APPENDIX C

Installing the Remote Syslog Collector

This appendix provides general information on how to install the Remote Syslog Collector on a remote Windows or UNIX system to process syslog messages.

The Remote Syslog Collector filters the Syslog messages before forwarding them to the Analyzer process on the LMS server.

Warning **Do not install Remote Syslog Collector on a system that has LMS 4.1 already installed.**

The Remote Syslog Collector and Syslog Analyzer Service on the LMS server uses SSL sockets to communicate with each other.

It functions as follows:

1. At startup, the Remote Syslog Collector looks for Syslog Analyzers already subscribed on the LMS Server and requests for the latest filter definitions.

- If the Syslog Analyzer is not reachable when queried, the Remote Syslog Collector logs all emblem compliant syslogs in the specified *downtime file* after filtering.

  The Syslog Collector Properties file is available at these locations:

  - On Solaris and Soft Appliance:

    /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties

  - On Windows:

    NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties

- If the Syslog Analyzer responds with the latest filters, the Remote Syslog Collector applies filters and forwards syslogs to the Syslog Analyzer.

2. At startup, the Syslog Analyzer tries to connect to all the subscribed Remote Syslog Collectors by passing the latest filters.

To subscribe or unsubscribe from a Remote Syslog Collector, select **Admin > Collection Settings > Syslog > Syslog Collector Status** from the menu.

After the Remote Syslog Collector connects to the LMS 4.1 Server, the Remote Syslog Collector entry is added to the Collector Status window of the LMS 4.1 Server.

To view the status of the subscribed Syslog Collector, select **Admin > Collection Settings > Syslog > Syslog Collector Status**.

This section describes how to set up Syslog between RSAC and LMS 4.1. This involves:

- Verifying Remote Syslog Collector Server Requirement
- Installing the Remote Syslog Collector
- Stopping the Remote Syslog Collector
- Uninstalling the Remote Syslog Collector

Verifying Remote Syslog Collector Server Requirement

The following section lists the necessary server requirements for Remote Syslog Collector:

- Table C-1 provides the server requirements for Remote Syslog Collector on Solaris.
- Table C-2 provides the server requirements for Remote Syslog Collector on Windows.
- Table C-3 provides the server requirements for Remote Syslog Collector on Soft Appliance.

Table C-1 Remote Syslog Collector Server Minimum Requirements on Solaris

Requirement Type	Minimum Requirements
Hardware	UltraSPARC CPU
Memory (RAM)	• 4 GB RAM and 8 GB Swap space.
Operating System	• Solaris 10
Browser (You need a browser only if you download the RSAC installation files from the LMS 4.1 server.)	Not Supported

Table C-2 Remote Syslog Collector Server Minimum Requirements on Windows

Requirement Type	Minimum Requirements
Hardware	IBM PC-compatible system with 1 GHz or faster Pentium processor, and 1 GB memory.
Memory (RAM)	2 GB RAM memory requirement with a Swap space of 4 GB.
Operating System	LMS 4.1 supports the following Windows systems: • Windows 2008 Server Standard Edition (SP1 and SP2) • Windows 2008 Server Enterprise Edition (SP1 and SP2) • Windows 2008 Standard Edition R2 (SP2) • Windows 2008 Enterprise Edition R2 (SP2)
Browser (You need a browser only if you download the Remote Syslog Collector installation files from the LMS 4.1 server.)	• Internet Explorer 8.x Standards Mode (Press F12 and select Standards Mode) • Firefox 4.0.x and 5.0.x for Windows

Table C-3 Remote Syslog Collector Server Minimum Requirements on Soft Appliance

Requirement Type	Minimum Requirements
Virtualization Systems	• VMWare ESX server 4.1 • VMWare ESXi server 4.1
Memory (RAM)	4 GB RAM memory requirement with a Swap space of 8GB.
Hard disk space	80 GB
Operating System	LMS 4.1 supports the following Windows systems: • Windows 2008 Server Standard Edition (SP1 and SP2) • Windows 2008 Server Enterprise Edition (SP1 and SP2) • Windows 2008 Standard Edition R2 (SP2) • Windows 2008 Enterprise Edition R2 (SP2)
Browser (You need a browser only if you download the Remote Syslog Collector installation files from the LMS 4.1 server.)	• Internet Explorer 8.x Standards Mode (Press F12 and select Standards Mode) • Firefox 4.x, and 5.x for Windows **Note** Only 32-bit IE and FF browsers are supported

The following Virtualization systems are supported:

- VMware ESX server 3.0.x
- VMware ESX Server 3.5.x
- VMWare ESX 4.0.x
- VMWare ESX 4.1
- VMWare ESXi 4.0
- Hyper V Virtualization

RSAC 5.1 works only with LMS 4.1.

You must uninstall the previous version of RSAC before installing the new RSAC which is provided with LMS 4.1 DVD. To install RSAC 5.1, see Installing the Remote Syslog Collector.

