Tool : Nagios

Monitoring Capabilities

- **Wide Range of Checks:** Out-of-the-box plugins cover most common monitoring needs, with a massive custom script/plugin library available.
- **Agent + Agentless:** Monitor with agents (NRPE, NCPA) for in-depth metrics, or remotely with SNMP, WMI, SSH, etc.
- **Threshold-Based Alerting:** Flexible alerting mechanisms (email, SMS, etc.) with escalation and dependencies.
- **Visualization:** Dashboards, reports, historical trending for analysis.

Licensing Cost

- **Nagios Core:** Free and open-source!
- **Nagios XI:** Commercial edition with enterprise features. Pricing is based on the number of monitored nodes/devices. Contact Nagios sales for a quote:

Customization

- **Plugins:** Write scripts or use community plugins for anything imaginable.
- **Configuration:** Highly configurable, defining hosts, services, commands, etc.
- **Integration:** APIs for integration with ticketing systems, reporting tools, etc.

When Nagios Might NOT Be Relevant

- **Massive Scale:** In extremely distributed environments with 10,000s of nodes, specialized tools might be better
- **Log-Centric Focus:** If primary need is log aggregation/analysis, other tools are more specialized.

Performance Metrics

- **Tool Availability:** Nagios itself should be highly available with uptime percentages.
- **Alert Response Time:** How quickly are alerts delivered to admins.
- **Time-to-Resolution (TTR):** Average time to fix issues identified.
- **Events Per Hour:** Volume can indicate infrastructure health.

KPIs for Tool Usage

- **# of active hosts/services:** Scope of monitoring
- **# of alerts per period:** Workload indication
- **% alerts leading to action:** Reveals alert quality
- **User adoption:** Are stakeholders finding it useful?

Additional Benefits

- **Proactive Problem Solving:** Prevents outages
- **Capacity Planning:** Trends help justify upgrades
- **Compliance:** Audit trails and reporting
- **Cost Savings:** Reduce downtime, optimize resources

Industry-Specific Use

- **Healthcare:** HIPAA compliance monitoring, patient data availability.
- **Finance:** PCI DSS compliance, suspicious activity detection.

Customer Success Stories - Reference

- **Versium Analytics:** Nagios allowed them to create a near self-healing system through automation.
- **Top Bank:** (With Nagios XI, the IT team gained a centralized view of their environment with time-saving automation that reduced manual tasks.
- You can find more case studies on the official Nagios website:

Core Capabilities and use cases for Tool Adoption.

Core Infrastructure & Services

- Server Uptime/Downtime: Basic availability monitoring (ping checks).
- CPU, Memory, Disk Usage: Track resource utilization on servers.
- Service Monitoring: Ensure critical services are running (HTTP, SMTP, SSH, etc.).
- Network Connectivity Monitoring: Monitor switches, routers, firewalls, and network links.
- Website Availability: HTTP checks, ensuring your website is reachable.
- DNS Server Responsiveness: Monitor the health of your DNS infrastructure.
- Database Health Checks: Test database connectivity and query execution.
- SSL/TLS Certificate Expiration: Alerts before certificates expire.
- File Integrity Monitoring: Detecting changes to critical configuration files.
- Log Monitoring: Monitoring log files for errors, warnings, or security events.

Applications & Environments

- Web Application Performance: Measure page load times and response times.
- API Monitoring: Check the availability and performance of internal or external APIs.
- VMware Monitoring: Track virtual machine status, resource usage, and guest performance.
- Hyper-V Monitoring: Similar monitoring for Microsoft Hyper-V environments.
- Docker Container Monitoring: Ensure container health and resource usage.
- AWS Monitoring: Track EC2 instances, RDS databases, and other AWS services.
- Azure Monitoring: Status and performance of Azure virtual machines and services.
- Cloud Application Monitoring: Check SaaS applications (Office365, Salesforce, etc.) for availability.
- IoT Device Monitoring: Sensor status, connectivity, data reporting.
- Temperature & Environmental Monitoring: Monitor server room conditions.

Network & Security

- Bandwidth Monitoring: Track utilization on network interfaces.
- Firewall Rule Monitoring: Detect changes to firewall policies.
- Intrusion Detection: Basic pattern-based anomaly detection within network traffic.
- VPN Tunnel Monitoring: Ensure VPN tunnel availability.
- Wireless Access Point Monitoring: Status and client connections.
- IP Address Tracking: Identify new or rogue devices on the network.
- Switch Port Monitoring: Track port status, errors, and traffic.

- VoIP Call Quality: Monitor MOS scores and other voice-specific metrics.
- Security Vulnerability Scanning: Integration with tools like OpenVAS for vulnerability discovery.
- Antivirus/Antimalware Status: Checking for software updates and definitions on clients.

Specific Use Cases

- Print Server & Printer Monitoring: Queue lengths, toner levels, device errors.
- Backup System Monitoring: Verify backup job completion and success.
- Storage Array Monitoring: Disk health, capacity, RAID status.
- HVAC System Monitoring: Alerts on temperature or humidity anomalies.
- Power Supply Monitoring: Track UPS battery health and status.
- Custom Application Monitoring: Monitoring via scripts or specialized plugins.
- Business Process Monitoring: Check completion of multi-step workflows with dependencies.
- Batch Job Monitoring: Ensure scheduled tasks complete successfully
- Development Environment Monitoring: Resource limits and availability for testing.
- Compliance Checks: Automate checks against regulatory requirements.

