

Einführung in Nagios

2006-03-02

Intro

Können Sie es sich leisten,
mit der Fehlersuche zu warten,
bis sich die Anwender über
nicht funktionierende Services
beschweren?

System- und Netzwerk- überwachung

Klassen von Überwachungswerkzeugen:

- Zustandsbeurteilung
 - gut/schlecht
- Visualisierung von Messwerten
 - z.B. Auslastung eines Interfaces über die Zeit
- Analyser
 - z.B. Protokollanalyser
 - Intrusion Detection Systeme (IDS)

Nagios: Design-Ziel

- gezielte Information des Administrators über Probleme
- Entlastung von den 99% OK-Zuständen

Beispiel Datensicherung:

- die tägliche OK-Meldung ermüdet
- Nagios-Prinzip:
 - Meldung, wenn Fehler beim Backup
 - Meldung, wenn Backup nicht durchgeführt
 - Admin kann sich bei Bedarf jederzeit über die Weboberfläche informieren.

... alles im grünen Bereich?

- Nagios konzentriert sich auf Ampelzustände:
 - grün = OK
 - gelb = WARNING
 - rot = CRITICAL
 - orange = UNKNOWN
- Verarbeitung von Performancedaten möglich, aber nicht Kernziel von Nagios.

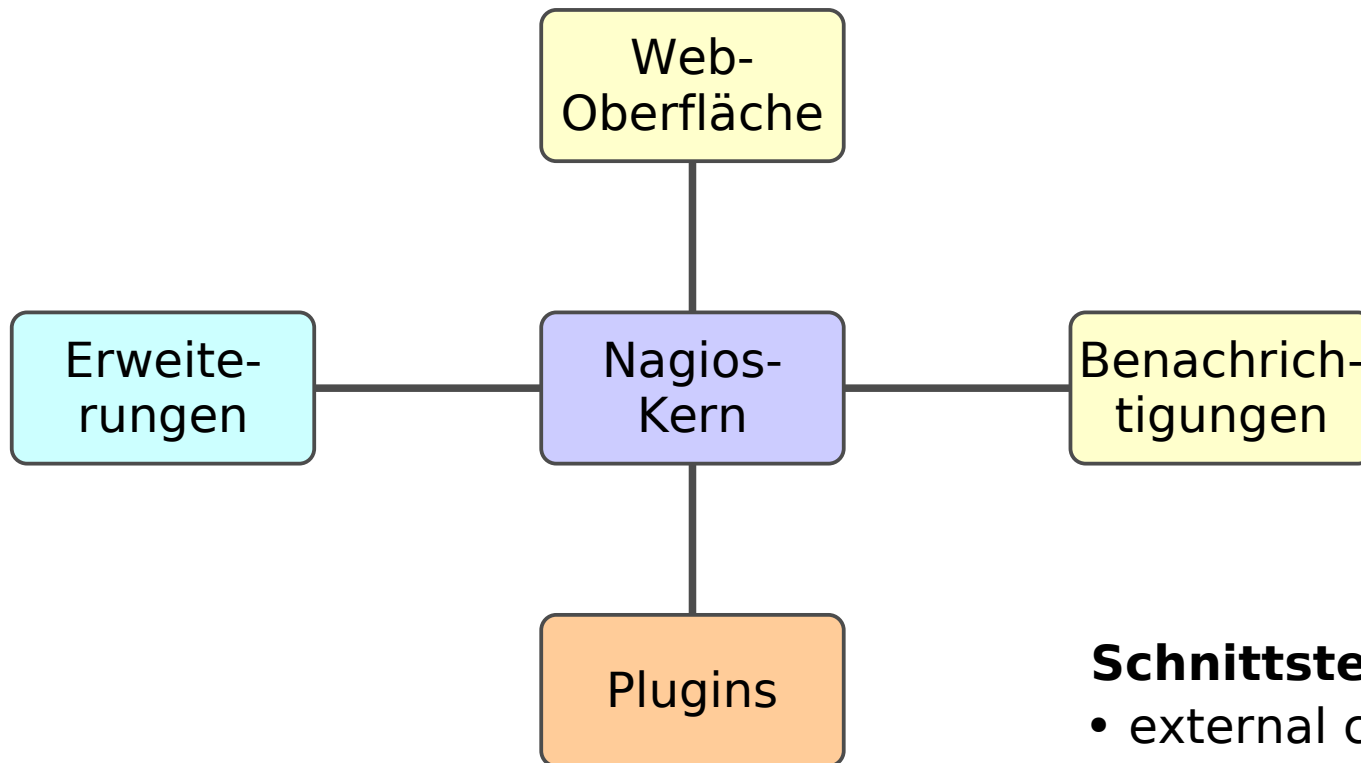
Andere Monitoring Tools

- Big Brother:
 - better than free license
 - MRTG
 - der Veteran
 - Cacti
 - flexibles, php-basiertes Werkzeug für die graphische Darstellung von Messwerten
- ... und viele andere ...

Nagios® : der Name

- ursprünglich: NetSaint
- Probleme mit gleichnamigen SecurityScanner
- Nagios = Network + hagios (griech: Heiliger)
- Der Name Nagios und das Nagios-Logo sind eingetragene Warenzeichen von Ethan Galstad

Nagios ist modular ...



Schnittstellen:

- external commands
- command file
- OCSP/OCHP
- event handler
- performance data
- nagios event broker

Plugins

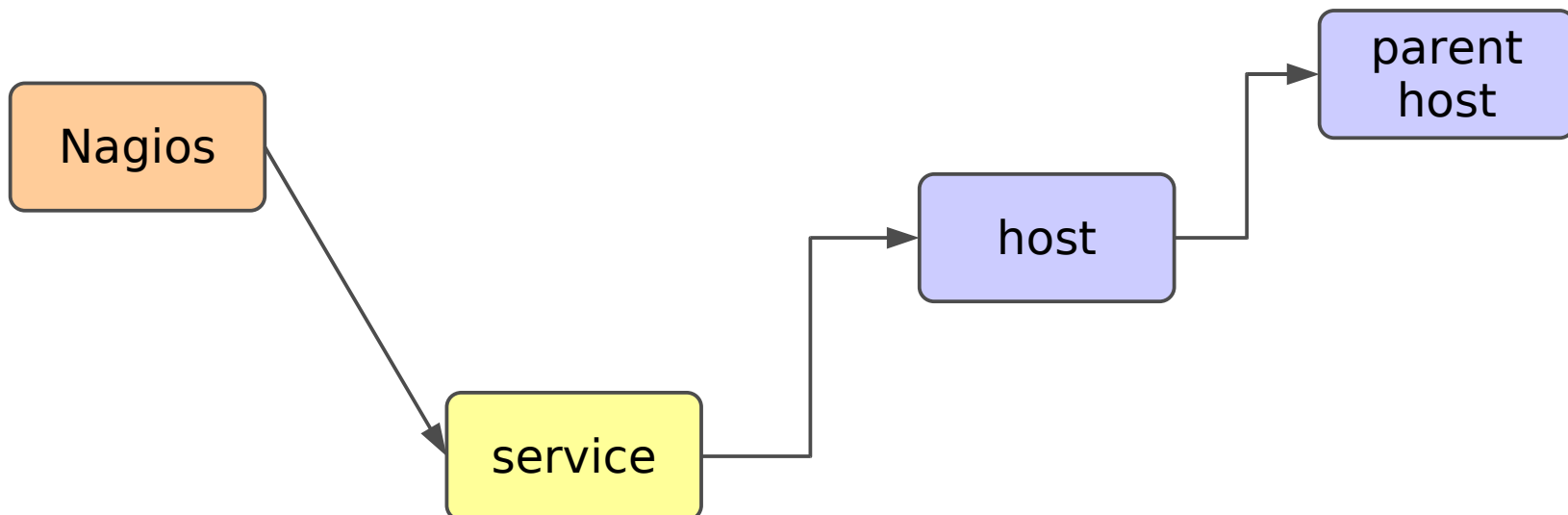
- externe, selbständige Programme
 - kommandozeilenorientiert
- Anforderung an Plugins:
 - einzeilige Textinformation für den Admin
 - Rückgabewert: 0=OK, 1=WARNING, 2=CRITICAL, 3=UNKNOWN
- Programm = ausführbar
 - kompilierte Programme, Shellskripte, Perl, Python, ... (unter Windows z.B. auch *.bat)

