Seminarausarbeitung

zum Thema „**Hardwaredatenquellen**“

Seminar „Systemmonitoring unter Linux“

von Shvalova Marina

Betreuer: Michael Kuhn

Sommersemester 2010

Universität Hamburg

Wissenschaftliches Rechnen

Inhaltsverzeichnis

1 Einleitung

Im Rahmen dieser Arbeit werden die Lösungen zum Überwachen und Kontrolle von Hardwaredatenquellen vorgestellt. Temperatur, CPU-Leistung, Lüfterdreherzahlen usw. am eigenen Rechner zu beobachten hilft frühzeitig Hardware- und Softwareprobleme zu erkennen, Datenverluste zu vermeiden und Fehlersuche zu erleichtern.

1.1. Aufbau der Arbeit

In Hauptteil wird die allgemeine Information zu den Hardwaresensoren vorgestellt, dabei wird es etwas genauer auf die Beschreibung von System Management Bus eingegangen. Zur Einführung wird das Überwachungstool „LM-Sensors“ dargestellt. Im Abschnitt „S.M.A.R.T.“ gibt es kurzen Überblick auf unterschiedliche Festplattenanschlüsse, da nicht alle Festplatten S.M.A.R.T. unterstützen, und es wird ausführlicher Auslesen und Interpretieren von den S.M.A.R.T.-Werten , S.M.A.R.T.-Testfunktionen und die Tools, die diese Werte auslesen können, vorgestellt. Im Abschnitt „SNMP“ geht es um die Funktionsweise von SNMP, Management Information Base, wie die Daten abgespeichert werden und auch um die Sicherheitsprobleme bei den verschiedenen Versionen von SNMP.

Anschließend wird es kurz auf die Überwachungstools wie Ganglia und Nagios eingegangen, die im Vergleich zu LM-Sensors und S.M.A.R.T. für das Überwachen von den ganzen Rechnerpools eingesetzt werden.

2 Hauptteil

2.1 Hardwaresensoren allgemein

Mit Hilfe von Hardware-Sensors-Chips, die sich auf vielen Motherboards befinden, lassen sich die Werte wie Prozessordrehzahlen, Spannungen und Lüfterumdrehungen überwachen. Die Werte werden über die sogenannten Southbridge-Chipsätze des Matherboards von Herstellern wie Intel, ALI oder VIA über den SM-Bus (System Management Bus) und/oder den I^2C-Bus ausgelesen.

2.1.1 System Management Bus

System Management Bus ist ein Zweileiterbus, wurde von Intel 1995 definiert und basiert auf dem I^2C-Serienprotokoll von Philips. Er hilft den Zustand von Komponenten zu erkennen und Hardwareeinstellungen vorzunehmen.

Ein Gerät, das einen SMBus besitzt, kann Herstellerinformationen zur Verfügung stellen, die Modell-/Seriennummer ausgeben, unterschiedliche Arten von Fehlern melden, den Status des Energiesparmodus anzeigen, , einen Status zurückgeben oder Steuerparameter annehmen. Da die Nutzung des SM-Busses detaillierte Kenntnis der vorliegenden Hardware voraussetzt, ist er für den Benutzer oft weder konfigurierbar noch zugänglich.

Sensoren auf dem Mainboard zeichnen laufend Werte auf. Die Treiber für diese Sensoren sind im Linux-Kernel enthalten und der Treiber des jeweiligen Mainboard-Sensors legt seine Daten in aller Regel unter „/proc“ ab. [1] Diese Werte beschreiben den Gesundheitszustand eines Rechners. Bei der schneller Auswertung der Daten können die im folgendem dargestellten Überwachungsprogramme helfen.

