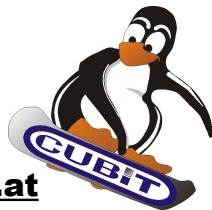


# Open Source based Network Management Monitoring virtueller Umgebungen



**CUBiT IT Solutions GmbH**  
**Ing. Peter-Paul Witta**

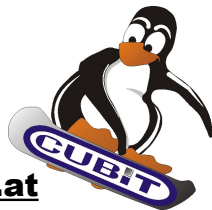
<paul.witta@cubit.at>  
<http://www.cubit.at/pres/>



# Ziele



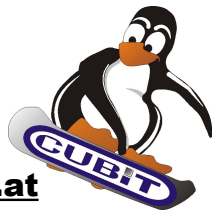
- Information wenn Dienste ausfallen
- über Systemstatus informieren und protokollieren (Verfügbarkeit)
- langfristige Statistiken als Grundlage für Entscheidungen (Aufrüstung bei Leistungsbedarf)
- Überprüfung von externen Dienstleistern (ISP, Telekom, Outsourcer) und deren SLA
- zentrale Informationsstelle
- automatisiertes Reagieren auf Probleme
- automatisierte Behebung
- Umbrella Management



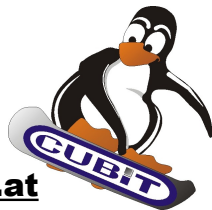
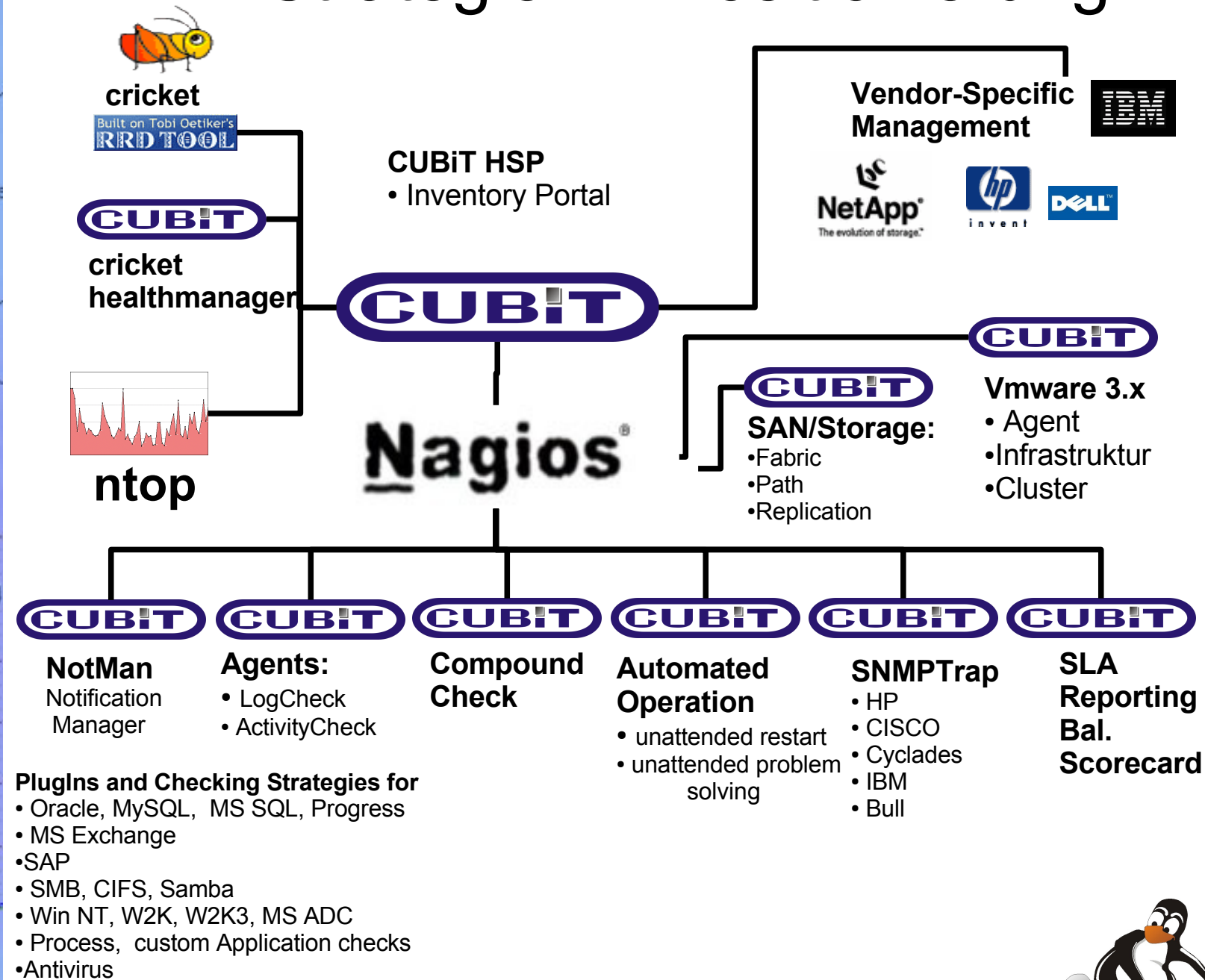
# Strategien