Was ist kritisch?

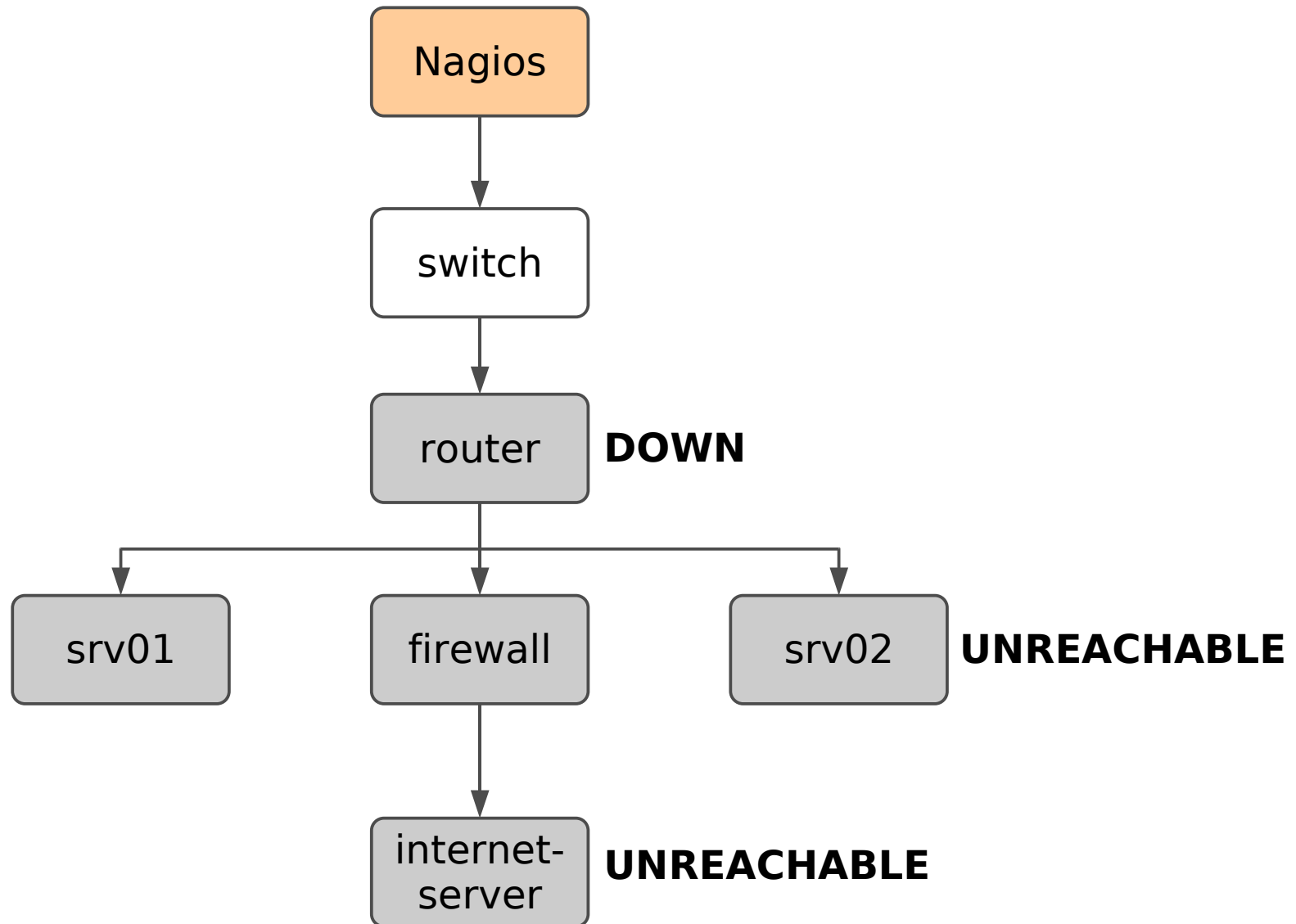
- Was kritisch ist und was nicht, legt der Administrator über Schwellwerte fest (je Check!)
- Schwellwertangaben abhängig vom Plugin
- Beispiele:
 - `check_icmp ... -w 200.0,40% -c 1000.0,80%`
 - `check_smtp ... -w 5.0 -c 8.0 ...`
 - `check_disk ... -w 10% -c 5% ...`

