

Serverüberwachung mit NAGIOS

Business-Online 2006: **linux.forum/nrw**

Referent: **Dr. Klaus Schmoltzi**
Warp9 GmbH, Münster
Email: klaus.schmoltzi@warp9.de
Internet: www.warp9.de

Serverüberwachung mit NAGIOS

- Agenda

- ➔ Motivation
- ➔ Monitoring
- ➔ Warum NAGIOS
- ➔ Erste Schritte
- ➔ Benachrichtigung
- ➔ Linux Systeme
- ➔ Windows Systeme
- ➔ SNMP
- ➔ Abschluss

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- **Zustand** der Server?
- **Erreichbarkeit** der Dienste?
- **Verfügbarkeit** des Netzwerkes?
- **Kümmerer**?
- **Erkennen** von Trends?
- **Einleiten** von Gegenmaßnahmen?

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- **Was** wird überwacht?
- **Womit** wird erfasst?
- **Wann** wird der Zustandswechsel permanent (Hard State)?
- **Wer** wird **wann** auf **welchen** Wegen informiert?
- **Wie** wird eskaliert?

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Ursprünglicher Name: **NetSaint**
- **Nagios = Network + Hagios** (Heiliger)
- Open Source Software (OSS)
- Unabhängig vom zu überwachenden System
- Modularer Aufbau
- Erweiterbar durch **Plugins**
- Reportingfunktionen
- Skalierbar

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- **Idee hinter NAGIOS**

- Nur Probleme werden gemeldet
- Komplette Übersicht im Web-Interface
- Durchführung von Checks zur Kontrolle der überwachten Systeme und Dienste
- Die Checks werden über Plugins realisiert
- Service-Checks in regelmäßigen Abständen
- Host-Checks nur bei Bedarf

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Wichtige Konfigurationsdateien

nagios.cfg	<i>Zentrale Konfigurationsdatei</i>
contacts.cfg	<i>Kontaktpersonen</i>
contactgroups.cfg	<i>Gruppe von Kontakten</i>
hosts.cfg	<i>Überwachte Systeme</i>
hostgroups.cfg	<i>Gruppe von Systemen</i>
services.cfg	<i>Überwachte Dienste u. Parameter</i>
checkcommands.cfg	<i>Def. der Checks mit entspr. Plugins</i>
misccommands.cfg	<i>Benachrichtigungsbefehle</i>
timeperiods.cfg	<i>Def. von Zeiträumen (z.B. 24x7)</i>

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Prinzip der Plugins
 - Externe Programme
 - Binaries, Skripte, Perl, Python, etc.
 - Definierte Rückgabewerte
 - **0 = OK**
 - **1 = WARNING**
 - **2 = CRITICAL**
 - **3 = UNKNOWN**

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Zustandswechsel

- Nagios kennt **Hard** und **Soft States**
- Der Zustand einer Abfrage (Check) geht nach einer Änderung in den Soft State
- Nach einer vorher bestimmten Anzahl an Wiederholungen wird aus einem Soft ein Hard State
- Erst nachdem ein Zustandswechsel in den Hard State übergegangen ist, wird versucht, eine Benachrichtigung zu senden

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Web-Interface

- Einfache Integration in Apache mit **nagios.conf**
- Über die Datei **cgi.cfg** werden die Zugriffsrechte auf bestimmte Bereiche des UI vergeben
- Die Zugriffsrechte werden durch die Parameter **authorized_for_** in der `cgi.cfg` festgelegt
- Es können **Rollen** für Benutzer definiert werden
- Der **htaccess**-Anmeldebenutzer wird an die `cgi.cfg` weitergegeben
- Integrierte **Reporting-Funktionen**

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Kontakt erstellen
 - **contacts.cfg** bearbeiten
 - Wichtige Parameter
 - contact_name
 - *_notification_period
 - *_notification_options
 - *_notification_commands
 - email

