Service- und Infrastrukturmanagement mit dem directINSIGHT:Director

CUBiT IT Solutions GmbH
Ing. Peter-Paul Witta

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

Einsatzziel

- 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
- Notifizierung und Eskalation
- Automatic response („self-repairing“)
- Compound Checks
- Statistiken: SLA-Auswertung und Korrelation
- Umbrella-System
- Monitoring-Netzwerk

Probleme von NAGIOS

- Nicht nur NAGIOS: „... basierten OpenSource Monitoring Systemen“
- manuell konfigurierte getrennte Systeme
- Aufwendiges Change Management
- Kein RBAC; Authorization schwierig
- Konfiguration komplex
- Ungeschliffenes Usermanagement
- Viele getrennt administrierbare OpenSource Tools notwendig und eingesetzt
- Nicht „aus einem Guss“
- Change Management und Interoperabilität oftmals schwierig
- Mehrfache Objektanlage notwendig

directINSIGHT:Director

- Appliance: keine Installation notwendig
- Einheitliches Interface
- Komplett webbasiert
- Nutzbare Default Konfigurationen und Default Werte
- RBAC ermöglicht teambasierte Administration mit delegierbaren Rechten
- Hohe Leistung: >5000 Services, >1000 Hosts in der kleinsten Appliance
- Keine Kompatibilitäts-Issues mit vorhandener Software
- Single Point of Administration: einmalige Objektanlage und -Wartung
- Import von Excel-Listen zur Datenbefüllung
- Volle NetApp Abbildung!

directINSIGHT:Director

NetApp Go further, faster · BROCADE · vmware · ORACLE

DTM webbased Manager

Plugins NetApp | Plugins Brocade/SAN | Plugins LAN | Plugins VMware | Plugins Oracle | Plugins App Check | Plugins Windows Exchange SQL Server

Alerting Tactical Monitoring

Nagios Middleware

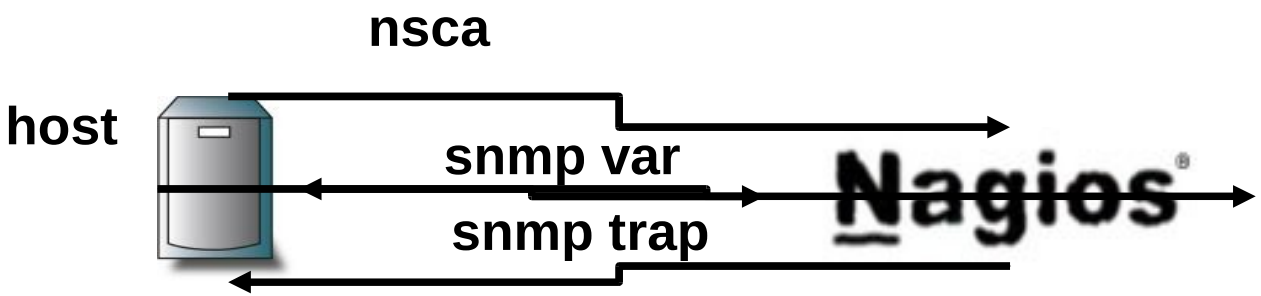
HSP Repository

Notman Alerting Services | Automatic Response Systems | Compound Checks | SLA Reporting | Messwert Analyse | Messwert SNMP | SNMP Traps

Komponenten: RRD

- Speicherung von Messwerten mit minimaler Speicherplatznutzung
- Abnehmen der Auflösung in der Vergangenheit
- Messwerte werden soweit möglich gleich mit NAGIOS erfasst
- Alternativ Messwerterfassung per SNMP oder anders
- Echtzeiterfassung notwendig!
- dynamische Schwellwert – Monitore: Aktionstrigger bei Schwellwert-Änderung

Monitoring Schnittstellen, Protokolle



nrpe (conf+plugin local)

syslog (local agent reqd)

- 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
- 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: RRD

- Speicherung von Messwerten mit minimaler Speicherplatznutzung
- Abnehmen der Auflösung in der Vergangenheit
- Messwerte werden soweit möglich gleich mit NAGIOS erfasst
- Alternativ Messwerterfassung per SNMP oder anders
- Echtzeiterfassung notwendig!
- dynamische Schwellwert – Monitore: Aktionstrigger bei Schwellwert-Änderung

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
- DTM PlugIns werden direkt via HSP konfiguriert

Komponenten: dID Plugins

- Einzeln oder im Paket lizensierbar
- Sinnvolle Default Werte vorhanden
- Individuelle Menükomponente samt PlugIn
- Vorkonfiguriert; eingespielt in < 5 Minuten
- Schnell und sicher aktiviert
- „custom“ PlugIn zu Integration beliebiger Nagios PlugIns vorhanden (im Expert-Mode)

PlugIns: 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

PlugIns: VMWare

- 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

PlugIns: Storageumgebungen

- In virtualisierten Speicherumgebungen ist einiges anders
  - nur Storageserver kennt Belegung (Auslastung)
  - Clone und Snapshots verfälschen Belegung aus Hostsicht
  - In den Storageserver 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

PlugIns: SAN

- Pfadanalyse
  - vom Host aus
  - Nutzung spezifischer Software ([Secure|Power]Path)
  - wie sieht der Host verschiedene Targets
  - welche Pfade sieht er
  - benutzt er die richtigen Pfade 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 Config-Änderungen

PlugIns NetApp

- Füllgrade
- Event-Monitoring mit ASUP
- Einbindung von SNMP ab OnTAP 7.3
- Nutzung von ONTAPI
- SnapMirror Monitoring
- Disk; Aggr; Vol Integrität
- Disk Utilization und andere Messwerte
- MetroCluster Monitoring inkl. Backend Brocade Switches
  - Monitoring von Fehlercountern
  - Monitoring aller Brocade Werte
- Einbindung in Korrellation und SLA Auswertung

PlugIns: LAN

- 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

- 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 G4

- 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
- SLA Daten

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) G4“

- 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

Automatic Response

- 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
- Automatisches Re-Provisioning von knappen Ressourcen
  - Vmware shares
  - Storage Space

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
- Balanced Scorecard
- Trend-Analyse und Massendaten

Specials: Mix It Right

- 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
- kein 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
- Livedemo heute vorhanden