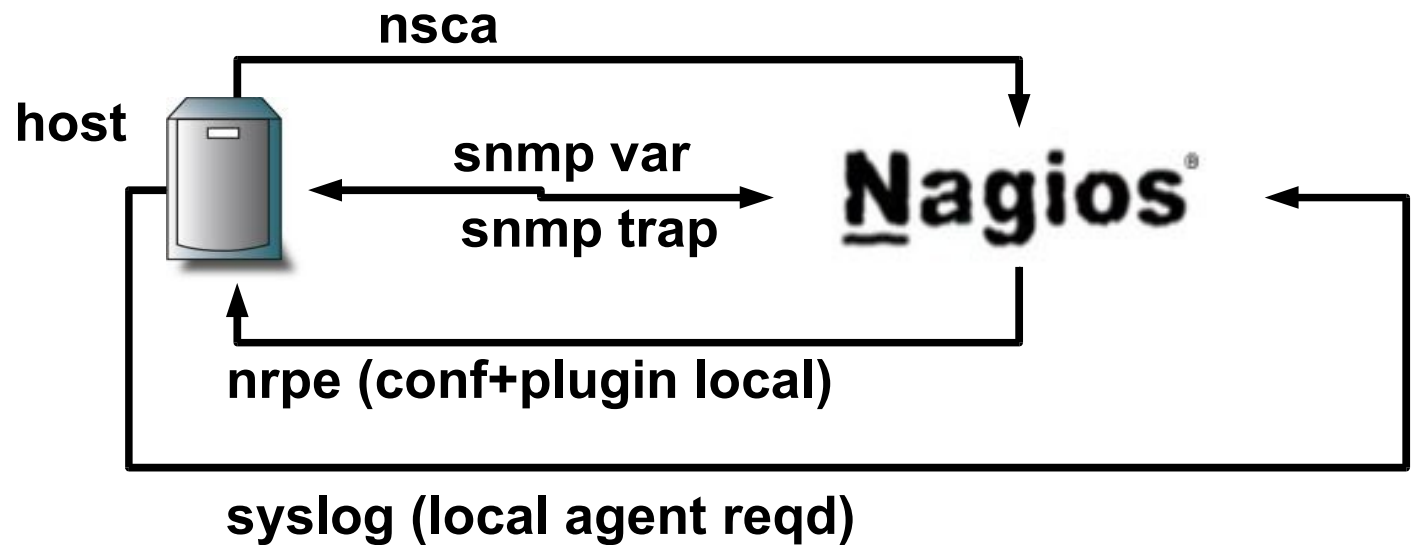
- Blackbox Monitoring -- von außen zugreifen wie ein Anwender
- Whitebox Monitoring -- von innen alle Komponenten einzeln funktionsprüfen
- Schwellwert Monitoring: Überwachen von Messwerten
- richtige Eskalation der Notifizierung
- ggf. automatic response („self-repairing“)
- Compound Checks
- Statistiken: Correlation, SLA-Auswertung
- Umbrella-System
- Monitoring-Netzwerk



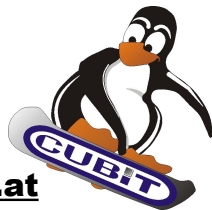
# Strategien – Positionierung



# Nagios Monitoring Schnittstellen



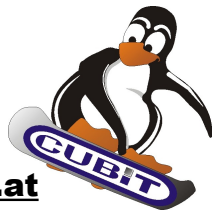
- NSCA: Schnittstelle mit der anderes Programm einen Passive Alert ins Nagios zur Weiterverarbeitung senden kann. Wird extern angestossen.
- NRPE: Schnittstelle, mit der Nagios Plugins (zur Feststellung der Systemverfügbarkeit) auf einem entfernten System gestartet werden können. Die Ausgabe und Prüfung erfolgt zentral im Nagios Core; wird von Nagios aus gestartet



