

Nagios / Icinga

OpenSource Network-Monitoring im großen Stil

Manuel Landesfeind

Institut für Mathematik
Georg-August-Universität Göttingen

This presentation can be used under the terms of the Creative-Commons CC-BY-SA 3.0 license

Nagios logo is owned by Nagios Enterprises; Icinga logo is owned by icinga.org

Jeder Admin braucht mal eine Kaffee-Pause!

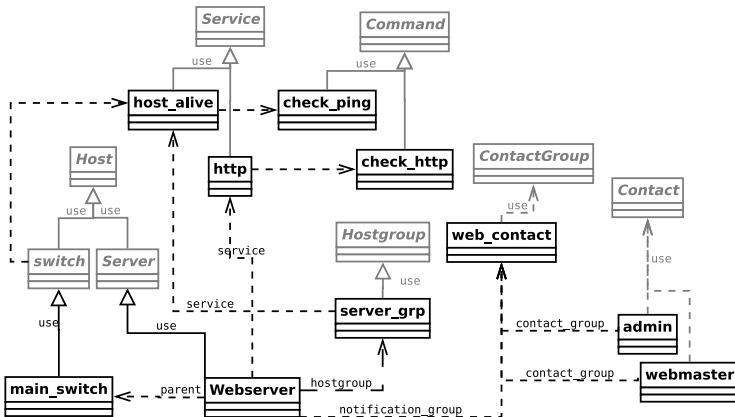
IT-Abteilungen haben **keine Zeit** für manuelles Monitoring.

Manuelles Monitoring ist in keinster Weise praktikabel.

⇒ **Automatisierte Lösungen müssen her!**

Nagios[®]

- ▶ Zentrale Instanz zum Überwachen eines Netzwerks (startet Tests, wertet sie aus und verwaltet die Ergebnisse)
- ▶ Webinterface präsentiert Ergebnisse (HTTP Authorisation)
- ▶ Enterprise Version enthält zusätzliche Features (z.B. Warnungen per SMS)
- ▶ “The Industry Standard In Open Source Monitoring” - nagios.org

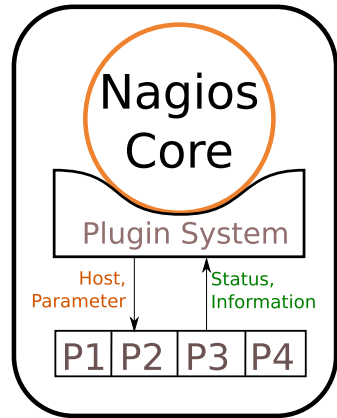


Wenige Basisobjekte umfassen z.B. Hosts, Services, Commands, Timeperiods.

Test Plugins sind eigenständige Programme

Exit-Status des Tests beschreibt Testergebnis (0=**OK**, 1=**WARNING**, 2=**CRITICAL**, 3=**UNKNOWN**).

Ausführliche Beschreibung des Ergebnisses über die Standard-Ausgabe (1. Zeile Zusammenfassung)



Beispiel-Programm:

```
#!/usr/bin/perl
use LWP::UserAgent;
my $IP = shift(@ARGV);

my $response = new LWP::UserAgent()->get($IP)
  or print "Can not connect: $!"
  and exit 2;

print $response->status_line;
my $code = substr( $response->status_line, 0, 3);

exit 2 if $code >= 500;
exit 1 if $code >= 300 && $code != 401;
exit 0;
```

Anlegen des Programms in der Konfiguration

```
define command{
  command_name check_http_responding
  command_line $USER1$/check_http_responding.pl $HOSTADDRESS$
}
```

- ▶ Simple Network Management Protocol (SNMP)
Abfrage von Statusinformation verschiedener Netzwerk-Geräte (v.a. Switches und Drucker), über RFCs standardisiert

- ▶ Nagios Remote Plugin Executor (NRPE)
Hosts führen Plugins aus und senden Informationen an Nagios (vgl. SNMP-Trap).