Service- und Host-Checks

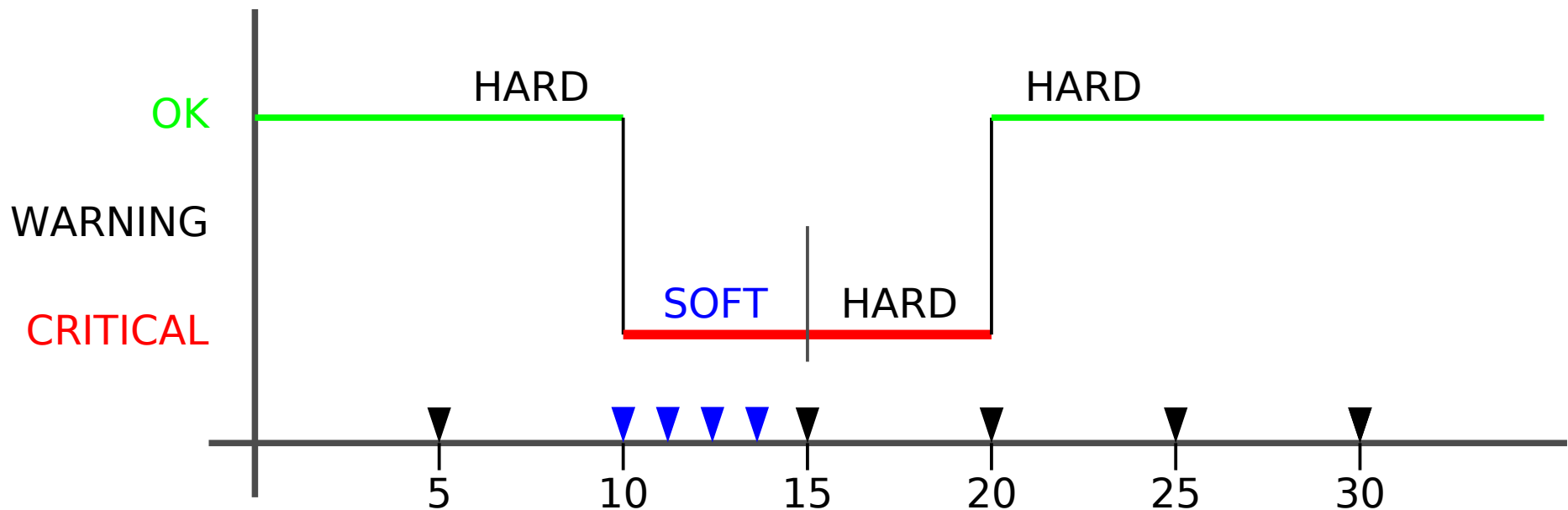
- Service-Checks werden regelmäßig ausgeführt
- Host-Checks nur bei Bedarf
- Empfehlung: immer Ping als Service definieren



