Open Source based Network Management

CUBiT IT Solutions GmbH
Ing. Peter-Paul Witta

<paul.witta@cubit.at>
http://www.cubit.at/lw04/

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) und deren SLA
- zentrale Informationsstelle
- automatisiertes Reagieren auf Probleme
- automatisierte Behebung

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“)

Strategien – Blackbox

- Blackbox Monitoring -- von außen zugreifen wie ein Anwender
- für Standard-Protokolle mit vorhandenen Plugins für FTP,HTTP,NFS, SMB (Samba/CIFS), Citrix,DNS und viele andere
- für eigene Anwendungen durchaus auch automatische Überprüfung der Business-Logik
- zB: Webshop: automat. Einkaufen, erzeugen eines speziell markierten Auftrages, der nicht weiterverarbeitet wird

Strategien – Messwerte

- laufende Überwachung von Leistungsdaten
- CPU, Netz, Plattenauslastung
- Überwachen von Tuningmaßnahmen, wie z.B. Cache-Hit-Ratio
- Alarm bei nicht optimaler Leistung
- Alarm bei bedrohlichem Zustand (Disk Full 90%)
- Alarm bei Aufrüstungsbedarf (80% Leitungsauslatung im Tagesmittel

Strategien – Whitebox

- Alle Teilkomponenten der Anwendung getrennt prüfen
- Notwendige Datenbanken, Anwendungen, Netzwerkequipment, Frontendserver, Netzwerke, Subsysteme,... ständig jeden einzeln prüfen
- Notwendig auch zur Problemlokalisierung
- liefert aber nicht gleiche Sicht wie Anwender sieht
- System- nicht Lösungsbezogen

Built on Tobi Oetiker's RRD TOOL

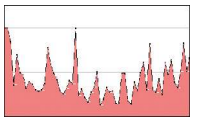
cricket
SNMP-Data
Data-based alerts

CUBiT

CUBiT HSP
- Inventory
- Web integration
- History
- Link to other products

Integration of Vendor-Specific Management
- HP ASM
- Compaq Remote Insight
- IBM eDIRECTOR
- Dell OpenManager
- Bull ESMpro

ntop



Nagios

CUBiT

Agents:
- LogCheck
- ActivityCheck

CUBiT

SNMPTrap
- HP
- CISCO
- Cyclade
- IBM
- Bull

CUBiT

Automated Operation
- unattended restart
- unattended problem solving

PlugIns and Checking Strategies for
- Oracle, MySQL, MS SQL, Progress
- MS Exchange
- SMB, CIFS, Samba
- Win NT, W2K, W2K3
- Process Check
- Kaspersky AntiVirus
- custom Application checks
- complex compound checks