# Komponenten: Nagios Schnittstellen (2)



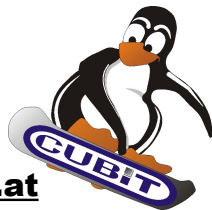
- SNMP Variables
- SNMP Trap
- SMTP
- Windows Eventlog
- Syslog
- SSH
- remote intelligence
- CRICKET
- NotMan



# Nagios Features



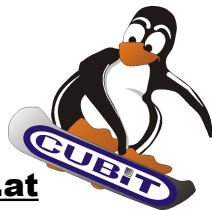
- Nagios Core Process zentral
- führt regelmäßig Plugins aus und wertet Ergebnis aus
- Nagios routet nur PlugIn Output, keine Umformung-> PlugIn muss Fähigkeit haben Situationen zu bewerten!
- empfängt passive Alerts
- Status-Änderungen lösen Events aus
- Events können gehandelt werden (default ist Notify)
- kaum eine Installation ohne Custom-made PlugIn
- PlugIn entspricht Parametrisierung anderer Systeme
- keine Angst vor PlugIns!



# Komponenten: Cricket



- altbekannter Vorgänger: MRTG
- Trennung Datenbank RRDTool und Präsentation (Cricket)
- entwickelt von Tobias Oetiker
- Speichern und Anzeigen von Messwerten; je weiter zurückliegend umso geringere Auflösung
- Messwernerfassung per SNMP oder anders
- Bsp Apache server-status
- Echtzeiterfassung notwendig!
- dynamische Schwellwert - Monitore



# Komponenten: Cricket



## Graphs for Proc-Counter (apache-ssl) (/server/cube1/proc-apache-ssl)

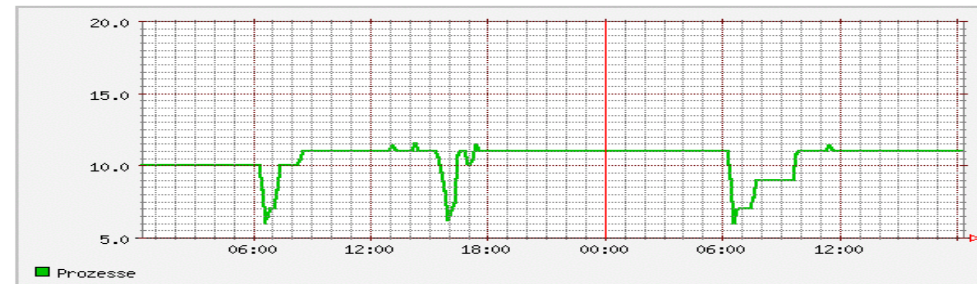
### Summary

Values at last update:  
Prozesse (for the day):  
Cur: 11.00  
Avg: 10.63  
Max: 11.79  
Last updated at Thu Apr 24 18:16:06 2003

### Time Ranges:

[ Daily ]  
[Weekly](#)  
[Monthly](#)  
[Yearly](#)  
[Short-Term](#)  
[Long-Term](#)  
[All](#)

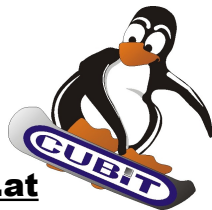
### Daily graph



**Cricket**  
Version 1.0.3

Bei Fragen zu den Grafiken kontaktieren Sie bitte  
[support@cubit.at](mailto:support@cubit.at)

Built on **Tobi Oetiker's**  
**RRDTOOL**



# Komponenten: Cricket



## Graphs for Overlay (/webserver/cubit-cluster)

### Summary

Values at last update for www-lga.cubit.at:

**Bearbeitete Zugriffe** (for the day):

**Cur:** 3.01 Zugriffe/s

**Avg:** 3.32 Zugriffe/s

**Max:** 8.66 Zugriffe/s

[?]

Last updated at Thu Apr 24 18:17:08 2003

Values at last update for www-lgb.cubit.at:

**Bearbeitete Zugriffe** (for the day):

**Cur:** 0.09 Zugriffe/s

**Avg:** 0.00 Zugriffe/s

**Max:** 0.00 Zugriffe/s

[?]

