CHAPTER 5

Configuring the Syslog Utility to Receive Cisco BAC Alerts

This chapter explains how to configure the syslog daemon after you install the Cisco Broadband Access Center (BAC). In case of a local data server, you can configure the syslog utility on any Cisco BAC component server to receive alerts from the system. For receiving the syslogs in a centralized server from all the BAC components such as RDU, DPE, CNR and KDC, you can configure the syslog daemon either on any Cisco BAC component server or on a separate server. These component servers are referred as Cisco server in this chapter.

Note Configuring the syslog file is an optional task.

Syslog is a client-server protocol that manages the logging of information on UNIX. Cisco BAC generates alerts through the syslog service. Cisco BAC syslog alerts are not a logging service; they notify that a problem exists, but do not necessarily define the specific cause of the problem.

The information related to the problem resides in the appropriate Cisco BAC log files, rdu.log and dpe.log. If you choose to configure the syslog file, syslog alerts are directed to a separate log file.

For more information on error messages and alerts, refer to the *Cisco Broadband Access Center 3.8 Administrator Guide*.

Configuring Syslogs on a Local Server

To configure the syslog utility on Solaris and Linux servers:

Step 1 Log in as *root* on the server.

Step 2 At the command line, create the log file.

For example:

```
# touch /var/log/bac.log
```

Step 3 Open the /etc/syslog.conf file with a text editor, such as *vi*.

Step 4 Add the following lines to the /etc/syslog.conf file:

```
local6.alert        /var/log/bac.log
local6.info         /var/log/bac.log
```

Note You must insert one or more tabs between the local6:info and */var/log/bac.log* information.

Step 5 Save and close the /etc/syslog.conf file.

Step 6 To force the syslog utility to take the new configuration, at the command line, enter:

```
# ps -ef  | grep syslogd
   root      217   1    0     Nov   26      ?    0:00      /usr/sbin/syslogd

   kill -HUP 217
```

Note The process ID (PID) in this example is 217, but may change when you run **ps -ef | grep syslogd**. Use the correct output from that command as the input to **kill -HUP**.

Syslog is now ready to receive alerts from Cisco BAC.

Configuring Centralized Solaris Server to Receive Syslogs

On Solaris machines, the LOG_FROM_REMOTE property specifies whether server messages are logged. By default, this property is enabled.

To configure a centralized server to receive syslog alters:

Step 1 Log into the server as root.

Step 2 By default the LOG_FROM_REMOTE property is enabled. In case it is not, you can enable it by setting it's value to true as shown in the following commands.

```
# svccfg -s svc:/system/system-log setprop config/log_from_remote = true
# svcadm refresh svc:/system/system-log
```

Step 3 Create a dummy file.

```
# touch /var/log/messages
```

Step 4 Add the following configuration in /etc/syslog.conf file:

```
local6.info             @loghost
local6.info             /var/log/messages
```

Step 5 Restart the syslog daemon.

```
# svcadm restart system-log
# tail -f /var/log/messages
```

Note Always use Tab while modifying /etc/syslog.conf. Using the space bar shows errors while you restart syslogd.

Configuring a Server to Send Syslog to Centralized Server on Solaris

After you configure syslog daemon on a centralized server, you must configure the Cisco BAC server to send messages to the centralized server. To do this, edit the /etc/hosts file on the server as explained below.

Step 1 Determine the IP address and fully qualified host name of the server logging host.

Step 2 Log into the server as *root*.

Step 3 To enable the server logging hostname, add the following entry in the /etc/hosts file:

For example;

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

The /etc/hosts file has the nickname loghost, for the server.

Step 4 Edit the /etc/syslog.conf file to send the syslog messages to the server.

For example;

```
local6.info    ifdef(`LOGHOST', /var/log/messages, @loghost)
```

Step 5 Restart the syslog daemon to get the server logging started.

```
# svcadm restart system-log
```

To test whether the syslog server is receiving the messages, stop the RDU server. The DPE and CNR servers will send a message indicating the connection failure.

Configuring Centralized Linux Server to Receive Syslogs

By default, syslog daemon on a centralized server does not expect to receive messages from the Linux Cisco BAC servers. You must configure the centralized server for the syslog daemon to start listening to these messages.

The syslog daemon checks the /etc/rsyslog.conf file to determine the expected names and locations of the log files it should create. It also checks whether the UDP syslog reception is configured in this file, as shown below:

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514
:FROMHOST-IP, isequal, "ipaddress" /var/log/rhel6.log
```

In the above line, replace *ipaddress* with the IP-address of the the client that will send message to the centralized Linux server, and replace *rhel6.log* with the intended log file name.

You must restart the syslog daemon for the changes to take effect:

```
/sbin/service rsyslog restart
```

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

```
netstat -an | grep udp | grep 514
```

The expected output for the above command is:

```
udp        0      0 0.0.0.0:514                 0.0.0.0:*
udp        0      0 :::514                      :::*
```

Configuring a Server to Send Syslog to Centralized Server on Linux

After you configure syslog daemon on the centralized server, you must configure the Cisco BAC server to send messages to it. To do this, edit the two files – /etc/hosts and /etc/rsyslog.conf – on the Cisco BAC server.

Step 1 Determine the IP address and fully qualified hostname of the server logging host.

Step 2 Log in as *root* on the server

Step 3 To enable the server logging hostname, add the following line in the /etc/hosts file (using vi editor):

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

In the above line, replace *IP-address* with the IP address of the centralized server to which the messages will be sent, and also replace *fully-qualified-domain-name* and `hostname` with the respective values for the centralized server.
`loghost` is an example of an optional nickname that you can use for the server, `hostname`.

Step 4 Edit the /etc/rsyslog.conf file (using vi editor) to add the following lines, to send the syslog messages to the centralized server:

```
local6.info             @loghost
local6.info             /var/log/messages
```

In the above lines, replace *loghost* with the actual nickname of the centralized server as entered in Step 3. Instead, if you have not configured the nickname, you can replace `loghost` with the hostname.

Step 5 Restart the syslog daemon to start server logging:

```
/sbin/service rsyslog restart
```

To test whether the syslog server is receiving the messages, stop the RDU server. The DPE and CNR servers will send a message indicating the connection failure.