Monitoring

Lästiges Übel oder sinnvolle Prophylaxe?

Christoph Stöttner
christoph.stoettner@edcom.de

Edcom Software & Consulting GmbH – Leopoldstraße 29 – 80802 München
+49 89 3840850 – info@edcom.de – www.edcom.de

Inhaltsverzeichnis

Monitoring ist effektiver Stressabbau

Was möchte man als Admin vermeiden?

- Ausfälle und nicht verfügbare Dienste zur Hauptgeschäftszeit
- Mitarbeiter melden Ausfall dem Support, bevor man selbst den Ausfall bemerkt
- Blackberry-Dienst läuft nicht und das Management meldet sich bei der IT Leitung
- Verschenkte Zeit bei der Ersatzteilbeschaffung

Unterscheidung der Admins

- Install and Forget
- Log-Analyse im Fehlerfall
- mehr oder weniger regelmäßiges Monitoring
  - je nach Arbeitsbelastung
  - einige automatisierte Meldungen mit verschiedenen Tools (HP Server Tools, Domino Events)
- Monitoring ist langweilig, wie kann man es automatisieren

Probleme lösen, bevor die

Anwender sie bemerken!

Warum?

- Arbeitsbelastung der Admins steigt
- Keine Zeit für regelmäßige Log-Analysen, Monitoring
- Wichtige Informationen verstreut im Netzwerk
  - Windows Events
  - Linux Syslog
  - Domino Log
- Ausfälle immer zur ungünstigsten Zeit
- Lieber in Ruhe reagieren, ohne Telefon-„Terror“ und Zeitdruck
- Ausfällen zuvorkommen

Beispiele - DB Backup falsch konfiguriert

- Backupskript der Datenbanksicherung läuft Amok
  - MSDE auf c:
  - Backup und Log auf c:
- 10:15 Uhr Warning Message Disk 80% Full
- 10:20 Uhr Critical Message Disk 95% Full
- Plattenplatz konnte freigegeben werden, bevor der Server stehen blieb

Beispiele - DB Backup falsch konfiguriert

- Backupskript der Datenbanksicherung läuft Amok
  - MSDE auf c:
  - Backup und Log auf c:
- 10:15 Uhr Warning Message Disk 80% Full
- 10:20 Uhr Critical Message Disk 95% Full
- Plattenplatz konnte freigegeben werden, bevor der Server stehen blieb

Ausfall zuvorgekommen

Keine aufwändige Fehlerbehebung notwendig!

Beispiele - iSeries Netzteil

iSeries (AS/400) Netzteil defekt

- Ausfall einer Netzwerkkarte

IST

- 17:00 Uhr Ausfall des Netzteils
- 8:00 Uhr Anruf eines Anwenders beim Support
- 8:15 - 8:30 Uhr Ersatzteilbestellung
- Ersatz nicht vor 12 Uhr im Haus

Soll

- 17:00 Uhr Ausfall des Netzteils
- 17:15 Uhr Mailalarmierung des Admins
- 17:30 Uhr Fehler gefunden → Ersatzteilbestellung läuft
- 7:35 Uhr Netzteil geliefert → Einbau → Anwendung läuft

Welche Informationen sind interessant?

- Gesamtüberblick über das Netzwerk
- Sammlung im Netz verteilter Daten
  - Windows Events
  - Linux Syslog
  - Auslastung von CPU, Memory und Storage
- Trends
  - CPU
  - Memory
  - Storage

Nutzen für die Abteilung / Firma

- Beleg für Service Level Agreements (SLA)
- Grundlage für Ersatzbeschaffungen
- Warnung bei Überschreitung von Grenzwerten
- Verlässlichkeit

Nutzen für den Admin

- ”Manuelles” Monitoring ist langweilig
- Automatisierung von Routineaufgaben
- Zeitgewinn für produktive Aufgaben
- Ruhiger Schlaf

Nagios

- Entwicklung gestartet von Ethan Galstad als NetSaint
- Betrieb unter Linux und UNIX möglich
- Open Source Software unter GPL
- Überwachungssystem für Devices und Dienste
- Überwachung verschiedenster IT Komponenten

Nagios

- Aktive Checks
- Verarbeitung passiver Events
- Webinterface für Präsentation und Reporting
- Flexibles Benachrichtigungssystem
- Erkennen von Trends
- Modular erweiterbar

Voraussetzungen

- Physikalischer Server oder virtuelle Maschine
  - Standard PC
  - evtl. GB-LAN
- Linux oder UNIX
  - Debian
  - Ubuntu
  - Red Hat
  - SuSE
- Compiler bzw. fertige Pakete
- Webserver Apache
- GD Library

Nagios Dämon

- zentrales Framework
- Konfiguration
- Zeitplanung (Scheduler)
- Weboberfläche
- Benachrichtigungen
- Logs

Nagios Plugins

- Überwachungsaufgaben
- Skripte, Agents
- Statusmeldungen:
  - OK
  - WARNING
  - CRITICAL
- Zusatzinfos, Performancedaten

Status Events

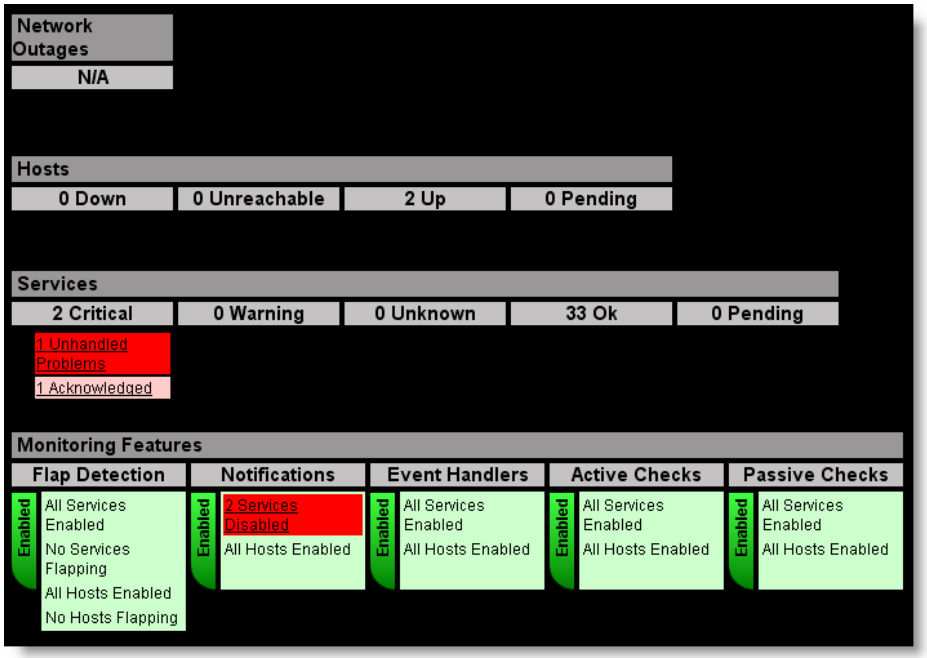
- Config:
  ```
  normal_check_interval 5
  retry_check_interval 2
  max_check_attempts 4
  ```
- Prüfung des Dienstes alle 5 Minuten
- bei Ergebniswechsel → Prüfung alle 2 Minuten
- Fehlerzustand nach 4 Tests, die zum gleichen Ergebnis führen → Eventhandler wird ausgeführt → Prüfinterval wieder 5 Minuten
- Reagieren auf Ereignisse
  - Bei OK → nicht OK
  - Bei nicht OK → OK
- Soft State
- Hard State
- Ausführen von Notifications, externen Skripten oder SNMP Traps

