

Let's do IT together!



IT-Haus Stammtisch – 24.02.2011

Nagios®

Stephan Langhard

&

Stefan Igelmund

IT-Systeme / Netzwerke

IT-Haus GmbH – Föhren

Agenda

- ▶ Einführung in Nagios
- ▶ Standarddienste überwachen
- ▶ Plugins
- ▶ Überwachung von Windowsrechnern
- ▶ Überwachung mit SNMP
- ▶ Performancedaten-Analyse
- ▶ Benachrichtigungen
- ▶ Visualisierung mit NagVis
- ▶ Was geht noch?

Was ist Nagios?

- ▶ Nagios ist ein Baukastensystem. Für jede Installation braucht man – je nach Gegebenheiten – andere Bausteine
- ▶ Nagios-Core
- ▶ Nagios-Plugins
- ▶ NRPE
- ▶ AddOns
- ▶ ...



Nagios-Core

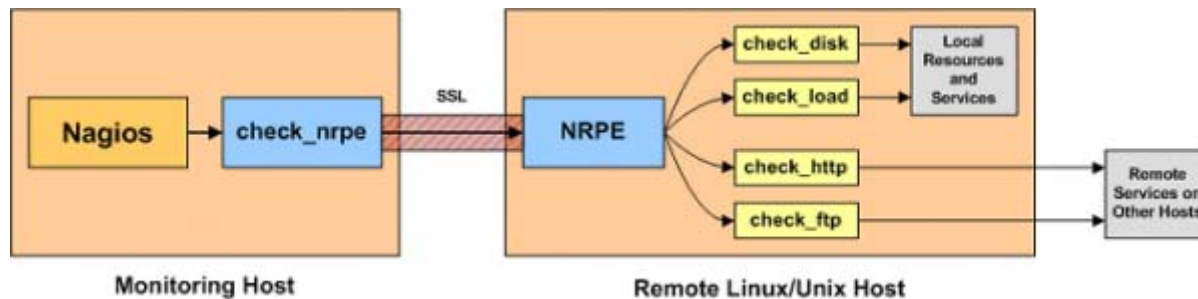
- ▶ Stellt das eigentliche Framework zur Verfügung
- ▶ Scheduler
- ▶ Führt Checks (Plugins) aus
- ▶ Führt Benachrichtigungen (Notifications) aus
- ▶ WebFrontend zur Übersicht und Administration

Nagios-Plugins

- ▶ Sammlung von offiziellen Plugins zum Ausführen aktiver Checks
- ▶ Programmiert in C/C++, Perl und anderen Skriptsprachen
- ▶ Zwingend für den Betrieb erforderlich

NRPE – Nagios Remote Plugin Executor

- ▶ Zwei Teile:
- ▶ Daemon für entfernten Rechner
- ▶ Plugin für Nagios Server
- ▶ Der Daemon führt Plugins auf dem entfernten Rechner aus und meldet das Ergebnis an Nagios
- ▶ Die Ausführung wird durch den Nagios Server angestoßen



AddOns

- ▶ Performancedaten-Analyse (PNP4Nagios, ...)
- ▶ Alternative WebFrontends zur Darstellung (NagVis, ...)
- ▶ Imagepacks
- ▶ Hunderte Plugins für verschiedene Aufgaben
- ▶ ...

Nagios Konfiguration

- ▶ Die gesamte Konfiguration von Nagios erfolgt über Objekte
- ▶ Hosts
- ▶ Services
- ▶ Hostgroups und Servicegroups
- ▶ Contacts und Contactgroups
- ▶ Commands
- ▶ Timeperiods
- ▶ ...
- ▶ Objekte können Templates benutzen

Beispielhost

```
define host {  
    host_name          nagios  
    alias              Nagios Server  
    address            127.0.0.1  
    check_command      check-host-alive  
    check_interval     5  
    retry_interval     1  
    max_check_attempts 5  
    check_period       24x7  
    contact_groups     admins  
    notification_interval 30  
    notification_period 24x7  
    notification_options d,u,r  
}
```

