LANline

Nr. 7, Juli 2004

30673 ISSN 0942-4172

Das Magazin für Netze, Daten- und Telekommunikation www.lanline.de

Sonderdruck für Sector Nord

IM TEST: SNAGVIEW VON SECTOR NORD

Verwaltung auf Linux-Basis

Die Systemmanagementlösung Snagview erweitert das Open-Source-Tool Nagios um verschiedene Agenten. Der Anbieter Sector Nord vertreibt Snagview als Bundle mit Servern von Fujitsu-Siemens einschließlich Vor-Ort-Installation und einführender Schulung. Die soll sicherstellen, dass auch weniger Linux-erfahrene Administratoren schnell damit zurecht kommen.

Mit dem Systemmanagement-Tool Snagview will Sector Nord das Monitoring von Servern, aktiven Netzkomponenten und geschäftskritischen Anwendungen zentralisieren. Als Basis dient die Open-Source-Lösung Nagios, die der Hersteller angepasst und um verschiedene Agenten erweitert hat. Es handelt sich um ein junges Produkt, die Entwicklungsarbeiten schreiten stetig voran. Derzeit lässt sich Snagview für die Überwachung von Servern einsetzen, die unter Windows, Netware, Linux, Solaris oder Reliant Unix laufen. Auch für SNMP (Simple Network Management Protocol) und die Datenbank von Oracle sind Agenten vorhanden. Der Agent für Microsoft SQL Server befindet sich derzeit in der Beta-Testphase und soll demnächst verfügbar sein, solche für Microsoft Exchange und Open VMS sind ebenfalls in Arbeit.

Sector Nord konzentriert sich auf das reine Monitoring. Eine Datenbank zum Beispiel könnte aus Mangel an Festplattenplatz stehenbleiben ("Out of Disk Space"). Dann bringt ein Neustart des Dienstes nichts. Deshalb hat Sector Nord die Funktion von Nagios, nicht mehr verfügbare Services automatisch neu zu starten, bei Snagview deaktiviert.

TESTUMGEBUNG Für den LANline-Test stellte Sector Nord einen Snagview-1.0-Server zur Verfügung, der auf einem Econel-30-System von Fujitsu-Siemens lief. Der Rechner war mit einem IDE-Hardware-RAID und Suse Linux Enterprise Server 8 (SLES 8) als Betriebssystem ausgestattet. Die Testumgebung bestand aus drei Servern mit Windows 2003, Windows 2000 und Suse Linux 8 sowie einem SNMP-fähigen Fast-Ethernet-Switch.

Das Snagview-System erreichte das Testlabor vollständig vorinstalliert. Ein Spezialist von Sector Nord führte an einem Vormittag die Basisinstallation durch. Der erste Schritt bestand darin, die Testsysteme über den Switch miteinander zu verbinden und per Ping zu prüfen, ob alle Netzwerk-Links korrekt funktionieren. Dann ging es daran, die Konfigurationsdateien des Snagview-Servers zu bearbeiten. Sie legen unter anderem fest, welche Dienste und Funktionen Snagview auf den hier eingetragenen Systemen überwacht. Zu den wichtigsten Dateien zählen die hosts.cfg mit den Servereinträgen, die hostgroup.cfg mit den Servergruppen – zum Beispiel nach Betriebssystemen unterteilt – und die services.cfg. Diese Datei enthält alle nötigen Informationen, um etwa per Ping die Verfügbarkeit von Servern zu überwachen oder Festplattenauslastung und CPU-Performance zu kontrollieren. Bei Webservern überwacht Snagview nicht nur die Verfügbarkeit des Webserverdienstes, sondern auch einzelne Webseiten.

Der Anschaulichkeit dienen zahlreiche Bilder und Symbole

VERWALTUNG Die Konfiguration von Snagview erfolgt bislang, abgesehen von SNMP, ausschließlich textbasiert. Der Administrator muss die Parameter für die zu überwachenden Server und Dienste in die verschiedenen Config-Dateien händisch eintragen. Befehlszeilen-Freaks kommen dabei per Copy and Paste sicherlich ganz flott voran. In größeren Netzwerken mit sehr vielen zu überwachenden Servern, Netzkomponenten und Anwendungen ist dieses Vorgehen allerdings nicht sonderlich komfortabel. Künftig soll Snagview deshalb über das Webinterface nicht nur das Monitoring, sondern auch die Konfiguration der Systeme durchführen können.