Last updated at Thu Apr 24 18:17:08 2003

*Time Ranges:*

[ Daily ]

[Weekly](#)

[Monthly](#)

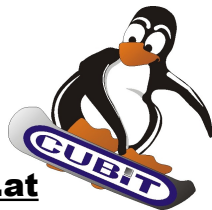
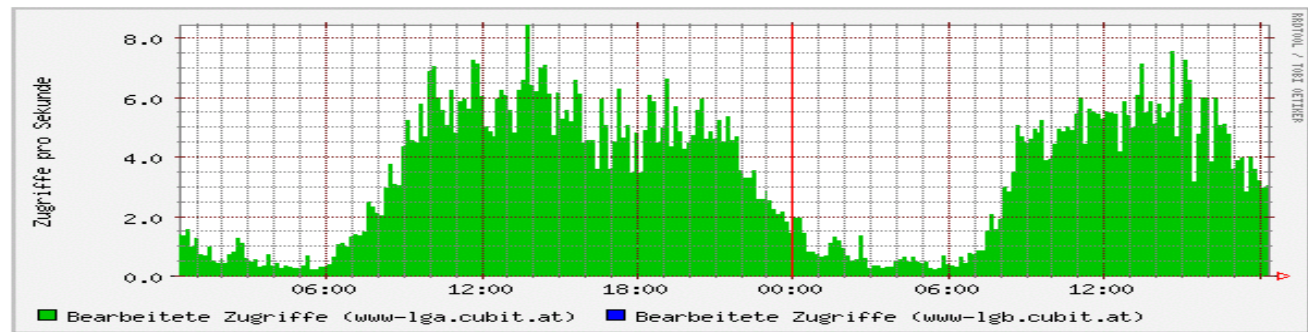
[Yearly](#)

[Short-Term](#)

[Long-Term](#)

[All](#)

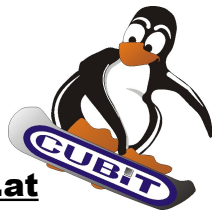
### Daily graph



# Komponenten: Nagios Plugins



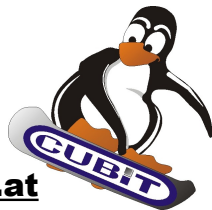
- vielfältig im Internet vorhanden
- in definierten Zeitabständen vom Nagios Core Prozess aufgerufen
- laufen auf dem Nagios Rechner oder mittels NRPE verteilt
- Returnwert im Nagios verarbeitet:  
4 Stati: OK, Warning, Critical, Unknown
- viele Standardprotokolle (Ftp,nfs, http,...) bereits abgedeckt
- neue Plugins sehr leicht erstellbar
- Migration von MON-Scripts  
z.B. einfach möglich
- Angebot: <http://www.cubit.at/?nav=produkte>



# Check von Windows

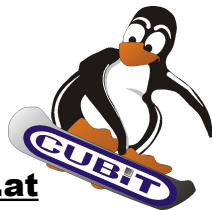


- NSClient (System und Anwendungen), Cricket-WMI, SNMP
- NagEvlog
- NTSyslog
- NRPE-NT
- AD Replication Check
- Registry-Lists
- Rollouts auf Windows
- ActiveState Perl, MS-MSFU
- CMD Restarts, SSH for Windows



# virtualisierte Umgebungen

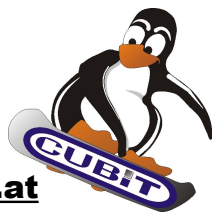
- Hostsystem, Gastsysteme
- Hostsysteme kritisch
- Gastsysteme Applikationsbezogen
- Tiefgehende Checks Hostsysteme
  - Netzwerkzugang
  - Storage Zugang (SAN/NAS/iSAN/vSAN)
  - Ressourcen
  - Clustersysteme: verteilte Funktion, übergreifende Checks
- Speichersysteme
  - „Blackbox“
  - tiefgehende Whitebox Checks auch in die Speichersysteme hinein



