CHAPTER 23

Logging Syslog Messages

Logging messages via syslog provides centralized error reporting for Cisco Access Registrar. Local logging and syslog logging can be turned on or off at any time by modifying the control flags in the **$INSTALLPATH/conf/car.conf** file.

Logging syslog messages requires a UNIX host running a ***syslog daemon*** as a receiver for Cisco AR messages. Cisco AR and the syslog daemon can be running on the same host or different hosts.

This chapter has the following sections:

syslog Messages

Messages sent to the following logs will be forwarded to **syslog** server in a slightly different format. The logs are:

- aregcmd_log
- config_mcd_[1..n]_log
- name_radius_[1..n]_log
- agent_server_[1..n]_log

Messages less than 1024 bytes in length display in the following format:

```
MMM DD hh:mm:ss hostname %CAR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description
```

Where:

MMM DD is the month and date that the message is received by the syslog server.

hh:mm:ss is the arrival time of the message.

hostname is the name of the syslog server.

severity is one of the following levels:

0 - emergency

1 - alert

2 - critical

3 - error

4 - warning

5 - notification

6 - informational

7 - debugging

mnemonic can be ***aregcmd***, ***name_radius***, ***agent_server*** and ***config_mcd*** for the identification of AR-relative subsystems.

#n is the id for the components: ***name_radius***, ***agent_server***, and ***config_mcd***

message_description provides detailed information of the message.

Messages greater than 1024 bytes in length display in multiple lines. At the end of each 1024 bytes line, three dots indicate a continuation of the message as follows:

```
MMM DD hh:mm:ss hostname %CAR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description: Configuration: text and more message text and more message text
and more message text and more message text and more message text and more message
text and more message text and more message text and more message text and more
message text and more message text and more message text and more message text and
more message text and more message text and more message text and more message text
and more message text and more message text and more message text and more message
text and more message text and more message text and more message text ...
```

The continuation of a message begins with three dots as follows:

```
MMM DD hh:mm:ss hostname %CAR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description: Configuration: ... text and more message text and more message
text and more message text and more message text and more message text and more
message text and more message text and more message text and more message text and
more message text and more message text and more message text
```

Example 1

```
May 19 14:28:44 dwlau-ultra2.cisco.com
%CAR-3-name_radius: #1, System: Remote LDAP Server.Unable to bind.
```

Example 2

```
May 19 14:28:45 dwlau-ultra2.cisco.com
%CAR-6-name_radius: #1, Server: Stopping server
```

Configuring Message Logging (Solaris)

Message logging is on by default, and all logs are stored in the **$INSTALL/logs** directory. To turn logging off, or to change the location where logs are stored, you must modify the **$INSTALLPATH/conf/car.conf** file.

In **$INSTALLPATH/conf/car.conf** file, the following lines control logging.

```
LOCAL_LOGGING [ON|OFF]
LOGDIR full_path
DATADIR full_path
SYSLOG_LOGGING [ON|OFF]
SERVER_IP_ADDRESS [ip_address]
FACILITY_LOCAL_NUMBER [0..7]
```

Where:

LOCAL_LOGGING enables (ON) or disables (OFF) the local logging function. (Local logging is on by default.)

LOGDIR specifies a full pathname to a different local log directory.

DATADIR specifies a full pathname to a different data directory.

SYSLOG_LOGGING enables (ON) or disables (OFF) the syslog logging function. (syslog logging is on by default.)

SERVER_IP_ADDRESS specifies the IP address of the host to which AR will send syslog messages.

FACILITY_LOCAL_NUMBER specifies the facility being used by the syslogd.

The following is an example

```
LOCAL_LOGGING OFF
SYSLOG_LOGGING ON
SERVER_IP_ADDRESS 209.165.200.224
FACILITY_LOCAL_NUMBER 7
```

Note You must first stop the Cisco AR server prior to changing the **car.conf** file, then restart the server. If you change the directory location where logs or database data are stored, you should also copy all log files or data files to that same directory before restarting the Cisco AR server.

Configuring Message Logging (Linux)

To enable **syslog** logging in Linux, you must modify the **syslog** file in the **/etc/sysconfig** directory. The following is the default syslog file.

```
# Options to syslogd
# -m 0 disables 'MARK' messages.
# -r enables logging from remote machines
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
```

```
SYSLOGD_OPTIONS="-m 0"
# 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="-x"
```

To enable logging of **syslog** messages, you must enable the **syslog** daemon to listen on port 514 by adding the -r flag to the SYSLOGD_OPTIONS line as follows:

```
SYSLOGD_OPTIONS="-m 0 -r"
```

Changing Log Directory

You can change the directory where local log messages are stored by adding the following line in the **$INSTALLPATH/conf/car.conf** file.

```
LOGDIR full_path
```

Where *full_path* is a full path to the directory where you want to store the log messages. For example, to store all system logs in **/var/log/AICar1**, add the following line in the **$INSTALLPATH/conf/car.conf** file:

```
LOGDIR /var/log/AICar1
```

You must first stop the Cisco AR server prior to changing the **car.conf** file. After changing the **car.conf** file, copy all existing log files to the new directory, then restart the server.

