TEMPLATE

VMware ESXi Hardening Checklist

A practical, vendor-neutral checklist for verifying ESXi management access, secure boot, lockdown behavior, logging, patch readiness, and production validation before deployment.

VMware ESXi Hardening Checklist

Use this checklist to verify that an ESXi host is ready for production use. It is designed for build, change control, and audit review.

Instructions:

- Check each item only after you have verified it in your environment.
- Record the owner, method of verification, and evidence.
- Mark any exceptions and the compensating control used.

---

1) Administrative access

Check	Yes/No	Evidence / Notes
Administrative access is limited to approved management networks, jump hosts, or bastion systems		
Only approved administrative identities can access the host management plane		
Shared administrative accounts are eliminated or explicitly justified		
Privileged local accounts are documented and reviewed		
Access paths not required for normal operations are disabled or blocked		

2) Authentication and authorization

Check	Yes/No	Evidence / Notes
Role-based access follows least privilege		
Directory-backed identities or centralized role mapping are configured as intended		
Group membership for privileged roles is reviewed and approved		
Break-glass or emergency access is documented and controlled		
Privileged access is logged and reviewable		

3) Secure boot and host trust

Check	Yes/No	Evidence / Notes
Hardware supports secure boot for the host		
Secure boot is enabled in firmware/boot settings		
Host reports the expected trusted boot state after restart		
Any firmware or boot-chain change was validated before production use		
Unexpected boot-state changes are treated as security events		

4) Lockdown and direct console access

Check	Yes/No	Evidence / Notes
Lockdown behavior matches the operational model used by the environment		

Direct local management is restricted where appropriate		
Recovery access paths are documented and tested		
Console-only emergency procedures are known to administrators		
The team has validated how to regain access during a management-plane outage		

5) Services, interfaces, and attack surface

Check	Yes/No	Evidence / Notes
Unused services are disabled		
Shell access is disabled unless required for a documented purpose		
Auxiliary management interfaces are restricted or disabled		
Only services required for operations and recovery remain enabled		
Any exception has a documented business and security rationale		

6) Logging, monitoring, and time synchronization

Check	Yes/No	Evidence / Notes
Host logs are forwarded off-host or retained in a protected logging system		
Access events are included in monitoring and alerting scope		
Configuration changes are logged and reviewable		
Security-relevant events are retained for the required period		
Time synchronization is configured and operating correctly		

Log timestamps can be trusted for incident investigation and correlation		

7) Patch and maintenance readiness

Check	Yes/No	Evidence / Notes
A patching process exists for the host and associated firmware		
Pre-change checks are defined and followed		
Maintenance mode or equivalent operational procedures are tested		
A rollback or fallback plan exists for failed maintenance		
Post-change validation is required after patching or firmware updates		
Patch and firmware status are current enough for the environment?s policy		

8) Configuration backup and drift detection

Check	Yes/No	Evidence / Notes
Approved host configuration is backed up or exported		
Baseline configuration is available for comparison		
Drift detection exists, manual or automated		
Configuration changes can be attributed to a change request or operator		
Recovery from configuration loss has been tested		

9) Certificates and trust relationships

Check	Yes/No	Evidence / Notes
Host certificate state is understood and documented		
Certificate changes are reviewed instead of ignored		
Administrators know what certificate warnings are expected		
Unexpected trust changes trigger validation		
Certificate lifecycle ownership is assigned		

10) Recovery and production validation

Check	Yes/No	Evidence / Notes
Lost access recovery steps are documented		
Failed update recovery steps are documented		
Boot failure recovery steps are documented		
The host has been validated in a non-production or controlled environment		
The final production acceptance review is complete		
Owners have signed off that the host is ready for production use		

Acceptance summary

Item	Status	Notes
Management plane access restricted		

Secure boot validated	
Lockdown behavior confirmed	
Least privilege reviewed	
Unused services disabled	
Logging and time sync verified	
Patch readiness confirmed	
Configuration backup/drift controls in place	
Certificates reviewed	
Recovery paths tested	

Final decision

- Approved for production: _____
- Approved with exceptions: _____
- Not approved: _____

Exceptions and compensating controls

Exception	Risk Owner	Compensating Control	Review Date

Sign-off

Name	Role	Signature / Approval	Date

Quick operational reminders

- Do not assume a control is present because it exists in the build template.
- Verify the effective state on the host.
- Test recovery before production use.
- Treat drift, unexpected trust changes, and certificate anomalies as review items.
- Re-run this checklist after major patching, firmware changes, or access model changes.