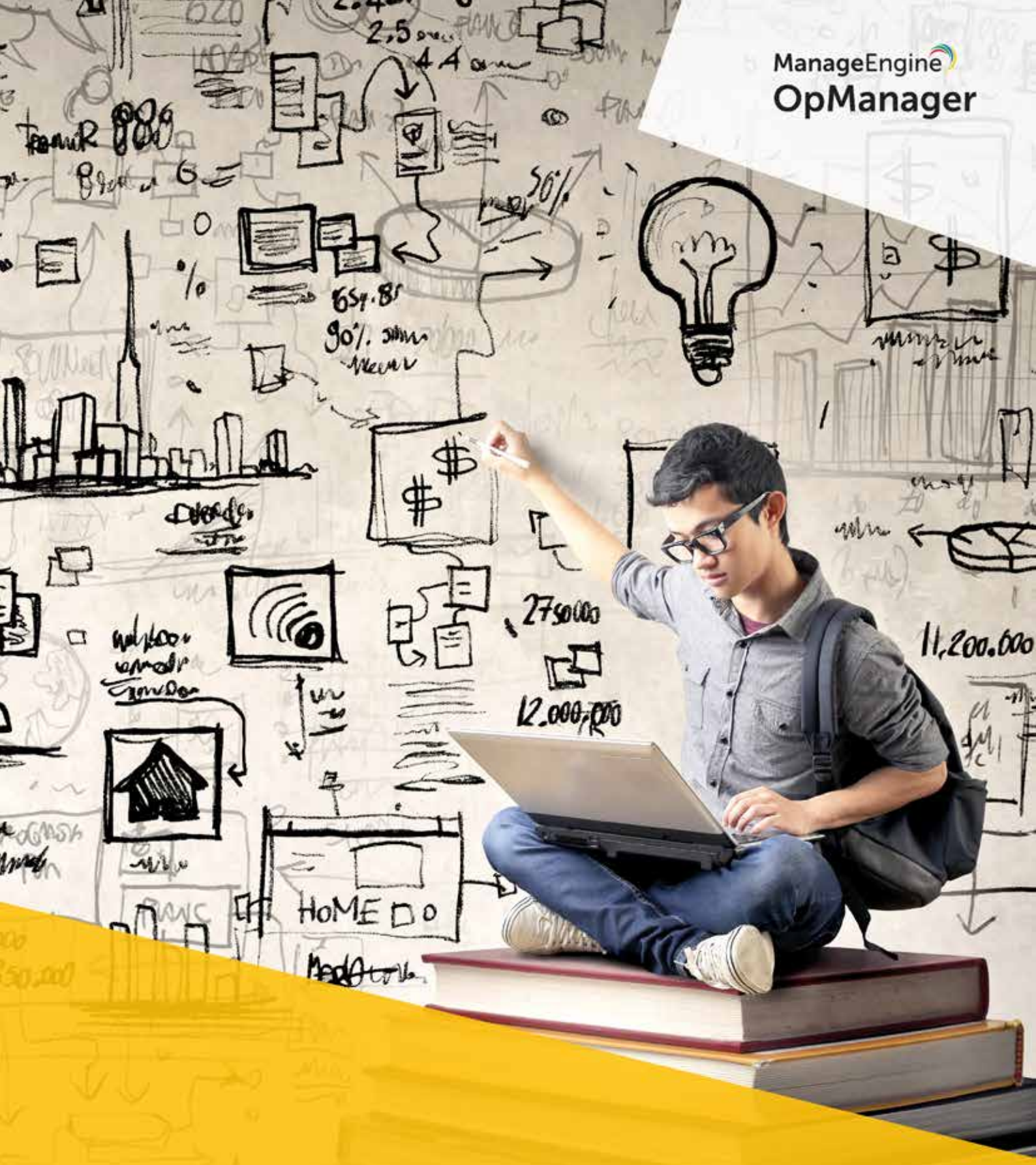
ManageEngine
OpManager




# Die Grundlagen des Netzwerk-Monitorings

Netzwerk-Monitoring-Basics, die jeder IT-Profi kennen sollte

- Nithin.S

www.manageengine.de/opmanager

# Einleitung

Wenn Unternehmen und Organisationen wachsen, nimmt nicht nur die Größe, sondern auch die Komplexität ihrer Netzwerke zu. Unabhängig von der Größe eines Unternehmens wird das Netzwerk zum Verwahrungsort für Daten und Informationen.
Die Fähigkeit, das Netzwerk und seine Komplexität zu verstehen, sowie kontinuierliche Informationen über seine Verfügbarkeit: Das sind die Schlüsselfaktoren, um die Integrität des Netzwerks und des Unternehmens aufrechtzuerhalten. Hierbei spielt das Netzwerk-Monitoring eine entscheidende Rolle.

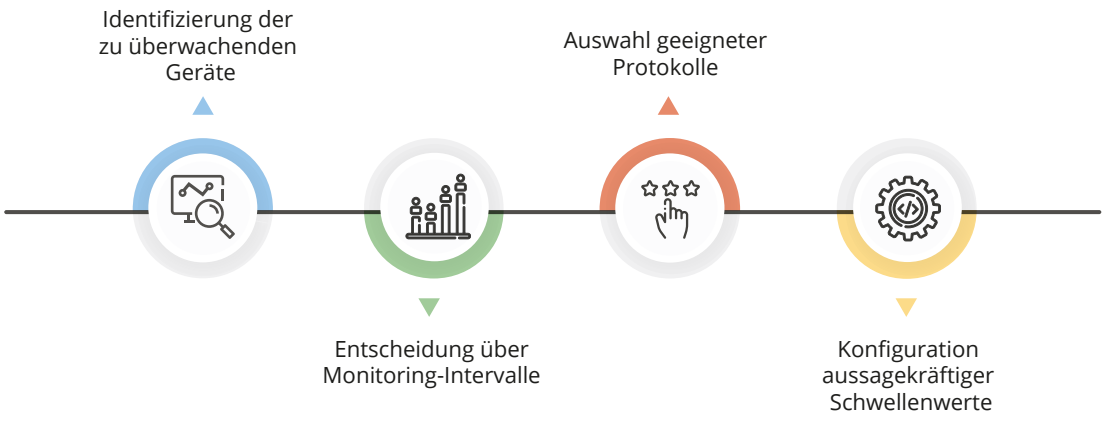
# Was ist Netzwerk-Monitoring?

Der Begriff „Network Monitoring“ ist in der IT-Branche heute allgemein bekannt. Netzwerk-Monitoring ist ein kritischer IT-Prozess, bei dem alle Netzwerkkomponenten wie Router, Switches, Firewalls, Server und Virtuelle Maschinen (VM) im Hinblick auf Fehler und Leistung überwacht und kontinuierlich bewertet werden, um ihre Verfügbarkeit aufrechtzuerhalten und zu optimieren.

Bei einem herausragenden Netzwerk-Monitoring spielt proaktives Vorgehen eine wichtige Rolle: Das Erkennen von Leistungsproblemen und Engpässen hilft dabei, Probleme proaktiv zu identifizieren, bevor diese zu Störungen oder kompletten Netzwerkausfällen führen.

Wichtige Aspekte des Netzwerk-Monitorings:

- Überwachung grundlegender Elemente
- Optimierung der Monitoring-Intervalle
- Auswahl geeigneter Protokolle
- Festlegen von Schwellenwerten



