Netz-Monitoring

Skalierbare und handhabbare Überwachung

Kai-Oliver Detken

Vorausschauendes Monitoren von Netzdiensten und Serversystemen ist heute fast ausschließlich auf die Verfügbarkeit ausgelegt, damit alle IT-Dienste immer zur Verfügung stehen. Durch Virtualisierung entstehen dabei auch in kleineren Umgebungen bereits beachtliche Topologien, die alle administriert und überwacht werden müssen. Zwar bieten Tools wie Nagios und Icinga, die sich heute als De-facto-Standard herauskristallisiert haben, umfangreiche Möglichkeiten, neue Komponenten einzubinden, aber dies beinhaltet auch einen hohen manuellen Konfigurationsaufwand. Hinzu kommt, dass die Abfragen nicht skalieren, sprich in größeren Umgebungen schnell an ihre Grenzen kommen. Check_MK bietet hier Abhilfe. Früher auf Nagios basierend, ist dieses Tool inzwischen allein einsetzbar und verspricht die Nutzung in größeren Netzumgebungen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Nagios hat sich in der Vergangenheit stark in Unternehmensnetzen verbreitet, da es ein Open-Source-Projekt ist und im Gegensatz zu proprietären Monitoring-Lösungen bestimmter Hersteller keine Lizenzkosten verlangt. Auf Nagios basieren auch Icinga und in der Vergangenheit Check_MK. Alle drei Lösungen entwickeln sich getrennt voneinander weiter. Es ist also Zeit für einen direkten Vergleich.

Nagios

Der Schwerpunkt von Nagios (www.nagios.org) ist das übergreifende System-Netz-Monitoring. Aktiv greift Nagios dabei nicht in bestehende Prozesse ein. Die Monitoring-Plattform ist eine modular aufgebaute Software, bestehend aus dem Nagios-Kern und externen Programmen, sog. Plugins, die die Überwachung von Hosts und deren Diensten durchführen. Neben zahlreichen mitgelieferten und frei verfügbaren Plugins lassen sich diese bei Bedarf auch selbst entwickeln und einbinden. Dies kann mit einer beliebigen Programmiersprache (z.B. Perl, C, C#, Java, Python, PHP) erfolgen. Bei Nagios kann exakt eingestellt werden, zu welchem Zeitpunkt ein Fehler oder eine Schwellwertüberschreitung vorliegt und man eine Mitteilung darüber erhalten möchte. Dies kann per SMS, E-Mail und/oder Telefon erfolgen. Einbeziehen kann Nagios sämtliche aktive Systeme im Netz. Das heißt, unabhängig vom Hersteller können alle Netzkomponenten und Serversysteme auf Basis von SNMP erfasst und überwacht werden. Dies kann sich auch auf Anwendungen wie z.B. Datenbanken herunterbrechen lassen. Programme könnten auf Updates überwacht werden und entsprechende E-Mails bei Änderungen verschicken.

Nagios besitzt bereits ein sehr detailliertes mehrstufiges Eskalationsmanagement. So braucht nicht bei jedem Zwischenfall alarmiert zu werden, sondern nur, wenn kritische Systeme betroffen sind. Dabei wird immer zwischen Hosts und Services unterschieden. Auch unterschiedliche Zeiten (Geschäftszeiten, Feierabend, Feiertage) und Mitarbeiter (IT-Administrator, Abteilungsleiter usw.) lassen sich unterscheiden. Eine Dienste- und Topologieübersicht ist über eine Weboberfläche möglich. Neben den typischen Netzdiensten wie SMTP, POP3, http, SNMP, NNTP, Ping usw. können gerade Serversysteme (CPU- und Disk-Auslastung, Systemlogs usw.) genauer untersucht werden. Aktive Netzsysteme wie Router und Switche sowie Temperatur- und Feuchtigkeitssensoren kann man ebenso mit einbeziehen.

Die grafische Darstellung der Überwachungsergebnisse und Logdateien erfolgt mittels Weboberfläche (*Bild 1*). Nagios benötigt dafür einen auf Linux/Unix basierenden Server für das Ausführen der Plugins und ebenfalls als Webserver für die Weboberfläche. Die Konfiguration der zu überwachenden Hosts wird mithilfe von Konfigurationsdateien durchgeführt. Die Benutzer und Gruppen werden über Linux-basierte Gruppen- und Benutzerverwaltung erstellt. Für den Zugriff auf das Webfrontend können dann die erstellten Benutzer in Nagios „freigeschaltet“ werden.

