Rsyslog-Server unter Debian 11 (Bullseye)

Was wollen wir?

Protokolldateien sind entscheidend für die Untersuchung und Fehlerbehebung von Fehlern. Sie sind die ersten Dateien, die Systemadministratoren untersuchen, um die wahrscheinliche Ursache eines Fehlers einzugrenzen und auf diese Weise Lösungen zur Behebung des Problems zu finden. In einer Infrastruktur mit Dutzenden oder Hunderten von Servern und anderen Geräten kann die Verwaltung von Protokolldateien eine Herausforderung darstellen. Und hier kommt rsyslog ins Spiel.

Warum wollen wir das?

Rsyslog ist ein Open-Source-Protokollierungsprogramm, das die Weiterleitung von Protokolldateien an einen zentralen Protokollserver in einem IP-Netzwerk erleichtert. Mit der zentralisierten Protokollierung können Administratoren die Protokolldateien mehrerer Systeme einfach von einem zentralen Punkt aus im Auge behalten. In diesem Beitrag führen wir dich durch die Installation und Konfiguration von Rsyslog Server auf Debian 11.

Lab Setup

Um zu demonstrieren, wie Rsyslog verwendet werden kann, um Protokolldateien von einem Clientsystem an den Rsyslog-Server zu senden, werden wir ein einfaches Lab-Setup wie gezeigt haben

- Rsyslog-Server: Debian 11 IP: 192.168.1.8

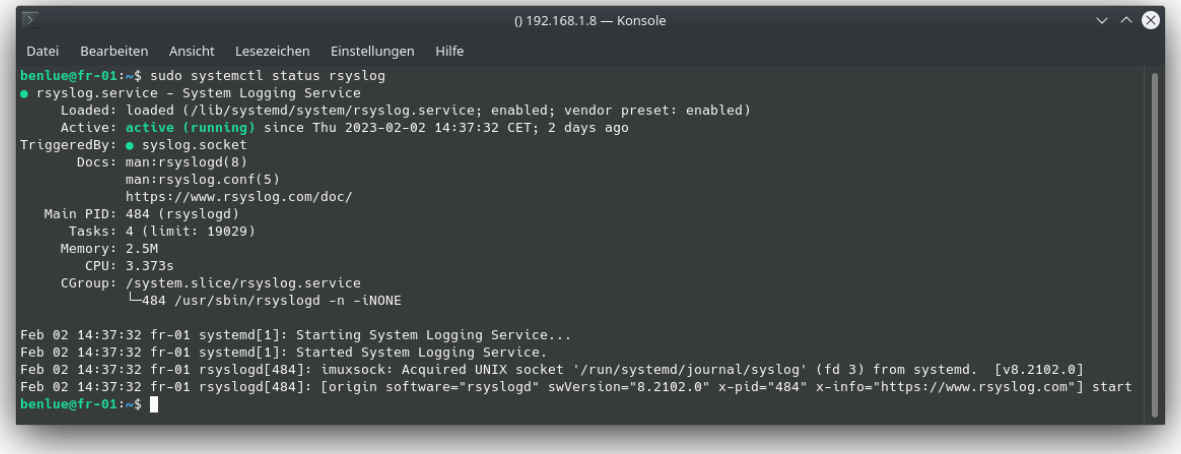
Schritt 1) Konfigurieren Sie Rsyslog auf dem Server

Wie bereits erwähnt, arbeitet Rsyslog in einem Client-Server-Modell, und wir beginnen mit der Konfiguration von Rsyslog auf dem Debian 11-Server. Unter Debian 11 wird Rsyslog standardmäßig installiert. Wenn Rsyslog aus irgendeinem Grund nicht vorhanden ist, können Sie es mit dem folgenden Befehl installieren:

```
$ sudo apt install -y rsyslog
```

Nach der Installation können wir den Betriebsstatus wie folgt überprüfen:

```
$ sudo systemctl status rsyslog
```



