**Setup SysLog Server on CentOS 6 / RHEL 6**

Today we will be looking into how to setup a centralized log management for Linux servers, this will help the Linux admin to have a multiple server logs into one single place. The Linux admin not required to login in to each servers for checking the logs, he can just login into the centralized server and start do the logs monitoring.

Linux labels (auth, cron, ftp, lpr, authpriv, news, mail, syslog, etc ,..) the log messages to indicate the type of software that generated the messages with severity (Alert, critical, Warning, Notice, info, etc ,..).

Make sure you have the following to setup log server.

**Two Linux servers ( server and client).**

**server.example.local 192.168.0.105**

**client.example.local  192.168.0.104**

### **Server setup:**

**Install syslog package, if you do not have it installed.**

[root@server ~]# yum -y install rsyslog

**Edit /etc/rsyslog.conf**

[root@server ~]# yum -y install rsyslog

**Uncomment the following to enable the syslog server to listen on the tcp and udp port.**

**From**

# Provides UDP syslog reception

#$ModLoad imudp

#$UDPServerRun 514

# Provides TCP syslog reception

#$ModLoad imtcp

#$InputTCPServerRun 514

**To**

# Provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514

# Provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

**Restart the syslog service**

[root@server ~]# service rsyslog restart

**Verify the syslog server listening.**

[root@server ~]# netstat -antup | grep 514

tcp 0 0 0.0.0.0:514 0.0.0.0:\* LISTEN 8081/rsyslogd

tcp 0 0 :::514 :::\* LISTEN 8081/rsyslogd

udp 0 0 0.0.0.0:514 0.0.0.0:\* 8081/rsyslogd

udp 0 0 :::514 :::\* 8081/rsyslogd

### **Client setup:**

**Edit /etc/rsyslog.conf**

[root@client ~]# vi /etc/rsyslog.conf

**At the end of file place the following line to point the client message log to the server**

\*.info;mail.none;authpriv.none;cron.none @192.168.0.105

**You can either mention hostname or ip address.**

**Restart the syslog service**

[root@client ~]# service rsyslog restart

**Now all the message logs are sent to the central server and also it keeps the copy locally.**

### **Firewall Port opening (Optional):**

**Mostly all the production environment are protected by hardware firewall, ask them to open the TCP & UDP 514. You can verify the port opening by issuing the following command from the client.**

[root@client ~]# telnet 192.168.0.105 514

Trying 192.168.0.105...

Connected to 192.168.0.105.

Escape character is '^]'.

If it didn’t give any reply, disable firewall on both client and server.

### **Test:**

**Monitor the activity from the log server, open the message log.**

[root@server ~]# tailf /var/log/messages

**Now restart xinetd service on client, Now you can get the service restart message on the syslog server.**

Oct 17 15:06:41 client xinetd[4280]: xinetd Version 2.3.14 started with libwrap loadavg labeled-networking options compiled **in**.

Oct 17 15:06:41 client xinetd[4280]: Started working: 0 available services

**By this way you can monitor the other logs such as secure, mail, cron logs etc.**