CHECKLIST

VMware ESXi Patch Management and Maintenance Mode Checklist

A practical checklist for preparing, patching, and validating ESXi hosts so maintenance mode transitions are safe, workloads evacuate cleanly, and hosts return to production without surprises.

VMware ESXi Patch Management and Maintenance Mode Checklist

Use this checklist to plan, execute, and validate ESXi host patching with maintenance mode as a control point for workload safety.

---

1) Scope and change preparation

- [ ] Confirm the host(s) in scope, maintenance window, and required change approval.
- [ ] Record current ESXi version, build number, vendor image profile, and patch baseline.
- [ ] Confirm the rollback plan, including restoration method and decision point for aborting the change.
- [ ] Verify cluster membership and whether the host participates in DRS, HA, vSAN, or other cluster services.
- [ ] Identify any dependencies that could affect evacuation:
- [ ] Shared storage accessibility
- [ ] vMotion readiness
- [ ] Distributed switch or port group dependency

- [ ] Host profile or compliance requirements
- [ ] Security baseline or hardening requirements

---

2) Cluster readiness check

- [ ] Confirm the cluster has enough spare capacity to absorb the host workloads.
- [ ] Review CPU headroom, memory headroom, and reservation pressure.
- [ ] Validate admission control impact if HA is enabled.
- [ ] Check for anti-affinity rules, affinity rules, or pinned workloads.
- [ ] Review active alerts, alarms, and recent task failures.
- [ ] Confirm no other host is already in maintenance mode unless the cluster can safely tolerate it.

---

3) Workload evacuation readiness

- [ ] Verify each VM on the host can move or be safely powered down.
- [ ] Identify VMs with any of the following constraints:
- [ ] CPU compatibility concerns
- [ ] Device pass-through or PCI device attachment
- [ ] Connected ISO or removable media dependency
- [ ] Storage policy limitations
- [ ] Snapshot chains or snapshot sprawl
- [ ] Application-level affinity requirements
- [ ] Confirm there are no management appliances, infrastructure services, or special-purpose workloads that must stay on the host.
- [ ] Ensure change owners for critical VMs are aware of the maintenance window.

---

4) Storage and network checks

- [ ] Confirm all required datastores are accessible from the remaining hosts.
- [ ] Validate storage policy compliance for workloads being moved.
- [ ] Confirm datastore latency is within normal operating range.
- [ ] Verify distributed switch, uplinks, and port groups are healthy.
- [ ] Confirm network configuration is consistent across hosts that will receive migrated VMs.
- [ ] Check for NIC, VLAN, or uplink issues that could affect post-migration connectivity.

---

5) Enter maintenance mode

- [ ] Start the evacuation process using the approved method.
- [ ] Confirm whether workloads are evacuated automatically, partially assisted, or require manual intervention.
- [ ] Watch for any VMs that remain pinned to the host.
- [ ] If maintenance mode fails, stop and identify the blocker before forcing the change.
- [ ] Document the reason if the host cannot enter maintenance mode cleanly.

If maintenance mode does not complete, classify the blocker:

- [ ] Mobility issue
- [ ] Capacity issue
- [ ] Storage issue
- [ ] Network issue

- [ ] Process issue
- [ ] Task or agent issue

---

6) Patch execution

- [ ] Confirm the patch source or image baseline is approved.
- [ ] Verify the patch matches the intended ESXi version and vendor support matrix.
- [ ] Apply the update using the approved process.
- [ ] Record the patch time, build number, and any warnings or errors.
- [ ] Reboot the host if required by the update.
- [ ] Confirm the host reconnects successfully after reboot.

---

7) Post-patch validation

- [ ] Confirm the host version and build match the intended target.
- [ ] Verify the host is healthy and responsive.
- [ ] Check for new alarms, errors, or degraded services.
- [ ] Confirm management agents are running normally.
- [ ] Validate network connectivity, vmkernel services, and storage paths.
- [ ] Check datastore visibility and path stability.
- [ ] Confirm the host is compliant with baseline, image, or policy expectations.

---

8) Exit maintenance mode safely

- [ ] Confirm no unresolved alarms or critical service issues remain.

- [ ] Verify the host is ready to accept workloads.
- [ ] Exit maintenance mode only after health checks pass.
- [ ] Confirm at least one test workload can be powered on or migrated if your process requires validation.
- [ ] Check that VM placement behaves as expected after the host returns to service.

---

9) Closeout and documentation

- [ ] Record the final host state and post-patch build number.
- [ ] Note any exceptions, manual interventions, or delayed workloads.
- [ ] Capture reasons for any failed maintenance mode attempt.
- [ ] Document corrective actions needed before the next maintenance window.
- [ ] Update the change record with results and any follow-up tasks.

Quick pass/fail checklist

Use this short version when you need a rapid go/no-go decision.

- [ ] Cluster has enough spare capacity.
- [ ] VM evacuation is expected to complete cleanly.
- [ ] Storage access is consistent on remaining hosts.
- [ ] Network configuration is stable and portable.
- [ ] No pinned, special, or exception workloads block evacuation.
- [ ] Host enters maintenance mode without manual workarounds.
- [ ] Patch applies successfully and host reboots cleanly.
- [ ] Host passes health, storage, network, and compliance checks.
- [ ] Host exits maintenance mode only after validation is complete.

Operator reminder

Maintenance mode is not just a prerequisite for patching. It is proof that the cluster can safely absorb the host?s workloads and return the host to production without hidden risk.

If a host will not enter maintenance mode, treat that as a finding to investigate, not a step to bypass.