Das Monitoring Ökosystem

Nagios / Icinga / Shinken und deren viele Erweiterungen

Sebastian 'tokkee' Harl
<sh@tokkee.org>

Grazer Linuxtage
20. April 2013

Monitoring-Systeme – Überblick

„Klassisch“ war Nagios® das Open-Source Monitoring-System der Wahl. Mittlerweile gibt es diverse Abspaltungen davon.

- Nagios 1 / 2 ;-)
- Nagios 3
- Nagios 4
- Icinga 1
- Icinga 2
- Shinken

Nicht-Nagios-ähnliche System

Nebenbei existieren (zum Teil auch schon seit Langem) diverse Monitoring-Systeme, die sich nicht aus dem Nagios-Umfeld entwickelt haben. Diese sind nicht Schwerpunkt dieses Vortrags!

- Observium
- OpenNMS
- Zabbix
- Zenoss
- ...

Komponenten eines Monitoring-Systems

Neben dem eigentlichen Monitoring-Kern werden diverse andere Komponenten benötigt:

- Monitoring-Plugins
- Web-Frontend
- Konfigurationswerkzeuge
- Aufbereitung von Performance-Daten
  $\rightarrow$ Performance-Analyse, Kapazitätsplanung
- Reporting
- ...

Monitoring-Plugins

Nagios Plugins: `http://nagiosplugins.org/`

- UNIX/Linux Basisüberwachung
- Basisüberwachung einiger Dienste (z.B. Jabber, PostgreSQL)
- Definition / Dokumentation von API und Verhalten von Plugins
  `http://nagiosplug.sourceforge.net/developer-guidelines.html`
  (Developer Guidelines)

Monitoring-Plugins (2)

teamix Monitoringplugins:
`https://teamix.org/projects/monitoringplugins`

- Juniper, NetApp Überwachung

ConSol Nagios Plugins: `http://labs.consol.de/nagios/`

- Oracle, MSSQL, DB2, Logfile Überwachung

Monitoring-Plugins (3)

op5 Plugins:
`http://op5.org/community/plugin-inventory/op5-projects`

- VMWare Überwachung

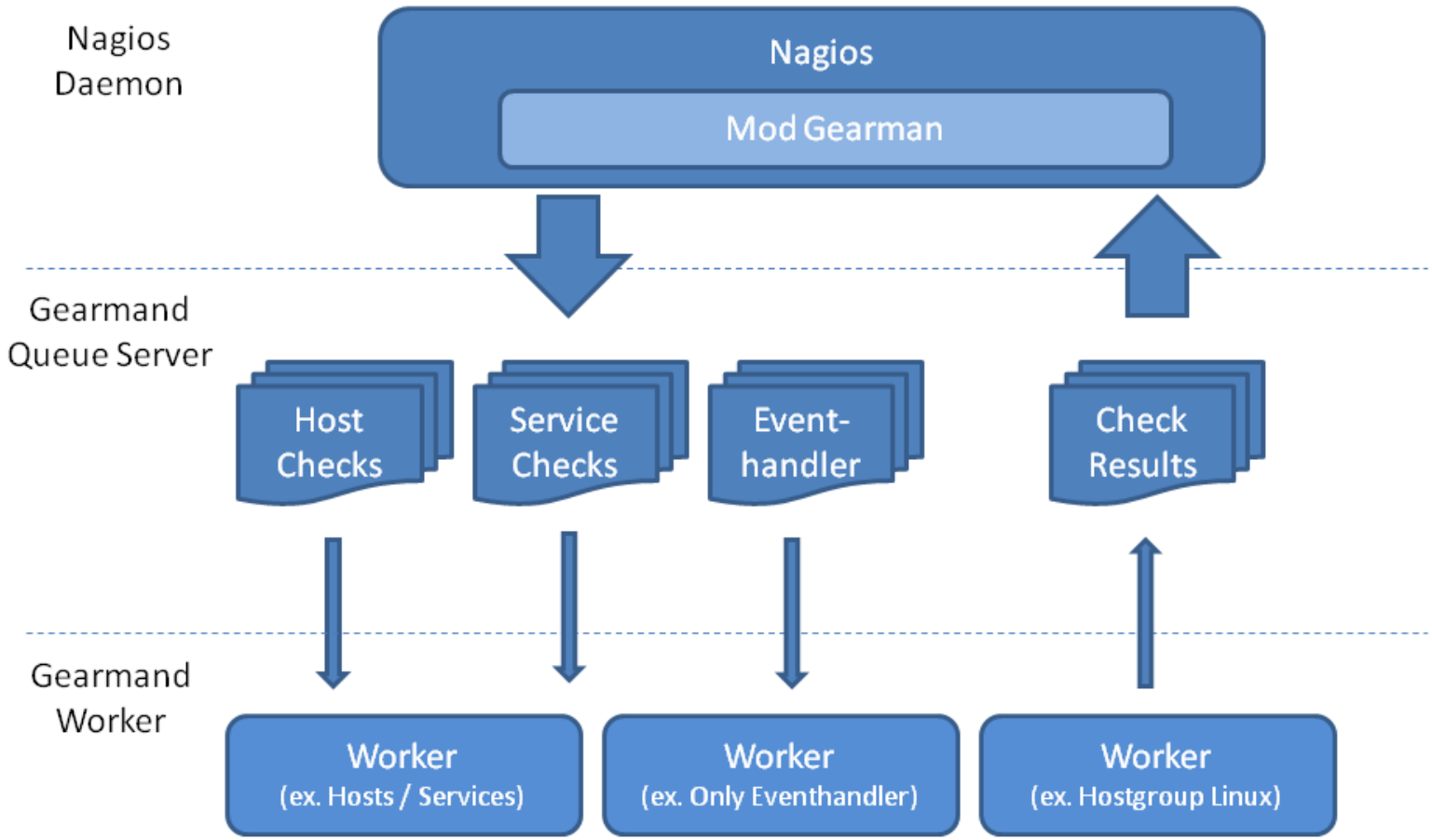
Netways Monitoringplugsin:
`https://www.netways.org/projects/plugins`

