Troubleshooting Broadband Access Center

This chapter provides the information on how to observe the RDU and DPE logs, and troubleshoot Cisco BAC.

This chapter includes the following sections:

- Troubleshooting Checklist, page 21-1
- Logging, page 21-2

Troubleshooting Checklist

While troubleshooting with Cisco BAC, use the checklist described in Table 21-1.

Table 21-1 Troubleshooting Checklist

Procedure	Refer to ...
1. Check whether the Cisco BAC processes are up on all systems on which Cisco BAC components are installed.	Using Cisco BAC Process Watchdog from the Command Line, page 9-2
2. Check the Cisco BAC component logs for indications of high-severity errors. These include the information logged for:	
– RDU	RDU Logs, page 21-5
– DPE	DPE Logs, page 21-8
3. View server uptime from the administrator user interface to confirm that the servers are not bouncing.	Viewing Servers, page 16-24
4. View the RDU and DPE service performance statistics from the administrator's user interface. Observe any abnormal numbers, such as extended transaction times.	Viewing Servers, page 16-24
5. Check the syslog alerts log.	Syslog Alert Messages, page 11-1
6. Check the operating system and hardware resources, such as:	
– Disk space	
– CPU time	
– Memory	

Table 21-1 Troubleshooting Checklist (continued)

Procedure	Refer to ...
7. If troubleshooting a specific device, view the history of the device configuration from the administrator user interface.	Viewing Device History, page 16-14
8. If troubleshooting a specific device, view the device instructions that are cached at the DPE.	The **show device-config** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.
9. Configure individual device troubleshooting from the administrator user interface and, after a period of time, inspect the troubleshooting log.	Configuring Device Troubleshooting, page 8-10
10. View device fault data for the system, the RDU, the DPE, or a specific device.	Device Faults, page 8-6
11. Configure a higher level of logging on the RDU or the appropriate DPE for detailed logging information.	The RDU Log Level Tool, page 21-5 The **log level** command as described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.

Logging

Logging of events is performed at both the DPE and RDU, and in some unique situations, DPE events are logged at the RDU to give them higher visibility. Log files are located in their own log directories and can be examined using any text file viewer. The files can be compressed to allow them to be easily e-mailed to the TAC or system integrators for troubleshooting and fault resolution.

This section describes:

- Log Levels and Structures, page 21-3
- Configuring Log Levels, page 21-4
- Rotating Log Files, page 21-4
- RDU Logs, page 21-5
- The RDU Log Level Tool, page 21-5
- DPE Logs, page 21-8
- Access Registrar Logs, page 21-8

Log Levels and Structures

The log file structure is described here, and illustrated in Example 21-1, and includes:

- Domain Name—This is the name of the computer generating the log files.
- Date and Time—This is the date on which a message is logged. This information also identifies the applicable time zone.
- Facility—This identifies the system which, in this case is the Cisco BAC.
- Sub-facility—This identifies the Cisco BAC subsystem or component.
- Security Level—The logging system defines seven levels of severity (log levels as described in Table 21-2) that are used to identify the urgency with which you might want to address log issues. The process of configuring log levels is described in Configuring Log Levels, page 21-4:

Table 21-2 Logging Levels

Log Level	Description
0-Emergency	System unstable. Sets the logging function to save all emergency messages.
1-Alert	Immediate action needed. Sets the logging function to save all activities that need immediate action and those of a more severe nature.
2-Critical	Critical conditions exist. Sets the logging function to save all error messages and those of a more severe nature
3-Error	Error conditions exist. Sets the logging function to save all error messages and those of a more severe nature.
4-Warning	Warning conditions exist. Sets the logging function to save all warning messages and those of a more severe nature.
5-Notification	A normal, but significant, condition exists. Sets the logging function to save all notification messages and those of a more severe nature
6-Information	Informational messages. Sets the logging function to save all logging messages available

Note Another level known as 7-DEBUG is used exclusively by Cisco for debugging purposes. Do not use this level except at the direction of the Cisco TAC.

- Msg ID—This is a unique identifier for the message text.
- Message—This is the actual log message.

Example 21-1 Sample Log File

Domain Name	Data and Time	Facility	Sub-facility	Security Level	Msg ID	Message
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0236:	BAC Regional Distribution Unit starting up
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0566:	Initialized API defaults
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0568:	Initialized server defaults

Domain Name	Data and Time	Facility	Sub-facility	Security Level	Msg ID	Message
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0569:	Created default admin user
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0574:	Loaded 6 license keys
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0575:	Database initialization completed in 471 msec
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0015:	Unable to locate manifest file
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0280:	Command error

Configuring Log Levels

You can configure logging levels for both the RDU and the DPE to suit your specific requirements. For example, the logging level for the RDU could be set to Warning, and the level for the DPE could be set to Alert.

Log messages are written based on certain events taking place. Whenever an event takes place, the appropriate log message and level are assigned and, if that level is less than or equal to the configured level, the message is written to the log. The message is not written to the log if the level is higher than the configured value.

For example, assume that the log level is set to 4-Warning. All events generating messages with a log level of 4 or less, are written into the log file. If the log level is set to 6-Information, the log file will receive all messages. Consequently, configuring a higher log level results in a larger log file size.