2.2 LM-Sensors

Linux Monitoring Sensors dient zum Auslesen von Lüfterdreherzahlen, Temperaturen, Spannungen und einigen weiteren Informationen des Mainboards auslesen und auf der Kommandozeile anzeigen lassen. (Abbildung 1.)

```
it8716-isa-0290
Adapter: ISA adapter
VCore:      +1.39 V  (min =  +0.00 V, max =  +4.08 V)
VDDR:       +0.00 V  (min =  +0.00 V, max =  +4.08 V)   ALARM
+3.3V:      +3.38 V  (min =  +0.00 V, max =  +4.08 V)
+5V:        +5.00 V  (min =  +0.00 V, max =  +6.85 V)
+12V:      +11.84 V  (min =  +0.00 V, max = +16.32 V)
in5:        +3.71 V  (min =  +0.00 V, max =  +4.08 V)
in6:        +0.00 V  (min =  +0.00 V, max =  +4.08 V)   ALARM
5VSB:       +4.84 V  (min =  +0.00 V, max =  +6.85 V)
VBat:       +3.06 V
fan1:      1344 RPM  (min =    0 RPM)
fan2:      1445 RPM  (min =    0 RPM)
fan3:      1527 RPM  (min =    0 RPM)
temp1:        +45°C  (low  =   -1°C, high =  +127°C)   sensor = diode
temp2:        +50°C  (low  =   -1°C, high =  +127°C)   sensor = thermistor
temp3:        +34°C  (low  =   -1°C, high =  +127°C)   sensor = thermistor
vid:       +1.550 V

k8temp-pci-00c3
Adapter: PCI adapter
Core0 Temp:
              +37°C
Core1 Temp:
              +41°C
```

Abbildung 1.

[1] Linux-Magazin 04/10

Die von LM-sensors ausgelesenen Werte kann man sich auch mit Hilfe von verschiedenen Tools so wie *ksensors, xsensors, computertemp* auf dem Desktop anzeigen lassen (Abbildung 2.).

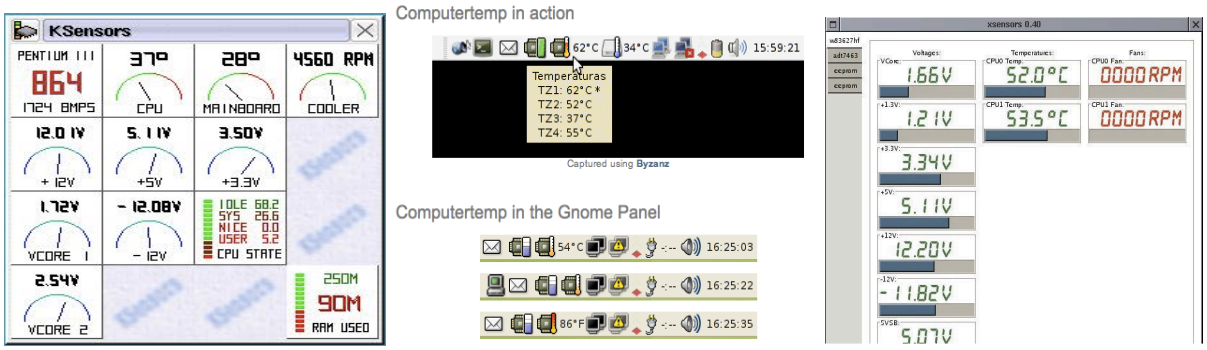

Abbildung 2.

2.3 S.M.A.R.T.

Das System zur Überwachung, Analyse und Statusmeldung (kurz S.M.A.R.T. genannt) ermöglich das Überwachen wichtiger Parameter und somit das frühzeitige Erkennen drohender Defekte. Damit ein Festplattendefekt nicht plötzlich auftritt, verfügen neuere Platten über ein S.M.A.R.T.-System. Wird es vom BIOS des jeweiligen PCs unterstützt, erscheinen beim Booten Warnmeldungen, wenn etwas nicht stimmt.

Realisierung des SMART-Standarts unterscheidet sich bei den Festplattenanschlüssen.

2.3.1 Unterschied nach Festplattenanschlüssen

Bei den in Computer *eingebauten* gibt es zwei: ATA und SCSI Standards. Beide kennen Health Status und deswegen zeigt das Laufwerk selbst an, ob es sich als „okay“ oder „problematisch“ einstuft. Sowohl ATA las auch SCSI unterstützen das Auslesen der Temperatur und mehrere Varianten von Selbsttests und Logbüchern. Die Kommandos und Datenformate sind bei ATA und SCSI völlig unterschiedlich.