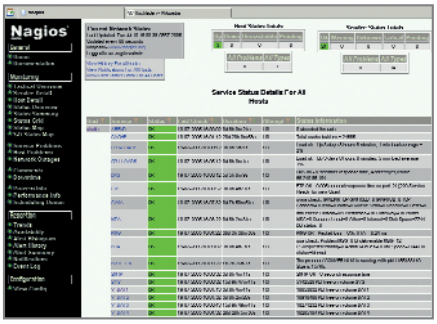

Bild 1: Serviceübersicht der Weboberfläche von Nagios

Mithilfe von Quittierungsmöglichkeiten (sog. Acknowledgement) ist erkennbar, ob sich schon jemand um das eingetretene Problem kümmert. Hier können auch Kommentare zum Lösungsstand hinterlegt werden. Mit verteiltem Monitoring ermöglicht Nagios die Übertragung von Überprüfungsergebnissen von entfernten Linux-/Unix-Hosts zum Überwachungsserver. „Service Dependencies" bieten bei einem Dienstausfall die Möglichkeit, dass nur über den Ausfall dieses Dienstes benachrichtigt wird und nicht über den Ausfall der sich dahinter befindlichen Prüfservices.

Plugin	Beschreibung
check_dbi	überprüft SQL-Datenbanken mittels dbi und prüft Performance gegen Schwellwerte
check_dhcp	überprüft die Verfügbarkeit eines DHCP-Servers im Netz
check_disk	überprüft freien Speicherplatz
check_dns	nutzt nslookup, um die Adressauflösung eines DNS-Servers zu überprüfen
check_ftp	überprüft FTP-Verbindungen
check_http	überprüft den Status eines HTTP(S)-Servers
check_icmp	verschickt ICMP-Pakete und liefert Performance-Daten zurück
check_load	überprüft die Systemauslastung
check_nagios	überprüft den Status eines Nagios-Prozesses
check_pop	überprüft POP-Verbindungen
check_procs	überprüft die Anzahl der laufenden Prozesse
check_smtp	versucht, eine SMTP-Verbindung an einem Host aufzubauen
check_ssh	versucht, eine SSH-Verbindung an einem Host aufzubauen
check_users	überprüft die auf einem System angemeldeten Benutzer

Tabelle 1: Beispiele von Service-Checks- und Performance-Plugins

Nagios bietet weiterhin einen „Event Handler" über den Shell- oder Perl-Skripte oder beliebige, über Kommandozeileninterpreter ausführbare Dateien gestartet werden können, um automatisiert Gegenmaßahmen bei einem Netzproblem einzuleiten.
Die Funktionen von Nagios lassen sich durch selbst geschriebene Plugins erweitern, die einen der vier Zustände für die Überwachung – OK, Warning, Critical oder Unknown – liefern können. Dadurch lässt sich alles prüfen, was elektronisch gemessen werden kann oder sich zählen lässt. Nagios liefert bereits standardmäßig viele Plugins für die wichtigsten Anwendungszwecke mit. Eine Auswahl zeigt *Tabelle 1*.

Icinga

Icinga (**www.icinga.org**) ist ein Fork von Nagios, der von einer deutschen Community im Jahr 2009 gestartet wurde, als die Weiterentwicklung bei Nagios nur schleppend voran ging. Viele Bugs wurden von der Community nicht oder nur sporadisch behoben. Daher spaltete man sich über Icinga ab – unter Beibehaltung der Kompatibilität zu Nagios. Patche werden nun schneller erstellt und eingespielt, so dass größere Rücksicht auf die Community genommen wird.

Icinga zeichnet sich insbesondere durch seine zusätzlichen Datenbankkonnektoren (z.B. für MySQL und PostgreSQL) und die moderne Weboberfläche aus. Letztere ist in unterschiedlichen Varianten (Icinga Classic, Icinga 2) nutzbar und bindet mobile Endgeräte sehr gut als Anzeigemöglichkeit ein (*Bild 2*). Die Plugins von Nagios lassen sich auch bei Icinga weiter nutzen.

