

Resource Manager Essentials and Syslog Analysis: How-To

Document ID: 13477

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

How to Configure Cisco Devices for Syslog

- Step-by-Step Instructions to Configure IOS Devices
- Step-by-Step Instructions to Configure Catalyst Devices

How to Configure Syslog

- How to Configure Syslog in Resource Manager Essentials 3.x
- How to Configure Syslog Automated Action
- How to Configure Remote Syslog

How to Verify Syslog is Running

- UNIX Machine
- NT Machine

How to Stop/Start Syslog Process

How to Determine What Syslog Messages Mean

How to Correct Syslog Timestamp

- Catalyst Switch
- Router
- Web Browser Client

How to Debug Syslog Automated Action

How to Display Received Syslog Messages in the Standard Report

How to Enable Debug for Syslog in RME

How to Change Default Syslog Settings for RME

Related Information

Introduction

Syslog Analysis controls the central log and track system error messages, exceptions, and other information, such as device configuration changes. You can use the logged error message data to analyze router and network performance. You can customize Syslog Analysis to produce the information and message reports.

Prerequisites

Requirements

Review the client and server prerequisites provided by the Installation Guide of your associated edition of CiscoWorks bundle. All command line references require ROOT id (UNIX) or Local Administrator (Windows) access, determined by your operating system platform.

Components Used

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

- Resource Manager 3.1
- Resource Manager 3.2
- Resource Manager 3.3
- Resource Manager 3.4
- Resource Manager 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.

How to Configure Cisco Devices for Syslog

Step-by-Step Instructions to Configure IOS Devices

Complete these instructions to configure IOS devices.

1. In order to ensure that logging is enabled, issue the **logging on** command.

```
Router(config)# logging on
```

2. In order to specify the Essentials server that is to receive the router syslog messages, issue the **logging ip_address** command. *ip_address* is the address of the server that collects the syslog messages.

```
Router(config)# logging 1.1.1.1
```

3. In order to limit the types of messages that can be logged to the **Essentials** server, set the appropriate logging trap level with the **logging trap informational** command. The **informational** portion of the command signifies severity level 6. This means all messages from level 0–5 (from emergencies to notifications) are logged to the **Essentials** server.

```
Router(config)#logging trap informational
```

Valid logging facilities are local0 through local7. Valid levels are:

- ◆ emergency
- ◆ alert
- ◆ critical
- ◆ error
- ◆ warning
- ◆ notification
- ◆ informational
- ◆ debug

4. In order to verify if the device sends syslog messages, run the **sh logging** command.

You see all the syslog messages that are sent. If you do not see syslog messages, ensure that this is configured:

```
logging on
logging console debug
logging monitor debug
logging trap debug
```

Step-by-Step Instructions to Configure Catalyst Devices

Complete these steps:

1. Ensure sure logging is enabled with the set **logging server enable** command.

```
Catalyst> (enable) set logging server enable
```

2. Specify the Essentials server that is to receive the router syslog messages, with the **logging server_ip** command. *server ip* is the IP address of the **Essentials** server.

```
Catalyst> (enable) set logging server 1.1.1.1
```

3. Limit the types of messages logged to the **Essentials** server. Enter **set logging level informational**, where **informational** signifies severity level 6. This means that all messages from level 0–5 (from emergencies to notifications) are logged to the **Essentials** server.

```
Catalyst> (enable) set logging server severity 6
```

4. In order to see if syslog messages are sent, use the **sh logging buffer** command.

You see syslog messages that are sent. If you experience problems with switches, try this configuration:

```
set logging level all 7 default

set logging server enable

set logging server 1.1.1.1 (your unix syslog server ip address)

set logging server facility LOCAL7

set logging server severity 7
#syslog set logging console enable
set logging server enable
set logging server 1.1.1.1
set logging level cdp 7 default
set logging level mcast 7 default
set logging level dtp 7 default
set logging level dvlan 7 default set logging level earl 7 default
set logging level fddi 7 default
set logging level ip 7 default
set logging level pruning 7 default
set logging level snmp 7 default
set logging level spantree 7 default
set logging level sys 7 default
set logging level tac 7 default
set logging level tcp 7 default
set logging level telnet 7 default
set logging level tftp 7 default
set logging level vtp 7 default
set logging level vmps 7 default
set logging level kernel 7 default
set logging level filesys 7 default
set logging level drip 7 default
set logging level pagp 7 default
set logging level mgmt 7 default
set logging level mls 7 default
set logging level protfilt 7 default
set logging level security 7 default
set logging level radius 7 default
set logging level udld 7 default
set logging level gvrp 7 default
set logging server facility LOCAL7
!
```

