SEA Health Monitoring for the Cisco UBR10012 Routers

First Published: November 16, 2009

Last Updated: November 16, 2009

Maintaining a log of major and critical events and alarms helps the system administrator in identifying and resolving the problems from further occurrence. There are various other methods for reproducing the problems but these methods have limitations. The System Event Archive (SEA) is a health monitoring feature. It maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. The SEA feature maintains a log of hardware and software events and alarms in the sea_log.dat file. These generated events can be analyzed and copied to the sea_log.dat file at the specified location. The Cisco IOS Release 12.2(33)SCC introduces the SEA feature for Cisco Universal Broadband Router 10012.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for SEA

The table shows the hardware and software compatibility prerequisites for this feature.

Table 1: SEA Support for the Cisco CMTS Routers Hardware and Software Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards or Jacket Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[1] **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[2] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2	• Cisco Wideband SPA 2

1 Supports DOCSIS 2.0 and IPv6 cable modems.
2 Supports DOCSIS 3.0 and IPv6 cable modems.

Restrictions for SEA

- SEA event log feature only supports PCMCIA ATA disk or Compact flash disk in adapter for PRE2.
- Due to a limitation (reference CDETS ID: CSCsz77977) for performing Online-Insertion-Removal (OIR) of the disk on PRE2, the following actions are recommended before performing an OIR of the disk on PRE2:
- Disable SEA logging using **no logging system** command, before performing an OIR of disk on PRE2.
- Enable SEA logging using **logging system** command, after performing OIR of disk on PRE2.
- Use different disk for SEA logging and for storing Cisco IOS image. For example, if disk0: is used to store IOS image and is referenced in boot system command, use disk1: for storing SEA logging.
- For PRE4, keep the SEA storage on boot flash: (which is the default disk).

Information About SEA

The following sections provide the details of the SEA feature:

Importance of System Health Monitoring

Keeping a regular check of health of a system is essential. To provide high-availability for a router without any downtime it is imperative to analyze the stability of a system. The stability of a system is determined by system log messages and debug traces. If any of the log messages are ignored for a significant time, it can bring a system down. Essentially, the system log messages help in analyzing the root cause of the generated event. To prevent downtime, the root cause of the problem can be identified and resolved.

Limitations of Existing Logging Mechanisms

The primary method of discovering the cause of system failure is system messages. When system messages do not provide the information needed to determine the cause of a failure, you can enable debug traces and attempt to recreate the failure. However, there are several situations in which neither of the above methods provides an optimum solution. Following are the limitations of the existing logging mechanism:

- Reviewing a large number of system messages can be an inefficient method of determining the cause of a failure.
- Debug trace is usually not configured by default.
- You cannot recreate the failure while using debug trace.
- Using debug trace is not an option if the switch on which the failure has occurred is part of your critical network.
- The problem is not reproducible when debug trace is enabled due to change in timings.
- If the system is part of a critical network, it is not advisable to recreate or debug the issue.
- Unless the problem is reproduced, the exact root cause of the system failure is not known.

Understanding the System Event Archive

The SEA feature addresses the shortcomings of the existing logging mechanism. The SEA feature can help debug issues without reproducing the problem. The SEA runs on the route processor (RP). SEA allows each CPU to report major and abnormal events to the RP using the out-of-band interface and log it into the non-volatile storage using the time-stamp. The RP logs its own events to the boot flash disk. The RP receives event messages from the cable line card and jacket card over IPC, and logs them to the boot flash.

Logging Location

By default, the SEA feature is enabled and events are stored in the log file ‘sea_log.dat’ with the timestamp. The events are stored in sea_log.dat along with the timestamp. The SEA feature requires either PCMCIA ATA Flash or Compact Flash disk for storage. By default, on PRE2 the SEA creates the log file on disk0:. The SEA command enables changing the location (disk) of the sea_log.dat file using the **logging system disk** *name* command. The size of the sea_log.dat file is 32 MB or 10% of the disk size or at least 448KB. The sea_log.dat file stores the most recent event messages in the log file in a circular fashion.

Note SEA feature does not automatically search for a disk if the default disk or explicitly configured disk is not inserted.

Managing SEA

This section describes how to manage the system event archive. The following SEA commands are used to manage the SEA functionality.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**logging system** **Example:** `Router(config)# logging system`	Enables the SEA logging feature. By default, the SEA feature is enabled. **Note** To disable the SEA logging feature, use the **no logging system** command.
Step 2	**logging system disk disk1:** **Example:** `Router(config)# logging system disk disk1:`	Changes the disk location on PRE2 or PRE4 for storing the SEA log messages. **Note** By default, SEA log messages are stored on disk0: for PRE2 and on boot flash: for PRE4.
Step 3	**show logging system** **Example:** `Router# show logging system`	Displays the latest SEA log messages stored in the sea_log.dat file.
Step 4	**show logging system disk** **Example:** `Router# show logging system disk`	Displays the disk used to store the sea_log.dat file.
Step 5	**copy logging system target** *filename* **Example:** `Router# copy logging system target filename`	Copies the sea_log.dat file to the destination file system.
Step 6	**clear logging system** **Example:** `Router# clear logging system`	Clears the events stored in the sea_log.dat file.
Step 7	**logging cmts sea** **Example:** `Router#config t`	Enables logging of system log messages to SEA.

