

14 Netzwerk- überwachung und -steuerung



- Überblick
- SNMP – Simple Network Management Protocol
- Datendefinitionen
- SNMP Implementierungen unter Linux
- Kommandos zur Datenbeschaffung
- Konfiguration des Net-SNMP Agenten
- Überwachung weiterer Parameter
- MRTG

14.1 Überblick



- immer größere Netze bieten immer mehr Dienste:
 - höherer Administrationsaufwand
 - höherer Überwachungsaufwand
- Entwicklung von SNMP

14.2 SNMP (1)



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

14.2 SNMP (2)



- Anwendungen auf den zu überwachenden Endgeräten (Clients) heissen Agenten
- Der Server zur Überwachung heisst Management Station/Host
- Zwei Möglichkeiten des Informationsaustausches:
 - Der Management Host kann Daten vom Agenten abfragen (poll)
 - Der Agent kann Meldungen an den Management Host senden (trap)

14.3 Datendefinitionen (1)



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

14.3 Datendefinitionen (2)



→ gängige MIBs

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

14.3.1 Namensraum und MIBs



- 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:
 - Cheops, TKined, MBrowser

14.3.2 SNMP-Agenten



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

14.3.3 Kommunikationscode der Agenten



- 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
 - get-bulk-request: Ermittle einen Block von Variablen
 - response: Antwort auf o.g. requests
 - set-request: Speichere einen bestimmten Wert in einer Variable
 - trap: Antwort auslöst durch einen Event-Trigger

14.4 Implementierungen



- Diverse für Linux, aber im folgenden wird Net-SNMP betrachtet
- entwickelt an der University of California in Davis
- steht unter GPL
- www.netsnmp.org
- wird oft noch unter dem Namen ucd-snmp geführt

14.5 Kommandos zur Datenbeschaffung



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

14.6 NetSNMP Agentenkonfig.



- /etc/ucdsnmpd.conf
- Zugangsberechtigung
- Authentifizierung
- mehrere Access Regeln möglich:
 - Regeln bestehen aus MIBs und Zugriffsmodi

14.6.2 „Enterprise“-Erweiterungen



- “Enterprises” - Unterbaum 1.3.6.1.4.1
- UCD-SNMP-MIB OID 2021
- Prozesstabelle unter OID 2
- Konfiguration mit Schlüsselwort „proc“ in der `ucdsnmpd.conf`
 - Angabe des Prozessnames und der minimal und maximal erlaubten Instanzen

```
proc ypbind 4 1
```

14.6.3 Externe Scripte



- netsnmp erlaubt die Ausführung eigener Programme
- Ergebnisse in enterprises.ucdavis Unterbaum OID 8
- Konfiguration durch das Schlüsselwort "exec"

```
#      oid          name      script      arguments
exec  .1.3.6.1.4.1.2021.51  myscript  /tmp/myscript
```

Rückgabe einzeilig mit max. 255 Zeichen

14.7 Überwachung weiterer Parameter



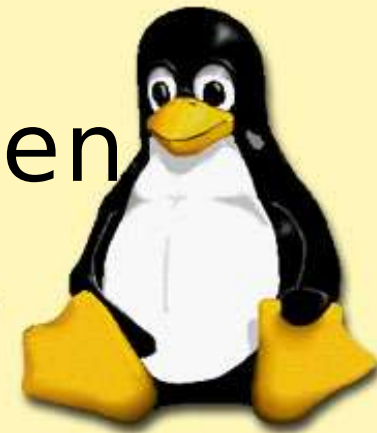
- Der enterprise.ucdavis Unterbaum erlaubt die Überwachung einiger weiterer Parameter wie Systemauslastung und Plattenbelegung und auch Programme mit mehrzeiliger Ausgabe können angewendet werden.
- So haben viele Hersteller von Netzwerkkomponenten ihren SNMP Agent um enterprise Funktionalitäten erweitert.
- es gibt auch gemeinsame Entwicklungen von Herstellern:
z.B: Printer MIB die inzwischen zum Standard geworden sind.

14.8 MRTG zur Zeitreihenanzeige



- MRTG: Multi Router Traffic Grapher
- Visualisierung der Belastung bestimmter Einheiten
(z.B. Netztraffic, Userzahl, Load ...)
- Perl-Skript zur Abfrage der SNMP Daten und Erzeugung von Grafiken
- <http://www.mrtg.org>
- Bestandteil vieler Distributionen

14.9 abschließende Anmerkungen



- SNMP ist einfach und flexibel
- das einzig plattform unabhängige Protokoll zur Netzwerküberwachung
- Nachteil ist das Sicherheitskonzept in den Versionen 1 und 2
- Vorsicht beim Setzen von Variablen