DECOIT

CeBIT 2011

CeBIT
cebit.com
HANNOVER
1.–5. MÄRZ 2011

Zentrales Monitoring von aktiven Netzkomponenten am Beispiel Icinga (Nagios)

Prof. Dr.-Ing. Kai-Oliver Detken
Geschäftsführer
DECOIT GmbH
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

Anforderung an Monitoring-Systeme

- Im Betrieb der meisten Netzwerke wird aus historischen Gründen ein reaktives Netzwerkmanagement umgesetzt
- Dies bedeutet, dass der Anwender einen Fehler im Betrieb bemerkt und den Administrator über den Fehler informiert
- Dieser hat dann die Aufgabe aus der Fehlermeldung des Anwenders die Fehlerursache zu ermitteln und danach umgehend den Fehler zu beheben. Analoges gilt für Überlastverhalten.
- Für den IT-Administrator ergeben sich damit mehrere Notwendigkeiten:
  - Er muss über den Zustand der betriebsrelevanten Dienste auf dem Laufenden sein
  - Er muss fundierte Aussagen über die Nutzung der Systeme machen können
  - Er muss die Trends in der Nutzung dokumentieren

Pro-aktives Netzmonitoring

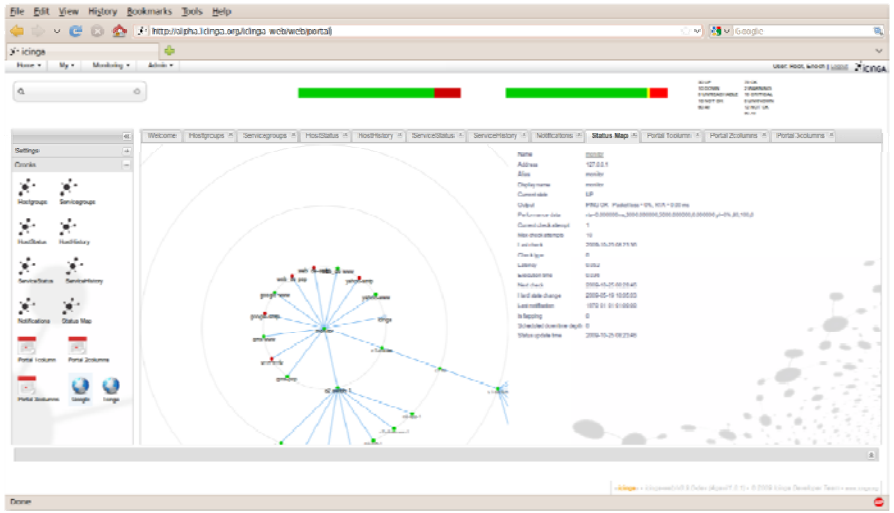
- Ein pro-aktives Netzmonitoring meldet Systemausfälle, bevor ein Anwender dieses bemerkt
- Der IT-Administrator hat bessere Pflegemöglichkeiten, da er den Zustand des Gesamtnetzes (Server, Clients, IP-Telefone, Netzwerk) kennt und darauf Einfluss nehmen kann
- Zusätzlich wird eine aktuelle Dokumentation ermöglicht, die interaktiv auf dem neusten Stand gehalten wird
- Langzeitstatistiken helfen auch nachträgliche Fehler analysieren zu können
- Auch an Feiertagen und Wochenende werden alle aktiven Systeme überwacht
- Fast beliebige Systeme lassen sich in ein solches Monitoring einbetten

Umfang von Icinga (Nagios)

- Icinga (Nagios) ist eine freie, modular aufgebaute Open-Source-basierte Monitoring-Software
- Mit Icinga lassen sich eine Vielzahl von Systemen überwachen: z.B. Linux, Windows, Netzwerkkomponenten usw.
- Lauffähig ist Icinga auf allen Linux-Plattformen
- Icinga ist ein Fork der Nagios-Lösung, um schneller und effektiver Neuerungen entwickeln und einbetten zu können; es ist vollständig kompatibel zu Nagios
- Die DECOIT GmbH hat die Open-Source-Software Nagios analysiert und über Icinga mit zusätzlichen Eskalationsfunktionen erweitert
- Bestandteile der Monitoring-Software sind:
  - Der Nagios-Kern
  - Plug-In-Systeme
  - Web-Interface
  - Benachrichtigungssystem