Beispielservice

```
define service {  
    host_name          nagios  
    service_description HTTP  
    check_command      check-http  
    max_check_attempts 5  
    check_interval     5  
    retry_interval     3  
    check_period       24x7  
    notification_interval 30  
    notification_period 24x7  
    notification_options w,c,r  
    contact_groups     admins  
}
```

Contacts

```
define contact {  
    contact_name          stefan  
    alias                 Stefan Igelmund  
    host_notification_period 24x7  
    service_notification_period 24x7  
    host_notification_options d,u,r  
    service_notification_options w,u,c,r  
    host_notification_commands hostnotifybyemail,  
                               hostnotifybyepager  
    service_notification_commands notifybyemail,  
                               notifybyepager  
    email                 sigelmund@it-haus.com  
    pager                 01721234567  
}
```

Contactgroups

```
define contactgroup {  
    contactgroup_name    admins  
    alias                Nagios Admins  
    members              stefan, ...  
}
```

Commands

```
define command {  
    command_name    check_pop  
    command_line    /usr/local/nagios/libexec/check_pop -H $HOSTADDRESS$  
}
```

Timeperiods

```
define timeperiod {  
    timeperiod_name      24x7  
    alias                 24/7  
    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  
    sunday                00:00-24:00  
}
```

Templatedefinition

```
define service {  
    name                generic-template  
    register            0  
    check_period        24x7  
    max_check_attempts 3  
    normal_check_interval 3  
    retry_check_interval 1  
    notification_interval 20  
    notification_period 24x7  
    notification_options w,u,c,r  
}
```

Templates verwenden

```
define service {  
    host_name          foobar  
    use                generic-template  
    service_description SSH  
    contact_groups    admins  
    check_command     check_ssh  
}
```

Plugins

- ▶ Die Standardplugins:
 - ▶ dns
 - ▶ ssh
 - ▶ http, https
 - ▶ ftp
 - ▶ ntp
 - ▶ ping
 - ▶ oracle, mysql
 - ▶ tcp, udp
 - ▶ snmp
 - ▶ smtp
 - ▶ ...

Plugins

- ▶ Plugins für NRPE, über ssh oder zur lokalen Ausführung:
 - ▶ RAM & Swap
 - ▶ Anzahl der Prozesse
 - ▶ Load bzw. CPU-Auslastung
 - ▶ Festplattenauslastung
 - ▶ Mailqueues
 - ▶ Interfacestatus
 - ▶ Interfacetraffic
 - ▶ ...
 - ▶ alles was man skripten kann 😊

Plugins

- ▶ Plugins aus der Community:
 - ▶ VMware
 - ▶ Citrix
 - ▶ USVs
 - ▶ Drucker
 - ▶ BizTalk
 - ▶ ...
- ▶ Nachteil: Die Plugins sind oft schlecht dokumentiert, veraltet oder funktionieren nur in sehr speziellen Umgebungen

Plugins entwickeln

- ▶ Plugins können in einer beliebigen Programmiersprache geschrieben werden
- ▶ Nagios erkennt anhand des Rückgabewertes den Erfolg eines Checks:
 - ▶ OK (0)
 - ▶ WARNING (1)
 - ▶ CRITICAL (2)
 - ▶ UNKOWN (3)
- ▶ Textausgaben des Plugins werden von Nagios ausgewertet und dargestellt

Windowsrechner überwachen

- ▶ „Klassische“ Dienste werden ganz normal überwacht:
 - ▶ IIS mit check_http
 - ▶ Exchange mit check_smtp, ...
- ▶ Alles andere funktioniert über SNMP oder ...
- ▶ ... spezielle Dienste für Windows:
 - ▶ NSClient
 - ▶ NSClient++
 - ▶ NC_Net
- ▶ Die Abfrage der Dienste erfolgt über „check_nt“

SNMP

- ▶ Mit SNMP lässt sich beinahe alles machen (sofern unterstützt):
 - ▶ Interfacetraffic
 - ▶ Load
 - ▶ Speicherauslastung
 - ▶ Laufende Prozesse
 - ▶ ...

