SNMP4Nagios

Grazer Linuxtage 2006

Peter Gritsch

Inhalte

- Motivation für Network Monitoring
- SNMP Grundlagen
- Nagios® Grundlagen
- *SNMP4Nagios* Plugins

Motivation für Network Monitoring

- Probleme erkennen bevor sie sich manifestieren
  - Defekte redundante Hardware (z.B. RAID-Platten)
  - Festplattenbelegung
- Ausfälle schnellstmöglich erkennen
  - Ausfall von Diensten
  - Ausfall von Geräten
- Fehlersuche erleichtern
- Argumentation gegenüber Entscheidungsträgern

Fragen zu Network Monitoring?

SNMP Grundlagen

- Simple Network Management Protocol
- Standardisiert
- Drei (relevante) Versionen (1, 2c, 3)

Bewertung

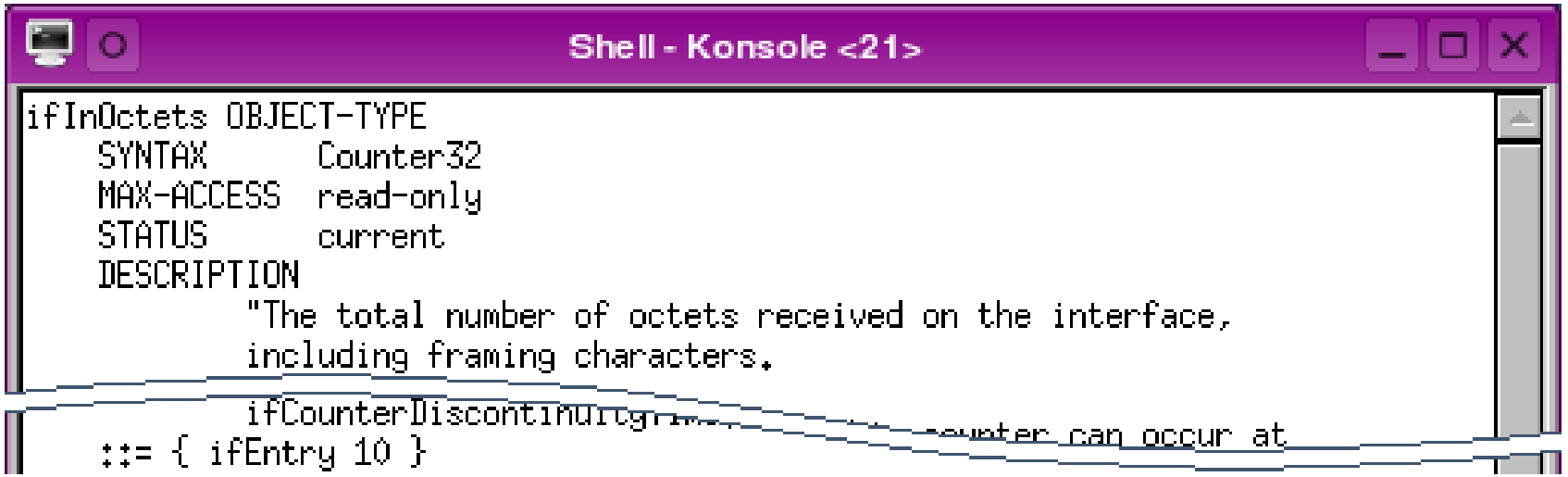
- Positiv:
  - Für “Anwender” sehr einfach
  - Für jedes ernsthafte Netzwerk-Gerät verfügbar
- Nachteile:
  - kaum vorhandene Sicherheit in den Versionen < 3
  - V3 wenig verbreitet
- Folgerung:
  - Management (V)LAN verwenden!

SNMP Terminologie

- Manager
  - Komponente, die Management Informationen verarbeitet
- Agent
  - Komponente, die Management Informationen zur Verfügung stellt
- Management Information Base
  - “Datenbank” der Management Informationen im Agent
  - Baumstruktur

Management Information Base

- Gebräuchlich: MIB-2 und Hersteller-spezifische MIBs
- Definition in “MIB files”



Object Identifiers

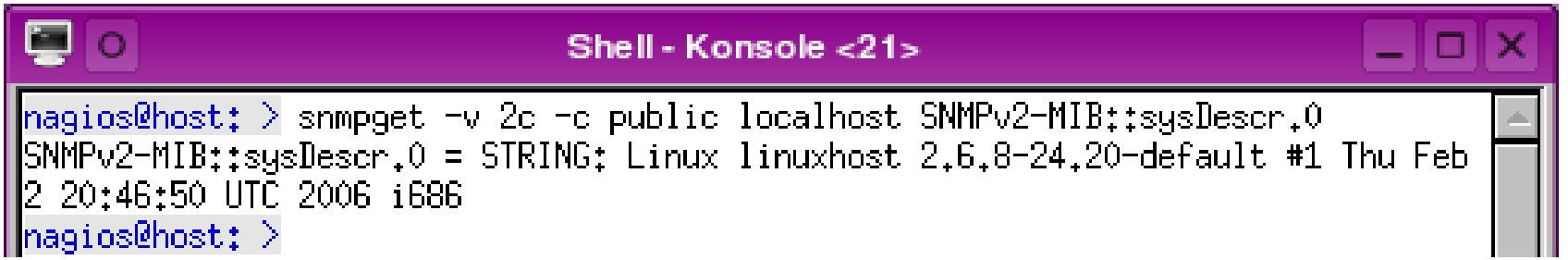
- Innerhalb des MIB-Baumes werden Objekte durch OIDs identifiziert
- Diese können als Text oder als Folge von Zahlen dargestellt werden:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
  - .1.3.6.1.2.1.1.2.0
  - SNMPv2-MIB::sysDescr.0

