Syslog: (Systemlogbuch)

Es werden 2 Dienste Benötigt: Der Klogd, er nimmt Kernel-Log's entgegen und Reicht sie an den "Syslog" weiter...

Der Syslogd oder Syslog-ng, einer dieser Dienste ist dann für das logging zuständig. Mit ihm können die Meldungen Sortiert und Archiviert werden.

Zum Starten beider dienste:

/etc/init.d/sysklogd start

Konfiguration:

Herkunft einer Meldung: (facility)

kern → Meldungen die vom Kernel Kommen.
lpr → Meldungen vom Drucksystem (lpr, cups)
auth → Meldungen vom Sicherheitssystem (login, su ...)
authpriv → Vertrauliche Meldungen vom Sicherheitssystem
mail → Meldungen vom Mailsystem (sendmail, postfix ...)
news → Meldungen vom News-System
cron → Meldungen vom Cron-Daemon
daemon → Meldungen von Deamon's die keine eigene Herkunft haben
syslog → Meldungen des Syslogger's
user → Meldungen normaler Anwendungsprogramme
ftp → Meldungen vom FTP-Server
uucp → Meldungen des UUCP-Systems
ocal0 - 7 → Frei Verwendbar

Prioritäten: (level)

none → Wird verwendet um Meldungen auszuschließen
debug → Wird zur Fehlersuche verwendet, hier wird jeder noch so kleine Programmablauf Protokolliert
info → Log's im normalen Programmablauf
notice → Protokollierung bemerkenswerter Sachen
warn → Warnungen aller Art
err → Fehlermeldungen aller Art
crit → Meldungen über Kritische ereignisse, die gerade noch mal gut gegengen sind.
alert → Meldungen, die ein sifortiges Eingreifen notwendig machen
emerg → Letzte Meldung vor dem Absturz

Der "syslogd": Konfigurationsdatei: /etc/syslog.conf

```
1.  kern.*                    -/var/log/kernel.log
2.  *.*;auth,authpriv.none     /var/log/messages
3.  *.=err                     /var/log/error.log
4.  *.*                       @172.16.109.240
5.  *.crit                     root
6.  *.*                        /dev/tty10
```

zu 1.) Alle Meldungen die vom Kernel kommen, egal welche Priorität sie haben derden mit Aktivem Cache in die Datei /var/log/kernel.log geschreiben.

zu 2.) Alle Meldungen, aller Prioritäten, mit Außnahme auth und authpriv, werden sofort in die Datei /var/log/messages geschrieben

zu 3.) Meldungen alle Herkunften, die genau die Priorität "err" haben werden sofort in die Datei /var/log/error.log geschrieben

zu 4.) Alle Meldungen werden an den Syslogger auf dem Rechner 172.16.109.240 weitergegeben

zu 5.) Alle Meldungen die Kritisch oder Schlimmer sind, werden dierekt in eine Root-Shell geschreiben.

zu 6.) Alle Meldungen werden auf dem Terminal /dev/tty10 ausgegeben

Der Syslog-ng:

Der "syslog-ng" ist der Nachfolger des "syslogd" er ist viel feiner konfigurierbar und viel leichter als Log-Server zu verwenden, da sich die Log's nach Rechner sortieren lassen.

Konfigurationsdatei: /etc/syslog-ng/syslog-ng.conf

```
1:
options                    {
                            chain_hostnames(0);
                            time_reopen(10);
                            time_reap(360);
                            log_fifo_size(2048);
                            create_dirs(yes);
                            group(adm);
                            perm(0640);
                            dir_perm(0755);
                            use_dns(no);
                            stats_freq(0);
                           };
```

```
2
source s_all            {
                        internal();
                        unix-stream("/dev/log");
                        file("/proc/kmsg" log_prefix("kernel: "));
                        };
3:
source s_remote         {
                         udp(ip("0.0.0.0") port(514));
                        };
4:
destination d_remote    {
                         file("/var/log/remote.log");
                        };
5:
destination d_messages  {
                         file("/var/log/messages");
                        };
6:
destination d_usb       {
                         file("/var/log/usbstick");
                        };
7:
destination d_rico      {
                         file("/var/log/rico.log");
                        };

8:
filter f_usb            {
                         match(/dev/sd.);
                        };
9:
filter f_mail           {
                         facility(mail) and priority(warn..emerg);
                        };
10:
filter f_rico           {
                         host("172.16.107."9);
                        };
11:
filter f_remote         {
                         not filter(f_rico);
                        };
12:
log                     {
                         source(s_remote);
                         filter(f_remote);
                         destination(d_remote);
                        };
```

```
13:
log                     {
                         source(s_all);
                         destination(d_messages);
                        };
14:
log                     {
                         source(s_all);
                         filter(f_usb);
                         destination(d_usb);
                        };
15:
log                     {
                         source(s_remote);
                         filter(f_rico);
                         destination(d_rico);
                        };
```

zu 01: Hier Werden Algemeine Optionen für den Syslogger festgelegt-

zu 02: Hier Wird eine Quelle namens ***s_all*** definiert die Daten kommen vom Syslogger selbst ***internal()***, aus der Datei ***/proc/kmsg*** und dem Streem ***/dev/log***

zu 03: Hier wird eine Quelle namens s_remote definiert die Daten kommen kommen fom UDP-Port 514

zu 04: Hier wird ein Ziel namens ***d_remote*** definiert, alles was an das Ziel ***d_remote*** geschickt wird landet in der Datei /var/log/remote.log

zu 05: …

zu 06: …

zu 07: …

zu 08: Hier wird ein Filter namens ***f_usb*** definiert, durch ***match(/dev/sd.)*** trifft dieser Filter auf alle Meldungen zu die, die Zeichenkette „***/dev/sd***" beinhalten.

Zu 09: Hier wird ein Filter namens ***f_mail*** definiert, der auf alle Meldungen mit der Herkunft „***mail***" und der Priorität „***warn***" oder schlimmer haben

zu 10: Hier wird ein Filter namens ***f_rico*** definiert der auf alle Meldungen, bei denen im Hostteil die IP 172.16.107.9 auftaucht.

Zu 11: Hier wird ein Filter namens ***f_remote*** definiert der auf alle Meldungen Zutrifft, auf die der Filter ***f_rico*** nicht zutrifft

zu 12: Hier werden nun alle Meldungen aus der Quelle ***s_remote*** auf die der Filter ***f_remote*** zutrifft in das Zeil ***d_remote*** geschrieben

zu 13: Hier werden alle Meldungen aus der Quelle ***s_all*** in das Ziel ***d_messages*** geschrieben.

Zu 14: Hier werden alle Meldungen aus der Quelle ***s_all*** , auf die der Filter ***f_usb*** zutrifft in das Ziel ***d_usb*** geschrieben

zu 15: Hier werden alle Meldungen aus der Quelle ***s_remote*** auf die der Filter ***f_rico*** zutrifft in das Ziel ***d_rico*** geschrieben