Enter **sh logging**

You see this output:

```
Logging buffer size: 500
timestamp option: enabled
Logging history size: 1
Logging console: enabled
Logging server: enabled
{1.1.1.1}
server facility: LOCAL7
server severity: debugging(7)
Current Logging Session: enabled
```

How to Configure Syslog

As root on SunOS, modify the **/etc/syslog.conf** file with commands to sort out the syslog messages from the source devices and to determine which logging facilities (levels) go in which files. You can make a back up of this file prior to modifications. There must be a tab between the logging facility level and file name. The file must exist and be writeable.

The **#Comment** section at the start of **syslog.conf** explains syntax for the system.

Do not put file information in the **ifdef** section. **Syslogd** must be restarted, by root, to acquire changes.

Ensure that the entry and the log file in the **syslog.conf** file are TAB-separated. Spaces do not work. Read the main page for **syslog.conf** for more information (main **syslog.conf**).

Examples

1. If **/etc/syslog.conf** is set for

```
local7.warn    /var/log/local7.warn
```

!--- Note: there must be a TAB character between the filename and the logging level

then the **warning, error, critical, alert,** and **emergency** messages come in on the local7 logging facility are logged in the **local7.warn** file. However, the **notification, informational,** and **debug** messages come in on the local7 facility and are not logged anywhere.

2. If **/etc/syslog.conf** is set for

```
local7.debug    /var/log/local7.debug
```

!--- Note: there must be a TAB character between the filename and the logging level

then the **debug, informational, notification, warning, error, critical, alert,** and **emergency** messages come in on the local7 logging facility are logged to the **local7.debug** file.

3. If **/etc/syslog.conf** is set for

```
local7.warn    /var/log/local7.warn
```

!--- Note: there must be a TAB character between the filename and the logging level

```
local7.debug    /var/log/local7.debug
```

!--- Note: there must be a TAB character between the filename and the logging level

then the **warning, error, critical, alert, and emergency** messages come in on the local7 logging facility are logged in the **local7.warn** file and the **debug, informational, notification, warning, error, critical, alert, and emergency** messages come in on the local7 logging facility are logged to the **local7.debug** file. (In other words, some messages go to both files!).

If **/etc/syslog.conf** is set for

```
*.debug    /var/log/all.debug
```

!--- Note: there must be a TAB character between the filename and the logging level

then all message levels from all logging facilities go to this file. For **RME syslog facility** the important line in **syslog.conf** is **local7.info /var/log/nmslog**. This is the file location you specify in Resource Manager Essentials (RMEs) syslog setup.

How to Configure Syslog in Resource Manager Essentials 3.x

After you configure your Cisco devices to send syslog messages to the CiscoWorks machine, the messages are first received as a flat file before they are populated to the Resource Manager database. You can locate flat file through the CiscoWorks Web Interface:

Resource Manager Essentials-> Administration > Syslog Analysis > Change Storage Options

It's important that the **Message Source** is correct. By default the Message Source points to **/var/log/syslog_info** (unix) or **CSCOpX\log\syslog.log** (Windows), but make sure that your syslog flat file receives new raw data from your Cisco routers/switches.

