Understanding Cisco IPICS Serviceability and Diagnostic Information

This chapter describes the serviceability and diagnostic information that is available for Cisco IPICS and contains the following sections:

Understanding the Serviceability Drawer

The Serviceability drawer is located in the Server tab of the Administration Console and contains the following windows:

- Dashboard—Provides you with Cisco IPICS system and resource information. For more information about the information that is included in this window, see the "Viewing the Information in the Dashboard Window" section on page 12-2.
- Diagnostics—Contains summary information about the Cisco IPICS server and the components of the Cisco IPICS system that interact with the server. From this window, you can also execute a diagnostic script and download the results of that diagnostic script and additional diagnostic information. For more information about this window, see the "Viewing Cisco IPICS Server Diagnostic Information" section on page 12-6
- System Logs—Displays logging information for Cisco IPICS. This information can be useful for troubleshooting or debugging your system. For more information about this window, see the "Viewing the Cisco IPICS System Logs" section on page 12-10.
- RCS Logs—Displays logging information for the radio controls service (RCS). For more information about this window, see the "Viewing the Cisco IPICS RCS Logs" section on page 12-13.
- System Event Notify—Lets you configure system even email notification, which provides email notification to a designated recipient when major system events occur. For more information about this window, see the "Configuring System Event Email Notifications" section on page 12-16.

Viewing the Information in the Dashboard Window

The dashboard window displays current, real-time information regarding the overall status of your system. This window displays the resources that you have used in your system and the resources that you have available. These resources range from system resources, such as central processing unit (CPU) and memory usage, to entity resources, such as channel, incident, VTG, user, license, and RMS details.

The format of this window includes multiple panes, one for each resource. Each pane is also known as a dashboard.

Tip To refresh the elements in this window and obtain the latest information, click **Refresh** at the top of the window.

This section contains the following topics:

Understanding the System Dashboard

The System Dashboard displays information about the Cisco IPICS policy engine, server memory and hard disk usage, and multicast address information. See Table 12-1 for all of the elements that are contained in this pane.

For related information about policy engine services and trace files, see the "Obtaining Information about Dial Engine Services" section on page 7-2 and the "Managing Tracing for the Policy Engine" section on page 7-3.

Table 12-1 Elements in the System Dashboard

Element	Description
Policy counts [multi-purpose, invitation]	The total number of policies (either active or inactive) that are available for the policy engine, grouped by multi-purpose and invitation policies. For more information about policy types, see the "Adding a Policy" section on page 8-4 and the "Managing Actions for a Policy" section on page 8-6.
Policy Engine status	The status of the policy engine. A status of Up indicates that the policy engine is active; a status of Down indicates that the policy engine is inactive.
Configured activity log size (in MB)	The maximum size of the activity log file. **Note** For more information about activity logs, see the "Managing Activity Logs" section on page 2-93.

Table 12-1 Elements in the System Dashboard (continued)

Element	Description
Current activity log size (in MB)	The current size of the activity log file.
Free memory (in MB)	The amount of random access memory (RAM) that is available in the Cisco IPICS server. The RAM is obtained from the Dual Inline Memory Modules (DIMMs) in the Cisco IPICS server.
Used memory (in MB)	The amount of RAM that the server currently uses.
CPU - percent idle	The percentage of CPU resources that are idle and available. The CPU resources are obtained from the CPU in the server.
Disk usage (in GB) [used / free / total]	The amount of disk space that is currently used in your server, the amount of free disk space that is currently available in your server, and the total amount of hard disk space that is available in your server.
Total/Available number of multicast addresses in pool	The total number of multicast addresses in the multicast address pool and the number of multicast addresses that are available. For more information about the multicast address pool, see the "Managing the Multicast Pool" section on page 2-39.

Understanding the Channel Dashboard

The Channel Dashboard displays information about the total number of channels, the number of enabled, disabled, active, and connected channels in your system, and the current status of those channels. For more information about channels and how they are used in Cisco IPICS, see the "Managing PTT Channels and Channel Groups" section on page 2-2.

See Table 12-2 for all of the elements that are contained in this pane.

