



Installing the Remote Syslog Analyzer Collector on UNIX

The Syslog Analyzer Collector can be installed 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.

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.

CISCO SYSTEMS



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.



Note

When the Essentials server is restarted, the Syslog Analyzer Collector loses the CORBA communication with the server. The Syslog Analyzer Collector must be manually restarted to restore the connection.

You can install the Syslog Analyzer Collector on both UNIX and Windows systems.

This document contains information on:

- [Upgrading a Syslog Analyzer Collector](#)
- [Preparing to Install a Syslog Analyzer Collector](#)
- [Installing the Syslog Analyzer Collector](#)
- [Uninstalling the Syslog Analyzer Collector](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

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, if necessary.
- Step 2** Remove the Syslog Analyzer collector from the directory in which it was installed.
-

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.

For Solaris Systems

JRE 1.2 is the lowest version you can use to run the remote Syslog Analyzer collector.

To obtain the JRE, refer to the Sun Microsystems' website or 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 `/tmp/jre.tar` file to the client machine.

Step 3 Enter:

```
# tar xvf /jre.tar
```

For AIX Systems

To obtain JDK 1.1.8, refer to the IBM website.

For HP-UX Systems

To obtain the latest version of the JRE, refer to the HP website.

Installing the Syslog Analyzer Collector

Step 1 Obtain the installation file from the Essentials server using either of the following methods:

- Using FTP from the `/opt/CSCOPx/htdocs/rdist/sysloga` directory of the Essentials server.
- Through a browser on the remote server at this location:

http://CiscoWorks2000_server:port/sysloga/SAC.html



Note To access this page, you must first log on to the CiscoWorks2000, and open a new browser window from the CiscoWorks2000 window.

- Step 2** Select SAC.bin.Z and save it.
- Step 3** Log in to the remote server as root.
- Step 4** Set the JRE CLASSPATH *variable* to the appropriate directory or Jar files.
- Step 5** Uncompress SAC.bin.Z by entering:

```
# uncompress SAC.bin.Z
```
- Step 6** Run the Bourne-shell script SAC.bin, for example, `sh SAC.bin`.
- Step 7** 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. These scripts are used to start and stop the Syslog Analyzer collector.



Note Ensure that the entry local7.info is present in /etc/syslog.conf, since the install routine does not add this entry to the syslog.conf file. If local7.info is not present, make an entry in /etc/syslog.conf file as follows: `local7.info /var/log/syslog_info`. Make sure there are no duplicate `local7.info` in the file. 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 If you have not already done so, modify the SAenvProperties.ini file in the following directory:

/opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/sac

Use the values in the [Properties Variables Table](#) to modify the SAenvProperties.ini file.

Table 1 *Properties Variables Table*

Variable	Description
FILE	File from which syslog messages are read. Set a value if a syslog daemon is running on the server.
SAC_PORT	Port number on which syslog messages are coming in, typically, port 514. Specify the port number from which Syslog Analyzer Collector reads syslog messages.
SAC_SERVER	Essentials server to which Syslog Analyzer Collector forwards parsed and filtered messages.
SAC_SERVER_PORT	Port number used by RmeOrb process on Essentials server. To check the port number: <ol style="list-style-type: none"> Using a browser, log in to the Essentials server. Select Server > Administration > Process Management > Process Status. The Process Status table appears. Scroll down and click RmeOrb. The Process Details window appears. In the Flags row, note the port number (after the -p option).
VERSION	Syslog Analyzer Collector version. Recommended version is 1.0.

Table 1 *Properties Variables Table (continued)*

Variable	Description
BINDAME	<p>Name used by Syslog Analyzer Collector to bind to OSAgent process. The value should be the same as value set for the SAC_SERVER variable and followed by ::SaReceiver.</p> <p>For example, if the SAC_SERVER variable is set to nm_bgdemo.cisco.com, then the BINDNAME variable should be set to nm_bgdemo::SaReceiver.</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 PX_HOST in the file, md.properties. This file is located in <i>install_dir</i>/lib/classpath, where <i>install_dir</i> is the directory in which CiscoWorks2000 is installed (C:\Program Files\CSCOpX by default).</p>
DEBUG_LEVEL	<p>Debug level in which you run the Syslog Analyzer Collector.</p> <p>Note It is recommended that you retain the default value, which is 4, as this reports error messages. Setting it to any other value might result in a large number of debug messages being reported.</p>
SA_APP_NAME	<p>Name Syslog Analyzer Collector uses for printed error or debug messages. It is recommended that you retain the default value, SyslogAnalyzer.</p>

Step 9 Configure the startup method.

You can either start up the Syslog Analyzer collector automatically, when the server boots or you can start it manually.

**Note**

Before you start the Syslog Analyzer collector automatically, make sure you have modified the SAenvProperties.ini file with the appropriate value.

To start the Syslog Analyzer collector when the server boots, add the start script (sacStart.sh) to the system boot startup files.

To start the Syslog Analyzer collector manually, you can do either of the following:

- To start the collector manually without passing arguments to it, enter:
- To start the collector manually and pass arguments to it:
 - 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 com.cisco.nm.sysloga.sac.TransProcess [arguments]
```

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

The [Arguments Table](#) contains more information on the arguments.

Table 2 Arguments Table

Arguments	
-sf <i>syslog file name</i>	syslog file name
-sp <i>syslog port #</i>	syslog port number
-bsn <i>bg server name</i>	Essentials server name
-bsp <i>bg server port</i>	Essentials port number
-bnd <i>orb bind name</i>	orb bind name

Table 2 Arguments Table (continued)

Arguments	
-dbg [1-6]	debug modes 1-6
-h	print usage information

- c. The Remote Syslog Analyser collects debug and error messages in a file. By default, this file is stored in the install directory:

`/opt/CSCOsac/lib/SyslogRemoteCollector.log`

If the install directory is changed, then the location of the log file is:

`/changed_dir/lib/SyslogRemoteCollector.log`

**Note**

Specify arguments only if you want parameters that differ from those in your SAenvProperties.ini file. You can specify either syslog filename or syslog port number for the Syslog Analyzer collector to read from; you cannot specify both at the same time. Use the values in the [Properties Variables Table](#) to modify the SAenvProperties.ini file.

- Step 10** To stop the Syslog Analyzer Collector, enter:

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

If the Sylog Analyzer Collector was started manually, you can stop the Java or JRE process.

Uninstalling the Syslog Analyzer Collector

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

```
rm -rf CSCOsac
```

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

<http://www.cisco.com/go/subscription>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://www.cisco.com/register/>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Installing the Remote Syslog Analyzer Collector on UNIX

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.

