**REDHAT 5 – SYSLOG**

**SYSLOG**

**Introduction**

There are hundreds of Linux applications on the market, each with their own configuration files and help pages. This variety makes Linux vibrant, but it also makes Linux system administration daunting. Fortunately, in most cases, Linux applications use the syslog utility to export all their errors and status messages to files located in the /var/log directory.

This can be invaluable in correlating the timing and causes of related events on your system. It is also important to know that applications frequently don’t display errors on the screen, but will usually log them somewhere. Knowing the precise message that accompanies an error can be vital in researching malfunctions in product manuals, online documentation, and Web searches.

syslog, and the logrotate utility that cleans up log files, are both relatively easy to configure but they frequently don’t get their fair share of coverage in most texts. I’ve included syslog here as a dedicated chapter to both emphasize its importance to your Linux knowledge and prepare you with a valuable skill that will help you troubleshoot all the Linux various applications that will be presented throughout the book

**syslog**

syslog is a utility for tracking and logging all manner of system messages from the merely informational to the extremely critical. Each system message sent to the syslog server has two descriptive labels associated with it that makes the message easier to handle.

* The first describes the function (facility) of the application that generated it. For example, applications such as mail and cron generate messages with easily identifiable facilities named mail and cron.
* The second describes the degree of severity of the message. There are eight in all and they are listed in Table 5-1:

You can configure syslog’s /etc/rsyslog.conf configuration file to place messages of differing severities and facilities in different files. This procedure will be covered next.

**The /etc/syslog.conf File**

The files to which syslog writes each type of message received is set in the /etc/rsyslog.conf configuration file. In older versions of Fedora this file was named /etc/syslog.conf.

This file consists of two columns. The first lists the facilities and severities of messages to expect and the second lists the files to which they should be logged. By default, RedHat/Fedora’s /etc/rsyslog.conf file is configured to put most of the messages in the file /var/log/messages.

**Activating Changes to the syslog Configuration File**

In versions of Redhat5 and Centos, this would be:

[root@bigboy tmp]# service syslog restart

**How to View New Log Entries as They Happen**

If you want to get new log entries to scroll on the screen as they occur, then you can use this command:

[root@bigboy tmp]# tail -f /var/log/messages

Similar commands can be applied to all log files. This is probably one of the best troubleshooting tools available in Linux. Another good command to use apart from tail is grep. grep will help you search for all occurrences of a string in a log file; you can pipe it through the more command so that you only get one screen at a time. Here is an example:

[root@bigboy tmp]# grep string /var/log/messages | more

You can also just use the plain old more command to see one screen at a time of the entire log file without filtering with grep. Here is an example:

[root@bigboy tmp]# more /var/log/messages

**Configuring the Linux Syslog Server**

By default syslog doesn’t expect to receive messages from remote clients. Here’s how to configure your Linux server to start listening for these messages.

As we saw previously, syslog checks its /etc/syslog.conf file to determine the expected names and locations of the log files it should create. It also checks the file /etc/sysconfig/syslog to determine the various modes in which it should operate. Syslog will not listen for remote messages unless the SYSLOGD\_OPTIONS variable in this file has a -r included in it as shown below.

# Options to syslogd

# -m 0 disables 'MARK' messages.

# -r enables logging from remote machines

# -x disables DNS lookups on messages received with -r

# See syslogd(8) for more details

SYSLOGD\_OPTIONS="-m 0 -r"

# Options to klogd

# -2 prints all kernel oops messages twice; once for klogd to decode, and

# once for processing with 'ksymoops'

# -x disables all klogd processing of oops messages entirely

# See klogd(8) for more details

KLOGD\_OPTIONS="-2"

You will have to save and restart syslog on the server for the changes to take effect.

**Configuring the Linux Client**

The syslog server is now expecting to receive syslog messages. You have to configure your remote Linux client to send messages to it. This is done by editing the /etc/hosts file on the Linux client named smallfry. Here are the steps:

1) Determine the IP address and fully qualified hostname of your remote logging host.

2) Add an entry in the /etc/hosts file in the format:

IP-address fully-qualified-domain-name hostname "loghost"

Example:

192.168.1.100 bigboy.my-site.com bigboy loghost

Now your /etc/hosts file has a nickname of “loghost” for server bigboy.

3) The next thing you need to do is edit your /etc/syslog.conf file to make the syslog messages get sent to your new loghost nickname.

\*.debug @loghost

\*.debug /var/log/messages

You have now configured all debug messages and higher to be logged to both server bigboy (“loghost”) and the local file /var/log/messages. Remember to restart syslog to get the remote logging started.

You can now test to make sure that the syslog server is receiving the messages with a simple test such as restarting the lpd printer daemon and making sure the remote server sees the messages.

**Linux Client**

[root@smallfry tmp]# service lpd restart

Stopping lpd: [ OK ]

Starting lpd: [ OK ]

[root@smallfry tmp]#

**Linux Server**

[root@bigboy tmp]# tail /var/log/messages

...

...

Apr 11 22:09:35 smallfry lpd: lpd shutdown succeeded

Apr 11 22:09:39 smallfry lpd: lpd startup succeeded

...

...

[root@bigboy tmp]#

**Conclusion**