Die *externen Festplatten* unterscheiden sich von den internen nur durch das Gehäuse und dessen Anschluss, es gibt auch mehrere Standards. So *USB* angeschlossenen Festplatten sind fast ausnahmslos keine SCSI sondern (S)ATA Platten und haben somit keinen direkten Zugriff auf S.M.A.R.T.-Funktionalität. Die USB-ATA-Bridges ermöglichen eine Tunnelung der ATA-Kommandos durch den USB-Anschluss. Die Treiber für externe

Festplatten unterstützen das aber nicht. Chip-Hersteller wie Cypress, JMicron oder SunPlusIT verwenden herstellerspezifische Kommandos, die von einigen Programmen beherrscht werden. Neuerdings gibt es auch USB-SATA-Bridges, die den herstellerunabhängigen SAT-Standard unterstützen. [2]

Firewire ermöglichen die Ermittlung von S.M.A.R.T.- Werten und sind besonders bei Apple-Rechner üblich, wird aber von MAC OS X nicht benutzt.

eSATA und ihre internen SATA-Pendants lesen die SMART-Werte problemlos aus.

Wenn die entsprechenden SAT-Kommandos zur Verfügung stehen können auch die SATA-Platten, die über *Serial Attached SCSI* (SAS) angeschlossen sind, geprüft werden.

2.3.2 S.M.A.R.T.-Werte auslesen und interpretieren

S.M.A.R.T.-Werte geben über viele Daten Auskunft, etwas Temperatur, Geschwindigkeit, Fehlerraten oder die Anzahl der geleisteten Betriebstunden einer Festplatte.

Die wichtigsten Attribute sind:

- Nummer des Attributs
- Name
- Value
- Worst
- Thresh
- RAW (Rohdaten)

Der „Value“ ist ein normierter Wert und stellt die Interpretation des jeweiligen Betriebsparameter durch die Platen-Firmware dar. Er wird auf 100 oder 253 normiert und dabei gilt es höher= besser (Ausnahmen: das Attribut „Temperature“ oder Ultra DMA CRC Error Count mit 200).

„Worst“ ist bislang schlechtester (kleinster) registrierte normierter Wert und Thresh gibt das Minimum dafür an, das nicht unterschritten werden soll, sonst wird der „S.M.A.R.T. status: FAILED“ gemeldet.

Jeder Wert wird zuerst als ein RAW-Data gespeichert. Dieser wird dann zum besseren Verständnis auf einer Werteskala von 0 bis 100, 200 oder 255 einsortiert. Die Rohdaten sind nicht bei allen Attributen vorhanden, können aber wertvolle Hinweise, zum Beispiel, zu den Betriebstunden, Zahl der defekten Sektoren usw. geben.

[2] http://de.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology

In der folgenden Übersicht[3] werden die häufigsten und die wichtigsten Parameter erläutert:

Raw Read Error Rate: Fehlerrate beim Lesen von Daten auf der Festplatte.

Spin Up Time: Zeit, die zum Erreichen der Platten-Endgeschwindigkeit benötigt wird.

Start/Stop Count: Anzahl der Start/Stop-Vorgänge.

Reallocated Sector Count: Zeigt die Anzahl der verbrauchten „Reservesektoren" an.

Seek Error Rate: Fehlerrate beim Lesen von Daten auf der Festplatte.

Power On Hours Count: Gesamtlaufzeit der Festplatte, je nach Hersteller in Stunden.

Power Cycle Count: siehe Start/Stop Count, aber ohne „Standby-Start/Stop-Vorgang"

Temperature: Aktuelle Temperatur der Festplatte.

Ultra DMA CRC Error Count: Deutet auf fehlerhafte Verbindungskabel, Steckkontakte oder Treiberprobleme hin.

Spin Retry Count: Anzahl der Festplatten-Fehlstarts – in Zusammenhang mit Spin Up Time betrachten.

2.3.3 S.M.A.R.T.-Testfunktionen

Die Testfunktionen lassen sich in drei Kategorien aufteilen: Onlinetest, Offlinetest und Selftest.

Der Onlinetest läuft unbemerkt an und erhebt die Daten zur Funktionsfähigkeit des Geräts, die dann in einer internen Tabelle gespeichert werden und die Fehlermeldungen in das interne Errorlog kommen. Die Daten die dem Onlinetest aus technischen Gründen versagt bleiben, werden von dem Offlinetest gesammelt. Die beiden Tests laufen bei der Aktivierung in regelmäßigen Abständen automatisch ab.

Der Selftest prüft die Software tatsächlich und wird nur auf Anforderung gestartet. Man unterscheidet noch drei Arten von Selftest: kurzer und langer Selftest dauern nur wenige Minuten und der Offline-Scan-Test braucht je nach der Größe der Festplatte eine Stunde oder länger.

