CHECKLIST

Hyper-V VM Network Segmentation and VLAN Configuration Checklist

A practical, vendor-neutral checklist for planning, validating, and documenting Hyper-V VLAN segmentation before production rollout.

Hyper-V VM Network Segmentation and VLAN Configuration Checklist

Use this checklist to verify that Hyper-V VLAN design, virtual switch placement, and guest configuration align with your intended security and routing boundaries before production rollout.

1) Define the segmentation goals

- [ ] Identify the traffic classes that must be separated (management, production, backup, storage, tenant, lab, security tooling, etc.).
- [ ] Define the security purpose for each segment: isolation, routing control, bandwidth control, compliance, or troubleshooting.
- [ ] Document which systems must communicate across VLAN boundaries.
- [ ] Confirm whether the goal is simple separation or a stricter security zone model.
- [ ] Decide whether any workload actually needs trunked VLAN access in the guest OS.

2) Map VLAN ownership and boundaries

- [ ] Assign a VLAN ID or equivalent network segment identifier to each traffic class.

- [ ] Confirm where VLAN tagging is expected to occur:
- [ ] Physical switch port
- [ ] Hyper-V host vNIC
- [ ] Guest virtual NIC
- [ ] Guest OS/network appliance
- [ ] Verify that only one layer is responsible for tagging unless a specific design requires more.
- [ ] Record which networks are allowed on the physical uplink.
- [ ] Remove any VLANs from the uplink that are not explicitly required.

3) Validate physical switch and uplink configuration

- [ ] Confirm the host uplink port mode matches the design.
- [ ] Trunk if the host carries multiple VLANs
- [ ] Access if the host carries only one untagged network
- [ ] Confirm the allowed VLAN list is restricted to approved segments.
- [ ] Confirm native/untagged VLAN behavior is intentional and documented.
- [ ] Check for VLAN mismatch between the physical switch and the Hyper-V host.
- [ ] Confirm link speed, duplex, and redundancy settings are appropriate for the workload.

4) Validate Hyper-V virtual switch design

- [ ] Confirm the correct virtual switch type is being used for each workload.
- [ ] Verify host vNICs are created only for the roles they support.
- [ ] Separate management traffic from guest workload traffic wherever possible.
- [ ] Confirm live migration, backup, storage, and management traffic are not unintentionally sharing the same path.
- [ ] Review switch-level policies that could affect segmentation or traffic visibility.

5) Validate host adapter placement

- [ ] Confirm the host management adapter is mapped to the intended VLAN.
- [ ] Confirm any backup adapter uses the intended backup VLAN.
- [ ] Confirm live migration traffic has a dedicated and documented path if required.
- [ ] Confirm storage traffic, if present, is isolated according to design.
- [ ] Ensure the host itself is not reachable from VLANs that should be isolated from administration.

6) Validate guest VM configuration

- [ ] Confirm each VM NIC is connected to the correct virtual switch or port group equivalent.
- [ ] Confirm access VLAN assignments are correct for single-segment VMs.
- [ ] Confirm trunk settings are used only for guests that must read or forward VLAN tags.
- [ ] Verify the guest OS network settings match the intended subnet, gateway, and DNS configuration.
- [ ] Confirm multi-NIC VMs have each adapter mapped to the correct security zone.
- [ ] Remove unnecessary secondary NICs from VMs that do not need them.

7) Confirm routing and firewall boundaries

- [ ] Verify default gateways are only present on the networks that require them.
- [ ] Confirm inter-VLAN routing exists only where explicitly approved.
- [ ] Check firewall rules between management, production, backup, and storage segments.
- [ ] Confirm the host and guest are not bypassing intended security controls.
- [ ] Validate that admin access paths are limited to authorized source networks.

8) Test isolation and connectivity

- [ ] Confirm each VM can reach only the networks it should access.
- [ ] Confirm management hosts can reach management subnets but not tenant-only networks.
- [ ] Confirm production VMs cannot access administrative segments unless approved.
- [ ] Confirm backup systems can reach backup targets without using the production path unless designed to do so.
- [ ] Confirm DNS, NTP, and other shared services are reachable from the correct segments.
- [ ] Test that blocked traffic is actually blocked, not merely untested.

9) Test operational traffic paths

- [ ] Validate live migration traffic under expected load.
- [ ] Validate backup and restore transport paths.
- [ ] Validate patching, maintenance, and emergency access paths.
- [ ] Validate console-only recovery procedures for network outage scenarios.
- [ ] Validate cluster or failover behavior if the environment uses HA features.
- [ ] Confirm any monitoring or security tooling can still function without broad network exposure.

10) Verify failure modes before production

- [ ] Confirm a VM still behaves correctly if a nonessential network path is unavailable.
- [ ] Confirm the host remains manageable if a guest VLAN fails.
- [ ] Confirm segmentation is preserved after reboot, failover, or migration.
- [ ] Confirm backup and recovery still work when production traffic is congested.
- [ ] Confirm failover does not place workloads on an incorrect VLAN or port profile.

11) Document the final design

- [ ] Record VLAN IDs, subnet ranges, gateways, and routing rules.
- [ ] Record which system owns tagging for each interface or adapter.
- [ ] Record which physical switch ports and host adapters are in scope.
- [ ] Record which VMs use access mode and which use trunk mode.
- [ ] Record validation results and any exceptions.
- [ ] Store the documentation where operations and incident response teams can access it.

12) Production readiness sign-off

- [ ] The design is simple enough to explain during incident response.
- [ ] The allowed VLANs are restricted to what the host actually needs.
- [ ] Management, backup, and workload traffic are separated where required.
- [ ] Isolation tests passed for both permitted and denied traffic.
- [ ] Operational traffic paths were tested, not assumed.
- [ ] Recovery documentation reflects the same segmentation model.
- [ ] The final configuration has been reviewed and approved.

Quick release gate

Do not move the workload into production until all of the following are true:

- [ ] The physical switch, Hyper-V switch, and guest configuration all agree on the intended VLAN path.
- [ ] The host can only carry approved VLANs.
- [ ] The VM sees only the network segments it is supposed to use.
- [ ] Live migration, backup, and recovery have been validated.

- [ ] The design and exceptions are documented.

Notes

- A VM having an IP address does not prove it is on the correct VLAN.
- The safest design is usually the simplest one that satisfies the security and routing requirement.
- If a workload does not need to tag or forward VLANs itself, do not enable that capability.
- Recheck segmentation after changes to switch ports, host networking, VM NICs, or recovery workflows.