Open Source based Network Management

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 – 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

Strategien – Positionierung

cricket

Built on Tobi Oetiker's RRD TOOL

CUBiT

cricket healthmanager

ntop

CUBiT

Nagios

CUBiT HSP
• Inventory Portal

Vendor-Specific Management

hp invent · IBM · DELL · Bull · NetApp The evolution of storage.

CUBiT CUBiT CUBiT CUBiT CUBiT CUBiT

NotMan
Notification Manager

Agents:
• LogCheck
• ActivityCheck

Compound Check

Automated Operation
• unattended restart
• unattended problem solving

SNMPTrap
• HP
• CISCO
• Cyclades
• IBM
• Bull

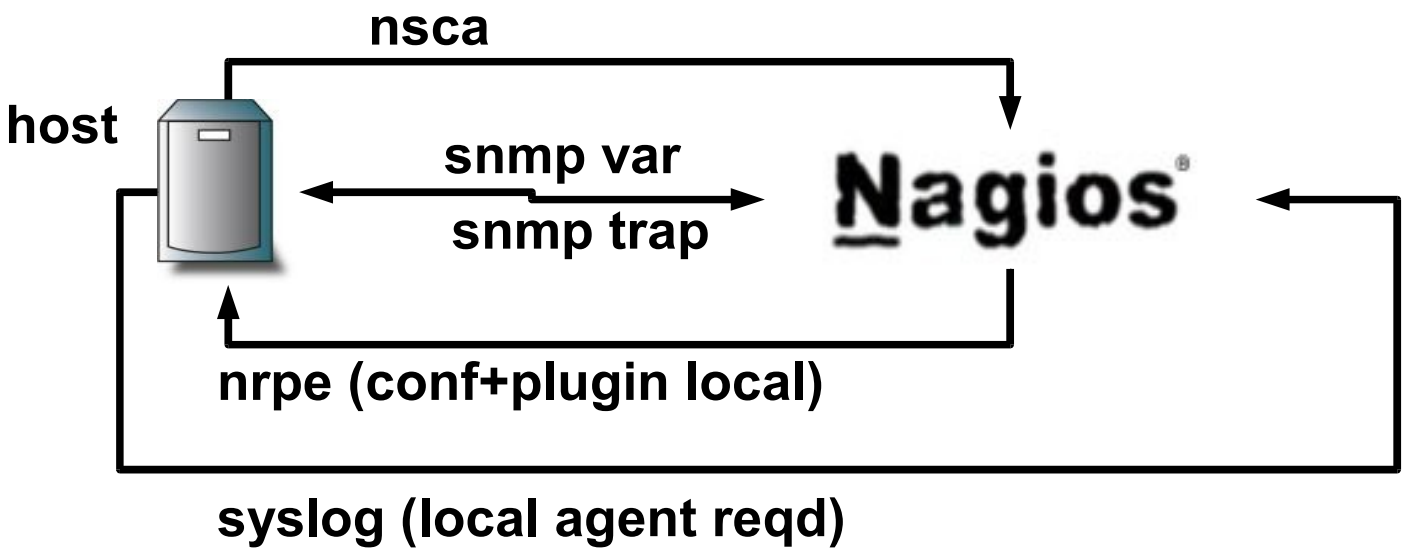
SLA Reporting Bal. Scorecard

PlugIns and Checking Strategies for
• Oracle, MySQL, MS SQL, Progress
• MS Exchange
•SAP
• SMB, CIFS, Samba
• Win NT, W2K, W2K3, MS ADC
• Process, custom Application checks
•Antivirus

Nagios 2.0

- Caching der CGI Objekte
- Servicegruppen
- Regexp
- schnellere Retention Data, Comments und Metadaten
- Export Interface für Export in NAMED PIPE (für Echtzeit Datenbank Interface)
- Höhere Leistung
- Host Checks auch passiv
- Automatische Wartungsfenster durch Abhängigkeiten

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

Komponenten: Nagios (2) Schnittstellen (2)