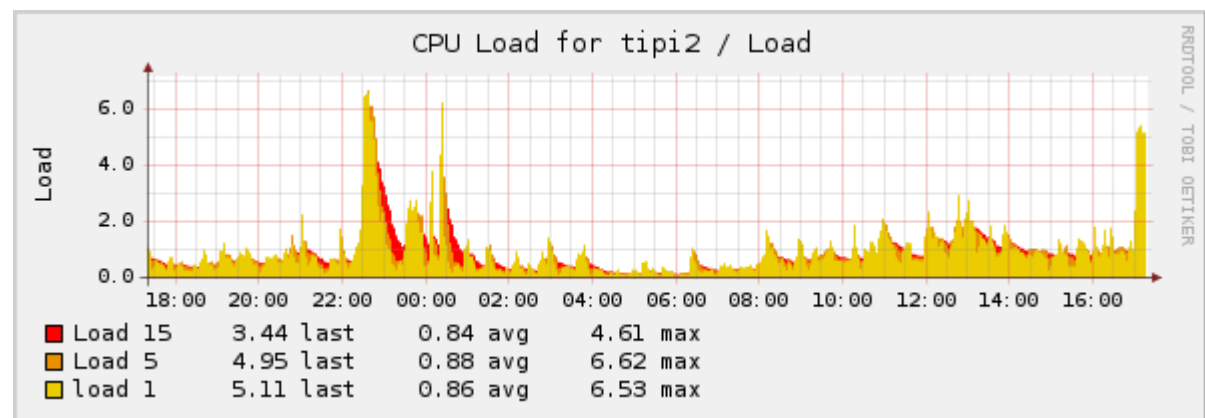
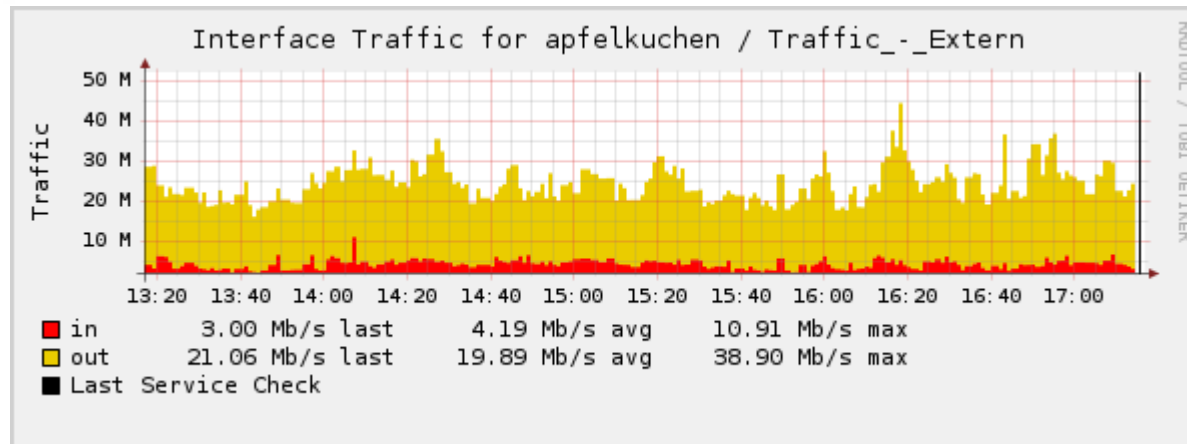
SNMP

- ▶ Jede etwas „bessere“ Hardware liefert eigene MIBs, um nahezu alle Daten des Systems auslesen zu können:
 - ▶ USV: Status, Restlaufzeit, Ausfälle, Spannungsschwankungen, Eventlog, ...
 - ▶ Sensoren: Temperatur, Luftfeuchtigkeit, Leistungsaufnahme, Lüfterdrehzahl, ...
 - ▶ Drucker: Betriebszeit, Tonerstatus, Printerqueue, ...
 - ▶ Netzwerkkomponenten: Traffic, Fehler, Trunks, VLANs, MAC-Adressen, Temperatur, Module, Interfacespeed, CPU-Last, RAM, ...
 - ▶ Firewalls: Traffic, Paketstatistiken, Auslastung, ...