[3] www.ovalnets.de/festplattenfehlerdiagnose-spezial-smart-werte-auslesen-und- interpretieren

Das Testergebnis wird in einem Selftest Log festgehalten und die Fehler kommen in das Error-Log, das Information zu den letzten 5 Fehlern enthält.

Alle drei Testvarianten belasten die Nutzung der Festplatte nur minimal, doch die ständigen Unterbrechungen durch Zugriffe verlängern nun die Testdauer.

2.3.4 Softwarelösungen zum Auslesen von S.M.A.R.T.-Werten

Es existieren verschieden Tools, um die S.M.A.R.T.-Werte graphisch anzeigen zu lassen. Mit Smatrtmontools und GSmartControl können die gespeicherten Werte unter Linux ausgelesen und übersichtlich in Tabellenform dargestellt werden.

Smartmontools

Linux-Version verfügt über keine graphische Oberfläche, die Daten werden per Kommandozeile ausgegeben. Je nach der Festplatte beschränkt sich Smartmontools entweder auf das Wesentliche (Abbildung 3.) oder liefert die ausführliche Diagnose (Abbildung 4.).

```
=== START OF INFORMATION SECTION ===
Device Model:     FUJITSU MHY2250BH
Serial Number:    K43CT832A909
Firmware Version: 0081000D
User Capacity:    250.059.350.016 bytes
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   8
ATA Standard is:  ATA-8-ACS revision 3f
Local Time is:    Thu Sep 30 16:57:02 2010 CEST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

Abbildung 3.

GSmartControl

Mit GSmartControl erhält man einen genauen graphisch dargestellten Überblick über den Zustand der Festplatte. (Abbildung 5.) Die angezeigten Bezeichnungen und Zahlenwerte sind anfangs wenig aussagekräftig. Wenn man mit dem Mauszeiger über diese Begriffe fährt, blendet die Software eine detaillierte Erklärung ein. Angezeigt werden auch allgemeine Informationen, wie Speicherkapazität, Seriennummer und Modellnamen der Festplatte.

