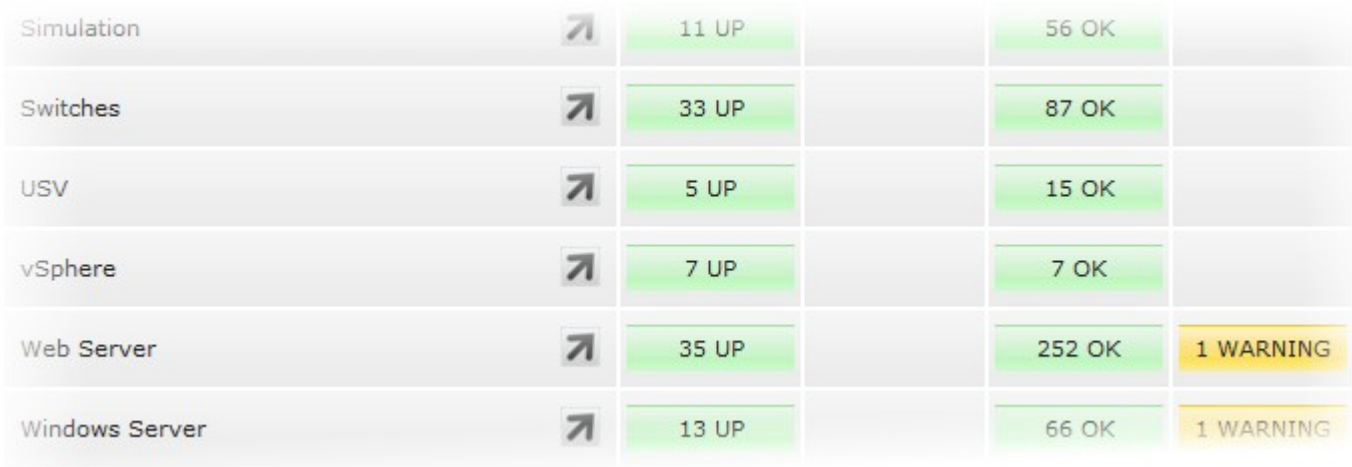
Opsera Opsview

Network, Server and Application Monitoring

Präsentation zum Thema System-Überwachung

von Sven Meyer



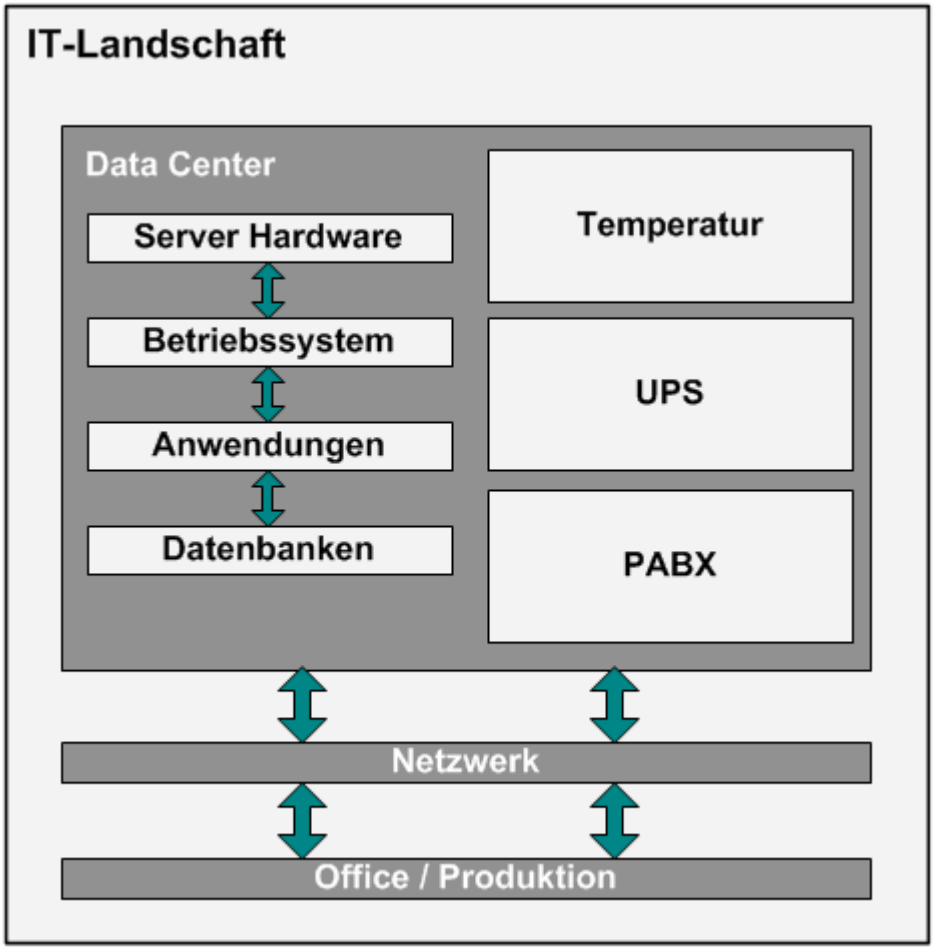
Übersicht

1. Allgemeines
2. Einführung in Nagios
3. Opsera Opsview

Allgemeines

Warum?

- Komplexe Infrastruktur
  - Fehleranfällig
- Fehlererkennung
  - Prävention
- *Hardware Consolidation*
  - *Virtualisierung*



Wie?

- SNMP (*Simple Network Management Protocol)*
  - Weitestgehend unterstützt
- WBEM (*Web Based Enterprise Management)*
  - WMI (Microsoft), OpenPegasus (RedHat), OpenWBEM (Novell)
- IPMI (*Intelligent Platform Management Interface)*
  - Hardware-seitiges Monitoring (z.B. Dell RAC, HP ILO)