# virtualisierte Umgebungen Console



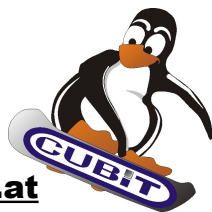
Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
<a href="#">console disk boot</a>	OK	29-01-2007 13:16:18	0d 4h 14m 56s	1/3	DISK OK - free space: /boot 62 MB (66% inode=99%):
<a href="#">console disk root</a>	OK	29-01-2007 13:17:59	0d 4h 14m 56s	1/3	DISK OK - free space: / 3161 MB (67% inode=90%):
<a href="#">console disk var log</a>	OK	29-01-2007 13:20:04	0d 4h 14m 56s	1/3	DISK OK - free space: /var/log 1794 MB (96% inode=99%):
<a href="#">console net nrpe</a>	OK	29-01-2007 13:20:38	0d 4h 14m 56s	1/3	TCP OK - 0.001 second response time on port 5666
<a href="#">console net ping</a>	OK	29-01-2007 13:22:30	0d 4h 14m 56s	1/5	PING OK - Packet loss = 0%, RTA = 0.21 ms
<a href="#">console net ssh</a>	OK	29-01-2007 13:22:58	0d 4h 14m 56s	1/3	SSH OK - OpenSSH_3.6.1p2 (protocol 2.0)
<a href="#">console net vmconsole</a>	OK	29-01-2007 13:24:39	0d 4h 14m 56s	1/3	TCP OK - 0.000 second response time on port 902
<a href="#">console net webaccess extern</a>	OK	29-01-2007 13:14:14	0d 4h 14m 56s	1/3	HTTP OK HTTP/1.1 200 OK - 3258 bytes in 0.004 seconds
<a href="#">console net webaccess intern 8005</a>	OK	29-01-2007 13:16:18	0d 4h 14m 56s	1/3	TCP OK - 0.001 second response time on port 8005
<a href="#">console net webaccess intern 8009</a>	OK	29-01-2007 13:17:59	0d 4h 14m 56s	1/3	TCP OK - 0.000 second response time on port 8009
<a href="#">console net webaccess intern 8080</a>	OK	29-01-2007 13:20:03	0d 4h 14m 56s	1/3	TCP OK - 0.000 second response time on port 8080
<a href="#">console proc cron</a>	OK	29-01-2007 13:20:38	0d 4h 14m 56s	1/3	PROCS OK: 1 process with args 'cron'
<a href="#">console proc snmpd</a>	OK	29-01-2007 13:22:30	0d 4h 14m 56s	1/3	PROCS OK: 1 process with args 'snmpd'
<a href="#">console proc xinetd</a>	OK	29-01-2007 13:22:58	0d 4h 14m 56s	1/3	PROCS OK: 1 process with args 'xinetd'
<a href="#">console sys load</a>	OK	29-01-2007 13:24:40	0d 4h 14m 56s	1/3	OK - load average: 0.02, 0.03, 0.00
<a href="#">console sys swap</a>	OK	29-01-2007 13:14:14	0d 4h 14m 56s	1/3	SWAP OK - 96% free (518 MB out of 541 MB)