- div. Hardware, SAP Überwachung
- Erweiterte Überwachung Linux-Systeme

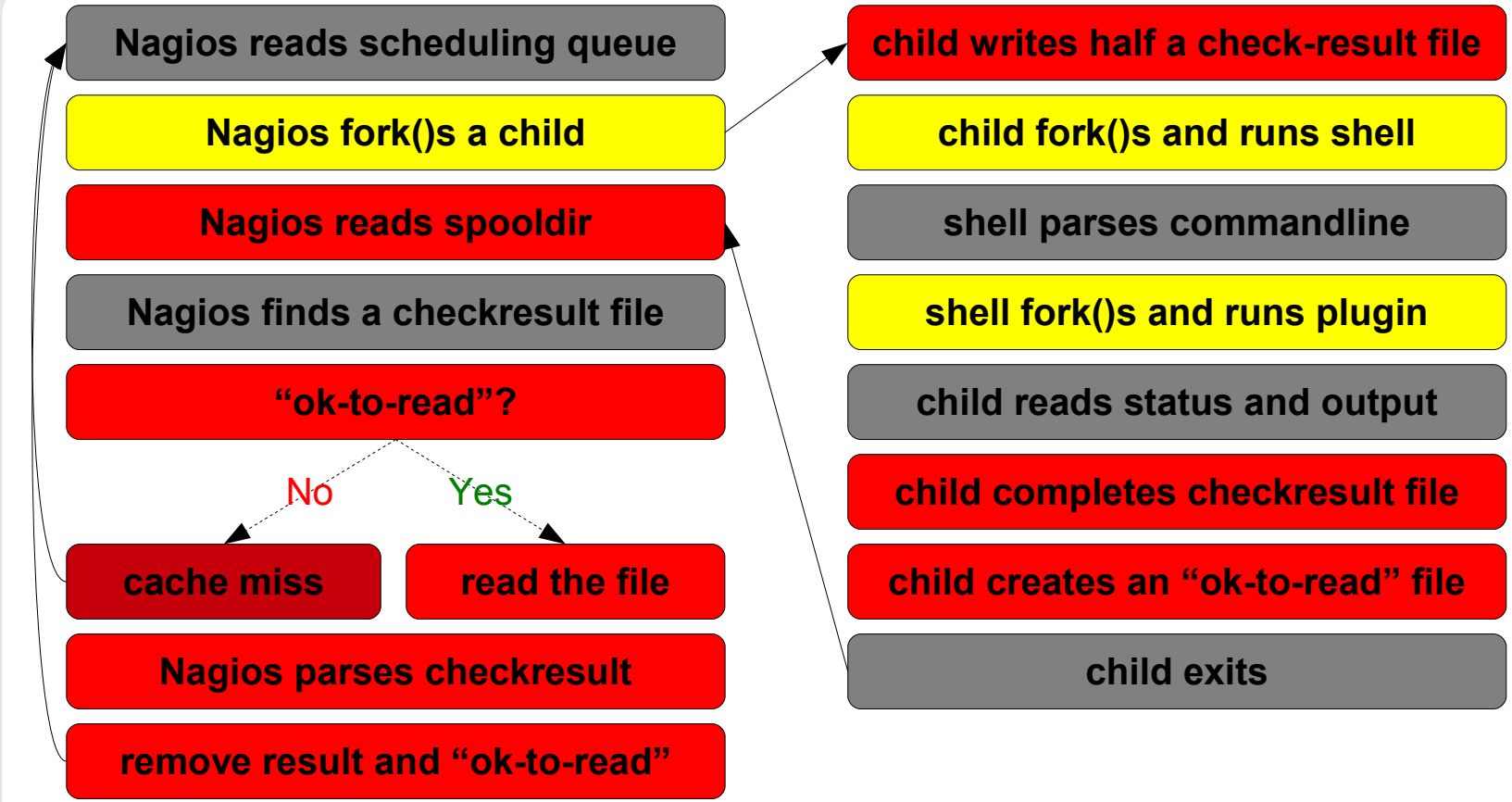
Core Erweiterungen

Lastverteilung, Distributed Monitoring

Mod Gearman: `https://labs.consol.de/nagios/mod-gearman/`



Current check flowchart - hotspots



Status Abfrage

MK Livestatus:

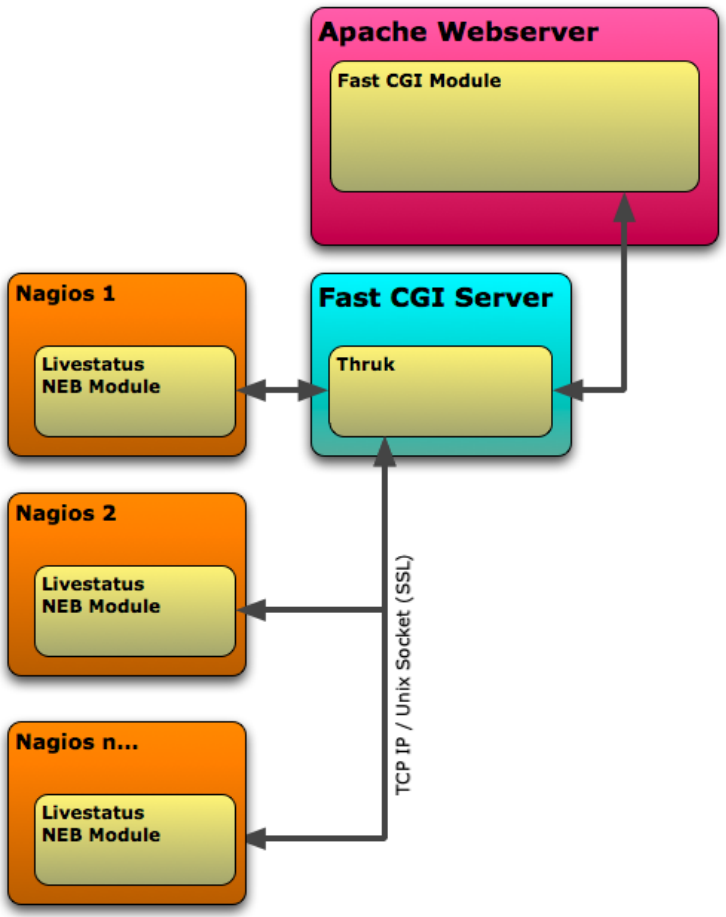
`http://mathias-kettner.de/checkmk_livestatus.html`

- Live-Abfrage von Status-Daten aus dem Monitoring-Kern
- Nagios, Icinga und Shinken
- keine Datenbank, kein messbarer Overhead
- Schnittstelle für viele Addons (Thruk, NagVis, NagiosBP, Multisite, ...)