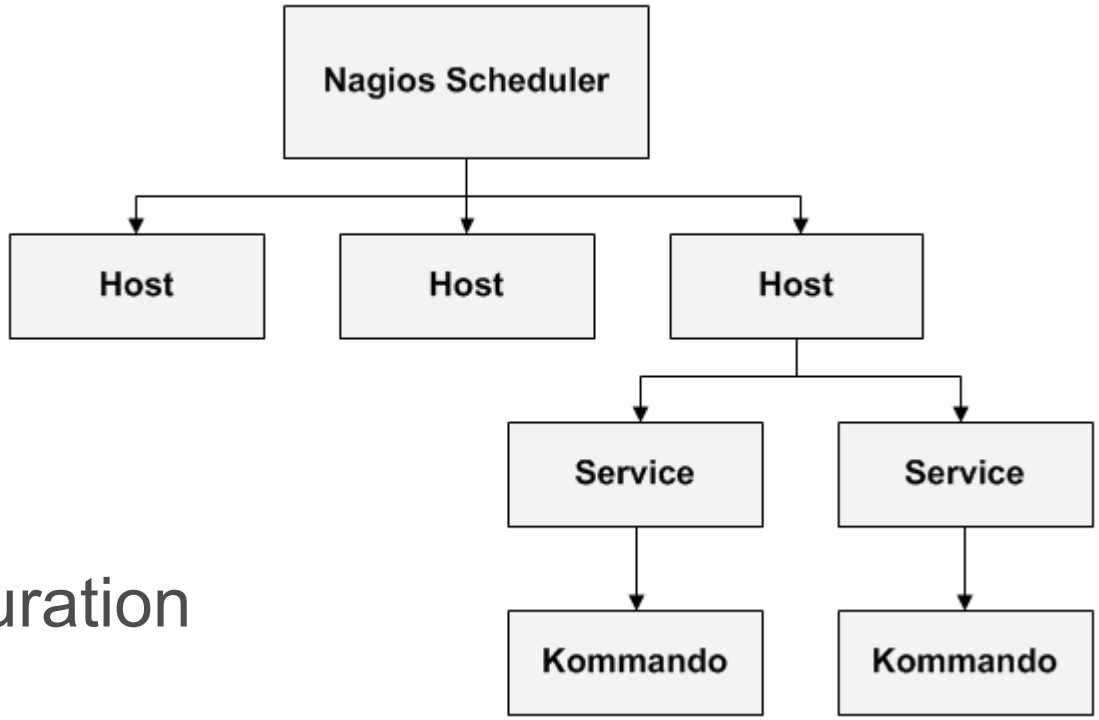
Polling und Events

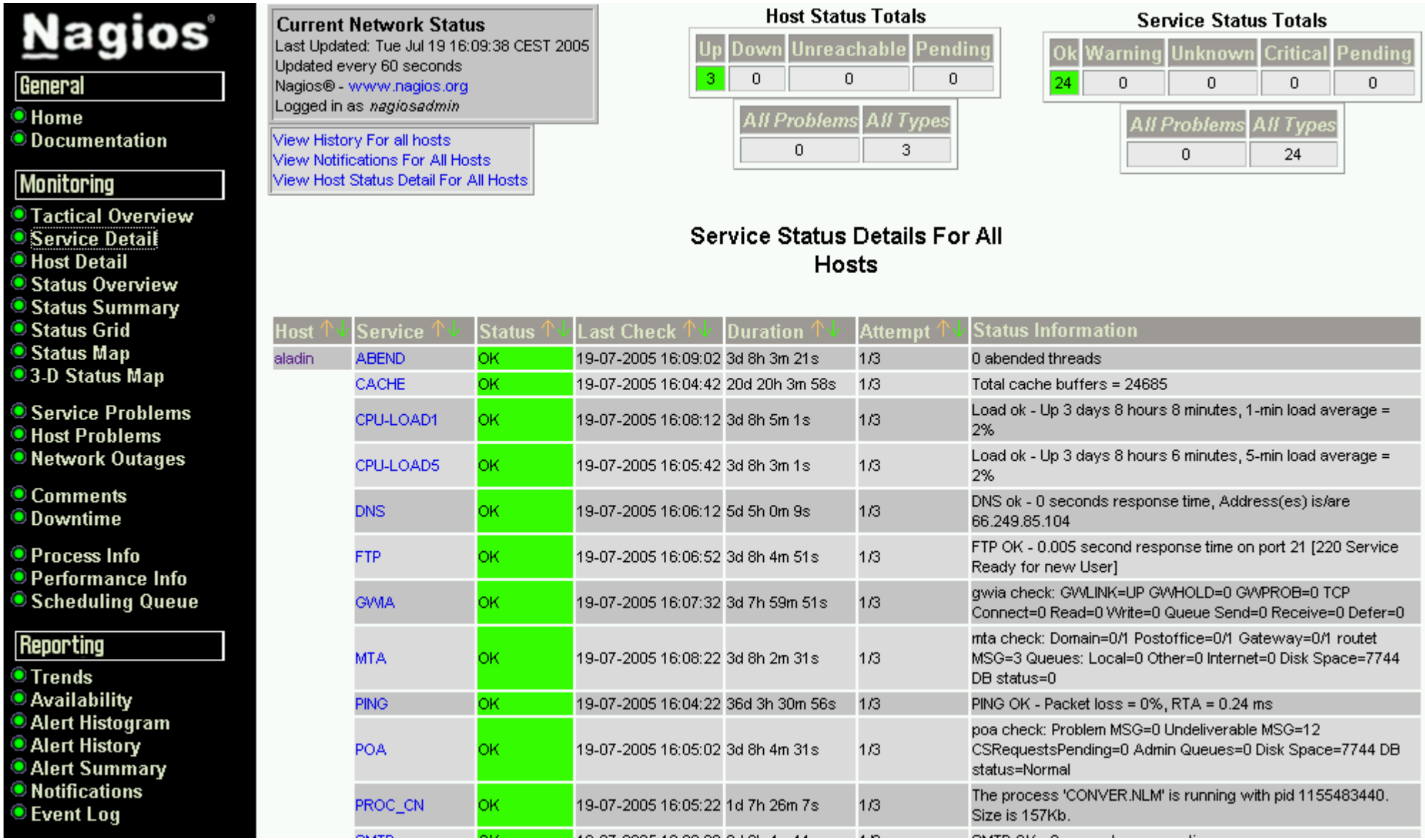
- *Polling*: zyklisches Abfragen
  - SNMP: Get / Response
    - snmpget -v2c -c public localhost 1.3.6.1.4.1.2021.10.1.3.3
  - CIM Query (WBEM)
    - SELECT * FROM Win32_Process
- *Events*: Warten auf Ereignis
  - SNMP: Traps
  - WBEM: Events
  - IPMI: Über SNMP Traps

Nagios

Überblick

- Open Source
- Quasi-Standard
- Erweiterbar
- „Relativ einfache“ Konfiguration
- Web-Frontend




Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Current Network Status
Last Updated: Tue Jul 19 16:09:38 CEST 2005
Updated every 60 seconds
Nagios® - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
3 0 0 0
All Problems All Types
0 3
Service Status Totals
Ok Warning Unknown Critical Pending
24 0 0 0 0
All Problems All Types
0 24
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
aladin ABEND OK 19-07-2005 16:09:02 3d 8h 3m 21s 1/3 0 abended threads
CACHE OK 19-07-2005 16:04:42 20d 20h 3m 58s 1/3 Total cache buffers = 24685
CPU-LOAD1 OK 19-07-2005 16:08:12 3d 8h 5m 1s 1/3 Load ok - Up 3 days 8 hours 8 minutes, 1-min load average = 2%
CPU-LOAD5 OK 19-07-2005 16:05:42 3d 8h 3m 1s 1/3 Load ok - Up 3 days 8 hours 6 minutes, 5-min load average = 2%
DNS OK 19-07-2005 16:06:12 5d 5h 0m 9s 1/3 DNS ok - 0 seconds response time, Address(es) is/are 66.249.85.104
FTP OK 19-07-2005 16:06:52 3d 8h 4m 51s 1/3 FTP OK - 0.005 second response time on port 21 [220 Service Ready for new User]
GWIA OK 19-07-2005 16:07:32 3d 7h 59m 51s 1/3 gwia check: GWLINK=UP GWHOLD=0 GWPROB=0 TCP Connect=0 Read=0 Write=0 Queue Send=0 Receive=0 Defer=0
MTA OK 19-07-2005 16:08:22 3d 8h 2m 31s 1/3 mta check: Domain=0/1 Postoffice=0/1 Gateway=0/1 routet MSG=3 Queues: Local=0 Other=0 Internet=0 Disk Space=7744 DB status=0
PING OK 19-07-2005 16:04:22 36d 3h 30m 56s 1/3 PING OK - Packet loss = 0%, RTA = 0.24 ms
POA OK 19-07-2005 16:05:02 3d 8h 4m 31s 1/3 poa check: Problem MSG=0 Undeliverable MSG=12 CSRequestsPending=0 Admin Queues=0 Disk Space=7744 DB status=Normal
PROC_CN OK 19-07-2005 16:05:22 1d 7h 26m 7s 1/3 The process 'CONVER.NLM' is running with pid 1155483440. Size is 157Kb.

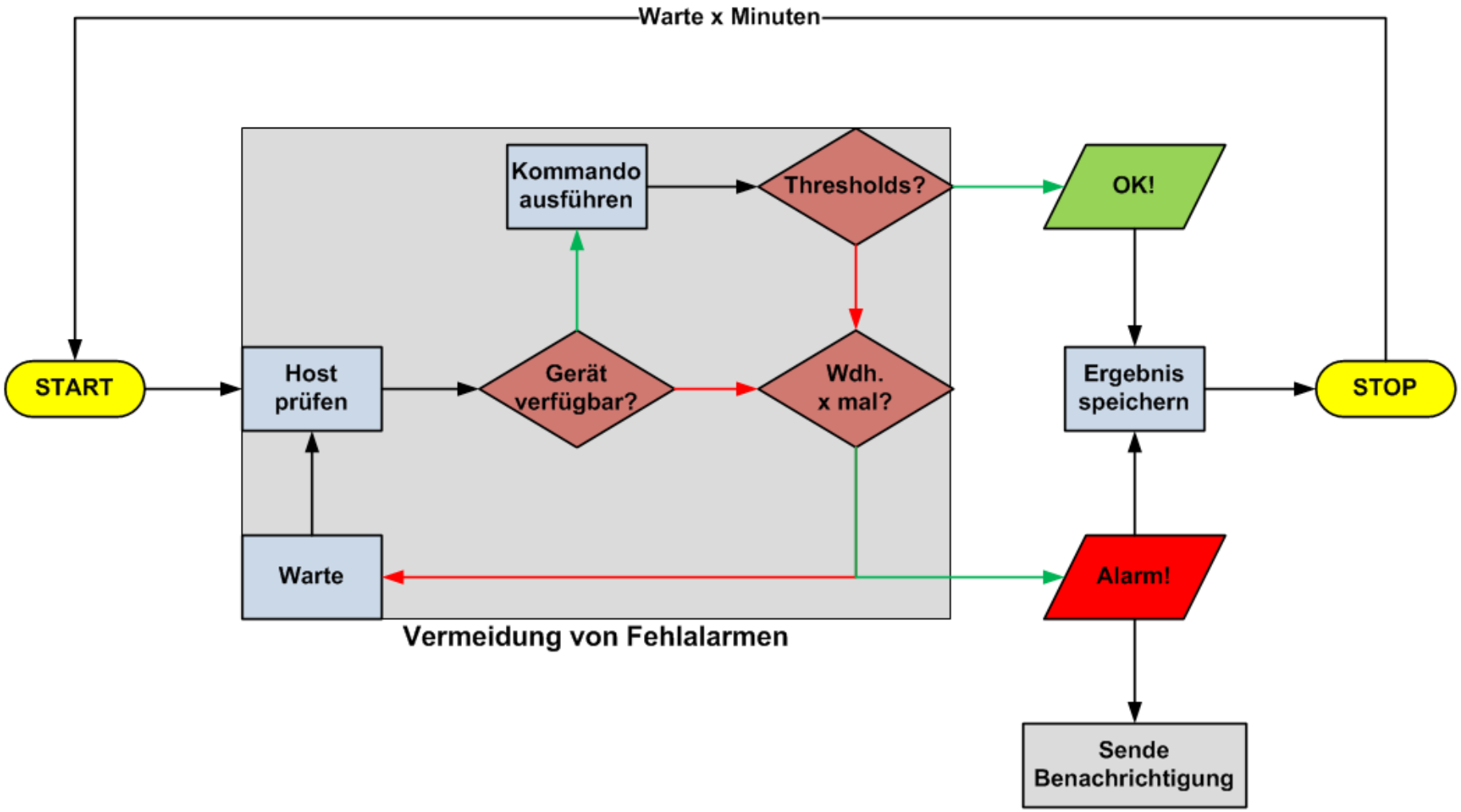
- Beispiel Konfiguration

```
define host{
    use generic-host
    host_name hogwarts
    alias Web- und SMB-Server
    address 192.168.1.1
    check_command check-host-alive
    max_check_attempts 10
    notification_interval 60
    notification_period 24x7
    notification_options d,u,r
}

define service{
    use generic-service
    host_name  hogwarts
    service_description  HTTP
    is_volatile  0
    check_period  24x7
    max_check_attempts  3
    normal_check_interval  3
    retry_check_interval  1
    contact_groups  server-admins
    notification_interval  120
    notification_period  24x7
    notification_options  w,u,c,r
    check_command  check_http
}
```