	Command or Action	Purpose
	Example: `Router(config)# logging cmts sea`	

Step 8	**logging cmts sea syslog-level warnings**
	Example:
	`Router# config t`
	Example:
	`Router(config)# logging cmts sea syslog-level warning`
		Configures the level of system log messages inclusive of and above the configured level to be stored in sea_log.dat file. The example shows the configuration to store system log messages with severity 'warning' and above to be stored in the sea_log.dat file.

Probable Scenarios and Useful SEA Commands

The table discusses the various scenarios and how to use the SEA commands for managing the event logs.

Table 2: Possible Scenarios and Useful SEA Commands

Possible Scenarios	Command Used	Explanation
To check whether SEA feature is enabled.	`Router# dir disk0:` `23 -rw-  6710888 May 16 2009 06:03:36 +00:00 sea_log.dat`	By default, SEA is enabled and the command is not shown under the "show running. To check the log file location, execute the **dir [diskname]** command from EXEC command mode. **Note** On PRE2, the default location to store the SEA log message is disk0:.
To check the latest SEA log messages.	`Router# show logging system`	To check the latest SEA log messages, execute the **show logging system** command from EXEC mode. The SEA log messages are stored with the actual time-stamp, slot/sub-slot number, name of software generating the system event, and the event message. **Tip** The sea_log.dat file is created as soon as the first SEA log message is stored in the file.
To check the current location to store the sea_log.dat file.	`Router# show logging system disk` `SEA log disk: disk0:`	If you are unsure of the disk currently storing the SEA event log messages, execute the **show logging system disk** command. As shown in the example, it displays the SEA log disk currently used to store the sea_log.dat file.
To check the last 'n' number of SEA event log messages.	`Router# show logging system last 5`	The system administrator can also check the desired number of last messages stored in the sea_log.dat file. Use the **show logging system last** *5* command to view the last 5 messages stored in the log file. **Tip** The valid range to display the last number of SEA messages is 1 to 10,000.
To change the location of the sea_log.dat file to a different disk.	`Router(config)# logging system disk disk1:` `You are configuring a different disk from the current log disk.`	To change the location of the sea_log.dat file execute the command **logging system disk diskname** from global configuration mode. **Note** After changing the disk, the new event log information is logged to the new location (in this example disk1:) and the log event information before the change disk is available at the old location (in this case disk0:).

Possible Scenarios	Command Used	Explanation

Copying the SEA event log messages to a target file.	`Router# copy logging system rcp`
	`Address or name of remote host []?`
	`192.0.2.1`
	`Destination username [Router]?`
	`username1`
	`Destination filename [sea_log.dat]?`
	
	`/auto/tftpboot-users/username1/sea_log.dat`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
		The advantage of SEA feature is that you can copy and back up SEA event log messages at specific target file locations. Use the **copy logging system target** *filename* command to copy the sea contents to the desired location.
		Note Copying the SEA event log file is useful when there is less disk space available on the disk or the disk is almost full.

To clear the SEA event log messages stored on the disk.	`Router# clear logging system`
	
	`Clear logging system operation will take a while.`
	`Do you want to continue? [no]: yes`
		After taking a back up of SEA event log messages, you can clear the event log details stored at the default location using the **clear logging system** command.
		Note Before clearing the event log messages, it is recommended to take a back up of the SEA event log messages to a target file system.

Configuring a different disk to store the sea_log.dat file without the disk being present, provides an error message.	`Router(config)# logging system disk disk1:` `disk1: does not exist in the system`	Before changing the location of the disk, check if the target disk is present on PRE2 or PRE4. If the disk is not present then the **logging system disk disk1:** command, generates an error message. **Note** SEA will not automatically search for the disk, if the default disk is not inserted.
Configuring bootflash: as the disk to store log messages on PRE2, provides an error message.	`Router(config)# logging system disk bootflash:` `bootflash: is not allowed`	The supported disk to store the sea_log.dat file is either PCMCIA ATA flash disk or Compact Flash disk in PCMCIA jacket. If bootflash: is configured to store the log messages on PRE2 using the logging system disk bootflash: command, it generates an error message. In the example, a linear flash disk is configured to store the SEA log messages, hence an error message is shown. **Note** The SEA event log messages cannot be stored on a linear flash disk.
Changing the level of system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.	`Router(config)# logging cmts sea syslog-level warning`	

Possible Scenarios	Command Used	Explanation
		By default, the system log event message to be stored in the log file is enabled with the severity-level of system log messages being set to 'errors'. Use the **logging cmts sea syslog-level warning** command to configure the system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.

Additional References

For additional information related to health monitoring, see the following references:

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Generic Online Diagnostics (GOLD)	GOLD feature for the Cisco UBR10012 Universal Broadband Router

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SEA for the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 3: Feature Information for System Event Archive (SEA) for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
System Event Archive (SEA) Support for the Cisco CMTS Routers	12.2(33)SCC	The System Event Archive (SEA) is a health monitoring feature that maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. This feature was introduced for the PRE2 and PRE4 route processors. The following commands are new or modified: • **logging system** • **show logging system** • **copy logging system** • **clear logging system** • **logging cmts sea** [**syslog-level** [**level**]]