On a Unix System, you can verify if the syslog collector is configured when you view the **/etc/syslog.conf** file:

```
# Added for Cisco Syslog Analyzer (begin)
local7.info /var/log/syslog_info
# Added for Cisco Syslog Analyzer (end)
#BEGIN CSCcmd - DO NOT EDIT THESE COMMENTS OR CONTENTS CONTAINED WITHIN
- local0 1
#
local0.emeerg;local0.alert;local0.crit;local0.err;local0.warning;local0.notice;local0.info
/var/adm/CSCOpX/log/dmgted.log
#
#END CSCcmd DO NOT EDIT BEFORE THIS LINE 1
~
~
```

On a Windows System, the location is defined in the registry [which can be viewed from res

```
<HKEY_LOCAL_MACHINE>\system\currentControlSet\Services\CRMlog\Parameters
```

```
LogFile = "CSCOpX\log\syslog.log"
```

Once syslog messages are received by the syslog flat file, CiscoWorks verifies if those syslog messages belong to any Cisco devices that are in the Resource Manager inventory list. If an exact match is not there, the syslog message deems it Invalid. Syslog messages that do match are deemed Processed.

You can verify this from **Resource Manager Essentials**→**Administration**→**Syslog Analysis**→**Syslog Collector Status**.

How to Configure Syslog Automated Action

Windows NT

Note: You must run the Perl script with the interpreter and specify the SMTP server. The command line must look like this:

```
drive:\%NMSROOT%\bin\perl sampleEmailScript.pl -text_message $M -email_ids someone@somepla
```

where NMSROOT is the Essentials installation directory, and \$M means that the entire message is passed to the script. The \$M can be replaced with \$D, which means that the device name is passed to the script.

For example:

```
C:\Program Files\CSCOpX\cgi-bin\sysloga>perl sampleEmailScript.pl -text_message $M -email_
```

where rooster.cisco.com is the MTA [SMTP mail server]

UNIX

The command line should look something like:

```
/%NMSROOT%/cgi-bin/sysloga/sampleEmailScript.pl -text_message $M -email_ids someone@somepl
```

How to Configure Remote Syslog

If you use a REMOTE SYSLOG COLLECTOR, make sure the JAVA version is 1.3.1.

Note: The remote log service does NOT specify to problem.

Installing a Remote Syslog Analyzer Collector

The Syslog Analyzer collector can be installed on a remote UNIX or Windows 2000/Windows NT machine 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 no longer want to run it on the remote UNIX or Windows NT server.

Note: Do not install Remote Syslog Analyzer Collector on a machine that has CiscoWorks2000 and Resource Manager Essentials already installed, or stop the CRM logger service before installing Remote Syslog Analyzer Collector. This is because CRM logger 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. This is why it is necessary to have NO NAT/PAT or firewalling between the server and client.
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.

Install the Syslog Analyzer collector on a UNIX system or on a Windows NT system.

How to Verify Syslog is Running

UNIX Machine

Make sure that syslogd is running by typing in `ps -ef | grep syslogd`, you should see the syslogd process returned.

Example:

```
Solaris7-box: /> ps -ef | grep syslogd
root 172      1  0   Feb 08 ?          0:11 /usr/sbin/syslogd
root 23793 23775  0 23:16:46 pts/6    0:00 grep syslogd
```

The first line in the above output indicates that **syslogd** is indeed running.

In order to restart the process type in: **kill -9***syslog_id* use **ps -ef |grep syslogd** to find *syslog_id* . In order to start the process type in: **/usr/sbin/syslogd**.

NT Machine

System message logging is not part of the Windows NT operating system. Therefore, Essentials provides syslog service to Windows NT users. The syslog service saves each system message to `$NMSROOT\log\syslog.log` (where `$NMSROOT` is the root directory of Essentials). Syslog Analysis reads the messages in this file, processes the messages, and writes them to the Essentials database. CGI scripts use the database information to generate system message reports.

Under **Start > Control Panel > Services**, check that CMF Syslog Service is running and that the `syslog.log` file exists. For Windows2000, go to **Start > Programs > Administrative Tools > Services**, select CMF Syslog Service.

How to Stop/Start Syslog Process

From the CiscoWorks2000 Web Interface, logged in with a user id with the appropriate roles:

- In order to stop the syslog process, do the following:
 1. Server Configuration (or CiscoWorks2000 Server) > Administration > Process Management > Stop Process.
 2. Select the Process Radio Button and scroll down to SyslogAnalyzer.
- In order to restart the syslog process, do the following:
 1. Server Configuration (or CiscoWorks2000 Server) > Administration > Process Management > Start Process.
 2. Select the Process Radio Button and scroll down to SyslogAnalyzer.