Auswahl Icinga/Nagios (1)

- Icinga (Nagios) bietet hohe Flexibilität durch zahlreiche Plug-Ins, die Checks durchführen und die Möglichkeit bieten diese selbst zu programmieren
- Überprüfungs-, Benachrichtigungsintervalle und verzögerte Benachrichtigungen lassen sich frei definieren
- Benachrichtigungsgruppen können angelegt werden
- Berücksichtigung der Abhängigkeiten zwischen den einzelnen Hosts
- Icinga (Nagios) bietet zudem ein Eskalationsmanagement



Auswahl Icinga/Nagios (2)

- Konsolidierte Bewertung von einzelnen Alarmen mittels Plug-Ins ist möglich
- Icinga erlaubt die Überwachung von Log-Dateien nach regulären Ausdrücken
- Möglichkeit ein verteiltes Monitoring durchzuführen
- Hochverfügbarkeit kann realisiert werden
- Add-Ons für weitreichende Visualisierung von Zuständen und Verarbeitung von Performancedaten
- Icinga (Nagios) ist Open Source (GPL)

DECOIT

Überwachung

- Icinga (Nagios) führt die Überwachung mittels Plug-Ins durch und unterscheidet dabei zwischen Host- und Service-Checks:
  - Host-Check
    - Testet einen Rechner auf Erreichbarkeit (ping)
  - Service-Check
    - Prüft gezielt einzelne Netzwerkdienste ab: z.B. HTTP, SMTP, DNS usw., laufende Prozesse, CPU-Last oder Logfiles
- Zustände im Icinga (Nagios) sind farbcodiert:
  - Services-Zustände:
    - OK (grün), WARNING (gelb), CRITICAL (rot), UNKNOWN (orange)
  - Hosts-Zustände:
    - UP (grün), DOWN (rot), UNREACHABLE (rot)