```
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_
FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   100   100   046    Pre-fail  Always       -
      0
  2 Throughput_Performance  0x0005   100   100   030    Pre-fail  Offline      -
      0
  3 Spin_Up_Time            0x0003   100   100   025    Pre-fail  Always       -
      0
  4 Start_Stop_Count        0x0032   098   098   000    Old_age   Always       -
      6393
  5 Reallocated_Sector_Ct   0x0033   100   100   024    Pre-fail  Always       -
      0
  7 Seek_Error_Rate         0x000f   100   100   047    Pre-fail  Always       -
      0
  8 Seek_Time_Performance   0x0005   100   100   019    Pre-fail  Offline      -
      0
  9 Power_On_Hours          0x0032   091   091   000    Old_age   Always       -
      4912
 10 Spin_Retry_Count        0x0013   100   100   020    Pre-fail  Always       -
      0
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -
      3840
192 Power-Off_Retract_Count 0x0032   100   100   000    Old_age   Always       -
      51544522812
193 Load_Cycle_Count        0x0032   090   090   000    Old_age   Always       -
      219681
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -
      39 (Lifetime Min/Max 15/49)
195 Hardware_ECC_Recovered  0x001a   100   100   000    Old_age   Always       -
      0
196 Reallocated_Event_Count 0x0032   100   100   000    Old_age   Always       -
      0
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -
      0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -
      0
199 UDMA_CRC_Error_Count    0x003e   200   253   000    Old_age   Always       -
      0
200 Multi_Zone_Error_Rate   0x000f   100   100   060    Pre-fail  Always       -
```

Abbildung 4.

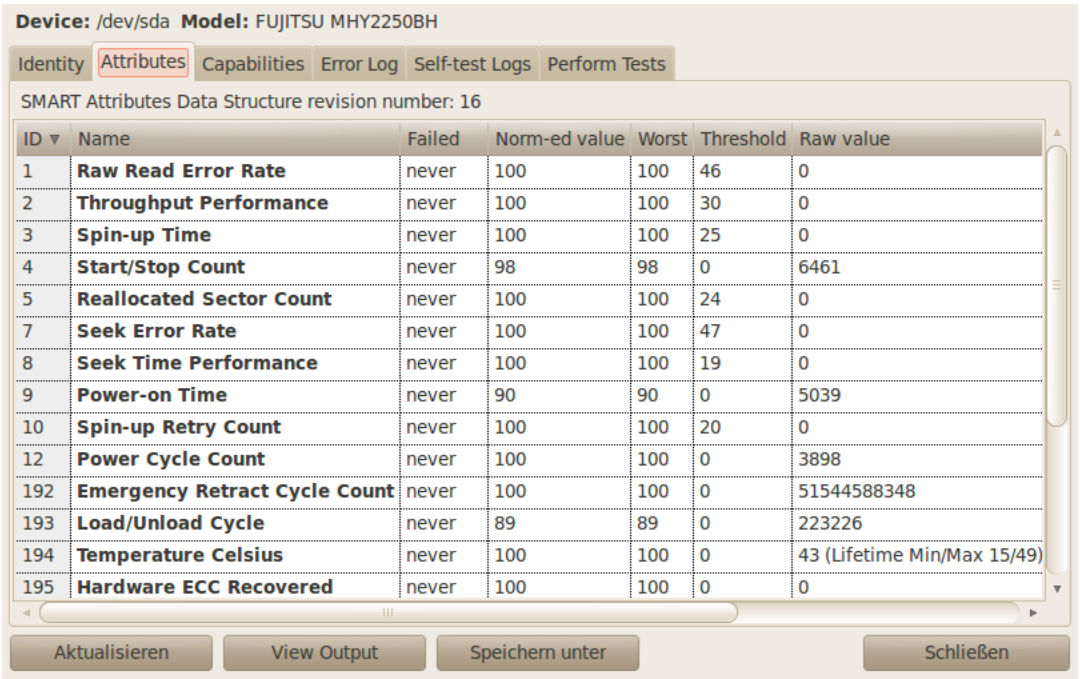

Abbildung 5.

2.3.5 S.M.A.R.T.-Fazit

S.M.A.R.T. gibt einen realistischen Überblick auf den aktuellen Zustand der Festplatte und hilft frühzeitig Probleme zu erkennen.

Es ist zu beachten, dass der S.M.A.R.T.-Mechanismus allein der Festplattenausfall nicht vorhersagen kann. So laut Google-Studie zur Ausfallursache von Festplatten hat ergeben, dass 36% ausgefallener Laufwerke zuvor keinerlei S.M.A.R.T.-Fehler gemeldet haben. [4] Deswegen sollte man trotz Frühwarnsystem wie S.M.A.R.T. regelmäßig Datensicherung durchführen, um Datenverluste vorzubeugen.

2.4 SNMP

SNMP (ausgeschrieben Simple Network Management Protocol) ist ein Netzwerk, das von IETF entwickelt wurde, um Netzwerkelemente wie zum Beispiel Router, Server, Switsches, Drucker, Computer von einer zentralen Station aus überwachen und steuern zu können. Das Protokoll regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Zu den wichtigen Aufgaben von SNMP gehört: Netzwerkkomponente überwachen, fernsteuern und fernkonfigurieren sowie auch das Erkennen und Benachrichtigen von Fehlern.

2.4.1 Funktionsweise

SNMP ruht auf zwei grundlegenden Eigenschaften: Supervisor und Agenten. Supervisor ist eine Managementkonsole von der aus der Netzadministrator die Verwaltungsaufgaben durchführt. Agenten sind Programme, die auf den überwachten Geräten laufen und deren Aufgabe das Einholen von Informationen über die unterschiedlichsten Objekte, ist. Diese Programme sind in der Lage über diese Agenten auf die Geräte zu zugreifen und auch selbst Einstellungen vorzunehmen oder Aktionen auszulösen.

Kommunikation zwischen Manager und Agenten erfolgt über ein Netzwerk, dazu gibt es sechs verschiedene Datenpakete[5], die gesendet werden können:

GET - zum Anfordern eines Management Datensatzes

[4] http://www.heise.de/newsticker/meldung/Google-Studie-zur-Ausfallursache-von-Festplatten-147178.html