Pakettypen

- GetRequest
- GetNextRequest
- GetBulkRequest (V2 und höher)
- GetResponse
- SetRequest
- Trap
- Inform (V2 und höher)

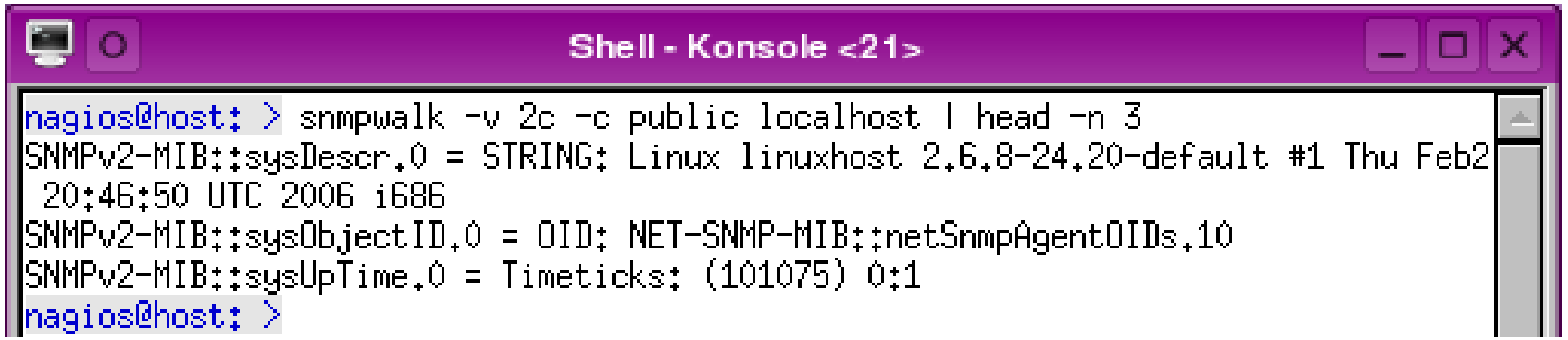
Net-SNMP Kommandos: snmpget

- Wird verwendet um einzelne Werte auszulesen
- Verwendet GetRequest- und GetResponse-Pakete
- Die OID des gesuchten Objekts muss genau bekannt sein.



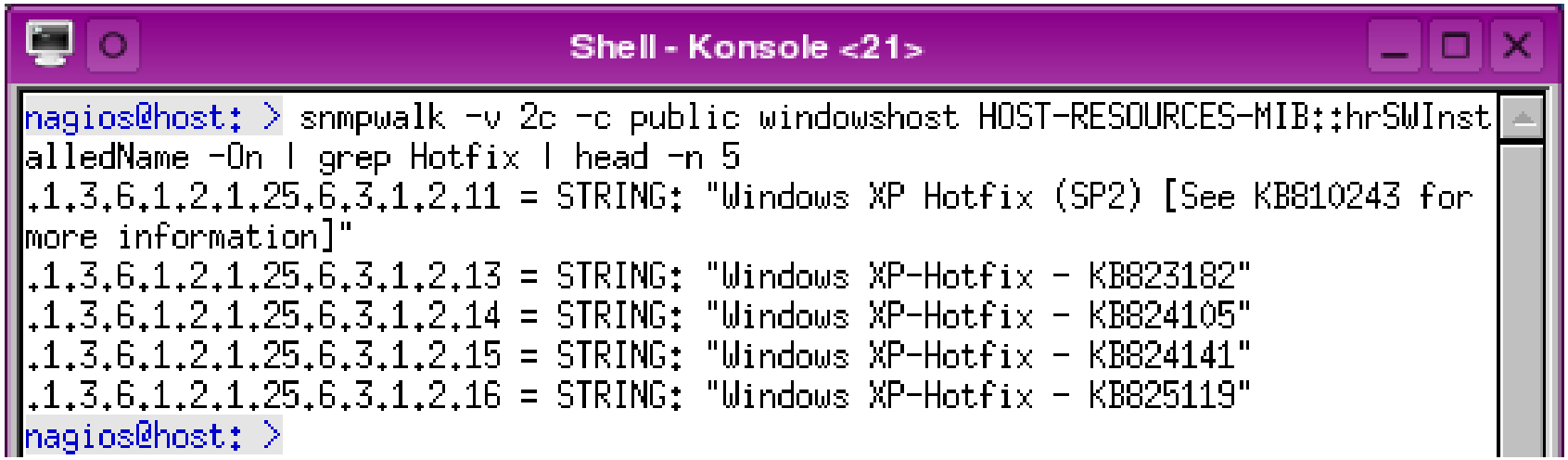
Net-SNMP Kommandos: snmpwalk

- Wird verwendet um mehrere Objekte abzufragen
- Verwendet GetNextRequest- und GetResponse-Pakete
- Wenn eine OID angegeben wird, dann bezeichnet sie den Ast, der ausgegeben werden soll.