DECOIT

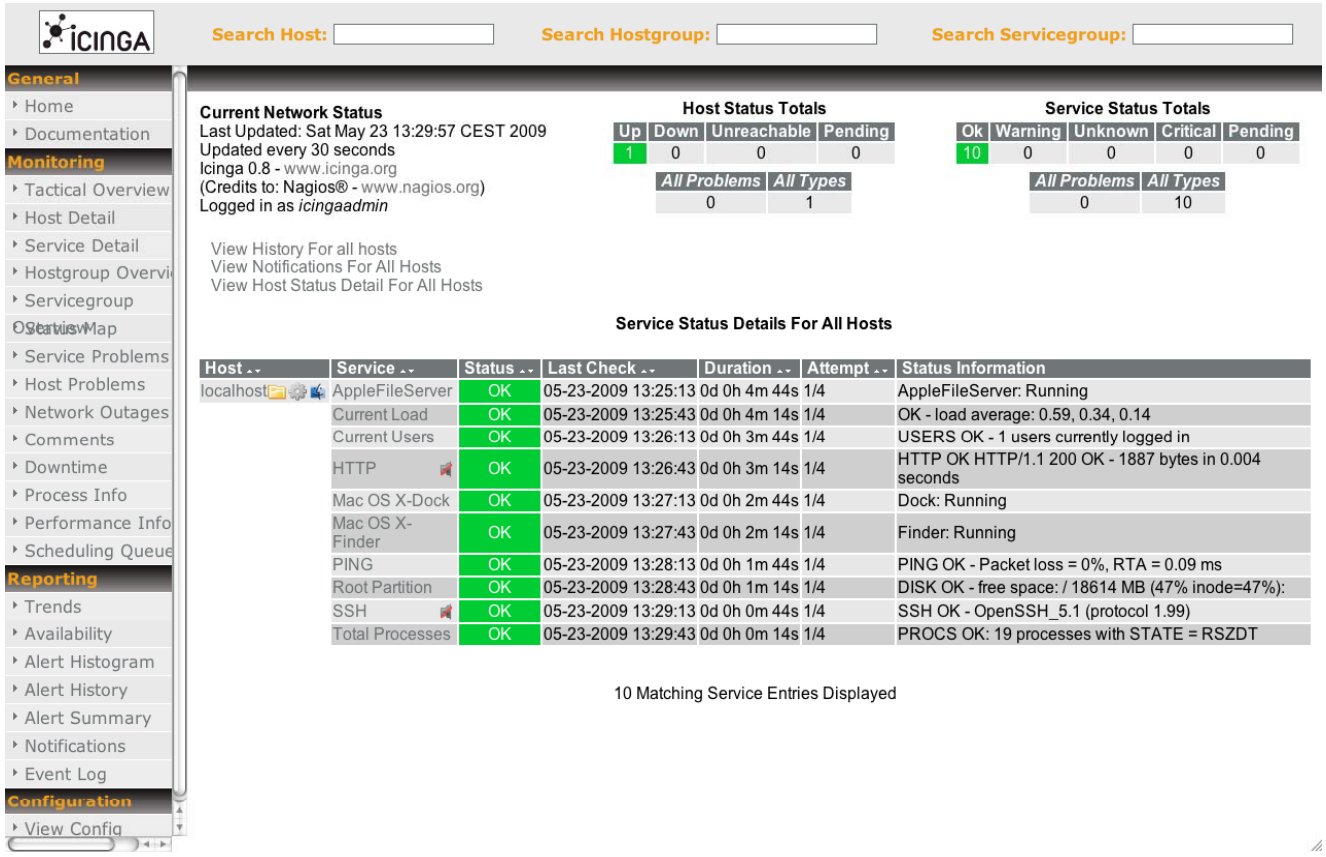
Plug-ins

- Ein Plug-in ist ein Programm (ein Shell- oder Perl-Skript), das einen der vier Zustände OK, WARNING, CRITICAL oder UNKNOWN liefert
- Damit kann Icinga (Nagios) alles prüfen, was sich elektronisch messen oder zählen lässt:
  - Temperatur und Luftfeuchtigkeit im Serverraum
  - Anwesenheit von Personen in einem Raum
  - etc.
- Icinga (Nagios) liefert bereits standardmäßig viele Plug-ins für die wichtigsten Anwendungszwecke mit
- Viele weitere Plug-ins stellt die Nagios-Austauschplattform Nagios-Exchange im Internet bereit
- Eigene Plug-ins lassen sich selbst entwickeln und hinzufügen

Web-Interface

- Web-Interface dient zur übersichtlichen grafischen Darstellung der Überwachungsergebnisse
- Bietet auch die Möglichkeiten für ein Gerät:
  - Überwachung ein- und auszuschalten
  - Benachrichtigungen an- und abzustellen
  - Acknowledges zu setzen
  - Kommentare zu hinterlassen
  - Wartezeiten zu planen
- Erlaubt einen Zugriff auf Logs und Reports über alle vergangene Ereignisse in einem gewählten Zeitintervall