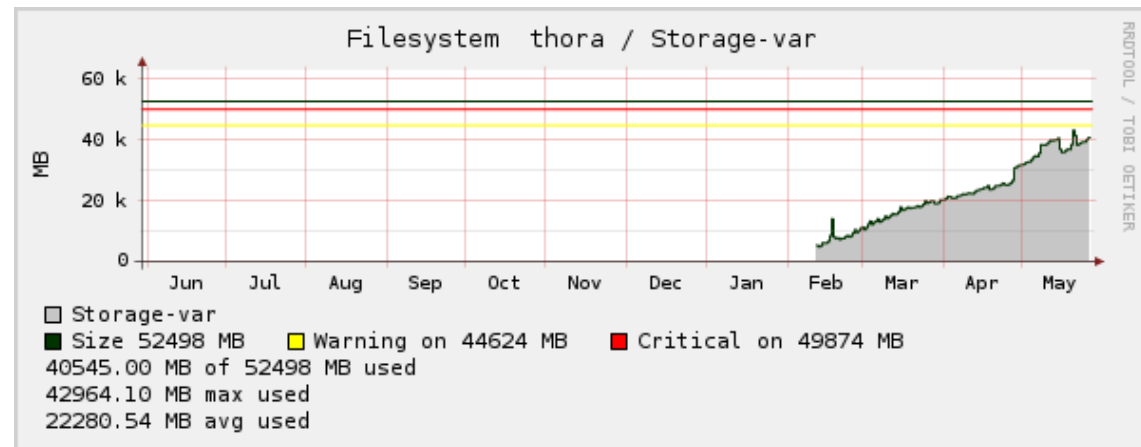
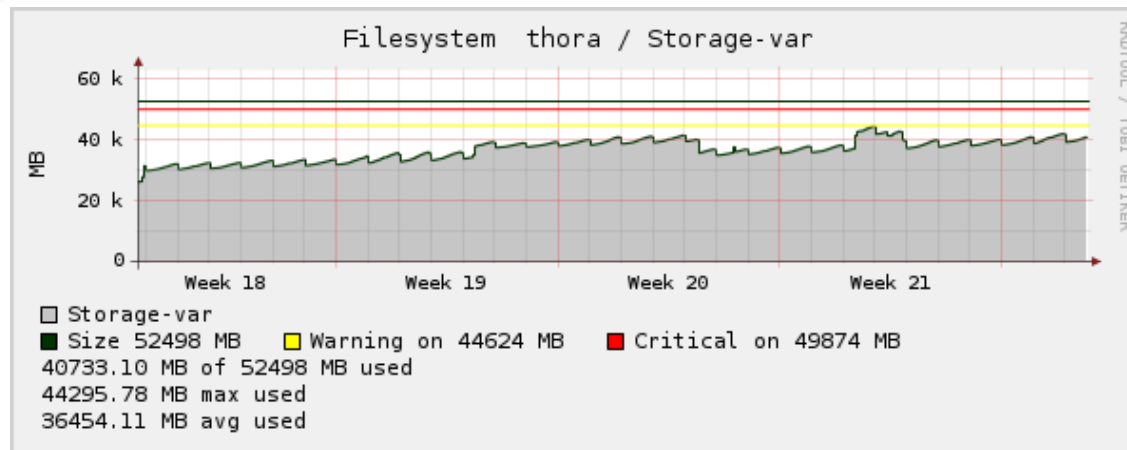
Performancedaten-Analyse