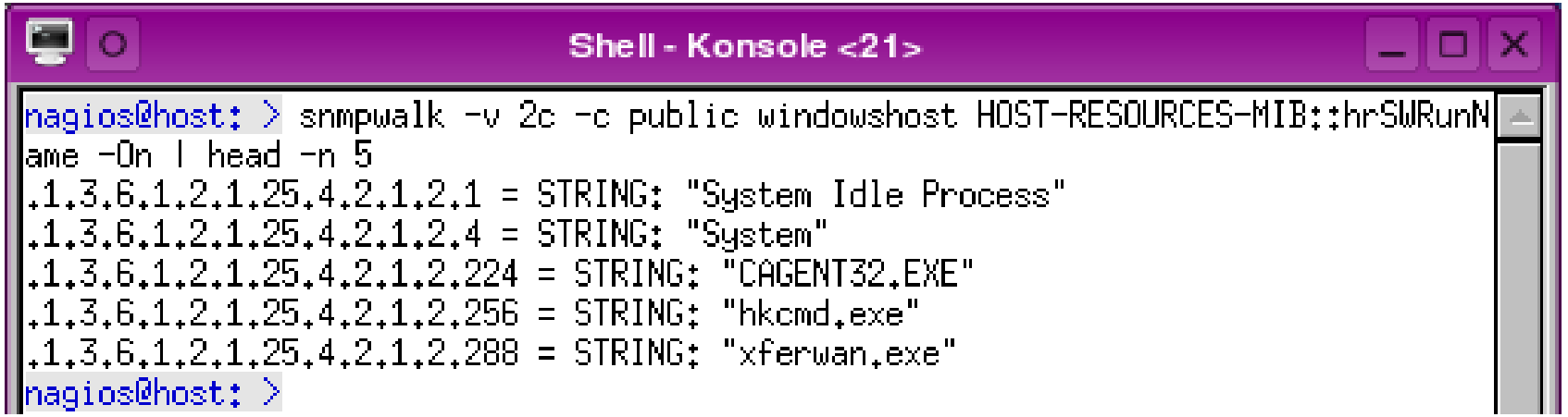
“public” und hrSWInstalledName

- Die Read-Only Community “public” ist auf sehr vielen Systemen per default konfiguriert
- Die installierte Software kann mit einem standardisierten MIB abgefragt werden



hrSWRunName

- Auch die laufenden Prozesse können mit dem Host-Resources-MIB abgefragt werden



Fragen zu SNMP?

Network Monitoring Systems

- Kommerzielle Network Management Systeme:
  - HP OpenView
  - IBM Tivoli
- Open Source Systeme:
  - Big Brother (strenggenommen *nicht* OSS)
  - Big Sister
  - OpenNMS
  - Nagios

Nagios Übersicht

- ist ein Network Monitoring System
- verfügt an sich nur über sehr wenige aber sehr durchdachte Features:
  - Scheduler
  - Konsolidierung von Ergebnissen (z. B. “host down” versus “host unreachable”)
  - Benachrichtigung bei und Eskalation von Problemen
  - Mechanismus um interne “commands” auszuführen
  - Mechanismen um externe “commands” zu starten

Nagios Plugins

- Funktionen werden zu einem großen Teil in Plugins realisiert
  - Service Checks
  - Host Checks
  - Notifications
  - Event Handlers
- Plugins sind ausführbare Programme

Advice for Beginners

- Relax - its going to take some time. [...]
- Read the documentation. [...] RTFM.
- Use the sample config files. [...]
- Seek the help of others.

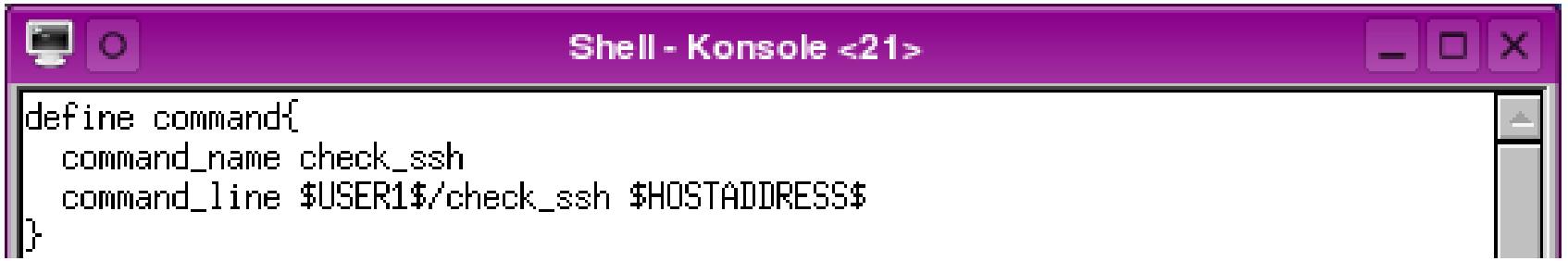
[http://nagios.sourceforge.net/docs/2_0/beginners.html]

Vereinfachter Ablauf

- Am Anfang war der Scheduler
  - startet aktive Service Checks
  - versucht dabei, Lasten zu verteilen

Aktive Service Checks

- werden durch Plugins realisiert
- sind als “commands” in das System integriert, z.B:

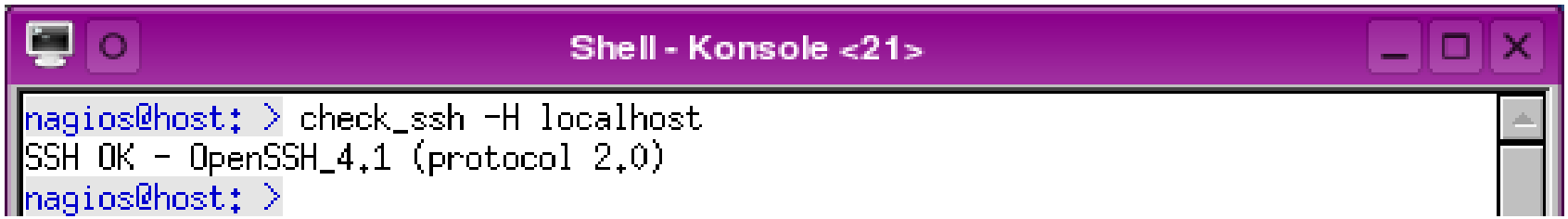


Check Plugins

- Standard-Plugins machen hauptsächlich “High-Level”-Checks, z. B. Dienste (http, smtp, pop3 etc.) bzw. lokale Checks
- `check_snmp` existiert, enthält aber kein “Wissen” über das geprüfte Objekt
- Mit NRPE und `check_by_ssh` existieren zwei weitere Möglichkeiten Zustände anderer Hosts zu prüfen

Check Plugins

- Nagios wertet Exit-Codes aus: 0 = OK, 1 = Warning, 2 = Critical, 3 = Unknown
- Plugins können eine Zeile für Menschen lesbare Information zurückgeben:



Performance Data

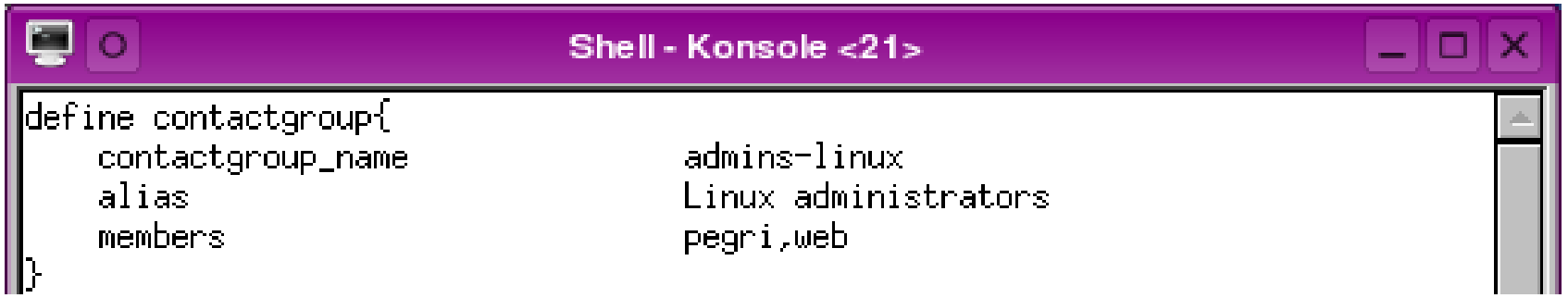
- Neuere Plugins können auch quantitative Informationen zur weiteren Verarbeitung zurückgeben
- Nagios selbst betrachtet alles nach einem Pipe-Zeichen (“|”) als “Performance Data”
- Vom Nagios Plugins Development Team werden weitergehende Anforderungen an das Format von Performance Data gestellt

Reapers

- Die “Reapers” überprüft regelmäßig die Ergebnisse von aktiven Checks
- Die Ergebnisse werden dann durch die “Core Service Monitoring Logic” verarbeitet
- Diese initiiert nach Bedarf Host Checks, Verständigungen etc.
- und scheduled die nächste Überprüfung eines Services