Use Cases detailed with sub category.

Core Infrastructure & Services

- **Server Uptime/Downtime:**
  - **Host Group Checks:** Monitor entire groups of servers (e.g., "web servers," "database servers") collectively.
  - **Differentiated Pings:** ICMP, TCP pings to specific ports, HTTP requests for granular testing.
  - **Escalations:** Tiered notifications (email to a team, then SMS to manager if no response).
  - **Scheduled Downtime:** Maintenance windows to suppress alerts.
- **CPU, Memory, Disk Usage:**
  - **Thresholds and Trends:** Alert on high usage, as well as sudden changes or unusual growth patterns.
  - **SNMP Traps:** Proactive alerts directly from devices supporting SNMP trap notifications.
  - **Predictive Disk Failures:** Integration with SMART data for warnings on pre-failure signs.
- **Service Monitoring:**
  - **Beyond On/Off:** Check service response content, not just port availability (e.g., ensure a web server returns an HTTP 200 code).
  - **Dependency Checks:** Prevent alert floods; if a core service is down, suppress alerts on dependent ones.
  - **Service Restart Actions:** Automatically attempt service restarts on failures.
- **Network Connectivity:**
  - **Layer 2 vs. Layer 3:** Ping switches, but also check routing tables on routers.
  - **Critical Path Monitoring:** Define critical network paths and monitor all devices along the way.
  - **Performance Baselines:** Track latency and packet loss over time, not just availability.
- **Website Availability:**
  - **Multi-Location Checks:** Simulate access from different geographic regions to identify localized issues.
  - **Content Verification:** Ensure the correct page loads, not just a generic server response.
  - **Broken Link Monitoring:** Periodically crawl your site, reporting on dead URLs.
- **DNS Server Responsiveness**
  - **Record Type Checks:** Test A records, MX records, etc., ensuring correct resolution.
  - **Recursive Query Testing:** Simulate how clients resolve external hostnames, identifying chain problems.
  - **DNSSEC Validation:** Monitor the integrity of digitally signed records (if applicable).
- **Database Health Checks**

    - **Query Response Time:** Track how long specific queries take to execute.
    - **Failed Connections:** Alert on database unavailability, even if the server itself appears up.
    - **Replication Lag:** Monitor delay in replication between primary and secondary databases.
- **SSL/TLS Certificate Expiration**
    - **Proactive Alerts:** Notify with plenty of lead time (30, 60, 90-day warnings).
    - **Bulk Checks:** Monitor certificates for a large number of websites or services.
- **File Integrity Monitoring**
    - **Scheduled vs. Real-time:** Periodic checks, or near-real-time alerting on changes.
    - **Whitelist/Blacklist:** Ignore known changes, focus on unexpected file modifications.
- **Log Monitoring**
    - **Centralized Log Aggregation:** Pull logs from multiple servers into Nagios.
    - **Regex-based Pattern Matching:** Define specific errors, security events, or patterns to watch for.
    - **Log Rotation Awareness:** Nagios adapts to log rotation schemes.

Applications & Environments

- **Web Application Performance**
    - **Synthetic Transactions:** Simulate multi-step user actions (login, search, etc.) for realistic timings.
    - **Resource Bottleneck Identification:** Break down load time into network vs. backend processing time.
    - **Third-Party Component Impact:** Check load times of external content or embedded ads.
- **API Monitoring**
    - **JSON/XML Response Parsing** Extract specific data from API responses for validation.
    - **Authentication Checks:** Ensure APIs requiring auth tokens respond as expected.
    - **Chained API Calls:** Test workflows depending on multiple API interactions in sequence.
- **VMware Monitoring**

    - **Host and Guest Monitoring:** Track both physical ESXi host metrics and individual VM health.
    - **Datastore Capacity Alerts:** Proactively alert on low space within datastores.
    - **VM Snapshot Tracking:** Monitor snapshot size, age, and potential impact on performance.
- **Hyper-V Monitoring**
    - **Virtual Network Monitoring:** Check health of Hyper-V virtual switches and network adapters.
    - **Integration with System Center:** Potentially pull additional data if you use SCOM for broader management.
    - **VM Replication Status:** Ensure VM replication is healthy (if used).
- **Docker Container Monitoring**
    - **Container Health Checks:** Ensure containers are running, not in a restarting loop.
    - **Resource Limits:** Monitor CPU/memory usage against any defined container limits.
    - **Dependency Mapping:** Understand if outages ripple through interconnected containers.
- **AWS Monitoring**
    - **Cost Monitoring:** Track EC2, S3, and other service usage costs.
    - **Auto Scaling Group Monitoring:** Ensure scaling groups function, triggering alerts on failures.
    - **Integration with CloudWatch:** Pull additional metrics from AWS's native monitoring service.
- **Azure Monitoring**
    - **Resource Group Checks:** Monitor resources within Azure Resource Groups collectively.
    - **Azure Service Health:** Incorporate status updates from Azure's status dashboard.
    - **Azure Automation Integration:** Trigger remediation scripts or actions based on Nagios alerts.
- **Cloud Application Monitoring**
    - **External vs. Internal Access:** Test SaaS reachability from both the internet and your internal network.
    - **Single-Sign-On (SSO) Failures:** Check login functionality with your identity provider.
- **IoT Device Monitoring**
    - **MQTT Support:** Monitor devices communicating via MQTT message brokers.