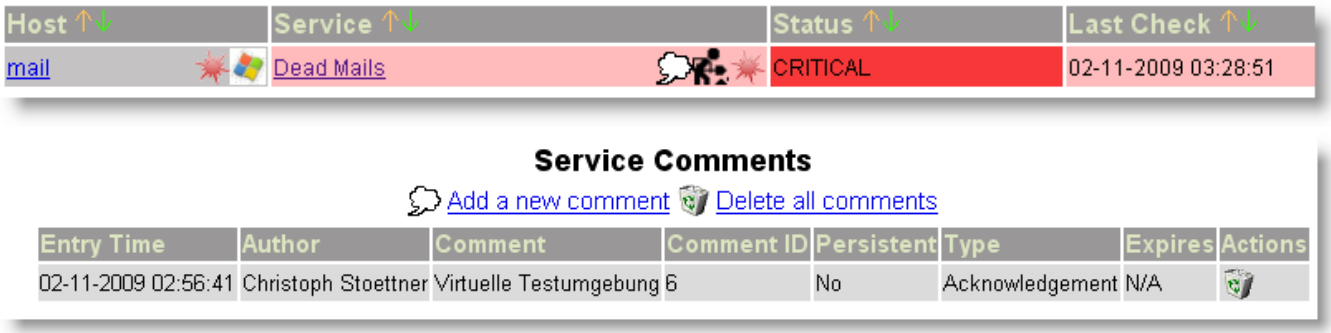
Alarmierungen

- E-Mail
- Jabber / Google Talk
- SMS
  - Mail2SMS
  - GSM Modem
- Twitter (bitte als Privat markieren)
- Prowl (für iPhone) `http://prowl.weks.net/`
- Sametime (in Arbeit)
- Eskalation
  - Meldung an zusätzliche Kontaktgruppen
  - alternative Kontaktmethoden

Webinterface

- Browser- und Clientunabhängig
- Schneller Überblick
- Dokumentation über Kommentare
  - Downtime
  - Arbeitsschritte
- Anzeige von Ausfällen
- über Themes anpaßbar





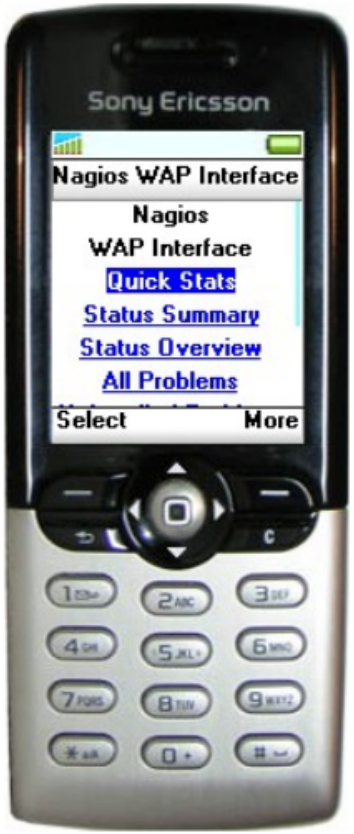
Host	Service	Status	Last Check
mail	Dead Mails	CRITICAL	02-11-2009 03:28:51

Service Comments

Add a new comment | Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
02-11-2009 02:56:41	Christoph Stoettner	Virtuelle Testumgebung	6	No	Acknowledgement	N/A	

WAP Interface



Was kann mit Nagios überwacht werden

- Oracle Databases
- MS SQL Server
- MySQL
- SAP
- DNS
- NTP

Was kann mit Nagios überwacht werden

- Switches und Router (managebar)
  - Auswertung
  - Steuerung über SNMP
- Drucker
- USV Anlagen
- syslog
- Umgebungssensoren (Temperatur, Luftfeuchte)

Was kann mit Nagios überwacht werden

- Switches und Router (managebar)
  - Auswertung
  - Steuerung über SNMP
- Drucker
- USV Anlagen
- syslog
- Umgebungssensoren (Temperatur, Luftfeuchte)

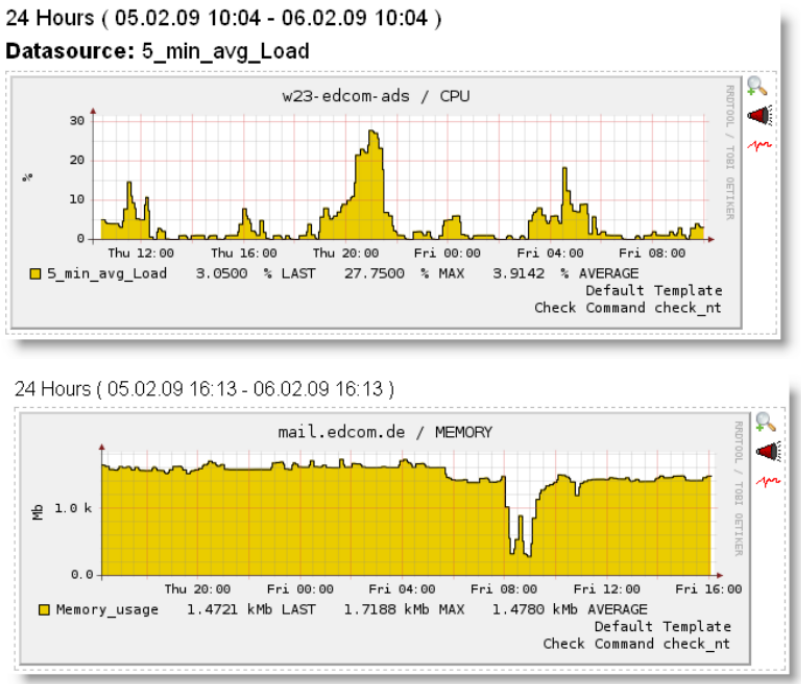
Alles was ein Skript ausführen kann!

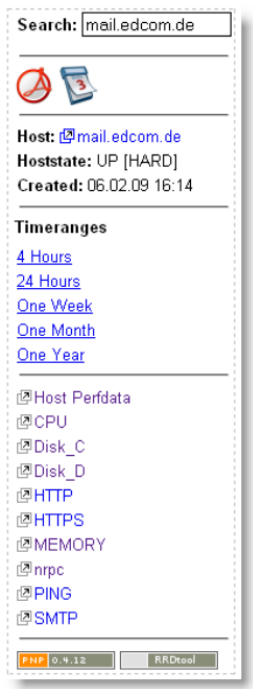
Erweiterungen

- pnp4nagios
  - http://www.pnp4nagios.org/
  - Performancedaten darstellen und speichern (rrd)
- NagVis
  - http://www.nagvis.org/
  - Visualisierung von Checkergebnissen
  - Visualisierung auf
    - Netzwerkplänen
    - Landkarten
    - Fotos
- Grafische Konfigurationstools
  - NagiosQL
  - Nagconf
  - Fruity
- OTRS (Open Trouble Ticket System) Integration
  - http://www.otrs.org
  - Öffnen und schliessen von Tickets durch Nagios
- Typo3 Integration (Portal)

