



Linux Admin Treff

17.12.2003

Systemüberwachung und -information mit SNMP



Go Back

Page 1 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Name: Daniel van Ross

Mail: dross@uni-math.gwdg.de

Web: www.uni-math.gwdg.de/dross

ehem. stud. Hilfskraft am Mathematischen Institut
Bachelorarbeit über SNMP-basiertes Überwachungssystem



Go Back

Page 2 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Was ist SNMP?

- Simple Network Management Protocol
- UDP basiert (Ports 161 und 162)
- verteilte Management Architektur
- teilt das Management Problem in zwei Teile:
 - Definition der verfügbaren Daten
 - Datenaustausch zwischen Client und Server



Go Back

Page 3 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Begriffe

- Anwendungen auf den zu überwachenden Geräten (Clients) heissen **Agenten**
- Der Server zur Überwachung heisst **Management Host** oder **Management Station**

Kommunikationswege

- Management Host kann Daten der Agenten abfragen - **poll**
- Agent kann Meldungen an Management Host senden - **trap**



Go Back

Page 4 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Datendefinitionen

- Ein Agent **muss** bestimmte Zustands-/ Kontrolldaten vorhalten
- Definitionen stehen in **Management Information Bases (MIBs)**
- MIBs definieren Variablen, deren Typ und Zugriffsrechte



Go Back

Page 5 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

SNMP Namensraum

- großzügig und universell erweiterbar
- baumartig strukturiert (Object Identifier Namespace)
- SMI (Structure of Management Information) definiert wie die Variablen innerhalb der MIBs festgelegt werden
- der für SNMP interessante Teil des SMI Baumes beginnt mit OID 1.3.6.1 (iso.org.internet.dod)
- Zahlreiche Tools zur Visualisierung von MIBs, z.B. Cheops, TKined, MBrowser



Go Back

Page 6 of 22

Full Screen

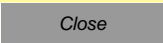
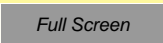
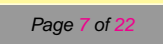
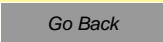
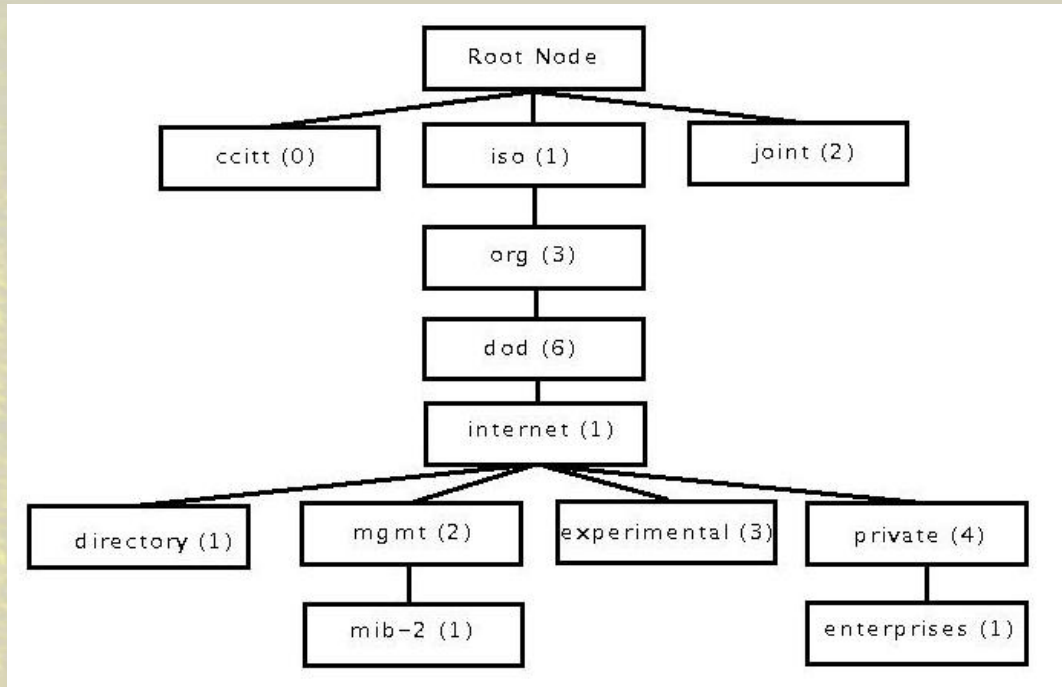
Close



SNMP Namensraum

Linux Admin Treff

17.12.2003





Linux Admin Treff

17.12.2003

gängige MIBs

system	überwachtes Gerät: Standort, Software, Uptime, ...
interfaces	reale und virtuelle Interfaces
ip	IP-Daten: Routingtabelle, Paketzähler, ...
tcp	TCP-Daten: bestehende Verbindungen, ...
udp	UDP-Daten: offene Ports, ...
snmp	Statistiken und Zähler des SNMP Agenten
host	Daten klassischer Workstations: CPU, Speicher, ...