Funktionsprinzip

- Checks/Kommandos
  - Plug-Ins: Skripte und/oder „kleine“ Programme
- Status über numerischen Rückgabewert
  - OK (0), Warning (1), Critical (2), Unknown (3)
- Host- und Service-States
  - Soft: Service-Check wird wiederholt
  - Hard: Benachrichtigung wird gesendet
- Host- und Service-Abhängigkeiten

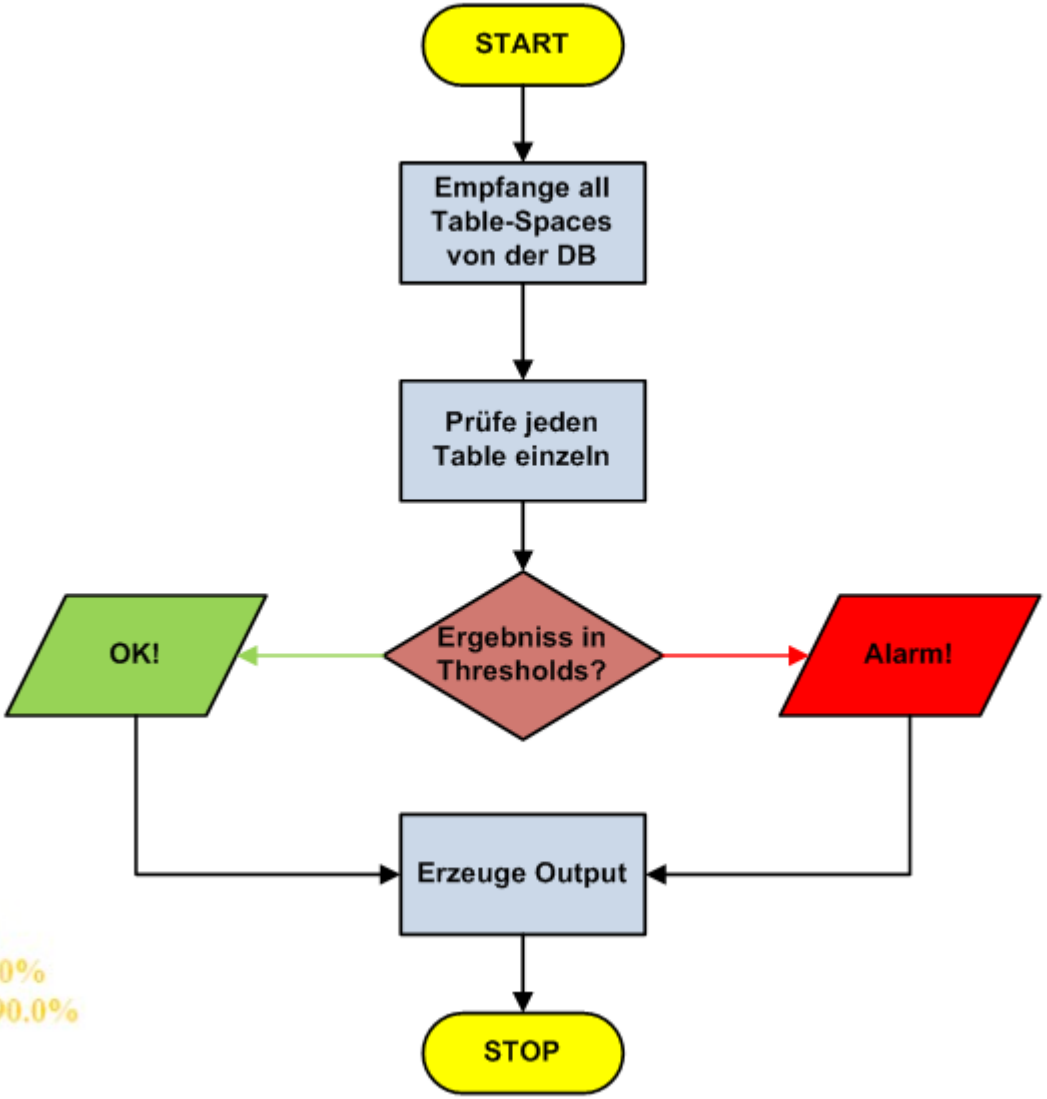
Funktionsprinzip



Beispiel: Plug-In

Pseudo code:

program *check_oracle_tablespaces*
  parseConfigurationAndThresholds()
  connectToDatabase()
  if *notConnected* **then** *sendAlert*
  else *getAllTableInformation* **end**
  while *notAllTablesChecked* **do**
    if *tableWithinThresholds* **then** *markAsOk*
    else *markStateAsCritOrWarn* **end**
  createOutputString
  returnWorstStateToNagios
end *check_oracle_tablespaces*




```
CRIT: WIP - Used: 382589 / 401920 MB (95.19%) >95.0%
WARN: EVAX03 - Used: 29812 / 32768 MB (90.98%) >90.0%
WARN: EVAX05P07 - Used: 92753 / 98304 MB (94.35%) >90.0%
WARN: EVAX05P10 - Used: 194381 / 208000 MB (93.45%) >90.0%
```

