Microsoft SCOM versus Open Source

Microsofts „System Center Operations Manager“ und der Nagios-Ableger „Icinga“ sind verbreitete IT-Monitoring-Lösungen. Hier eine Gegenüberstellung der beiden Werkzeuge.

Von **Markus Bäker***

Wer seine Entscheidung für eine Monitoring-Lösung fundiert fällen möchte, sollte nicht als Erstes auf die Lizenzkosten schauen. Auch auf Basis einer ideologischen Vorliebe für kommerzielle oder Open-Source-Angebote sollte keine Auswahl getroffen werden. Relevant für einen Entschluss, den man auch Vorgesetzten gegenüber begründen kann, muss eine objektive Abwägung der Vor- und Nachteile inklusive der geschätzten Gesamtkosten für die Einführung und den Betrieb der Software sein.

Start mit Ist-Analyse

Den Ausgangspunkt für die Auswahl des Monitoring-Tools sollten immer eine Ist-Analyse der Umgebung und die Planung zusätzlicher Systeme für die Zukunft bilden. Aufgelistet werden sollten alle zu überwachenden Server-Arten und deren Betriebssysteme sowie andere Objekte im Netz wie Switches, Firewalls, die unterbrechungsfreie Stromversorgung (USV), Türsteuerungen, Telefonanlagen oder Anlagensteuerungen. Bei dieser Untersuchung interessiert auch, über welche Schnittstellen ein System verfügt, um an die gewünschten Informationen zu gelangen. Die notwendigen Überwachungsparameter werden ebenso definiert.

Zur Auswahl stehen dann zahlreiche Monitoring-Lösungen, die sich je nach IT-Landschaft sehr unterschiedlich für den individuellen Einsatz eignen. Oft stellt sich hier auch die Frage, ob man auf ein kommerzielles Produkt oder auf ein Open-Source-Werkzeug zurückgreifen soll. Um diese Entscheidung zu erleichtern, werden einander im Folgenden zwei namhafte Systeme exemplarisch gegenübergestellt:

Open-Source-Vertreter Icinga

Auf der einen Seite Icinga, das im Jahr 2010 von einem Teil der Nagios-Community ins Leben gerufen wurde und seitdem mit beeindruckendem Tempo weiterentwickelt wird. Die Grundfunktionen sind nach wie vor in beiden Open-Source-Systemen ähnlich, daher gelten die in diesem Beitrag gemachten Aussagen gleichermaßen für beide Varianten. Bestärkt wird dies durch die uneingeschränkte und beabsichtigte Kompatibilität von Icinga mit Nagios und all seinen Add-ons.

Für die kommerzielle Seite steht aus der Reihe der System-Center-Produkte von Microsoft der Operations Manager, der häufig als prinzipielle Konkurrenz von Open Source angesehen wird. SCOM liegt derzeit in Version 2007 R2 vor und verfügt mit den integrierten Cross Platform Extensions auch über eine Anbindung an Teile der Nicht-Microsoft-Welt.

Anhand dieser verbreiteten Lösungen sollen grundlegende Unterschiede und Gemeinsamkeiten zwischen Monitoring-Systemen aufgezeigt werden.

Die Datensammlung

Einer der Hauptunterschiede zwischen beiden Produkten ist die Art und Weise, wie die Daten der überwachten Systeme gesammelt werden. Icinga verfolgt hier einen eher zentralistischen Ansatz und sammelt die Daten direkt vom Icinga-Server aus ein, während SCOM dies von Agenten erledigen lässt. Beide Systeme erlauben aber auch die Wahl des jeweils anderen Wegs. So ist es beispielsweise möglich, auf Icinga-überwachten Systemen einen Dienst zu installieren, der das Sammeln und Versenden der Daten übernimmt (so genannte passive Checks). ▶

Eckdaten im Vergleich

	Nagios/Icinga	System Center Operations Manager
Lizenzmodell	Open Source	proprietär, Sourcecode für Cross-Platform-Provider offen
Überwachungsmodell	unterscheidet zwischen Hosts und Services	objektorientiertes Modell
Grundsätzlicher Überwachungsansatz	Server fragt Clients ab, alternativ passive Checks	agentenbasierend: Clients schicken Check-Ergebnis; alternativ agentless
Performance-Überwachung	möglich inklusive Round Robin Database (NagiosGraph)	integriert inklusive Data Warehouse
Reaktion auf Alarme	Benachrichtigung und Event Handler	Benachrichtigung, Diagnostic und Recovery Tasks
Hinzufügen neuer Clients	manuell (config files, teilweise Web-basierend)	automatisches Discovery über ADDS oder Netzwerk
Knowledge Base	nicht vorhanden	in Management Packs mitgeliefert, erweiterbar
Schwellwerte	manuell setzen	in MPs mitgeliefert
SLA-Überwachung	durch Add-ons möglich	durch kostenloses MP möglich
Verknüpfung mit Fremdprodukten	per E-Mail-Event-Handler	fertige Konnektoren zu Tivoli, HP OpenView, BMC Remedy ARS