Table 12-2 Elements in the Channel Dashboard

Element	Description
Total number of channels	The total number of channels that you have configured in the Cisco IPICS server.
Number of enabled channels	The number of channels that are enabled.
Number of disabled channels	The number of channels that are disabled.
Media Connection Count (for enabled channels)	This field represents the total number of media connection assignments that are mapped to enabled channels in the **Configuration > Channels** window. If any enabled channel has more than one media connection assignment, this number will be greater than the number of enabled channels.
Number of active channels	The number of enabled channels that are present in a virtual talk group (VTG).

Understanding the Incident Dashboard

The Incident Dashboard displays information about the total number of incidents and the number of active and inactive incidents in your system. For more information about channels and how they are used in Cisco IPICS, see the "Managing Incidents" section on page 2-78.

See Table 12-3 for all of the elements that are contained in this pane.

Table 12-3 Elements in the Incident Dashboard

Element	Description
Total number of incidents	The total number of incidents that you have configured in the Cisco IPICS server.
Number of active incidents	The number of incidents that are active.
Number of inactive incidents	The number of incidents that are inactive.

Understanding the Virtual Talk Group Dashboard

The Virtual Talk Group Dashboard displays information about the number of VTGs and inactive VTGs in your system. For more information about VTGs, see the "Managing VTGs" section on page 4-2.

See Table 12-4 for all of the elements that are contained in this pane.

Table 12-4 Elements in the Virtual Talk Group Dashboard

Element	Description
Number of VTG templates	The number of VTG templates, or inactive VTGs, that exist in the server.
Number of active VTGs	The number of VTGs that are currently active.

Understanding the User Dashboard

The User Dashboard displays information about the number of users who are logged in to the Administration Console, the number of users who are logged in to Cisco IPICS by using a Cisco Unified IP Phone, and the number of users who are logged in to Cisco IPICS by using the IDC. For more information about users, see the "Managing Users" section on page 3-1.

See Table 12-5 for all elements in the user dashboard.

Table 12-5 Elements in the User Dashboard

Element	Description
Number of users logged in to the administration console	The total number of users who are logged in to the Administration Console.
Number of Cisco Unified IP phone users logged in to Cisco IPICS	The total number of Cisco Unified IP Phone users who are logged in to the Cisco IPICS system.

Table 12-5 Elements in the User Dashboard (continued)

Element	Description
Number of IDC users logged in to Cisco IPICS	The total number of IDC users who are logged in to the Cisco IPICS system.
Number of users dialed in to Cisco IPICS	The total number of users who are using the dial-in functionality of the Cisco IPICS system.

Understanding the License Dashboard

The License Dashboard displays total number licenses for various items and the current status of those items. For more information about licenses, see the "Managing Licenses" section on page 2-83.

Table 12-6 describes the elements that are contained in this pane.

Table 12-6 Elements in the License Dashboard

Element	Description
Concurrent LMR Ports	The number of concurrent LMR ports that your Cisco IPICS system is licensed to use and the number of LMR ports that are available for use.
Concurrent Dial Users	The total number of concurrent dial users that your system is licensed for and the number of dial users that the system can currently accept.
Concurrent Dispatch Console Silver Users	The total number of concurrent IDC Silver users that your system is licensed for and the number of IDC Silver users that the system can currently accept.
Concurrent Multicast Ports	The number of concurrent multicast ports that your Cisco IPICS system is licensed to use and the number of multicast ports that are available for use.
Concurrent Gateway P25 Vocoders	The number of concurrent P25 channels that your Cisco IPICS system is licensed to use and the number of P25 channels that are available for use.
Concurrent Cisco Unified IP Phone Users	The total number of concurrent Concurrent Cisco Unified IP Phone users that your system is licensed for and the number of Cisco Unified IP Phone that the system can currently accept.
Concurrent ISSI Gateway Servers	The number of concurrent ISSI Gateway servers that your Cisco IPICS system is licensed to use and the number of ISSI Gateway servers that are available for use.
Concurrent EndToEnd P25 Vocoders	The number of concurrent connections to end-to-end P25 channels that your Cisco IPICS system is licensed to use and the number of concurrent connections to end-to-end P25 channels that are available for use.
Concurrent Mobile Endpoint Users	The total number of concurrent mobile client (endpoint) users that your system is licensed for and the number of mobile endpoint users that the system can currently accept.

