CHECKLIST

Checklist: Securing Azure Virtual Machines with Just-In-Time Access

A practical checklist for evaluating, validating, and rolling out Just-In-Time access for Azure virtual machines before production use.

Checklist: Securing Azure Virtual Machines with Just-In-Time Access

Use this checklist to validate whether Just-In-Time (JIT) access is a good fit for your Azure virtual machine environment and to confirm the control is ready for production use.

---

1) Confirm the use case

- [ ] The VM needs administrative access only occasionally, not continuously.
- [ ] Exposing SSH, RDP, or similar management ports all the time is not justified.
- [ ] Reducing inbound exposure is an explicit security objective.
- [ ] The team understands that JIT access is a reduction control, not a replacement for identity, patching, or segmentation.
- [ ] The VM is a good candidate for temporary, auditable access windows.

2) Identify the exact administrative access needed

- [ ] The required management port(s) are documented.
- [ ] Only necessary ports are included in the JIT policy.

- [ ] Non-administrative ports are excluded from the JIT scope.
- [ ] The expected access method is clear: SSH, RDP, or another approved service.
- [ ] The VM owner and operators agree on which access paths are acceptable.

3) Define the policy boundaries

- [ ] The allowed port list is as narrow as possible.
- [ ] The access duration is short enough for the workflow.
- [ ] Source restrictions are defined for specific IPs or trusted ranges where feasible.
- [ ] The policy aligns with incident response and maintenance procedures.
- [ ] The approval process is documented and understood by operators.
- [ ] The policy does not rely on overly broad or permanent exceptions.

4) Validate identity and authorization controls

- [ ] Users requesting access are authenticated through strong identity controls.
- [ ] Least privilege is applied to who can request or approve access.
- [ ] Approval rights are limited to appropriate roles.
- [ ] Emergency access procedures are defined and tested.
- [ ] There is no shared or uncontrolled administrative access path.

5) Check network and routing assumptions

- [ ] The VM?s network path is understood before enabling JIT.
- [ ] Any peering, routing, firewall, or segmentation rules are reviewed.
- [ ] Temporary access will not unintentionally bypass other controls.
- [ ] The source IP used during access will match the policy expectations.
- [ ] Connected network designs have been considered before production rollout.

6) Verify logging and auditability

- [ ] Access requests are logged.
- [ ] Approvals or denials are logged.
- [ ] Connection attempts are logged.
- [ ] The time access was granted and revoked is recorded.
- [ ] Logs are retained according to operational and compliance requirements.
- [ ] Logs can be reviewed during incident response or audits.

7) Test the control before production

- [ ] Confirm the management port is closed before a request is made.
- [ ] Request access for a valid test window.
- [ ] Verify the port opens only during the approved time period.
- [ ] Verify the source restriction is enforced.
- [ ] Connect successfully during the window using the approved method.
- [ ] Confirm the port closes again when the window expires.
- [ ] Repeat the test with at least one realistic operational scenario.

8) Validate operational workflows

- [ ] Maintenance procedures account for request and approval time.
- [ ] Incident response procedures account for urgent but controlled access.
- [ ] Operators know how to request access quickly when needed.
- [ ] Escalation paths are defined if approval is delayed.
- [ ] The workflow does not create unsafe workarounds.
- [ ] The team has tested how JIT behaves under time pressure.

9) Review security trade-offs

- [ ] The added process overhead is acceptable to the operations team.
- [ ] The policy is not so restrictive that users bypass it.
- [ ] The policy is not so broad that it weakens the security benefit.
- [ ] The environment still uses patching, hardening, and segmentation as required controls.
- [ ] The access model does not assume JIT alone will stop compromise.

10) Decide whether it is production ready

- [ ] The technical workflow works as expected.
- [ ] The business workflow fits maintenance and incident operations.
- [ ] The approval and audit trail satisfy security requirements.
- [ ] The logging is sufficient to explain who accessed what, when, and from where.
- [ ] The team understands the limitations and trade-offs.
- [ ] The rollout has an owner and a review date.

Go-live checklist

Before enabling JIT in production, confirm the following:

- [ ] The policy is limited to the required administrative ports.
- [ ] The request duration is short and justified.
- [ ] Source restrictions are as narrow as practical.
- [ ] Logging is enabled and reviewed.
- [ ] Operators and approvers know the workflow.
- [ ] Fallback procedures exist if access is delayed.

- [ ] The team has verified that access closes automatically after the window.

Common warning signs

Pause the rollout if any of these are true:

- [ ] Administrative ports still need to remain open most of the time.
- [ ] Source restrictions cannot be enforced reliably.
- [ ] Requests and approvals are not logged.
- [ ] Operators plan to bypass the process for convenience.
- [ ] The team has not tested the access expiration behavior.
- [ ] The VM depends on continuous direct access to function normally.

Quick decision rule

- Use JIT access when a VM can operate with administrative ports closed most of the time.
- Reconsider the access model when constant direct access is part of normal operations.

Final validation questions

- [ ] Can we prove the port is closed before access is requested?
- [ ] Can we prove it opens only for the approved window?
- [ ] Can we prove it closes again automatically?
- [ ] Can we explain who requested access, who approved it, and why?
- [ ] Can we support this workflow during real incidents without unsafe shortcuts?

If the answer to all of these is yes, the environment is likely ready for production use of Just-In-Time access.