- ▶ Nagios selbst wertet keine Performancedaten aus!
- ▶ Die meisten Nagios-Plugins liefern aber Performancedaten:
 - ▶ TCP OK 0.000 - second response time on port 80 |
time=0.000163s;;;0.000000;10.000000
 - ▶ SMTP OK - 0.004 sec. response time |
time=0.003762s;;;0.000000
 - ▶ Load : 4.71 3.66 3.53 : OK |
load_1_min=4.71;5;10 load_5_min=3.66;5;10 load_15_min=3.53;5;10
- ▶ Externe Programme können diese auswerten und visualisieren

Perfomancedaten-Analyse mit PNP



Performancedaten-Analyse mit PNP



Benachrichtigungen

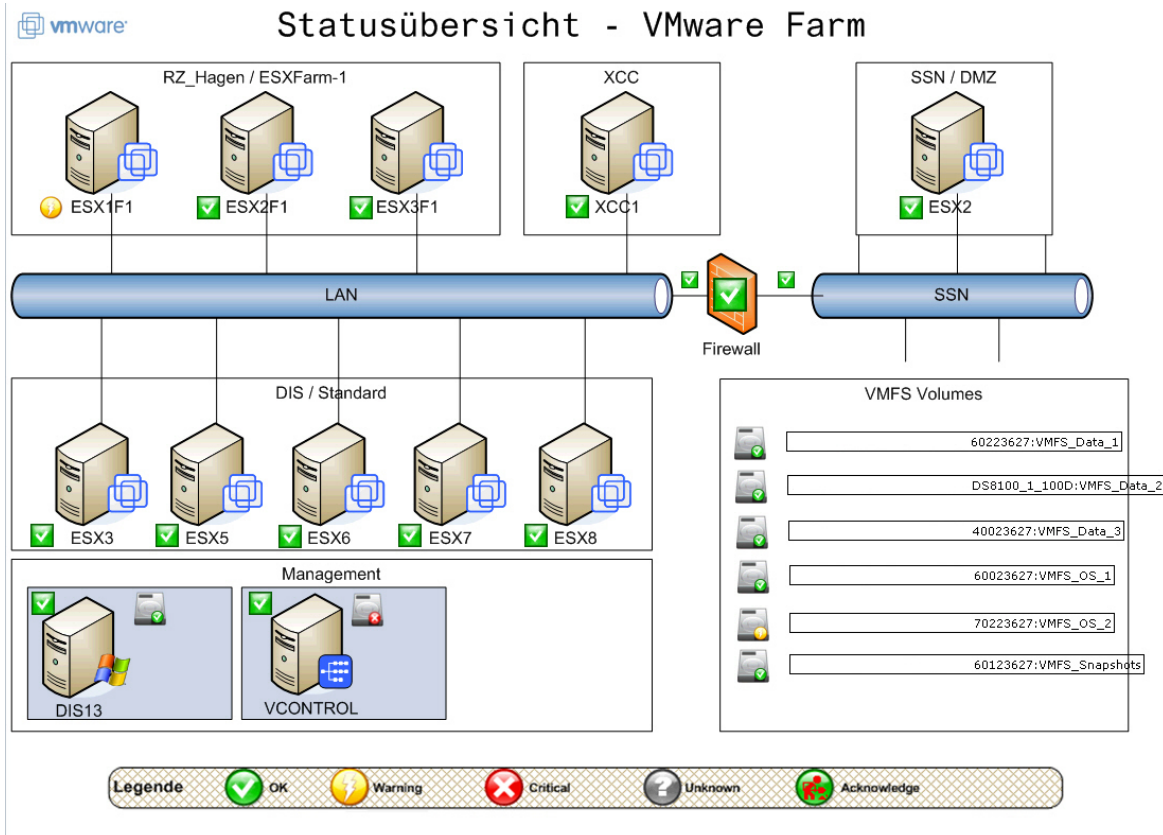
- Notifications sind auch „nur“ eine Kommandodefinition

```
define command{  
    command_name        hostnotifybyemail  
    command_line        /usr/bin/printf "%b" "***** Nagios  
*****\n\nNotification Type: $NOTIFICATIONTYPE$ $HOSTACKAUTHOR$\nHost:  
$HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo:  
$HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /usr/bin/mail -s "Host  
$HOSTSTATE$ alert for $HOSTNAME$!" $CONTACTEMAIL$  
}
```