Installing the Remote Syslog Collector

Perform the following to install the Remote Syslog Collector on both platforms.

- Installing on Solaris
- Installing on Windows
- Installing on Soft Appliance

Prerequisites for installing a Remote Syslog Collector:

- LMS 4.1 and RSAC 5.1 should be installed.
- If you install LMS Service Pack on the LMS server, you must install the same Service Pack on the RSAC server.

  The LMS Service Pack versions must be same in the LMS Server and RSAC Server.
- LMS 4.1 should not be installed on the server where you need to install the Remote Syslog Collector. (If LMS 4.1 is installed, the Syslog Collector is installed by default).

This section also contains:

- Subscribing to a Remote Syslog Collector
- Starting the Remote Syslog Collector
- Stopping the Remote Syslog Collector
- Uninstalling the Remote Syslog Collector

Installing on Solaris

To install the Remote Syslog Collector on a Solaris system:

Step 1 Mount the LMS 4.1 DVD.

The RSAC installables are available in the RSAC directory on LMS 4.1 DVD.

Step 2 Enter the following to start the installation:

```
# cd RSAC
# ./setup.sh
```

Step 3 Follow the wizard instructions to install the product.

After the installation of Remote Syslog Collector, select **Admin > System > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

After Installation, you need to configure the collector.properties file if required. If not, you can use the defaults. See Understanding the Syslog Collector Properties File.

Installing on Windows

To install the Remote Syslog Collector on a Windows system:

Step 1 Navigate to the RSAC folder on the LMS 4.1 DVD.

Step 2 Double-click the **Setup.exe** file to start the installation.

Step 3 Follow the wizard instructions to install the product.

After the installation of Remote Syslog Collector, select **Admin > System > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

After Installation, you need to configure the collector.properties file if required. If not, you can use the defaults. See Understanding the Syslog Collector Properties File.

Installing on Soft Appliance

To install the Remote Syslog Collector on a LMS Soft Appliance system (OVA file):

Step 1 Go to http://www.cisco.com/cisco/software/release.

Step 2 Download the rsac51-190.ova file to the VMware server where you want to deploy the OVA image.

Step 3 Follow the installation steps for installing the LMS Soft Appliance OVA file in the section Installing LMS Soft Appliance - OVA Image.

After the installation of Remote Syslog Collector, select **Admin > System > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

To install the Remote Syslog Collector on a LMS Soft Appliance system (ISO file):

Step 1 Go to http://www.cisco.com/cisco/software/release.

Step 2 Download the Remote_Syslog_Collector_5_1.iso file to the VMware server where you want to deploy the ISO image.

Step 3 Follow the installation steps for installing the LMS Soft Appliance ISO file in the section Installing LMS 4.1 Soft Appliance - ISO Image.

After the installation of Remote Syslog Collector, select **Admin > System > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

Subscribing to a Remote Syslog Collector

Step 1 Download the Peer certificate from the system where Remote Syslog Collector is running.

Step 2 Upload the Peer certificate to the system where Remote Syslog Collector is running.

Step 3 Select **Admin > Collection Settings > Syslog > Syslog Collector Status**.

The Collector Status dialog box appears with this information:

Column	Description
Name	Hostname or the IP address of the host on which the Collector is installed.
Update Time	Date and time of the last update. By default, this dialog box is updated every 5 minutes. Time and time zone are those of the LMS Server.
Uptime	Time duration for which the Syslog Collector has been up.
Forwarded	Number of forwarded Syslog messages.
Dropped	Number of unprocessed Syslog messages.
Invalid	Number of invalid Syslog messages.
Filtered	Number of filtered messages. Filters are defined with the Define Message Filter option (select **Admin > Network > Notification and Action Settings > Syslog Message Filters** from the menu). For details about defining filters, see *Administration of Cisco Prime LAN Management Solution 4.1*.
Received	Number of Syslog messages received.
Test Collector Subscription	Click to test a Syslog collector that's already subscribed or that's going to be subscribed.
Subscribe	Click to subscribe a Syslog collector.
Unsubscribe	Select the Syslog collector and click Unsubscribe to unsubscribe the Syslog collector.

Step 4 Click **Subscribe**.

The Subscribe Collector dialog box appears.

Step 5 Enter the address of the Common Syslog Collector to which you want to subscribe to.

Step 6 Click **OK**.

The Syslog Analyzer is subscribed the Syslog Collector that you specified. This can be either the Syslog Collector on the LMS server, or a remotely installed Syslog Collector.

Starting the Remote Syslog Collector

To start the Remote Syslog Collector, enter **`pdexec SyslogCollector`** at the command prompt on the machine where Syslog Collector is installed. It starts by default.