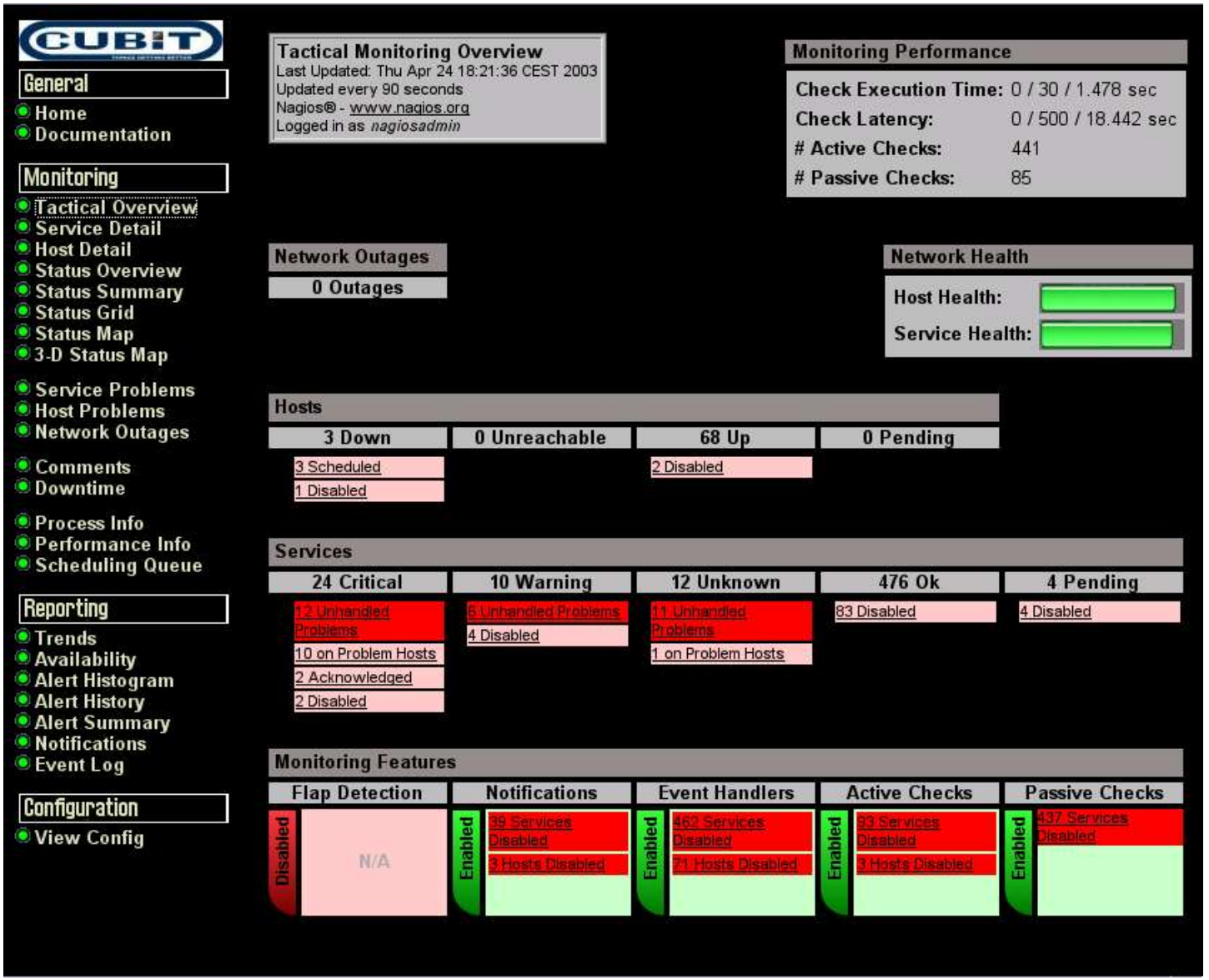
Komponenten

- Nagios
- Cricket
- Integration von lokal laufenden Agenten: logcheck, activitycheck
- Integration von Syslog, SMTP, und anderen Diensten mit NSCA
- Einbindung SNMP Traps: trapreceiver
- HSP Portalsystem
- Alerting via SMS, Email, ICQ über Nagios
- ntop und rrd für Statistikdaten

Komponenten: Nagios

- altbekannt; bis 2001 Netsaint, danach Nagios
- entwickelt von Ethan Galstad
- Best Of Breed: Vergleich mit MON und Big Brother
- zentrale Schaltstelle, „Information HUB“
- Offene Schnittstellen:
- NSCA (Nagios Service Check Acceptor)
- NRPE (Nagios Remote Plugin Executor)
- Ayamon Inc