Web-Interface – Service Detail

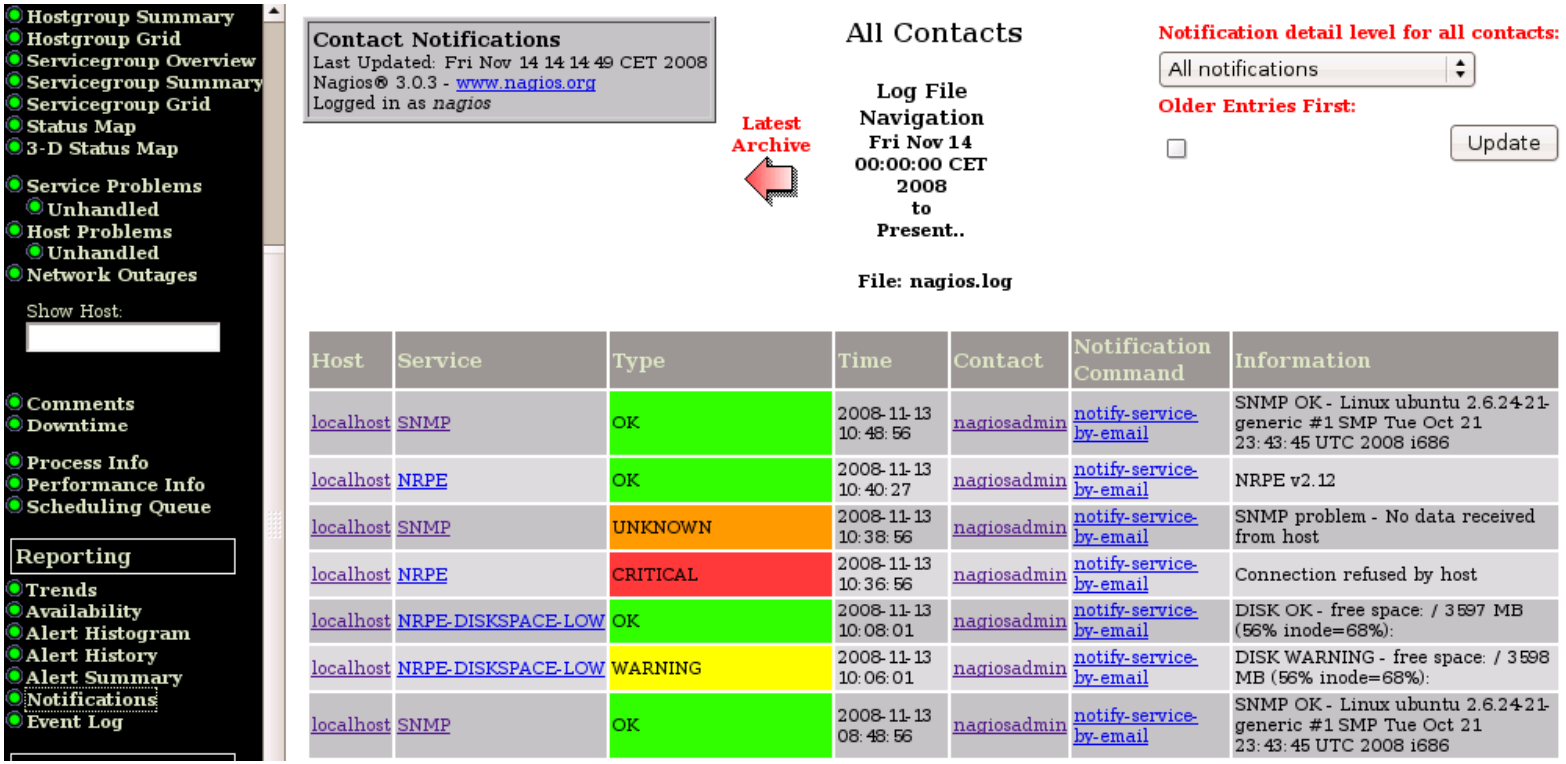


DECOIT

Eskalation und Benachrichtigungen

- Nagios besitzt ein ausgefeiltes Benachrichtigungssystem
- Es lässt sich einstellen wann welche Personengruppen über welche Zustände und Ereignisse informiert werden
- Beim Ausfall oder bei der Über-/Unterschreitung von Grenzwerten, bietet Nagios verschiedene Formen von Benachrichtigungen an: E-Mail, SMS, Anruf, Pager, Instant Messaging (Jabber, ICQ), SNMP-Traps etc.
- Nachrichten lassen sich zu beliebig festgelegten Zeiträumen versenden:
  - Kombinationen von Zeitraum-, Wochentag- und Uhrzeit-Angaben (auch einzelne Kalendertage)
  - z.B. nur E-Mail an Administratoren zur Arbeitszeit und sonst SMS
- Die DECOIT GmbH hat die vorhandenen Eskalationsstufen bei Icinga erweitert
  - Die Erweiterung ermöglicht es, Eskalationsstufen zusätzlich mit Bedingungen zu belegen
  - Nur wenn die Bedingungen zutreffen, wird eine Eskalationsstufe eskaliert
  - Somit ist es nun möglich, in Abhängigkeit des Zustands eines Dienstes, unterschiedliche Kontaktpersonen von Problemen zu unterrichten