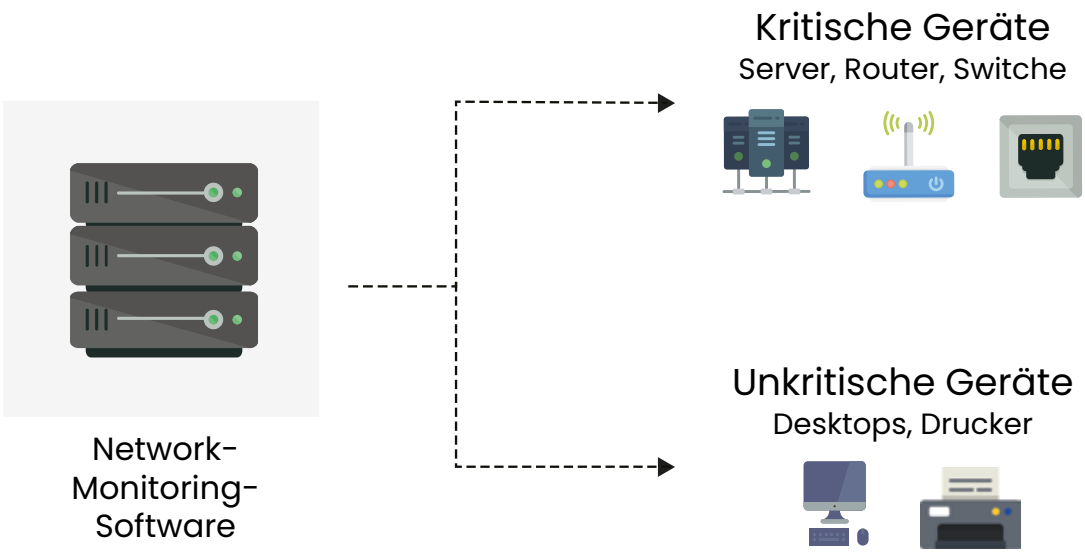
### Wussten Sie schon?

- Branchenumfragen schätzen die Kosten eines Netzwerkausfalls auf rund 5.600 US-Dollar pro Minute. Das sind über 300.000 US-Dollar pro Stunde.
- Nur 2 Prozent der Unternehmen sind in der Lage, einen Netzwerkausfall innerhalb einer Stunde zu beheben. Meistens dauert es deutlich länger – durchschnittlich 4,78 Stunden.

## Überwachung grundlegender Elemente

Fehlerhafte Netzwerkgeräte beeinträchtigen die Netzwerkleistung – sofern sie nicht frühzeitig erkannt werden. Das zeigt, wie wichtig eine kontinuierliche Überwachung des Netzwerks und den damit verbundenen Geräten ist. Neben der Geräteverfügbarkeit gibt es jedoch noch eine Reihe weiterer Faktoren, die das ordnungsgemäße Funktionieren eines Netzwerks beeinflussen können.

Der erste Schritt zu einem effektiven Netzwerk-Monitoring besteht darin, festzustellen, welche Geräte und damit verbundenen Leistungskennzahlen überwacht werden müssen. Während Geräte wie Desktops und Drucker nicht kritisch sind und daher nicht so engmaschig überwacht werden müssen, übernehmen Server, Router und Switches geschäftskritische Aufgaben und sollten daher kontinuierlich überwacht werden.



## Monitoring-Intervalle

Ein Monitoring-Intervall bestimmt die Häufigkeit, mit der Netzwerkgeräte sowie zugehörige Kennzahlen abgefragt werden, um den Leistungs- und Verfügbarkeitsstatus zu ermitteln. Die Wahl geeigneter Überwachungsintervalle hilft Ihnen dabei, das Netzwerk-Monitoring-System und damit auch Ihre Ressourcen zu entlasten.

Welches Monitoring-Intervall am besten geeignet ist, hängt von der Art des Netzwerkgeräts oder Parameters ab. Bewährt haben sich folgende Werte: Die Geräteverfügbarkeit sollte im Minutentakt, CPU- sowie Speicherstatistiken alle fünf Minuten und die Festplattenauslastung alle 15 Minuten überprüft werden. Wesentlich kürzere Monitoring-Intervalle für alle Geräte würden Ihr Netzwerk unnötig belasten und sind auch nicht notwendig, um kritische Aspekte der Netzwerkleistung zu erkennen.

## Verwendete Protokolle

Beim Monitoring eines Netzwerks und seiner Geräte wird üblicherweise ein Protokoll verwendet, das sicher ist und wenig Bandbreite benötigt, um die Netzwerkleistung möglichst wenig zu beeinträchtigen. Die meisten Netzwerkgeräte und Linux-Server unterstützen die Protokolle SNMP und CLI, während Windows-Geräte das WMI-Protokoll unterstützen.

