

# Monitoring komplexer IT-Infrastrukturen

Viele Unternehmen stehen heute vor der Frage, wie immer komplexer werdende IT-Infrastrukturen proaktiv überwacht und die Ergebnisse in angemessener Weise übersichtlich grafisch aufbereitet werden können.

IBH bietet dafür die ideale Lösung, die mit der freien Software Nagios und weiteren Open Source Software-Werkzeugen in zwei unterschiedlichen Varianten realisiert werden kann:

- Hosting der Monitoring-Lösung im IBH-eigenen Rechenzentrum

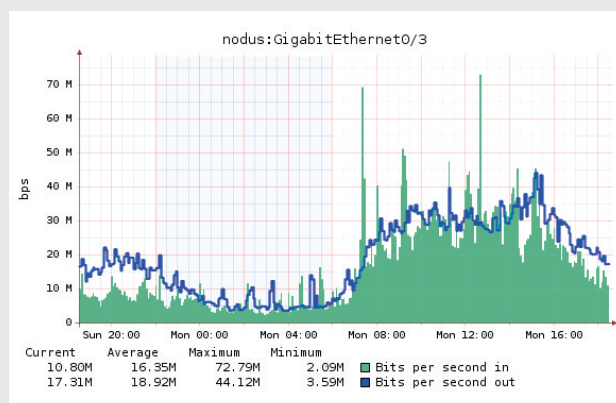
Über eine VPN-Verbindung zum Kundennetzwerk können alle Serviceobjekte gemäß Vertrag überwacht werden.

- Betrieb der Monitoring-Lösung im Netzwerk des Kunden

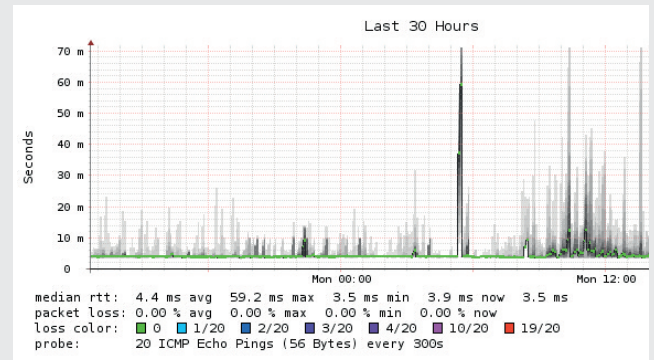
Diese Monitoring-Lösung erfordert im Allgemeinen keine VPN-Verbindung zu IBH und wird in der Regel vom Kunden selbst betrieben. Je nach Vertrag kann IBH über Mails oder per SMS über Probleme informiert werden.

Beim Hosting im IBH-eigenen Rechenzentrum sind alle erforderlichen Infrastrukturleistungen ebenfalls im Angebot enthalten – sei es die Klimatisierung der Systeme, die redundante Stromversorgung oder die redundante Internet-Anbindung für die sichere VPN-Verbindung zum Kundennetzwerk.

Grundlage für den Einsatz von Nagios und der zusätzlichen Software-Werkzeuge bildet eine Debian GNU/Linux Installation inkl. Update-Service von IBH. Damit ist gewährleistet, dass ein aktuelles, dem technischen Stand entsprechend sicheres und von IBH gepflegtes Betriebssystem für das Monitoring zum Einsatz kommt.



Visualisierung der Bandbreitennutzung mit Torrus



Visualisierung des Antwortzeitverhaltens mit SmokePing

Für den Monitoring Service wird das linuxbasierte Grundsystem um folgende Software-Anwendungen ergänzt:

- Nagios** Überwachung der Verfügbarkeit von definierten Serviceobjekten (z. B. Switche, Router, Server etc.)
- Torus** Erfassung von Messwertreihen über wichtige Kenngrößen, wie z. B. Fehler-rate und Portauslastung für Switche
- SmokePing** gezielte Erfassung von Jitter, Latenzzeiten und Paketverlusten im Netzwerk

Weitere Softwarekomponenten können das Monitoring entsprechend der zu überwachenden Technik ergänzen.

Unter dem Aspekt der Erhöhung der Verfügbarkeit werden für die Monitoring-Services häufig auch virtualisierte Server eingesetzt. Bei Problemen mit der Virtualisierungsplattform selbst können diese aber möglicherweise nicht erkannt und gemeldet werden. Daher spricht aus Erfahrung vieles dafür, dennoch einen dedizierten physikalischen Server einzusetzen.