pnp4nagios

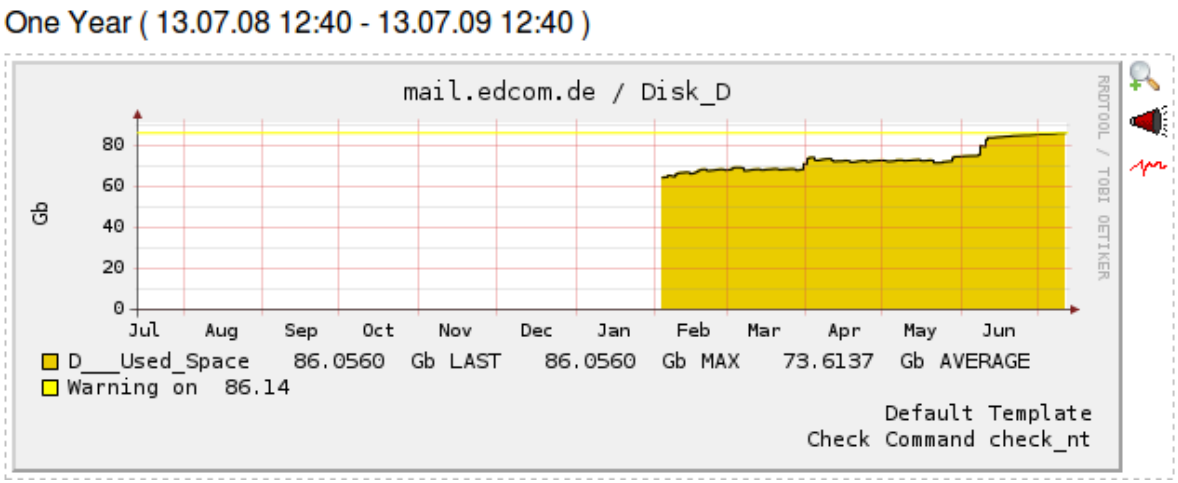
- Zusätzliche Komponente zur Darstellung von Performance-Daten
- Export in PDF und XML möglich
- nagios.cfg: `process_performance_data=1`



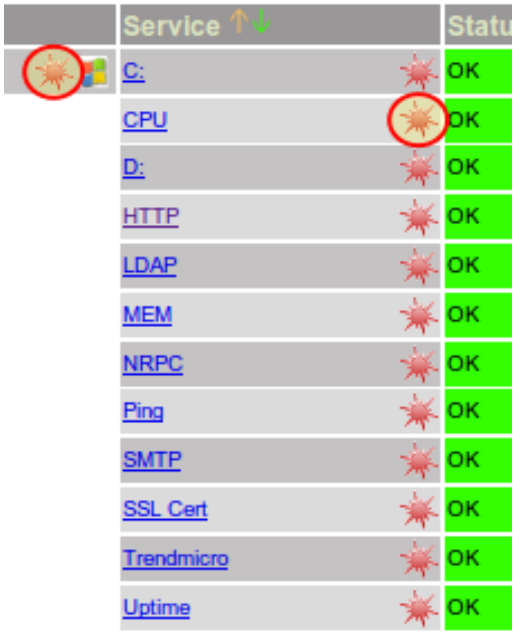


pnp4nagios

- Zusätzliche Komponente zur Darstellung von Performance-Daten
- Export in PDF und XML möglich
- nagios.cfg: `process_performance_data=1`



Einbinden von pnp4nagios



Link für Host

- Eintrag in hosttemplate:

```
action_url \
/nagios/pnp/index.php?host=$HOSTNAME$
```

Link für Services

- Eintrag in servicetemplate:

```
action_url \
nagios/pnp/index.php?host=$HOSTNAME$&srv=$SERVICEDESC$
```

Einträge in das Hosttemplate erfolgen in einer Zeile ohne den ”\”!

NagVis

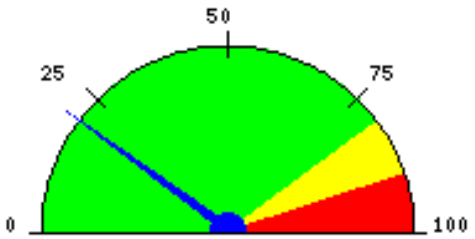
Visualisierung von Prüfergebnissen auf Grafiken, Karten oder Fotos

- Voraussetzung:
  - ndo2db (aktuelle Beta)
  - MySQL
- Variable Gruppierung
  - logisch (z.B. alle Applikationsserver)
  - physikalisch (z.B. alle Hosts in einem Rack)
  - geographisch (z.B. alle Hosts in einer Region)
  - Geschäftsprozesse (für Abhängigkeiten)
  - seit Version 1.4: Gadgets (Tachos)

NagVis

Visualisierung von Prüfergebnissen auf Grafiken, Karten oder Fotos

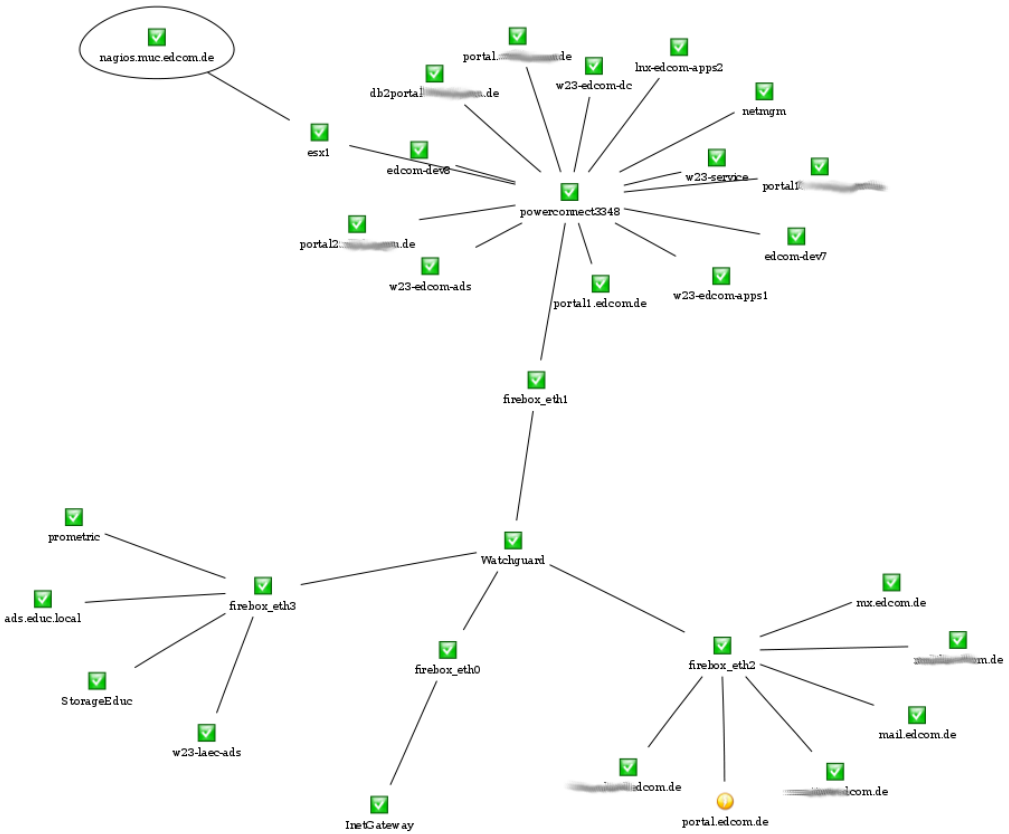
- Voraussetzung:
  - ndo2db (aktuelle Beta)
  - MySQL
- Variable Gruppierung
  - logisch (z.B. alle Applikationsserver)
  - physikalisch (z.B. alle Hosts in einem Rack)
  - geographisch (z.B. alle Hosts in einer Region)
  - Geschäftsprozesse (für Abhängigkeiten)
  - seit Version 1.4: Gadgets (Tachos)