Table 12-6 Elements in the License Dashboard (continued)

Element	Description
Concurrent UMS Servers	The number of concurrent UMS servers that your Cisco IPICS system is licensed to use and the number of UMS servers that are available for use.
Concurrent DFSI Talk Groups	The total number of concurrent DFSI talk groups that your system is licensed for and the number of DFSI talk groups that the system can currently accept.
Concurrent DFSI Servers	The total number of concurrent DFSI servers that your system is licensed for and the number of DFSI servers that the system can currently accept.
Concurrent Dispatch Platinum Users	The total number of concurrent IDC Platinum users that your system is licensed for and the number of IDC Platinum users that the system can currently accept.

Understanding the RMS/UMS Dashboard

The RMS/UMS Dashboard displays information about the available number of voice ports that your system is licensed to use. For more information about the RMS, see the "Managing the RMS" section on page 2-45. For more information about the UMS, see the "Managing the UMS" section on page 2-56.

See Table 12-7 for all of the elements that are available in this pane.

Table 12-7 Elements in The RMS Dashboard

Element	Description
RMS *rms-hostname*	The status for the RMS with the specified *rms-hostname*. For more information, see the Status field in Table 2-16 on page 2-48.
Total/Available voice ports	The total number of voice ports that are configured for your server and the number that are available for use.

Viewing Cisco IPICS Server Diagnostic Information

The Diagnostics window displays diagnostic information for various components of the Cisco IPICS server.

When you access the Diagnostics window, Cisco IPICS runs a script to obtain the diagnostic information; this information displays in the Diagnostic Summary pane. To refresh the pane and display the most current diagnostic information for your server, click the **Execute Diagnostic Script** button, which is located on the lower left side of the window.

To download all diagnostic information that is included in this window, along with the ipics.log file, click the **Download Diagnostic Results** button. For more information about how to download the diagnostic results, see the "Downloading the Server Diagnostic Information" section on page 12-9.

For more information about the log severity information that is included in each message, see the "Understanding the System Log Severities" section on page 12-11.

See Table 12-8 for all of the elements that are contained in the Diagnostic Summary pane.

Table 12-8 Elements in the Diagnostic Summary Pane

Element	Description
Cisco IPICS Server Hostname:	The host name of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **hostname**
Cisco IPICS Server Current Date and Time:	The current date and time of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **date**
Cisco IPICS Server OS Version:	The version of the Cisco IPICS operating system that is currently installed on the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **versions**
Cisco IPICS Server Software Version:	The current version of the Cisco IPICS server software. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **versions**
Cisco IPICS Server Software Version upgrade history:	The date and time that the current version of Cisco IPICS was installed and provides a history, with release versions, of the times that the software has been uninstalled or upgraded. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/ipics-release.history**
Hardware Platform Details:	Detailed information for the hardware platform. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/hwprofile**
CPU Details:	Detailed information for the CPU. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /proc/cpuinfo**
Cisco IPICS Server Network Interface Card Information:	The configuration of the Network Interface Cards (NICs), and the packets that have been transmitted and received on the NICs, that are installed on the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session. [root]# **ifconfig**

Table 12-8 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Uploaded License File Name(s):	The name of the license file(s) that have been uploaded onto the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **ls -l ${TOMCAT_HOME}/webapps/license/***
Uploaded License File Contents:	The contents of the license file(s) that have been uploaded onto the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/license/***
Cisco IPICS Database Status:	The current status of the database. The database can be either online or offline. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **onstat -**
Cisco IPICS Tomcat Web Server Status:	The current status of the Tomcat service. The Tomcat service functions as the Web server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **top-ipics**
Cisco IPICS Radio Control Service Status:	The current status of the Cisco IPICS Radio Control service. This service controls serial radios. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **service ipics_rcs status**

Table 12-8 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS Server Hard Disk Utilization Information:	Usage information for the hard disks in the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **df -a**
Cisco IPICS IDC Configuration File Contents:	The contents of the idc.ini file. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/ipics_server/pmcdownloads/idc.ini** **Note** Cisco IPICS uses the idc.ini file to determine how to communicate with the Cisco IPICS server. The idc.ini file is present only if you have generated an IDC installer. If you have not yet generated the IDC installer file, Cisco IPICS displays the following message: `Cannot find any idc.ini files under the /opt/cisco/ipics/tomcat/current/webapps/ipics_files/store/installer folder.` For more information about the idc.ini file, and how to generate an IDC installer, see the "Managing IDC Versions" section on page 2-114.