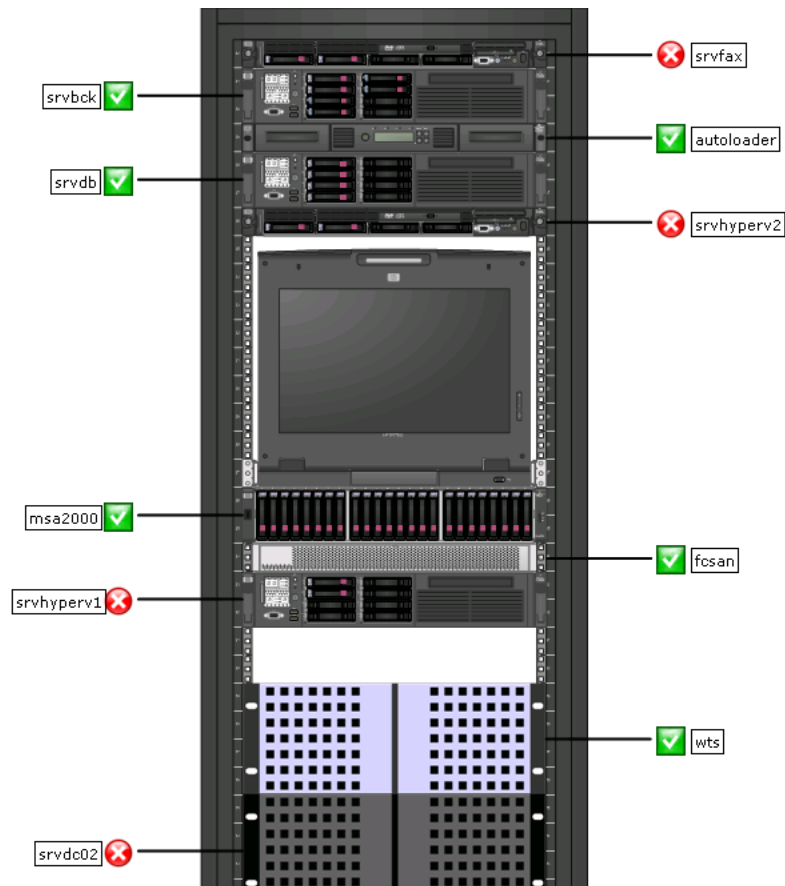
- Benachrichtigung via E-Mail, SMS, IM, ...