Note Specifying a path for local logging does not affect the storage location of syslog messages.

Configuring syslog Daemon (syslogd)

You must specify the facility from which *syslogd* will receive messages and the file into which the messages will be deposited.

In the syslog server's **/etc/syslog.conf** file, the following line might be needed.

```
local<n>.info <tab> <tab> <tab> /var/log/filename.log
```

Note Use at least one <tab> as a field separator.

Where:

local*n*—is the facility being used for syslogd; ***n*** must be a value from 0-7 and match the FACILITY_LOCAL_NUMBER used in AR's **car.conf** file.

/var/log/—is the path to the file that stores **syslogd** messages.

filename.log—is the file that stores **syslogd** messages. You can give this file a name of your choice.

Creating a Log File

To create a syslog log file, complete the following steps:

Step 1 Log in as user ***root***.

Step 2 Enter the following command, where ***filename.log*** is a name you choose.

touch ***filename.log***

Step 3 Change permissions on the syslog log file by entering the following:

chmod 664 ***filename.log***

Restarting syslogd

To restart the **syslog** daemon, log in as user ***root*** and enter the following commands:

/etc/init.d/syslog stop

/etc/init.d/syslog start

Managing the Syslog File

Left unmanaged, the **syslog** file will grow in size over time and eventually fill all available disk space in its partition. Cisco AR writes log files and session data (to persist user sessions) in the same disk partition where Cisco AR is installed.

In normal operation, log files consume a large amount of disk space. If log files are not managed regularly, Cisco AR might not have sufficient disk space to write session data. To avoid this, you should move the Cisco AR log files directory to a different disk partition than the one where Cisco AR writes session data, as described in Changing Log Directory.

Using a cron Program to Manage the syslog Files

Cisco recommends that you use the **cron** program to manage the **syslog** files.

The following example **crontab** file performs a weekly archival of the existing **syslog** file (named **ar_syslog.log** in this example). This scheme keeps the previous two week's worth of **syslog** files.

```
#
#  At 02:01am on Sundays:
#  Move a weeks worth of 'ar_syslog.log' log messages to 'ar_syslog.log.1'.
#  If there was a 'ar_syslog.log.1' move it to 'ar_syslog.log.2'.
#  If there was a 'ar_syslog.log.2' then it is lost.
01 02 * * 0 cd /var/log;
if [ -f ar_syslog.log ];
then if [ -f ar_syslog.log.1 ];
then /bin/mv ar_syslog.log.1 ar_syslog.log.2;
fi;
```

```
/usr/bin/cp ar_syslog.log ar_syslog.log.1;
>ar_syslog.log;
fi
```

Note Consider using move (**mv**) or copy (**cp**) commands to store the previous week's syslog files in a different disk partition to reserve space for the current syslog file.

To add this **crontab** segment to the existing **cron** facility in **/usr/spool/cron/crontabs** directory, complete the following steps at the syslog server console.

Step 1 Log in as user ***root***.

Step 2 Enter the following command:

crontab -e

Server Up/Down Status Change Logging

Cisco AR supports RADIUS server up/down detection and logging. The information messages are saved in the **$INSTALL/logs/name_radius_1_log** file where **$INSTALL** is the Cisco AR installation directory. Each message consists of a header and a message description.

Header Formats

The format of a header entry is:

mm/*dd*/*yyyy HH*:*MM*:*SS* name/radius/*n* Error Server 0

Example Log Messages

Following are the descriptions and types of messages that can be found within the <*AR_install_dir*>**/logs/name_radius_1_log** file.

1. Cisco AR detects a Remote Server when it responds for the first time or after it is reentered into Cisco AR's server pool for retry. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP!

   The following is an example header and message:

   ```
   09/14/1999 17:56:32 name/radius/1 Error Server 0
   Remote Server dave-ultra (171.69.237.99:1645) is UP!
   ```

   Cisco AR detects the Remote Server is not responding to its request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is DOWN!

   The following is an example header and message:

   ```
   09/14/1999 17:57:12 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.237.99:1645) is DOWN!
   ```

2. Cisco AR receives no response from the Remote Server after the server is reentered into Cisco AR's server pool for retry. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) remains DOWN!

   The following is an example header and message:

   ```
   09/14/1999 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.237.99:1645) remains DOWN!
   ```

3. The Remote Server is responding to the first retry but not the initial request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP but slow!

   The following is an example header and message:

   ```
   09/14/1999 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.237.99:1645) is UP but slow!
   ```

4. The Remote Server is responding to the second retry request but not the initial request or the first retry request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP but very slow!

   The following is an example header and message:

   ```
   09/14/1999 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.237.99:1645) is UP but very slow!
   ```

5. The Remote Server has been marked inactive and is being put back into Cisco AR's server pool for later use. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is being reactivated for later use.

   The following is an example header and message:

   ```
   09/14/1999 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (209.165.200.224:1645) is being reactivated for later use.
   ```