SOP OF SYSLOG SERVER

10.128.3.17 SIDCSYSLOG01

10.128.3.16 SIDCSYSLOG02

Live Log file : /var/log/syslog-ng.log

Syslog path of all devices

Path : /var/log/syslog-ng/X.X.X.X.

IDC syslog configuration

Crontab for Log rotation on both Servers

```
-bash-4.1# crontab -l
05  01 * * * /home/logrotate
-bash-4.1#
```

# How to put Any device ip for Log rotation

File /home/logrotate open the file and the end add entry as per below screen shot.

```
cd /var/log/syslog-ng/10.22.30.159/old
find -mtime +35 -exec rm {} \;
cd /var/log/syslog-ng/10.22.30.159/
gzip messages
mv messages.gz /var/log/syslog-ng/10.22.30.159/old/messages-`date +"%Y%m%d"`.gz
```

Step 3: And then create the directory as

mkdir /var/log/syslog/IP/old

# How to View New Log Entries as They Happen

Pointed N/w divice ip are Located in

/var/log/syslog-ng/X.X.X.X/messages

# Troubleshooting queries

Log not generating

Ip need to configured for log rotation

Partion full.

User creation and addition in to group