



Installing the Remote Syslog Analyzer Collector

This appendix provides general information on how to install the Remote Syslog Analyzer Collector (RSAC) on a remote UNIX system to process Syslog messages. If necessary, it can also filter the Syslog messages before forwarding them to the Syslog Analyzer process on the Essentials server. You can uninstall the Syslog Analyzer Collector later, if you do not want to run it on the remote UNIX server.



Note

Do not install RSAC on a machine that has CiscoWorks and Resource Manager Essentials already installed, or stop the CMF Syslog Service before installing RSAC.

This is because CMF Syslog Service will hook to the UDP port and read all the syslog messages. When the SacNTService tries to connect to the same port, it gets a ‘address not found’ exception, and would not read any syslog messages arriving on the port.

The Syslog Analyzer Collector uses CORBA, an Essentials system service, to communicate with the Essentials server. It functions as follows:

1. At startup, the Syslog Analyzer Collector tries to connect to the Syslog Analyzer on the Essentials server through CORBA (RmeOrb process), which runs on the Essentials server.

2. After it is connected, the Syslog Analyzer Collector:
 - a. Obtains the filters it needs from the Essentials server to filter syslog messages.
 - b. Sends status to the Syslog Analyzer process about the collected Syslog messages, including the number of messages read, number of messages filtered, and number of messages with bad syntax. It also forwards unfiltered messages to the Syslog Analyzer process.

**Note**

If Essentials server is restarted, the Syslog Analyzer Collector loses the CORBA communication to the server. The Syslog Analyzer Collector will automatically restore the connection.

This section describes how to set up Syslog. This involves:

- [Verifying RSAC Server Requirement](#)
- [Upgrading a Syslog Analyzer Collector](#)
- [Preparing to Install a Syslog Analyzer Collector](#)
- [Installing the Syslog Analyzer Collector](#)
- [Starting Up the Syslog Analyzer Collector](#)
- [Stopping the Syslog Analyzer Collector](#)
- [Uninstalling the Syslog Analyzer Collector](#)

Verifying RSAC Server Requirement

Table A-1 provides the server requirements for RSAC:

Table A-1 RSAC Server Minimum Requirements

Requirement Type	Minimum Requirements
Hardware	Sun Sparc Ultra 10
Memory (RAM)	128 MB
Available disk drive space	<ul style="list-style-type: none"> • 500 MB on the partition on which you install RSAC (the default is /opt). • Swap space equal to the amount of memory (RAM). For example, if your system has 128 MB of RAM, you need 128 MB of swap space.
Software	Solaris 2.7 and 2.8
Browser (You need a browser only if you download the RSAC installation files from the Essentials server.)	Netscape 4.76

Upgrading a Syslog Analyzer Collector

If you have previously installed a remote Syslog Analyzer Collector with Java Runtime Environment (JRE) 1.1.6, and you are upgrading to a new remote collector, you must:

-
- Step 1** Uninstall JRE 1.1.6.
 - Step 2** Uninstall the Syslog Analyzer Collector. To do this see, [Uninstalling the Syslog Analyzer Collector, page A-8](#)
 - Step 3** Install a version of JRE that is 1.2.1 or higher.
You can now reinstall Syslog Analyzer Collector.
-

Preparing to Install a Syslog Analyzer Collector

Make sure JDK or JRE is installed on the machine on which you will install the Syslog Analyzer Collector. On a Solaris system, JRE 1.2 is the lowest version you can use to run the remote Syslog Analyzer Collector.

You can access the Sun Microsystem's site for JRE 1.2 and above at the following URL:

<http://java.sun.com/products/jdk/1.2/jre>

or you can obtain it from the server as follows:

Step 1 Obtain the JRE from the server in the `/opt/CSCOPx/lib/jre` directory by entering:

```
#cd /opt/CSCOPx/lib/
#tar cvf /jre2.tar jre2
```

Step 2 Using FTP, transfer the `/jre2.tar` file to the client machine.