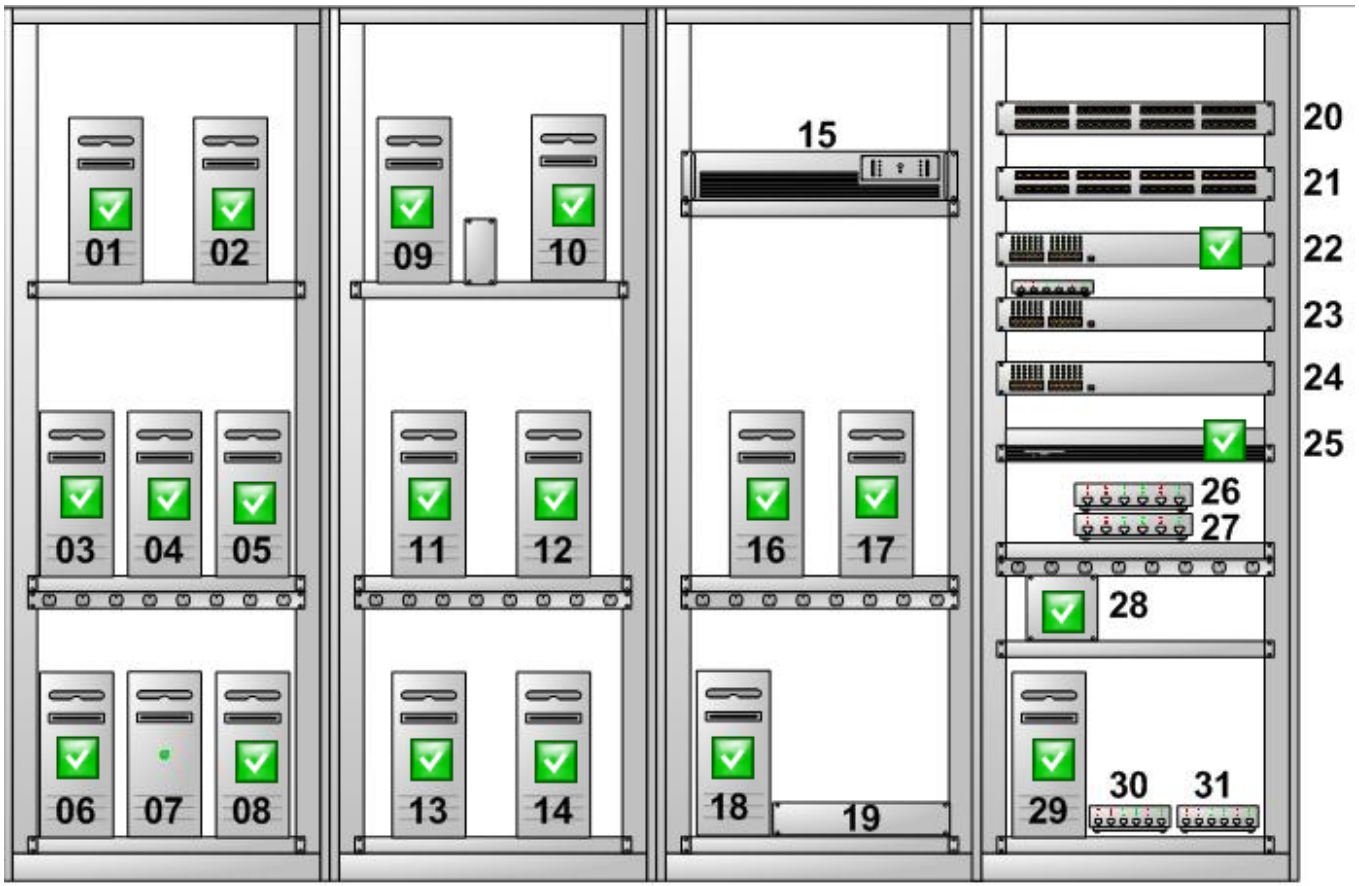
Beispiele für Nagvis

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

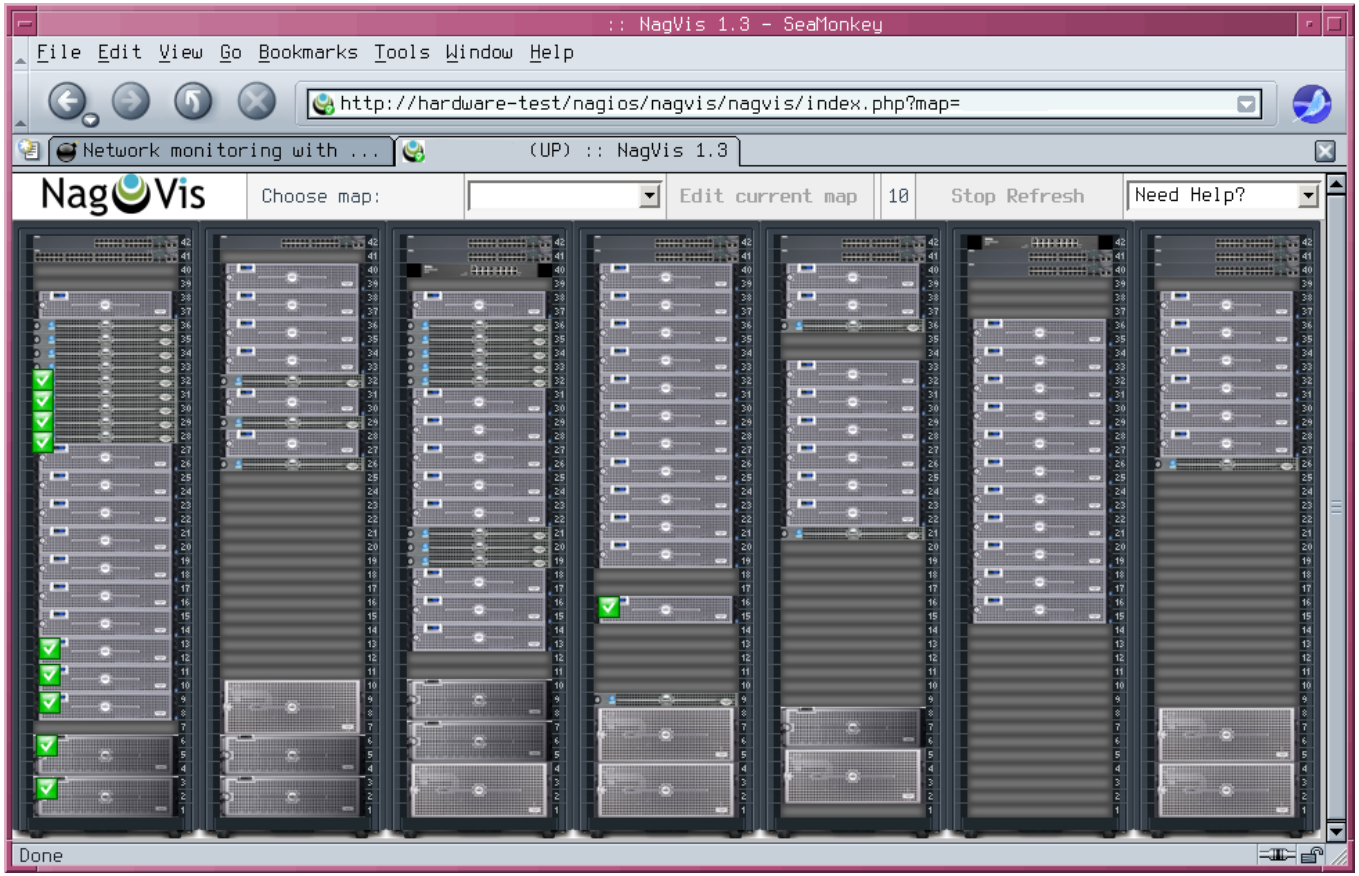
Beispiele für Nagvis



Beispiele für Nagvis



Beispiele für Nagvis



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

Beispiele für Nagvis

Quelle: `http://www.nagvis.org`
(c) by Dave Rearden

Domino Monitoring

Verschiedene Check-Plugins für das Domino Monitoring

- einfacher Pingtest
- Betriebssystemwerte
- Antwortzeiten von Netzwerkports
- spezielle Checks für Protokolle
- Überprüfen laufender Prozesse oder Services
- Abfrage von Statistikwerten per SNMP
- Verarbeitung von SNMP Traps