Frontends

Thruk

Thruk: `http://thruk.org/`

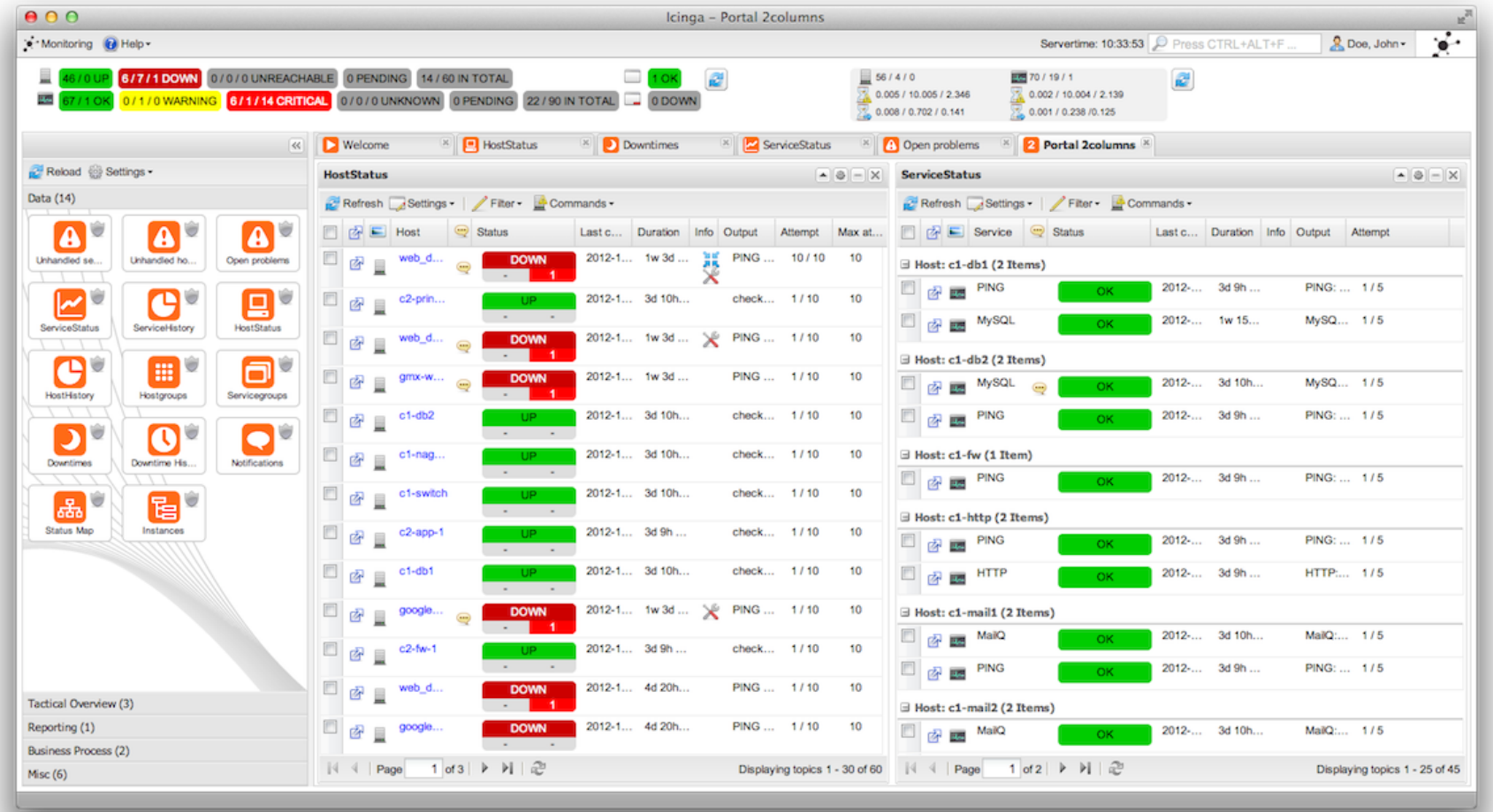


- mehrere (auch unterschiedliche) Backends
  $\Rightarrow$ distributed monitoring
- verwendet Livestatus
- div. Plugins, z.B.:
  - Config Tool
  - Panorama (Dashboard)
  - Reports
  - Statusmap
- mächtige Filter

Icinga Web

Icinga Web: `https://www.icinga.org/about/icingaweb/`

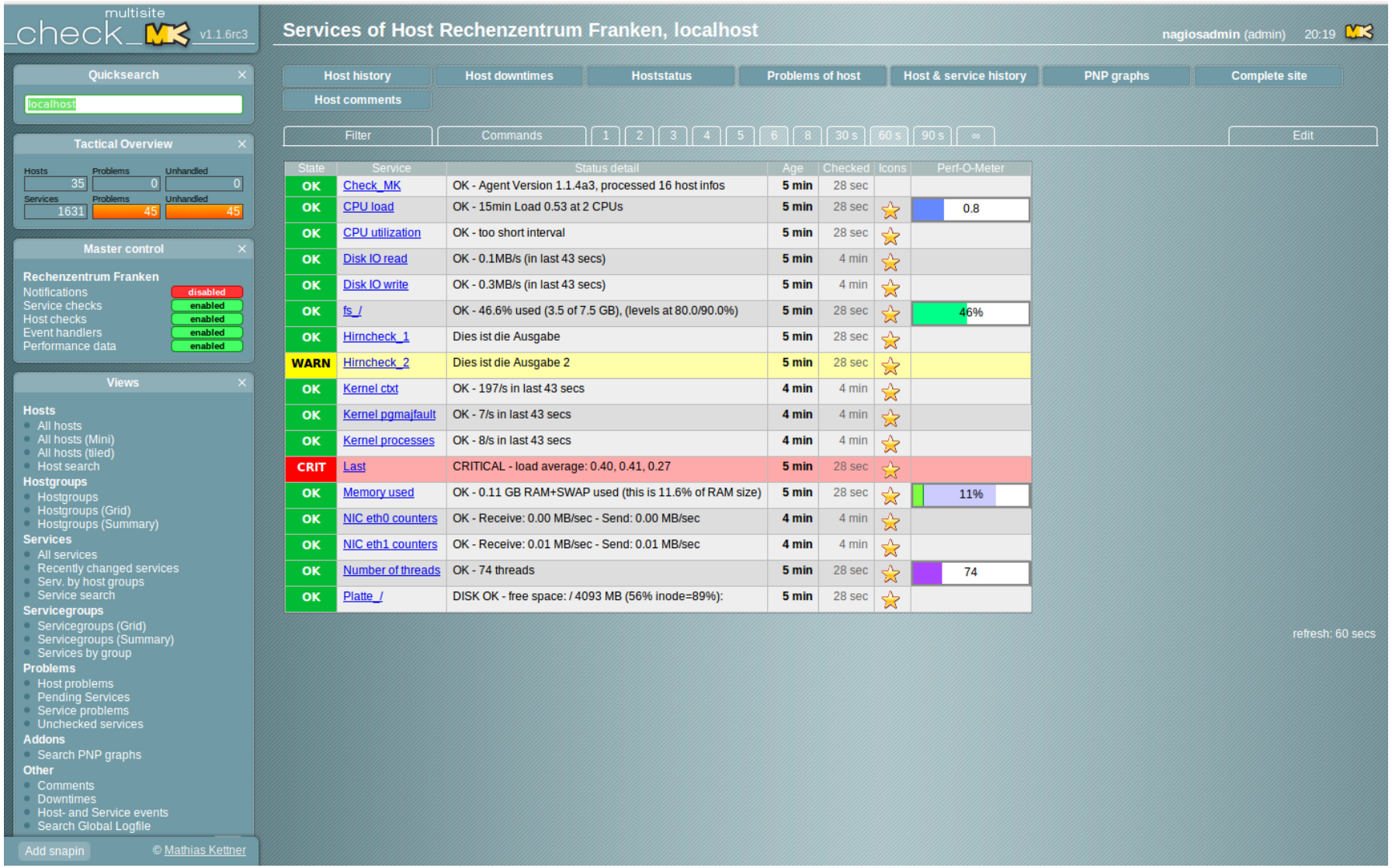
- AJAX-Webinterface
  $\Rightarrow$ dynamische Sortierung/Gruppierung, Suche
- Erweiterbar durch sog. „Cronks“
- flexible Berechtigungsstruktur