Visualisierung mit NagVis

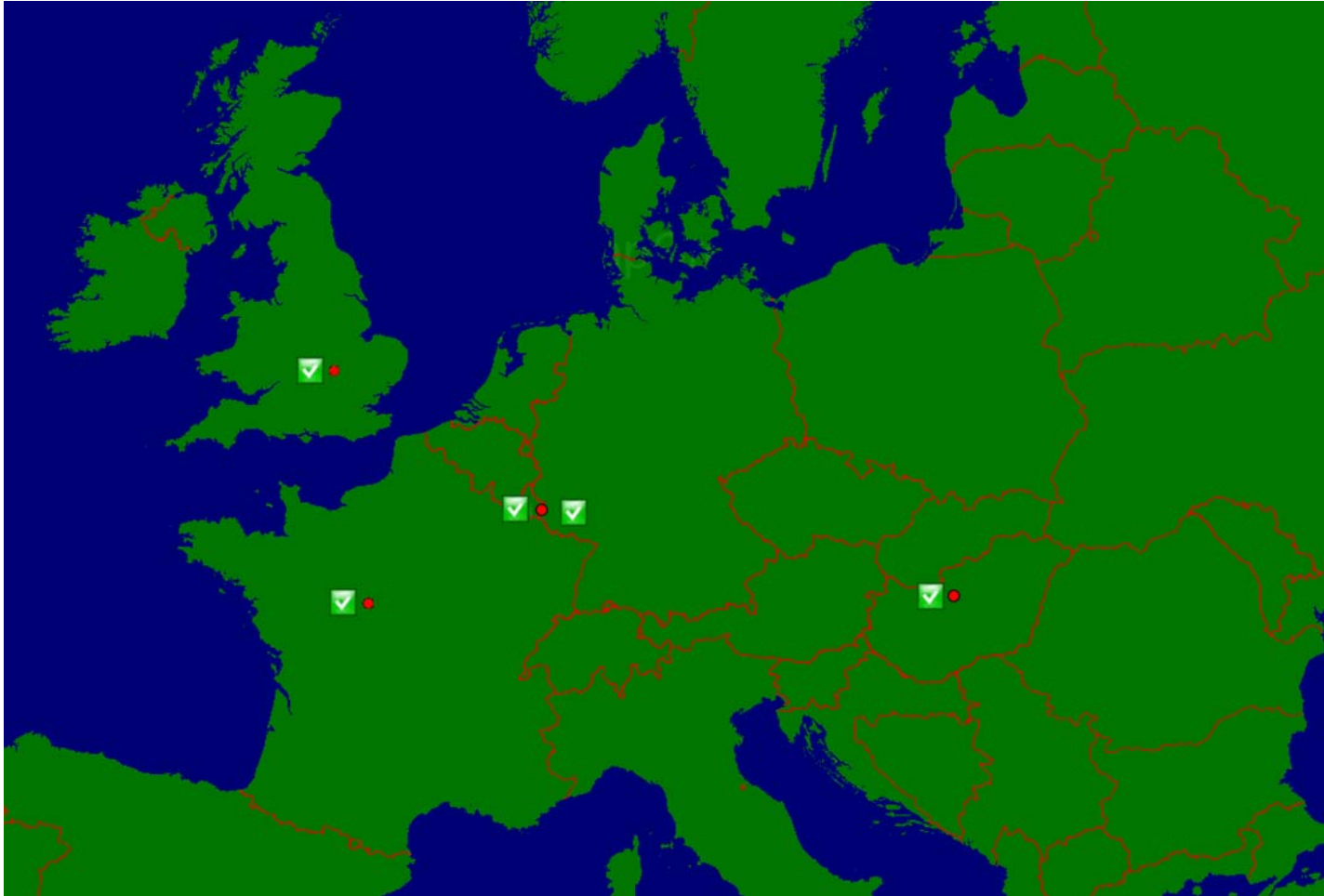
- Darstellung der Daten auf frei erstellbaren Maps



Visualisierung mit NagVis



Visualisierung mit NagVis



Was geht noch?

- ▶ Verteilte, hochverfügbare Systeme
- ▶ Host- und Serviceabhängigkeiten
- ▶ Eventhandling
- ▶ Eskalationsmanagement
- ▶ ...

Und nun...

- ▶ Herzlichen Dank für Ihren Besuch und Ihre Aufmerksamkeit !
- ▶ Stephan Langhard
- ▶ slanghard@it-haus.com
- ▶ Tel: +49 6502 9208-110
- ▶ Stefan Igelmund
- ▶ sigelmund@it-haus.com
- ▶ Tel: +49 6502 9208-110

Kontakt Daten

IT-HAUS GmbH

Europa-Allee 26-28

D-54343 Föhren (A1/A48 Ausfahrt Föhren)