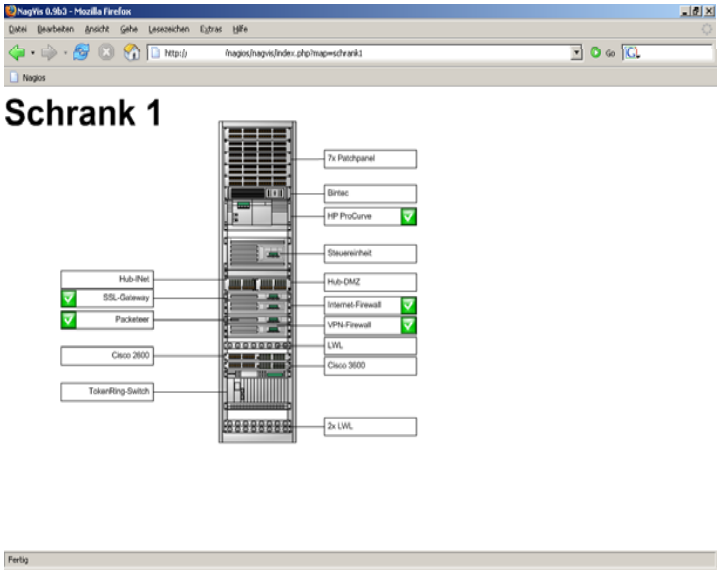
Benachrichtigungen

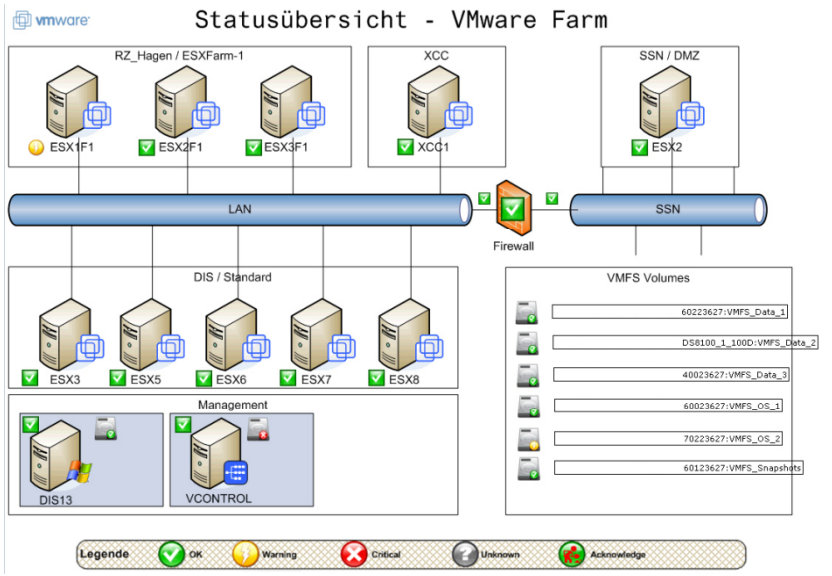


Host	Service	Type	Time	Contact	Notification Command	Information
localhost	SNMP	OK	2008-11-13 10:48:56	nagiosadmin	notify-service-by-email	SNMP OK - Linux ubuntu 2.6.24-21-generic #1 SMP Tue Oct 21 23:43:45 UTC 2008 i686
localhost	NRPE	OK	2008-11-13 10:40:27	nagiosadmin	notify-service-by-email	NRPE v2.12
localhost	SNMP	UNKNOWN	2008-11-13 10:38:56	nagiosadmin	notify-service-by-email	SNMP problem - No data received from host
localhost	NRPE	CRITICAL	2008-11-13 10:36:56	nagiosadmin	notify-service-by-email	Connection refused by host
localhost	NRPE-DISKSPACE-LOW	OK	2008-11-13 10:08:01	nagiosadmin	notify-service-by-email	DISK OK - free space: / 3597 MB (56% inode=68%):
localhost	NRPE-DISKSPACE-LOW	WARNING	2008-11-13 10:06:01	nagiosadmin	notify-service-by-email	DISK WARNING - free space: / 3598 MB (56% inode=68%):
localhost	SNMP	OK	2008-11-13 08:48:56	nagiosadmin	notify-service-by-email	SNMP OK - Linux ubuntu 2.6.24-21-generic #1 SMP Tue Oct 21 23:43:45 UTC 2008 i686