Betriebssystemwerte

- CPU Auslastung

CPU Load	OK	2009-03-23 15:47:23	2d 22h 5m 54s	1/3	CPU Load 2% (5 min average)

- Festplattenbelegung

C:\ Drive Space	OK	2009-03-23 15:46:54	2d 22h 6m 25s	1/3	c: - total: 11.99 Gb - used: 8.76 Gb (73%) - free 3.23 Gb (27%)

- Speicherbedarf

Memory Usage	OK	2009-03-23 15:44:15	2d 22h 7m 38s	1/3	Memory usage: total:2450.63 Mb - used: 1790.33 Mb (73%) - free: 660.30 Mb (27%)

- Uptime

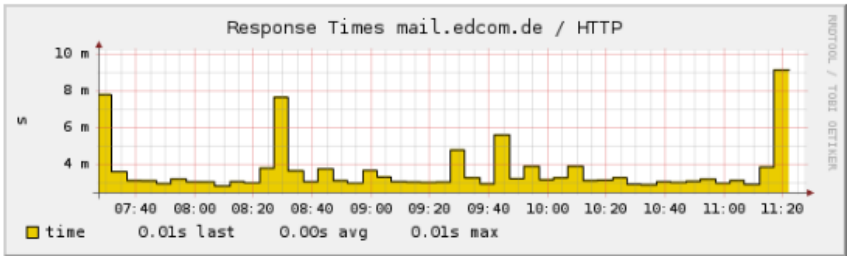
Uptime	OK	2009-03-23 15:50:02	2d 22h 10m 16s	1/3	System Uptime - 4 day(s) 0 hour(s) 7 minute(s)

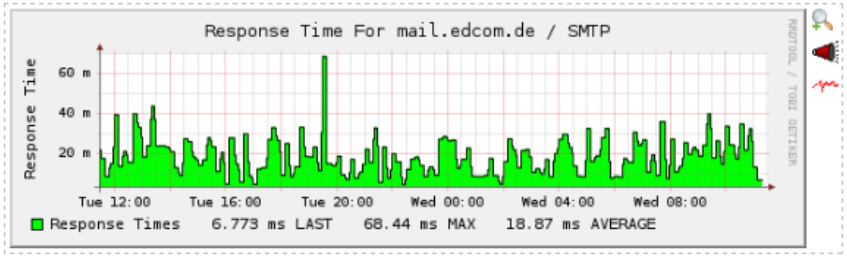
Antwortzeiten der Netzwerkports

`check_tcp -H host -p port`

- NRPC – 1352
- SMTP – 25, SMTPS – 465
- LDAP – 389, LDAPS – 636
- HTTP – 80, HTTPS – 443
- IMAP – 143, IMAPS – 993
- POP3 – 110, POP3S – 995

Service	Status
C:	OK
CPU	OK
D:	OK
HTTP	OK
LDAP	OK
MEM	OK
NRPC	OK
Ping	OK
SMTP	OK
SSL Cert	OK
Trendmicro	OK
Uptime	OK





Spezielle Protokoll Checks

- es wird nicht nur geprüft, daß der Port antwortet
- check_smtp:
  - `check_smtp -H host -p port -e expect -C command -f from addr -A authtype -U authuser -P authpass -w warn -c crit -t timeout -S -D days -v`
  - Anmeldung wird geprüft
  - vorgegebene Antwort kann geprüft werden
  - Gültigkeit des SSL Zertifikats
- check_ldap:
  - `check_ldap -H <host> -b <base_dn> -p <port> -a <attr> -D <binddn> -P <password> -w <warn_time> -c <crit_time> -t timeout`
  - Anonymous Bind
  - Benutzer Bind

Spezielle Protokoll Checks – HTTP

- `check_http -H <vhost> | -I <IP-address> -u <uri> -p <port> -w <warn time> -c <critical time> -t <timeout> -L -a auth -e <expect> -s string -l -r <regex> | -R <case-insensitive regex> -P string -m <min_pg_size>:<max_pg_size> -4|-6 -N -M <age> -A string -k string -S -C <age> -T <content-type> -j method`
- Überprüfung Antwortzeit
- Anmeldung möglich (-A)
- Https Abfragen möglich
- Warnung beim Unterschreiten der SSL-Key Gültigkeit nach Tagen
- Suche nach Strings oder Regular Expressions auf der Webseite
- Überprüfen der Größe der aufgerufenen Seite

Laufende Dienste unter Windows

- nsclient(++) muß am Server installiert sein
- Überprüfung, ob ein Dienst läuft
- `check_nt -v SERVICESTATE -l <Dienstname>`
- ”Lotus Domino Server (dDomData)”
- `<Dienstname>` kann auch eine kommagetrennte Liste sein

Domino Service	OK	09-23-2009 12:56:12	0d 0h 1m 42s	1/3	OK: All services are in their apropriate state.

Laufende Prozesse unter Windows

- nsclient(++) muß am Server installiert sein
- überprüft laufende Binaries
- `check_nt -v PROCSTATE -d SHOWALL -l <Dateiname>`
- namgr.exe
- nrouter.exe
- nsmtp.exe

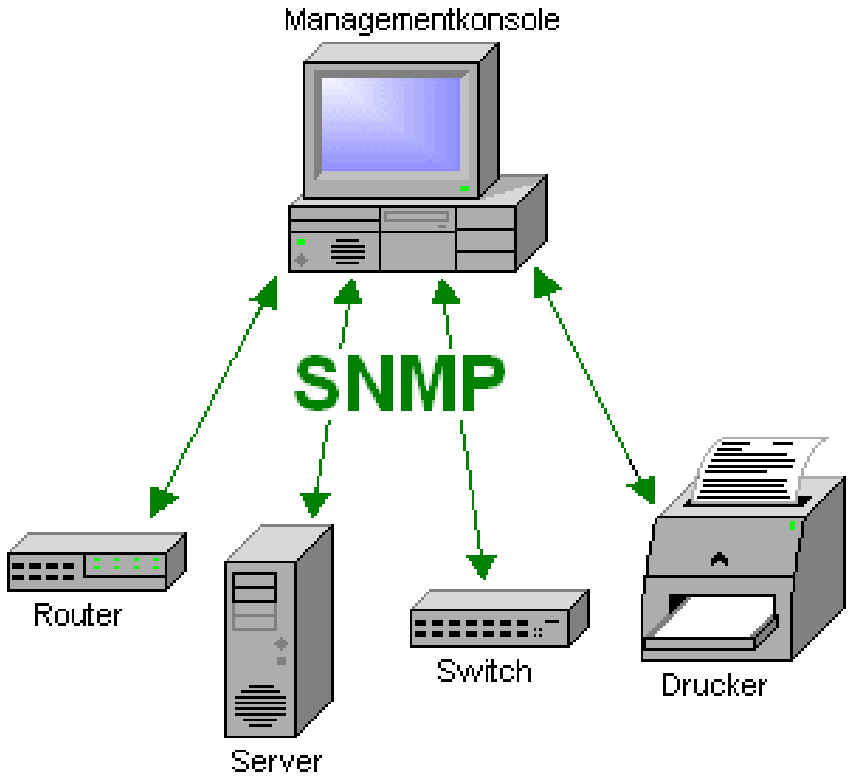
Amgr	OK	09-23-2009 13:19:43	0d 0h 0m 38s	1/3	namgr.EXE: Running
Router	OK	09-23-2009 13:19:50	0d 0h 0m 31s	1/3	nrouter.EXE: Running