Stopping the Remote Syslog Collector

To stop the Remote Syslog Collector, enter **`pdterm SyslogCollector`** at the command prompt on the machine where Syslog Collector is installed.

Uninstalling the Remote Syslog Collector

Perform the following to uninstall RSAC:

- Uninstallation on Windows
- Uninstallation on Solaris
- Uninstallation on Soft Appliance

Uninstallation on Windows

To uninstall on a Windows system:

Step 1 Select **Start > Programs > CiscoWorks > Uninstall CiscoWorks**.

The Uninstallation dialog box appears, displaying all of the installed components.

Step 2 Select **Remote Syslog Collector**.

Step 3 Click **Next** to begin uninstalling the selected component.

Uninstallation on Solaris

To uninstall on a Solaris system:

Step 1 Enter these commands as root to start the uninstall program:

```
# cd /
# NMSROOT/bin/uninstall.sh
```

Step 2 Follow the prompts from the uninstallation wizard.

Uninstallation on Soft Appliance

Uninstallation of Remote Syslog Collector is not supported in the Soft Appliance.

Understanding the Syslog Collector Properties File

After installing the Syslog Collector on a remote machine, you need to check the Syslog Collector Properties file to ensure that the Collector is configured properly.

The Syslog Collector Properties file is available at these locations:

- On Solaris and Soft Appliance:

  /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties
- On Windows:

  NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties

The following table describes the Syslog Collector Properties file:

Timezone-Related Properties	Description
TIMEZONE	The timezone of the machine where the Syslog Collector is running. Enter the correct abbreviation for the timezone. For example, the time zone for India is IST. For the correct Timezone abbreviation, see the Timezone file in the following locations: • On Solaris and Soft Appliance: /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst • On Windows: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\TimeZone.lst
COUNTRY_CODE	Country code for the Syslog Collector. We recommend that you set the country code variable with the appropriate country code, to make sure that the Syslog timestamp conversion works correctly. For example, if you are in Singapore, you must set the country code variable as **`COUNTRY=`***SGP*.
TIMEZONE_FILE	The path of the Timezone file. This file contains the offsets for the time zones. After installing the Syslog Collector, ensure that the offset specified in this file is as expected. If it is not present or is incorrect, you can add the Timezone offset according to the convention. The default paths are: • On Solaris and Soft Appliance: /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst • On Windows: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\TimeZone.lst

Timezone-Related Properties	Description
General Properties	
SYSLOG_FILES	Filename and location of the file from which syslog messages are read. • On Solaris and Soft Appliance: /var/log/syslog_info • On Windows: *NMSROOT*\log\syslog.log
DEBUG_CATEGORY_NAME	Name Syslog Collector uses for printed ERROR or DEBUG messages. The default category name is SyslogCollector. We recommend that you do not change the default value.
DEBUG_FILE	Filename and location of the Syslog Collector log file containing debug information: • On Solaris and Soft Appliance: /var/adm/CSCOpx/log/CollectorDebug.log • On Windows: *NMSROOT*\log\CollectorDebug.log
DEBUG_LEVEL	Debug levels in which you run the Syslog Collector. We recommend that you retain the default INFO, which reports informational messages. Setting it to any other value might result in a large number of debug messages being reported. If you change the debug level, you must restart the Syslog Collector. The values for the Debug levels are: • Warning • Debug • Error • Information
DEBUG_MAX_FILE_SIZE	The maximum size of the log file containing the debug information. The default is set to 5 MB. If the file size exceeds the limit that you have set, Syslog Collector writes to another file, based on the number of backup files that you have specified for the DEBUG_MAX_BACKUPS property. For example, if you have specified the number of backups as 2, besides the current log file, there will be two backup files, each 5MB in size. When the current file exceeds the 5 MB limit, Syslog Collector overwrites the oldest of the two backup files.
DEBUG_MAX_BACKUPS	The number of backup files that you require. The size of these will be the value that you have specified for the DEBUG_MAX_FILE_SIZE property.

Timezone-Related Properties	Description
Miscellaneous Properties	
READ_INTERVAL_IN_SECS	The interval at which the Collector polls the syslog file. The default is set to 1 second.
QUEUE_CAPACITY	The size of the internal buffer, for queuing syslog messages. The default is set to 100000.
PARSER_FILE	The file that contains the list of parsers used while parsing syslog messages. • On Solaris and Soft Appliance: /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/FormatParsers.lst • On Windows: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\FormatParsers.lst
SUBSCRIPTION_DATA_FILE	The Syslog Collector data file that contains the information about the Syslog Analyzers that are subscribed to the Collector. • On Solaris: /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Subscribers.dat • On Windows: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Subscribers.dat
FILTER_THREADS	The number of threads that operate at a time for filtering syslog messages. The default is set to 1.
COLLECTOR_PORT	The default port of the Syslog Collector. The default is set to 4444. The port where the collector listens for registration requests from Syslog Analyzers.