To configure the log level on the DPE, using the **log level** command from the DPE command line. See the *Cisco Broadband Access Center 3.8 DPE CLI Reference,* for detailed information.

To configure the log level on the RDU, see The RDU Log Level Tool, page 21-5.

Rotating Log Files

All log files, except *perfstat.log*, are numbered and rolled over based on a configured maximum file size. The default maximum file size is 10 MB. (To configure the maximum file size from the API, use the `ServerDefaultsKeys.SERVER_LOG_MAXSIZE` property.) After a log file touches the configured limit, the data is rolled over to another file. This file is renamed in the *XXX.N*.log format, where:

- *XXX*—Specifies the name of the log file.
- *N*—Specifies any value between 1 and 100.

For example, once *rdu.log* reaches the 10 MB limit, it is renamed as *rdu.1.log*. With every 10-MB increase in file size, the latest file is renamed as *rdu.2.log*, *rdu.3.log*, and so on. So, the *rdu.7.log* file will contain data more recent than *rdu.4.log*. However, the latest log information is always stored in *rdu.log*.

In the case of the *perfstat.log* file, the file is renamed everyday. The file is rolled over in the perfstat.*N*.log format, where *N* is any value between 1 and 100. For example, *perfstat.100.log* will be the oldest log while *perfstat.1.log* will be the most recent renamed *perfstat.log* file.

Cisco BAC stores up to 10 log files at a given time. For a list of log files in the RDU and DPE servers, see RDU Logs, page 21-5, and DPE Logs, page 21-8, respectively.

Agent logs are rotated using the cron task that executes at 5 mins intervals by default. The time duration can be configured in the logrotate file available in the /etc/cron.d/ directory. The agent log files are checked every 5 mins (value configured in logrotate file) and if size exceeds value for the parameter size in bpragent_consolelog available in /etc/logrotate.d/ directory, logs will be rotated.

RDU Logs

The RDU has two logs that it maintains in the *BPR_DATA/rdu/logs* directory:

- *rdu.log*—Records all RDU events according to the configured logging severity level. (See Setting the RDU Log Level, page 21-6, for instructions on setting the default log levels.) To view *rdu.log*, see Viewing the rdu.log File, page 21-5.
- *audit.log*—Records all high-level changes to the Cisco BAC configuration or functionality including the user who made the change. To view *audit.log*, see Viewing the audit.log File, page 21-5.
- *troubleshooting.log*—Records detailed device information for troubleshooting a specific device, or a group of devices without turning logging on, and without searching through log files for device- or group-specific information. To view *troubleshooting.log* from the administrator user interface, see Viewing Device Troubleshooting Log, page 8-12.
- *perfstats.log*—Records device performance statistics to help troubleshoot issues related to system performance. For more information, see Monitoring Cisco Broadband Access Center, page 11-1.

Viewing the rdu.log File

You can use any text processor to view the *rdu.log* file. In addition, you can view the log file from the administrator user interface. To do this:

Step 1 Choose the **RDU** tab under **Servers**.

The View Regional Distribution Unit Details page appears.

Step 2 Click the **View Details** icon () corresponding to RDU Log File.

The View Log File Contents page appears, displaying data from *rdu.log*.

Viewing the audit.log File

You can use any text processor to view the audit.log file. In addition, you can view the log file from the administrator user interface. To do this:

Step 1 Choose the **RDU** tab under **Servers**.

The View Regional Distribution Unit Details page appears.

Step 2 Click the **View Details** icon corresponding to Audit Log File.

The View Log File Contents page appears, displaying data from audit.log.

The RDU Log Level Tool

Use the RDU log level tool to change the current log level of the RDU from the command line, using the **setLogLevel.sh** command. This tool is located in the BPR_HOME/rdu/bin directory. Table 21-2 identifies the available log levels and the types of message written to the log file when enabled.

We recommend that you keep the RDU logging level at the Warning level to help maintain a steady operations state. The Information level is recommended to be used with caution if you need to maintain steady state performance during debug operations.

You should exercise caution when running with the Information level set because this creates a great number of log entries, which in itself can adversely impact performance.

Note The RDU process has to be up to execute the log level tool. Also, you must be a privileged user to run this tool by using the **setLogLevel.sh** command.

Using the RDU Log Level Tool

All examples assume that the user name for the RDU is **bacadmin**, the password for the RDU is **changeme**, and the RDU server is up.

Enter this command to run the RDU log level tool:

```
setLogLevel.sh [0..6] [-help] [-show] [-default] [-debug]
```

where:

- *-[0..6]*—Identifies the logging level to be used. For a list of available levels, see Table 21-2.
- **-help**—Displays help for the tool.
- **-show**—Displays the current log level set for the RDU server.
- **-default**—Sets the RDU to the installation default level 5 (notification).
- **-debug**— Sets an interactive mode to enable or disable tracing categories for RDU server.

Note You should only enable the debug settings that the Cisco support staff recommends.

You can also use this tool to perform these functions:

- Setting the RDU Log Level, page 21-6
- Viewing the RDU's Current Log Level, page 21-7

Setting the RDU Log Level

You can use this tool to change the logging level from one value to any other value.

