Add rsyslog server functionality to Linux

27.10.23

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

Add rsyslog server functionality to Linux

Overview

To receive logs from other hosts we can set up rsyslog to receive logs from other hosts. It's been explained in various ways various sites, which is a bit confusing so here is one that is most straightforward and works for me, as simply put as possible. This is an UDP setup and it is done with CentOS / RHEL 7.

Note that this adds logging per host (including localhost) under /var/log/remote in addition to your existing logging so it will increase your log partition usage. If you want to replace the existing logs with this solution you must apply a stop rule at the /etc/rsyslog.conf. I did not explore that so if you do please leave a message here so I can update this guide accordingly.

Log directory

Make a directory and relabel (selinux) it for syslog use

```
mkdir /var/log/remote
chcon --reference /var/log /var/log/remote
```

Rsyslog configuration

Edit /etc/rsyslog.conf so that before UDP syslog configuration you add this new template configuration:

```
$template RemoteLog, "/var/log/remote/%HOSTNAME%/%programname%.log"
*.* -?RemoteLog
```

After which you uncomment the UDP syslog reception lines:

```
$ModLoad imudp
$UDPServerRun 514
```

Firewall

Open UDP port 514 to the hosts you want to receive log from. I use iptables so I added this line to /etc/sysconfig/iptables

```
-A INPUT -p udp -m udp --dport 514 -s 192.168.120.0/24 -j ACCEPT
```

After which reload iptables with

```
systemctl restart rsyslog
```

Start using

Restart rsyslog

```
systemctl restart rsyslog
```

And you should start getting /var/log/remote/<hostname> directories under which the log files appear.

Comments

All comments and corrections are welcome.