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

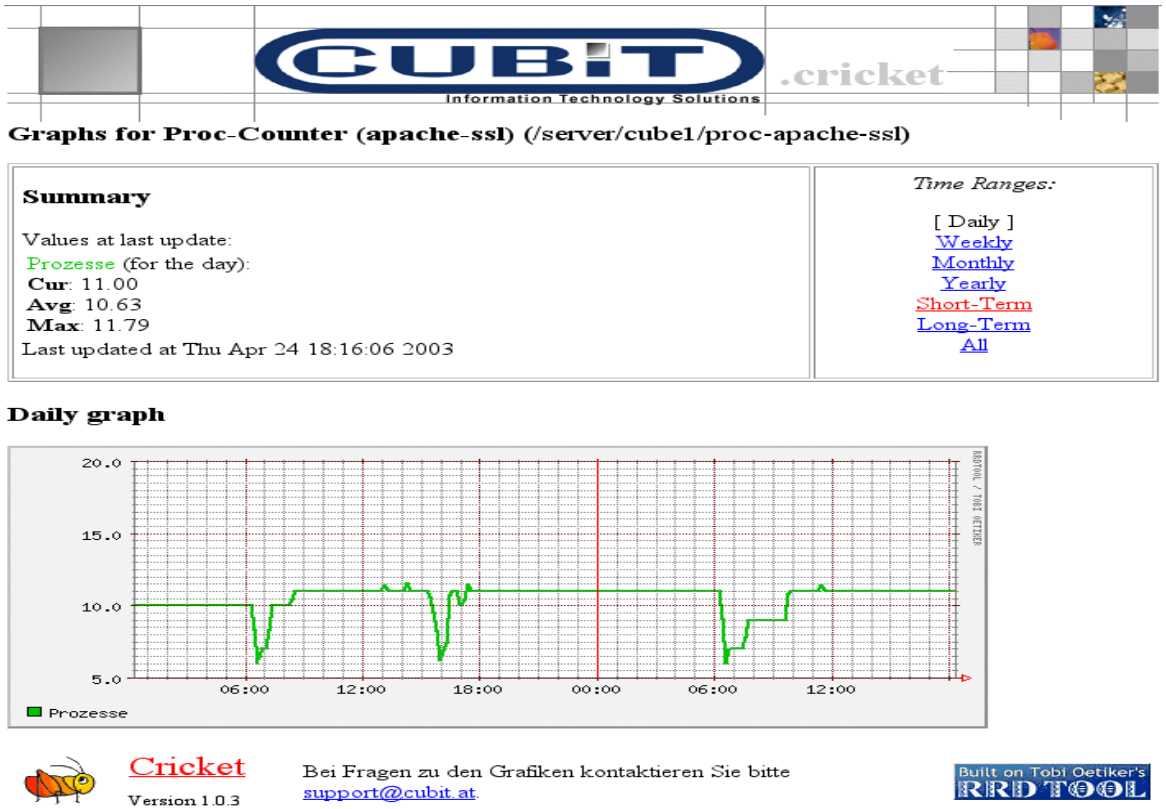
Nagios Features

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

Komponenten: Cricket



Komponenten: Cricket

Graphs for Overlay (/webserver/cubit-cluster)

Summary

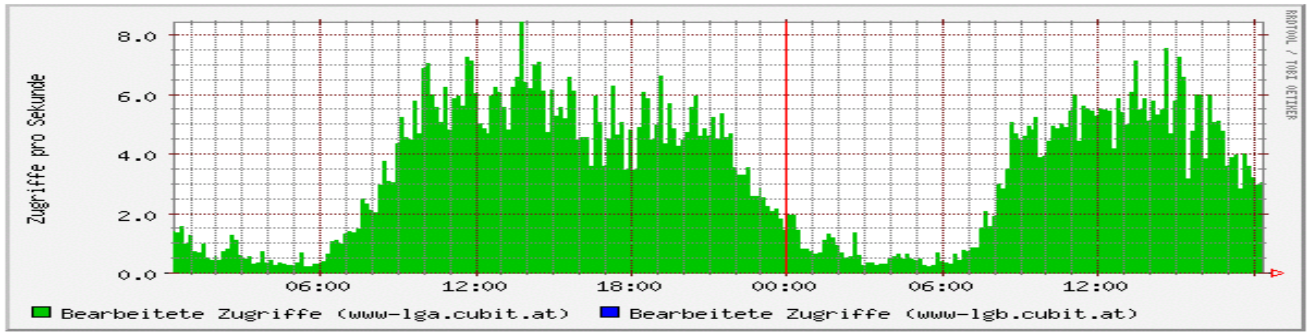
Values at last update for www-lga.cubit.at:
Bearbeitete Zugriffe (for the day):
Cur: 3.01 Zugriffe/s
Avg: 3.32 Zugriffe/s
Max: 8.66 Zugriffe/s
[?]
Last updated at Thu Apr 24 18:17:08 2003

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

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

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%
- autmat. Einhalten von Service-Profilen
- Event-Routing mit Notification Manager
- GUI zum Routen der Events
- Vertretungsfunktion, Schablonen, Berechtigungen

Addon-Tools: ntop, E2E

- ntop: Open Source Tool: Echtzeit Netzwerkscan
- 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

SLA Tool

- Ermitteln von Verfügbarkeiten
- Automatischer Check mit SLA
- Zieleinhaltung wird berichtet
- individuelle Servicezeiten pro Objekt
- Drill-Down Webreport
- Print-PDF
- nachträgliche Kosmetik an Kommentaren und Daten um Klarheit zu verschaffen
- Web based Reporting Tool
- Trend-Analyse und Massendaten

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)

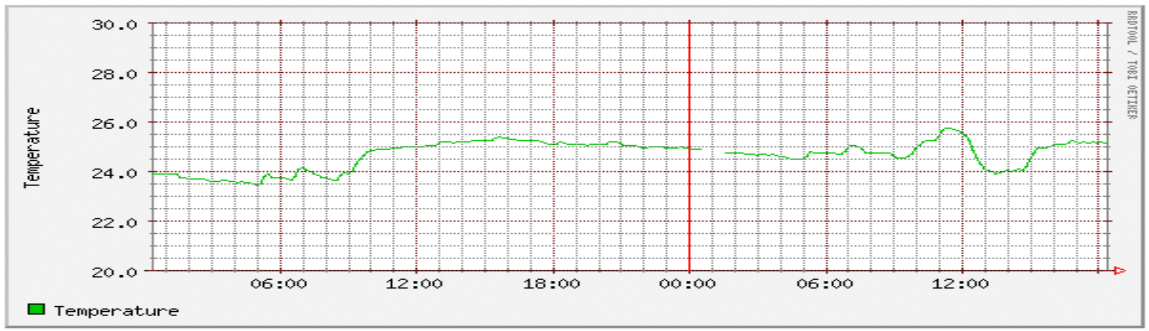
Summary

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
- Reporting via Nagios: Report der Produktionszahlen via Nagios Infrastruktur
- Konfigurationsprüfung via Nagios

Vergleich kommerzielle Systeme

- komplex genug
- keine Hierachie, 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 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

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 PlugIns

- richtiger Nutzen erst mit spezifisch geschriebenen Plugins („Harry Potter Monitor“, LogIn-Check)
- 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 - sonstige

- 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
- **KEINE ANGST VOR PLUGINS!**
- Netzwerkmonitoring/management via Nagios: Nagios als Auftragsvergabe zur Problembehebung durch externe Dienstleister