Sylog Server für den Einsatz mit der CCU

Was

Einen Sylog-NG Server welcher die Log Einträge der CCU speichert.

Warum

Weil die CCU Firmware (egal ob eine Originale CCU2 oder eine LXCCU) nur die letzten 1000 Einträge bis zum Neustart speichert. Damit also mehr als 1000 und auch nach einem Neustart gespeichert werden sollte ein Syslog Server verwendet werden.

Mit einer LXCCU Installation auf einem Raspberry PI habt ihr auch diese Möglichkeit den Syslog Server auf der gleichen Hardware zu Installieren!

Installation

Syslog Server

Zum Installieren einfach auf einer root Konsole folgendes ausführen:

```
aptitude install syslog-ng
```

Auch müsst ihr zustimmen das der rsyslog ersetzt wird von syslog-ng, wenn also diese Meldung kommt:

The following actions will resolve these dependencies:

```
   Remove the following packages:
```

1) rsyslog

Accept this solution? [Y/n/q/?]

Könnt ihr diese einfach mit [Enter] bestätigen.

Nun müsst ihr den syslog auch so konfigurieren das dieser aus dem lokalen Netzwerk Daten entgegen nimt, dazu öffnet ihr die Datei

```
vi /etc/syslog-ng/syslog-ng.conf
```

und ändert den Source Block auf diesen:

```
########################
# Sources
########################
# This is the default behavior of sysklogd package
# Logs may come from unix stream, but not from another machine.
#
source s_src {
       system();
       internal();
};

# If you wish to get logs from remote machine you should uncomment
# this and comment the above source line.
#
#source s_net { tcp(ip(127.0.0.1) port(1000) authentication(required)
encrypt(allow)); };
source s_net {
        udp(ip(0.0.0.0) port(514));
        tcp(ip(0.0.0.0) port(514));
};
```

und im Destination Block am ende diese Zeilen:

```
# network Log
destination network { file("/var/log/net.log" owner("root") group("root")
perm(0640)); };
```

und am Ende der Datei noch den log Eintrag

```
log { source(s_net); destination(network); };
```

Dann nich den Syslog Dienst neu starten damit diese Änderungen übernommen werden:

```
service syslog-ng restart
```

zum Testen ob der Syslog auch läuft und bereit ist aus dem Netzwerk Daten zu Empfangen:

```
netstat -lnp|grep syslog
```

hier sollte nun folgendes angezeigt werden:

```
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
5160/syslog-ng
udp        0      0 0.0.0.0:514             0.0.0.0:*
5160/syslog-ng
unix  2      [ ACC ]     STREAM     LISTENING     10323    5160/syslog-ng
/var/lib/syslog-ng/syslog-ng.ctl
```

Logrotate

Damit das Logfile nicht Unendlich groß werden kann richten wir noch eine Rollierung und Kompression der alten Logs nach Linux Standard ein indem wir in der Datei:

```
vi /etc/logrotate.d/syslog-ng
```

folgenden Block am Ende einfügen:

```
/var/www/log/net.log {
   rotate 7
   daily
   compress
   delaycompress
   postrotate
      /usr/sbin/invoke-rc.d syslog-ng reload >/dev/null
   endscript
}
```

CCU2 Einrichten

Damit die CCU2 ihre Systemmeldungen an den Syslog Server weitersendet müsst ihr dort im Web GUI unter

```
Einstellungen / Systemsteuerung / Zentralen Wartung
```

unten im Feld [Syslog-Server Adresse:] die IP Adresse des Syslog Servers eingeben auf dem ihr den Syslog Server soeben Installiert habt.

Nicht vergessen auf [Einstellungen übernehmen] zu Klicken!

Tips

Zum „Mitlesen“ des Syslogs könnt ihr auf einer Konsole einfach:

```
tail -f /var/log/net.log
```

Ausführen und es werden alle Änderungen an der Datei direkt angezeigt, mit der Tastenkombination [STRG] + [C] könnt ihr diese wieder verlassen.