TEMPLATE

Azure VM Hardening Validation Checklist Template

A practical, vendor-neutral checklist template for validating Azure virtual machine hardening before production use. Covers identity, network exposure, OS configuration, patching, logging, and operational verification.

Azure VM Hardening Validation Checklist Template

Use this template to validate that an Azure virtual machine is hardened without breaking required operations. Complete each section before production approval and retain evidence for audit and change control.

---

1) Environment details

Workload name: _____ Application owner: _____
System owner: _____ Environment: ? Dev ? Test ? Stage ? Prod VM name(s): _____ OS: _____
Hardening baseline version/date: _____ Review date: _____

---

2) Scope and change summary

What changed? _____
_____

Why was the change made? _____

_____

Planned maintenance window: _____ Rollback plan location: _____
Approver: _____

---

3) Identity and administrative access

Checklist

- [ ] Only required administrative accounts exist
- [ ] Shared admin accounts are removed or formally justified
- [ ] Stale, unused, or orphaned accounts are removed or disabled
- [ ] Local administrator membership is reviewed and minimized
- [ ] Routine operations do not require standing admin access
- [ ] Elevated access is time-bound or approval-based where possible
- [ ] Break-glass access is documented, protected, and monitored
- [ ] Service accounts are documented with owners and purpose
- [ ] Automation accounts have only required permissions
- [ ] Account review evidence is recorded

Notes / evidence

_____

_____

---

4) Network exposure

Checklist

- [ ] Inbound access is limited to required ports only
- [ ] Source IP ranges are restricted to approved management or application sources
- [ ] Public IP exposure is justified and documented
- [ ] Administration is not open to the public internet unless explicitly approved
- [ ] Network security rules and host firewall rules are aligned
- [ ] East-west traffic is restricted to required tiers and systems
- [ ] Unused management ports are closed
- [ ] Custom admin interfaces are not exposed unnecessarily
- [ ] Network segmentation supports the workload design
- [ ] Connectivity paths were tested after changes

Required ports and sources

Port / Protocol	Purpose	Allowed Source(s)	Approved?
			?
			?
			?

Notes / evidence

---

5) Operating system hardening

Checklist

- [ ] Unneeded services are disabled
- [ ] Unused remote access methods are disabled
- [ ] Local firewall rules are restrictive by default
- [ ] Secure authentication settings are enforced where feasible
- [ ] Legacy components are removed or disabled
- [ ] Diagnostic tools and temporary setup features are reviewed for removal
- [ ] File and registry permission changes are intentional and documented
- [ ] Baseline settings match the approved hardening standard
- [ ] OS configuration drift is monitored
- [ ] Required management features remain functional

Notes / evidence

---

6) Patch and image hygiene

Checklist

- [ ] OS patch source is defined
- [ ] Maintenance window is documented
- [ ] Rollback method is defined and tested where practical
- [ ] Restart behavior is understood and approved
- [ ] Latest security updates are installed or scheduled
- [ ] Package/application dependencies are reviewed
- [ ] Base image or golden image is current
- [ ] Image is treated as a controlled artifact
- [ ] Reused images are reviewed before deployment
- [ ] Patch compliance reporting is available

Patch details

Patch source: _____ Next scheduled window: _____
Rollback owner: _____

Notes / evidence

_____

_____

---

7) Agents, extensions, and tooling

Checklist

- [ ] Only approved agents and extensions are installed
- [ ] Each agent has a documented purpose
- [ ] Agent permissions are reviewed and minimized
- [ ] Agent network and dependency requirements are understood
- [ ] Disabled agents are tracked and re-enabled or removed
- [ ] Monitoring agent health is visible
- [ ] Backup agent status is visible
- [ ] Configuration management tooling is current
- [ ] Unused remote management tools are removed
- [ ] Third-party tools were reviewed for necessity

Approved agents / extensions

Name	Purpose	Owner	Required?
			?
			?
			?

Notes / evidence

---

8) Logging and monitoring

Checklist

- [ ] Failed logons are logged and reviewed
- [ ] Configuration changes are logged
- [ ] Service start/stop events are captured where feasible
- [ ] Security logs are forwarded to a central system
- [ ] Alerts exist for unexpected exposure or policy drift
- [ ] Monitoring covers critical services and ports
- [ ] Log retention meets operational and audit requirements
- [ ] Time synchronization is enabled and consistent
- [ ] Monitoring is tested after hardening changes
- [ ] Visibility remains sufficient for incident response

Notes / evidence

_____

_____

---

9) Recovery and operational readiness

Checklist

- [ ] Backup status is verified
- [ ] Restore procedure is documented
- [ ] Recovery point/objective expectations are known
- [ ] Administration path remains available for emergencies
- [ ] Required support access is documented
- [ ] Health checks succeed after hardening changes
- [ ] Application owner confirms workload functionality
- [ ] OS login access was validated for approved users
- [ ] Change did not block patching or maintenance workflows
- [ ] Rollback criteria are defined

Notes / evidence

---

10) Verification from an attacker’s view

Perform a final validation as if you were testing the machine from an unauthorized perspective.

Checklist

- [ ] Unapproved inbound ports are not reachable
- [ ] Administrative interfaces are not exposed broadly
- [ ] Default or unnecessary accounts cannot be used
- [ ] Privileged access is limited and reviewed

- [ ] Unexpected services are not listening
- [ ] Network paths are not broader than intended
- [ ] Monitoring detects failed access attempts
- [ ] The host behaves as expected after reboot
- [ ] The workload still meets business requirements
- [ ] Findings are recorded and remediated

Validation results

Tools/tests used: _____ Unexpected exposure found? ? No ? Yes If yes, describe: _____

_____

---

11) Approval decision

Go-live decision

- [ ] Approved for production
- [ ] Approved with conditions
- [ ] Not approved

Conditions / follow-up actions

_____

_____

_____

Security reviewer: _____ Operations reviewer: _____
Application owner: _____ Date: _____

---

12) Short hardening summary

A secure VM should expose only the minimum necessary services, ports, accounts, and privileges while remaining supportable for administration, patching, recovery, and auditability. If each control can be explained and verified before production, the hardening baseline is likely sound.

Optional change log

Date	Change	Reason	Completed by