

# Table of Contents

<b><u>How to Set Up and Debug the Syslog Facility on a Sun Workstation Using the RME SyslogAnalyzer Application</u></b> .....	<b>1</b>
<u>Document ID: 15381</u> .....	1
<u>Introduction</u> .....	1
<u>Prerequisites</u> .....	1
<u>Requirements</u> .....	1
<u>Components Used</u> .....	1
<u>Conventions</u> .....	2
<u>Set Up and Debug the Syslog Facility on a Sun Workstation with the RME SyslogAnalyzer Application</u> .....	2
<u>Set Up the Syslog Facility on a Sun Workstation</u> .....	3
<u>Set Up the Syslog Facility from a Remote Sun Workstation to the Local RME SyslogAnalyzer</u> .....	4
<u>Workaround for the Remote Syslog</u> .....	5
<u>Install a SyslogAnalyzer Collector</u> .....	5
<u>Stop the SyslogAnalyzer Collector</u> .....	7
<u>NetPro Discussion Forums – Featured Conversations</u> .....	7
<u>Related Information</u> .....	7

# How to Set Up and Debug the Syslog Facility on a Sun Workstation Using the RME SyslogAnalyzer Application

Document ID: 15381

---

## **Introduction**

### **Prerequisites**

Requirements

Components Used

Conventions

### **Set Up and Debug the Syslog Facility on a Sun Workstation with the RME SyslogAnalyzer Application**

#### **Set Up the Syslog Facility on a Sun Workstation**

#### **Set Up the Syslog Facility from a Remote Sun Workstation to the Local RME SyslogAnalyzer**

Workaround for the Remote Syslog

#### **Install a SyslogAnalyzer Collector**

#### **Stop the SyslogAnalyzer Collector**

#### **NetPro Discussion Forums – Featured Conversations**

#### **Related Information**

---

## **Introduction**

This document describes how to set up and debug the syslog facility on a Sun workstation with the Resource Manager Essentials (RME) SyslogAnalyzer application.

This configuration is valid for all devices that generate syslog messages and support syslog facility. Refer to the CD One Documentation for details of CiscoWorks hardware and software requirements.

## **Prerequisites**

### **Requirements**

There are no specific requirements for this document.

### **Components Used**

The information in this document is based on these software versions:

- RME 3.1
- RME 3.2
- RME 3.3
- RME 3.4
- RME 3.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Set Up and Debug the Syslog Facility on a Sun Workstation with the RME SyslogAnalyzer Application

Complete these steps:

1. On the router, issue the **show logging** command and check that a device logs to the IP of RME.

Here is an example:

```
router# show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes,
0 overruns)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 660 messages logged
  Logging Exception size (4096 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 663 message lines logged
    Logging to 172.17.246.149, 663 message lines logged
    Logging to 172.17.246.105, 663 message lines logged
    Logging to 172.17.246.128, 663 message lines logged
Log Buffer (4096 bytes):
ion failure for SNMP req from host 172.17.246.105
1d05h: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
172.17.246.105
1d05h: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
172.17.246.105
...
...
...
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
to up
4d20h: %OSPF-5-ADJCHG: Process 1, Nbr 192.1.1.5 on Serial0/0 from LOADING to FULL,
Loading Done
4d22h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
4d22h: %OSPF-5-ADJCHG: Process 1, Nbr 192.1.1.5 on Serial0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
4d22h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
4d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to down
4d22h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
4d22h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
4d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
4d22h: %OSPF-5-ADJCHG: Process 1, Nbr 192.1.1.5 on Serial0/0 from
LOADING to FULL, Loading Done
```

2. Log in as a root on the Sun (RME) server and look for the entries that start with **syslogd** .

Here is an example:

```
# lsof | grep syslogd | more
:::
```

```

syslogd      152   root    4u   inet  0x30000162028  0t0  UDP  *:syslog (Idle)
:::
syslogd      152   root    9w   VREG 136,0      4203525 2196144 /var/log/syslog_info
:::

```

This syslog listens on port UDP 514, which you find in the `/etc/services` file.