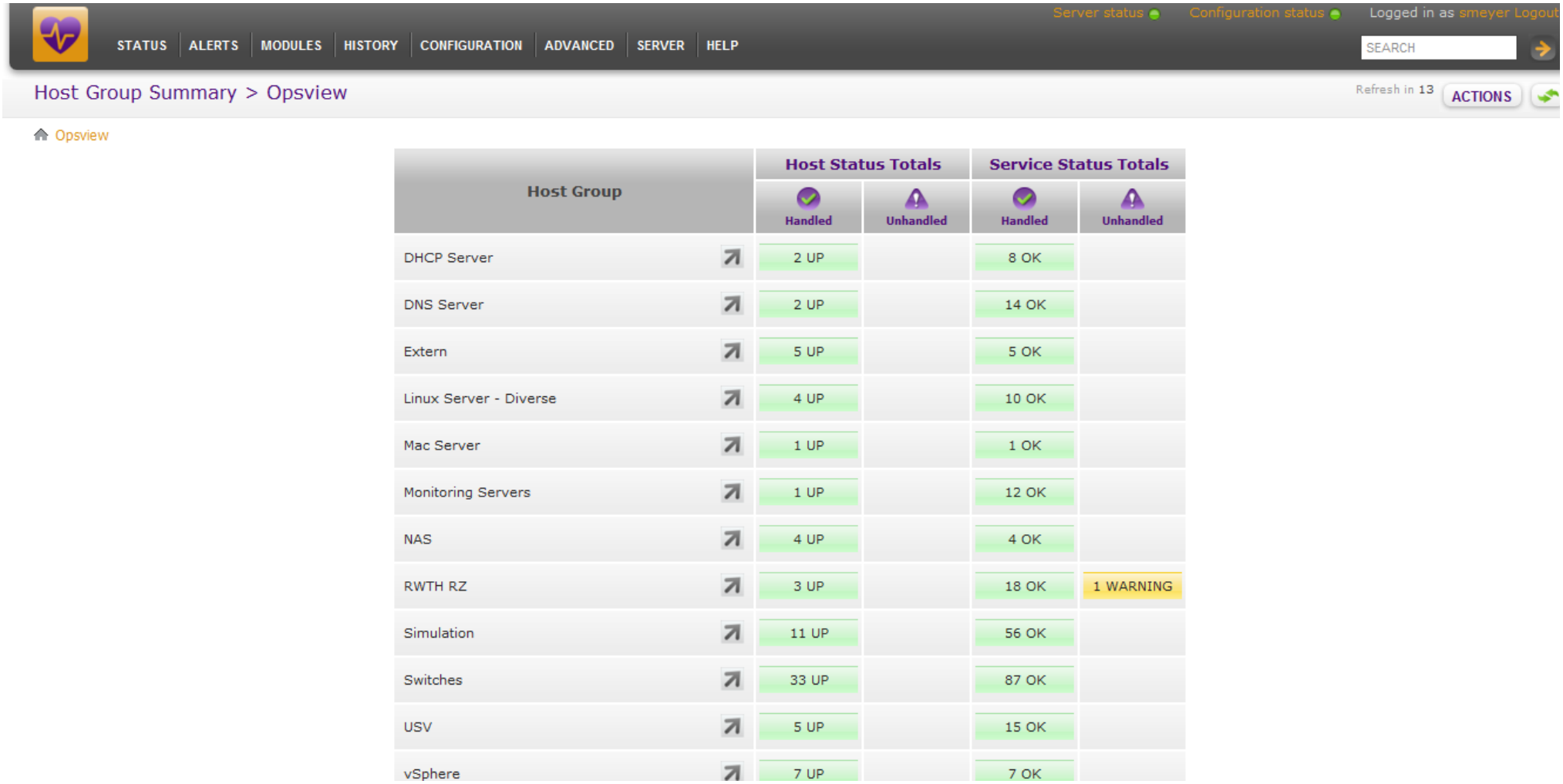
Formatiere Ausgabe, Rückgabewert 2

Opsview

Was ist Opsview?

- Opsview ist kein Ersatz für Nagios
  - Eher „modernes“ Front-End
- Tool-Sammlung
  - Nagios
  - Web-Interface
  - MRTG
  - NMIS
  - NagVis
  - Data Warehouse

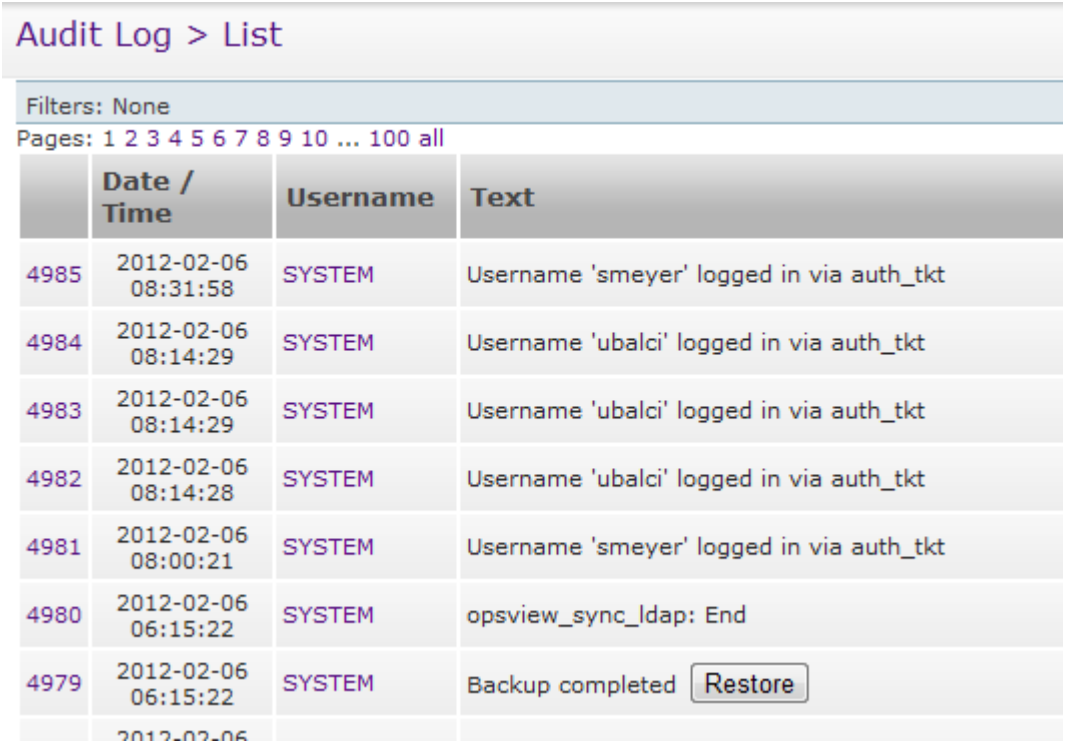
Was ist Opsview?



Host Group	Host Status Totals		Service Status Totals	
	Handled	Unhandled	Handled	Unhandled
DHCP Server	2 UP		8 OK	
DNS Server	2 UP		14 OK	
Extern	5 UP		5 OK	
Linux Server - Diverse	4 UP		10 OK	
Mac Server	1 UP		1 OK	
Monitoring Servers	1 UP		12 OK	
NAS	4 UP		4 OK	
RWTH RZ	3 UP		18 OK	1 WARNING
Simulation	11 UP		56 OK	
Switches	33 UP		87 OK	
USV	5 UP		15 OK	
vSphere	7 UP		7 OK	

Vergleich zu Nagios

- Web-Interface
  - Status-Übersicht
  - Administration
  - AD Integration
  - Audit-Log
- Data Warehouse
  - Reporting
- Externe Tools
  - Out-of-the-box