Komponenten: Nagios -Web



Komponenten: Nagios (2) 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

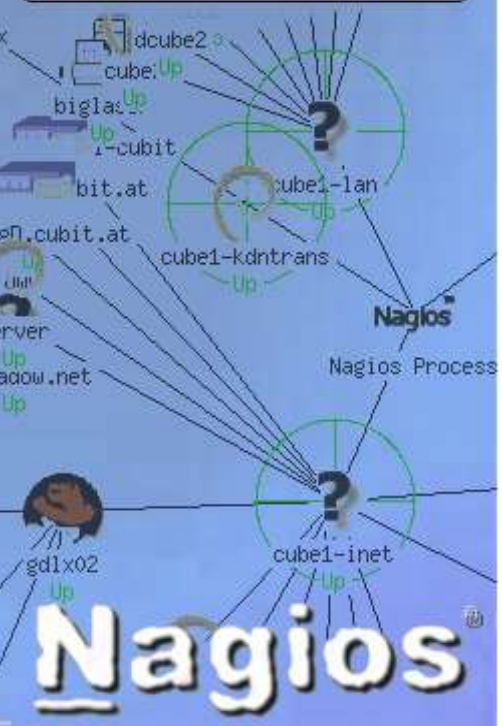
Nagios Features

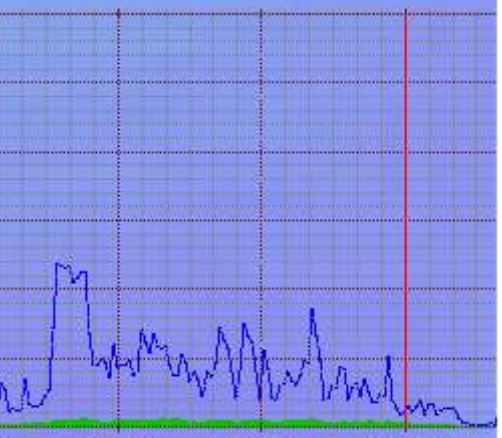
- Nagios Core Process zentral
- führt regelmäßig Plugins aus und wertet Ergebnis aus
- empfängt passive Alerts
- Status-Änderungen lösen Events aus
- Events können gehandelt werden (default ist Notify)
- Notifizierungen werden wiederholt solange sie lt. Konfiguration wiederholt werden sollen
- Eskalation bei Notifizierung möglich

