass ? Fail ? N/A	_____

---

3) Authentication and privilege controls

Item	Status	Notes
Administrative access uses named accounts or controlled groups	? Pass ? Fail ? N/A	_____
Shared admin credentials not used for routine operations	? Pass ? Fail ? N/A	_____
Local root account restricted to break-glass or recovery use	? Pass ? Fail ? N/A	_____
Break-glass access documented, stored securely, and monitored	? Pass ? Fail ? N/A	_____
Role assignments reviewed for least privilege	? Pass ? Fail ? N/A	_____

---

4) Service and shell exposure

Item	Status	Notes
SSH disabled when not actively required	? Pass ? Fail ? N/A	_____
ESXi Shell disabled when not actively required	? Pass ? Fail ? N/A	_____
Remote troubleshooting features time-bound if enabled	? Pass ? Fail ? N/A	_____

Only required management services enabled	? Pass ? Fail ? N/A	_____
Temporary access changes tracked and removed after use	? Pass ? Fail ? N/A	_____

---

5) Logging, auditability, and time sync

Item	Status	Notes
Host logs forwarded off-host to a central destination	? Pass ? Fail ? N/A	_____
Log retention supports review and incident investigation	? Pass ? Fail ? N/A	_____
Authentication events are visible in logs	? Pass ? Fail ? N/A	_____
Configuration changes are auditable	? Pass ? Fail ? N/A	_____
Time synchronization is working correctly	? Pass ? Fail ? N/A	_____

---

6) Patch, lifecycle, and drift control

Item	Status	Notes
Patch management process defined and current	? Pass ? Fail ? N/A	_____
Hardening baseline checked after patching or upgrades	? Pass ? Fail ? N/A	_____
Host replacement / remediation process includes revalidation	? Pass ? Fail ? N/A	_____
Unauthorized changes are detected through review or automation	? Pass ? Fail ? N/A	_____

---

7) Quick validation checks

Mark each item before approving the host for production use.

- ? Management access is limited to approved administrative networks.
- ? SSH and shell access are disabled unless actively needed.
- ? Local accounts are limited and periodically reviewed.
- ? Administrative actions are attributable to named identities.
- ? Logs are forwarded off-host and retained for investigation.
- ? Hardening settings are revalidated after patching or lifecycle changes.

---

8) Findings and remediation

Findings

- Finding: _____
- Risk: _____
- Owner: _____
- Target date: _____
- Status: ? Open ? In progress ? Closed
- Finding: _____
- Risk: _____
- Owner: _____
- Target date: _____
- Status: ? Open ? In progress ? Closed
- Finding: _____

- Risk: _____
- Owner: _____
- Target date: _____
- Status: ? Open ? In progress ? Closed

---

9) Approval

- Overall result: ? Approved ? Approved with findings ? Not approved
- Approver: _____
- Approval date: _____
- Notes: _____

---

10) Minimal acceptance criteria

A host should not be treated as production-ready until all of the following are true:

- Management access is restricted to known administrative paths.
- Routine admin work does not depend on shared root access.
- Unnecessary services and shells are disabled.
- Logs are centralized and reviewable.
- Time is synchronized.
- Hardening settings are included in patch and drift validation.

References for internal use

- Management network design

- Access review records
- Patch and lifecycle procedures
- Logging and monitoring standards
- Break-glass credential procedure