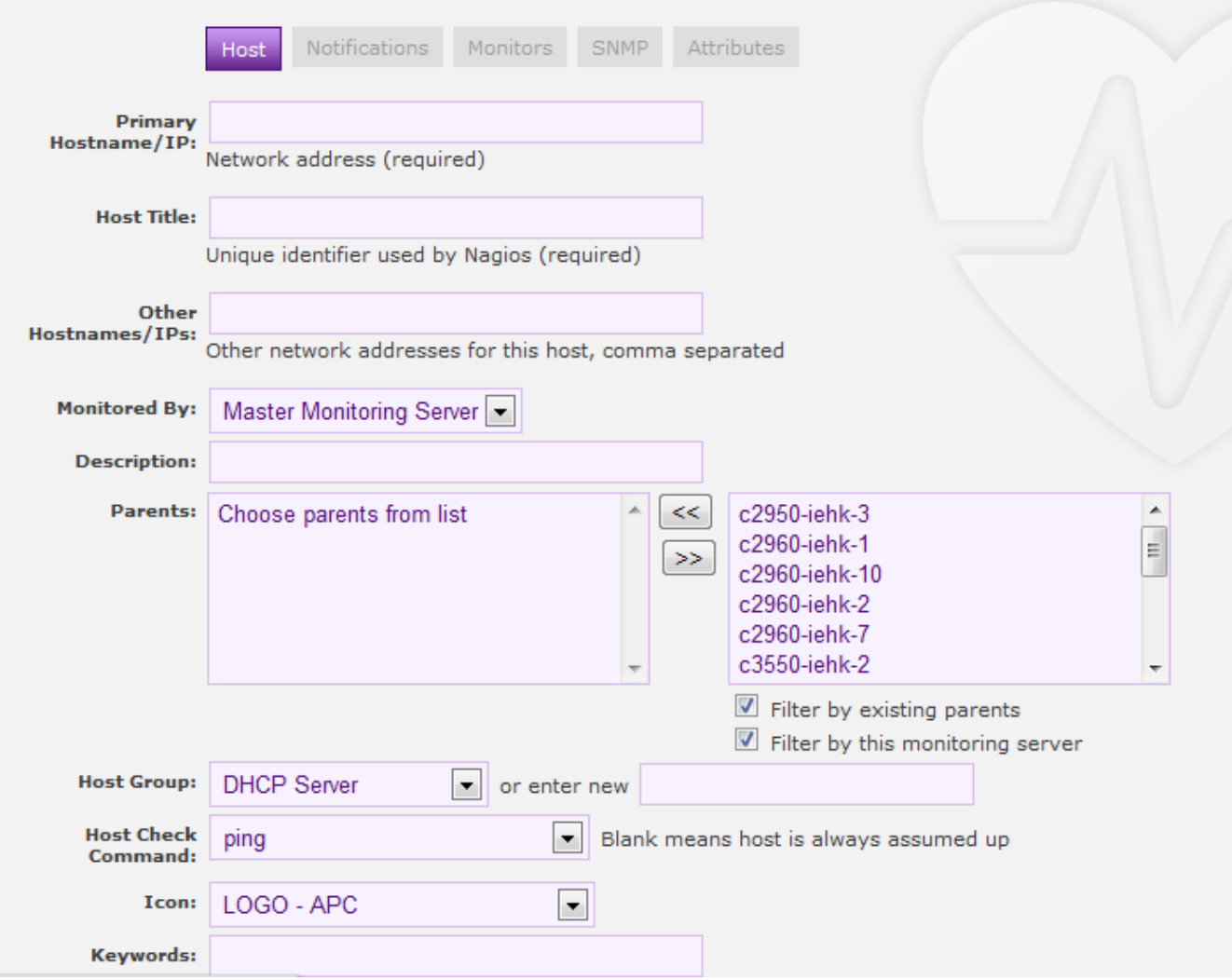
Audit Log > List

Filters: None

Pages: 1 2 3 4 5 6 7 8 9 10 ... 100 all

	Date / Time	Username	Text
4985	2012-02-06 08:31:58	SYSTEM	Username 'smeyer' logged in via auth_tkt
4984	2012-02-06 08:14:29	SYSTEM	Username 'ubalci' logged in via auth_tkt
4983	2012-02-06 08:14:29	SYSTEM	Username 'ubalci' logged in via auth_tkt
4982	2012-02-06 08:14:28	SYSTEM	Username 'ubalci' logged in via auth_tkt
4981	2012-02-06 08:00:21	SYSTEM	Username 'smeyer' logged in via auth_tkt
4980	2012-02-06 06:15:22	SYSTEM	opsview_sync_ldap: End
4979	2012-02-06 06:15:22	SYSTEM	Backup completed Restore

Konfiguration



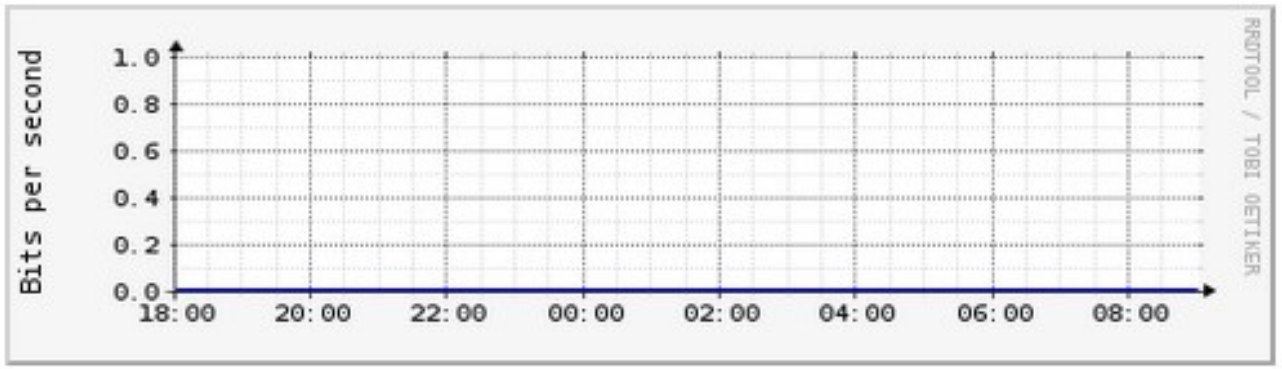

```
define host{
    use generic-host
    host_name hogwarts
    alias Web- und SMB-Server
    address 192.168.1.1
    check_command check-host-alive
    max_check_attempts 10
    notification_interval 60
    notification_period 24x7
    notification_options d,u,r
}

define service{
    use generic-service
    host_name  hogwarts
    service_description  HTTP
    is_volatile  0
    check_period  24x7
    max_check_attempts  3
    normal_check_interval  3
    retry_check_interval  1
    contact_groups  server-admins
    notification_interval  120
    notification_period  24x7
    notification_options  w,u,c,r
    check_command  check_http
}
```