[5] http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol

GETNEXT - um den nachfolgenden Datensatz abzurufen (um Tabellen zu durchlaufen)

GETBULK - um mehrere Datensätze auf einmal abzurufen, wie z. B. mehrere Reihen einer Tabelle

SET - um einen Datensatz eines Netzelementes zu verändern

RESPONSE - Antwort auf eines der vorherigen Pakete

TRAP - unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.

Die Get-Pakete dienen dazu, die Daten über die jeweilige Station anzufordern, dabei werden sie von Manager zu einem Agenten gesendet. Der Agent antwortet mit einem Response-Paket, in dem entweder die Daten die angefordert waren enthalten sind oder eine Fehlermeldung.

Ein Manager kann mit einem Set-Paket die Werte bei dem Agenten verändern, Einstellungen vornehmen oder Aktionen auslösen. Der Agent bestätigt die neuen Werte mit einem Response-Paket wieder.

Wird bei der Systemüberwachung ein Fehler von Agenten erkannt, kann er diesen mit Hilfe eines Trap-Paketes unaufgefordert an den Manager melden. Dabei bestätigt der Manager diese Pakete nicht, somit kann der Agent nicht feststellen, ob der Trap angekommen ist oder nicht.

2.4.2 Management Information Base

Management Information Base (kurz MIB) ist eine Art Datenbank, die die von SNMP gesendete Daten ablegt und speichert sie. Das heißt, dass die Werte die von einem Manager über die gemanagte Netzwerkkomponente ausgelesen und verändert werden können, werden in MIB beschrieben. Die Informationen der MIB werden in Baumstruktur dargestellt, deren einzelne Zweige entweder durch Nummern oder alphanumerische Bezeichnungen aufgeführt werden können. An einem genauen Beispiel, ist die MIB-2 unter „iso.org.dod.internet.mgmt.MIB-2“ zu finden oder lässt sich durch die Zahlenreihe 1.3.6.1.2.1 eindeutig identifizieren. (Abbildung 6.) Dabei wird diese Zahlenreihe als Object Identifier (OID) genannt.

Mit Hilfe der MIB-Dateien sind die Managementprogramme in der Lage den Aufbau der Daten beim Agenten darzustellen und sie abzufragen, ohne dass der Benutzer die OID selber kennen muss.

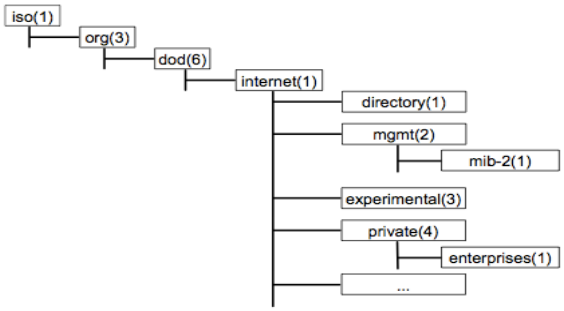

Abbildung 6.

2.4.3 SNMP-Versionen und Sicherheitsprobleme

Mit SNMP ist es möglich per UDP bestimmte Systeminformationen abzufragen du sogar einige Einstellungen zu ändern. Ein Schwachpunkt einiger SNMP-Versionen ist die Sicherheit, daher stammt die scherzhafte Deutung der Abkürzung SNMP als „Security ist not my problem".

Die Versionen 1 und 2c bieten fast keine Sicherheitmechanismen. Es ist keine Anmeldung mit dem Kennwort und Benutzernamen möglich, sondern es werden sogenannte Communities verwendet. Dabei sind die Communities[6] die einfachen Namen, die auf Standartwerten „public" und „private" belassen werden. Man kann auch einen sehr langen und komplizierten Community-Namen verwenden, der Nachteil ist jedoch, dass SNMP-Pakete nicht verschlüsselt sind und deshalb sehr einfach von einem Angreifer abgefragt werden können.[7]

In der aktuellen Version 3 wurden die Sicherheitsmechanismen deutlich erweitert, dadurch ist die Komplexität gestiegen, was dazu geführt hat, dass diese Version nicht so weit verbreitet ist.

SNMP stellt kein grundsätzliches Problem dar, und wird auch von größeren Netzwerküberwachungstools wie Nagios genutzt. Sicherheitshalber sollte SNMP deaktiviert sein oder zumindest an den Netzgrenzen blockiert werden.

[6] http://www.heise.de/newsticker/meldung/Systeme-verraten-sensible-Daten-per-SNMP-186430.html

[7] http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol

2.5 Netzwerküberwachung

