Systemd Journald - Aktivierung des Remotelogging

Hauseigenes Apt-Repo: https://apt.iteas.at 

Seit Systemd ist Journald der Systemlogger. Auch hier ist es wie bei Syslog-NG möglich einen zentralen Loggingserver zu etablieren. Und das wesentlich einfacher als mit dem Urgestein. Im diesen Beispiel bauen wir einen zentralen Journald Server und einen Client. Der Abgleich der Daten erfolgt der einfachhalber heit über HTTP, unverschlüsselt.

Installation der Serverkomponente

Getestet mit Ubuntu 16.04

Also ersters installieren wir uns das Remoteservice nach und erstellen die benötigten Verzeichnisse.

```
apt-get install systemd-journal-remote
mkdir -p /var/log/journal/remote
chown systemd-journal-remote:systemd-journal-remote /var/log/journal/remote
```

Kopieren des Servics und Modifikation.

```
cp /lib/systemd/system/systemd-journal-remote.service /etc/systemd/system/.
```

```
nano /etc/systemd/system/systemd-journal-remote.service
```

Wir änderen hier lediglich die Kommunikationsart.

```
...
-           --listen-https=-3
+           --listen-http=-3
...
```

Nun noch Systemd selbst durch die getätigen Änderungen neu laden, den Service in den Autostart setzen und aktivieren.

```
systemctl daemon-reload
systemctl enable systemd-journal-remote.socket
systemctl start systemd-journal-remote.service
systemctl status systemd-journal-remote.service
```

Um das ganze doch in HTTPS zu verwalten gibt es noch die Konfigurationsdatei `/etc/systemd/journal-remote.conf` . Hier kann die gewünschten Zertifikate setzen. Diese müssen dann natürlich auch am Client vorhanden sein.

Installation des Clients

Getestet mit Ubuntu 16.04

Also ersters installieren wir uns das Remoteservice nach.

```
apt-get install systemd-journal-remote
```

Nun müssen wir der Konfiguration `/etc/systemd/journal-upload.conf` unseren Server eintragen.

```
[Upload]
URL=http://logserver.local:19532
#ServerKeyFile=/etc/ssl/private-journal-upload/journal-upload.pem
#ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
#TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Uploadservice aktivieren und starten:

```
systemctl enable systemd-journal-upload.service
systemctl restart systemd-journal-upload.service
systemctl status systemd-journal-upload.service
```

Und schon hat man den ersten Client der die Logs zentral in Echtzeit ablegt. Schon ne Feine Sache :)

Benutzung/Bedienung

Um nun auf dem Logserver die gewünschten Meldungen zu durchsuchen gelten die selben Regelen wie lokal. Der Unterschied ist das man am Logserver das gesamte Verzeichnis durchsuchen kann (alle Clients) oder einzelne Dateien (jede Datei ein Client).

Ein paar Beispiele

Meldungen des Postfixserver eines bestimmten Clients:

```
journalctl --file remote-2001:430:1e0c:567:425b:14f:cee9:1e1f.journal -u
postfix.service
```

Das komplette Journallog des Clients folgen:

```
journalctl --file remote-2001:430:1e0c:567:425b:14f:cee9:1e1f.journal  -f
```

Alle Clients Live mitsehen, aber nur „Priorität 3“ Meldungen anzeigen:

```
journalctl -D /var/log/journal/remote  -f -p3
```

Suchen nach Datum und Zeit:

```
journalctl --since "2022-12-06 20:00" --until "2022-12-07 03:00" >
${HOSTNAME}_syslog.txt
```

Sehr genau ist auch die Manpage. Wer es gerne ein wenig besser aufbereitet haben möchte und einigen guten Beispielen kann gerne hier nachschauen.

Grafische Tools

Ich habe mich hier mal mit dem Programm Ksystemlog versucht. Installiert aus KDE NEON USER Edition (16.04) Das Programm ist einfach bedienbar, hat eine Fülle von brauchbaren Features und ist top aktuell. Es hat die Möglichkeit auch Remoteserver einzubinden. Dies hat auch funktioniert, leider sehe trotzdem hier keine Logs. Ich werde mich aber diesbezüglich mal schlau machen. Man würde sich mit dem Tool viel Arbeit ersparen.

Lokal hab ich es mal auf Herz und Nieren durch getestet. Ich kann sagen es lässt keine Wünsche offen. Man kann sogar jedes einzelne vorhanden Systemdservice anklicken und Auswerten.

From:
https://deepdoc.at/dokuwiki/ - **DEEPDOC.AT - enjoy your brain**

Permanent link:
https://deepdoc.at/dokuwiki/doku.php?id=server_und_serverdienste:systemd_journald_-_aktivierung_des_remotelogging&rev=1673608995

Last update: **2023/01/13 12:23**