CUBIT

open source for enterprise

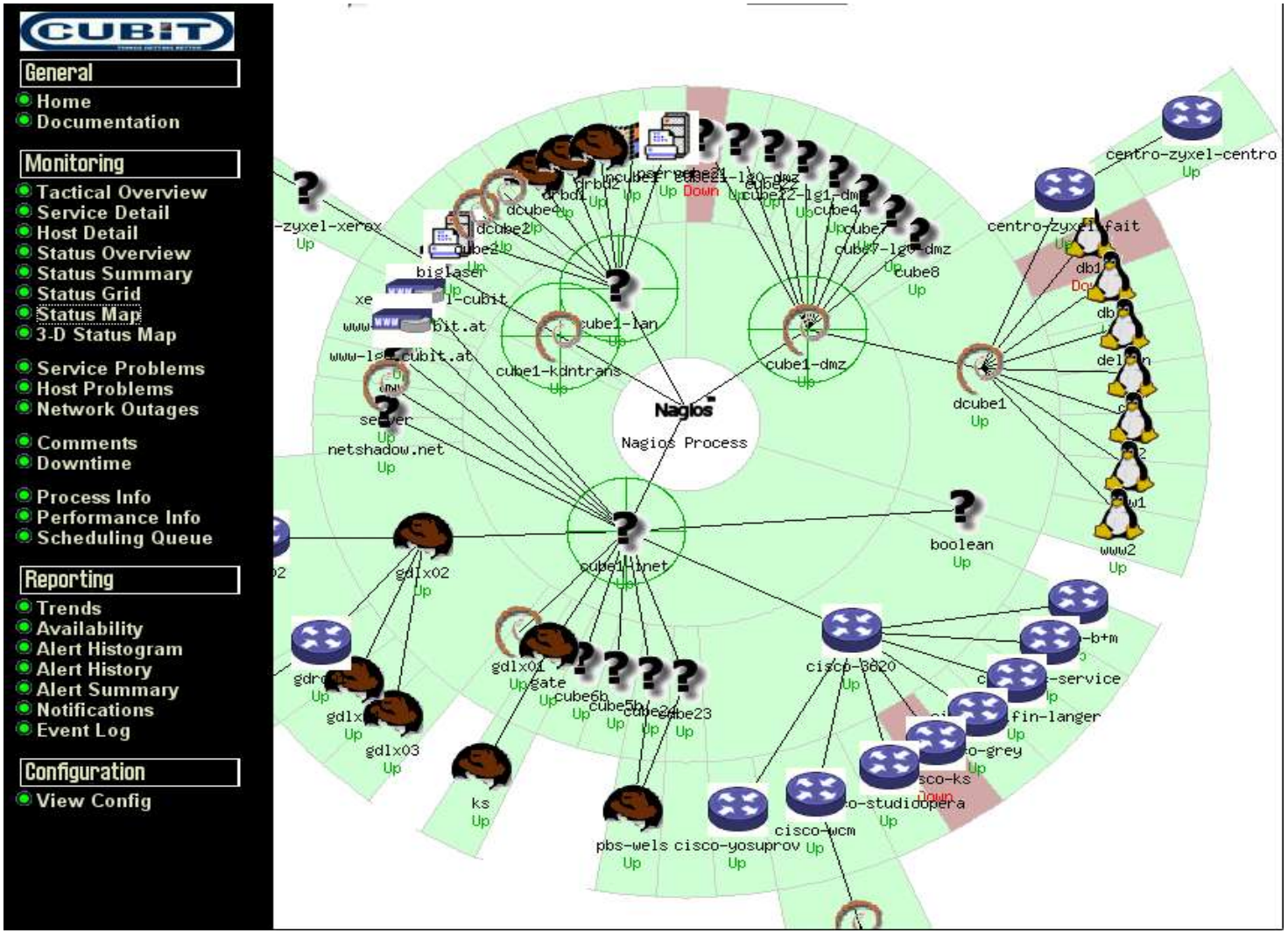
linuxwochen





OpenSource
Network Management

Nagios Enterprise Console



Nagios Features (2)

- Optimiert: nicht-erreichbare Rechner und Dienste werden erst gar nicht geprüft
- Scheduling Queue Management
- Kann Messwerte auslesen und in RRDTool/Cricket einleiten
- Web-Interface und GNOME-Interface zu Nagios-Core
- Stati können auch anders ausgelesen werden, zB Website um direkt Anwender „freundlich“ zu Informieren
- kann via Email, SMS und ICQ notifizieren

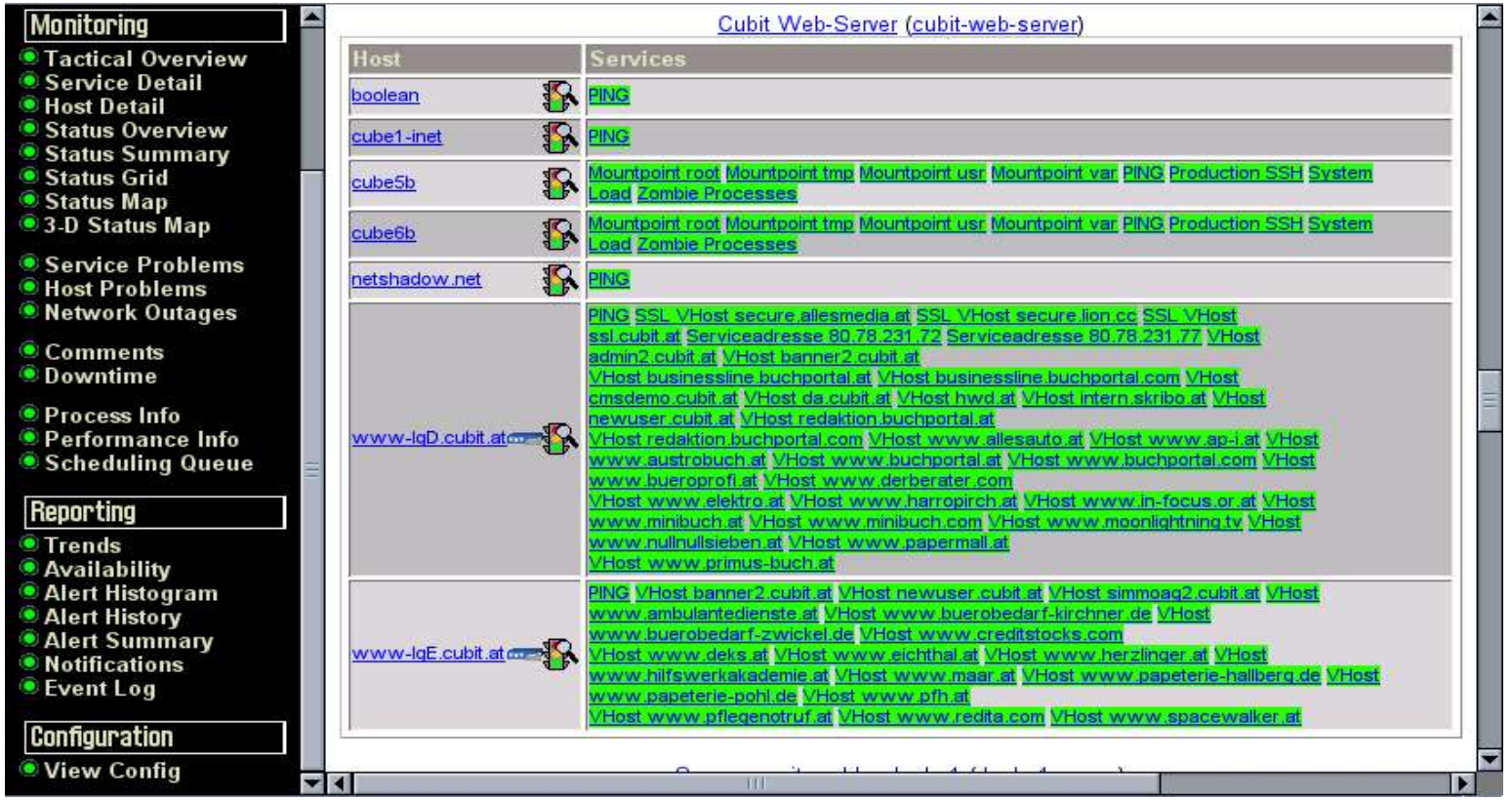
Nagios (3)

