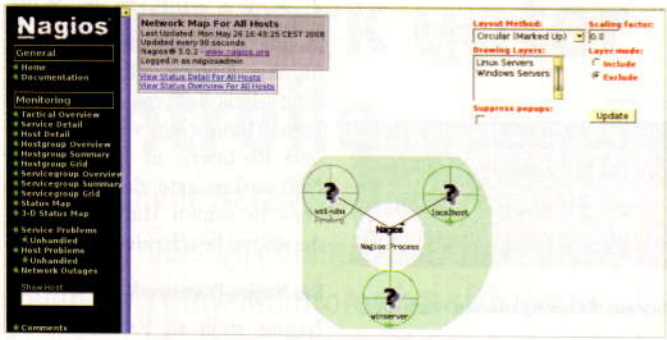
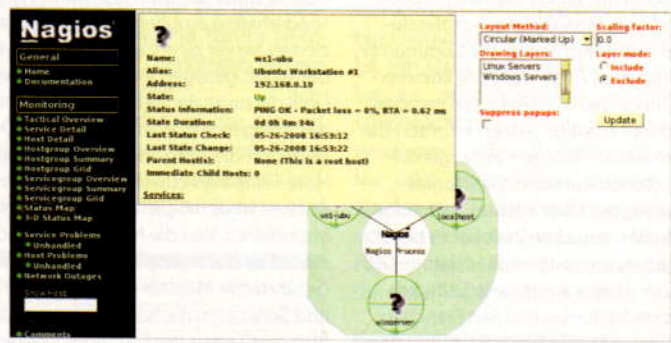


In der Status-Map visualisiert Nagios sehr schön die Infrastruktur Ihres lokalen Netzes

bekannt zu machen. Für die eigentlichen Prüfungen sind die Check-Plugins (Nagios-Plugins) verantwortlich, von denen Sie übrigens auch jederzeit eigene in einer beliebigen Sprache entwickeln können, da sämtliche Schnittstellen sauber definiert sind. Die saubere Definition der Schnittstellen hat schon vor Jahren dazu geführt, dass die Entwicklung des Nagios-Frameworks sowie der Check- und Prüf-Plugins getrennte Wege nimmt. Das eigentliche Nagios-Paket von **www.nagios.org** enthält lediglich den Daemon sowie die CGI-Skripte des Webinterfaces. Sinnvoll einsetzen können Sie Nagios daher erst, wenn Sie mindestens die Basis-Plugins von **www.nagios.org** installiert haben. Weitere Plugins finden Sie unter **www.nagiosplugins.org** oder **nagiosplug.sourceforge.net**. Außerdem gibt es zahlreiche Addon-Module, mit denen Sie Nagios ebenfalls erweitern können. Die CGIs des Webinterfaces kommunizieren mit Nagios über eine named pipe (external command file). Die von den Plugins durchgeführten Tests oder Prüfungen bilden die Grundlage der Nagios-Überwachungsstrategie. In Abhängigkeit des Rückgabewertes einer solchen „Prüfung" (z.B. Erfolg oder Misserfolg) reagiert das Nagios-Framework je nach gewählter Konfiguration mit einer breiten Palette von Möglichkeiten von der stillschweigenden Kenntnisnahme bis hin zur aktiven Schadensabwehr.

Nagios' Konfigurationsdateien

Die Konfigurationsdateien sind modular aufgebaut und ermöglichen die Überwachung einer sehr großen Anzahl von Diensten und Hosts. In komplexen Umgebungen lässt sich mit Nagios sogar verteiltes Monitoring realisieren. Auch für die Benachrichtigung des Administrators stehen ausgefeilte Optionen zur Verfügung, etwa per Mail, SMS oder Win-PopUp. Außerdem steht dem Administrator das Webfrontend zur Verfügung, das nicht nur zur Konfiguration von Nagios dient, sondern dem Administrator mit Ampelfarben eindeutig signalisiert, bei welchen Diensten oder Hosts Achtsamkeit geboten ist oder Handlungsbedarf besteht. Mit Netzwerkgrafen, Trends oder Statistiken lassen sich Statusänderungen bei Hosts oder Diensten detailliert zurückverfolgen. Weiter dient das Webfrontend mit seiner Status Map auch zur komfortablen Visualisierung der Netzwerktopologie und erlaubt zudem die Kontrolle und direkte Einflussnahme auf das Netzwerk-Tool.