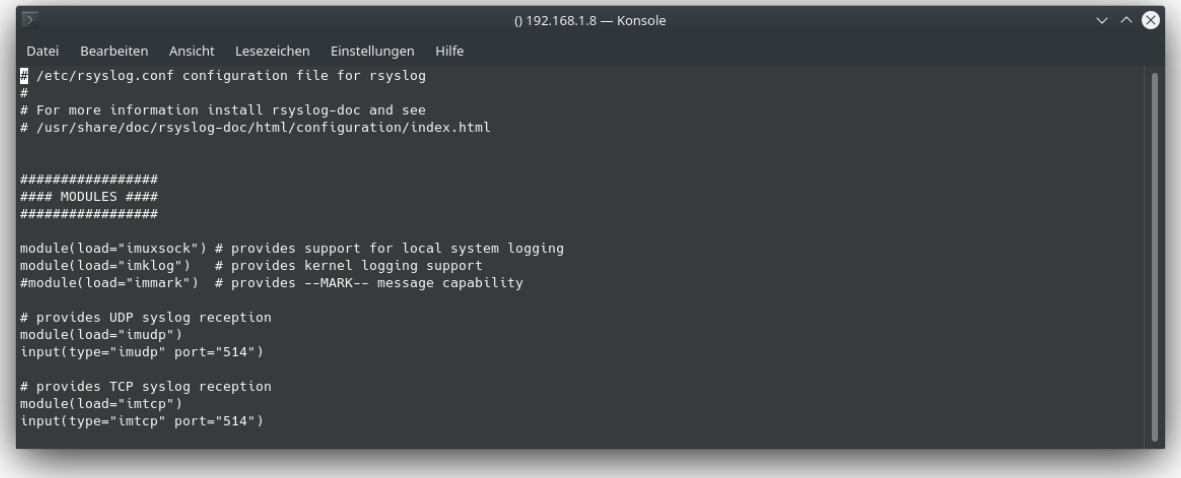
Als Nächstes konfigurieren wir rsyslog für die Ausführung im Servermodus. Die Konfigurationsdatei ist die Datei /etc/rsyslog.conf . Bearbeiten Sie es also mit Ihrem bevorzugten Texteditor.

```
$ sudo vi /etc/rsyslog.conf
```

Kommentiere die folgenden Zeilen aus, die den UDP- und TCP-Syslog-Empfang von Remote-Clients ermöglichen.

Code: /etc/rsyslog.conf

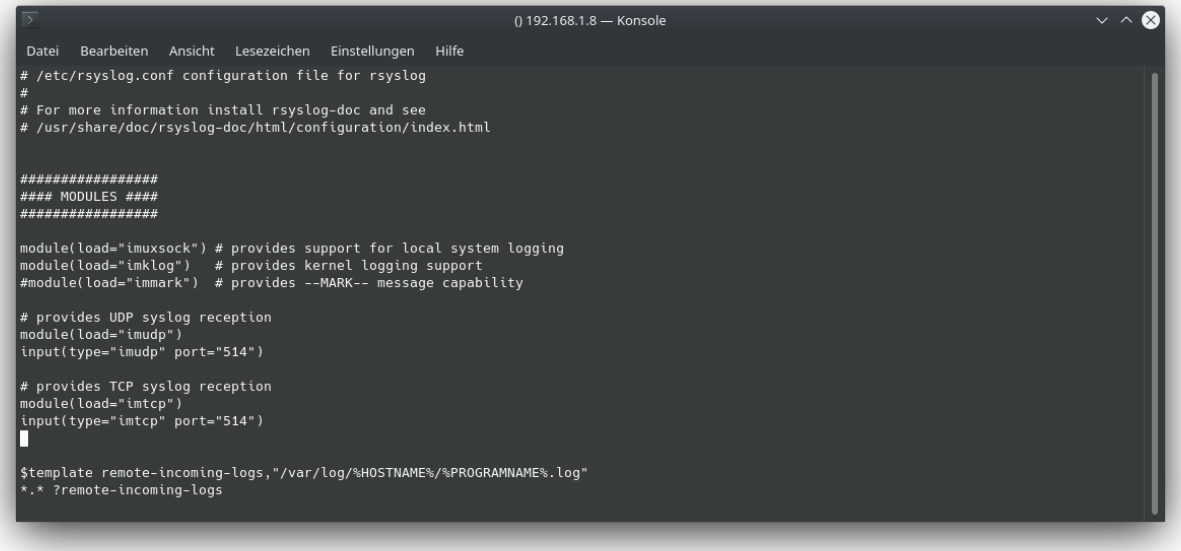
```
#          stellt          das          UDP-Syslog-Empfangsmodul          bereit
(load="imudp")
input(type="imudp"                                                    port="514")

#          stellt          das          TCP-Syslog-Empfangsmodul          bereit
(load="imtcp")
input(type="imtcp" port="514 ")
```