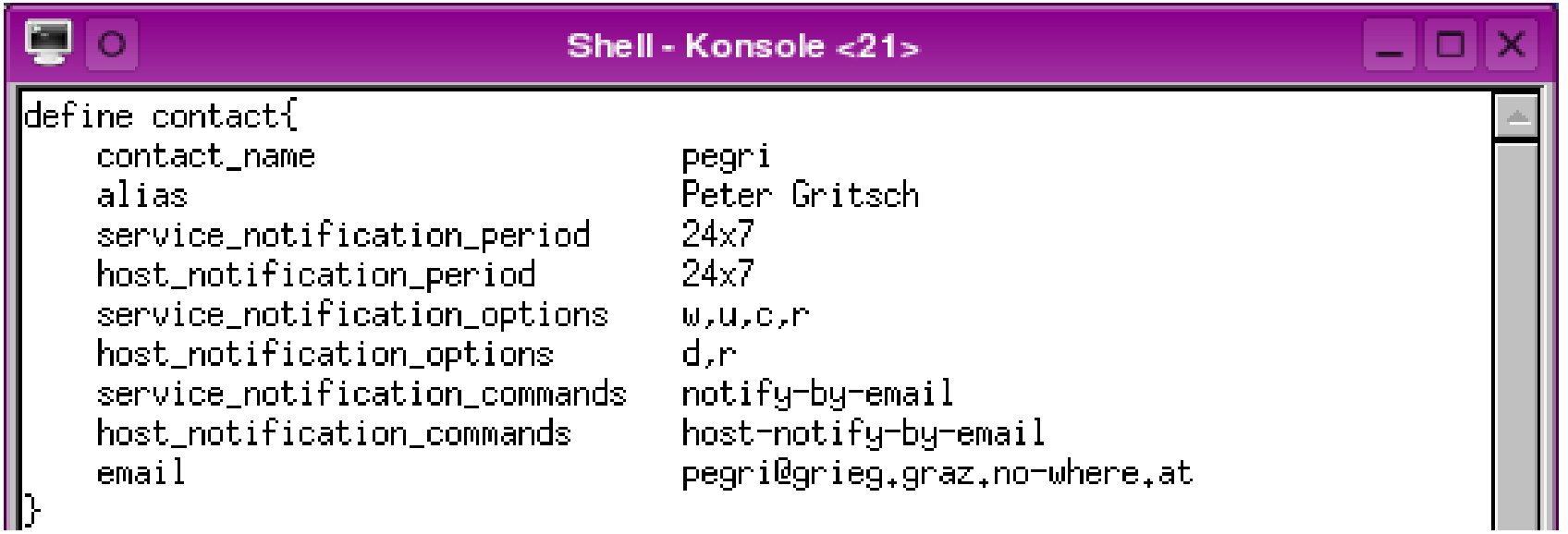
Contactgroups

- “Contactgroups” fassen Kontakte zusammen, die gemeinsam verständigt werden sollen
- Typische Kontakt-Gruppen sind z.B: “linux-server”, “networking”



Contacts

- Beschreiben wer, wann und wie verständigt werden soll



Webinterface

- siehe dort

Fragen zu Nagios?

SNMP4Nagios

- *SNMP4Nagios* ist eine Sammlung von Nagios Plugins
- Diese verwenden SNMP um Services zu überprüfen
- Derzeit gibt es rund 50 Plugins (45 bzw. 57)
- Unterstützt werden Standard-MIBs und Hersteller-spezifische MIBs von Brocade, Cisco, Compaq/HP, Network Appliance sowie SNMP-Informant und Net-SNMP

Konstruktive Faulheit

- (Fast) alle mehrfach verwendeten Funktionen, sind in den “Helpers” codiert.
- Die Plugin-Sourcen umfassen praktisch nur die spezifischen Code-Teile
- Dadurch auch konsistente Kommandozeilen-Parameter
- und relativ wenig Aufwand für die Erstellung neuer Plugins