# virtualisierte Umgebungen ESX

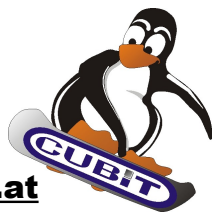


<a href="#">esx-host queststate</a>	OK	29-01-2007 13:16:18	0d 4h 14m 56s	1/3	VHosts: 2/2 up (1064), (1059)
<a href="#">esx-host net nicstatus all</a>	OK	29-01-2007 13:17:59	0d 4h 14m 56s	1/3	OK: 2 OK (vnic0,vnic1)
<a href="#">esx-host net nicstatus vnic0</a>	OK	29-01-2007 13:20:04	0d 4h 14m 56s	1/3	OK: (vnic0) duplex mode is Full, speed is 1000 Mbps, link is Up
<a href="#">esx-host net nicstatus vnic1</a>	OK	29-01-2007 13:20:38	0d 4h 14m 56s	1/3	OK: (vnic1) duplex mode is Full, speed is 1000 Mbps, link is Up
<a href="#">esx-host net vmkping</a>	OK	29-01-2007 13:22:30	0d 2h 46m 51s	1/3	OK: Packet loss: 0%, RTA = 0.187 ms
<a href="#">esx-host net vmkping</a>	OK	29-01-2007 13:22:58	0d 2h 46m 51s	1/3	OK: Packet loss: 0%, RTA = 0.391 ms
<a href="#">esx-host proc vmx</a>	OK	29-01-2007 13:24:40	0d 4h 14m 56s	1/3	PROCS OK: 2 processes with args 'vmware-vmx'
<a href="#">esx-host storage availability-local</a>	OK	29-01-2007 13:14:15	0d 2h 48m 14s	1/3	OK: Read-Write test successful
<a href="#">esx-host storage availability-nfs-esx_reidko nfs</a>	OK	29-01-2007 13:16:18	0d 0h 54m 53s	1/3	OK: Read-Write test successful
<a href="#">esx-host storage availability-san-esx_reidko san1</a>	OK	29-01-2007 13:18:01	0d 0h 54m 19s	1/3	OK: Read-Write test successful
<a href="#">esx-host storage availability-san-esx_reidko san2</a>	OK	29-01-2007 13:20:04	0d 1h 35m 11s	1/3	OK: Read-Write test successful
<a href="#">esx-host storage availability-san-esx_reidko san3</a>	OK	29-01-2007 13:20:38	0d 2h 48m 14s	1/3	OK: Read-Write test successful
<a href="#">esx-host storage paths</a>	OK	29-01-2007 13:22:30	0d 3h 53m 10s	1/3	OK: All preferred paths are active
<a href="#">esx-host storage usage-local</a>	OK	29-01-2007 13:22:58	0d 2h 1m 51s	1/3	OK: 38.5 % used ( 39.640 GB free)
<a href="#">esx-host storage usage-nfs-esx_reidko nfs</a>	OK	29-01-2007 13:24:40	0d 2h 47m 51s	1/3	OK: 64.8 % used ( 15.126 GB free)
<a href="#">esx-host storage usage-san-esx_reidko san1</a>	WARNING	29-01-2007 13:14:14	0d 0h 59m 38s	3/3	WARNING: 85.3 perc. used ( 3.901 GB free)
<a href="#">esx-host storage usage-san-esx_reidko san2</a>	WARNING	29-01-2007 13:16:18	0d 2h 35m 13s	3/3	WARNING: 85.3 perc. used ( 3.901 GB free)
<a href="#">esx-host storage usage-san-esx_reidko san3</a>	OK	29-01-2007 13:18:00	0d 2h 4m 11s	1/3	OK: 64.0 % used ( 26.990 GB free)
<a href="#">esx-host storage usage all</a>	WARNING	29-01-2007 13:20:06	0d 0h 53m 57s	3/3	STORAGE USAGE WARNING: san-esx_reidko_san2: 85 %, san-esx_reidko_san1: 85 %
<a href="#">esx-host sys cpu</a>	OK	29-01-2007 13:20:38	0d 3h 19m 50s	1/3	CPU-OK: CPU-Usage 10% (Userspace: 1%, Kernel: 1%, I/O-Wait: 8%)
<a href="#">esx-host sys io</a>	OK	29-01-2007 13:22:30	0d 3h 35m 50s	1/3	OK: 120 kB/s (in: 0 kB/s, out: 120 kB/s)
<a href="#">esx-host sys mem</a>	CRITICAL	29-01-2007 13:22:58	0d 13h 31m 15s	3/3	CRIT: Memory free: 3067Mb (80.6%) [Total available 3806Mb] Memory split: pvt/shr/bal/swp = 19.54%/80.45%/0%/0%



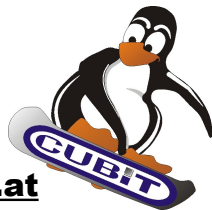
# virtualisierte Umgebungen 3 Cluster

- Aussage über Cluster
  - Abfrage aller Member
  - Korrelation der Ergebnisse
    - läuft eine VM nur einmal?
    - läuft eine VM überhaupt?
    - welche Vorgänge schlugen fehl?
    - sind DRS Anforderungen gedeckt?
    - wie ist DAS Auslastung?
  - Sind genug Hardwareressourcen vorhanden?
  - (geplant) Ist Vcenter aktuell synchron?