Downloading the Server Diagnostic Information

Cisco IPICS displays the diagnostic summary of your system in the Diagnostic Summary pane. You can download this diagnostic summary, along with the current system log information, to your PC.

When you download the diagnostic summary, Cisco IPICS creates a tar file that contains the diagnostic summary and the most current ipics.log file. For more information about the ipics.log file, see the "Understanding the System Log Severities" section on page 12-11.

To download the server diagnostic information, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > Diagnostics**.

Step 2 Click **Download Diagnostic Results**.

The File Download dialog box displays.

Step 3 Click **Open** to open the tar file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The tar file opens and displays the following files:

- The **tacout** file contains the latest diagnostic summary information.
- The **ipics.log** file contains the latest log information for Cisco IPICS.
- The **lmgrd.log** file contains log information for the license manager.

Step 4 To save the tar file to your PC, click **Save**.

A Save As dialog box displays.

Step 5 Navigate to the location on your PC where you want to save the tar file.

Step 6 Click **Save**.

The system unpacks the **tacout**, **ipics.log** and **lmgrd.log** files from the tar file, saves the files to the location that you specified, and closes the Save As dialog box.

Step 7 Use a text file viewer on your PC to view the log files.

Note You must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Viewing the Cisco IPICS System Logs

Cisco IPICS provides the ability to view the latest server log information in the System Logs window. The Recent System Log Entries pane in the **Serviceability > System Logs** window contains the log information that shows you the processes that have occurred in the different components of the Cisco IPICS system. For example, you can view the recent Tomcat service or policy engine entries. The information that is contained in these logs can help you to troubleshoot problems that you might encounter with Cisco IPICS.

Tip To refresh this window and see updated status information, click **Refresh**.

You can view the log information by using the Administration Console or you can save the log to a file and download it to your PC.

Note Cisco IPICS provides you with other logs that are not available in the **System Logs window**. You can view and download logs such as the Activity Log in the Administration Console. Cisco IPICS provides additional logs that are available by accessing the server with a console terminal.

This section includes the following topics:

Understanding the System Log Severities

The system log entries include messages of different severities. These messages range from informational-level messages to messages that indicate that a fatal error has occurred with Cisco IPICS.

Table 12-9 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 12-9 System Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Messages that are similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane.
FATAL	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privileges. Also, FATAL messages display in red in the Recent System Log Entries pane. If you continue to encounter FATAL errors, or if you experience unexpected system failures, contact your Cisco technical support representative for further analysis.

Note By default, Cisco IPICS does not capture the TRACE and DEBUG messages in the system logs. Cisco recommends that you do not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Searching the System Logs By ERROR or WARNING Messages

To visually identify the type of status messages that display in the Recent System Log Entries pane, Cisco IPICS displays log entries of differing severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.
- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

Cisco IPICS displays the total number of ERROR, WARNING and INFO messages in the Status Summary area, directly below the Recent System Logs pane.

You can also view each ERROR or WARNING message by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Determine if there are any ERROR or WARNING messages in the log by viewing the Status Summary area, which is indicated by colored dots.

The Status Summary area provides you with the total number of messages that appear in the Recent System Log Entries pane.

If the number of red (ERROR) or blue (WARNING) messages is greater than zero, proceed to the next step.

Step 3 From the drop-down list that is located in the upper right of the window, choose one of the following options:

- **Errors—**To find ERROR-level messages
- **Warnings—**To find WARNING-level messages

Step 4 Click the arrow buttons to navigate and view each ERROR or WARNING message:

- Click **|<** to find the first message in the System Log.
- Click **<** to move backward one message in the System Log.
- Click **>** to move forward one message in the System Log.
- Click **>|** to move to the last message in the System Log.

Note If you are viewing the first message in the System Log, the **|<** and **<** arrow buttons appear dimmed. If you are viewing the last message in the System Log, the **>** and **>|** arrow buttons appear dimmed.

Downloading System Logs

Cisco IPICS displays the most current system log information in the Recent System Log Entries pane and allows you to download all of the system logs to your PC.

Cisco IPICS saves the log information in sequential log files, starting with ipics.log and continuing with ipics.log.1 through ipics.log.10.

- Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches a maximum size of approximately 5.2 MB.
- When the ipics.log file reaches its maximum size, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data.

  This process of filling and incrementing files continues until you have ten system log files that range from ipics.log.1 to ipics.log.10, in addition to the most recent ipics.log file.
- When you have accumulated ten files, Cisco IPICS automatically purges the oldest file.

When you download your system logs, Cisco IPICS creates a zip file of all the ipics.log files.

The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

To download the system logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Click **Download** at the bottom of the window, under the **Recent System Log Entries** pane.

The File Download dialog box displays.

Step 3 Click **Open** to open the ipics_logs.zip file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The zip file opens and displays the list of ipics.log files.

Note To view the log file, you must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Step 4 To save the zip file to your PC, click **Save**.

A Save As dialog displays, from which you can navigate to the location to save the zip file on your PC.

Step 5 If you chose to save the zip file, click **Save**.

The system unzips the files from the zip file, saves the files to the location you specified, and closes the Save As dialog box.

Viewing the Cisco IPICS RCS Logs

Cisco IPICS provides the ability to view the latest radio controls service (RCS) log information in the RCS Logs window. The Recent RCS Log Entries pane in the **Serviceability > RCS Logs** window contains the log information that shows information about the serial RCS and the radios that it controls. The information that is contained in these logs can help you to troubleshoot problems that you might encounter with serial radio control.

Tip To refresh this window and see updated status information, click **Refresh**.

You can view the log information by using the Administration Console or you can save the log to a file and download it to your PC.

Note Cisco IPICS provides you with other logs that are not available in the **RCS Logs window**. You can view and download logs such as the Activity Log in the Administration Console. Cisco IPICS provides additional logs that are available by accessing the server with a console terminal.

This section includes the following topics:

Understanding the RCS Log Severities

The RCS log entries include messages of different severities. These messages range from informational-level messages to messages that indicate that a fatal error has occurred with Cisco IPICS.

Table 12-10 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 12-10 RCS Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.
ERROR	Messages that are similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane.
FATAL	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privileges. Also, FATAL messages display in red in the Recent System Log Entries pane. If you continue to encounter FATAL errors, or if you experience unexpected system failures, contact your Cisco technical support representative for further analysis.

Note By default, Cisco IPICS does not capture the TRACE and DEBUG messages in the RCS logs. Cisco recommends that you do not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Searching the RCS Logs By ERROR or WARNING Messages

To visually identify the type of status messages that display in the Recent RCS Log Entries pane, Cisco IPICS displays log entries of differing severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.
- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

Cisco IPICS displays the total number of ERROR, WARNING and INFO messages in the Status Summary area, directly below the Recent RCS Logs pane.

You can also view each ERROR or WARNING message by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > RCS Logs**.

Step 2 Determine if there are any ERROR or WARNING messages in the log by viewing the Status Summary area, which is indicated by colored dots.

The Status Summary area provides you with the total number of messages that appear in the Recent RCS Log Entries pane.

If the number of red (ERROR) or blue (WARNING) messages is greater than zero, proceed to the next step.

Step 3 From the drop-down list that is located in the upper right of the window, choose one of the following options:

- **Errors—**To find ERROR-level messages
- **Warnings—**To find WARNING-level messages

Step 4 Click the arrow buttons to navigate and view each ERROR or WARNING message:

- Click **|<** to find the first message in the RCS Log.
- Click **<** to move backward one message in the RCS Log.
- Click **>** to move forward one message in the RCS Log.
- Click **>|** to move to the last message in the RCS Log.

Note If you are viewing the first message in the RCS Log, the **|<** and **<** arrow buttons appear dimmed. If you are viewing the last message in the RCS Log, the **>** and **>|** arrow buttons appear dimmed.

Downloading RCS Logs

Cisco IPICS displays the most current RCS log information in the Recent RCS Log Entries pane and allows you to download all of the RCS logs to your PC.

Cisco IPICS saves the log information in sequential log files, starting with rcs.log and continuing with rcs.log.1 through rcs.log.10.

- Cisco IPICS records RCS log information in the ipics.log file and continues to add data to it until the file reaches a maximum size of approximately 1 MB.
- When the rcs.log file reaches its maximum size, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new rcs.log file to capture the most current log data.