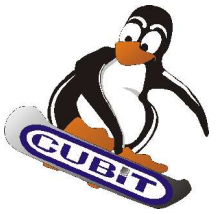
- rege Community
- enorme Anzahl Plugins verfügbar
- optional mod_perl-ähnlichen integrierten Interpreter um fork/exec/precompile Zyklen zu optimieren
- leichtes Plugin-Interface; Plugin-Erstellung einfach
- bestehende mon-Scripts und Eigenentwicklungen können leicht migriert werden

Nagios-Konfiguration (4)

- althergebracht (mit Web-Konfiguration NAGAT)
- alternativ Template-basiert
- Vererbung mit Templates
- überlegte Struktur entscheidet über erfolgreiche Implementierung
- Generation der Intial-Config aus NMAP Scan möglich (sonst kein auto-discover)
- Nagios 1.2: Wildcards!

Nagios-Screenshot





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
- Messwerterfassung per SNMP oder anders
- Bsp Apache server-status
- Echzeiterfassung notwendig!

Komponenten: Cricket

CUBIT Information Technology Solutions .cricket

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

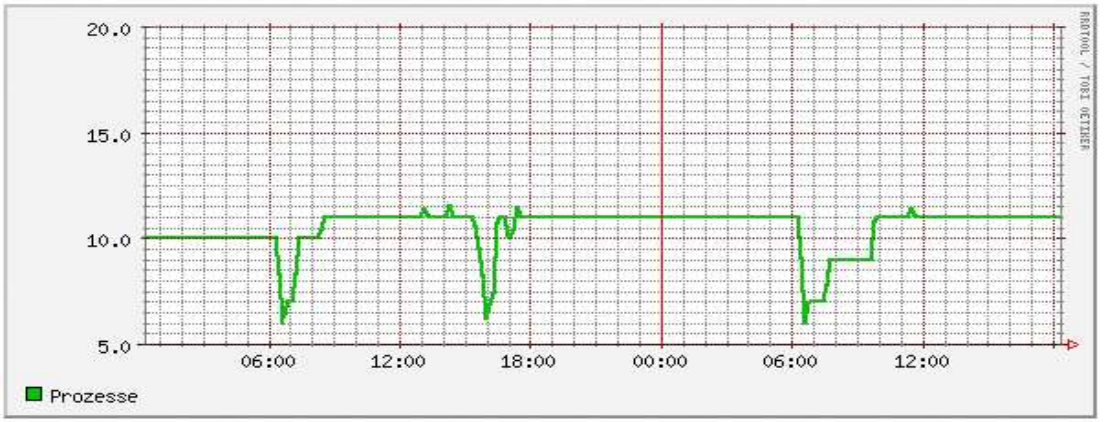
Summary

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.