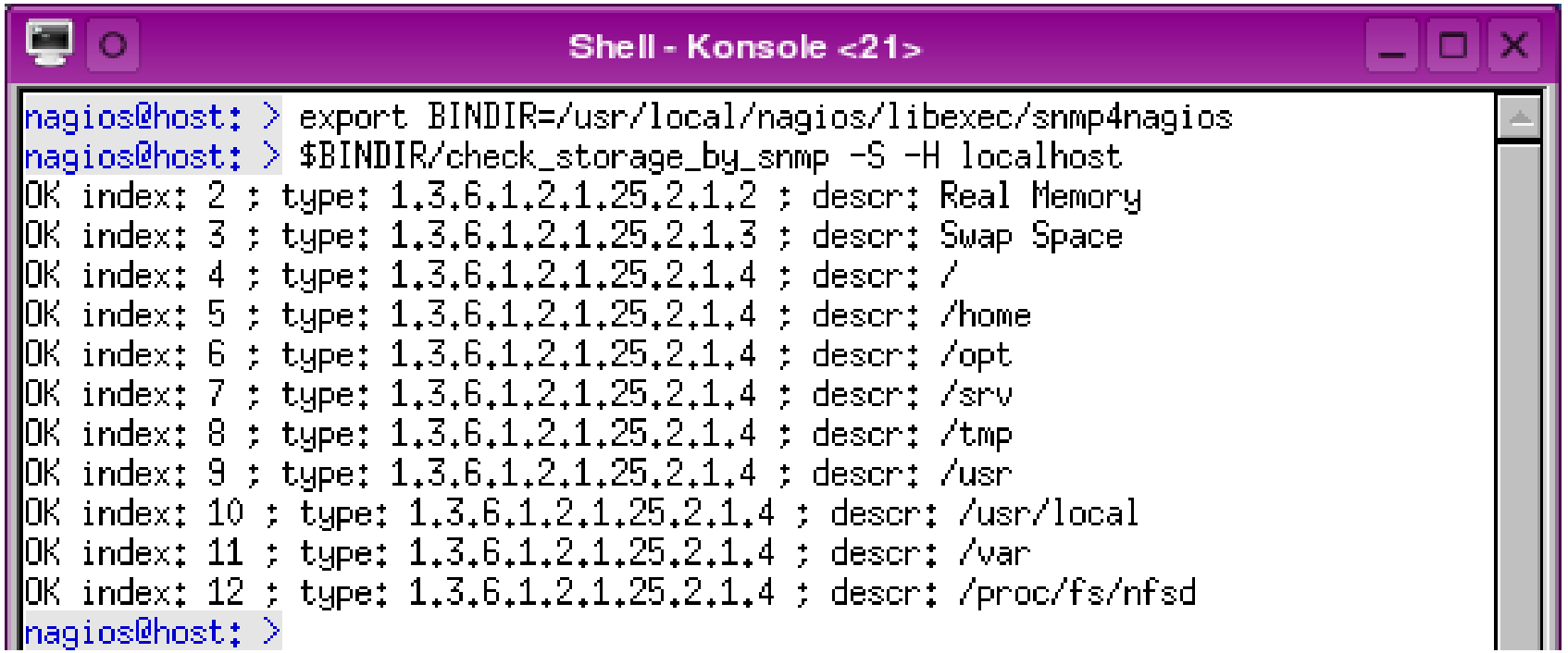
Features

- Alle Plugins unterstützen “Scanning”
- Alle Plugins, die Performance Daten unterstützen, können diese selbst loggen und plotten.
- Fehler werden ins Syslog geschrieben

Scanning

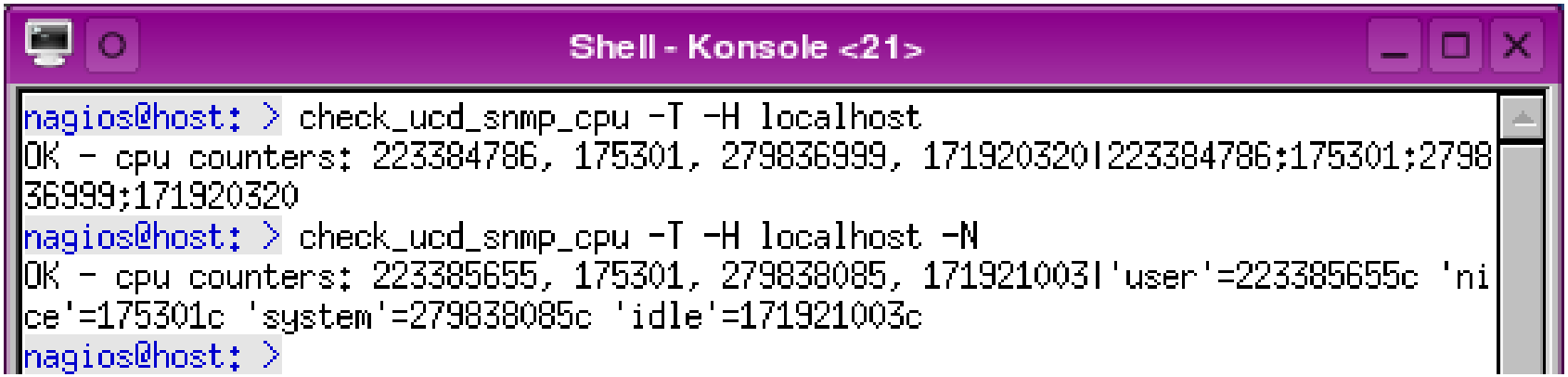
- Erkennt welche Resourcen überwacht werden können
- Liefert für die Konfiguration relevante Informationen
- Sollte in lokale Skripte zur Konfiguration von Hosts eingebunden werden

Scanning


Shell - Konsole <21>
nagios@host: > export BINDIR=/usr/local/nagios/libexec/snmp4nagios
nagios@host: > $BINDIR/check_storage_by_snmp -S -H localhost
OK index: 2 ; type: 1.3.6.1.2.1.25.2.1.2 ; descr: Real Memory
OK index: 3 ; type: 1.3.6.1.2.1.25.2.1.3 ; descr: Swap Space
OK index: 4 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /
OK index: 5 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /home
OK index: 6 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /opt
OK index: 7 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /srv
OK index: 8 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /tmp
OK index: 9 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /usr
OK index: 10 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /usr/local
OK index: 11 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /var
OK index: 12 ; type: 1.3.6.1.2.1.25.2.1.4 ; descr: /proc/fs/nfsd
nagios@host: >

Performance Data

- *SNMP4Nagios* unterstützt ein “natives” und das vom Nagios Plugins Developement Team propagierte Format für Performance Data