Icinga – Portal 2columns
Monitoring
Help
Servertime: 10:33:53
Press CTRL+ALT+F ...
Doe, John
46 / 0 UP
6 / 7 / 1 DOWN
0 / 0 / 0 UNREACHABLE
0 PENDING
14 / 60 IN TOTAL
67 / 1 OK
0 / 1 / 0 WARNING
6 / 1 / 14 CRITICAL
0 / 0 / 0 UNKNOWN
0 PENDING
22 / 90 IN TOTAL
1 OK
0 DOWN
Welcome
HostStatus
Downtimes
ServiceStatus
Open problems
Portal 2columns
Reload
Settings
Data (14)
Unhandled se...
Unhandled ho...
Open problems
ServiceStatus
ServiceHistory
HostStatus
HostHistory
Hostgroups
Servicegroups
Downtimes
Downtime His...
Notifications
Status Map
Instances
Tactical Overview (3)
Reporting (1)
Business Process (2)
Misc (6)
HostStatus
Refresh
Settings
Filter
Commands
Host
Status
Last c...
Duration
Info
Output
Attempt
Max at...
Page 1 of 3
Displaying topics 1 - 30 of 60
ServiceStatus
Service
Host: c1-db1 (2 Items)
Host: c1-db2 (2 Items)
Host: c1-fw (1 Item)
Host: c1-http (2 Items)
Host: c1-mail1 (2 Items)
Host: c1-mail2 (2 Items)
Page 1 of 2
Displaying topics 1 - 25 of 45

MK Multisite

MK Multisite:
`http://mathias-kettner.de/checkmk_multisite.html`

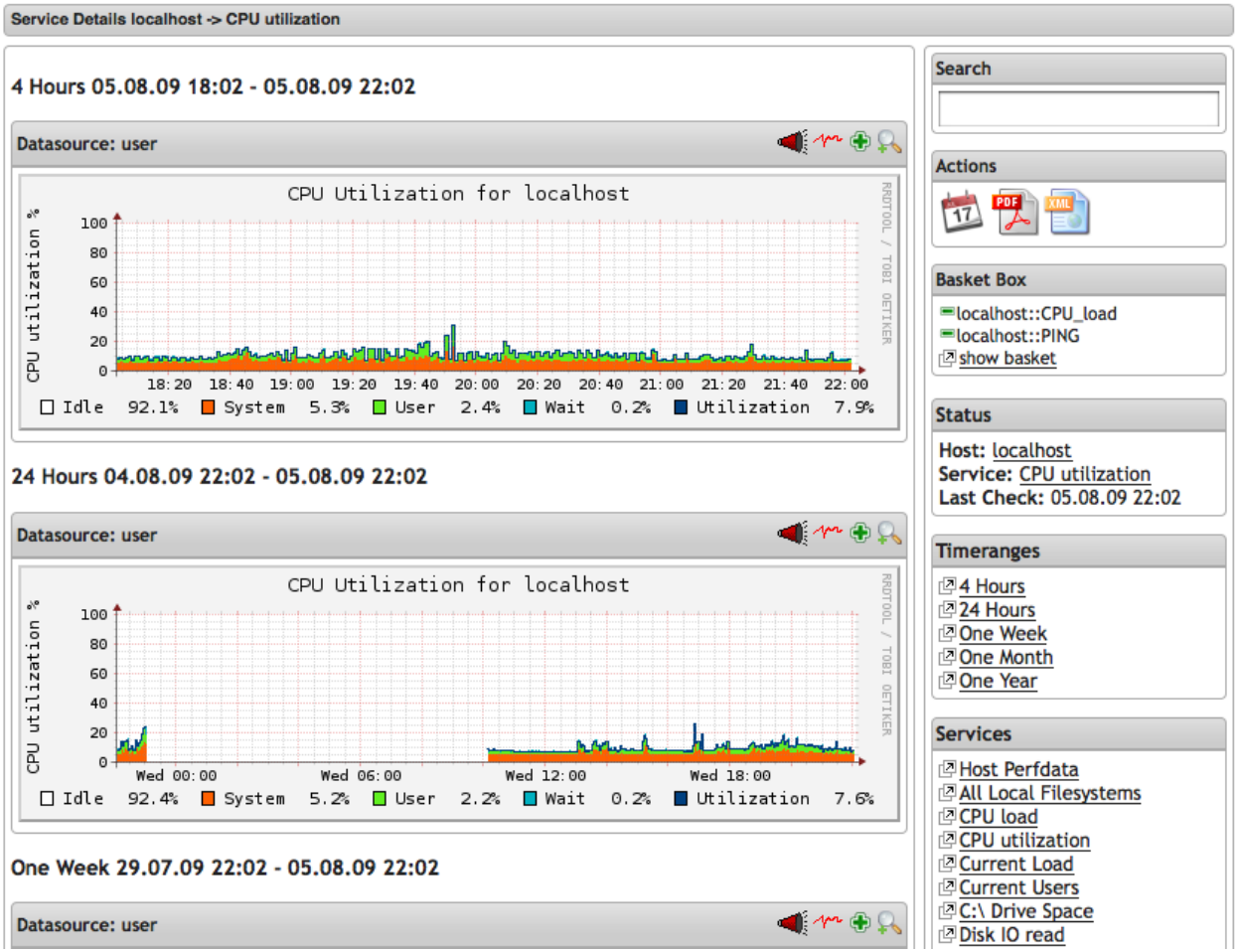
- verwendet Livestatus
- distributed monitoring
- Plugins und Benutzer-definierte Sidebar
- konfigurierbare Ansichten mit mächtigen Filtern


