Technical Bulletin CS-12-33

Using Syslog for Logging of Complete SIP Messaging on Spectralink 84-Series Handsets

This bulletin provides detailed information on how to use syslog to log the complete text of every SIP message in the least disruptive manner.

System Affected

Spectralink 84-Series Handsets

Description

Syslog is a standard for forwarding log messages in an IP network.

Polycom phones can be configured to log the complete text of every SIP message they send or receive. Logging the complete text of SIP messages provides an alternative tool for debugging problems when the use of a network capture tool such as Wireshark is not available. However, logging SIP messages using the default method of logging to the phone's flash file system causes an excessive load on the phone's CPU, making the phone unresponsive and possibly even causing it to reboot. This quick tip describes how to use the syslog facility on the phone to capture the logged information and reduce the load on the phone.

This technical bulletin contains information on:

- Requirements
- Configuration
- Performance Considerations
- Summary
- Example Configuration

For more information on syslog, refer to Syslog Menu of the current 84-Series Administrator's Guide at http://support.spectralink.com/resources/spectralink-84-series-wireless-telephone-admin-guide.

Requirements

You must have the following:

- The machine running the syslog server must be accessible by the phone.
- If the syslog messages are to be sent over TCP, the syslog server must be TCP capable.
- If the phone is configured to use TLS as the transport, then either a syslog server that supports TLS is needed or a front-end server that supports TLS such as Stunnel—http://www.stunnel.org—must also be available.

Configuration

To configure the phone to send log messages to the syslog server, refer to the 84-Series Administrator's Guide.

Logging to the Syslog Server Only

To reduce the load on the phone, you should configure it to only log to the syslog server and not to the phone's flash file system. Make the following changes to your phone's configuration file:

- log.render.stdout="0"
- log.render.file="0"

Setting the Log level for SIP Messages

The default loglevel for log messages from the SIP module is set to 4. For the SIP module to log the text of any SIP messaging it sends or receives, this level must be set to 0. Make the following changes to your phone's configuration file:

- log.level.change.sip="0"

The rendering level for syslog must also be changed to 0. It may be set either from the phone's Syslog Menu or via the device.syslog.renderLevel parameter in your phone's configuration file.

Using TLS to Transport Syslog Messages

If the SIP messaging being logged is considered sensitive, the phone can be configured to use TLS to transport the syslog messages. This can be set from the phone's Syslog Menu->Server Type. By default, the syslog server type is UDP.

If you decided to use TLS, the syslog server must also support TLS or a front-end server must provide TLS support. One such server is the open source Stunnel server available at http://www.stunnel.org . An example configuration using stunnel and the open source version of

syslog-ng (http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/) is available in Example Configuration.

Performance Considerations

Network Bandwidth

Use of syslog to capture SIP messaging results in an approximate 10 fold increase in network traffic over the original SIP messaging. This is a result of the additional information that is added to each line of the SIP message by the logging subsystem and the fact that each line output by the logging subsystem results in a separate syslog message.

Summary

In situations where getting a network capture is not a viable option turning up SIP logging and using syslog to save the messages is an alternative. It is not advisable to have all of your sites' phones configured this way all of the time, because of the increased load on the network. However, if you are troubleshooting a specific phone, the additional load is negligible.

Using syslog to capture regular log messages at the default log levels will also not dramatically impact a well designed network.

Example Configuration

The following example shows the configuration of stunnel and syslog for TLS.This example is from a Linux machine running SuSe 10.1 . It is assumed that the syslog and stunnel servers are running on the same machine.

To configure stunnel and syslog for TLS:

1. Obtain and install a copy of stunnel and syslog-ng.
2. Obtain a signed server side certificate for the syslog machine from one of the public CA's or create your own CA and server certificate.

For more information, refer to “Installing Certificates on Spectralink 84-Series Handsets” on the Spectralink Support Portal at http://support.spectralink.com/resources/installing-certificates-spectralink-84-series-handsets.

3. In the stunnel.conf file, set `CAfile` to point to the location of your CA certificate.

   The stunnel.conf file is usually located in the /etc/stunnel/ folder on a Linux machine.

4. In the stunnel.conf file, set `cert` to point to the signed server certificate and `key` to point to the corresponding key file.

5. In the stunnel.conf file, add the following lines:

   ```
   [syslog]

   accept = 14680

   connect = 127.0.0.1:5140
   ```

   This will accept syslog TLS messages from any IP address, and forward them to the localhost port 5140.

6. If the CA certificate is a custom one, add it to the phone.

   For more information, refer to “Installing Certificates on Spectralink 84-Series Handsets”.

7. In the syslog-ng config file, add the following lines:

   ```
   source stunnel {tcp(ip("127.0.0.1")

   port(5140)

   max-connections(1));};
   ```

8. Restart both syslog and stunnel.

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com