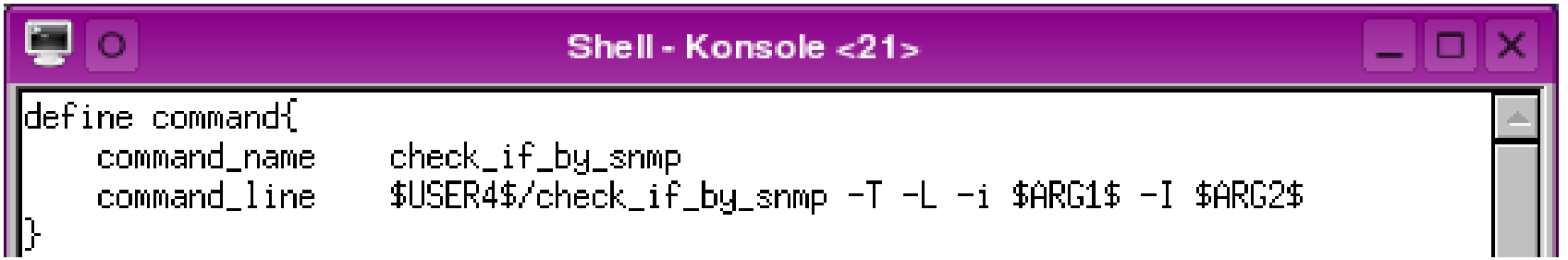


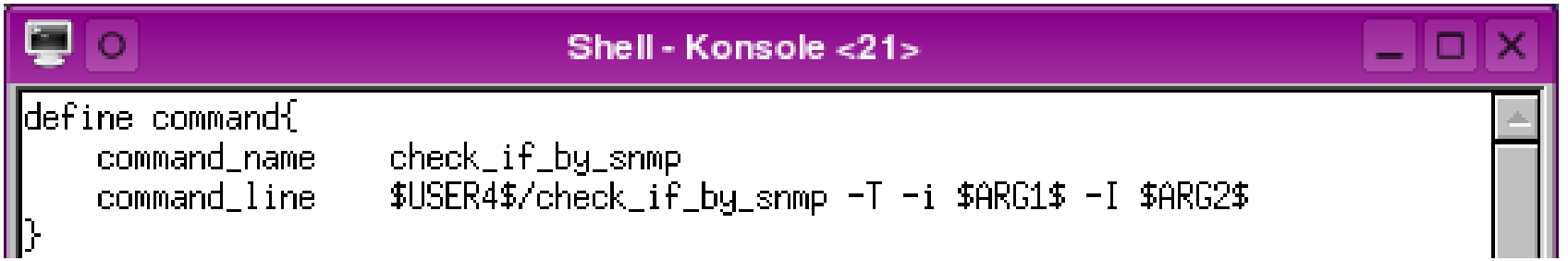
Logging

- Die Plugins können die Performance Daten selbst (bzw. durch die librrd) archivieren.
- Vorteile
  - Einfachheit
  - Geschwindigkeit
  - “Wissen” um die Zusammenhänge einzelner Werte
  - kaum Konfigurationsaufwand
- Nachteile
  - kaum Konfigurationsmöglichkeiten