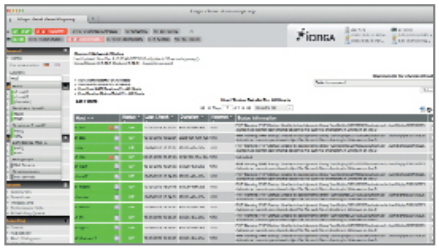

Bild 2: Weboberfläche von Icinga Classic

Um Icinga zu erweitern, kann die gewünschte Funktionalität beispielsweise als Plugin oder Addon hinzugefügt werden. *Tabelle 2* zeigt mögliche Addon-Erweiterungsbeispiele von Nagios, die ebenfalls bei Icinga zum Einsatz kommen könnten. Eine Variante ist das Tool PNP, das Graphen aus den Nagios-Daten heraus erstellt. Diese Graphen lassen sich dann in die Icinga-Oberfläche nahtlos einbinden (*Bild 3*). Icinga bietet eine große Anzahl an Schnittstellen für den Datenaustausch und ist sehr modular aufgebaut. Die Skalierbarkeit und Handhabung ist allerdings ähnlich wie bei Nagios. Das heißt, die Konfiguration ist aufwendig und jede Anfrage wird einzeln vorgenommen. Das schränkt den Einsatz in sehr großen Umgebungen ein.

Check_MK

Check_MK (**http://mathias-kettner.de/check_mk.html**) wurde ursprünglich im Jahr 2008 als Addon (siehe *Tabelle 2*) für Nagios von Mathias Kettner entwickelt, der die Performance und damit die Skalierbarkeit deutlich erhöhen wollte. Inzwischen löst man sich immer mehr von Nagios, indem ein eigener Micro Core entwickelt wurde, der nun eigenständig genutzt werden kann (*Bild 4*). Als Lizenz kommt GPLv2 oder Eula zum Einsatz.
Der erste Ansatz von Check_MK verfolgte das Sammeln der notwendigen Informationen auf einem Host, um ein separates Verschicken zu vermeiden. Check_MK verbindet sich dazu zum Host über TCP. Der check_mk_agent auf dem Host empfängt alle relevanten Daten und sendet diese in einem Stück als ASCII-Text zurück. Check_MK filtert die Performance-Daten heraus und schreibt sie direkt in eine Round-und-Robin-Datenbank (RRD). Check_ MK nimmt die relevanten Daten, vergleicht sie mit den Warning/Critical-Levels und überträgt alle Ergebnisse des Hosts als passive Prüfungen. Durch das Reduzieren der TCP-Verbindungen werden die überwachten Rechnersysteme geschont, und weniger Prozesse reduzieren die Last auf dem zentralen Monitoring-Server. Ein weiterer Nebeneffekt ist, dass auch wenige Prüfintervalle unterstützt werden können, wodurch die erfassten Messdaten eine höhere Genauigkeit besitzen. Die Performance von Check_MK skaliert dadurch auch für größere Umge-bungen. So lässt sich ein verteiltes Monitoring mit einer virtuellen Instanz einrichten, um z.B. mehr als 30.000 Hosts überwachen zu können.

Check_MK ermöglicht die automatische Diensterkennung, um so den Pflegeaufwand gering zu halten. Überwachte Dateisysteme, Netz-Ports, Prozesse, Datenbanken, Festplatten usw. werden automatisch auf einem Host gefunden und in das Monitoring aufgenommen. Dadurch verbessert sich die Handhabung erheblich und erleichtert die Arbeit des Administrators. Die Wahrscheinlichkeit, dass das Monitoring kontinuierlich auf dem neuesten Stand bleibt, erhöht sich dadurch ebenfalls. Eine regelbasierte, hierarchische Konfiguration ermöglicht es zudem, eine entsprechende Ordnerstruktur zu verwalten, die alle Richtlinien übersichtlich hält.

Um die Arbeit weiter zu erleichtern, werden durch Check_MK bereits über 600 Check-Plugins und eigene Agenten mitgeliefert. Sie können u.a. zur Überwachung von Betriebssystemen, Anwendungen, Netzkomponenten, Speichern und Temperatursensoren eingesetzt werden. Dabei werden ebenfalls die automatische Serviceerkennung sowie entsprechende Performance-Darstellungen unterstützt. Über das Webinterface können die Check-Plugins direkt parametrisiert werden. Es lassen sich zusätzlich auch herkömmliche Nagios-Plugins einbinden.