Step 3 Enter:

```
# tar xvf /jre2.tar
```

Step 4 Obtain the installation file from the Essentials server using either of the following methods:

Through FTP:

1. Navigate to the remote Essentials server:
 - On Solaris: `/opt/CSCOPx/htdocs/rdist/sysloga`
 - On Windows: (By default, FTP is not available on the Windows system.) `NMSROOT/htdocs/rdist/sysloga`.

where `NMSROOT` is the CiscoWorks installed directory.
2. Copy the `SAC.bin.Z` file.

or

Through a browser on the remote server:

1. Log in to the CiscoWorks server.
2. Browse to Syslog Remote Collector file location page:
 - If SSL is enabled on the CiscoWorks Server, the URL is:
`https://CiscoWorks-server:1742/sysloga/SAC.html`

- If SSL is not enabled, the URL is:
 `http://CiscoWorks-server:1741/sysloga/SAC.html`
 - 3. Click on UNIX Remote Collector and download the SAC.bin.Z file.
-

Installing the Syslog Analyzer Collector

- Step 1** Log in to the remote server as root.
- Step 2** Set the JRE CLASSPATH *variable* to the appropriate directory or Jar files.
- Step 3** Uncompress SAC.bin.Z by entering:
- ```
uncompress SAC.bin.Z
```
- Step 4** Run the Bourne-shell script SAC.bin. For example, `sh SAC.bin`.
- Step 5** When the installation script prompts you to install the CSCOsac package, select a directory:
- If you do not select a directory, the product is installed in the /opt directory, by default.
  - If you do select a directory, enter the fully qualified pathname to the directory so that a symbolic link can be made to it from the /opt directory.



### Caution

Do not remove the symbolic link between the /opt directory and the selected directory.

---

The installation script creates a `sacStart.sh` script and a `sacStop.sh` script in the /opt/CSCOsac/lib directory (Where /opt/CSCOsac is the default RSAC installation directory.). These scripts are used to start and stop the Syslog Analyzer collector.

- Step 6** Ensure that the entry `local7.info` is present in /etc/syslog.conf file. This is because the install routine does not add this entry to the syslog.conf file. Also, the first occurrence of local7.info must contain the path for the Syslog message source.

If `local7.info` is not present, make an entry in the /etc/syslog.conf file as follows: `local7.info /var/log/syslog_info`.

- Step 7** Restart the syslog daemon after making the changes.
- The script will also prompt you for the location of the JRE or Java executable. For example:
- If the JRE or Java executable is installed in `/usr/jdk1.2/bin`, enter:  
`/usr/jdk1.2/bin`
  - If JRE or Java executable is installed in `/opt/CSCOpX/lib/jre2/bin/sparc/native-threads/` enter:  
`/opt/CSCOpX/lib/jre2/bin/sparc/native-threads`
- Step 8** Before you start the Syslog Analyzer collector, modify the `SAenvProperties.ini` file in the following directory:
- `/opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/sac`  
where `/opt/CSCOsac` is the default RSAC installation directory.
- Step 9** Use the values in the [Table A-2](#) to modify the `SAenvProperties.ini` file. See [Table A-3](#) for detailed description of RSAC `SAenvProperties.ini` file variables.
-

## Starting Up the Syslog Analyzer Collector

You can use two methods to start up the Syslog Analyzer collector:

- [Automatically Starting Up Syslog Analyzer Collector](#)
- [Manually Starting Up Syslog Analyzer Collector](#)

### Automatically Starting Up Syslog Analyzer Collector

To start the Syslog Analyzer collector when the server boots, add the start script

```
sacStart.sh
```

to the system boot startup files.

### Manually Starting Up Syslog Analyzer Collector

To start up RSAC manually, you can either use CLI or SAenvProperties.ini file. Since the UNIX shell does not allow you to enter a long RSAC command using CLI, you must use the SAenvProperties.ini file to enter such commands.

For example, on Korn shell, if you enter a RSAC command, longer than 256 characters, the command gets truncated after 256 characters. In this case, you must use the SAenvProperties.ini file to enter this RSAC command.