    - **Device Firmware Updates:** Track device firmware versions for security or feature checks.
    - **Sensor Data Anomaly Detection:** Baseline normal ranges for sensors, alerting on deviations.
- **Temperature & Environmental Monitoring**
    - **Multi-Sensor Correlation:** Map sensors to server racks, visually identifying hotspots in your data center.
    - **Power Redundancy Checks:** Ensure multiple power feeds to a rack are operational.

Network & Security

- **Bandwidth Monitoring**
    - **Interface Traffic Shaping:** Integration with tools for traffic shaping/QoS if needed.
    - **NetFlow/sFlow Analysis:** Monitor traffic patterns and source/destination breakdowns.
- **Firewall Rule Monitoring**
    - **Diff-Based Change Tracking:** See exact edits to rule sets, not merely that a change was made.
    - **Policy Anomaly Detection:** Alert on overly permissive rules or conflicts.
- **Intrusion Detection**
    - **Signature-Based Checks:** Basic pattern matching on network traffic (supplement with a full IDS/IPS for deeper capability).
    - **Behavior-Based Anomaly Detection:** Identify unusual traffic patterns even without explicit signatures.
- **VPN Tunnel Monitoring**
    - **Site-to-Site and Remote Access:** Monitor both types of VPN connectivity.
    - **Tunnel Throughput:** Track bandwidth utilization within VPN tunnels.
- **Wireless Access Point Monitoring**
    - **Rogue AP Detection:** Identify unauthorized APs on your network.
    - **Signal Strength Mapping:** Integration with some Wi-Fi management tools for heatmaps.

Specific Use Cases

- **Print Server & Printer Monitoring**
    - **Paper Jam Notifications:** Alert on specific printer error codes indicating paper tray issues.

    - **Toner/Ink Level Tracking:** Proactive alerts before the toner/ink runs out.
    - **Print Queue Monitoring:** Notify if the print queue becomes abnormally long or stalled.
- **Backup System Monitoring**
    - **Job Success/Failure:** Beyond just start/end, check for explicit success indicators in backup logs.
    - **Tape Drive Health:** Monitor SMART data on LTO tape drives, if available.
    - **Cloud Backup Verification:** Check files are accessible in cloud storage post-backup.
- **Storage Array Monitoring**
    - **Vendor-Specific Plugins:** Tap into specialized plugins for EMC, NetApp, Dell, etc.
    - **Predictive Failure Alerts:** Monitor pre-failure signs based on array-specific sensor data.
    - **Capacity Forecasting:** Graph storage usage trends to plan expansions proactively.
- **HVAC System Monitoring**
    - **Failure Modes:** Monitor not just temperature, but fan status, compressor status, etc.
    - **Redundancy Checks:** If you have multiple HVAC units, ensure failover works as intended.
- **Power Supply Monitoring**
    - **Battery Degradation Tracking:** Track battery capacity health over time on UPS devices.
    - **Generator Fuel Level Monitoring:** If supported, track fuel levels for extended outage scenarios.
    - **Automatic Power Testing:** Some plugins support scheduled UPS self-tests to validate functionality.
- **Custom Application Monitoring**
    - **Writing Your Own Plugins:** Use Perl, Python, Bash, etc., to monitor bespoke applications.
    - **Internal API Calls:** Check health endpoints exposed by internal applications.
    - **Transaction Flows:** Simulate multi-step user interactions within custom applications.
- **Business Process Monitoring**
    - **Order Processing Workflow:** Track state changes of orders within an e-commerce system.
    - **Support Ticket Pipelines:** Check if tickets move through stages (open, in-progress, closed) within help desk systems.

    - **Batch Job Dependencies:** Ensure jobs run in sequence, alerting on failures in upstream tasks.
- **Development Environment Monitoring**
    - **Build Server Status:** Check if automated builds succeed or fail.
    - **Temporary Resource Tracking:** Ensure dev VMs are cleaned up after a set time for cost control.
    - **Test Coverage:** Integrate with code testing tools to track coverage metrics.
- **Compliance Checks**
    - **Automated Policy Audits:** Map Nagios checks to sections of PCI-DSS, HIPAA, or other standards.
    - **Configuration Drift Detection:** Alert on changes that push systems out of compliance.

Important Considerations:

- **Plugin Availability:** While Nagios is immensely flexible, it relies on finding or creating the right plugins for your specific needs.
- **Plugin Quality:** Community plugins vary in quality and maintenance level.
- **Extensibility:** Nagios is powerful, but it might have a steeper learning curve compared to more "turnkey" monitoring solutions.