Nagios

Jens Link jenslink@quux.de

September 2008

Wer bin ich?

- Freiberuflicher Consultant
- Schwerpunkt: komplexe Netzwerke, Netzwerksecurity, Netzwerkmonitoring, Troubleshooting
  - Routing und Switching (Cisco)
  - Linux (seit > 12 Jahren)
  - Netzwerkmonitoring (Nagios, Cacti)
  - DNS, DHCP, RADIUS, SQUID, ...
  - Firewalls (Linux, Check Point)

Was ist Nagios überhaupt? (I)

- Nagios ist ein sehr flexibles und skalierbares webbasiertes System zum Monitoring von Hosts und Diensten
- Ursprünglich hieß das Projekt NetSaint, musste aber wegen Namensproblemen umbenannt werden
- Nagios setzt sich aus den Worten **N**etwork und H**agios** zusammen
- Nagios sollte auf allen *NIX Plattformen lauffähig sein
- Überwachen lassen sich eine Vielzahl von Systemen, z.B. *NIX, Windows, Cisco, ...

Was ist Nagios überhaupt? (II)

Die Flexibilität von Nagios zeigt sich in

- einer Plugin-Architektur. Plugins dienen der Überwachung und lassen sich in jeder beliebigen Sprache schreiben. Es gibt eine Vielzahl fertiger Plugins.
- der Möglichkeit SNMP und Syslogmeldungen auszuwerten.
- Hosts und Dienste in Gruppen zu gliedern
- Abhängigkeiten zwischen Host zu berücksichtigen
- der Möglichkeit viele unterschiedliche Alarmierungsgruppen und Arten einzurichten.
- der Möglichkeit Reports zur Verfügbarkeit aus den gewonnen Daten zu erstellen.

Nagios im Vergleich zu anderer Software

- Gegenüber vielen anderen (kommerziellen) Lösungen bietet Nagios durch seine Architektur eine unheimliche Flexibilität.
- Wie jede Software kommt Nagios mit einem Preis: Auch wenn die Software nichts kostet muss man Zeit und Arbeit in die Konfiguration und die Wartung stecken.
- Nagios dient vorrangig der Überwachung der Verfügbarkeit eines Dienstes, über zusätzliche Tools kann man aber die gewonnen Daten auch über einen längeren Zeitraum grafisch darstellen.
- Konfiguration von Nagios geschieht über Textdateien. Es gibt keine (brauchbare) GUI.

Checks

Checks werden über Plugins realisiert und können

- lokal vom Nagios Host ausgeführt werden und greifen über das Netz auf andere Hosts zu, z.B.
  - Ist der Webserver verfügbar? (PING, HTTP, HTTPS)
  - Kann ich den Router zum Internet erreichen?
- auf entfernten Rechnern laufen über eine entsprechende Software (NRPE, NSCA) ausgeführt werden.
  - Wie sieht die Auslastung der Festplatten aus?
  - Läuft ein bestimmter Dienst noch?

Alarmierungen (I)

Nagios bietet die Möglichkeit

- verschiedene Gruppen für verschieden System einzurichten, also z.B. je eine für DB-Admins, Netzwerkadmins, Firewalladmins, Windowsadmins, ...
- verschiedene Gruppen für verschieden Zeiten einzurichten, also z.B. Alarmierung während der normalen Arbeitszeiten eine Adresse, außerhalb der Arbeitzeit an eine andere Adresse.

Alarmierungen (II)

Neben **e-Mail** können auch folgende Möglichkeiten der Benachrichtigung verwendet werden:

- SMS
- Jabber
- IRC
- ...

Der Phantasie sind keine Grenzen gesetzt (Nagios + Asterisks?).

Plugins (I)

Die eigentlichen Tests werden über Plugins realisiert. Im einfachsten Fall ist ein Plugin ein Shell-Script, welches einen von 3 Werten zurückliefert:

- Ok
- Nicht Ok
- Unbekannt

Standardmäßig wird eine Vielzahl von Plugins mitgeliefert, viele andere Plugins findet man auf `http://www.nagiosexchange.org`.

Plugins (II)

Mit die mitgelieferten Plugins sind u.A. folgende Tests möglich:

- CPU-Auslastung
- Speicher-Auslastung
- Festplatten-Auslastung
- SSH, SMTP, HTTP(s), ...

Bei Plugins kann man auch durchaus auch ältere Versionen einsetzen und ein fertiges Paket für die gewählte Distribution verwenden.

Konfiguration (I)

```
define host{
        use                     linux-server
        host_name               smokehead.quux.de
        alias                   smokehead.quux.de
        address                 80.244.248.190
        parents                 localhost
        }
```

Konfiguration (II)

```
define service{
        use                             generic-service
        host_name                       smokehead.quux.de
        service_description             PING
        check_command                   check_ping \
                                        !100.0,20%!500.0,60

        }
```

Konfiguration (III)

```
define contact{
        contact_name                    nagiosadmin
        use                             generic-contact
        alias                           Nagios Admin
        email                           jenslink@quux.de
        }
```

Konfiguration (IV)

```
define timeperiod{
        timeperiod_name 24x7
        alias           24 Hours A Day, 7 Days A Week
        sunday          00:00-24:00
        monday          00:00-24:00
        tuesday         00:00-24:00
        wednesday       00:00-24:00
        thursday        00:00-24:00
        friday          00:00-24:00
        saturday        00:00-24:00
        }
```

Demo

Fragen?

Fragen?

Danke

Ich danke für die Aufmerksamkeit.

Kontakt

eMail	jenslink@quux.de
Jabber	jenslink@guug.de
PGP Fingerprint	D9FF E215 6686 6194 FFC8
	A135 19CF A676 DB85 EF91

Werbung (Teil II)

- Jeden 1. Donnerstag im Monat: Treffen der sage@guug-Berlin. Details unter `http://www.guug.de/lokal/berlin`
- Im Oktober: Vortrag an der TU-Berlin zum Thema:

OTRS - Open Ticket Request System