Auch die Installation ist über die Open Monitoring Distribution (OMD) vereinfacht worden. Über ein sog. RPM-Paket kann so eine komplette Monitoring-Umgebung auf einer Standard-Linux-Distribution aufgesetzt werden. Über die Webanwendung WATO ist Check_MK komplett grafisch konfigurierbar (*Bild 5*), wodurch keine tiefergehenden Linux-Kenntnisse notwendig sind. Zukünftig sind weitere Leistungsmerkmale geplant, wie Agent Bakery zum einfachen Zusammenstellen von Agenten, Harmonisierung von Checks, Verarbeiten und Aufbereiten großer Logdateimengen sowie dynamische Graphen und Messwerte in Sekundenintervallen.

Add-on-Erweiterungen	Beschreibung
Check_MK	Add-on zum vereinfachten und beschleunigten Betriebssystem- und SNMP-Monitoring
N2RRD	zum Speichern der Performance-Daten in Round-Robin-Datenbanken
NagiosEventDB	Ereignisdatenbank für Nagios z.B. für SNMP-Traps, Syslog-Meldungen usw.
NagiosGrapher	Tool zur Generierung von Graphen anhand von Nagios-Performance-Daten
NagiosQL	webgestützte Administrationsoberfläche für Nagios 2.x und 3.x
Nagios-virt	zur Überwachung von virtuellen Maschinen mithilfe der libvirt-Schnittstelle
Nagvis	Visualisierung der Überwachungsergebnisse
PerfParse	Datenbankanbindung zur Verarbeitung von Nagios-Performance-Daten
PNP	Tool zur Generierung von Graphen aus Nagios-Daten
Thruk	verbesserte Weboberfläche für große und verteilte Umgebungen

Tabelle 2: Auswahl von Zusatzprogrammen für Nagios & Co

Bild 4: Dashboard von Check_MK

Bild 3: PNP-Integration bei Icinga 2

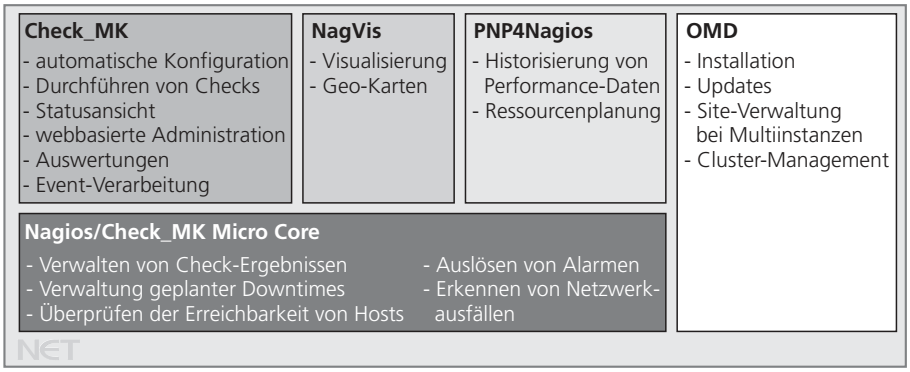

Bild 5: Architektur von Check_MK

Fazit

Das Open-Source-Projekt Nagios, das in Europa eine große Verbreitung besitzt, hat sich gezwungenermaßen weiterentwickelt bzw. es haben sich entsprechende Projekte abgespalten, um die Nachteile Skalierbarkeit, Handhabung und Performance in den Griff zu bekommen. Zwar wurde auch Nagios selbst professionalisiert, aber die umständliche Konfiguration und schlechte Skalierbarkeit blieben erhalten. Das Fork-Projekt Icinga konnte mit einer moderneren Weboberfläche, integrierten Datenbank-Checks und Anbindung mobiler Endgeräte punkten. Auch werden in der überwiegend deutschen Community Patche und Bugfixes schneller erstellt.

Speziell Check_MK hat hingegen die Nagios-Basis revolutioniert, indem es die bekannten Probleme gänzlich ausräumte. Um auch die letzten Schwächen auszumerzen, wird man sich künftig sogar von dem Nagios-Kern verabschieden und auf komplette Unabhängigkeit setzen. Der Vorteil, Plugins und Addons der Nagios-Plattform nutzen zu können, bleibt aber erhalten.

Der Markt steht zwischenzeitlich nicht still und hält mit Zabbix (www.zabbix.com) ein weiteres mächtiges Monitoring-Tool bereit, das vom asiatischen Markt nach Deutschland drängt. Es skaliert ähnlich gut wie Check_MK und wird in großen Umgebungen verwendet. Dabei hat es sich völlig unabhängig von Nagios entwickelt. Von daher darf man gespannt sein, wie sich Check_MK zukünftig auch gegen solche Konkurrenz behaupten wird. *(bk)*