SNMP ist ein weit verbreitetes Netzwerk-Management- und -Monitoring-Protokoll. Die meisten Netzwerkelemente sind mit einem SNMP-Agenten gebündelt, der nur aktiviert sowie konfiguriert werden muss, um mit dem Netzwerk-Management-System (NMS) zu kommunizieren. Wenn Sie den SNMP-Lese-/Schreibzugriff auf einem Gerät erlauben, haben Sie die volle Kontrolle über dieses Gerät. Mit SNMP können Sie auch die gesamte Konfiguration eines Geräts austauschen. Ein Netzwerk-Monitoring-System unterstützt IT-Administratoren dabei, ihr Netzwerk in den Griff zu bekommen, indem sie SNMP-Lese-/Schreibrechte einrichten und die Befugnis für andere Benutzer einschränken.

Netzwerkausfallzeiten können viel Geld kosten. In den meisten Fällen melden Anwender Netzwerkprobleme an das Netzwerk-Management-Team. Dies ist ein reaktiver Ansatz für das Netzwerk-Monitoring. Die größte Herausforderung besteht jedoch darin, Leistungs-engpässe proaktiv zu identifizieren.

Hierbei spielen Schwellenwerte eine große Rolle: Sie variieren allerdings von Gerät zu Gerät sowie je nach Anwendungsfall.

## Sofortige Benachrichtigung beim Überschreiten von Schwellenwerten

Das Konfigurieren geeigneter Schwellenwerte hilft dabei, die auf Servern und Netzwerkgeräten ausgeführten Ressourcen und Dienste proaktiv zu überwachen. Üblicherweise können Sie – je nach Bedarf und individuellen Präferenzen – jedes Gerät mit eigenen Intervall- oder Schwellenwerten versehen. Mehrstufige Werte sind besonders hilfreich, um auftretende Fehler zu klassifizieren und aufzuschlüsseln. Gleichzeitig können Sie die Schwellenwerte nutzen, um sich automatisch alarmieren zu lassen, bevor ein Gerät ganz ausfällt oder einen kritischen Zustand erreicht.

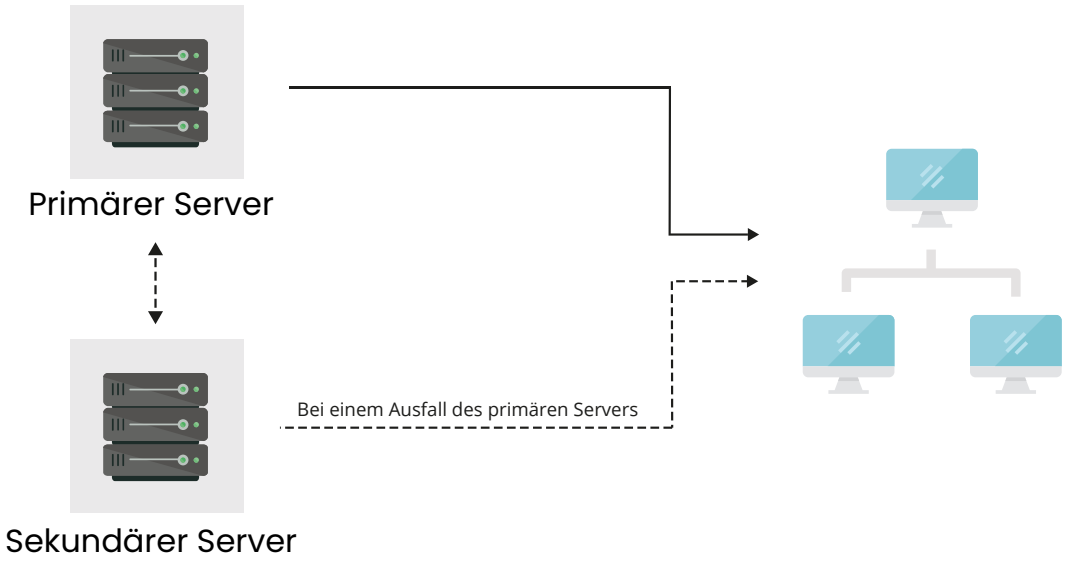
## Dashboards und individuelle Anpassungen