* kann sowohl **host**, als auch **service** sein

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- notification_options
 - service: **w**arning, **u**nknown, **c**ritical, **r**ecover
 - host: **d**own, **u**nreachable, **r**ecovery, **n**one
- Kontaktgruppe erstellen
 - **contactgroups.cfg** bearbeiten
 - Wichtige Parameter
 - contactgroup_name
 - alias
 - members

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Host erstellen
 - **hosts.cfg** bearbeiten
 - Wichtige Parameter
 - use *<Template-Name>*
 - host_name
 - address *<IP-Adresse>*
 - check_command *check-host-alive*
 - contact_group

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Abfragebefehl erstellen
 - **checkcommands.cfg** bearbeiten
 - Der eigentliche Befehl wird mit dem Aufruf eines **Plugins** definiert
 - Wichtige Parameter
 - `command_name`
 - `command_line` <Plugin mit Optionen>

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Beispiel mit **check_disk** Plugin
 - `./check_disk -w 35% -c 15% -p /dev/hda2`
 - Parameter
 - `-w <Prozent>` *Warning* falls geringer
 - `-c <Prozent>` *Critical* falls geringer
 - `-p <Partition>` Zu prüfende Partition
- Eintrag in **checkcommands.cfg**
 - `command_line $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$`
 - Der Strings **\$USER1\$** und **\$ARGx\$** sind Makrodefinitionen für Pfade und Variablen

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Abfrage erstellen
 - **services.cfg** bearbeiten
 - Host und Abfragebefehl werden verknüpft
 - Wichtige Parameter
 - use <Template-Name>
 - host_name <host1>, <host2>, ...
 - service_description
 - *_check_*
 - notification_*
 - check_period
 - contact_groups
 - check_command

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Details zu `*_check_*`
 - `normal_check_interval` <Minuten>
 - `retry_check_interval` <Minuten>
 - `max_check_attempts` <Anzahl>
- Details zu `notification_*`
 - `notification_interval` <Minuten>
 - `notification_period` <Timeperiod>
 - `notification_options` <Was wird gemeldet>
warning, unknown, critical, recover

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Email
 - Normaler Benachrichtigungsweg
 - Ausfall Email-Server oder Internet-Gateway?
 - **notify-by-email** in contacts.cfg
- SMS / Pager
 - Handy über USB oder serielle Schnittstelle am Nagios-Server
 - gnokii für Nokia Handys
 - **notify-by-epager** in contacts.cfg

Serverüberwachung mit NAGIOS

Zwei Möglichkeiten der Überwachung:

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

1. Nagios Remote Plugin Executor (NRPE)

- NRPE führt als Daemon auf Anfrage die vordefinierten Checks aus
- Auf dem Nagios-Server wird die Abfrage mit **check_nrpe -H <host> -c <check>** gestartet

2. Checks über SSH

- Die Plugins werden wie bei NRPE auf dem Remote Host installiert
- Über eine SSH-Verbindung werden die Plugins aufgerufen
- Aufruf vom Nagios-Server mit dem Plugin **check_by_ssh**

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Nagios Remote Plugin Executor (NRPE)
 - NRPE_NT Paket als Dienst installieren
 - Paket „Basic NRPE_NT Plug-ins“ installieren
 - Die Checks werden vollständig in der Datei **nrpe.cfg** konfiguriert und remote über **check_nrpe** vom Nagios-Server aufgerufen
 - Der NRPE-Dienst muss vom Administrator gestartet werden

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

- Überwachung von Switchen, USVs, ...
 - Simple Network Management Protocol
 - Plugin check_snmp
 - Übergabe von OID, Hostname und Community String
 - Nagios kann ein komplettes SNMP-Tool wie HP OpenView nicht vollständig ersetzen
 - Das Umsetzen von SNMP-Traps in Nagios-Events kann mit dem SNMP Trap Translator durchgeführt werden (www.snmpptt.org)

Serverüberwachung mit NAGIOS

- Motivation
- Monitoring
- Warum NAGIOS
- Erste Schritte
- Benachrichtigung
- Linux Systeme
- Windows Systeme
- SNMP
- Abschluss

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Weitere Infos: www.nagios.org
www.nagiosexchange.org

Download des Vortrags auf www.warp9.de