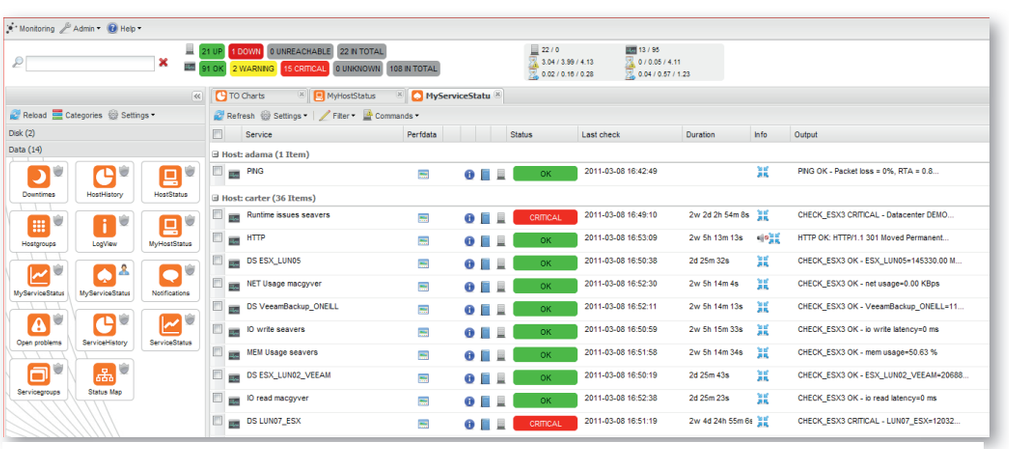
Quelle: Markus Bäker

▶ Ebenso ist es möglich, den SCOM-Server zum aktiven Sammeln von Daten zu bewegen, zum Beispiel bei Netzkomponenten oder anderen agentenlosen Systemen.

Wohin mit der Sammellogik?

Beide Vorgehensweisen haben Vor- und Nachteile. Bei einem Sammeln der Daten müssen alle Konfigurationen und Anpassungen nur am zentralen Server vorgenommen werden, da es keine dezentralen Agenten gibt. Beim Einsatz von Agenten wiederum kann ein Teil der Sammellogik auf den Client verlagert werden und damit den Server entlasten. So reicht es, wenn der Agent den Füllstand einer Festplatte überprüft und beim Überschreiten eines Schwellwertes einen Alarm auslöst (Modell SCOM), wohingegen ohne Agent (Modell Icinga) in regelmäßigen Intervallen eine entsprechende Kenngröße an den Server übermittelt wird und dieser dann entscheidet, ob ein Alarm ausgelöst wird. Dies belastet nicht nur den Server, sondern auch die Netzverbindung. Ein einzelner SCOM-Server ist laut Microsoft für die Überwachung von bis zu 3000 Agenten ausgelegt.

Natürlich gibt es Dienste, die besser „von außen“ überwacht werden, zum Beispiel ein Mail-Server. Ein Verbindungsversuch zum entsprechenden Port muss erfolgreich sein, sonst erfolgt ein Alarm. Genauer betrachtet reicht das aber nicht ganz aus. Handelt es sich nur um ein Mail-Relay, so wäre interessant, ob die angenommenen Mails auch schnell weitergeleitet werden können. Handelt es sich um einen Web-Server, der auf eine nachgelagerte Datenbank zugreift, sollte dieser mit einer korrekt generierten Seite antworten und nicht nur mit einer beliebigen. Oft ist demnach die Kombination beider Monitoring-Verfahren sinnvoll, also ein Agent, der den Service und abhängige Komponenten überwacht, sowie ein externer Verbindungsversuch, wie ihn auch ein Client vornimmt.



Die Web-Schnittstelle von Icinga mit der Darstellung der zu einem Host gehörigen Dienste und ihres Status.

Microsoft löst das Problem der dezentralen Umkonfiguration seiner Agenten dadurch, dass der Administrator die einzelnen Konfigurationsänderungen zentral am Server vornimmt und diese dann automatisch an die Agenten übertragen werden. Icinga löst das Problem des dezentralen Sammelns über passive Checks, die es Clients erlauben, einen Status an einen zusätzlichen Service auf dem Icinga-Server zu melden, und diesen dann in die normale Ereigniskette einsortiert und dort abarbeitet.