Die besten Daten sind nur dann hilfreich, wenn sie für die jeweilige Zielgruppe verständlich dargestellt werden. Gerade für IT-Administratoren ist es wichtig, dass sie nach ihrer Anmeldung sofort über kritische Kennzahlen informiert werden. Idealerweise sollte Ihnen ein Netzwerk-Dashboard einen schnellen Überblick über den aktuellen Status geben und kritische Kennzahlen von Netzwerkgeräten (z. B. Router, Switche, Firewalls, Server, Services, Drucker und Unterbrechungsfreie Stromversorgungen (USV)), Anwendungen und URLs enthalten. Eine gute Netzwerk-Monitoring-Lösung sollte idealerweise Widgets unterstützen, mit denen sich allgemeine sowie spezifische Leistungskurven in Echtzeit überwachen lassen. So können Administratoren Probleme schnell beheben und Geräte aus der Ferne überwachen.

## Hohe Verfügbarkeit und Ausfallsicherheit

Was passiert, wenn der Server, auf dem Ihr gewohntes Netzwerk-Monitoring läuft, abstürzt oder die Netzwerkverbindung verliert? In diesem Fall möchten Sie höchstwahrscheinlich sofort benachrichtigt werden und möchten zudem, dass ein Standby-Netzwerk-Monitoring automatisch übernimmt. Um eine hohe Verfügbarkeit eines Monitoring-Systems zu gewährleisten, sollte Ihnen jedes einzelne Netzwerkereignis – z. B. ein Leistungsabfall von Geräten, ungenügende Bandbreiten, DoS-Angriffe usw. – sofort mitgeteilt werden, damit Sie schnell geeignete Gegenmaßnahmen einleiten können.

Die sogenannten Failover- und Failback-Funktionalitäten stellen sicher, dass Netzwerkumgebungen stets durch einen sekundären Standby-Server überwacht werden. Wenn ein Fehler auf dem primären Server auftritt, ist der sekundäre Server sofort einsatzbereit, um die Datenbank abzusichern. Damit wird eine vollständige Netzwerk- und Geräteverfügbarkeit gewährleistet.




Vorteile eines Failover-Systems:

- Server-Ausfälle werden sofort erkannt.
- Sofortige Benachrichtigung per E-Mail bei einem Ausfall des primären Servers
- 100-prozentige Betriebszeit (Uptime) und unterbrechungsfreies Netzwerk-Management
- Automatisierter und nahtloser Wechsel vom primären zum Standby-Server und umgekehrt

# Die Wahl des richtigen Netzwerk-Monitoring-Tools

## Künstliche Intelligenz und Maschinelles Lernen

Da sowohl Netzwerk-Monitoring-Tools als auch Technologien wie Künstliche Intelligenz (KI) und Maschinelles Lernen (ML) von Daten leben, lassen sie sich in der Regel gut kombinieren. So können sich Netzwerk-Monitoring-Tools durch ML-Methoden beispielsweise an ihre Netzwerkumgebung anpassen und auf Grundlage der verfügbaren Daten proaktiv Vorschläge unterbreiten.

Möglichkeiten eines Netzwerk-Monitorings mit KI und ML:

- Lastverteilung basierend auf der Nutzung
- Intelligentere Benachrichtigungsprofile
- Anpassung des Netzwerks und die Fähigkeit, automatisch Korrekturmaßnahmen zu ergreifen
- Prognosen

## Automatisierung

Durch die rasante Entwicklung von Anwendungen für KI steht die Automatisierung an einem Wendepunkt. Automatisierung hilft Netzwerk-Monitoring-Tools, aufgrund von Schwellenwerten oder eines einzuhaltenden Satzes von Regeln/Kriterien zu reagieren. Zudem können Monitoring-Tools mit ihr Probleme automatisch erkennen und beheben (proaktives Monitoring), Warnmeldungen versenden und Vorschläge für eine bessere Netzwerkleistung und -wartung (je nach Nutzung und Priorität) unterbreiten.