multisite
check_MK v1.1.6rc3
Services of Host Rechenzentrum Franken, localhost
nagiosadmin (admin) 20:19
Quicksearch
localhost
Tactical Overview
Hosts 35 Problems 0 Unhandled 0
Services 1631 Problems 45 Unhandled 45
Master control
Rechenzentrum Franken
Notifications disabled
Service checks enabled
Host checks enabled
Event handlers enabled
Performance data enabled
Views
Hosts
All hosts
All hosts (Mini)
All hosts (tiled)
Host search
Hostgroups
Hostgroups
Hostgroups (Grid)
Hostgroups (Summary)
Services
All services
Recently changed services
Serv. by host groups
Service search
Servicegroups
Servicegroups (Grid)
Servicegroups (Summary)
Services by group
Problems
Host problems
Pending Services
Service problems
Unchecked services
Addons
Search PNP graphs
Other
Comments
Downtimes
Host- and Service events
Search Global Logfile
Add snapin
© Mathias Kettner
Host history
Host downtimes
Hoststatus
Problems of host
Host & service history
PNP graphs
Complete site
Host comments
Filter
Commands
1 2 3 4 5 6 8 30 s 60 s 90 s ∞
Edit
State Service Status detail Age Checked Icons Perf-O-Meter
OK Check_MK OK - Agent Version 1.1.4a3, processed 16 host infos 5 min 28 sec
OK CPU load OK - 15min Load 0.53 at 2 CPUs 5 min 28 sec 0.8
OK CPU utilization OK - too short interval 5 min 28 sec
OK Disk IO read OK - 0.1MB/s (in last 43 secs) 5 min 4 min
OK Disk IO write OK - 0.3MB/s (in last 43 secs) 5 min 4 min
OK fs_/ OK - 46.6% used (3.5 of 7.5 GB), (levels at 80.0/90.0%) 5 min 28 sec 46%
OK Hirncheck_1 Dies ist die Ausgabe 5 min 28 sec
WARN Hirncheck_2 Dies ist die Ausgabe 2 5 min 28 sec
OK Kernel ctxt OK - 197/s in last 43 secs 4 min 4 min
OK Kernel pgmajfault OK - 7/s in last 43 secs 4 min 4 min
OK Kernel processes OK - 8/s in last 43 secs 4 min 4 min
CRIT Last CRITICAL - load average: 0.40, 0.41, 0.27 5 min 28 sec
OK Memory used OK - 0.11 GB RAM+SWAP used (this is 11.6% of RAM size) 5 min 28 sec 11%
OK NIC eth0 counters OK - Receive: 0.00 MB/sec - Send: 0.00 MB/sec 4 min 4 min
OK NIC eth1 counters OK - Receive: 0.01 MB/sec - Send: 0.01 MB/sec 4 min 4 min
OK Number of threads OK - 74 threads 5 min 28 sec 74
OK Platte_/ DISK OK - free space: / 4093 MB (56% inode=89%): 5 min 28 sec
refresh: 60 secs