- Zur Gewährleistung einer Hochverfügbarkeit von Applikationen ist die Überwachung der Infrastruktur eine notwendige Voraussetzung.
- In der Praxis haben sich für das Monitoring freie Softwareprodukte wie Nagios, Torrus und SmokePing auf der Basis von Debian GNU/Linux bewährt.
- Die Erfahrung zeigt, dass dedizierte physikalische Server für das Monitoring besser geeignet sind als virtuelle Maschinen. Auf einem Monitoring-Server sollten keine weiteren Dienste für Management- oder produktive Aufgaben zum Einsatz kommen.

**Current Network Status**  
 Last Updated: Tue Mar 15 10:04:33 CET 2011  
 Updated every 90 seconds  
 Nagios® Core™ 3.2.1 - www.nagios.org  
 Logged in as nagiosadmin

**Host Status Totals**

Up	Down	Unreachable	Pending
89	1	0	0

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
282	2	0	1	0

**Service Status Details For All Hosts**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
nodus	NPE-Inlet	WARNING	2011-03-15 10:01:52	11d 20h 30m 33s	3/3	SNMP WARNING - Sensor1 *37* °C
	NPE-Outlet	WARNING	2011-03-15 10:04:18	0d 0h 17m 15s	3/3	SNMP WARNING - Sensor2 *41* °C
sw-ibh-02	PING	CRITICAL	2011-02-07 14:28:11	35d 19h 39m 23s	3/3	PING CRITICAL - Packet loss = 100%

3 Matching Service Entries Displayed

Das Nagios Web-Interface zeigt Komponenten im Zustand „Warnung“ und „Kritisch“

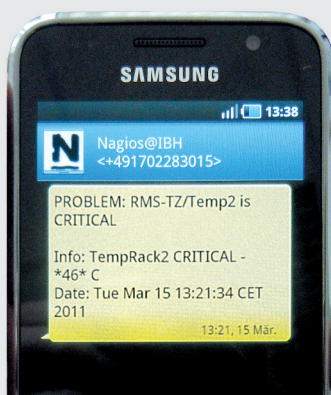
Prinzipiell gilt, dass der Server ausschließlich für das Monitoring eingesetzt wird und darauf keine weiteren Dienste für sonstige produktive Zwecke oder andere Managementaufgaben betrieben werden.

Je nach Vertrag oder Abstimmung kann der Kunde oder IBH die administrative Hoheit über das System erhalten. Der Kunde erhält in jedem Fall mindestens den lesenden Zugriff auf das Monitoring-System. Die Benachrichtigungswege sind sehr flexibel einstellbar. Das Monitoring-System wird bei Erreichen oder Überschreiten definierter Schwellwerte und damit verbundener Warnmeldungen sowie bei Fehlerzuständen je nach Vereinbarung E-Mails an IBH und/oder an vereinbarte E-Mail-Adressen des Kunden versenden.

Wenn das Monitoring-System im Rechenzentrum von IBH betrieben wird oder wenn der Kunde in seinem

Netzwerk über ein SMS-Gateway verfügt, können kritische Zustände auch per Kurznachricht (SMS) übermittelt werden.

Das IBH-eigene Monitoring-System kommt auch zur Überwachung eines Monitoring-Systems im Kundennetzwerk zur Anwendung. Damit ist sichergestellt, dass beim Ausfall von Komponenten, die eine Benachrichtigung per E-Mail und/oder SMS vom System des Kunden verhindern, dieser Ausfall von IBH rechtzeitig erkannt werden kann.



Von Nagios verschickte SMS

- Die Überwachung muss die komplette Infrastruktur einschließen, wie Stromversorgung, USV-Anlage, Klimatechnik, Server- und Speichersysteme, Backup-system, Netzwerkkomponenten, Leitungswege, Internetzugang etc.
- Auch ein Monitoring-Server sollte überwacht werden. Auf vertraglicher Basis kann die Überwachung des Monitoring-Servers auch von IBH übernommen werden bzw. auf Kundenwunsch kann der kunden-eigene Monitoring-Server in das Monitoring-System von IBH integriert werden.
- Das umfassende Know-How von IBH wird durch Zertifizierungen verschiedener Hersteller ergänzt, die die Kompetenz zur Implementierung der Lösung in heterogenen Umgebungen bestätigen. Dies schließt Netzwerke und Server von HP, Cisco u. a. ein.