Analyse der Datenquellen

Bei diesem Entscheidungskriterium ist also interessant, wie und wo die Mehrzahl der benötigten Informationen gewonnen werden kann. Ein weiteres Kriterium wäre es, wenn der zu überwachende Server durch eine Firewall geschützt ist. In diesem Fall ist unter Umständen eine Abfrage „von außen“ per Icinga nicht möglich, aber ein Senden des SCOM-Agenten „von innen“ erlaubt.

Das Data Warehouse

Betrachtet man bei den beiden Systemen das „Data Warehouse“, also die Ablage der gewonnenen Daten, so treten gravierende Unterschiede zutage. Während SCOM auf den etablierten SQL Server setzt, sind die Ansätze bei Nagios, eine Datenbank wie MySQL zu verwenden, bisher eher von mäßigem Erfolg gekrönt. Tatsächlich setzt ein Großteil der Nagios-Server immer noch auf die Speicherung in Dateien. Dass dies zu Performance-Problemen etwa aufgrund von Größe und Locking führt, dürfte keine Überraschung sein. Erfreulich ist allerdings, dass die Icinga-Entwickler sich besonders diesen Punkt in die Arbeitsbücher geschrieben ha-

ben. Eine Historie von Performance-Daten (Antwortzeiten, Füllstand etc.) kann mit Icinga nur sinnvoll über Add-ons erreicht werden, die einfach zu integrieren sind. Der SCOM sammelt die Daten per Agent und ermöglicht von Haus aus entsprechende Statistiken.

Auto-Discover – manuelle Pflege

Relevant ist auch, wie zu überwachende Systeme erfasst werden. SCOM bietet hier ein Auto-Discover, sowohl (sub-)netzwerkbasierend als auch Active-Directory-integriert, wohingegen Icinga seine Informatio-nen aus einer oder aus mehreren Textdateien bezieht. Diese werden zwar von einigen Administratoren automatisch erzeugt, in den meisten Fällen jedoch nach wie vor von Hand gepflegt, was recht fehleranfällig ist. Diese Fehleranfälligkeit lässt sich jedoch durch sinnvolle Vorlagendefinitionen für die einzelnen Überprüfungen erheblich reduzieren. Hintergrundinformationen über das System selbst, also Hauptspeicher, Prozessortyp, Betriebssystem etc., werden in Icinga über eine „Extended Host Information“ ebenfalls von Hand erfasst. Der SCOM liest diese Informationen direkt aus und stellt sie zur Verfügung. Durch die seit einiger Zeit erhältlichen Cross Platform Extensions ist dies nicht auf Windows-Systeme beschränkt. Der Zugriff auf diese möglichst aktuellen Information kann eine wertvolle Hilfe bei einer Störungsbeseitigung oder Fehlersuche sein.

Customizing und Pflege

Ein wesentlicher Aufwand bei der Einrichtung einer Überwachungssoftware entsteht durch das Customizing beziehungsweise die Pflege des Systems. Das Einrichten neuer Überwachungen und Alarme sowie das Anpassen der Schwellwerte verursacht den größten Aufwand innerhalb eines Einführungsprojekts. Es ist somit von Vorteil, wenn auf fertige Skripte zurückgegriffen werden kann. Für Nagios hat die sehr aktive Community bereits über 390 nützliche Add-ons bereitgestellt. Auch im SCOM-Umfeld existiert eine starke Community, die Management Packs (MP) vorhält. In diesen MPs werden alle Informationen hinterlegt, die für die Erkennung, Überwachung, Alarmierung und das Reporting der zu überwachenden Systeme benötigt werden. Das MP wird in SCOM importiert und automatisch an die Agenten verteilt. Durch Discovery Tasks entscheiden diese, ob die Überwachung für sie relevant ist.

Dieser Aufbau ist ein großer Vorteil von SCOM in einer Microsoft-lastigen Umgebung, da umfangreiche und kostenlose Management Packs zu allen wesentlichen Produkten von Microsoft angeboten werden. In denen ist zum Beispiel das fundierte Produktwissen der Exchange-Entwickler hinterlegt, die sinnvolle Schwellwerte und mögliche Lösungen eines Problems in der integrierten Knowledge Base beschrieben haben. So beinhaltet das Active Directory Server 2008 Management Pack über 850 fertige Regeln zu Überwachung des ADDS. Auch viele Drittanbieter bieten MPs an.