Laufende Prozesse unter Linux

- Umweg über `check_by_ssh`
- Lokale Abfrage von `check_multi`
  - nur ein Connect zum Server notwendig
  - Ein Serverprozess muss laufen:
    `check_procs -c 1:1 -C server`
  - Zwei Updateprozesse sollen laufen:
    `check_procs -w 2:2 -C update`

SNMP

- **S**imple **N**etwork **M**anagement **P**rotocol
- Protokoll um Netzwerkelemente zu überwachen und steuern
- Fernsteuerung, Fernkonfiguration und und Fehlererkennung



SNMP Installation

Windows

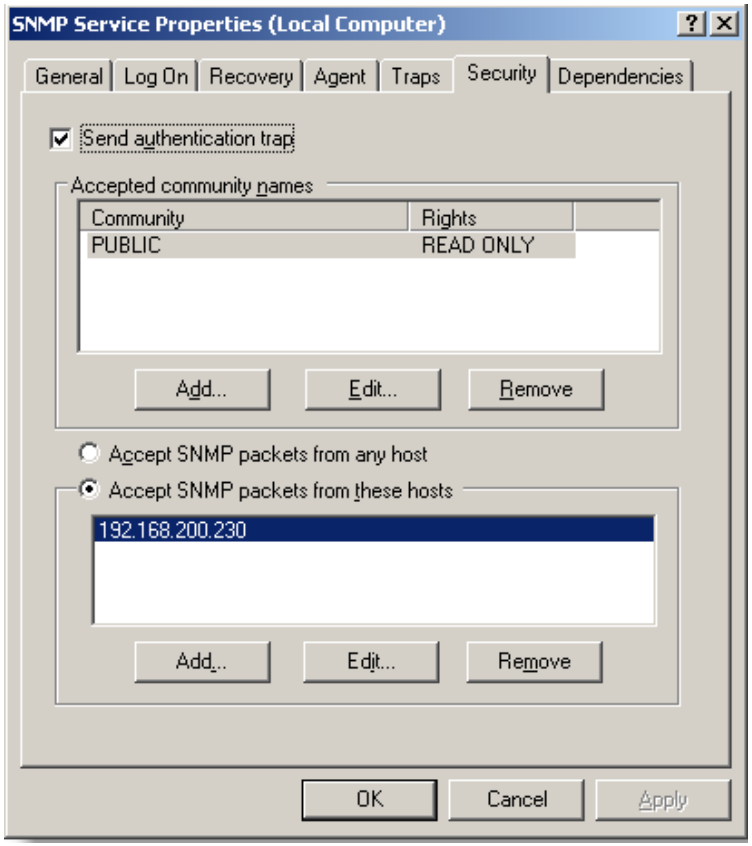
- zusätzlicher Dienst
- Konfiguration unter Diensteigenschaften
- Sicherheitseinstellung beachten!

Linux

- net-snmp
- Config für SMUX!

Domino

- Insnmp -Sc
- Tasks:
  - queryset
  - intrcpt
  - collect

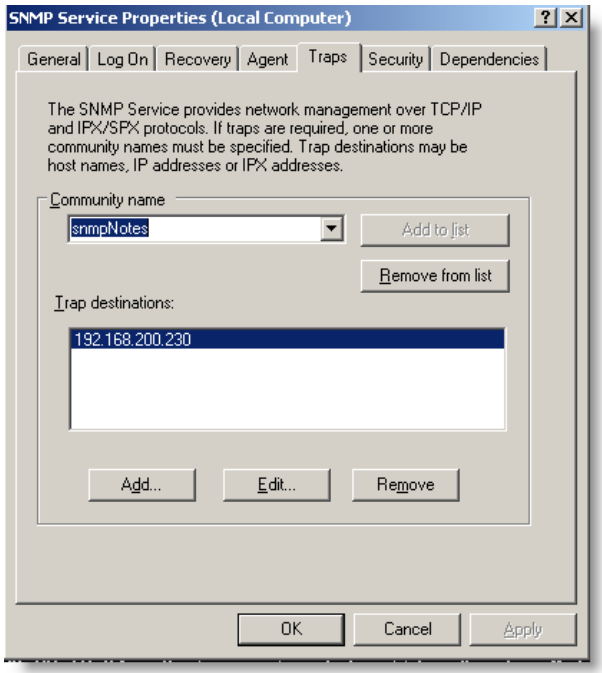


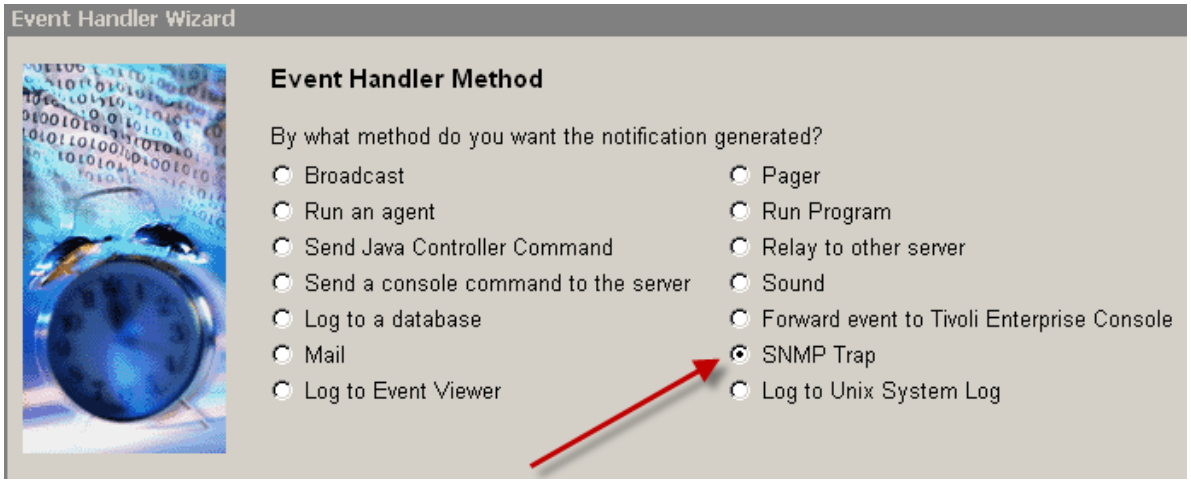
Interessante Statistikwerte

- Mail.Dead
- MAIL.Waiting
- Server.AvailabilityIndex
- Server.ExpansionFactor
- check_domino_eknori.pl:
  - `http://www.eknori.de` - Danke Ulrich!
  - check_domino_eknori.pl -H host -o Mail.Dead -c 9 -w 6
  - check_domino_eknori.pl -H host -o Synchronized DAOS.Engine.Catalog -c ”Needs Resync” -w Resyncing
- check für File Anzahl des DAOS Verzeichnisses s. `http://www.eknori.de`

