CHECKLIST

Shielded VM Readiness Checklist for Hyper-V Workloads

A practical checklist to assess whether a Hyper-V workload is ready for Shielded VM protection, including prerequisites, operational impacts, recovery planning, and production rollout checks.

Shielded VM Readiness Checklist for Hyper-V Workloads

Use this checklist to decide whether Shielded VM features are a good fit for a Hyper-V workload and to verify that the operational model is ready before production rollout.

---

1) Workload fit and threat model

- [ ] The workload contains sensitive data, secrets, privileged code, or regulated information.
- [ ] The threat model includes host-level abuse, compromised fabric administration, or offline disk access.
- [ ] The main security concern is protection from the virtualization layer, not only network exposure.
- [ ] The business impact of unauthorized host-side inspection has been assessed.
- [ ] The workload is important enough to justify added operational complexity.

Not a strong fit if:

- [ ] The VM is routine or low-risk and does not store sensitive content.

- [ ] The primary problem is only guest OS hardening or network isolation.
- [ ] Operators frequently depend on ad hoc host-side troubleshooting.
- [ ] The environment cannot support stricter change control and policy enforcement.

---

2) Platform and trust prerequisites

- [ ] The Hyper-V environment supports the required Shielded VM capability.
- [ ] A trusted or guarded fabric model is available and documented.
- [ ] Attestation or equivalent trust validation is in place for host start decisions.
- [ ] Required key management or protection services are available and secured.
- [ ] The guest OS and VM configuration are supported for protected operation.
- [ ] Boot and security settings required by the workload are compatible with the protection model.
- [ ] Infrastructure ownership and responsibilities are clearly separated.

Validate before rollout:

- [ ] Confirm what state the host must prove before the VM can start.
- [ ] Confirm who can approve or modify fabric trust settings.
- [ ] Confirm where recovery keys, policies, and certificates are stored and who can access them.
- [ ] Confirm how trust failures are detected and escalated.

---

3) Security boundary and access control

- [ ] Only approved operators can manage protected VM workflows.

- [ ] Fabric administrators do not have unrestricted access to guest secrets.
- [ ] Administrative roles are separated between virtualization, security, and application teams.
- [ ] Access to management tools is limited and audited.
- [ ] The process for making host or fabric changes is documented and controlled.
- [ ] The organization accepts that some host-level convenience will be intentionally removed.

Check for overexposure:

- [ ] No routine process depends on attaching guest disks directly from the host.
- [ ] No routine process depends on inspecting sensitive guest contents from the hypervisor.
- [ ] No undocumented backdoors exist for bypassing the protection model.

---

4) Guest hardening and baseline controls

- [ ] Guest patching and maintenance are still part of the operating standard.
- [ ] Secure Boot is enabled where appropriate and validated as part of the VM baseline.
- [ ] Guest credentials, service accounts, and secrets are protected inside the VM.
- [ ] Logging, monitoring, and alerting are available from inside the guest.
- [ ] Network segmentation is still enforced for the workload.
- [ ] Least privilege applies inside the guest as well as in the fabric.
- [ ] The team understands that Shielded VM features do not replace guest hardening.

Reminder:

- [ ] Review whether network segmentation, VLAN design, and guest hardening are already sufficient for lower-risk workloads.

- [ ] Use Shielded VM protection only when the workload truly needs stronger protection against the host itself.

---

5) Operational workflow readiness

- [ ] The team knows how the VM will be provisioned, started, paused, and recovered.
- [ ] Standard maintenance steps are documented for protected guests.
- [ ] Troubleshooting workflows rely on guest telemetry rather than host-side inspection.
- [ ] Change control is in place for fabric or policy updates that might affect VM startup.
- [ ] The operations team understands that ad hoc disk attachment may be blocked or restricted.
- [ ] The incident response process includes protected VM scenarios.
- [ ] The team knows what happens if attestation or trust checks fail.

Questions to answer:

- [ ] Who approves changes that affect guarded fabric trust?
- [ ] Who is allowed to troubleshoot the VM if the host cannot be used for inspection?
- [ ] What is the fallback path if the VM will not start due to a trust failure?
- [ ] How are support events handled without weakening the protection boundary?

---

6) Backup, restore, and disaster recovery

- [ ] Backups are designed for protected guests, not just ordinary storage copies.
- [ ] Restore procedures have been tested end to end.
- [ ] The backup solution does not require casual host-side exposure of protected disks.

- [ ] Recovery keys, policies, and related dependencies are included in DR planning.
- [ ] The team understands how to restore the VM without breaking the protection model.
- [ ] Backup verification includes a test restore, not only a successful backup job.
- [ ] RPO and RTO expectations are realistic for a protected workload.

Test before production:

- [ ] Can the VM be restored to a trusted environment and start successfully?
- [ ] Can the team prove the restore without exposing protected contents?
- [ ] Can the workload be recovered after a fabric or attestation issue?
- [ ] Is the DR site prepared for the same trust requirements as production?

---

7) Monitoring, audit, and evidence

- [ ] Audit logging covers administrative actions on the fabric and protected VM lifecycle.
- [ ] Security events from the guest are forwarded to a central logging platform.
- [ ] The team can tell whether a VM failed because of policy, trust, or configuration issues.
- [ ] Monitoring includes both availability and security-relevant signals.
- [ ] Evidence for compliance or internal review can be collected without breaking the model.
- [ ] Alerts exist for unexpected management changes or failed attestation events.

Minimum evidence to keep:

- [ ] VM protection scope and approval record.
- [ ] Attestation or trust validation results.

- [ ] Backup and restore test results.
- [ ] Incident response and exception procedures.
- [ ] Ownership and role separation documentation.

---

8) Production readiness check

Before enabling production use, confirm all of the following:

- [ ] The workload clearly needs protection against host-side access.
- [ ] The platform prerequisites are met and tested.
- [ ] The security and operations teams agree on ownership boundaries.
- [ ] Recovery, backup, and incident handling have been tested.
- [ ] The support team understands the reduced host visibility model.
- [ ] The business accepts the trade-off between stronger protection and less administrative convenience.
- [ ] A pilot deployment succeeded with a noncritical sensitive workload.
- [ ] There is a documented rollback or exception path if needed.

---

9) Go / no-go decision

Go if:

- [ ] The workload is sensitive enough to justify the control.
- [ ] The environment can support guarded or attested operations reliably.
- [ ] The team has tested backup, restore, and troubleshooting workflows.
- [ ] Roles, responsibilities, and audit requirements are clear.

No-go if:

- [ ] Operators still need frequent host-level inspection of the VM.
- [ ] The infrastructure cannot reliably prove trust before startup.
- [ ] Recovery has not been tested.
- [ ] The added complexity outweighs the security benefit.

---

10) Final sign-off notes

- Workload name: _____
- Owner: _____
- Environment: _____
- Risk justification: _____
- Approved by: _____
- Date: _____

Summary statement

- [ ] Shielded VM protection is justified for this workload.
- [ ] The operational model can support the protection boundary.
- [ ] Production rollout may proceed.

Quick reminder

Shielded VM features are most valuable when the host and fabric are part of the threat model. They are not a substitute for guest hardening, network segmentation, or good operational discipline. They are a stronger boundary for workloads that must stay protected from infrastructure-level access.