Graylogserver

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

Je verteilter die Anwendungen, umso wichtiger ist die zentrale Logspeicherung. Immer mehr Anwendungen werden in privaten oder öffentlichen Clouds betrieben. Die Anwendungen laufen also nicht mehr auf realen Servern, sondern in virtuellen Maschinen oder Containern. Mit diesem Trend zu leichtgewichtigeren Umgebungen verändert sich auch ihre Lebensdauer. Anstatt einen Server immer wieder manuell zu hegen und zu pflegen, werden Container oder virtuelle Maschinen direkt neu erstellt und alte Versionen gelöscht. Ohne ein zentrales Logmanagement gehen die Logs der Anwendungen also verloren und damit auch eine wichtige Informationsquelle, die gebraucht wird, um Development und Operations bei der Untersuchung von Fehlern zu unterstützen.

Gleichzeitig beobachten wir eine Entwicklung, die von Applikationsservern und monolithischen Applikationen weggeht hin zu verteilten Anwendungen, bei denen jede Business-Capability von einem eigenen Microservice umgesetzt wird. Gerade in verteilten Umgebungen ist es für den Betrieb und die Softwarewartung schwierig, Anfragen über verschiedene Knoten zu verfolgen und in den einzelnen Applikationslogs nach Hinweisen zu suchen. Traditionell müssen sich die Administratoren dazu an jedem Knoten anmelden und dann die Logs durchforsten oder sie manuell zusammentragen. Das ist zeitaufwändig und skaliert nicht.

Genau an dem Punkt kommt Graylog in's Spiel. Mit Graylog ist es ein leichtes Logs zentral von den verschiedensten Geräten zu verwalten.

Installation auf Ubuntu 18.04

Offizell nur für Debian 9 und Ubuntu 16.04 gültig. Funktioniert aber auch einwandfrei mit 18.04. Offizelle Anleitung hier. Vorausetzung ist unter anderem Java und MongoDB.

```
apt update
apt install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen
apt install mongodb
systemctl daemon-reload
systemctl enable mongod.service
systemctl restart mongod.service
```

Elasticsearch

Graylog 2.5.x sollte mit Elasticsearch 6.x verwendet werden.

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add
-
echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | tee -
a /etc/apt/sources.list.d/elastic-6.x.list
```

```
apt update && apt install elasticsearch
```

Stelle sicher dass, das Konfigurationsfile `/etc/elasticsearch/elasticsearch.yml` und der „cluster name“ auf „graylog“ gesetzt wird. Und/oder kommentiere die Zeile ein:

```
cluster.name: graylog
```

Nach der Konfiguration kann man Elasticsearch starten:

```
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl restart elasticsearch.service
```

Installation von Graylog selbst

Nun kann man Graylog mit dem Repo installieren.

```
wget
https://packages.graylog2.org/repo/packages/graylog-2.5-repository_latest.de
b
dpkg -i graylog-2.5-repository_latest.deb
apt update && apt install graylog-server
```

Als erstes konfiguriert man Graylog in der Datei `/etc/graylog/server/server.conf` und fügt die Optionen `password_secret` (pwgen -N 1 -s 96) und `root_password_sha2` hinzu. Diese Optionen sind verpflichtend. Ohne diese startet Graylog nicht.

Um `root_password_sha2` zu generieren bedienst man sich z.B. folgendem Befehle:

```
echo -n "Enter Password" && head -1 </dev/stdin | tr -d '\n' | sha256sum |
cut -d" " -f1
```

Das Passwort wird mit dem Benutzer „admin“ mit den Login am Webinterface http://FQDN:9000 verwendet.

`password_secret` laut Anleitung in der Konfigdatei generieren. Danach sind noch die 3 Zugriffe für Graylog zu konfigurieren:

```
web_listen_uri = http://fqdn:9000/
rest_listen_uri = http://fqdn:9000/api/
rest_transport_uri = http://fqdn:9000/api/
```

Und den Server starten:

```
systemctl daemon-reload
systemctl enable graylog-server.service
systemctl start graylog-server.service
```

Übertragen von Logs zu Graylog

Das Prinzip funktioniert gleich wie bei syslog/rsyslog. Am Graylogserver gibt es jede Menge Inputs/Plugins. Syslog ist eines davon und muss im Webinterface aktiviert werden. „System –> Notes –> Note auswählen –> Manage Inputs“. Normalerweise würde man Sysloginput auf Port 514 (Defaul) konfigurieren. Leider kann man dann nur als Root darauf zugreifen. Wir haben nun die Möglichkeit mit IPtables das Port um zu mappen, z.B.

```
iptables -t nat -A PREROUTING -p tcp --dport 514 -j REDIRECT --to 1514
iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to 1514
```

Oder wir setzen das Port am Input gleich auf 1514 UDP. Das ist die einfachste Lösung.

Konfiguration des Clients

Auf Linux muss Rsyslog installiert und folgendes Konfig gesetzt werden:

```
nano /etc/rsyslog.d/51-remote.conf

*.* @FQDN.bla.local:1514;RSYSLOG_SyslogProtocol23Format
```

Nun noch den Dienst durchstarten:

```
systemctl restart rsyslog.service
```

Danach werden die Logs bereits übertragen. Drucker, Switch, Fortigate und usw. sind da auch ganz einfach zu konfigurieren.