- To start the collector without passing it arguments (using SAenvProperties.ini), enter:

```
sh /opt/CSCOsac/lib/sacStart.sh
```

where /opt/CSCOsac is the default RSAC installation directory.

- To start the collector with passing it arguments on CLI:
  - a. Set your classpath to `/opt/CSCOsac/classpath`, for example, if the default shell is `csh`, enter: `setenv CLASSPATH`

```
#{classpath}:/opt/CSCOsac/lib/classpath
```

- b. Pass the Syslog Analyzer collector arguments by entering:

```
java -Xbootclasspath/p:RSAC_install_directory/lib/classpath/
vbjorb.jar:RSAC_install_directory/lib/classpath/
vbjapp.jar com.cisco.nm.sysloga.sac.TransProcess [arguments]
```

where `RSAC_install_directory` is the RSAC installation directory. By default, it is `/opt/CSCOsac`.

The `TransProcess` executable is located in the `/opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/sac` directory.



#### Note

Specify arguments only if you want parameters that differ from those in your `SAenvProperties.ini` file. Use the values in [Table A-2](#) to modify the `SAenvProperties.ini` file. See [Table A-3](#) for detailed description of the ini file variables.

## Stopping the Syslog Analyzer Collector

To stop the Syslog Analyzer collector, enter:

```
sh /opt/CSCOsac/lib/sacStop.sh
```

or

you can stop the Java or JRE process if it was started manually.

## Uninstalling the Syslog Analyzer Collector

To uninstall the Syslog Analyzer Collector, enter the following in the `/opt` directory:

```
rm -rf CSCOsac
```

## Properties Variables Table

See [Table A-2](#) for detailed description of RSAC SAenvProperties.ini file variables.

**Table A-2 Properties Variables Table**

| Variable        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>BINDNAME</i> | <p>Name used by Syslog Analyzer collector to bind to OSAgent process. Value should be the same as value set for <i>SAC_SERVER</i> and followed by <i>::SaReceiver</i>.</p> <p>For example, if <i>SAC_SERVER</i> is set to <i>nm_bgdemo.cisco.com</i>, then <i>BINDNAME</i> should be set to <i>nm-bgdemo::SaReceiver</i>.</p> <p>Make sure the name you enter for this variable matches the Essentials server name exactly.</p> <p>To find out the name under which the Essentials server is registered, refer to the value set for <i>PX_HOST</i> in the <i>NMSROOT/lib/classpath/md.properties</i> file located on the Essentials server. (Where <i>NMSROOT</i> is the Essentials installed directory.)</p> |
| <i>COUNTRY</i>  | <p>Country code for the Syslog Remote Collector.</p> <p>To ensure that the Syslog timestamp conversion works correctly, we recommend that you set the country code variable with the appropriate country code.</p> <p>For example, if you are in Singapore, you must set the country code variable as <i>COUNTRY=SGP</i>.</p> <p>For a list of country codes, see the file, <i>CountryCode.txt</i>, located in the directory:</p> <p><i>\$NMSROOT/lib/classpath/com/cisco/nm/sysloga/CountryCode.txt</i></p> <p>where <i>NMSROOT</i> is the Essentials installed directory.</p> <p>The country code is the 3-letter abbreviation specified in the <i>CountryCode.txt</i> (in column A 3).</p>                 |

Table A-2 Properties Variables Table (continued)