SNMP Traps in Domino

- DDM generiert SNMP Trap Events und versendet diese an Nagios
  - Trap Empfänger in Windows definiert
  - Event Handler ”SNMP Trap” definieren
- Nagios empfängt Trap über SNMPTT





SNMP Trap in Nagios

- `http://www.snmptt.org/`
- etwas umständlich zu konfigurieren
- mit `snmpttconvermib` die Hersteller MIB umwandeln
- oder manuell in `/etc/snmp/snmptt.conf` pflegen
- passiver Eintrag, daher muß manuell der Status auf OK gesetz werden
- z.B. mit dem check_dummy Plugin

trap	WARNING	2009-03-23 11:56:09	15d 21h 33m 47s	1/1	Access to server mail.stoeps.local/stoeps is slow. [FADN-7PNSEP] on CN=mail.stoeps.local/O=stoeps
carefresh	CRITICAL	2009-03-23 15:42:58	5d 6h 33m 46s	1/1	CA Refresh on CA Process: 'tell ca refresh' finished. Use 'tell ca status' to check result.

Sametime

- Prüfen der Domino Tasks
  - nStAddin.exe
  - nStMeetingServer.exe
- Prüfen der Sametime Dienste
  - ”Sametime Server”
- Prüfen der Ports 1533, 8081

STAddIn	OK	09-23-2009 22:34:49	0d 0h 0m 35s	1/3	nstaddin.EXE: Running
STMeetingServer	OK	09-23-2009 22:34:56	0d 0h 0m 28s	1/3	nstmeetingserver.exe: Running
Sametime Port	OK	09-23-2009 22:35:05	0d 0h 0m 19s	1/3	TCP OK - 0.021 second response time on port 1533
Sametime Service	OK	09-23-2009 22:35:15	0d 0h 0m 9s	1/3	OK: All services are in their apropriate state.

Blackberry Server

- Prüfen der Domino Tasks
  - nBES.exe
- Prüfen der Blackberry Dienste
  - ”Blackberry Dispatcher”
  - ”Blackberry Router”
- Prüfen des MS SQL Server
- `check_blackberry` für SNMP Statistikwerte
  - Srpconnect
  - Lizenzen
  - Pending Messages
  - Version

BB Lizenzen	OK	09-23-2009 23:09:37	0d 0h 4m 43s	1/3	OK: Licenses used: 8
BB Pending MSG	OK	09-23-2009 23:09:12	0d 0h 5m 7s	1/3	OK: Pending Mails: 0
BB SRPConnect	OK	09-23-2009 23:10:19	2d 13h 34m 6s	1/3	OK: Successful connected to SRP-Router. Last Connection: 2009-09-20 23:44:46
BB Version	OK	09-23-2009 23:10:49	2d 14h 33m 30s	1/3	BlackBerry Enterprise Server Version: 5.0.0.133
BES Task	OK	09-23-2009 23:14:11	0d 0h 0m 8s	1/3	nbes.EXE: Running
Blackberry Dispatcher	OK	09-23-2009 23:09:54	0d 0h 4m 25s	1/3	OK: All services are in their apropriate state.
Blackberry Router	OK	09-23-2009 23:10:16	0d 0h 4m 3s	1/3	OK: All services are in their apropriate state.

Ironport Monitoring

```
check_ironport hostname user password parameter
warning_nro critical_nro
```

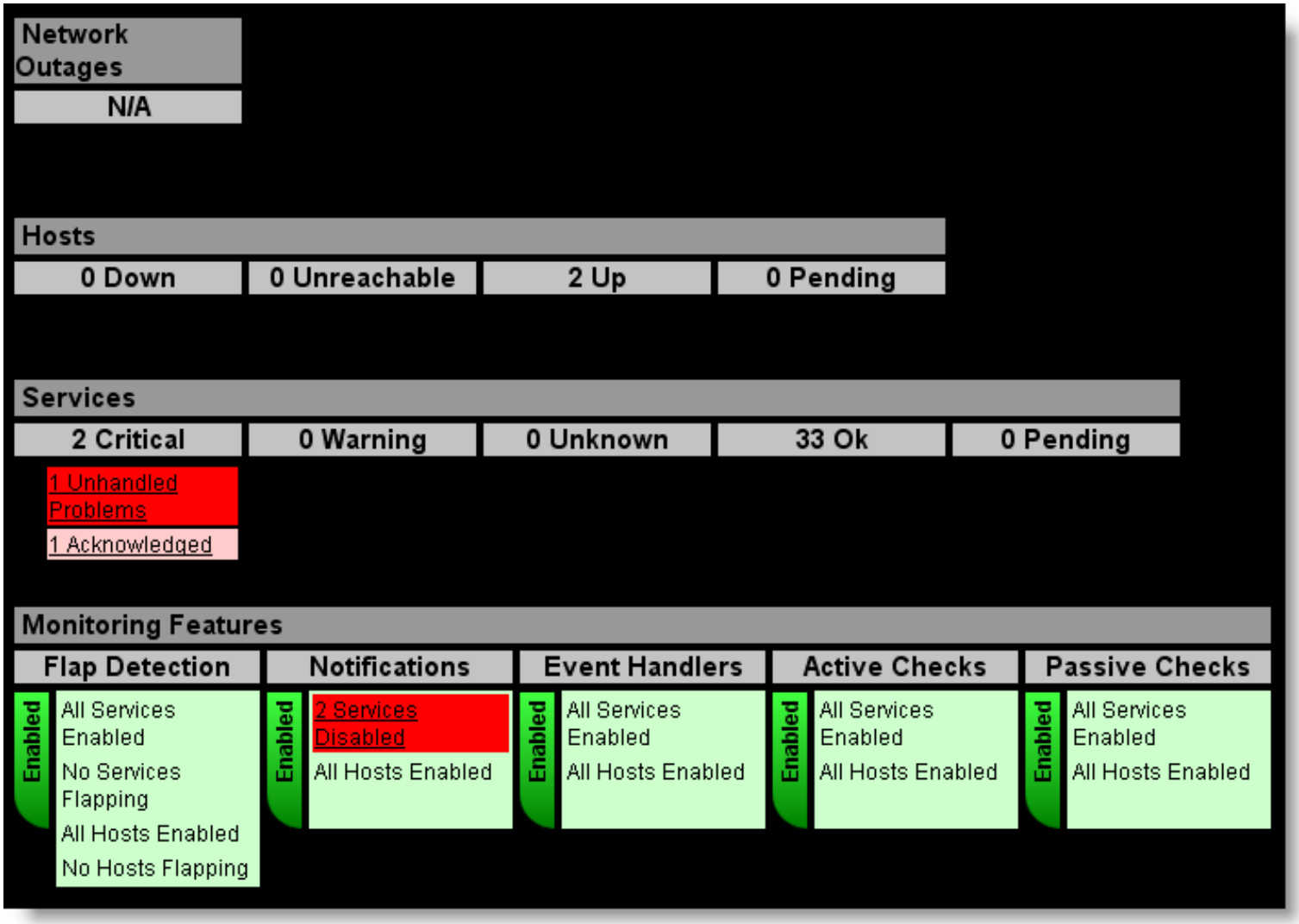
- status
- cpu
- ram
- msgxhour
- conn_in
- conn_out
- workqueue
- msgs_in_quarantine
- disk_util
- queuedisk_usage
- vof_license
- sophos_license
- ipspam_license
- cm_license