**Note:** If there is no `lsof` package, try `netstat` instead.

3. Issue the **pdshow SyslogAnalyzer** command.
4. Look for the process ID (PID) number and issue the **lsof | grep pid-above** command.
5. Look for an entry such as this:

```

cwjava      16970   bin     21r  VREG  136,0      4204008 2196144 /var/log/syslog_info

```

In this example, 16970 is the PID on an internal Cisco test server. The PID links the syslog of the RME to the syslog daemon and `syslog_info` file of the operating system.

Syslog now fills up with the syslog messages from devices.

6. To check for these syslog messages, issue the **more /var/log/syslog\_info** command.

If you do not find that syslog fills up with the syslog messages, debug the `syslogd`, as shown here:

```

# ps -ef | grep syslogd

root  xxxxx      1  0   Sep 10 ?          0:01 /usr/sbin/syslogd
root  28375 28307   0 14:55:34 pts/8    0:00 grep syslogd

# kill -9 xxxxx (syslogd)
# script /tmp/case.syslog
# syslogd -d
....
^C
# exit

```

7. Check the debug output for this error:

```

cflne(1): (local7.info                /var/log/syslog_info)
logerror(1): syslogd: line 37: unknown priority name "info"

```

If the output contains this error, edit the `/etc/syslog.conf` file to add this line at the end of the `/etc/syslog.conf` file:

```

local7.debug /var/adm/log

```

**Note:** `/var/adm/log` is the full path name of the log file.

**Note:** The white space in the `local7` line in the `syslog.conf` file must be tabs; spaces do not work on a Sun.

## Set Up the Syslog Facility on a Sun Workstation

Complete these steps:

1. Log in as a root.
2. Edit the `/etc/syslog.conf` file to add this line at the end of the `/etc/syslog.conf` file:

```

local7.debug /var/adm/log

```



If the log of the syslog messages occurs on a remote Sun server, export the file system with the `syslog_info` and mount it on the CiscoWorks Sun server. To do this, create a symbolic link to `/var/log/syslog_info` from the mounted `cisco_syslog_info` file. This method is the best way to redirect RME to read the syslog file. However, make sure that no other process locks the `syslog_info` file to prevent access to the file by syslog messages.

## Workaround for the Remote Syslog

Complete these steps:

1. On the remote server, issue the `cd /etc/exports` command to change directories, and then add the entry `/var/log to.a.nice.server.com(ro,root_squash)`.

```
# /var/log to.a.nice.server.com(ro,root_squash)
```

This restarts the Network File System (NFS) server.

2. On the CiscoWorks, issue the `mount -F nfs local.nice.server:/var/log /mnt/log` command to mount the NFS.
3. On RME, change the storage options to `/mnt/log/syslog_info`.
4. To verify that the changes have taken place, issue these commands:

```
# lsof -i :514
COMMAND PID USER FD TYPE DEVICE SIZE/OFF INODE NAME
inetd 122 root 7u inet 0x603a65b8 0t0 TCP *:shell (LISTEN)
syslogd 148 root 3u inet 0x60f98a40 0t0 UDP *:syslog (Idle)
#

# lsof /var/log/syslog_info
COMMAND PID USER FD TYPE DEVICE SIZE/OFF INODE NAME
syslogd 148 root 13w VREG 135,0 12425378 781848 /var/log/syslog_info
cwjava 23489 bin 8r VREG 135,0 12425378 781848 /var/log/syslog_info
cwjava 23489 bin 21r VREG 135,0 12425378 781848 /var/log/syslog_info
```

## Install a SyslogAnalyzer Collector

Another workaround solution for remote syslog is to install a SyslogAnalyzer Collector. Complete these steps:

1. Verify the installation of Java Development Kit (JDK) or Java Runtime Environment (JRE) on the machine on which you plan to install the SyslogAnalyzer collector.

For Solaris Systems:

**Note:** JRE version 1.2 is the earliest version you can use to run the remote SyslogAnalyzer Collector. Access the Sun Microsystems Downloads for JRE version 1.2 and later, or complete these steps to obtain a later version from the server:

- a. Issue the `cd /opt/CSCOpX/lib/` command and the `tar CVF /jre2.tar jre2` command to obtain the JRE from the server.