Netzwerktopologie



Zustände



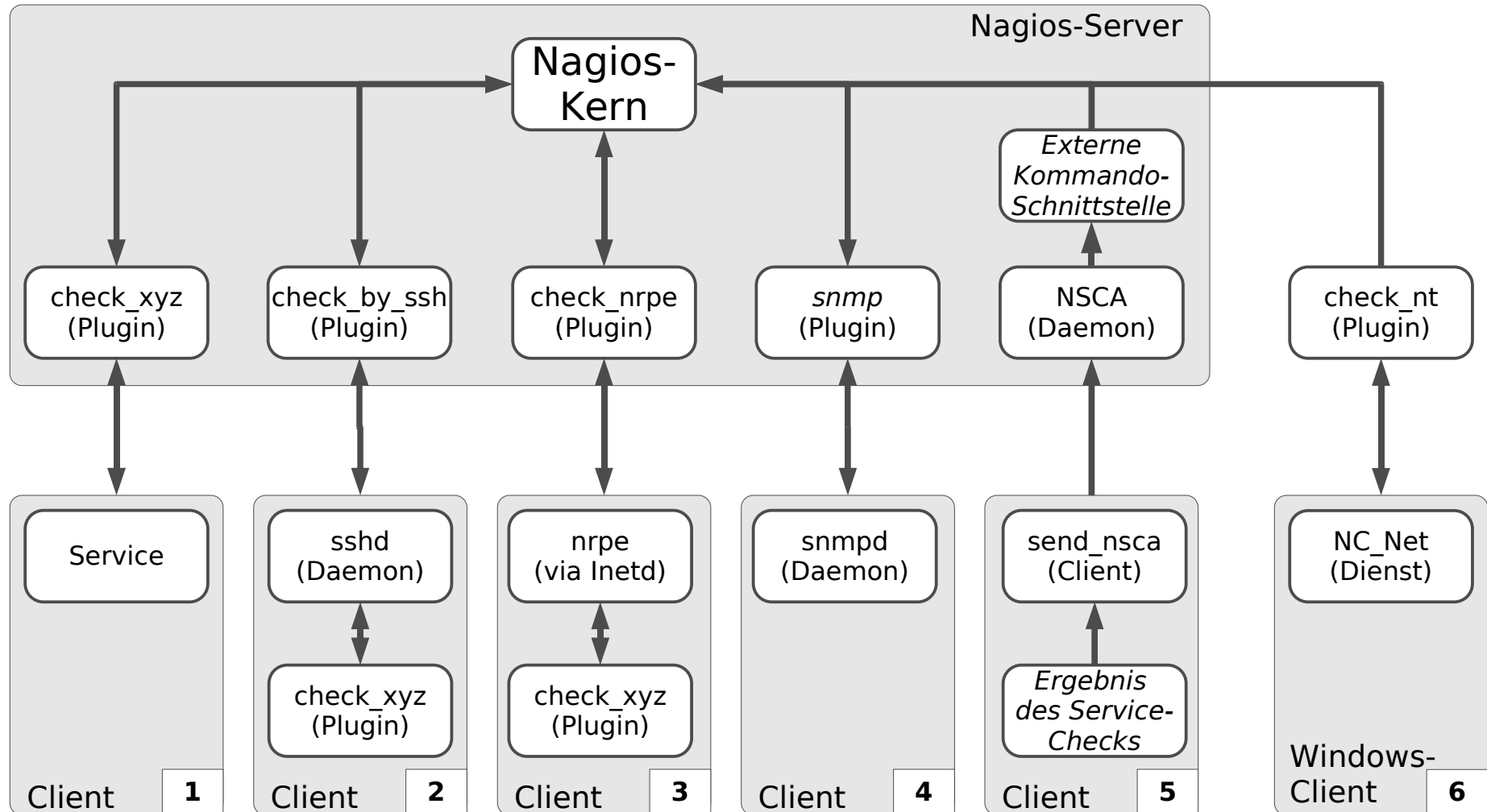
Soft State:

- Logging
- Eventhandler ausführen
- keine Benachrichtigung, aber Anzeige in der Weboberfläche

Hard State:

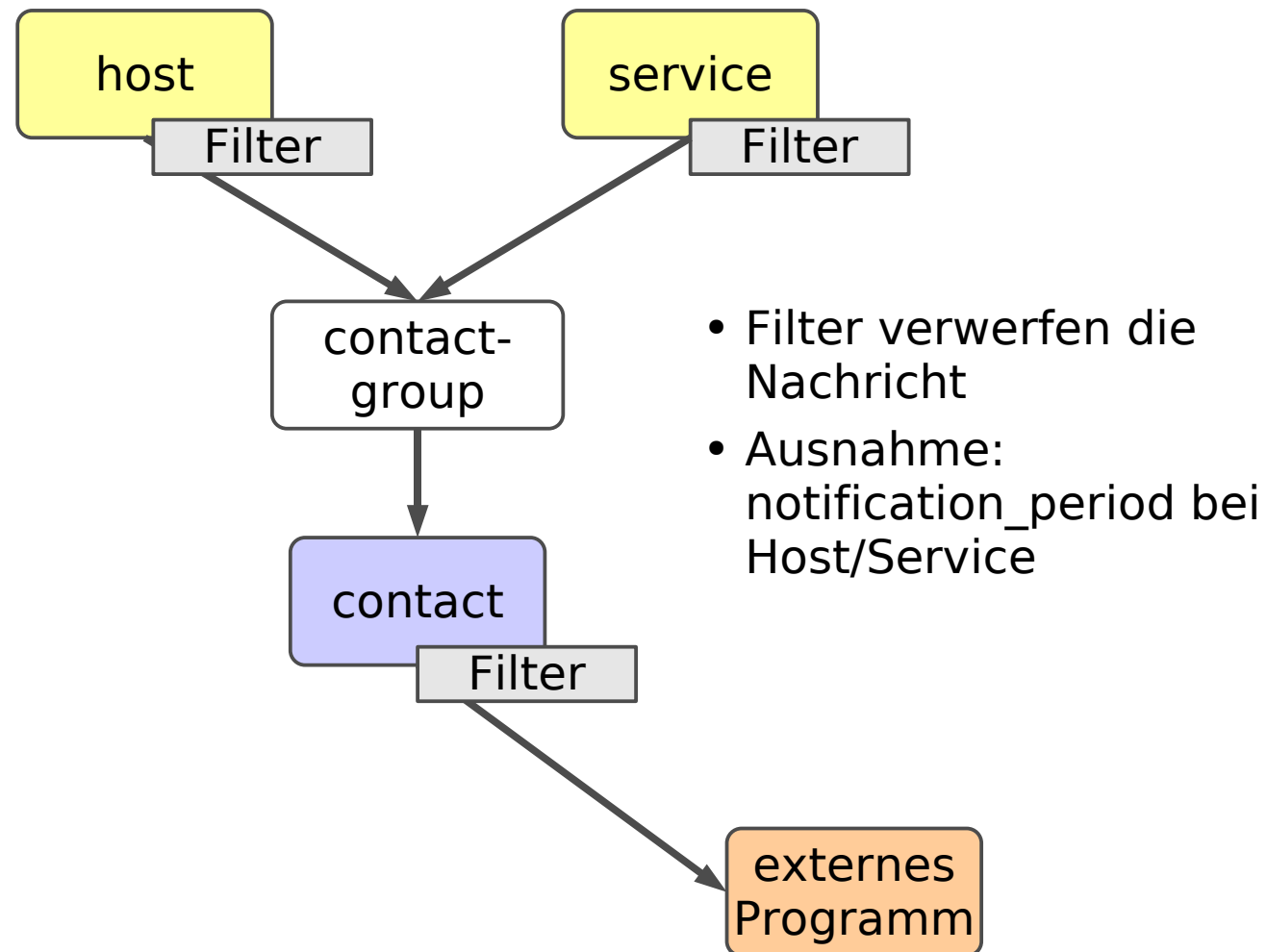
- Logging
- Eventhandler ausführen
- Benachrichtigung incl. Anzeige in der Weboberfläche