Füge danach die folgenden Zeilen ein, um die Vorlage zu definieren, die der Rsyslog-Daemon verwendet, um eingehende Protokolle von Client-Systemen zu speichern.

Code

```
$template            remote-incoming-logs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?remote-incoming-logs
```



Die Protokolldateien verwenden die folgende Namenskonvention:

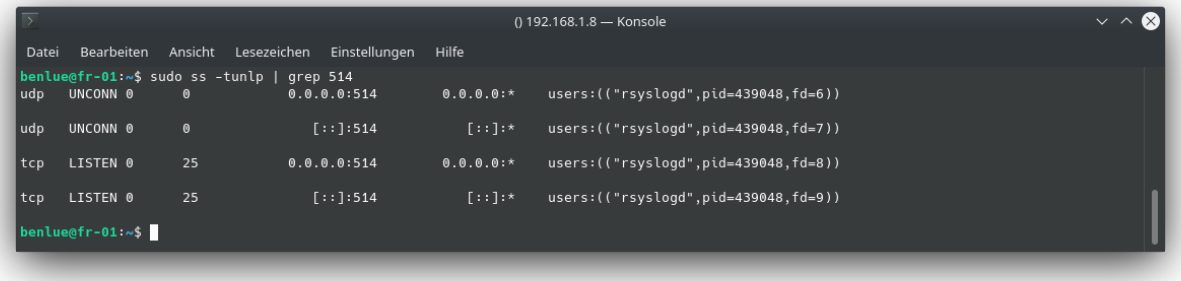
- /%HOSTNAME%/ – Dies ist der Hostname des Client-Systems.
- /%PROGRAMNAME%/ – Dies identifiziert das Client-Programm, das die Protokolldatei erstellt hat.

Um die Änderungen zu übernehmen, starte den rsyslog-Daemon neu.

```
$ sudo systemctl restart rsyslog
```

Standardmäßig lauscht rsyslog auf Port 514

```
$ sudo ss -tunlp | grep 514
```



Schritt 2) Konfiguriere die Firewall-Regeln für rsyslog

Der Rsyslog-Daemon wird wie erwartet auf dem Server ausgeführt. Wenn du eine UFW-Firewall ausführst, achte darauf, dasss Port 514 zuzulassen wird um eingehende Protokollnachrichten zuzulassen.

```
$ sudo ufw allow 514/tcp
$ sudo ufw allow 514/udp
```

Lade dann die Firewall neu, um die Firewall-Regel wie folgt anzuwenden.

```
sudo ufw reload
```

Disclaimer:

WIe immer gilt: Alle Anleitungen/Tutorials sind nach bestem Wissen und Gewissen verfasst, gehen immer von den definierten Software/Firmware-Versionen aus und sind auf das englische GUI ausgelegt.

Es gibt keine Garantie auf Erfolg. Im Falle eines Misserfolges hilft aber die Community hier sicherlich weiter.

Keiner der Autoren oder der Betreiber des Forums ist für die aus der Nutzung resultierenden Probleme/Herausforderungen verantwortlich.

Jegliche hier beschriebenen Schritte erfolgen ausnahmslos in eigener Verantwortung des Durchführenden.

Eltern haften für ihre Kinder.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!