Add-On NagVis

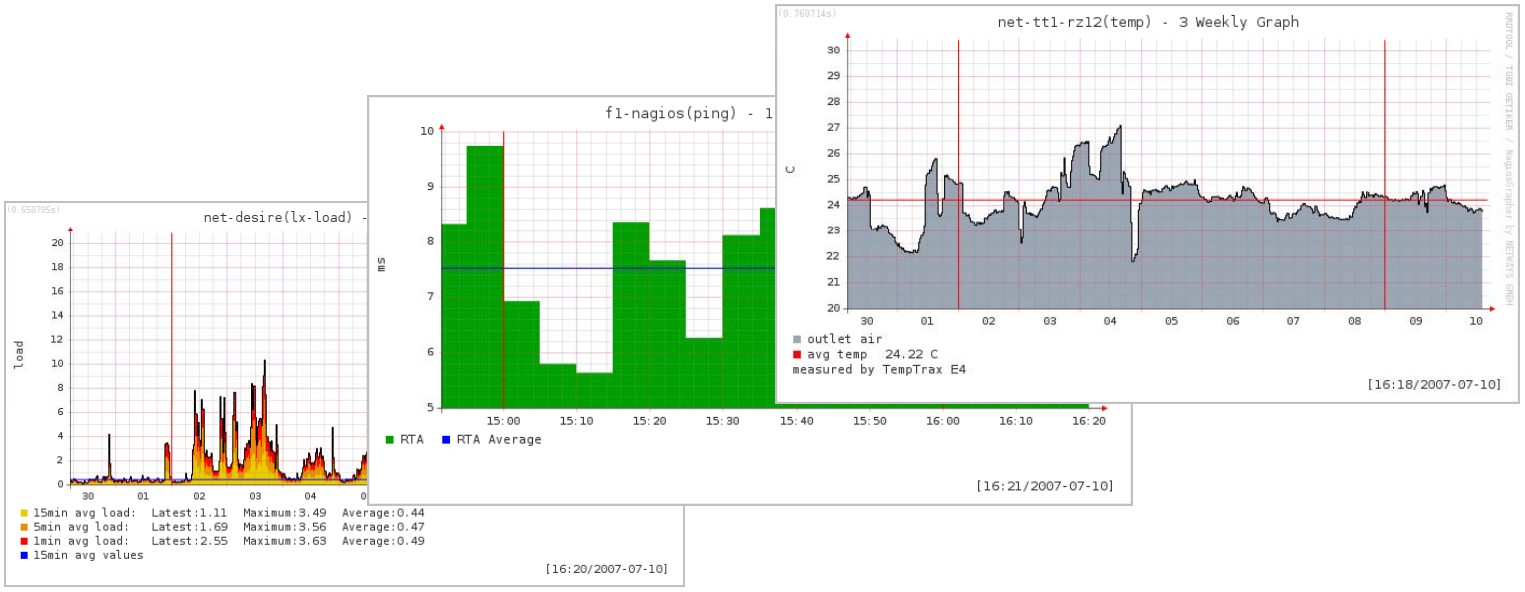
- NagVis ist ein Add-On zu Nagios, um Host- und Service-Zustände zu visualisieren
- NagVis untersteht der GNU General Public License (GPL)





Add-On NagiosGrapher

- NagiosGrapher ist ein Add-On für die Generierung von Grafiken und Performancecharts aus den Rückgabewerten der Überwachung
- Der NagiosGrapher untersteht der GNU General Public License (GPL)