The following example illustrates how to set the RDU logging level to the warning level, as indicated by the number 4 in the **setLogLevel.sh** command. The actual log level set is not important for the procedure, it can be interchanged as required.

To set the RDU logging level:

Step 1 Change directory to BPR_HOME/rdu/bin.

Step 2 Run the RDU log level tool using this command:

```
setLogLevel.sh 4
```

This prompt appears:

```
Please type RDU username:
```

Step 3 Enter the RDU username at the prompt. In this example, the default username (bacadmin) is used.

```
Please type RDU username: bacadmin
```

This prompt appears:

```
Please type RDU password:
```

Step 4 Enter the RDU password for the RDU at the prompt. In this example, the default password (**changeme**) is used.

```
Please type RDU password: changeme
```

This message appears to notify you that the log level has been changed. In this example, the level was 5, for notification, and is now 4, for warning.

```
RDU Log level was changed from 5 (notification) to 4 (warning).
```

Viewing the RDU's Current Log Level

You can use this tool to view the RDU log and determine which logging level is configured before attempting to change the value.

To view the RDU's current logging level:

Step 1 Change directory to BPR_HOME/rdu/bin.

Step 2 Run this command:

```
setLogLevel.sh -show
```

This prompt appears:

```
Please type RDU username:
```

Step 3 Enter the RDU username (**bacadmin**) and press **Enter**.

```
Please type RDU username: bacadmin
```

This prompt appears:

```
Please type RDU password:
```

Step 4 Enter the RDU password (**changeme**) and press **Enter**.

```
Please type RDU password: changeme
```

This message appears:

```
The logging is currently set at level: 4 (warning)

All tracing is currently disabled.
```

DPE Logs

The DPE maintains its logs at the BPR_DATA/dpe/logs directory.

- *dpe.log*—Records all events having the configured default level. In situations where the DPE undergoes catastrophic failure, such as engaging in a series of system crashes, the catastrophic errors are also logged into the rdu.log file.
- *perfstats.log*—Records device performance statistics to help troubleshoot issues related to system performance. For more information, see Monitoring Cisco Broadband Access Center, page 11-1.

Viewing the dpe.log File

You can use any text viewer to view the *dpe.log* file. In addition you can use the **show log** command, from the DPE CLI, to view the log file. See the *Cisco Broadband Access Center 3.8 DPE CLI Reference*, for additional information.

You can also view the DPE log file using the Cisco BAC administrator user interface. To do this:

Step 1 Choose **Servers > DPEs**.

Step 2 Click the link corresponding to the DPE whose log file you want to view.

The View Device Provisioning Engines Details page appears.

Step 3 To view the contents of the *dpe.log* file, click the **View Details** icon against DPE Log File in the Log Files area.

Access Registrar Logs

Cisco BAC generates trace messages from Cisco Access Registrar RADIUS server extensions. The RADIUS server trace resides in the **PAR-install-path/name_radius_1_trace directory**; PAR-install-path is a variable and is specific to the value that you enter. The default location for the RADIUS server log file is /opt/CSCOar/logs/name_radius_1_trace.

The trace messages emitted using the RADIUS server extensions are based on the extension trace level setting. You can set values (described in Table below) at the trace level; the number you set makes that number the current setting of the extension-trace-level attribute for all extensions.

Use the **aregcmd** command trace to set the trace level in the specified server to a new value. The trace level governs how much information is displayed about the contents of a packet. When the trace level is zero, no tracing is performed. The higher the trace level, the more information displayed. The highest trace level currently used by the PAR server is trace level 5.

Note Although the highest trace level supported by the PAR server is trace level 5, an extension point script might use a higher level. There is no harm in setting the trace to a level higher than 5.

The trace levels are inclusive, meaning that if you set trace to level 3, you will also get the information reported for trace levels 1 and 2. If you set trace level 4, you also get information reported for trace levels 1, 2, and 3. When you do not specify a server, PAR sets the trace level for all of the servers in the current cluster. When you do not specify a value for the trace level, PAR displays the current value of the trace level. The default is 0.

The syntax for setting the trace level is:

trace [*server*] *[level*]

Table 21-3 Trace Levels

Log Level	Description
0	No trace performed.
1	Report when a packet is sent or received or when there is a change in a remote server's status.
2	Indicates the following: • Which services and session managers are used to process a packet • Which client and vendor objects are used to process a packet • Detailed remote server information for LDAP and RADIUS, such as sending a packet and timing out • Details about poorly formed packets • Details included in trace level 1
3	Indicates the following: • Error traces in TCL scripts when referencing invalid RADIUS attributes. • Which scripts have been executed • Details about local UserList processing • Details included in trace levels 1 and 2
4	Indicates the following: • Information about advanced duplication detection processing • Details about creating, updating, and deleting sessions • Trace details about all scripting APIs called • Details included in trace levels 1, 2, and 3
5	Indicates the following: • Details about use of the policy engine including: – Which rules were run – What the rules did – If the rule passed or failed – Detailed information about which policies were called • Details included in trace levels 1, 2, 3, and 4