Überwachung

Man kann mit ganz einfachen Mitteln einen Server überwachen. Zur Kontrolle der Partitionsbelegung, des RAM-Verbrauchs, der CPU-Auslastung, der internen und externen IP, der Prozesse oder der Systemlaufzeit reichen Kommandozeilen-Tools meist völlig aus.

Empfehlenswerte Nachinstallationen

1. Infoprogramm INIXI
   Aufruf mit `inixi -v7` mit maximalem Informationsgehalt
2. Taskmanager htop
   Aufruf mit `htop`
   Der Taskmanager lässt sich flexibel konfigurieren.
3. Hardwareanalyse
   Bei Hardware-Fragen oder Problemen halten Sie sich an das Display-Message-Tool dmesg für Kernel-Nachrichten. Zur besseren Lesbarkeit ist immer Schalter „-T“ zu empfehlen, Zusätzlich sollte das simple Format-Tool ccze nachinstalliert werden.
   Aufruf mit `dmesg –T | ccze -A '' - ''IP-Tables automatisch ''speicher''n` ''iptables-persistentapt-get install ''

```
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

Logdateien

Die wichtigsten Infos liefern die Dateien unter „/var/log“. Mit root-Rechten auf der Konsole kannst du diese mit den üblichen Kommando-Tools durchsuchen

Einen genauen Überblick, was sich auf dem Server getan hat, liefert logwatch

- auth.log
  protokolliert im Klartext und ausführlich alle Systemanmeldungen. Wer in aller Kürze die erfolgreichen und gescheiterten Log-ins kontrollieren will, kann sich zusätzlich an die Dateien „/var/log/wtmp“ (erfolgreich) und „/var/log/btmp“ (gescheitert) halten. Diese binären Dateien lassen sich am bequemsten mit last (erfolgreich) und lastb (gescheitert) auslesen
  :`last -200`
  `lastb -200 root`
  Gezeigt werden hier jeweils die letzten 200 Anmeldungen, die sich – wie das zweite Beispiel zeigt – auch auf ein bestimmtes Konto filtern lassen.
- syslog
  st das Systemlogbuch und zeigt Ereignisse aller Art, die an den syslogd-Daemon berichten – vorwiegend Kernel-, Hardware-und Cron-Ereignisse
- dpkg.log
  vermerkt alle manuellen (De-)Installationen und automatischen Updates. Ergänzend und in mancher Hinsicht übersichtlicher lohnt sich in diesem Zusammenhang auch der Blick in die Datei „/var/log/apt/history.log“

- /var/log/samba
  Hier findest du für jedes zugreifende Netzgerät ein eigenes Protokoll – entweder mit Host-Namen oder lokaler IP-Adresse. Infos zur Hardware liegen bekanntlich im Klartext im Verzeichnis „/proc“. Wo Ihnen die Detailschärfe eines Tools wie inxi nicht ausreicht, können Sie diese Dateien mit cat auslesen. Prominente Kandidaten sind cpuinfo, meminfo, mounts, partitions, version.

Monitoring Tools

Eine Sammlung von verschiedensten Monitoringtools (Server, Netzwerk, Apache, Mysql etc.) findest du hier

From:
http://wiki.waldhofer.at/ - **Wiki von Franz**

Permanent link:
http://wiki.waldhofer.at/doku.php?id=ubuntu:ueberwachung&rev=1522678485

Last update: **2021/11/04 18:57**