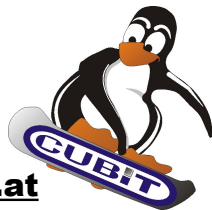
# Storageumgebungen

- In virtualisierten Speicherumgebungen ist einiges anders
  - nur Stageserver kennt Belegung (Auslastung)
  - Clone und Snapshots verfälschen Belegung aus Hostsicht
  - In den Stageserver hineinschauen
    - Komponenten einzeln betrachten
    - Auslastungszähler
    - Prüfung interner Parameter
  - Nutzung von SNMP und/oder Befehlsshell
  - Prüfung von Performance- und Systemwerten
  - Prüfung der Synchronität von Spiegeln
  - Hardwaremonitoring



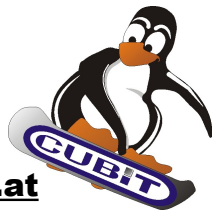
# Storageumgebungen

- Pfadanalyse
  - vom Host aus
  - Nutzung spezifischer Software ([Secure|Power]Path)
  - wie sieht der Host verschiedene Targets
  - welche Pfade sieht er
  - benutzt er die richtigen und sind alle da?
  - Alarm bei Path Failover
  - Alarm bei Targetverlust
- Fabric Check
  - Prüfung Fabric Switches
  - Prüfung kritischer Verbindungen (ISL, Path)
  - Fabricdienste da (SnS, ...)
  - Zoninginformation
  - Alarm auch bei Configchecks



# kritische Netzwerkkumgebungen

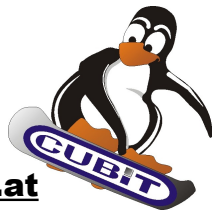
- kritisch bei ISCSI, CIFS, NFS (NAS/iSAN)
- Prüfung wichtiger Ports
- Prüfung wichtiger Channels
  - Alarm bei Verlust einzelner Links
- Prüfung der Neighborhood Tables
- sehen Switches einander?
- Sehen Switches wichtige Server?
- Sehen wichtige Server MAC-Adressen wichtiger Ressourcen im ARP Layer (Ethernet)?
- iSCSI, iSAN
  - Prüfung ob Target Portale da
  - Mapping möglich
  - Targets erreichbar



# Komponenten: SNMP (1)



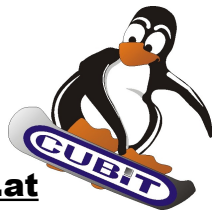
- große Unterstützung von Herstellern von Geräten
- Server, Router, Switch, jede Hardware kann heute SNMP Variablen ausgeben und Traps senden
- Abfrage von SNMP-Variablen wie Interface-Traffic, Systembelastung, Plattenauslastung, Temperatur,...
- Einleitung in Cricket
- Bei Überschreitung von Schwellwerten Alarm via NSCA in Nagios



# Komponenten: Trapreceiver



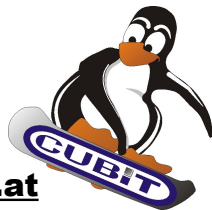
- SNMP Trap Support:
- Geräte können bei Fehlern sog. Traps als Alarm generieren
- Dieser Event wird von außen ins Nagios eingeleitet
- Definition Linux Server als Trap Target in den Geräten
- trapreceiver empfängt Trap und leitet ihn via NSCA ins NAGIOS weiter
- einfachste Installation, im Gerät nur IP-Addr. des Trapreceiver-Hosts eingeben



# Komponenten: Compound Checks



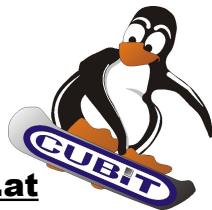
- Erheben korrelierter Systemzustände (in Beziehung setzen) durch Aufruf mehrerer Plugins
- oder Auswertung aktueller Nagios-Stati
- Neu-Bewertung der verbundenen (korrelierten) Situation in Plugin-Logik
- Definition neuer Zustand für Situation
- Rückmeldung
- Beispiele
  - Cluster-Check für Web-Anwendungsarchitekturen
  - Cluster-Check für MS Transaction Server
  - beliebige weitere Punkte



# HSP Portalsystem G2



- Web-basiertes Portal (Apache/MySQL)
- verlinkt zu nachgelagerten Systemen
  - Vendor-SM, Ntop, Cricket, SSH, VNC,...
- Wartungs- und Zusatzinformationen
  - Wartungsverträge
  - Kontakte
  - Logbücher
- Hardware Profile Inventory
  - MAC-Adressen, CPU, Memory, Disks
- Beziehung VM/Hostsystem



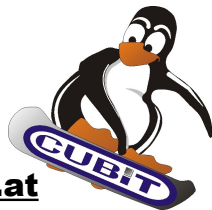
# HSP Portalsystem G2-2



CPU-Informationen					
vendor_id	cpu_family	model_name	cpu_mhz	cache_kb	Optionen
GenuineIntel	15	Intel(R) Xeon(TM) CPU 2.40GHz	2399.397	512 KB	