| Variable                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>DEBUG_LEVEL</i>      | <p>Debug level in which you run the Syslog Analyzer collector.</p> <p><b>Note</b> It is recommended that you leave the default 4, which reports ERRORS. Setting it to any other value might result in a large number of debug messages being reported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <i>FILE</i>             | <p>File from which syslog messages are read. Set a value if a syslog daemon is running on the server. This variable is applicable only on UNIX systems.</p> <p>On UNIX systems, specify file from which Syslog Analyzer collector will read syslog messages. By default, device syslog messages go to the file pointed to by the local7 facility in /etc/ syslog.conf.</p> <p><b>Note</b> The first occurrence of local7 in the syslog.conf file, must contain the path for the Syslog message source.</p>                                                                                                                                                                        |
| <i>LOGFILE_LOCATION</i> | <p>Location and filename to save the Syslog Remote Collector log file.</p> <p>By default this file is stored in the install directory.</p> <p><b>On Solaris:</b><br/> /opt/CSCOsac/lib/SyslogRemoteCollector.log<br/> Where /opt/CSCOsac is the default RSAC installation directory.<br/> If the install directory is changed, then the location of the log file is:<br/> /changed_dir/lib/SyslogRemoteCollector.log</p> <p><b>On Windows:</b><br/> c:\Program Files\SyslogRemoteCollector.log<br/> If the install directory is changed, then the location of the log file is:<br/> drive_name:\location_directory\logfile_name</p> <p><b>Note</b> You must mention the path.</p> |
| <i>SA_APP_NAME</i>      | <p>Name Syslog Analyzer collector uses for printed ERROR or DEBUG messages. We recommend that you leave the default, SyslogAnalyzer.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table A-2 Properties Variables Table (continued)

| Variable                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>SAC_PORT</i>                 | <p>Number of the port on which syslog messages are coming in, typically, port 514. This variable is applicable only on Windows systems.</p> <p>On Windows systems, specify number of port from which Syslog Analyzer collector reads syslog messages.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>SAC_SERVER</i>               | Essentials server to which Syslog Analyzer collector forwards parsed and filtered messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <i>SAC_SERVER_PORT</i>          | <p>Number of port used by RmeOrb process on Essentials server.</p> <p>To check port number:</p> <ol style="list-style-type: none"> <li>Using a browser, log in to the Essentials server.</li> <li>Select CiscoWorks Server &gt; Administration &gt; Process Management &gt; Process Status.<br/>The Process Status table is displayed.</li> <li>Scroll down and click RmeOrb. The Process Details window is displayed.</li> <li>In the Flags column, note the port number (after the -p option).</li> </ol>                                                                                                                                                                                                                                                                              |
| <i>UNSENT_SLG_MSG_FILE_NAME</i> | <p>Name of the local log file where RSAC should write the received messages when the CiscoWorks Server is down.</p> <p>If you have specified a valid location and a file name, the Syslog messages will be stored in the specified location with the specified file name. Otherwise the file will be stored in the default location with the default log file name.</p> <p>If you have not specified a valid location but only a file name, the Syslog messages will be stored in the default location with the specified file name.</p> <p>On Windows the default location and filename is:<br/>C:\Program Files\unsentSyslogMessages.log</p> <p>On Solaris the default location and filename is:<br/>/opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/<br/>unsentSyslogMessages.log</p> |

## Properties Arguments Table

See [Table A-3](#) for detailed description of RSAC SAenvProperties.ini file variables arguments.

**Table A-3** *Properties Arguments Table*

| Switch /Arguments                             | Description                                                                                       |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>-bnd</b> <i>BINDNAME</i>                   | orb bind name                                                                                     |
| <b>-bsn</b> <i>SAC_SERVER</i>                 | Essentials server name                                                                            |
| <b>-bsp</b> <i>SAC_SERVER_PORT</i>            | Essentials port number                                                                            |
| <b>-cc</b> <i>COUNTRY</i>                     | Country code for the Syslog Remote Collector.                                                     |
| <b>-dbg</b> <i>DEBUG_LEVEL</i>                | Debug modes 1-6                                                                                   |
| <b>-h</b>                                     | Print usage information                                                                           |
| <b>-lf</b> <i>LOGFILE_LOCATION</i>            | Syslog Remote Collector log file location.                                                        |
| <b>-pr</b> <i>path to SAenvProperties.ini</i> | Path of the Property file name                                                                    |
| <b>-sf</b> <i>FILE</i>                        | Syslog file name                                                                                  |
| <b>-uf</b> <i>UNSENT_SLG_MSG_FILE_NAME</i>    | Name of the local log file where RSAC should write the received messages when the Server is down. |