



Qualitätssicherung mit Nagios bei tubIT

tubIT Stammtisch 07.05.2009

Eckart Fellner

IT Dienstleistungszentrum der TU Berlin



Qualitätssicherung mit Nagios bei tubIT

- Motivation
- Nagios
 - Objekte
 - Plugins
 - Tests
- Ausblick

Vormittag, 10 Uhr

Der Chef tobt ...

... seine Präsentation liegt auf dem
WWW-Server, der nicht antwortet ...



Also wird die Hotline angerufen,
die Hotline fragt den Webmaster:

Der WWW-Server funktioniert tadellos.
Also liegt es wohl am Netz ?
Oder am AFS, LDAP, Kerberos ?



Die Suche dauert länger, als die Lösung.

Nagios® ist ein einfaches, aber sehr flexibles Werkzeug zum Testen von Services und Rechnern ('hosts').

Vorteile:

- Nagios kennt nur vier Zustände:
 - OK, Warnung, kritisch, unbekannt
- Nagios ist flexibel, da eigene Tests ('plugins') sehr einfach integriert werden können.

Nachteile:

- Aufwändige Konfiguration
- Gefahr der Überflutung mit Statusmeldungen
- Wird leicht unübersichtlich

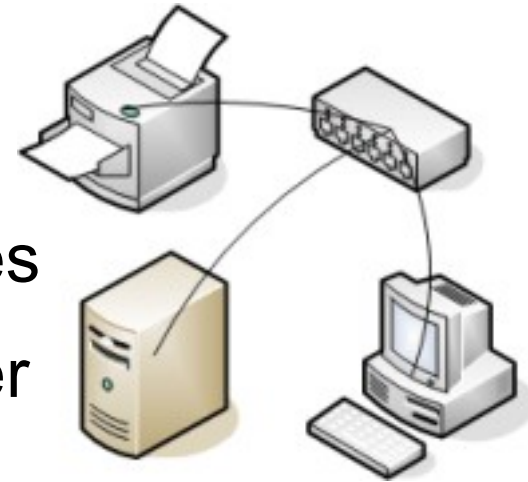
Zielgruppe sind Systemadministratoren

Nagios kennt im Wesentlichen folgende Objekte:

- Hosts und Host Groups
- Services und Service Groups
- Contacts und Contact Groups
- Commands
- Timeperiods

Hosts sind ein zentrales Objekt von Nagios mit folgenden wesentlichen Attributen:

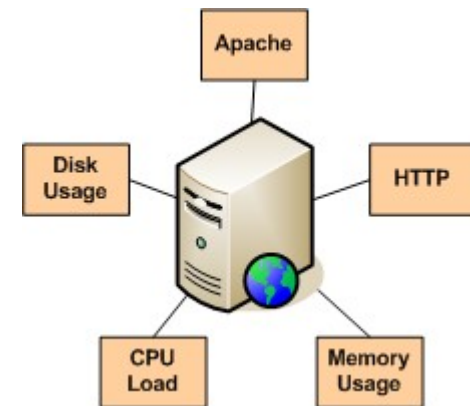
- Hosts sind typischerweise Geräte wie Server, PCs, Drucker, Router
- Sie bedienen einen oder mehrere Services
- Sie können in einer Beziehung zueinander stehen



Hosts können in *Host Groups* zusammengefasst werden.

Services sind an Hosts gebunden und können folgende Eigenschaften haben:

- Eigenschaften von Hosts, wie z.B. CPU-Auslastung
- Services des Hosts, wie z.B. Web- oder Maildienste



Services können in *Service Groups* zusammengefasst werden.

Contacts sind Personen, die über die Test-ergebnisse informiert werden.