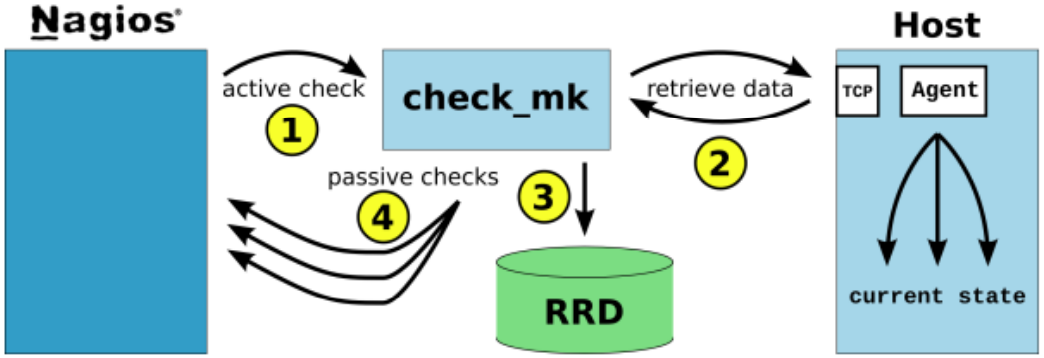


DECOIT

Check_MK

- Entwickeltes Add-On von Mathias Kettner
- Lizensiert unter GNU GPL Version 2
- Verbesserte Performance bei großer Anzahl von Checks
  - Durch Sammeln der Infos vom Host auf dem Host
  - Einfachere Konfiguration durch automatische Inventur
  - Nur eingeschränkt nutzbar, da nicht alles mit Check_MK abgedeckt werden kann
- Clients sind vorhanden für
  - Linux
  - Solaris
  - Windows

Funktionsweise von Check_MK



1. Für jeden Host triggert Icinga einen aktiven check per Check-Intervall. Dieser Check ruft check_mk als Plug-in auf.
2. Check_mk verbindet sich zum Host via TCP. Der check_mk_agent auf dem Host empfängt alle relevanten Daten und sendet diese in einem Stück als ASCII-Text zurück.
3. Check_mk filtert die Performance-Daten heraus und schreibt sie direkt in die Round Robin Datenbank.
4. Check_mk nimmt die relevanten Daten, vergleicht sie mit den warning/critical levels und überträgt alle Ergebnisse des Hosts als passive Prüfungen.

Icinga/Nagios-Funktionen

- Überwachen von Windows-, Linux-PCs, Druckern, Router/Switch/Hubs, Services wie HTTP, FTP, Webserver, Datenbanken, USV, SSH, SMTP, POP3, IMAP, NNTP, PING
- SNMP-Unterstützung von SNMPv1, SNMPv2c und SNMPv3
- Flexibel durch zahlreiche Plug-ins und die Möglichkeit diese selbst zu programmieren
- Eingebautes Eskalationsmanagement
- Quittierungen (sog. Acknowledgement) können verwendet werden
- Verteiltes Monitoring wird ermöglicht
- Überprüfungs-, Benachrichtigungsintervalle und verzögerte Benachrichtigungen können frei definiert werden
- Verfügbarkeitsreports können als CVS-Dateien exportiert werden
- Für Benachrichtigungen können Gruppen angelegt werden
- Eine konsolidierte Bewertung von einzelnen Alarmen mittels Plug-Ins ist möglich
- Reine Open Source (GPL-) Lizenz beinhaltet keine Lizenzkosten und freie Erweiterungsmöglichkeiten

Fazit

- Es gibt viele verschiedene Möglichkeiten, um aktives Netzwerk- und Servermonitoring zu betreiben
- Die DECOIT GmbH setzt dabei auf die Kombination verschiedener Systemlösungen, um das Beste aus verschiedenen Welten nutzen zu können
- Icinga spielt dabei eine zentrale Rolle, da es erweiterbar ist und dadurch auf neue Anforderungen anpassbar ist
- Die Visualisierung des Netzes, seiner Server und Daten bekommt einer immer höheren Bedeutung, da auf der einen Seite die Verfügbarkeit ansteigt und auf der anderen Seite Virtualisierungstechniken das Netz immer unübersichtlicher werden lassen
- Neben der Verfügbarkeit profitiert auch die IT-Sicherheit vom Monitoring

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de

Consultancy & Internet Technologies