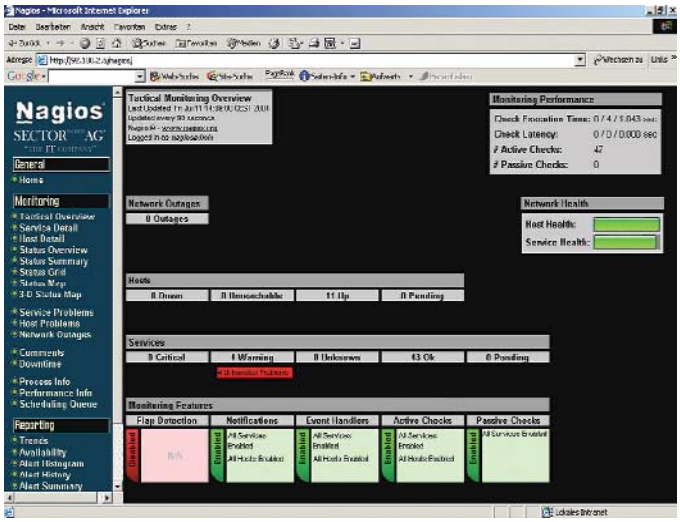
Umständlich ist bisher auch die Konfiguration von Netzwerk-Switches, da der Administrator jeden Link einzeln für die Überwachung parametrisieren

muss. Hier verspricht Sector Nord ebenfalls Abhilfe. Geplant ist, dass sich künftig mehrere Links gleichzeitig in einem Schritt konfigurieren lassen. Auch die Übersichtlichkeit soll dann zunehmen. So muss ein Administrator, der die Link-Geschwindigkeit der Switch-Ports überwachen will, bisher die Übertragungsrate in der Textdatei in Bit-Werten angeben. Bei den vielen Nullen kann da schnell ein Fehler passieren. Bislang speichert Snagview alle Informationen in Textdateien ab. Diese lassen sich für eine weitere Auswertung in Datenbanken importieren. Eine Version, die die erfassten Daten direkt in einer Datenbank ablegt, ist in Vorbereitung.

MONITORING Nach den Einträgen für die zu überwachenden Host-Systeme galt es, die Agenten zu installieren. Dies ging zügig und ohne Probleme vonstatten. Es folgte die Definition der Überwachungsregeln: Überwachung der Host- und Switch-Verfügbarkeit per Ping-Befehl, Kontrolle der Link-Übertragungsrate auf den Switch-Ports, Überwachung der Festplattenauslastung aller Host-Partitionen.

Der Administrator legt fest, welches Ereignis welche Alarmkategorie auslöst. Dadurch lässt sich die Häufigkeit der Benachrichtigungen steuern. Snagview verwendet unter anderem die Kategorien Warning, Critical, Unknown, Recoverable, Down und Unreachable. Zudem ist es möglich, Zeitfenster für die Überwachung vorzugeben und zum Beispiel Datenbanken während geplanter Wartungszeiten aus dem Monitoring herauszunehmen. Die Konfigurationsdateien geben auch vor, auf welchem Weg Snagview den Systemverwalter bei kritischen Ereignissen benachrichtigt. Zur Wahl stehen unter anderem E-Mail und SMS. Traps verschickt der SNMP-Agent von Snagview bislang nicht.

Mit dem Webinterface lassen sich alle von Snagview kontrollierten Systeme einfach und übersichtlich überwachen. Die Status-Map stellt die Systeme grafisch dar. Der Administrator wählt hierfür unterschiedliche Symbole und mit der so genannten "Layout Method" verschiedene Sichten, um sich zum Beispiel nur eine bestimmte Host-Gruppe anzeigen zu lassen. Mithilfe von Parent-Beziehungen sind verschachtelte Hierarchien möglich. Das verbessert die Übersichtlichkeit in großen Netzen. Eine automatische Netzwerk-Discovery, wie sie andere Tools bieten, hat Sector Nord bislang nicht implementiert.