Addons

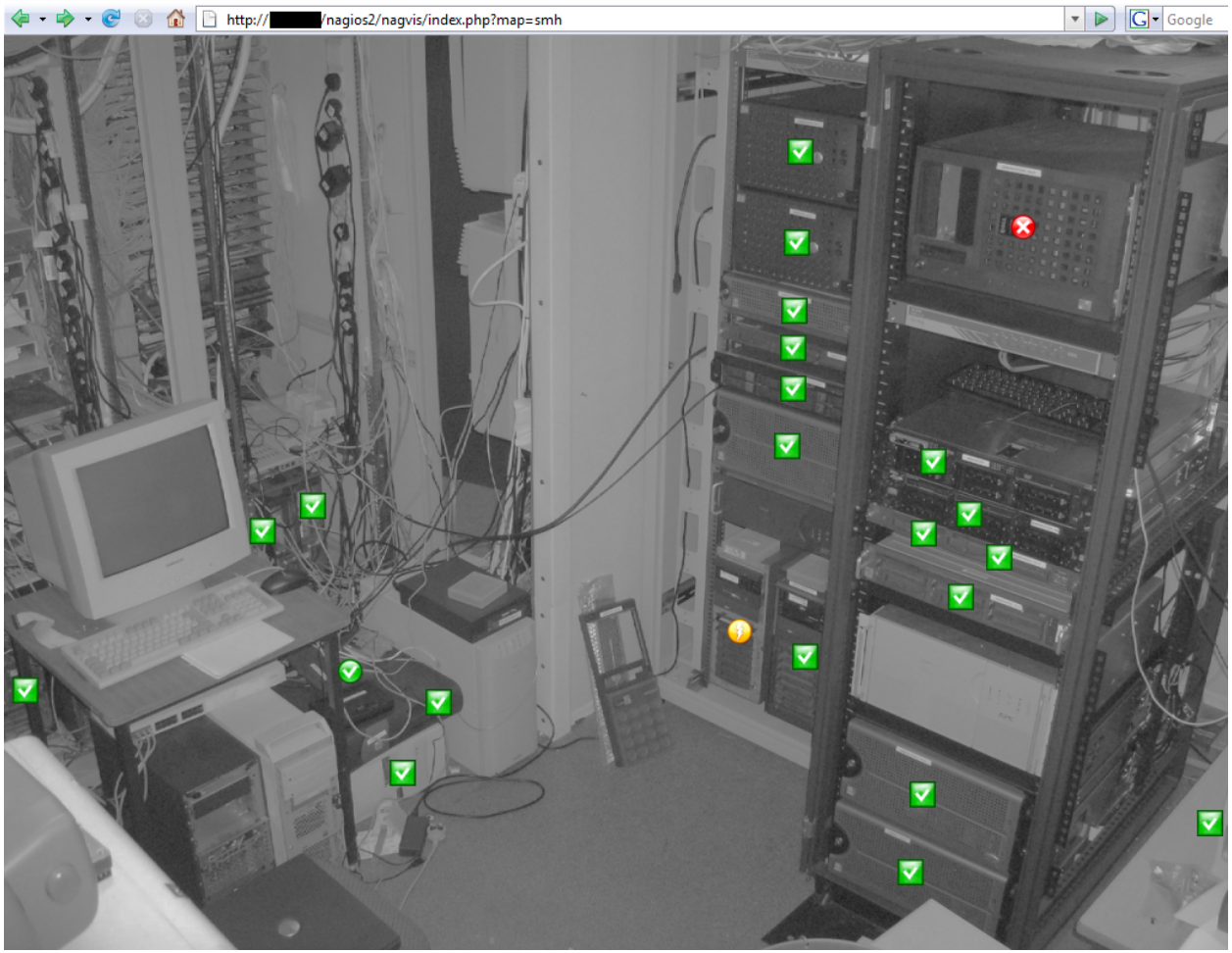
PNP4Nagios

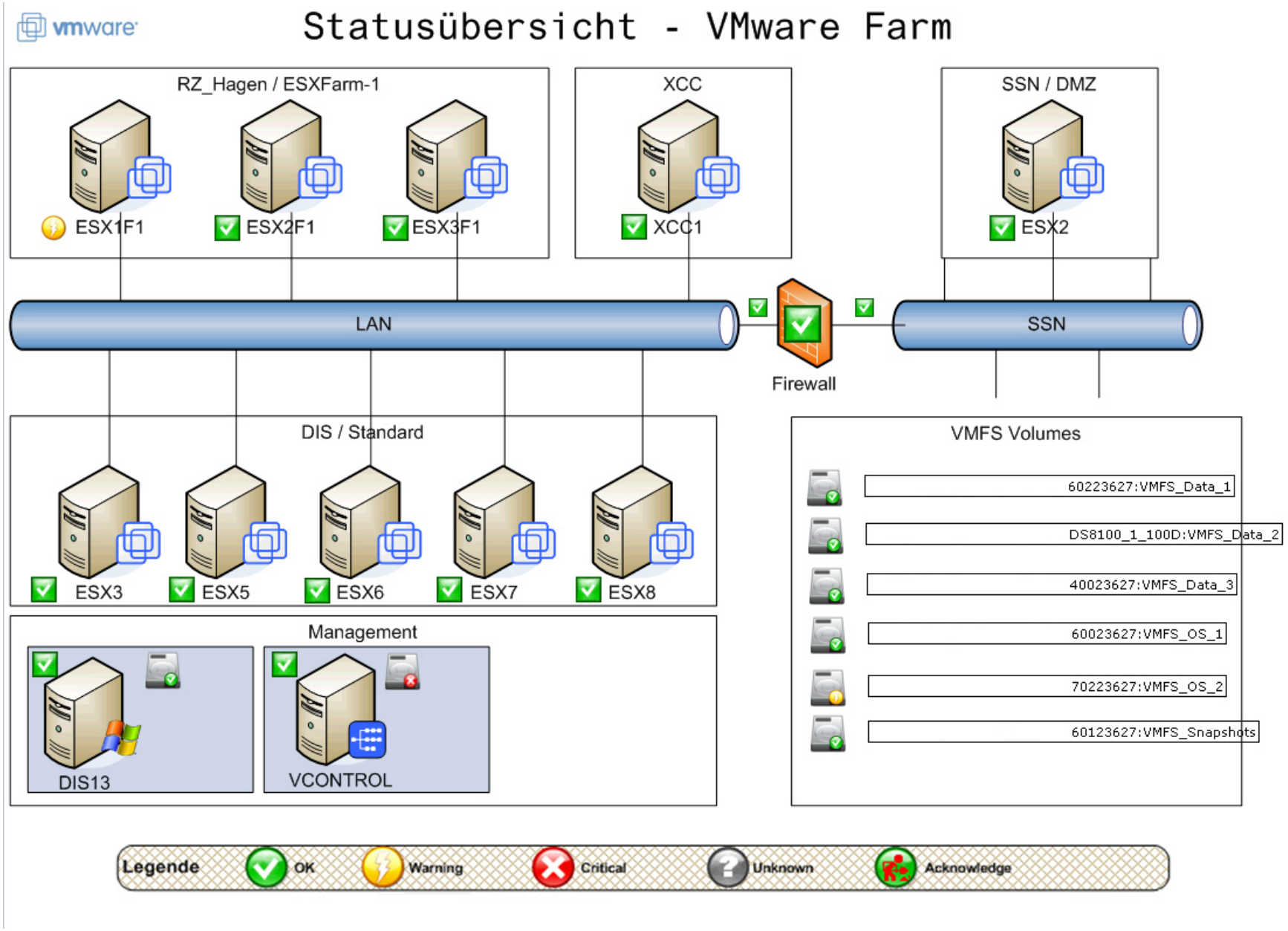
PNP4Nagios: `http://www.pnp4nagios.org/`



NagVis

NagVis: `http://www.nagvis.org/`




vmware
Statusübersicht - VMware Farm
RZ_Hagen / ESXFarm-1
ESX1F1
ESX2F1
ESX3F1
XCC
XCC1
SSN / DMZ
ESX2
LAN
Firewall
SSN
DIS / Standard
ESX3
ESX5
ESX6
ESX7
ESX8
Management
DIS13
VCONTROL
VMFS Volumes
60223627:VMFS_Data_1
DS8100_1_100D:VMFS_Data_2
40023627:VMFS_Data_3
60023627:VMFS_OS_1
70223627:VMFS_OS_2
60123627:VMFS_Snapshots
Legende
OK
Warning
Critical
Unknown
Acknowledge

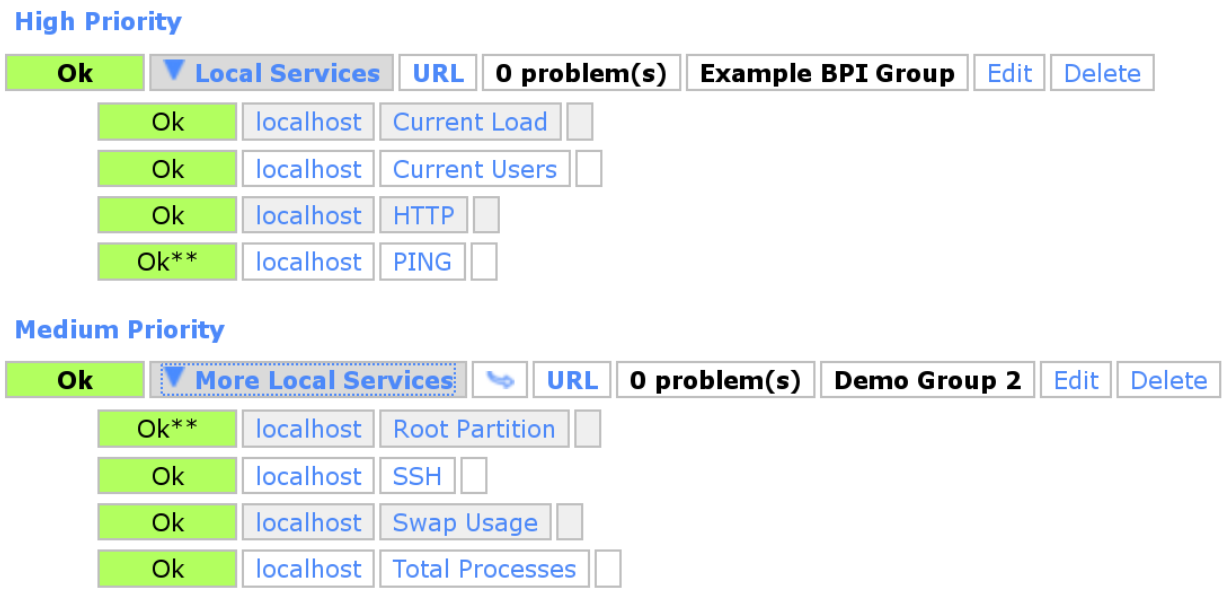
Business Prozesse

Nagios Business Process Addons:

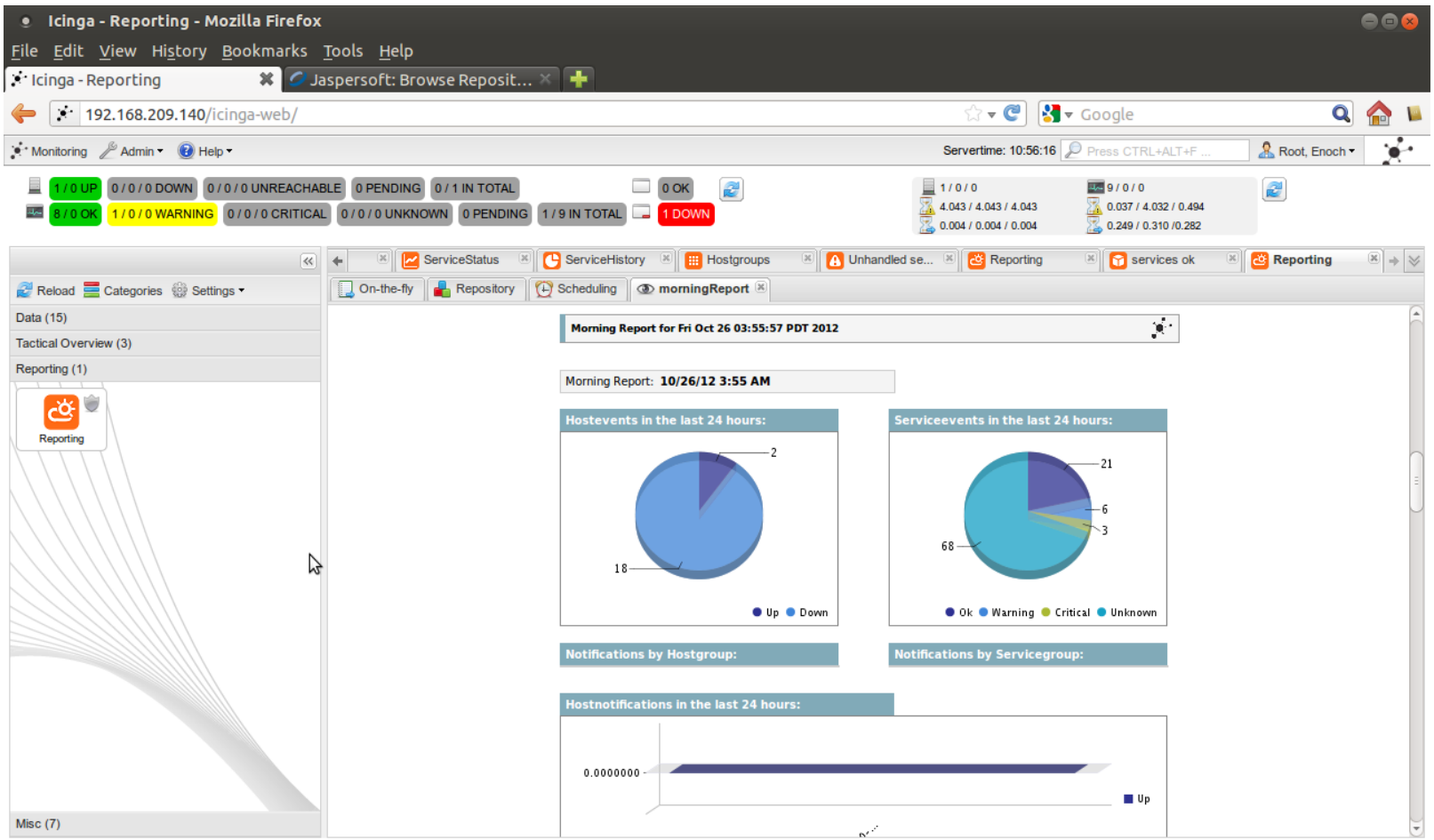
`http://bp-addon.monitoringexchange.org/`

Nagios Business Process Intelligence:

`http://assets.nagios.com/downloads/exchange/nagiosbpi/nagiosbpi.zip`

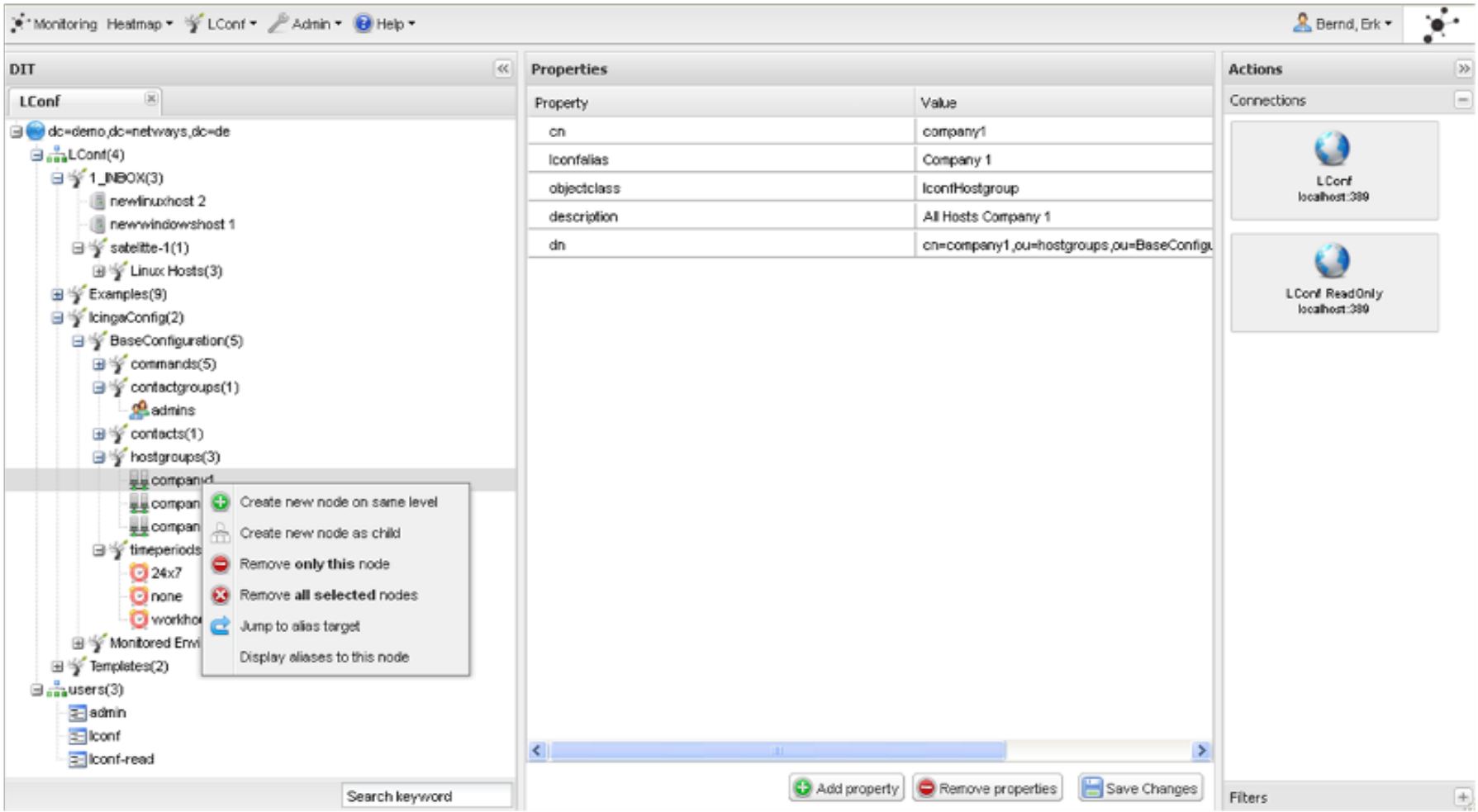


Reports mit Jasper



Konfiguration

- **Thruk!** :-)
- **LConf:** `https://www.netways.org/projects/lconf`
- **NConf:** `http://www.nconf.org/`
- Auto-Konfiguration (?!)
  - Wann macht das Sinn?
  - **Check_MK:** `http://mathias-kettner.de/check_mk.html`
  - nmap (nmap2nagios), traceroute
  - CMDB?


