Monitoring Component Logs

This chapter describes how you can monitor the Prime Cable Provisioning components.

Logging of events is performed at component level, and in some unique situations, DPE events are additionally logged at the RDU to give them higher visibility. Log files are stored in their own log directories and can be examined by using any text processor. You can compress the files for easier e-mailing to the Cisco Technical Assistance Center or system integrators for troubleshooting and fault resolution. You can also access the RDU and DPE logs from the Admin UI.

This chapter describes:

Log Levels and Structures

The log file structure, illustrated in Table 2: Sample Log File, 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 Prime Cable Provisioning.
- Sub-facility—This identifies the Prime Cable Provisioning subsystem or component.
- Severity Level—The logging system defines seven levels of severity (as described in the following table) that are used to identify the urgency with which you might want to address log issues. The process of configuring these severity levels is described in Command Default Configuring Severity Levels.

Table 1: Severity 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.

Log Level	Description
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 Technical Assistance Center.	

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

Table 2: Sample Log File

Domain Name	Data and Time	Facility	Sub- facility	Severity Level	Msg ID	Message
bac.example.com:	2013-02-08 22:43:23,341 EST:	%CPCP-	RDU-	5	0236:	Prime Cable Provisioning Regional Distribution Unit starting up
bac.example.com:	2013-02-08 22:43:23,711 EST:	%CPCP-	RDU-	5	0566:	API defaults
bac.example.com:	2013-02-08 22:43:25,211 EST:	%CPCP-	RDU-	5	0567:	Network Registrar defaults
bac.example.com:	2013-02-08 22:43:25,321 EST:	%CPCP-	RDU-	5	0568:	Server defaults

Domain Name	Data and Time	Facility	Sub- facility	Severity Level	Msg ID	Message
bac.example.com:	2013-02-08 22:43:26,721 EST:	%CPCP-	RDU-	5	0570:	DOCSIS defaults
bac.example.com:	2013-02-08 22:43:26,911 EST:	%CPCP-	RDU-	5	0571:	Computer defaults
bac.example.com:	2013-02-08 22:43:27,221 EST:	%CPCP-	RDU-	5	1018:	CableHome WAN-MAN defaults
bac.example.com:	2013-02-08 22:43:27,321 EST:	%CPCP-	RDU-	5	1019:	CableHome WAN-Data defaults
bac.example.com:	2013-02-08 22:43:27,711 EST:	%CPCP-	RDU-	5	0707:	PacketCable defaults
bac.example.com:	2013-02-08 22:43:28,561 EST:	%CPCP-	RDU-	5	0569:	Created default admin user
bac.example.com:	2013-02-08 22:43:28,711 EST:	%CPCP-	RDU-	5	0575:	Database initialization completed in [471] msec

Command Default Configuring Severity Levels

You can configure the severity levels of logging for all components to suit your specific requirements. For example, the severity 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 severity 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.

Note The KDC is not considered in this log file.

To configure the severity level on the DPE, use the **log level** command from the DPE command line. For detailed information, see the Cisco Prime Cable Provisioning 6.1.3 DPE CLI Reference Guide.

To configure the log level tool on the RDU, see Using the RDU Log Level Tool.

Rotating Log Files

All log files are numbered and rolled over based on a configured maximum file size. The default maximum file size is 25 MB. (To configure the maximum file size from the application programming interface (API), use the *ServerDefaultsKeys.SERVER_LOG_MAXSIZE* property.) Once 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 200.

Note The RDU and DPE servers store up to 200 log files at a given time. For a list of log files in these servers, see subsequent sections.

For example, once *rdu.log* reaches the 25-MB limit, it is renamed as *rdu.1.log*. With every 25-MB increase in file size, the latest file is renamed as *rdu.2.log*, *rdu.3.log*, and so on. So, the *rdu.4.log* file will contain data more recent than *rdu.7.log*. The latest log information, however, is always stored in *rdu.log*.