From the command line, logged into the CiscoWorks Server as root (UNIX) or local administrator (Windows):

- In order to stop the syslog process, do the following:
 1. Go to the CCOpx\bin directory.
 2. Issue the command: **pdterm SyslogAnalyzer**
- In order to restart the syslog process, do the following:
 1. Go to the CCOpx\bin directory.
 2. Issue the command: **pdexec SyslogAnalyzer**

How to Determine What Syslog Messages Mean

- IOS Syslog Structure
- Catalyst Syslog Structure
- Configuring Syslog on UNIX

1. Go to CCO at: <http://www.cisco.com/>
2. Go to **Service & Support**.
3. Go to **Technical Documents > Cisco Product Documentation > Multi-layer LAN Switches > Catalyst 5000 Family Switches**.
4. Choose the software image version.

For example: Switch Software Documentation, Release 5.1 > System Message Guide (5.1) > Message and Recovery Procedures.

All syslog messages are available here. The same procedure can be used to find syslog message information for other devices.

How to Correct Syslog Timestamp

Catalyst Switch

In order to ensure that timestamp is enabled, issue the following command, ensuring that set time and set timezone are correct:

```
set logging timestamp enable
```

Router

In order to ensure the correct time is displayed, issue the following command, ensuring that **set clock** has correct time in enable mode and correct timezone is specified in with **set clock timezone** in global config:

```
sh clock
```

Note: Check **DATE** on the device. If the timestamp on the device is older than the timestamp on the RME machine, the log messages will be put in the **unexpected device** category.

Web Browser Client

Ensure that the date/time information on the client machine is accurate. Otherwise, RME reports no records in

the Standard report and other reports.

On the global configuration on the router, ensure that you have the following:

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

How to Debug Syslog Automated Action

If Syslog Automated Action is not working, use the simplest of Automated Actions to isolate the problem. Go to the Automated Action service, find the command you are trying to execute, and verify if the syslog message is being received.

You must first test the Automated Action to see if it works on its own and that there are no syntax errors. Next test the Automated Action service to see if it can initiate commands/scripts that work on a consistent basis and have no dependencies.

For Window NT/2000, use the start command to bring up a DOS prompt, since we know this command works.

For UNIX, use the touch command to create or modify a file.

If the command doesn't work and you verified that the correct syslog message was received, contact Cisco Technical Assistance Center to help troubleshoot the activation of the Automated Action.

How to Display Received Syslog Messages in the Standard Report

If the RME server is receiving syslog messages but not displaying them in the standard report, check the **syslog.log/syslog_log** file. If the entries are entered using IP address, make sure RME has the device entered the same way. If the entries are entered in via DNS names, make sure RME has the device entered using the DNS name and DOMAIN NAME!

In order to collect messages for devices using the RME Syslog Collector, each device must be entered into RME. The RME machine must be completely DNS resolvable (use the **nslookup** command). The DNS records must match both **forward** and **backward** queries. Check **timestamp** for devices.

How to Enable Debug for Syslog in RME

In order to turn on debugging from the command line, use the following syntax:

```
> pdmsg SyslogAnalyzer: TYP:=DBG VAL:=2
```

In order to turn off debugging from the command line, use the following syntax:

```
> pdmsg SyslogAnalyzer: TYP:=DBG VAL:=4
```

Listed below is the key to the numbers in the syntax above:

- 2 is for debugging
- 3 is for informational messages
- 4 is for normal logging

The debug output is in the **SyslogAnalyzer.log** file. If you are using Solaris, the debug output is in the **daemons.log** file.

How to Change Default Syslog Settings for RME

Syslog Analysis runs every thirty seconds by default. In order to change the default settings you have to change them in the **Sa.properties** file, found in:

CSCOpX/lib/classpath/com/cisco/nm/sysloga/sa/Sa.properties. (backslashes for NT)

Related Information

- **RME Syslog Collector Checklist**
 - **Remote Syslog Analyzer/Collector not Binding to the RME Server**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 10, 2006

Document ID: 13477
