Linux - Setting up a Logging Server

Summary

This is to setup a logging server to capture logs from any servers on your network.

Prerequisites

Install of a RedHat or Rocky Linux minimal install

Configuration

You will need to edit the file "/etc/rsyslog.conf"

Editing the file

```
vi /etc/rsyslog.conf
```

You will need to change to the following to allow port 514 to be open

```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

Then simply restart the rsyslog deamon

```
systemctl restart rsyslog
```

Multi Host Logging to one server

```
vi /etc/rsyslog
```

Add the following

Before this entry "#### RULES ####"

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
. ?RemoteLogs
```

This will enable for all host/servers to log to their own folders

The entry should look like this

```
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")

#custom
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~

#### RULES ####
```

The directive $template tells , rsyslog daemon to gather and write all of the received remote messages to seperate logs under /var/log, based on the hostname (client machine name) and remote client facility (program/application) that generated the messages as defined by the settings present in the template RemoteLogs. The second line “*.* ?RemoteLogs” means record messages from all facilities at all severity levels using the RemoteLogs template configuration. The third lines makes the append happen.

Setup Log Rotate

Create a log file configuration file

```
vi /etc/logrotate.d/sfl
```

then add the following, and change the ending folder name(s)

```
/var/log/sfl*
/var/log/SFL*
/var/log/vcenter*
/var/log/MFB*
/var/log/mfb*
{
    rotate 2
    maxsize 200k
    daily
}
```

Run to make sure the config is good

```
logrotate -d /etc/logrotate.d/sfl
```

Setup Host Servers

This is what to setup on the servers you wish to log to one server

You must login to the server and then edit the following file

```
vi /etc/rsyslog.conf
```

Once opened you have to add at the end of the file the following to log everything

```
*.* @192.168.253.86:514    # use @ for UDP Protocal
*.* @@192.168.253.86:514    # use @@ for TCP Protocal
```

You can also setup specific logging by doing the following

```
auth.* @192.168.253.86:514    # only for authentication based records
```

Results

This is what your folder will look like with the host name of the server or device

```
drwx------  2 root   root       42 Aug 29 22:30 RT-AC5300-RANGE-25D1EC7-C
drwx------  2 root   root       82 Aug 29 22:32 SFL-LIN-000
drwx------  2 root   root       87 Aug 29 22:32 sfl-web-004
```

This is a look within a folder of a server

```
[/var/log]# cd SFL-LIN-000/


root@SFL-LIN-000.ONLING.COM : Linux : Thu Aug 29 22:35:01 :
[/var/log/SFL-LIN-000]# ls -lrt
total 16
-rw------- 1 root root 850 Aug 29 22:30 rsyslogd.log
-rw------- 1 root root  56 Aug 29 22:32 sssd_kcm.log
-rw------- 1 root root 948 Aug 29 22:32 systemd.log
-rw------- 1 root root 251 Aug 29 22:32 CROND.log
```

Revision #8
Created 30 August 2024 00:36:28 by Steve Ling
Updated 27 November 2024 01:21:02 by Steve Ling