Für einen einzelnen Rechner reichen die obengenannten Smartmontools oder lm-sensors Möglichkeiten zweifellos aus. Wer aber einen ganzen Rechnerpool überwachen muss, braucht einen höheren Automatisierungsgrad. Eine Möglichkeit ist, *Ganglia* oder *Nagios* damit zu beantragen. Im folgendem werden die Tools kurz vorgestellt.

2.5.1 Ganglia

Ganglia ist ein Überwachungstool für Hochleistungssysteme wie Cluster oder Grids. Das Programm zeigt nicht nur Informationen zur Performance der einzelnen Rechner im Cluster an sondern gibt auch einen Überblick über die Leitung des gesamten Cluster-Systems. Es werden dabei verschiedene Techniken eingesetzt: wie XML zur Darstellung der Daten, XDR für den portablen Datentransport oder RRDtool zum Speichern und Visualisieren der Daten. [8]

2.5.2 Nagios

Nagios ist ein satusorientirtes, plug-in-basiertes Monitoring-Framework zum Überwachen von komplexen IT-Infrastrukturen, das, wie es oben schon erwähnt wurde, SNMP zur Kommunikation benutzt. Mit der Monitoring Software Nagios können sämtliche Ressourcen Ihres Netzwerks, wie Server, Router, Switches und Dienste dargestellt und überwacht werden.

Nagios überwacht per Netzwerk die Verfügbarkeit von Diensten und informiert den Administrator, wenn etwas nicht mehr gut läuft. Somit hilft Nagios Administratoren Netzwerkprobleme schnell zu beseitigen, bevor ein Ausfall auftreten kann und damit die Verfügbarkeit des Netzwerkes und die Zufriedenheit der Benutzer signifikant zu steigern.[9]

Nagios wird auch zur Überwachung des Netzwerks im Rechenzentrum des Fachbereichs Informatik eingesetzt.

[8] http://ganglia.sourceforge.net/

[9] http://www.nagios.org/about/

3 Zusammenfassung

Vorliegende Seminararbeit gibt einen genaueren Überblick über die möglichen Tools, die zum Auslesen von Hardwaredatenquellen unter Linux eingesetzt werden können. Es wurden sowohl einfache Tools wie lm-sensors vorgestellt als auch solche die einen detalierten Überblick geben, wie zum Beispiel Smartmontools und SNMP.

Zusammengefasst kann man mit Hilfe von *lm-sensors* Temperatur, Netzteilspannungen und Lüfterdreherzahlen auslesen. *S.M.A.R.T.* erlaubt das Auslesen relevanter „Platten-Gesundheitsparameter“ und kann somit etwaige Festplattenprobleme feststellen. *SNMP* ist ein Netzwerkprotokoll mit dem Netzwerkadministratoren die Netzbelange verwalten und Netzprobleme untersuchen können.

Diese Lösungen reichen zum Überwachen von einzelnen Rechnern zu Hause. Zum Monitoring von ganzen Rechnerpools können *Ganglia* oder *Nagios* eingesetzt werden.

Literaturquellen

Hardwaresensoren

http://www.hubertus-sandmann.homepage.t-online.de/l_sens.htm

Linux-Magazin 04/10

SMBus

http://www.smbus.org/

LM-Sensors

http://www.lm-sensors.org/

http://arktur.schul-netz.de/wiki/index.php/Installationshandbuch:Sensors (Abbildung 1.)

http://ksensors.sourceforge.net/ (Abbildung 2.)

http://freshmeat.net/projects/xsensors (Abbildung 2.)

http://computertemp.berlios.de/screenshots.php (Abbildung 2.)

SMART

http://de.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology

http://smartlinux.sourceforge.net/smart/attributes.php

http://sourceforge.net/apps/trac/smartmontools/wiki

http://stephan.win31.de/platten.htm

http://gsmartcontrol.berlios.de/home/index.php/en/Home

http://www.heise.de/newsticker/meldung/Google-Studie-zur-Ausfallursache-von-Festplatten-147178.html

SNMP

http://www.snmplink.org/

http://www.profinet.felser.ch/technik/SNMP.pdf (Abbildung 6.)

http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol

http://www.heise.de/newsticker/meldung/Systeme-verraten-sensible-Daten-per-SNMP-186430.html

Ganglia

http://ganglia.sourceforge.net/

Nagios

http://www.nagios.org/about/