Telefon: +49 6502 9208-0

Telefax: +49 6502 9208-850

E-Mail: info@it-haus.com

Internet: www.it-haus.com



Wir sind für Sie da

Geschäftsstellen:

Berlin

Alboinstrasse 56
D-12103 Berlin
Telefon: +49 30 75621796
Telefax: +49 30 75621180

Föhren

Europa-Allee 28
D-54343 Föhren
Telefon: +49 6502 9208-0
Telefax: +49 6502 9208-850

Köln

Am Grauen Stein 3
D-51105 Köln
Telefon: +49 221 8064609

Nürnberg

Tillystraße 2
D-90431 Nürnberg
Telefon: +49 911 6554770

Service Points:

Cottbus

Wilhelm-Külz-Straße 15
D-03046 Cottbus

Gießen

Friedrich-List-Straße 3
D-35398 Gießen

Dresden

Schandauer Straße 34
D-01309 Dresden
Telefon: +49 351 3122266
Telefax: +49 351 3123534

Hamburg

Julius-Vosseler-Straße 42
D-22527 Hamburg
Telefon: +49 40 56060157
Telefax: +49 40 56060158

Meerbusch

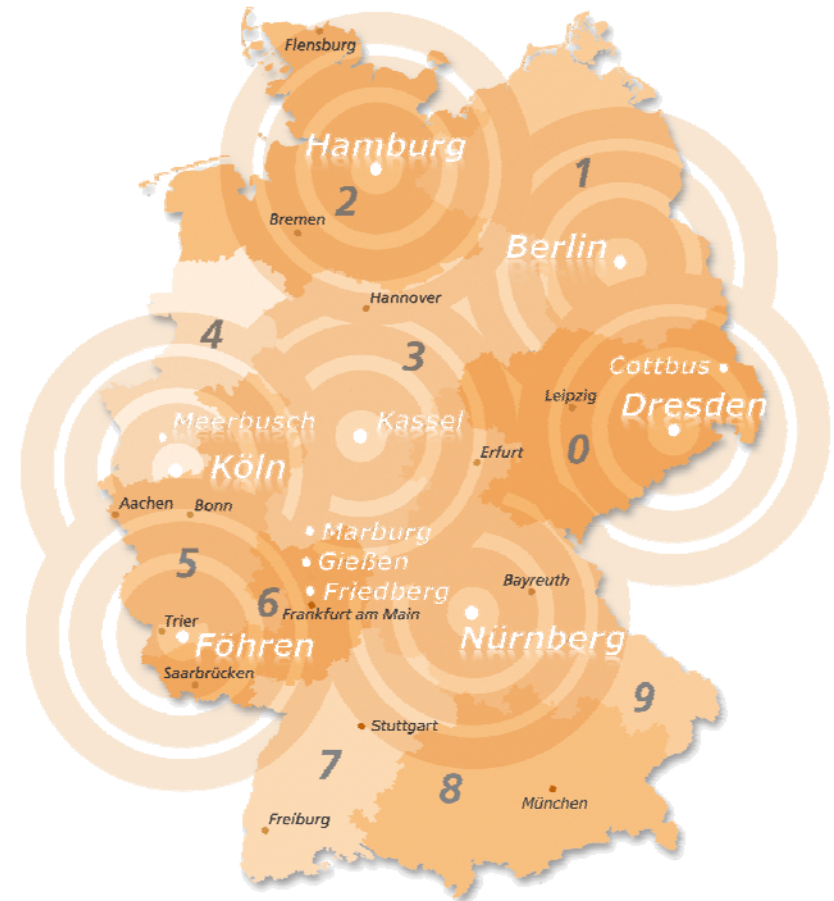
Niederdonker Straße 24
D-40667 Meerbusch
Telefon: +49 2132 5940064

Friedberg

Am Dachspfad 23
D-61169 Friedberg

Kassel

Werner-Heisenberg-Straße 5
D-34123 Kassel



Marburg

Bahnhofstraße 13
D-35037 Marburg