

Zusammenfassung Tag 23

Die Systemprotokollierung

- Linux protokolliert hauptsächlich nach /var/log
- Haupt-Logdateien sind /var/log/messages (CentOS, SuSE, u.a.) bzw. /var/log/syslog (Debian-Derivate)
- Es gibt für viele spezielle Ereignisse dedizierte Logfiles (auth.log, kern.log, btmp und wtmp)
- Standardmäßig wird ein Ringpuffer genutzt, d.h. die ältesten Meldungen werden irgendwann überschrieben
- Andere Komponenten, wie Serverdienste, erstellen teilweise eigene Unterverzeichnisse für ihr Logging unter /var/log
- Logeinträge erfolgen normalerweise in Klartext (btmp und wtmp sowie das Systemd-Journal sind Ausnahmen)
- Das Programm cce ermöglicht die Einfärbung von Logeinträgen

Das Syslog-Konzept verstehen

- Syslog ist ein alter Standard, der von vielen Systemen unterstützt wird
- Syslog-Meldungen haben einen bestimmten Aufbau:
 - Herkunft(Facility)
 - Schweregrad (Severity)
 - Ereignis
- Der Syslog-Daemon rsyslogd ist der verbreitetste unter Linux, er wird in /etc/rsyslog.conf konfiguriert

Das Syslog-Konzept verstehen

Facilities

0 – kernel messages (kern)
1 – user-level messages (user)
2 – mail system (mail)
3 – system daemons (daemon)
4 – security/authorization messages (aut)
5 – messages generated internally by syslog (syslog)
6 – line printer subsystem (lpr)
7 – network news subsystem (news)
8 – UUCP subsystem (uucp)
9 – clock daemon (cron)
10 – security/authorization messages (authpriv)
11 – FTP daemon (ftp)
...
16 – local0
17 – local1
...
23 – local7

} Frei definierbar

Severities

0 – Emergency
1 – Alert
2 – Critical
3 – Error
4 – Warning
5 – Notice
6 – Informational
7 – debug

Facility + Severity = Selector

Beispiele:

mail.=err
auth,authpriv.*
.;auth,authpriv.none
local5.err
local1.*
daemon.*
*.alert

Action

/var/log/syslog
-/var/log/syslog
asterix
@192.168.1.205
/dev/console

rsyslogd
/etc/rsyslog.conf

/var/log/mailerr.log
/var/log/auth.log
-/var/log/syslog
-/var/log/mylog.log
@192.168.1.205
/dev/tty8
root,eric

Den Syslog-Daemon konfigurieren

- rsyslogd läuft als Daemon im Kontext des Benutzers syslog
- /etc/rsyslog.conf ist die Hauptkonfigurationsdatei, die hauptsächlich Dateien unter /etc/rsyslog.d einbindet
- unter Ubuntu wird die Datei /etc/rsyslog.d/50-default.conf eingebunden, die die hauptsächlichsten Einträge enthält. Das kann auf anderen Distributionen anders geregelt sein.
- bei CentOS sind diese Regeln direkt in /etc/rsyslog.conf enthalten

Remote-Logging konfigurieren

- in rsyslog.conf muss das Modul imudp oder imtcp aktiviert werden
- Standardmäßig wird Port 514/udp genutzt
- Auf dem Syslog-Client wird in den Regeln in /etc/rsyslog.conf ein Eintrag erzeugt, dessen Action @<Server-Adresse> enthält

Logrotate nutzen

- Mit dem Programm logrotate können Logfiles rotiert werden
- logrotate läuft nicht als Dienst, sondern wird durch Systemd (Ubuntu) bzw. crond (CentOS) gestartet
- Die Konfiguration von Logrotate findet sich in /etc/logrotate.conf
- Sie enthält Einstellungen zum Rotationszyklus, der Anzahl der aufzuhebenden Backlogs, u.a.
- unter /etc/logrotate.d/ finden sich ggf. weitere Dateien zur Konfiguration bestimmter Komponenten des Systems, z.B. CUPS oder Apache2

Das Systemd-Journal

- Das Systemd-Journal ist eine zweite Log-Ebene, Systemd loggt parallel zu Syslog
- Der dafür zuständige Dienst ist journald
- Das Journal kann über den Befehl journalctl angezeigt werden
- Der Befehl unterstützt zahlreiche Optionen zur Formatierung, Filterung und Anzeige alter Journale