Logging

- Logging :: Kein Logging

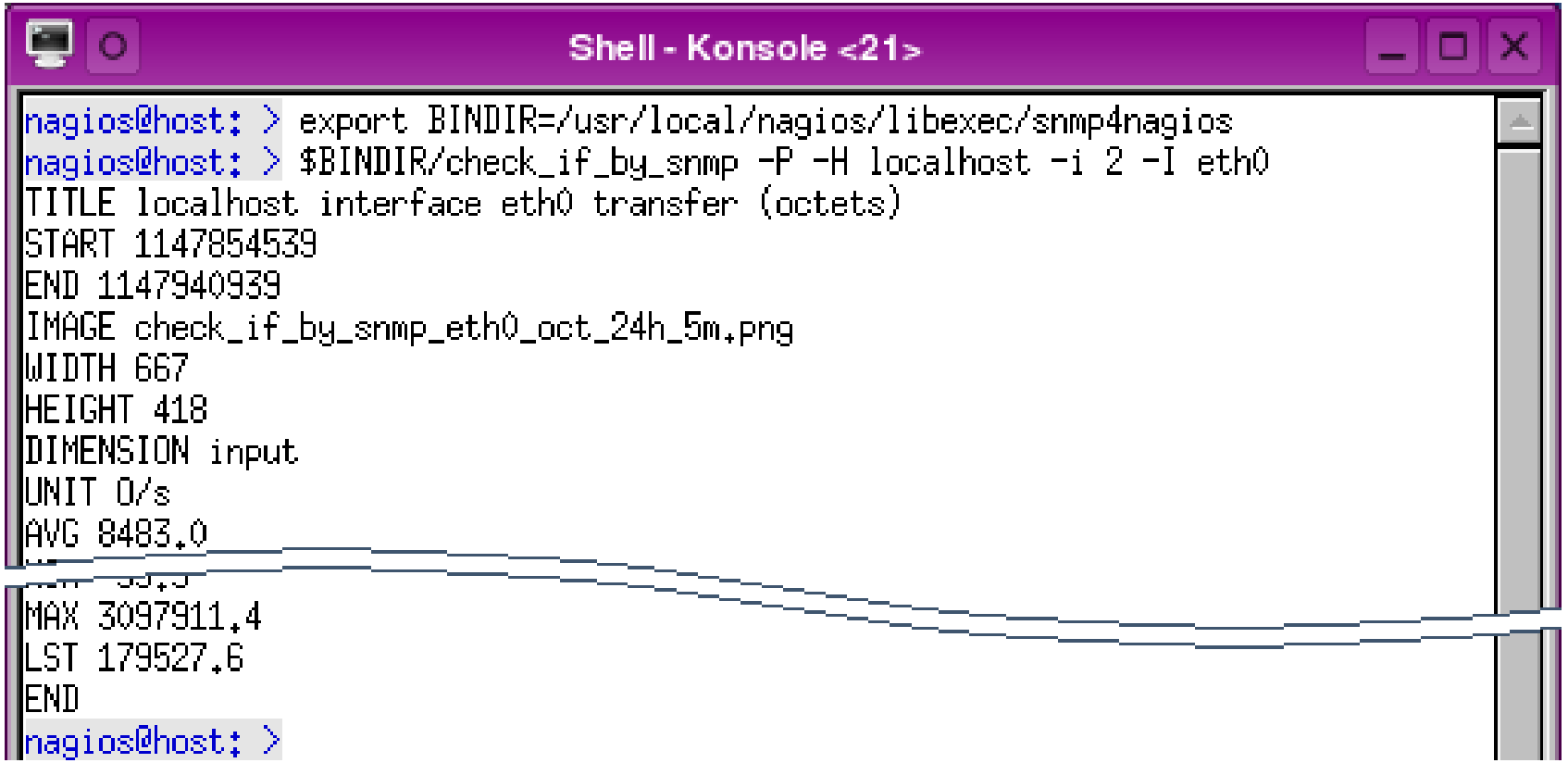




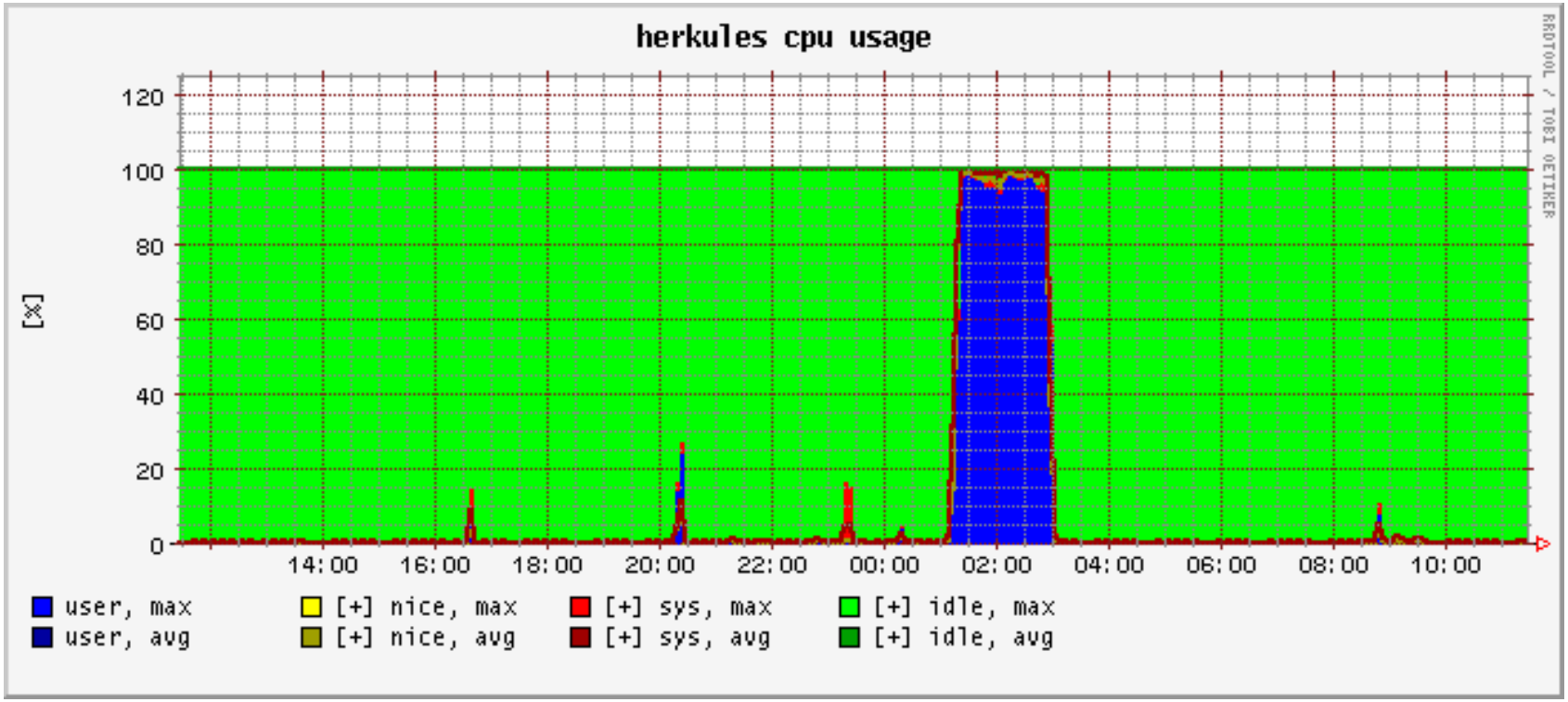
Plotting

- Archivierte Daten können geplottet werden
- Plugins sollten wiederum in lokale Skripte eingebunden werden
- Dafür werden Informationen über die Plots ausgegeben, z.B. Titel, Dateiname und Abmessungen

Plotting


Shell - Konsole <21>
nagios@host: > export BINDIR=/usr/local/nagios/libexec/snmp4nagios
nagios@host: > $BINDIR/check_if_by_snmp -P -H localhost -i 2 -I eth0
TITLE localhost interface eth0 transfer (octets)
START 1147854539
END 1147940939
IMAGE check_if_by_snmp_eth0_oct_24h_5m.png
WIDTH 667
HEIGHT 418
DIMENSION input
UNIT O/s
AVG 8483.0
MAX 3097911.4
LST 179527.6
END
nagios@host: >

Plotting


herkules cpu usage
[%]
120
100
80
60
40
20
0
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
user, max
user, avg
[+] nice, max
[+] nice, avg
[+] sys, max
[+] sys, avg
[+] idle, max
[+] idle, avg
RRDTOOL / TOBI OETIKER

Fragen zu *SNMP4Nagios*?

Vielen Dank für eure Aufmerksamkeit!