Built on Tobi Oetiker's RRD TOOL

Komponenten: Cricket

- Apache Server-Status

Graphs for Overlay (/webserver/cubit-cluster)

Summary

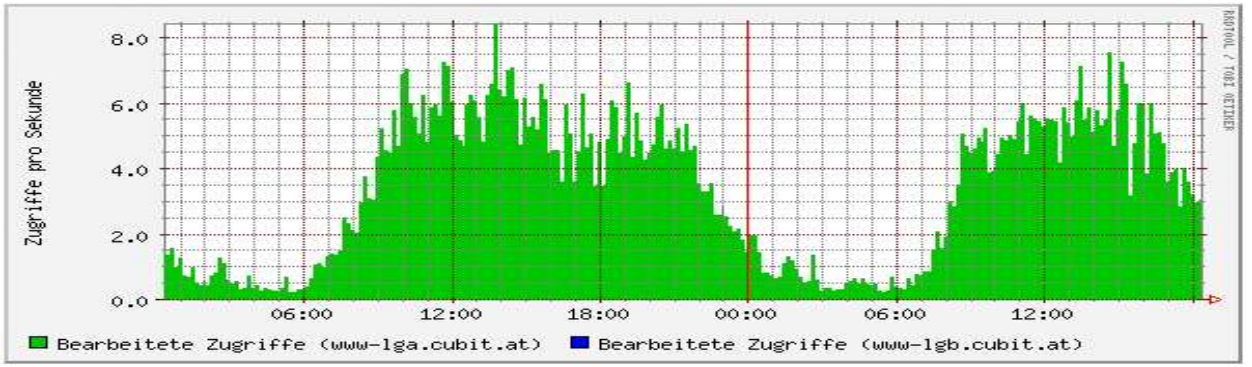
Values at last update for www-lga.cubit.at:
Bearbeitete Zugriffe (for the day):
Cur: 3.01 Zugriffe/s
Avg: 3.32 Zugriffe/s
Max: 8.66 Zugriffe/s
[?]
Last updated at Thu Apr 24 18:17:08 2003

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: Agenten

- Eigenentwicklung CUBiT
- Activitycheck reagiert wenn Files sich nicht in definierten Zeitabständen ändern
- Logcheck liest Logfiles, reagiert auf per Regexp definierte Meldungsmuster
- Alarm ins Nagios per NSCA (exotische Plattformen per Email)
- Logcheck läuft als Cronjob, Activitycheck als Service

Komponenten: Nagios Plugins

- vielfältig im Internet vorhanden
- in definierten Zeitabständen vom Nagios Core Porzess 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

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

HSP Portalsystem

- 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
- Daten auch zu anderen Zwecken nutzbar

HSP Portalsystem 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	

Komponenten: SMTP-NSCA

- viele Geräte können von Haus aus Mails senden im Fehlerfall: Disk-Arrays, RAID-Treiber (3dm)
- Email-Alarm leicht integrierbar (CRON-Jobs, AS/400 Anwendungen)
- procmail-Filter generiert NSCA Aufruf bei einlangender SMTP Nachricht mit Textübergabe
- Einfache Anbindung existierender „Mail-Monitorings“

Event-Handling

- un-attended Operation
- automat. Reagieren auf Probleme
- Reduktion Service-Calls und Alarme um typisch 70%
- autmat. Einhalten von Service-Profilen
- Event-Routing mit Notification Manager (geplant)
- GUI zum Routen der Events
- Vertretungsfunktion, Schablonen, Berechtigungen

ntop

- Open Source Tool: Echtzeit Netzwerkscan
- Statistiken und Web-Output
- rrd Output
- NetFlow/sFlow Input
- kann in Standorten mitinstalliert werden
- kann im Core dediziert laufen
- Achtung: Tuning der Tabellen für Performance und Speichermanagement notwendig
- Sonst potentiell Systemabsturz

Specials: Mix It Right

- besondere Betriebszustände mit eigenen Lösungen ansteuern
- SNMP Auslesen von Switchdaten, Netzwerkstrukturen, Ports
- Master-Checksysteme implementieren für komplexe Abbildungen
- durchaus auch eigene Clients für Protokolle entwickeln
- Diagnosesystem in Multi-Tier Anwendungen integrieren -- Selbstdiagnose die von Nagios-Plugin geparsed wird

Specials: Temperatur

CUBiT Information Technology Solutions .cricket

Graphs for Rack001 (/temp/rack001)