Vorteile der Automatisierung im Netzwerk-Monitoring:

- Möglichkeit, sich wiederholende Aufgaben zu automatisieren
- Automatisierte Konfiguration und Backup-Bereitstellung auf allen Geräten
- Automatisches Erkennen und Überwachen neuer Geräte
- Proaktive Fehlerbehebung und Einleitung von Abhilfemaßnahmen
- Geplante Berichtserstellung

## Funktionen

Jedes Netzwerk-Monitoring-Tool enthält Funktionen, mit denen sich grundlegende Netzwerk-Kennzahlen wie die Bandbreite, die Verfügbarkeit und die Nutzung überwachen lassen. Eine effiziente Lösung sollte zudem gängige Protokolle (SNMP, WMI und CLI) und Technologien (NetFlow, sFlow, jFlow und Paket Sniffing) unterstützen. Zusätzliche Features wie konfigurierbare Warnmeldungen, Funktionen zur Berichterstellung und anpassbare Dashboards vereinfachen die Nutzung derartiger Tools durch den Anwender und helfen dabei, relevante Informationen im Blick zu behalten. Bevor Sie sich allerdings für eine Netzwerk-Monitoring-Lösung entscheiden, sollten Sie sich zunächst darüber klar werden, welche grundlegenden Anforderungen und Funktionen für Ihr Unternehmen erforderlich sind. Neben den Features gibt es noch einige weitere kritische Aspekte, die Sie bei der Auswahl berücksichtigen sollten.

## Verteilte Netzwerke

Es kommt vor, dass sich das Unternehmensnetzwerk erheblich vergrößert – z. B. bei einer Fusion oder einer Übernahme. In solchen Fällen wächst das neue Netzwerk innerhalb kürzester Zeit erheblich und verteilt sich auf neue lokale Netzwerke, Niederlassungen, Kundennetzwerke (im Falle von Managed Service Providern (MSP)), Rechenzentren und die Cloud. Das zusammengelegte Netzwerk abzusichern, kann kostspielig werden, sowohl was das Management als auch was die Fehlerbehebung betrifft. Dabei ist gerade in verteilten Netzwerken eine ständige Überwachung der Verfügbarkeit und Bandbreitenauslastung notwendig.

Herausforderungen beim Monitoring verteilter Netzwerke:

- **Zentralisierte Kontrolle:** Überwachung mehrerer entfernter Standorte von einem zentralen Standort aus durch Steuerung von spezifischen Probes, um Leistungsprobleme zu visualisieren
- **Netzwerk-Maintenance:** Instandhaltung des Netzwerks und Fehlerbehebung bei Problemen
- **Sprachbarriere:** Anzeige von Statistiken in verschiedenen Sprachen für die gesamte Umgebung an einem zentralen Punkt

## Umfang

Die mangelnde Transparenz eines Tools ist ein Problem, dem IT-Operatoren und Systemadministratoren häufig begegnen. Um den Überblick über Ihr Netzwerk zu behalten, sollten Sie ein Netzwerk-Monitoring-Tool wählen, das Ihnen einen umfassenden, konsolidierten und detaillierten Einblick in verschiedene Netzwerk-Aspekte bietet. Gleichzeitig sollten Sie flexibel auswählen können, was Sie genau sehen möchten. Idealerweise werden die verschiedenen Informationen dabei auf einem einzigen Bildschirm mit übersichtlichen Diagrammen und intuitiven Grafiken dargestellt. Einige Netzwerk-Monitoring-Tools lassen sich zudem erweitern, um komplexere Operationen durchzuführen. Daher sollten Sie darauf achten, dass Sie ein Tool auswählen, das Add-ons und Integrationen unterstützt. So können Sie einen breiteren Aspekt Ihres Netzwerks überwachen.

## Skalierbarkeit

Die Skalierbarkeit des Netzwerks ist ebenfalls wichtig bei der Auswahl eines effizienten Netzwerk-Monitoring-Tools. Ein Netzwerk-Monitoring-Tool ist dann als skalierbar anzusehen, wenn es sich an sich verändernde Anforderungen und Wünsche eines Unternehmens und seiner Anwender anpassen kann.