CPU	OK	09-24-2009 10:28:28	14d 12h 41m 5s	1/3	CPU OK: 0%
FTP	OK	09-24-2009 10:28:57	29d 0h 57m 49s	1/3	FTP OK - 0.010 second response time on port 21 [220 mx.edcom.de IronPort FTP server (V$) ready.]
IPLICENSE	OK	09-24-2009 10:27:28	29d 0h 46m 49s	1/3	IronPort Anti-Spam License OK: 364 days remaining
MsgInQuarantine	OK	09-24-2009 10:31:12	29d 0h 53m 15s	1/3	MSG In Quarantine OK: 0
MsgPerHour	OK	09-24-2009 10:32:47	29d 0h 56m 34s	1/3	MAIL RATE OK: 20 msgs/hr
Ping	OK	09-24-2009 10:24:22	85d 23h 54m 49s	1/3	OK - 10.0.0.12: rta 2.338ms, lost 0%
Queue	OK	09-24-2009 10:28:28	29d 0h 56m 25s	1/3	QUEUE OK: msgs
RAM	OK	09-24-2009 10:28:58	29d 0h 48m 52s	1/3	RAM OK: 4%
SMTP	OK	09-24-2009 10:29:04	29d 0h 55m 54s	1/3	SMTP OK - 0.004 sec. response time
Status	OK	09-24-2009 10:31:15	29d 0h 56m 16s	1/3	STATUS OK: online
Workqueue	OK	09-24-2009 10:33:42	0d 0h 0m 9s	1/3	WORKQUEUE OK: 0 msgs

Sonstiges

- Quickr
  - Überprüfung des http-Tasks
- Websphere (Portal)
  - über separates Plugin
  - Portlet
- Monitoring der Mailzustellung
  - Kombitest möglich
  - Versand SMTP-Mail
  - Empfang per POP3
- vorgelagerte Mailgateways
  - SMTP Check
  - Betriebssystemüberwachung etc.
- per SNMP Netzwerkports Status

Demo

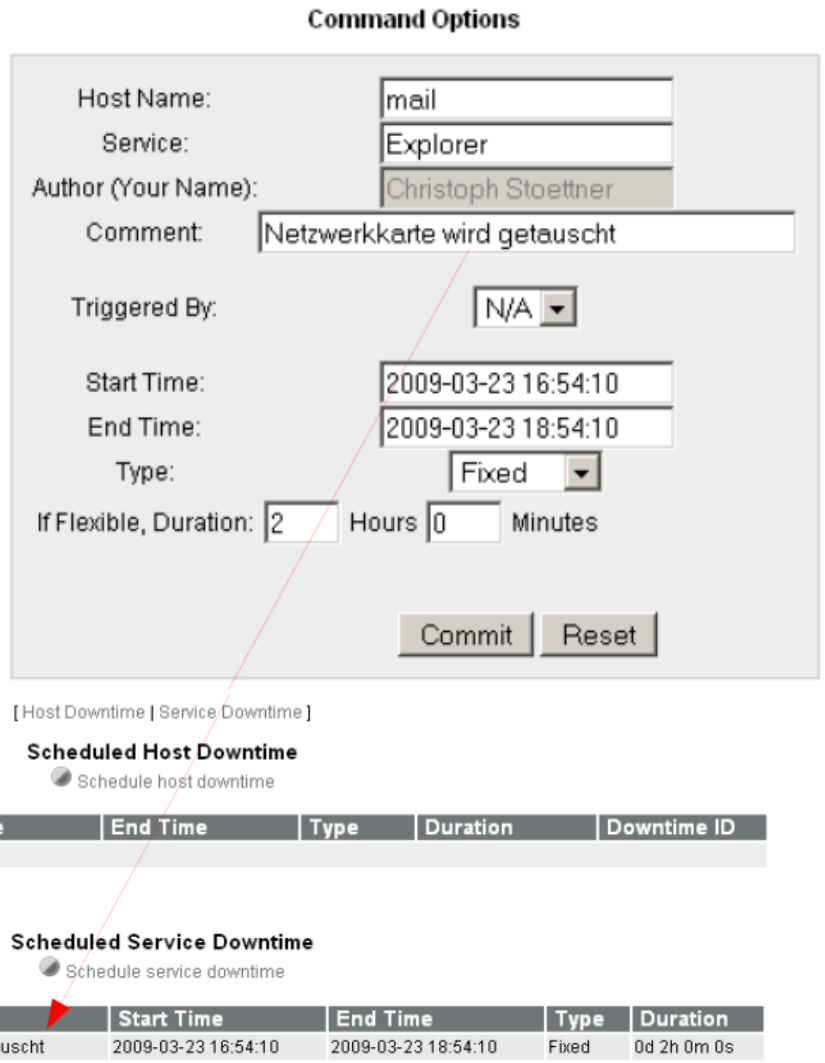

Network Outages
N/A
Hosts
0 Down
0 Unreachable
2 Up
0 Pending
Services
2 Critical
0 Warning
0 Unknown
33 Ok
0 Pending
1 Unhandled Problems
1 Acknowledged
Monitoring Features
Flap Detection
Enabled
All Services Enabled
No Services Flapping
All Hosts Enabled
No Hosts Flapping
Notifications
Enabled
2 Services Disabled
All Hosts Enabled
Event Handlers
Enabled
All Services Enabled
All Hosts Enabled
Active Checks
Enabled
All Services Enabled
All Hosts Enabled
Passive Checks
Enabled
All Services Enabled
All Hosts Enabled

Eventhandler

- Neben Notifications können auch Events ausgelöst werden
- Skripte starten im Fehlerfall
  - auch Soft State möglich
  - Restart Server (SNMP / Remoteskript)
  - Task neustarten
  - Drucker Queue bereinigen
- Restart Skripte mit Bedacht einsetzen

Geplante Downtime

- zur Vermeidung von Notifications
- Eingabe über die Weboberfläche
- Skript per GPO
- Skript z.B. vor Offline Backups



Hochverfügbarkeit

Aktiv – Aktiv

- beide Nagios Server führen Checks aus
- einer alarmiert
- 2. Server kontrolliert Hauptserver
- 2. Server dann manuell aktivieren für Alarm

Aktiv – Passiv

- Heartbeat von passivem Nagios
- Selbstaktivierung bei Ausfall von Server 1

Ressourcen im Netz

- `www.nagios.org`
- `www.nagiosexchange.org` (Plugin-Addon-Sammlung)
- `www.nagiosportal.de` (Foren)
- `www.nagiosforge.org`
- `www.nagioswiki.org`

Zusammenfassung

- Nagios übernimmt viele Routine-Aufgaben
- Einarbeitung und Einsatz lohnt sich in vielerlei Hinsicht
- Mehrwert durch:
  - Aufzeichnung der Daten
    - Antwortzeit
    - Festplattenplatzentwicklung
    - Beleg für Verfügbarkeit
  - Verlässliche Alarmierung
    - Mail
    - IM
    - SMS

Ruhiger Feierabend

Fragen?

Vielen Dank für die Aufmerksamkeit!

Einen ruhigen Feierabend mit Nagios

Bitte die Bewertungsbögen nicht vergessen!

Monitoring

Lästiges Übel oder sinnvolle Prophylaxe?

Christoph Stöttner
christoph.stoettner@edcom.de

Edcom Software & Consulting GmbH – Leopoldstraße 29 – 80802 München
+49 89 3840850 – info@edcom.de – www.edcom.de