domotz

NMS Accelerator 101

NETWORK MONITORING SUCCESS CHECKLIST

1 Prepare Your Environment

- ☐ Confirm **deployment type**: Windows, Linux, Hyper-V, NAS, or appliance.
- ☐ Verify **collector resources** (CPU, memory, storage) meet requirements.
- ☐ Plan for **redundancy & segmentation** (don't treat your collector as one-and-done).

2 Credentials & Access

- ☐ Gather **device credentials** Domotz will need (SNMP v2/v3, SSH, WMI, API keys, cloud controller logins).
- ☐ Test credentials before onboarding devices.
- ☐ Remove default SNMP strings and enforce **secure standards**.

3 Automated Discovery & Inventory

- ☐ Run the **Domotz discovery scan** to identify all connected devices (routers, switches, firewalls, Wi-Fi, servers, endpoints).
- ☐ Validate that **every device is classified** (managed vs unmanaged doesn't matter — impact does).
- ☐ Confirm **inventory auto-updates** as the environment changes.

4 Define What to Monitor

- ☐ Select devices with **highest business impact**:
  - → Core infrastructure (routers, switches, firewalls)
  - → Critical services (servers, storage, VPN, cloud gateways)
  - → User touchpoints (Wi-Fi APs, VoIP, cameras, printers)
- ☐ Apply **standard monitoring policies** across clients/sites for consistency.

5 Metrics That Matter

- ☐ Enable collection of the **essential four metrics**:
  - → Availability (uptime)
  - → CPU & memory load
  - → Interface utilization
  - → Connectivity/latency
- ☐ Use SNMP OIDs and vendor-specific extensions where available.

6 Baselines & Thresholds

- ☐ Establish a **performance baseline** (2–4 weeks of normal data).
- ☐ Define thresholds for alerts based on baseline behavior (avoid false positives).
- ☐ Use **delta monitoring** (rate of change) for disk space, bandwidth spikes, etc.
- ☐ Document baseline templates for MSP rollouts.

7 Alerts & Notifications

- ☐ Configure **meaningful alerts** (avoid flapping).
- ☐ Define **critical vs. warning** thresholds.
- ☐ Set up **escalation rules** (who gets notified and how).
- ☐ Integrate alerts with your **PSA/ticketing system** for streamlined workflows.

8 Reporting & KPIs

- ☐ Define **KPIs relevant to stakeholders** (firewall capacity, CPU growth, bandwidth trends).
- ☐ Schedule regular reports for both **tech teams** and **business leaders**.

9 Security & Compliance

- ☐ Regularly review monitored device configurations.
- ☐ Standardize on a **"gold config"** for core devices.
- ☐ Monitor for **open ports, rogue devices, duplicate IPs**.
- ☐ Document compliance checks for client SLAs.

10 Continuous Improvement

- ☐ Upskill your team — start with metrics, then expand to traffic flows, baselines, and configs.
- ☐ Add **custom OIDs and vendor-specific monitoring** over time.
- ☐ Use **topology mapping** to validate network resilience.
- ☐ Run post-incident reviews to refine alerts, thresholds, and reports.