Note For *rdu_auth.log* and *rdu_crs.log*, the default maximum size is 10MB and the RDU server stores up to 100 log files at any given point of time. However, these values can be configured using the file log4j.xml located at the directory BPR_HOME/rdu/conf. You must restart the RDU for every change made to the file.

Regional Distribution Unit Logs

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

- *rdu.log*—Records RDU processing according to the configured default severity level. (For instructions on setting the default log levels, see Setting the RDU Log Level.)
- *audit.log*—Records high-level changes to the Prime Cable Provisioning configuration or functionality including the user who made the change.
- *rdu_auth.log*—When a user tries to authenticate itself to RDU, authentication related information gets captured in this log.
- *rdu_crs.log*— Records all the CRS related activities such as enable, disable, pause, and resume. Logs are also written when a CRS request starts execution, is deleted, replaced with an identical request, and when the execution is completed. After executing every 1000 devices *rdu_crs.log* records the number of failed devices, device identifiers (MAC address, DUID, and FQDN) for which configuration regeneration have failed, status of pause on failure threshold, and warning messages are displayed if the failure threshold percentage is exceeded.

When you enable logging of informational messages (log level 6-Information), the RDU logs additional messages that expose batch-processing operations. These messages also contain information on elapsed time and rate.

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 Admin UI.

To view the file:

Step 1 Choose **Server > Regional Distribution Unit**.

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 Admin UI.

To view the file:

Step 1 Choose the Regional Distribution Unit tab under **Servers**.

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

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

Viewing the *rdu_auth.log* and *rdu_crs.log*File

You can use any text processor to view the *rdu_auth.log* and *rdu_crs.log* file. You cannot view these log files from the admin UI.

Setting the Log Level for *rdu_auth.log* and *rdu_crs.log*

The logging level for *rdu_auth.log* and *rdu_crs.log* can be set using the file log4j.xml located in the directory BPR_HOME/rdu/conf. By default, only informational messages are logged. You must restart the RDU, after making any changes in the log level.

Setting the Behind Device Threshold Log Level

A warning message is logged in *rdu.log* whenever the CPE count behind a DOCSIS modem reaches the threshold value assigned in the following properties:

/rdu/log/cpe/threshold : To set the threshold limit after which if the behind devices count increases, the warning message is logged in RDU logs. The default threshold value is 400.

/rdu/log/cpeCountOnUpdate/enable :

- **-** When the value is set to false, during the configuration regeneration of a Cable Modem, if threshold value increases then the warning message is logged.

- **-** When the value is set to true, during the configuration regeneration of a Cable Modem/Behind Devices(CPE), if threshold value increases then the warning message is logged.

The default value is false.

The properties are hidden by default and have to be added in *rdu.properties* file to modify the default values. After making changes in the property file, restart the RDU. The log level must be set to the warning level.

Output Message Format

When the value is set to false:

```
The number of device records behind the DOCSIS modem [1,6,0a:00:00:00:00:01] has reached
[3005],
of its configured threshold [3000].
```

When the value is set to true:

```
The number of device records behind the DOCSIS modem [1,6,0a:00:00:00:00:02] has reached
the configured threshold [3005].
```

Using 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 not applicable for *rdu_crs.log* and *rdu_auth.log*. This tool resides in the *BPR_HOME/rdu/bin* directory.

The following table identifies the available severity levels and the types of messages written to the log file when enabled.

Table 3: RDU 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.

Log Level	Description
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.	

We recommend that you keep the RDU severity 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 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.

Syntax Description

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

- **-**[*0..6*]—Identifies the severity level to be used. For a list of available levels, see Table 3: RDU Logging Levels, on page 6.
- **-help**—Displays help for the tool.
- **-show**—Displays the current severity 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 the 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
- Viewing the Current Log Level of RDU

Setting the RDU Log Level

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

The example described in this section assumes that the RDU server is up, the username for the RDU is admin, and the password is changeme.

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. In this example, the default username (**admin**) is used.