Netzwerk-Informationen			
interface	inet_addr	mac_addr	Optionen
eth1	172.23.64.68	00:0B:CD:37:4B:0E	
eth1	172.23.64.66	00:0B:CD:37:4B:0E	
eth3	172.24.128.66	00:05:5D:7D:2B:4D	
eth0	10.7.0.1	00:0B:CD:37:4B:77	

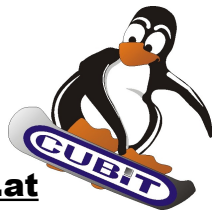
Festplatten			
filesystem	size	mounted on	Optionen
/dev/cciss/c0d0p7	6015880	/home	
/dev/cciss/c0d0p1	197546	/boot	
/dev/cciss/c0d0p3	1521984	/	
/dev/cciss/c0d0p2	5039856	/usr	
/dev/cciss/c0d0p5	20159916	/var	
/dev/sda1	10080488	/var/lib/mysql	



# Notification Manager „NotMan(n) G2“



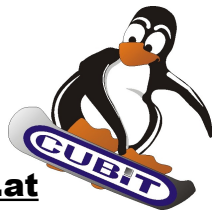
- grafisches Abonnieren von Alarmen
- Aussendung in Echtzeit an alle abonnierten Empfänger
- Kriterien: Uhrzeit, Medium (SMS, Email, Voice), Wochentag, Feiertag, Alarmklasse, Systemgruppen
- freundlicher Assisten (auch für nicht-IT User)
- Addon Tool: keine Rekonfiguration von Nagios notwendig
- kein Restart von Nagios bei Änderungen notwendig
- MySQL basierend
- hohe Leistung, hoher Durchsatz
- geplant: Zeitzonen-Routing  
Voice IVR



# Event-Handling



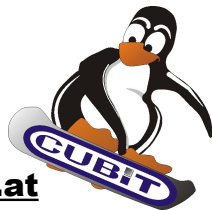
- un-attended Operation
- automat. Reagieren auf Probleme
- Reduktion Service-Calls und Alarme um typisch 70%
- automat. Einhalten von Service-Profilen
- Event-Routing mit Notification Manager
- GUI zum Routen der Events
- Vertretungsfunktion, Schablonen, Berechtigungen
- Automatisches Re-Provisioning von knappen Ressourcen
  - Vmware shares
  - Storage Space



# Addon-Tools: ntop, E2E



- ntop: Open Source Tool: Echtzeit Netzwerkskan
- Statistiken und Web-Output, rrd Output
- NetFlow/sFlow Input
- kann in Standorten mitinstalliert werden oder im Core dediziert laufen
- Achtung: Tuning der Tabellen für Performance und Speichermanagement notwendig
- E2E: eigene Plugins für Standorte
- etwa SAP Login und Transaktionsdurchführung
- dient zur SLA -Kontrolle und tactical operation

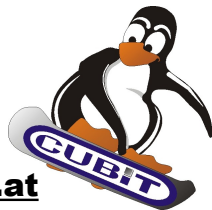




# Specials: Mix It Right (2)



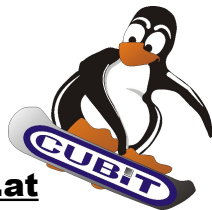
- Umsatz pro Minute von Shopsystemen: Kein Umsatz=Fehler (Heuristik!)
- Alarm bei Änderungen von Konfigurationsfiles -- Information wenn jemand Konfiguration ändert
- Direkte Einbindung von NSCA in Businesslogik -- eigene Anwendung spricht direkt mit Nagios Enterprise Konsole
- Antwortzeiten- und Ergebnisüberwachung
- Nagios leitet Alarme ggf. auch weiter -- an Nagios oder auch an BMC
- Reporting via Nagios: Report der Produktionszahlen via Nagios Infrastruktur
- Konfigurationsprüfung via Nagios



# Integration



- via HSP können Webtools eingebunden werden
- keine Ersatz für Management Tools (Switch Management, Server Management)
- zentrale Kommandozentrale
- Nagios Core Process als Information Hub
- Duale Information
- spezielle Systeme (Switch Management etc.) berichten an Nagios



# Danke



- weitere Informationen: <mailto:paul.witta@cubit.at>
- <http://www.cubit.at>
- ItnT 2007 Stand A0330
- Livedemo möglich