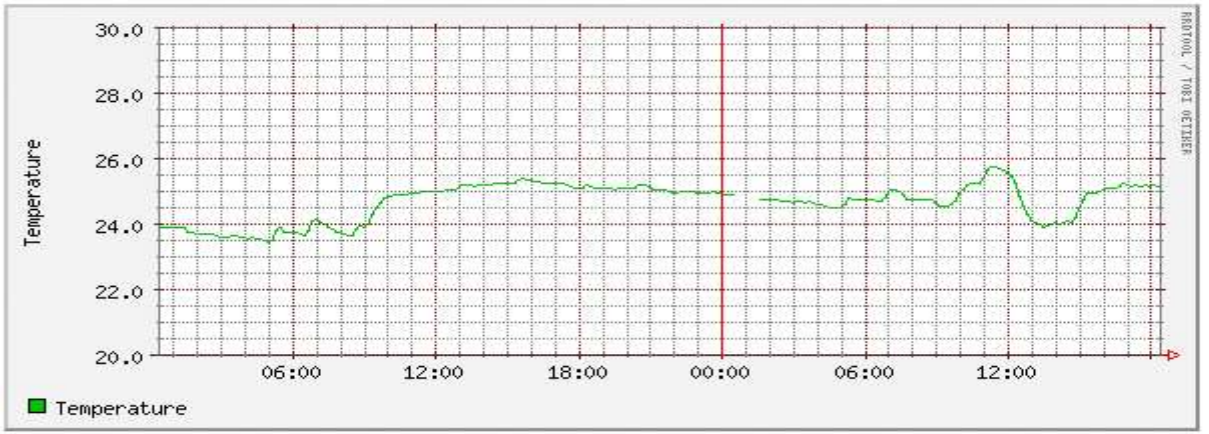
Summary

Values at last update:
Temperature (for the day):
Cur: 25.15 °C
Avg: 24.87 °C
Max: 25.75 °C
[?]
Last updated at Thu Apr 24 18:17:05 2003

Time Ranges:

[Daily]
Weekly
Monthly
Yearly
Short-Term
Long-Term
All

Daily graph



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

Praxiserfahrungen

- Vor- und Nachteile im Vergleich zu Big Brother und Mon
- Vor- und Nachteile im Vergleich zu kommerziellen Systemen
- Integration mit anderen Systemen

Unterschiede BB / Mon

- komplexere Konfiguration, mehr Möglichkeiten
- mehr „fertig“ im Vergleich zu Mon
- mehr Plugins verfügbar
- keine unnötigen Checks
- detailliertere Möglichkeiten
- objektorientierte Konfiguration – Template-based

Vergleich andere

- komplex genug
- keine Struktur, ein-dimensionale Gruppenstruktur mit nur einer Ebene
- daher Namensgebung und Wildcards wichtig!
- variabel Konfigurierbar
- Aufwand bei gleichem Ergebnis konstant
- Anzahl überwachter Systeme ist kostenneutral
- Aufwand Implementierung evtl. komplizierter, wenig Support für exotische kommerzielle Systeme