Go Back

Page 8 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

SNMP Agenten

- jede Netzwerkkomponente, die sich mit SNMP verwalten lässt verfügt über einen SNMP Agenten
- meist Softwarelösung in den Endgeräten
- Implementation in aktiven Komponenten meist hersteller-spezifisch
- für Linux Workstations diverse Implementationen in fast jeder Sprache
- Funktionalität unterscheidet sich meist in den unterstützten MIBs



Go Back

Page 9 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Kommunikationscode der Agenten

fünf grundlegende Operationen

- **get-request:**
Ermittle den Wert einer bestimmten Variable
- **get-next-request:**
Ermittle den Wert der nächsten Variable ohne ihren genauen Namen zu kennen
- **response:**
Antwort auf o.g. requests
- **set-request:**
Speichere einen bestimmten Wert in einer Variable
- **trap:**
Antwort ausgelöst durch einen Event-Trigger



Go Back

Page 10 of 22

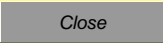
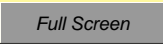
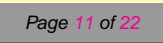
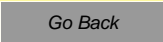
Full Screen

Close



SNMP Versionen

- Version 1
 - Grundbefehle
 - Community Strings zur Authentifizierung
- Version 2 (experimental)
 - Erweiterung der Befehle um get-bulk, notification, inform, report
 - Version 2c: community based
 - Version 2u: user based
- Version 3 (draft)
 - user based und verschlüsselt





Linux Admin Treff

17.12.2003

SNMP unter Linux

- im Folgenden wird NetSNMP betrachtet
- entwickelt an der University of California in Davis
- steht unter GPL
- www.netsnmp.org
- wird oft noch unter dem Namen ucd-snmp geführt



Go Back

Page 12 of 22

Full Screen

Close



Kommandos zur Datenbeschaffung

- Voraussetzungen:
 - Community String zur Authentifizierung
 - Agent muss Management Station akzeptieren
- Syntax:
snmpget target-host community Variable
- weitere Programme aus dem Net-SNMP Paket:
snmpgetnext, snmpwalk, snmpset, snmptranslate, snmpdf,
snmpnetstat, snmpstatus



Go Back

Page 13 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Eigenheiten von NetSNMP

- eigener Bereich im Enterprises Unterbaum 1.3.6.1.4.1.2021
- z.B. Prozesstabelle unter ...2021.2
Konfiguration über “proc” in der snmpd.conf des Agenten
- z.B. eigene Programme unter ...2021.5x
Konfiguration über “exec” in der snmpd.conf



Go Back

Page 14 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Überwachungssoftware

zumindest für den Privatgebrauch frei:

- Big Brother: www.bb4.com
- Big Sister: bigsisiter.graef.com
- Nagios (früher NetSaint) www.nagios.org

kommerzielle Systeme:

- HP OpenView www.hp.com/openview
- IBM Tivoli www.tivoli.com



Go Back

Page 15 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Überwachungssoftware

Big Brother / Big Sister

- + einfache Konfiguration
- + viele Zusatzmodule

- proprietäres Protokoll
- erfordert Client auf Zielrechner

Nagios

- + WAP-Interface
- + differenzierte Überwachung
- + Netzwerk-Map

- aufwendige Konfiguration



Go Back

Page 16 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

gewünschte Funktionalität

- Keine proprietären Protokolle
- Lokalisierung der Endgeräte (Abfrage der Switches)
- einfache Erweiterbarkeit
- Sicherung der Zustandsdaten in einer Datenbank



Go Back

Page 17 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

reale Tests vs. SNMP

- Netzwerkdienste: Prozess läuft, aber tut er, was er soll



Go Back

Page 18 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

(noch) fehlende Funktionalität

- Benachrichtigungsmöglichkeit
- Frontend zum Pflegen der Daten



Go Back

Page 19 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

nicht behandelte SNMP Funktionalität

- AgentX - Erweiterungen
- Management Funktionen



Go Back

Page 20 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Ressourcen

MIBs

- <http://www.ibr.cs.tu-bs.de/cgi-bin/sbrowser.cgi>
- <http://www.wtcs.org/snmp4tpc/mibs.htm>
- <http://www.mibdepot.com>
- <http://www.oidview.com/mibs/detail.html>
- http://www.somix.com/support/mib_resources.php

Sonstiges

- <http://www.phenoelit.de/dpl/dpl.html>



Go Back

Page 21 of 22

Full Screen

Close



Linux Admin Treff

17.12.2003

Literatur

SNMP allgemein

- Mauro und Schmidt, Essential SNMP, O'Reilly

Big Brother

- Fuckerieter, Großer Bruder, Linux Magazin 09/2002

Big Sister

- Aeby und Fritsch, Große Schwester, Linux Magazin 12/2003

NetSaint / Nagios

- von Suchodoletz, Der Netzheilige, Linux Magazin 09/2002
- Ruzicka, Alles im Blick, Linux Magazin 03/2003



Go Back

Page 22 of 22

Full Screen

Close