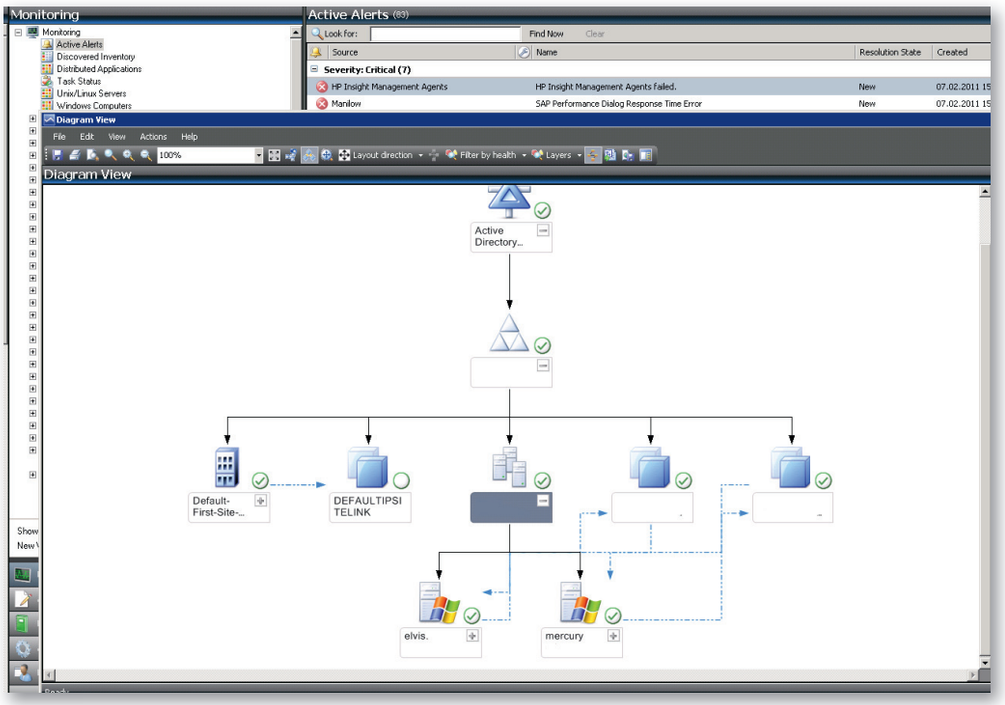
Alarme und mehr

Nachdem ein Fehler festgestellt wurde, kann ein bei beiden Produkten ähnlicher Alarm gegeben sowie eine automatisierte Problemlösung angestoßen werden. Ein einfaches Beispiel wäre ein SSH-Dienst, der auf einem Linux-System regelmäßig abbricht. Hier kann ein Administrator benachrichtigt werden, der den Fehler manuell behebt, oder man automatisiert die Aufgabe und lässt den Prozess durch das Management-System neu starten. In Icinga übernimmt das der „Event Handler“, in SCOM sind dafür „Diagnostic“ beziehungsweise „Recovery Tasks“ zuständig. Der Wunsch nach einer fehlerfreien IT ist so zwar noch nicht erfüllt, durch automatisierte Workarounds ist jedoch ein weiterer Schritt getan.

Ein Überwachungssystem steht im Allgemeinen nicht alleine da. Daher ist eine Ankopplung an andere Systeme von Bedeutung. Als bestes Beispiel wären Konnektoren für Ticketsysteme zu nennen. Hier bietet SCOM fertige Schnittstellen zu bekannten Lösungen wie das „Action Request System“ (AR System) von Remedy. Da die meisten Systeme auch E-Mail-Nachrichten in Tickets umwandeln können, ist über diesen Weg ebenso eine Verknüpfung mit Icinga möglich.

Hierarchien

In größeren Umgebungen ist ein hierarchischer Aufbau der Monitoring-Lösung wünschenswert. So wären standortbezogene Management-Server denkbar, die ihren Status einem zentralen Server melden. Dadurch wird auch die Last verteilt. Icinga unterstützt diesen Ansatz durch diverse Add-ons wie NSCA oder mod_gearman. Der Operations Manager lässt sich ebenfalls verschachteln. Alternativ ist auch der Einsatz von Gateway-Servern möglich, die die Meldungen von einem Standort sammeln und komprimiert weiterleiten. *(ue)*



Die Verwaltungskonsole von Microsofts System Center Operations Manager. Im Vordergrund ist der automatisch erkannte Aufbau des Active Directory abgebildet.

To do's im Vorfeld

- Klar definieren, was und wie tief überwacht werden soll;
- Lizenzkosten den geschätzten Aufwänden gegenüberstellen;
- Automatisierung von Problemlösungen vorantreiben;
- Monitor nicht als eigenständiges System betrachten, sondern als Komponente in einer Systemlandschaft (Ticket-Tools);
- gegebenenfalls Produkte kombinieren, zum Beispiel über SCOM2Nagios.

***Markus Bäker** ist Senior Systemingenieur bei der TechniData IT-Service GmbH in Markdorf am Bodensee.