Bleiben Sie in der Status-Map mit der Maus über einem der Server stehen, zeigt Nagios Details des betreffenden Servers an

Nagios überwacht

Wie beschrieben, setzt sich das Nagios-Framework aus Konfigurationsdateien, Prüf-Programmen und weiteren, nicht direkt zum Nagios-Paket gehörenden Nagios-Plugins zusammen. Mit Hilfe der modular aufgebauten Konfigurationsdateien im Kern des Konstruktes machen Sie Nagios die zu überwachenden Objekte bekannt. Die wichtigsten Nagios-Konfigurationsdateien sind „nagios.cfg" und „cgi.cfg", die Sie bei jeder Nagios-Installation finden. Je nach Komplexität der Überwachungsstruktur gibt es auch noch weitere. Dazu gesellen sich die in Anzahl und Bezeichnung variierenden Objektdefinitionsdateien, in denen Sie die zu überwachenden Objekte definieren. Sie können solche Objektdefinitionen für Rechner (host), Dienste (service), Kommandos (command), Kontakte (contact) und Kontaktgruppen (contactgroup) und noch einige Objekttypen mehr vornehmen. Die wichtigsten sind naturgemäß „Host" und „Service". Ein „Host" ist für Nagios stets das grundlegende Objekt, aus dem sich andere Objekttypen ableiten. Das Definieren eines zu überwachenden Hosts ist relativ einfach. Ein „Host" kann so ziemlich jedes Gerät sein, das über eine eigene IP-Adresse verfügt. Ein „Service" ist im Nagios-Jargon allerdings nicht ganz so eindeutig, denn Nagios meint mit einem Service nicht etwa einen Netzwerkdienst oder zu startenden Prozess, sondern einen einem ausgewählten Host zugeordneten Test, für dessen Durchführung ein extra definiertes „Kommando" oder ein Plugin verantwortlich ist.

Prüfen und Abwägen

Letztendlich funktioniert die Überwachung von Netzwerkobjekten wie Hosts und Services durch Nagios dadurch, dass Nagios die Statusmeldungen der von den Nagios-Plugins und -Skripten durchgeführten Tests überwacht und auswertet. Soweit die Theorie. Das jeweilige Ergebnis (Rückgabewert eines Plugins) fungiert dann als Auslöser für das Eingreifen (event handler) oder das ausgefeilte Benachrichtigungssystem. Stößt Nagios auf eine Zustandsänderung, erhöht es beispielsweise auch die „Frequenz" der durchgeführten Service-Checks, was natürlich problematisch ist, wenn ein Mitarbeiter einfach seinen Rechner herunterfährt, ohne Nagios „davon zu unterrichten". Selbstverständlich obliegt es nicht dem Anwender oder dem Host, sich „Gedanken" um Nagios zu machen. Tatsächlich testet Nagios beim Fehlschlagen eines Service-Checks zunächst immer, ob die Ursache des Fehlschlagens eventuell in einer Reihe von „typischen" vorgelager-

Host-Checks bei Nagios 3

Bei Nagios 2 prüft Nagios Hosts in der Regel nur dann, wenn ein Service-Check ins Leere gelaufen ist. Dieser Logik lag der Gedanke zugrunde, dass das System funktionstüchtig sein muss, wenn der getestete Service den Status OK zurückliefert. Anders herum führt Nagios einen Host-Check aus, sollte ein Service-Check negativ ausfallen. Zwar lassen sich auch bei Nagios 2 Host-Checks regelmäßig anstoßen, allerdings setzt Nagios 2 dann alle anderen Prüfungen aus, bis es den Zustand des Hosts für „geklärt" hält. Außerdem prüft Nagios 2 im Fehlerfall nicht nur den betreffenden Host, sondern alle in der Host-Map bekannten Hosts. Leider führt dieser Umstand in sehr großen Netzen dazu, dass Nagios minutenlang keine Service-Checks mehr ausführt. Nagios 3 dagegen behandelt, um diesem Umstand abzuhelfen, Host-Checks wie Service-Checks und kann diese auf Wunsch auch regelmäßig auslösen. Dadurch betrachtet Nagios 3 den Status eines Hosts für einige Sekunden als gültig und muss daher keinen weiteren Host-Check ausführen. Stellt Nagios 3 allerdings ein Host-Problem fest, überprüft auch Nagios 3 weitere betroffene Hosts ebenfalls.