CHAPTER 5

Logging Syslog Messages to Remote Linux Server

This chapter describes how to forward the Syslog messages to a destination (for example, *server-syslog*) from a linux client that runs the Configuration Engine software application (for example, *oer-host*).

Step 1 Configuring the Linux Syslog Server (server-syslog) to receive messages.

By default, Syslog does not expect to receive messages from remote clients. Here is how to configure your Linux server to start listening for these messages.

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 an **-r** included in it as shown below.

Here is an example of how to configure the */etc/sysconfig/syslog* file to receive the Syslog messages.

```
# 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"
```

Here is how the */etc/syslog.conf* file should look on the Syslog Server:

***.debug /var/log/messages**

Step 2 You must restart Syslog on the server for the changes to take effect.

The server now listens on UDP port 514, which you can verify using either one of the following netstat command variations:

/etc/init.d/syslog restart

[root@server-syslog tmp]#

Note Make sure that your destination Syslog server is configured to receive the messages from another host by specifying the **-r** option.

Step 3 Configuring the Linux Client:

a. The Syslog server (*server-syslog*) is now expecting to receive Syslog messages.

b. Configure your remote Linux client to send messages to the Syslog server.

This is done by editing the */etc/hosts* file on the Linux client named *oer-host*:

- Determine the IP address and fully qualified hostname of your remote logging host.
- Add an entry in the */etc/hosts* file in the format:

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

For example:

```
10.10.10.1      server-syslog.domain.com server-syslog    loghost
```

Now your */etc/hosts* file has a nickname of "loghost" for the *server-syslog* server.

Step 4 Edit the */etc/syslog.conf* file to send Syslog messages to your new "loghost" nickname.

```
*.debug                 @loghost
*.debug                 /var/log/messages
```

In this example all information messages and higher are being logged to both *server-syslog* server ("loghost") and the local */var/log/messages* file.

Step 5 Restart Syslog:

/etc/init.d/syslog restart

Step 6 Run a test to verify that the destination Syslog server is receiving the messages in the */var/log/messages* file. Every Configuration Engine message has the "OER_MC" tag attached.

Summary

The following files must be modified on the destination server:

- */etc/sysconfig/syslog*
- */etc/syslog.conf*

The following files must be modified on the client sending the messages to the server:

- */etc/hosts*
- */etc/syslog.conf*

Note For more information on rules for logging into Syslog, see the Linux manual.
At the command prompt, enter: **man syslog.conf**.