Mit dem Tactical Overview behalten Systemverwalter auch in größeren Netzwerken alle wichtigen Vorgänge im Blick

TACTICAL OVERVIEW Zu den wichtigsten Funktionen von Snagview zählt der Tactical Overview: Er zeigt auf einen Blick, wo es brennt. Vor allem in größeren Netzen sehen Administratoren damit sofort, welche Systeme sich in einem kritischen Zustand befinden. Eine detaillierte Auskunft über den aktuellen Zustand der überwachten Komponenten liefern die Menüpunkte "Service Detail" und "Host Detail". Sie zeigten während der Tests den Zustand der Systeme immer korrekt an und lösten bei Überschreitung der definierten Schwellwerte zuverlässig den gewünschten Alarm aus. Die umfassendsten Informationen findet der Administrator im Event-Log, das via Web-GUI zugänglich ist. Sobald es vollläuft, archiviert die Lösung das alte Log und legt eine neue Datei an. Snagview kann verschiedene Reports erstellen, so über die Verfügbarkeit der Systeme. Eine Auswertung ist aber bislang nur bezüglich der Häufigkeit von Alarmmeldungen möglich. Wünschenswert wären weiter gehende Korrelationsfähigkeiten, um zum Beispiel zu erfahren, wie voll die Festplatten waren, als ein Alarm erfolgte.

PREISE Die Preise hat Sector Nord flexibel gestaltet: Das Basispaket besteht aus einem Bundle mit Serverhardware und vorinstallierter Snagview-Software. Es kostet inklusive Windows- und Linux-Agenten 4999 Euro mit dem Tower-Server Econel 30 und 5999 Euro mit der Rack-Version RX100, beide von Fujitsu-Siemens Computers. Die Systemagenten für Reliant Unix, Solaris und Netware schlagen jeweils mit 1499 Euro zu Buche, der Oracle-Agent mit 1999 Euro. Für 2499 Euro sind die SNMP- und die Baan-IV-Komponenten erhältlich. Die Lizenzen sind unlimitiert: Der Administrator darf jeden Agenten auf beliebig vielen Systemen installieren.

Im Grundpreis enthalten ist die Vor-Ort-Installation sowie ein Tag Basisschulung und zusätzlich jeweils ein halber Tag Training pro Agent. Für die schnelle Systemwiederherstellung liefert Sector Nord ein Image der Installation mit. Ebenfalls inklusive sind drei Jahre Vor-Ort-Support für die Serverhardware. Für ein Jahr Support der Basisinstallation berechnet der Anbieter 799 Euro. Der entsprechende Preis für den SLES 8 beträgt 849 Euro. Der Agenten-Support kostet zwischen 270 und 450 Euro jährlich.

FAZIT Das Einrichten der Überwachungsfunktionen von Snagview sollten Unternehmen zumindest im ersten Schritt den Spezialisten von Sector Nord überlassen. Denn bei der bislang erforderlichen textdateibasierten Konfiguration können sich schnell Fehler einschleichen, wenn die nötige Erfahrung fehlt. Der Hersteller hat immerhin in Aussicht gestellt, dass die Konfiguration künftig auch über das Webinterface möglich sein soll. Verbesserungspotenzial besteht zudem bei den Reporting-Funktionen, die bislang keine weiterführenden Korrelationen erlauben.

Gut gelungen ist die Weboberfläche. Sie ist übersichtlich gestaltet und leicht zu bedienen. Administratoren dürften mit den verschiedenen Monitoring-Aufgaben deshalb schnell zurechtkommen. Für die Konfiguration ist dagegen schon eine Portion Linux- und Netzwerk-Know-how erforderlich.

(Christoph Lange/wg)

Info: Sector Nord
Tel.: 04488/52620
Web: www.sectornord.de