- ▶ Nagios-Fork von Mai 2009
- ▶ Nagios Entwickler integrierten langerwartete Features nur langsam
- ▶ Module und Tests vollständig kompatibel zu Nagios
- ▶ Features sind z.B.: einheitliche API, Unterstützung weiterer (Relationalen) Datenbanken, verbessertes Webinterface

Basis ist die Konfiguration eines DHCPD, welche geparkt und dann als Icinga Host Konfiguration geschrieben wird.

```
...
# Switches
group switch{
  host switch01 {
    hardware ethernet de:ad:be:ef:00:01;
    fixed-address 10.10.10.1;
  }
}

# Rechnerserver
group rechnerserver {
  host knecht1 {
    hardware ethernet de:ad:be:ef:00:02;
    fixed-address 10.10.10.10;
  }
}
...
```

dhcpd.conf

```
define host {
    use          linux-server
    host_name    switch01
    alias        switch01 (de:ad:be:ef:00:01)
    address      10.10.10.1
    hostgroups   switch
}

define host {
    use          linux-server
    host_name    knecht1
    alias        knecht1 (de:ad:be:ef:00:02)
    address      10.10.10.10
    hostgroups   rechnerserver
}
```

Icinga host.cfg

<erno> hm. I've lost a machine.. literally _lost_. it responds to ping, it works completely, I just can't figure out where in my apartment it is.

<http://bash.org/?5273>

Manuelle Listenführung über Standorte von Maschinen führen zu regelmäßigen Inventarisierung-Orgien...

...und welcher Admin läuft schon gern durch das ganze Haus?!

Allerdings ist jede Maschine über ihre MAC-Adresse eindeutig erkennbar (ja, ja... ich weiß!).

SNMP-fähige Switches liefern “Maschine-an-Port” Zuordnungen

.1.3.6.1.2.1.2.2.1.8.101 = INTEGER: up(1)	⇒ Port 1 online
.1.3.6.1.2.1.2.2.1.8.102 = INTEGER: down(2)	⇒ Port 2 offline
...	...
.1.3.6.1.2.1.17.4.3.1.2.233.183.201.186.20.58 = INTEGER: 1	⇒ de:ad:be:ef:13:37
.1.3.6.1.2.1.17.4.3.1.2.233.183.201.186.20.59 = INTEGER: 2	⇒ de:ad:be:ef:13:39
...	...

Zusammen mit einer (relativ) konstanten Port-Raum-Tabelle kann dies genutzt werden, um eine Liste aller Maschinen-Standorte zu generieren.

switch05	port	link up	name	ip	room	plug
	02	•	kopier	134.76.82.83	002	2
	03	•	blomer	134.76.82.0	003	1
	04	•	mathpc14	134.76.82.214	003	2
	05	•	fachschaftsrechner	134.76.82.0	004	1
	06	•	rcafete	134.76.82.48	004	2
	07	•	unkown host 00:0c:76:4d:e0:a9		117	1

Gleichzeitig wirkt dieser Lookup als Intrusion-Detektion.

Wann macht der Einsatz von Network-Monitoring Sinn?

Sowie auch nur **eine weitere Person** von der IT Abteilung abhängig ist!

Nagios/Icinga ab ca. 5+ Services (www-, ftp-, Festplatten-Server)

Integration in ein bestehendes Netzwerk

Basis-Konfiguration mit "20-Min-Quickstart-Quide". Konfiguration kann man beliebig komplex aufsetzen.

Nagios

- ▶ <http://www.nagios.de>
- ▶ http://nagios.sourceforge.net/docs/3_0
- ▶ <http://exchange.nagios.org>

Icinga

- ▶ <http://www.icinga.org>
- ▶ <http://www.youtube.com/user/Icinga>

SNMP

- ▶ <http://net-snmp.sourceforge.net>
- ▶ <http://sourceforge.net/projects/opensnmp>