MRTG

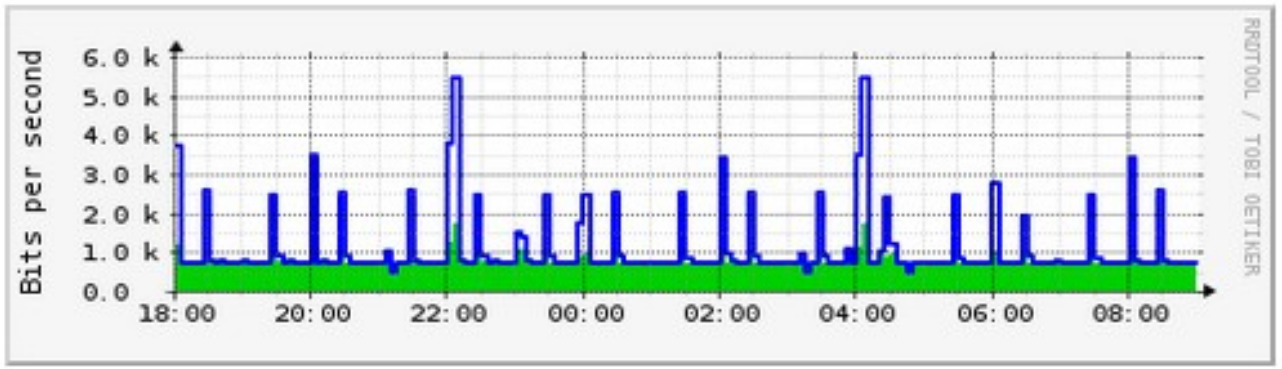
Network Traffic

Host	Network Tra
c2940-iehk-1	MRTG Graphs
c2950-iehk-1	MRTG Graphs
c2950-iehk-2	MRTG Graphs
c2950-iehk-3	MRTG Graphs
c2960-iehk-1	MRTG Graphs
c2960-iehk-10	MRTG Graphs
c2960-iehk-11	MRTG Graphs
c2960-iehk-12	MRTG Graphs
c2960-iehk-13	MRTG Graphs