  This process of filling and incrementing files continues until you have ten system log files that range from rcs.log.1 to rcs.log.10, in addition to the most recent rcs.log file.
- When you have accumulated ten files, Cisco IPICS automatically purges the oldest file.

When you download your system logs, Cisco IPICS creates a zip file of all the rcs.log files.

The system logs are located in the following directory:

/opt/cisco/rcs/logs

To download the RCS logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > RCS Logs**.

Step 2 Click **Download** at the bottom of the window, under the **Recent RCS Log Entries** pane.

The File Download dialog box displays.

Step 3 Click **Open** to open the rcs_logs.zip file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The zip file opens and displays the list of rcs.log files.

Note To view the log file, you must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Step 4 To save the zip file to your PC, click **Save**.

A Save As dialog displays, from which you can navigate to the location to save the zip file on your PC.

Step 5 If you chose to save the zip file, click **Save**.

The system unzips the files from the zip file, saves the files to the location you specified, and closes the Save As dialog box.

Configuring System Event Email Notifications

The system event email notifications feature provides a way for the system to send notification to a designated email recipient if any of the following major system events occur. The trigger values that are shown are the default values. You can adjust these values as needed.

- The 1 minute load average exceeds 5
- The 5 minute load average exceeds 3

- Memory usage exceeds 75%
- User CPU usage exceeds 70%
- System CPU usage exceeds 40%
- I/O wait exceeds 40%
- The node manager process starts or stops
- The server HA state changes (active/standby)
- Any partition is more than 90% full, except for the /documents partition which sends notifications after it is 75% full.

The following sections describe the system event email notification feature:

- Configuring and Enabling System Event Email Notifications, page 12-17
- Disabling System Email Notifications, page 12-17
- Changing System Event Trigger Values, page 12-18

Configuring and Enabling System Event Email Notifications

After you configure and enable system email notifications, the system sends email messages to the designated recipient when major system events occur

To configure and enable system email notifications, perform the following steps.

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Event Notify**.

Step 2 In the SMTP Server field, enter the hostname or IP address of the Simple Mail Transfer Protocol (SMTP) server that is to be used for sending the notifications.

Step 3 In the Receiver (Administrator) Email ID field, enter the email address or mailing-list alias to which system event notifications are to be sent.

Step 4 Click **Enable**.

Disabling System Email Notifications

When you disable system email notifications, the system sends does not send email messages when major system events occur

To disable system email notifications, perform the following steps.

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Event Notify**.

Step 2 Click **Disable**.

Changing System Event Trigger Values

You can change the values at which system events are triggered. In this way, you can adjust the sensitivity for system events and, therefore, adjust the number of system event notifications that the system sends. For example, if the system is configured to trigger an event when CPU usage is greater than 75%, you can do either of the following:

- Decrease the CPU usage value (for example, to 65%) to make the system event more sensitive, which will result in more system event notifications being generated and sent.
- Increase the CPU usage value (for example, to 85%) to make the system event less sensitive, which will result in fewer system event notifications being generated and sent.

To change system event trigger values, perform the following procedure:

Before you begin

Obtain the following information:

- Hostname or IP address of the Cisco IPICS server
- Cisco IPICS server bash shell root credentials

Procedure

Step 1 Log in to the Cisco IPICS server bash shell using the root account.

Step 2 Enter the **vi /etc/monit.d/alerts.monitrc** command to open the alerts.monitrc file:

The VI editor opens and displays the contents of the alerts.monitrc file in command mode. The alerts.monitrc file contains a list of the system events and trigger values. For example, the list might look something like this:

```
check system localhost
    if loadavg (1min)     >   5 then alert
    if loadavg (5min)     >   3 then alert
    if memory usage       > 75% then alert
    if cpu usage (user)   > 90% then alert
    if cpu usage (system) > 40% then alert
    if cpu usage (wait)   > 40% then alert
```

Step 3 Enter insert mode and change one or more of the system event trigger values.

Step 4 Press the **ESC** key to exit insert mode.

The VI editor enters command mode.

Step 5 Enter **:q** to save the updated alerts.monitrc file and exit the VI editor.

Step 6 Enter the **monit reload** command to reinitialize the monit daemon.

Step 7 Enter the **monit status** command to verify your changes.