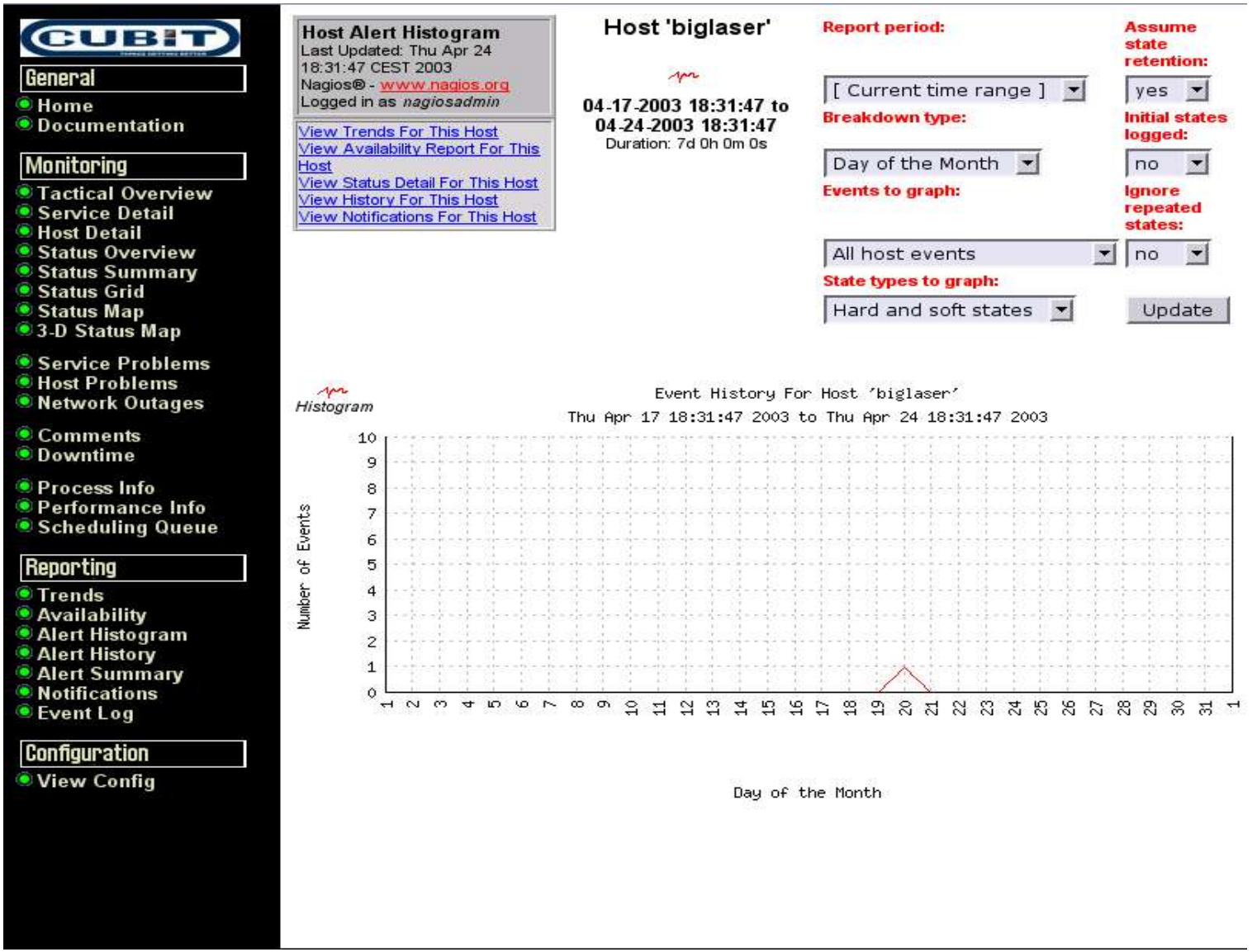
Integration

- via Host-spezifischer Website 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

Projekterfahrung

- Bedarf muss gegeben sein (Netzwerkgröße, Dienstanzahl)
- für kleinere Anwendungen ASP-Ansatz (shared Nagios-Server, Mandantenfähig)
- Struktur in Abbildung wichtig (Org/Geo)
- Evtl. verteiltes Monitoring um Last zu teilen
- eigene Failover-Lösung: Checks die als „Backup“ fahren werden erst bei Versagen des Primärservers aktiv
- Statistiken wichtig

Projekterfahrung - Stats



Projekterfahrung (2)

- richtiger Nutzen erst mit spezifisch geschriebenen Plugins („Harry Potter Monitor“)
- standardisierte Schnittstelle in Multi-Tier Anwendungen sinnvoll um Aufwand für die Erstellung eigener Plugins zu senken
- Support für Industriestandard-Hardware oft nicht so gut, Verständnisproblem bei Anwendern
- Dienstleister kann Know-How einbringen, Consulting vor Allem bei Aufbau Template-Struktur und Monitoring-Strategie wichtig

Projekterfahrung (3)

- Implementierungsaufwand nicht negierbar
- Implementierungsaufwand relativ unabhängig von Lösung, relativ unabhängig davon, ob Lösung GPL/OS ist oder nicht
- viele IT-Teams sind zu klein um selbst voll zu Implementieren
- Dienstleister für Implementierung sinnvoll
- Netzwerkmonitoring/management via Nagios: Nagios als Auftragsvergabe zur Problembehebung durch externe Dienstleister