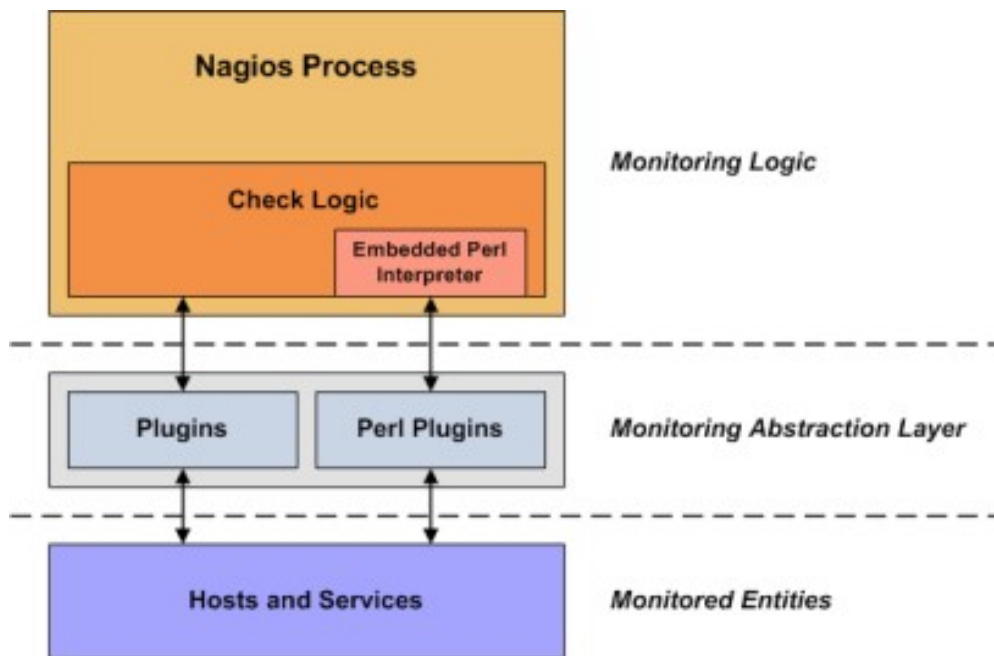
Die Benachrichtigung kann über verschiedene Wege erfolgen, z.B. E-Mail, SMS



Contacts können in *Contact Groups* zusammengefasst werden.

- Mit *Commands* werden (Test-) Programme definiert für
 - Host- und Service-Tests
 - den Versand von Benachrichtigungen
 - die Behandlung von Ereignissen
- In *Timeperiods* wird definiert, wann die Tests durchgeführt und zu welcher Zeit Nachrichten versandt werden sollen.

Nagios enthält nur Logik, aber keine eigenen Testprogramme.



Für die Tests benutzt Nagios (fast) beliebige externe Programme, die *Plugins*.

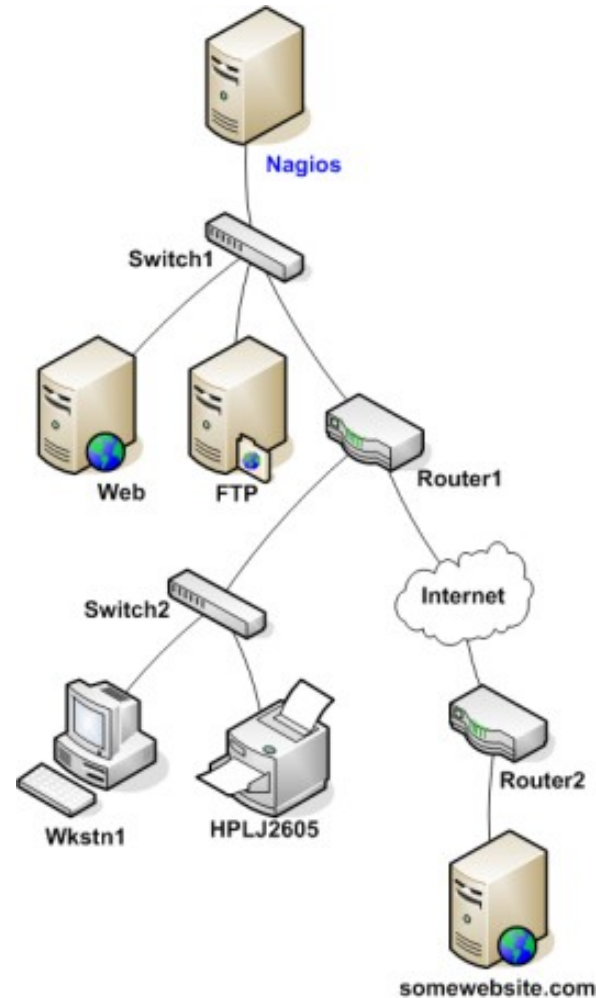
Vorteil:

- Alles, was programmiert werden kann, kann auch getestet werden.
- Die Plugins können unabhängig von Nagios (weiter-) entwickelt und an eigene Bedürfnisse angepasst werden.