Please type RDU username: **admin**

This prompt appears:

Please type RDU password:

Step 4 Enter the RDU password for the RDU. 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 Current Log Level of RDU

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

The example described in this section assumes that the:

- RDU server is up.
- Username for the RDU is **admin.**
- Password is **changeme.**

To view the current logging level of the RDU:

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 (**admin**) and press **Enter**.

```
Please type RDU username: admin
```

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.
```

Provisioning Web Services Log

The PWS maintains a *pws.log* file in the *BPR_DATA/pws/logs* for SOAP and *BPR_DATA/restpws/logs* for RESTful directory. The file contains log information of the PWS component. *The other log file called pws_console.log* is the Tomcat console log and is located at *BPR_DATA/agent/logs* directory. By default, the PWS log level is set to INFO.

Using the PWS Log Level Tool in CLI

Use the PWS log level tool (ws-cli.sh) to change the current log level of the PWS. This tool resides in the *BPR_HOME/pws/bin* for SOAP and *BPR_HOME/restpws/bin* for RESTful directory.

The following table identifies the available severity levels and the types of messages written to the pws.log file. These log levels can be altered during run time.

Table 4: PWS Logging Levels

Log Level	Description
ERROR	Records all PWS error messages.
WARN	Records all PWS warning messages.
INFO	Records information regarding PWS operations.
DEBUG	Records debug information that helps you to dress any error.

It is recommended that you set the PWS log level to the default INFO level. Using ws-cli.sh, you can change the log level to DEBUG if you are planning to troubleshoot the system. You should exercise caution when running with the DEBUG level because this creates a great number of log entries, which in itself can adversely impact performance.

Note Loggers are applicable only at runtime and are set to the default values every time you restart the PWS. To retain the runtime log details, use the command -sap that will save the modifications being made to the logger. These changes will not change even after you restart the PWS.

Syntax Description

ws-cli.sh

- **-ll**—Lists all the loggers and it's severity level. You can also use --listlog.
- **-sl**—Sets the log level. You can also use --setlog.

You can also use this tool to perform these functions:

- Setting the PWS Log Level
- Viewing the Current Log Level of PWS

PWS Loggers

For PWS, Prime Cable Provisioning provides loggers for every operation type. The different logger names are:

- api_group—Provides log details about groups.
- api_device_type—Provides log details about device type.
- api_file—Provides log details about files.
- api_cos—Provides log details about class of service.
- api_device—Provides log details about devices.
- api_search—Provides log details about search operation.
- api_dhcpcriteria—Provides log details about DHCP criteria.
- api_session—Provides log details about sessions.
- root—Can be set to provides generic log details.

Setting the PWS Log Level

You can use this tool to change the logging level from one value to another value. The following example illustrates how to set the PWS logging level to the DEBUG level, as indicated by the number 4 in the **ws-cli.sh** command. The actual log level is not important for the procedure; it can be interchanged as required. The example described in this section assumes that the PWS server is up**.**

To set the PWS logging level:

Step 1 Change directory to *BPR_HOME/pws/bin* for SOAP and *BPR_HOME/restpws/bin* for RESTful.

Step 2 Run the PWS log level tool using this command. This will change the log level from INFO to DEBUG.

```
# ws-cli.sh -sl <root=DEBUG>
```

Step 3 Save the changes by using the command:

```
# ws-cli.sh -sap
```

Viewing the Current Log Level of PWS

You can use this tool to view the PWS log and determine which logging level is configured before attempting to change the value. The example described in this section assumes that the PWS server is up.

To view the current logging level of the PWS:

Step 1 Change directory to *BPR_HOME/pws/bin* for SOAP and *BPR_HOME/restpws/bin* for RESTful.

Step 2 Run this command:

```
# ws-cli.sh-ll <logger>
```

In case you have not included logger in the CLI command, it lists all the loggers and it's log levels.

Device Provisioning Engines Log

The DPE maintains a *dpe.log* file in the *BPR_DATA/dpe/logs* directory. The file contains records of 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.

The *SNMPService.logyyy.log* log file is used by the DPE, when PacketCable is enabled on the DPE server, to provide detailed debugging information. You use the **service packetcable** *1..1* **show snmp log** command from the DPE command-line interface (CLI) to view this file, which resides in the *BPR_DATA/dpe/logs* directory. For PacketCable command usage, see the Cisco Prime Cable Provisioning 6.1.3 DPE CLI Reference Guide.

Note PacketCable logging messages are sent to the *dpe.log* file and the detailed SNMP debugging is sent to the *SNMPService.logyyy.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. For additional information, see the Cisco Prime Cable Provisioning 6.1.3 DPE CLI Reference Guide.

You can also view the DPE log file using the Prime Cable Provisioning Admin UI.

To view the file:

Step 1 Choose **Servers > Device Provisioning Engines**.

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

The View Device Provisioning Engines Details page appears.

Cisco Prime Network Registrar Logs

Prime Cable Provisioning generates log messages from Cisco Prime Network Registrar DHCP server extensions. The DHCP server log resides in the *cnr-install-path/name_dhcp_1_log* directory; *cnr-install-path* is a variable and is specific to the value that you enter. The default location for the DHCP server log file is */var/nwreg2/local/logs/name_dhcp_1_log*.

The log messages emitted via the DHCP server extensions are based on the extension trace level setting. You can set values (described in the following table) at the trace level; the number you set makes that number the current setting of the **extension-trace-level** attribute for all extensions.

Table 5: DHCP Server Extension Trace Levels

Level	Description
0	Logs error and warning conditions. Sets the extensions to emit all error and warning messages and those of a more severe nature.
1	Logs server interactions, which include configuration instructions obtained from the DPE and configuration generation requests that are forwarded to the RDU.
2	Logs processing details, which include individual configuration commands and attribute values forwarded in instruction generation requests.
3	Logs internal processing for extensions debugging, which includes hexadecimal dumps of messages.
4	Logs debugging of extension background operations, which include polling of DPE status.

You can change the extension trace level by using the Network Registrar web UI. To change the level:

Step 1 Open the Network Registrar local web UI.

Step 2 From the menu, click **DHCP**, then **DHCP Server**.

Step 3 Click the Local DHCP Server link.

Step 4 On the Edit DHCP Server page, expand the Extensions attribute category.

Step 5 Set the **extension-trace-level** value, then click **Modify Server**.

Step 6 Reload the DHCP server.

Note For detailed information on logging performed by the DHCP server, see the Cisco Prime Network Registrar End-User Guides.

Admin UI Log

The Admin UI maintains a adminui.log file in the BPR_DATA/adminui/logs directory where all the Admin UI related logs are stored. The other log file called tomcat_console.log is the Admin UI Tomcat console log and is located at *BPR_DATA/agent/logs* directory. By default, the Admin UI log is set to the INFO level.

Using the Admin UI Log Level Tool

The following table identifies the available severity levels and the types of messages written to the adminui.log file.

Table 6: Admin UI Logging Levels

Log Level	Description
ERROR	Records all Admin UI error messages.
WARN	Records all Admin UI warning messages.
INFO	Records information regarding Admin UI operations.
DEBUG	Records debug information that helps you to address any error.
TRACE	Records details about any server traces.

These log levels can be altered but Admin UI(Tomcat) needs to be restarted for the log level to take effect. It is recommended that you set the Admin UI log severity level to the INFO level. You can set the log level to DEBUG if you are planning to troubleshoot the system. You should exercise caution when running with the DEBUG level because this creates a great number of log entries, which in itself can adversely impact performance.

Setting the Admin UI Log Level

By default, the Admin UI log level is set to INFO. To change the log level, you need to edit the file logback.xml located at: /opt/CSCObac/rdu/adminUI/conf. It can also be changed using adminui-cli.sh file located at : /opt/CSCObac/rdu/adminUI/bin.

The file contains multiple loggers and to change the log level to say DEBUG, edit the file using a text editor as following:

```
logger name="com.cisco" level="DEBUG" additivity="false”
```

You must restart the tomcat server for the new log level to take effect.