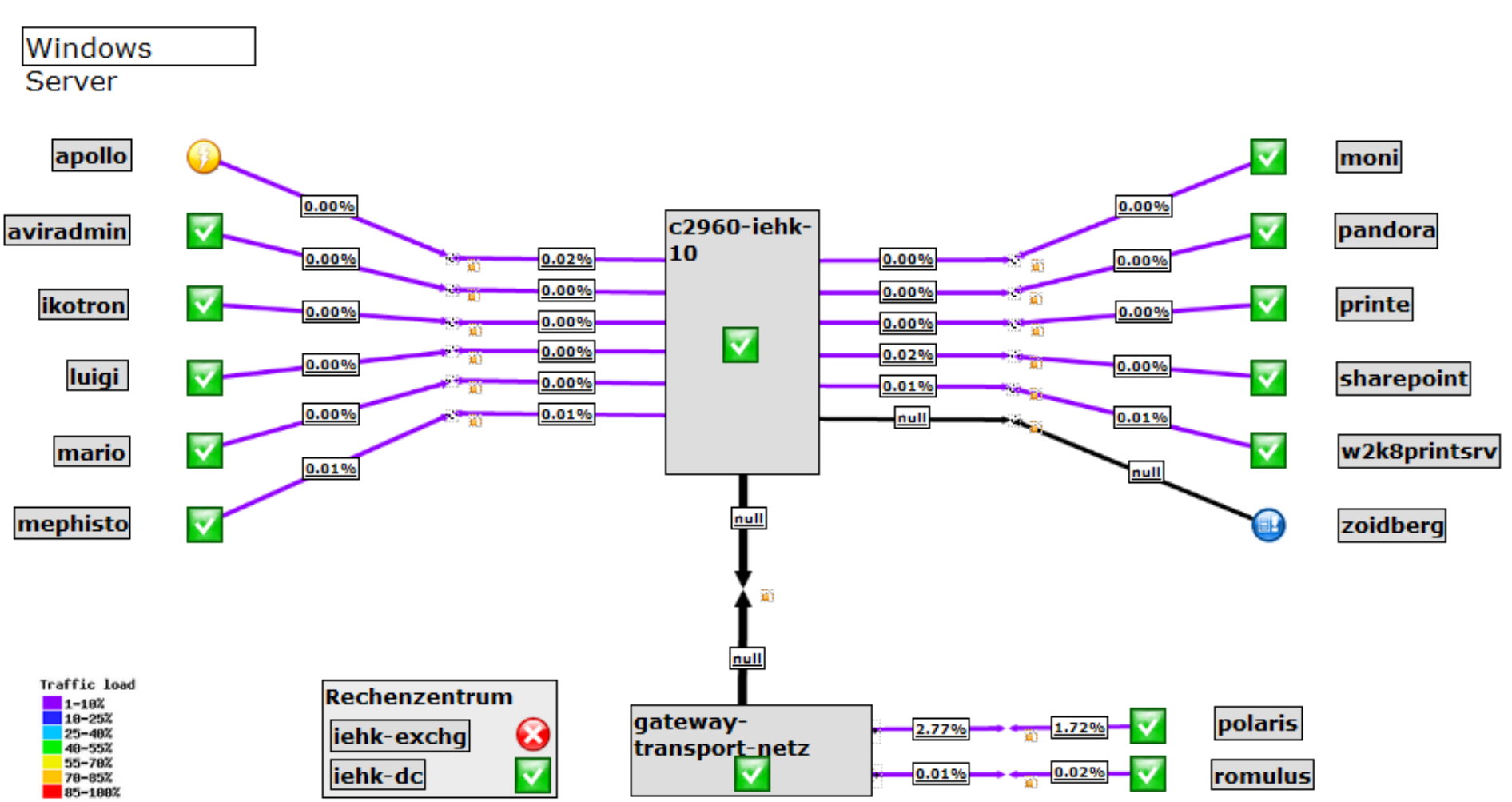
Vlan1



Vlan348

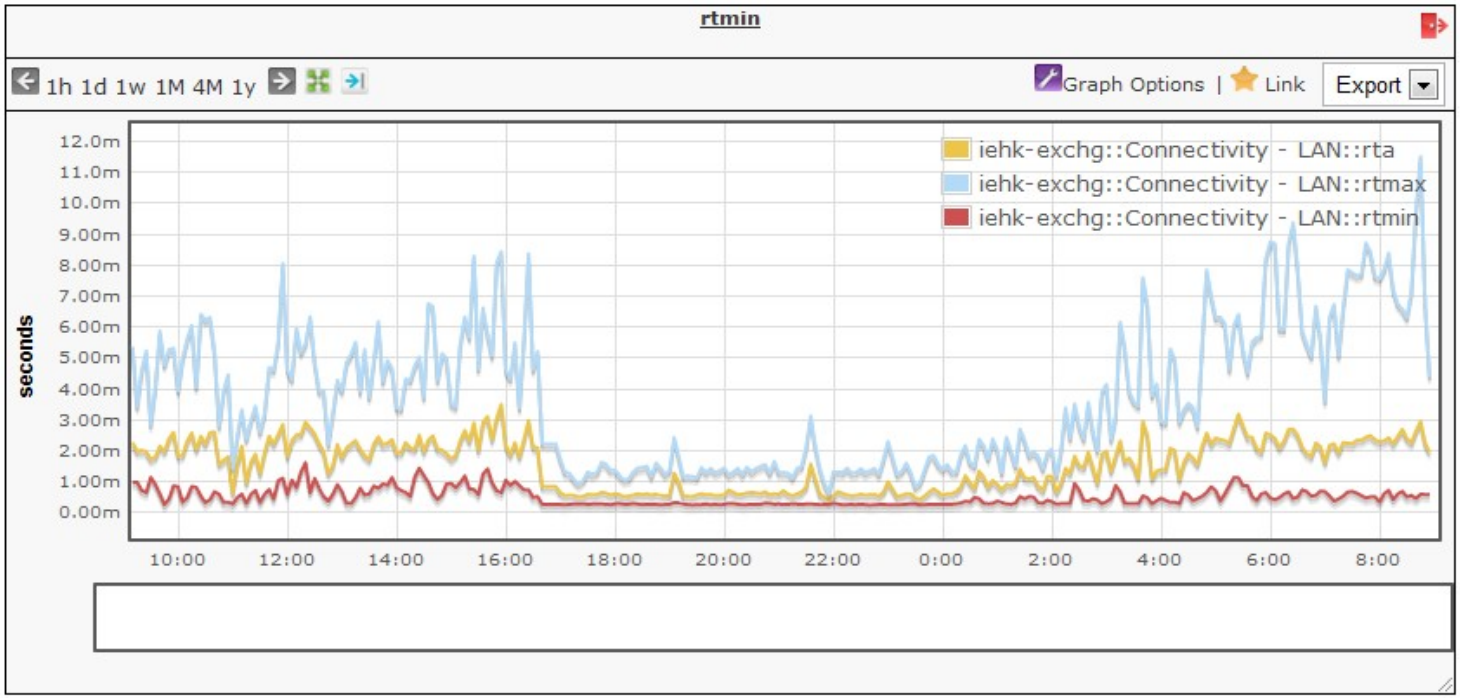


NagVis


Windows Server
apollo
aviradmin
ikotron
luigi
mario
mephisto
0.00%
0.02%
0.01%
c2960-iehk-10
null
moni
pandora
printe
sharepoint
w2k8printsrv
zoidberg
Traffic load
1-10%
10-25%
25-40%
40-55%
55-70%
70-85%
85-100%
Rechenzentrum
iehk-exchg
iehk-dc
gateway-transport-netz
2.77%
1.72%
0.01%
0.02%
polaris
romulus

Data Warehouse

- Data Warehouse
  - Speicherung von historischen Daten
  - Angeschlossenes DBMS (hier MySQL)
  - Reports, Dashboards



Warnings - Last 24h

7

Criticals - last 24h

0

CPU [%] - 24h avg.

36.11

Memory [%] - 24h avg.

89.09

Total checks - last 24h

8215

rta [ms] - 24h avg.

0.18

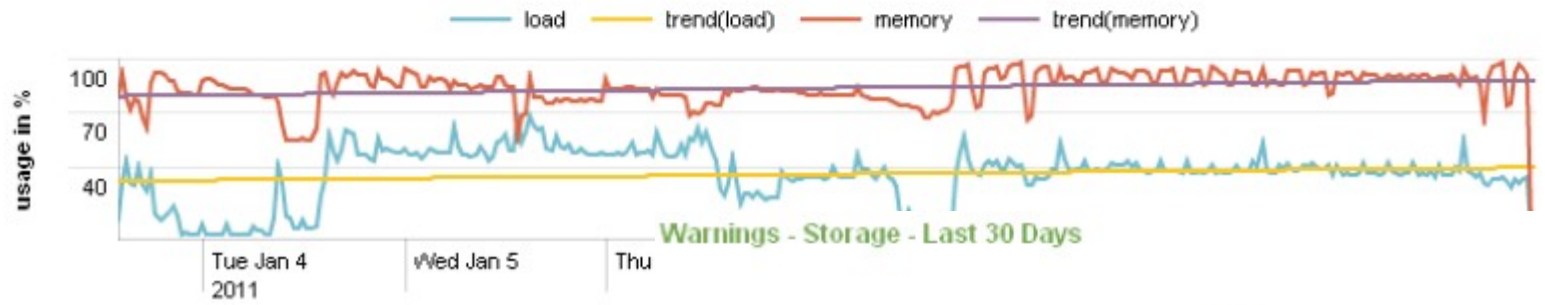
BW In [MB/s] - 24h avg.

0.06

BW Out [MB/s] - 24h avg.

0.14

Performance Metrics - 7d avg.



Warnings - Storage - Last 30 Days

Benachrichtigungen

PROBLEM: SNMP - Load is CRITICAL

helpdesk@iehk.rwth-aachen.de

Aktionen

An: Sven Meyer

Montag, 6. Februar 2012 04:39

PROBLEM: SNMP - Load is CRITICAL on host nagios3

Host: nagios3 (127.0.0.1)
Description: Opsview Master Server

Service: SNMP - Load
State: **CRITICAL**

Date & Time: Mon Feb 6 04:39:28 CET 2012

Additional Information:
1 CPU, load 99.0% > 95% : CRITICAL

- Acknowledge service problem
- Delay next notification
- Disable notifications for this service
- Schedule service check

Notification #1

Nachteile

- Höhere Anforderung als Nagios Core
- Web-Interface erlaubt keine externen CGIs
    - z.B. Nagios BPI Plug-Ins
- Konfiguration ausschließlich über Front-End
- Data Warehouse nur bedingt sinnvoll