Skalierbarkeit hilft einem Netzwerk, mit erhöhter Produktivität, Trends, neuen Anforderungen und Anpassungen Schritt zu halten und stellt dabei sicher, dass die Gesamtleistung des Netzwerks unabhängig von seiner Größe nicht beeinträchtigt wird.

## Bewertungen

Bei der Auswahl eines Netzwerk-Monitoring-Tools ist es üblich, die auf dem Markt verfügbaren Lösungen zu analysieren und kennenzulernen. Bewertungs-Websites bieten eine einfache Möglichkeit, verschiedene Aspekte eines Tools kennenzulernen; sie zeigen zudem auf, welche spezifischen Funktionen sich von denen anderer Tools abheben. Analysten führen umfassende Primär- und Sekundärrecherchen durch, für die sie ein großes Netzwerk an Quellen nutzen, darunter Enduser/Kunden, Technologieanbieter und Branchenführer. Sie können auch Inhalte aus akademischen, journalistischen und wissenschaftlichen Quellen enthalten. Die Bewertungen durch etablierte Analystenhäuser wie Gartner und EMA können daher weitere Hilfestellung bei der Auswahl des richtigen Netzwerk-Monitoring-Tools für Ihr Unternehmen bieten.

## Preise

Auf dem Markt gibt es verschiedene Lizenzmodelle, die sich nach der Anzahl der Geräte, Knoten (Nodes) oder Server richten. Das geeignete Lizenzschema kann basierend auf der Größe des Netzwerks, der Art der Lösung (Überwachung oder Verwaltung) und der Skalierbarkeit des Netzwerks bestimmt werden. Dabei sollten Sie sowohl die Kosten des Produkts (einschließlich der jährlichen Wartung und der für Einrichtung, Add-ons, Integrationen und Schulungen aufgewendeten Zeit) als auch die potenziellen Einsparungen mit berücksichtigen. Eine transparente Preispolitik sorgt dafür, dass es keine versteckten Kosten gibt.

## Bewertung

Viele Software-Anbieter stellen kostenlose Testversionen ihrer Tools zur Verfügung, um Ihnen Erfahrungen aus erster Hand zu ermöglichen, damit Sie genau wissen, was Sie bekommen. Es ist wichtig, dass Sie das Produkt vor dem Kauf selbst ausprobieren und Produkt-Demos nutzen, um sich mit den Funktionen vertraut zu machen und ein Gefühl für die Benutzeroberfläche zu bekommen.

# Netzwerk-Monitoring mit OpManager

OpManager ist eine proaktive Netzwerk-Monitoring-Lösung mit leistungsstarken Features, die IT-Administratoren helfen, Netzwerkausfälle schnell zu beheben und ihr Netzwerk im Griff zu behalten.

Mit OpManager ist es einfach:

- den Status und die Leistung aller Netzwerkgeräte zu überwachen.
- Muster im Netzwerk-Traffic aufzuspüren.
- das Netzwerk proaktiv mit mehrstufigen Schwellenwerten zu überwachen.
- Änderungen und Konfigurationen im Netzwerk zu automatisieren.
- WAN-Probleme oder die VoIP-Leistung zu analysieren und Fehler zu beheben.
- mit anpassbaren Dashboards detaillierte Einblicke ins Netzwerk zu erhalten.
- über alle Warnungen auf dem Laufenden zu bleiben – dank fortschrittlichem Fault- und Alarm-Management-System.
- die Betriebskontinuität durch hohe Verfügbarkeit und Failover-Support sicherzustellen.

## Ihr ManageEngine-Partner:

**MicroNova AG**
Unterfeldring 6
D-85256 Vierkirchen

Tel.: +49 8139 9300-456
E-Mail: sales-ManageEngine@micronova.de
Support: support-ManageEngine@micronova.de
Web: www.ManageEngine.de

**Jetzt kostenlos testen** **Online-Demo**

Weitere Informationen zu OpManager finden Sie unter

www.manageengine.de/opmanager