Nachteil:

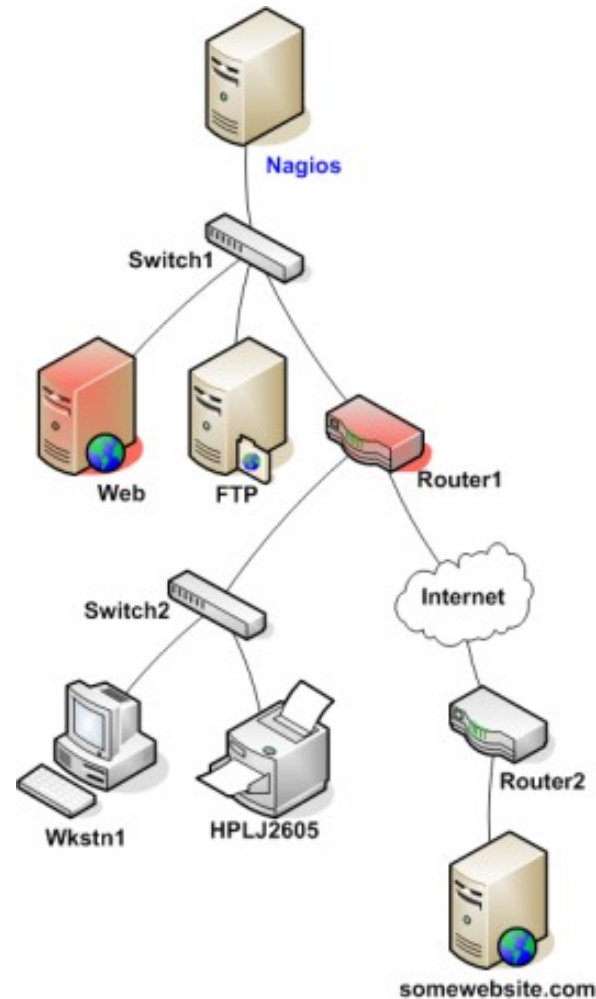
- Nagios „weiß“ nicht, was getestet wird und
- hat dementsprechend auch keine Logik, die Ergebnisse zu interpretieren.

In Nagios können Abhängigkeiten von Hosts und Services definiert werden.

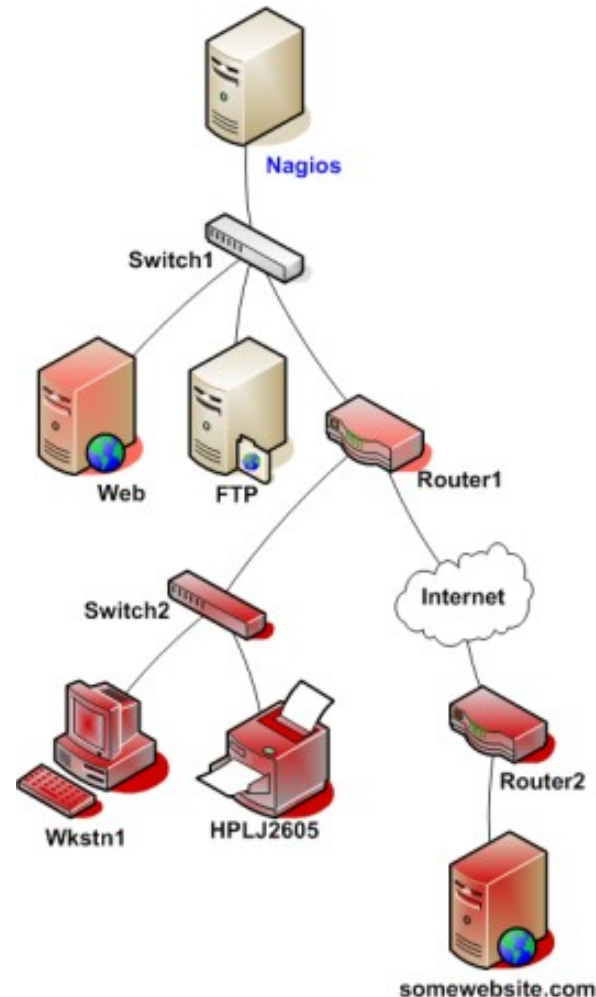


Nagios Tests

Fallen einzelne
Hosts oder
Services aus, z.B.
Server *Web* und
Router1 ...



... dann erkennt die Logik von Nagios selbständig die Nichterreichbarkeit der „dahinter“ liegenden Hosts und Services.



Derzeit werden

- 540 Hosts (davon 470 Netzwerkgeräte) und
- 976 Services

mit Nagios überwacht.

Der Zugang erfolgt für registrierte Nutzer mit dem tubIT-Account.

- Verbesserung der grafischen Darstellung
- Ergänzende Informationen zu Hosts
- Standard-Plugins zum Test von lokalen Services (Festplatte, Load, ...)
- Webinterface zum Verwalten von einfachen Standardaufgaben

Zugang:

<https://nag-2.tubit.tu-berlin.de/nagios/>

Accounts:

gast

fio