Use the `/opt/CSCOpX/lib/jre` directory.

- b. Use FTP to transfer the `/tmp/jre.tar` file to the client machine.
- c. Issue the `tar xvf /jre.tar` command.

2. Obtain the installation file from the Essentials server with one of these two methods:

- ◆ Through FTP from the /opt/CSCOpX/htdocs/rdist/sysloga directory of the Essentials server
  - ◆ Through a browser on the remote server
3. Save the SAC.bin file.
  4. Log in to the remote server as root.
  5. Set the JRE CLASSPATH variable to the appropriate directory or Jar files.
  6. Run the Bourne-shell shar script SAC.bin.

Issue the **sh SAC.bin** command.

7. When the installation script asks you where you want to install the CSCOsac package, choose a directory.

If you do not choose a directory, the product automatically installs in the /opt directory.



**Caution:** Do not remove the symbolic link between the /opt directory and the chosen directory.

If you do choose a directory, enter the fully qualified path name to the directory so that there is a symbolic link to the directory from the /opt directory.

The installation script creates a sacStart.sh script and a sacStop.sh script in the /opt/CSCOsac/lib directory. These scripts start and stop the SyslogAnalyzer collector.

The script also asks for the location of the JRE or JDK. For example, if the JRE or JDK is in /usr/jdk1.2, enter:

```
/usr/jdk1.2 5
```

8. If you have not already done so, modify the SAenvProperties.ini file in the /opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/sac directory.

Use the values in the Properties Variables to modify the SAenvProperties.ini file, as this example shows:

```
# pwd
/opt/CSCOsac/lib/classpath/com/cisco/NM/sysloga/sac
# more SAenvProperties.ini
FILE= /var/log/22syslog_info
SAC_PORT = 9000
SAC_SERVER = to.a.nice.server.com
SAC_SERVER_PORT = 42342
VERSION = 1.1
BINDNAME = a.nice.server::SaReceiver
DEBUG_LEVEL=6
SA_APP_NAME=SyslogAnalyzer
LOGFILE_LOCATION=/tmp/SyslogRemoteCollector.log
```

9. Configure the startup method.

You can use one of two methods to start up the SyslogAnalyzer Collector:

- ◆ Automatically when the server boots

To start the SyslogAnalyzer Collector when the server boots, add the start script (**sacStart.sh**) to the system boot startup files.

**Note:** Before you start the SyslogAnalyzer Collector automatically, make sure you have modified the SAenvProperties.ini file with the appropriate values.

- ◆ Manually

To start the SyslogAnalyzer Collector manually, perform one of these two procedures:

◇ To start the collector manually, but not pass it arguments, issue the **sh /opt/CSCOsac/lib/sacStart.sh** command.

◇ To start the collector manually and pass it arguments, complete these steps:

- 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 SyslogAnalyzer Collector arguments.

Enter:

```
java  
com.cisco.nm.sysloga.sac.TransProcess  
[arguments]
```

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

The Java executable file is under the bin directory of your JDK or JRE.

**Note:** Specify arguments only if you want parameters that differ from those in your SAenvProperties.ini file. You can specify either the syslog filename or the syslog port number for the SyslogAnalyzer Collector to read from; you cannot specify both at the same time. Set the values in the SAenvProperties.ini file accordingly. See Step 8 of this section to modify the SAenvProperties.ini file.

## Stop the SyslogAnalyzer Collector

To stop the SyslogAnalyzer Collector, issue the **sh /opt/CSCOsac/lib/sacStop.sh** command.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

<a href="#">NetPro Discussion Forums – Featured Conversations for Network Management</a>
<a href="#">Network Infrastructure: Network Management</a>
<a href="#">Virtual Private Networks: Network and Policy Management</a>

## Related Information

- [CiscoWorks Resource Manager Essentials Tech Notes](#)
- [Technical Support – Cisco Systems](#)

