rsyslog

rsyslog är installerat per default. rsyslog är en Linux-tjänst som hanterar skickande och/eller mottagande av syslog. Saknas den så installera med `apt install rsyslog`.

Redigera filen `/etc/rsyslog.conf`. Lägg här till en rad i stil med *.* @syslog.domain.net:514. rsyslog använder sig av TCP 514.

Vid förändringar i filen måste tjänsten startas om med `sudo service rsyslog restart`. Kontrollera tjänstens status med `sudo service rsyslog status`.

Exempelkonfiguration, skicka loggfiler

Här är en exempelkonfiguration på hur rsyslog kan skicka loggfiler över UDP 514.

```
! Lägg först till nedan modul i /etc/rsyslog.conf
module(load="imfile" PollingInterval="10")

! Skapa ny konffil /etc/rsyslog.d/ för applikationen
# Definiera en mall för syslog
template(name="TraditionalFormatWithHost" type="string" string="%timegenerated% %HOSTNAME%
%syslogtag%%msg%\n")

# Lägg till inputs för dina loggfiler från olika mappar
input(type="imfile"
      File="/data/docker/dns1/dnsserver_config/_data/logs/*.log"
      Tag="app-dns1"
      Severity="info"
      Facility="local0")

input(type="imfile"
      File="/data/docker/ntp1/_data/logs/*.log"
      Tag="app-ntp1"
      Severity="info"
```

```
      Facility="local0")

# Dynamisk vidarebefordran till Graylog för alla taggar som börjar med "app-"
if $programname startswith 'app-' then {
    action(
        type="omfwd"
        Target="graylog-docker.jehrlander.net"
        Port="514"
        Protocol="udp"
        template="TraditionalFormatWithHost"
    )
    stop
}

! Apparmor blockerar per default tillgång till mapparna för rsyslog. Den behöver ha åtkomst till överliggande mappar. Lägg till mapparna i  /etc/apparmor.d/usr.sbin.rsyslogd, ex:
/data/docker**
/data/docker/dns1/dnsserver_config/_data/logs/* r,

! Ladda om apparmor därefter
sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.rsyslogd
```

Verifiera med `sudo tail -f /var/log/syslog | grep rsyslog`. Starta om rsyslog med `sudo systemctl restart rsyslog` vid behov och förändringar.

Revision #10
Created 7 May 2025 09:32:56 by Jehrlander
Updated 5 February 2026 14:52:20 by Jehrlander