Monitoring
Heatmap
LConf
Admin
Help
Bernd, Erk
DIT
LConf
dc=demo,dc=netways,dc=de
LConf(4)
1_INBOX(3)
newlinuxhost 2
newwindowshost 1
satellite-1(1)
Linux Hosts(3)
Examples(9)
IcingaConfig(2)
BaseConfiguration(5)
commands(5)
contactgroups(1)
admins
contacts(1)
hostgroups(3)
company1
timeperiods
24x7
none
Monitored Envi
Templates(2)
users(3)
admin
lconf
lconf-read
Search keyword
Create new node on same level
Create new node as child
Remove only this node
Remove all selected nodes
Jump to alias target
Display aliases to this node
Properties
Property
Value
cn
company1
lconfalias
Company 1
objectclass
lconfHostgroup
description
All Hosts Company 1
dn
cn=company1,ou=hostgroups,ou=BaseConfigu
Add property
Remove properties
Save Changes
Actions
Connections
LConf
localhost:389
LConf ReadOnly
localhost:389
Filters

Datensammler

Nagios und seine Alternativen haben sehr viel Overhead pro tatsächlich abgefragtem Datensatz (ist auch nicht der Fokus). Andere Systeme können das gut / besser und sollten eingebunden werden.

- **collectd:** `http://collectd.org/`
  - hochauflösende, vielseitige UNIX / Linux Performancedaten
- **EventDB, NagTrap, NSTI:**
  `https://www.netways.org/projects/eventdb`
  `http://sourceforge.net/projects/nagtrap/`
  - SNMP Traps, Syslog, Eventlog
- **Observium:** `http://www.observium.org/`
  - SNMP Queries, Inventory
- RRDtool, SQL, o.ä. von „beliebigen“ Systemen befragen

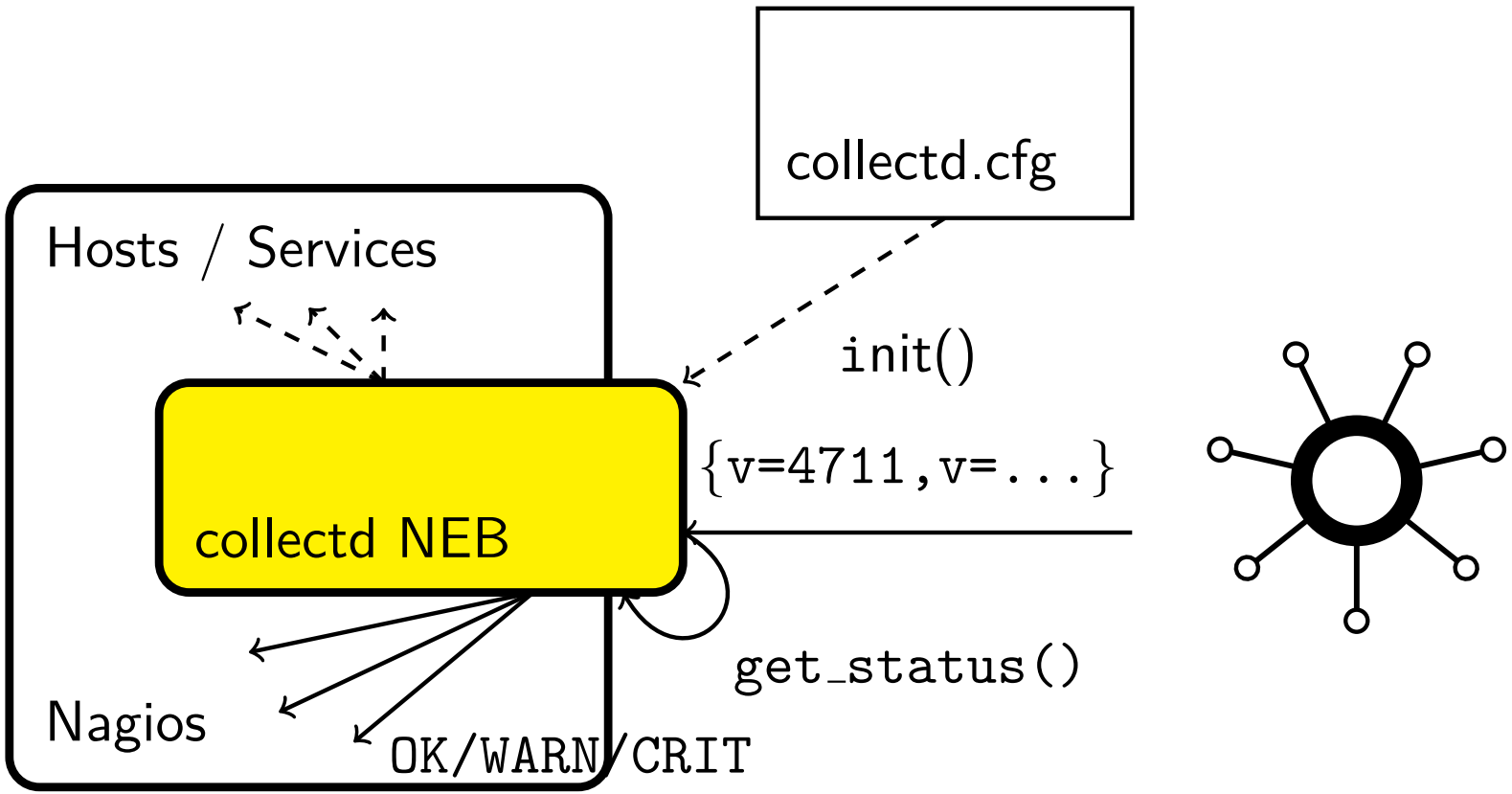
Datensammler – „state-of-the-art“

Üblicherweise aktive Abfrage von externen Systemen, beispielsweise:

```
% collectd-nagios -s /var/run/collectd-unixsock \
                  -H FQDN -n df/df-root \
                  -d free -d used -g percentage
OKAY: 31.289281 percent |
  free=46196220000.000000;;;;
  used=101446100000.000000;;;;
```

(Umbrüche nur auf den Folien)

Datensammler – schön wäre ...



Siehe auch: `https://collectd.org/wiki/index.php/Collectd-nagios`

Oder auch: spezialisierter Mod Gearman Worker

Noch Zeit? Thruk Demo!

Thruk Demo

Das Monitoring Ökosystem

Danke für die Aufmerksamkeit!

Fragen?

Kontakt: Sebastian ‘tokkee’ Harl
<sh@tokkee.org> – http://tokkee.org/

Feedback: http://glt13-programm.linuxtage.at/
https://pentabarf.linuxtage.at/feedback/GLT13/event/207.de.html