Logging Syslog Messages

Logging messages via syslog provides centralized error reporting for Cisco Prime Access Registrar (Prime 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 Prime Access Registrar messages. Prime Access Registrar and the syslog daemon can be running on the same host or different hosts.

This chapter contains 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 %Prime AR-[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 Prime Access Registrar-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 %Prime AR-[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 %Prime AR-[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
%Prime AR-3-name_radius: #1, System: Remote LDAP Server.Unable to bind.
```

Example 2

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

Configuring Message Logging

To enable **syslog** logging in Linux, you must modify the **syslog.conf** 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=”-r -m 0”
```

For RHEL version 7.0 and above, you must update the /etc/rsyslog.conf file with the following information and restart the syslog service:

```
$ModLoad imudp.so
$UDPServerRun 514
SYSLOGD_OPTIONS="-r -m 0"
localn.info <tab> <tab> <tab> /var/log/filename.log
```

To restart the syslog service:

```
systemctl restart rsyslog.service
```

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 Prime Access Registrar'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 Syslog Log File

To create a syslog log file:

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*

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 Prime Access Registrar 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.

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. Prime Access Registrar writes log files and session data (to persist user sessions) in the same disk partition where Prime Access Registrar is installed.

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

Using a cron Program to Manage the Syslog Files

We recommend 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.

Using a cron Program to Manage the Syslog Files

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

Prime Access Registrar 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 Prime Access Registrar 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. Prime Access Registrar detects a Remote Server when it responds for the first time or after it is reentered into Prime Access Registrar'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:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0
   Remote Server dave-ultra (171.69.127.99:1812) is UP!
   ```

   Prime Access Registrar 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:

   ```
   10/12/2013 17:57:12 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) is DOWN!
   ```

2. Prime Access Registrar receives no response from the Remote Server after the server is reentered into Prime Access Registrar'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:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) 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:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) 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:

```
10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
server dave-ultra (171.69.127.99:1812) is UP but very slow!
```

5. The Remote Server has been marked inactive and is being put back into Prime Access Registrar'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:

```
10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
server dave-ultra (209.165.200.224:1812) is being reactivated for later use.
```

Logging Subscriber Data

Prime Access Registrar stores all subscriber message details including Diameter request and response in a separate log file called **Subscriber_log** under $INSTALLPATH/logs folder. To log subscriber data for a selected Diameter client or remote server, you must set the corresponding **UserLogEnabled** parameter to True.

Message Format:

```
Date|Time|Diameter-Message-Type|User-Name(IMSI) \
|MSISDN|Subscirption-Id|Origin-Host|Host-IP-Address|Product-Name|Origin-Realm|Destin\
ation-Host|APN-Name|Session-id|Result_Code|Result-Description|UELocalIPAddress|Non-3\
GPP-IP-Access
```

Logging User IP Information

Prime Access Registrar provides an option to capture the username as part of the aregcmd_log during login failures. The following parameter is added under ***/Radius/Advanced*** to support this feature:

DisplayUserForFailedLogin—If this option is enabled, during login failures, username is captured along with the failure reason as part of the aregcmd_log.

Also, for all the configuration, login, and logout activities, Prime Access Registrar displays the end user IP in the aregcmd_log. With this enhancement, Prime Access Registrar will start logging the end user's IP address, which is the immediate first hop IP for every aregcmd activity.

Support for Logging Timeout Packets

With this enhancement, Prime Access Registrar starts logging information about all packets that timeout i.e. packets which are not responded to within the specified timeout period.

A sample log file content is provided below:

```
07/04/2020 14:08:35.904 name/radius/1 Info System 0 Remote Server REM_76 has not responded
Cmd code: 303 request for user-name 97000000051 in 1 try
```

Logging System Statistics

With this enhancement, Prime Access Registrar allows you to collect following statistics data for a configured duration:

- CPU Utilization
- Memory Utilization
- NFSIOstats
- Peak Worker Thread Queue / sec (for reporting of All Workers Temporarily Busy warning)

Global Statistics:

- TimedOut MAR/SAR/UDR
- Throttled Packets Count
- PacketsInUse Count
- DEA EAP Multi-Round Auth Success Responses
- DER Challenge Requests Count
- DuplicateSessionID Packets Count
- TimerQueue Entries Count

Per Connection Statistics:

- TimedOut MAR/SAR/UDR
- Throttled Packets Count
- Dropped DuplicateSessionID Packets Count
- Dropped Outgoing Responses for STA/AAA/DEA
- Dropped Incoming Responses for MAA/SAA/UDA/CEA/DWA
- Incoming Requests per Second
- Outgoing Requests per Second,
- Retransmitted Requests per Second
- Incoming Responses per Second
- Outgoing Responses per Second

A new parameter **SystemStatsLogFrequencyInSecs** is added under ***/Radius/Advanced/Diameter/TransportManagement***, which when set to a non-zero value, allows you to log the above statistics for the configured duration. By default this value is set to zero. The system statistics are saved in the **system_stats_log** file.

Logging Worker Queue Size

Reporting of **All Workers Temporarily Busy** warning has been added to the System Stats Log under the parameter **Peak Worker Thread Queue / sec,** and is only reported if the condition has occurred during the last statistics interval.