Viele Wege führen zum Ziel



entnommen aus: "Nagios" von Wolfgang Barth, Open Source Press 2005, Seite 80

Benachrichtigungen I



siehe auch: "Nagios" von Wolfgang Barth,
Open Source Press 2005, Seite 222

Benachrichtigungen II

host/
service

```
notifications_enabled=1
notification_options=c,w,u,r,f
notification_period=24x7
notification_interval=120
contact_group=admin
```

contact

```
host_notification_options
service_notification_options
host_notification_period
service_notification_period
```

Benachrichtigungen III

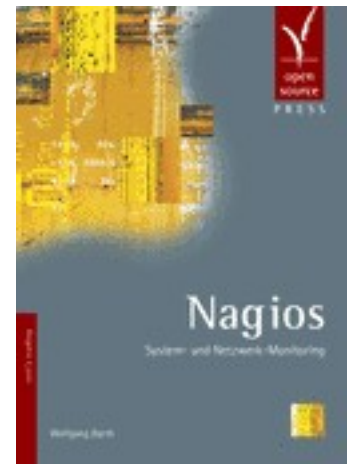
- Eskalationsmanagement
 - Information anderer/weiterer Kontaktgruppen
 - Veränderung von `notification_interval`
 - Beispiel: 3x Email, dann 1x SMS, dann Email an den Chef
- Dependencies
 - Unterdrückung von Nachrichten abhängig vom Zustand anderer Services/Hosts
 - Beispiel: Disk-Check (lokales Plugin) abhängig von NRPE

Viele weitere Features ...

- Acknowledgements
- Downtime
- Reporting:
 - auch über Host/Service-Gruppen
 - berücksichtigt wahlweise Downtime
 - Reporting über Zeitfenster, z.B. Mo-Fr. 07h-17h
- Eventhandler
- Flapping

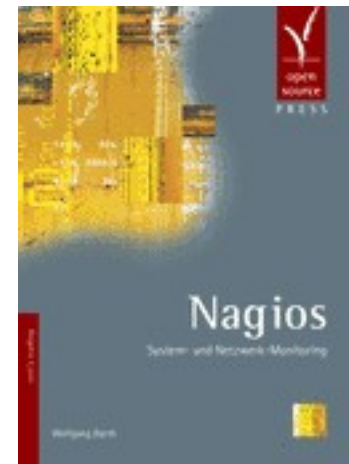
Nagios: das Buch ;-)

- Teil I: Inbetriebnahme
 - Installation aus dem Quellcode
 - Erstellung einer Anfangskonfiguration
 - der erste Start
- Teil II: En Detail
 - Grundlagen: Zustände, Topologien
 - Plugins: remote, lokal, helper
 - Remote-Start von Plugins: SSH, NRPE
 - SNMP (incl. Einführung in SNMP)
 - Benachrichtigungssystem



Nagios: das Buch II

- Fortsetzung Teil II:
 - External Command File Schnittstelle
 - NSCA: Mechanismus, verteiltes Monitoring
 - Weboberfläche
 - Performancedaten graphisch dargestellt
- Teil III: spezielle Einsatzzwecke
 - Windows-Server
 - Temperaturüberwachung
 - SAP-Systeme



Ressourcen

- Nagios Homepage:
`www.nagios.org`
- Nagios-Austauschplattform:
`www.nagiosexchange.org`
- Nagios-Portal:
`www.nagios-portal.de`
- Mailinglisten:
`listi.jpberlin.de/mailman/listinfo/nagios`
`www.nagios.org/support/maillinglists.php`

last page ;-)

**Vielen Dank für Ihre/Eure
Aufmerksamkeit**

Fragen?