## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Alarms</td>
<td>3</td>
</tr>
<tr>
<td>VCS logs</td>
<td>4</td>
</tr>
<tr>
<td>Event Log</td>
<td>4</td>
</tr>
<tr>
<td>Configuration Log</td>
<td>4</td>
</tr>
<tr>
<td>Network Log</td>
<td>4</td>
</tr>
<tr>
<td>Call and search history</td>
<td>5</td>
</tr>
<tr>
<td>Calls</td>
<td>5</td>
</tr>
<tr>
<td>Search history</td>
<td>5</td>
</tr>
<tr>
<td>Diagnostic logging</td>
<td>6</td>
</tr>
<tr>
<td>Using diagnostic logging</td>
<td>6</td>
</tr>
<tr>
<td>Advanced logging levels</td>
<td>6</td>
</tr>
<tr>
<td>Wireshark</td>
<td>7</td>
</tr>
<tr>
<td>NTP server</td>
<td>8</td>
</tr>
</tbody>
</table>
Introduction

This document provides guidelines for the collection of logs and other diagnostic information to assist in the resolution of issues with the Cisco TelePresence Video Communication Server (Cisco VCS).

It is intended for use by the Cisco VCS system administrator or other support engineer.

Alarms

New, unacknowledged alarms are indicated in the top right corner of every VCS web page.

To see the details of each alarm, click on the alarm indicator, or go to Status > Alarms.

The Alarms page shows the type of alarm and which peer in a cluster (if applicable) it is affecting. It also indicates the remedial action to take to resolve the alarm. Alarms that are not important in an installation’s particular circumstances can be acknowledged.

Alarms are also listed when logging in to the command line interface (CLI).
VCS logs

There are three types of VCS logs which can be seen by going to Status > Logs > [type]. These are passive logs, which the administrator can view and filter, but cannot interact with in other ways.

Event Log

The Event Log shows key events that have occurred on the VCS including call events, login events and alarms. Red events indicate events that have failed; green indicates events that have succeeded.

You can use the Filter options to search for specific URIs or keywords. The Event Log is the same as the messages files in the system snapshot.

Syslog

The Event Log can also be sent to one or more external syslog servers, for remote system monitoring. This is configured on the Logging page (System > Logging).

Up to four syslog servers can be specified.

Configuration Log

The Configuration Log provides a list of changes made to the VCS configuration by the system and through the web interface or CLI. It also shows from which IP address and user the changes were made.

This log is useful when reviewing a system which has started to behave unexpectedly - any changes made to the system can be reviewed to see if they may have had an impact on the state of the system.

Network Log

The Network Logs are similar to the Event Logs, in that they both show SIP and H.323 messaging. However the Network Logs also shows call routing decisions made based on the VCS search rules.
Call and search history

Calls

Current call status and historical calls can be seen on the Call status and Call history pages (Status > Calls > Calls and Status > Calls > History respectively).

- **Current calls**: the information shown includes the routing, bandwidth allocation and protocol being used.
- **Historic calls**: release cause information is also shown.

Search history

The Search history page (Status > Search history) shows the decisions the VCS made to route a call, based on transforms, FindMe profile and search rules, zones and soon.

This information is useful if calls are not hitting their intended destinations. It assists in working out why a call may be heading in a different direction to that which was expected.
Diagnostic logging

Diagnostic logging (Maintenance > Diagnostics > Diagnostic logging) is active logging. The administrator can start and stop the logs as required and also insert text marker strings in to the log files as required. These markers can be useful for marking certain stages in reproducing a complex call scenario for example.

Using diagnostic logging

Diagnostic logging supports different log levels:

- Network log level set to *Debug* is equivalent to the legacy VCS "netlog 2" logging from the console; it provides protocol level logs for analyzing call signaling flows.
- Network log level and Interworking log level both set to *Debug* is equivalent to the legacy VCS IWF tracing; these provide protocol level logs for analyzing call signaling flows, together with additional information about decisions VCS made when interworking calls between SIP and H.323, including codec conversion.
- B2BUA log level set to *Debug* enables protocol logging for the B2BUA. This may be used on its own, or together with Network and/or Interworking log levels.

When the log levels have been set as appropriate, click *Start new log* to start the logging. Note, this will raise an alarm to indicate that the VCS is running with a higher log level than normal. This alarm will be cleared when the logging is stopped.

Any steps to reproduce a problem should now be performed. If the steps are complicated, multiple markers can be inserted into the log file which is being generated, using the Marker field and Add marker button. These markers can then be searched for in the resulting log file to find the right section of messaging for the step being performed.

When the scenario is complete, click *Stop logging*.

The log can be downloaded for analysis or to send in to a support team, by clicking *Download log*.

Advanced logging levels

If instructed by the support organization, you can more finely tune the log levels before starting diagnostic logging. This is configured on the Network log level and Support log level pages (Maintenance > Diagnostics > Advanced > Network log configuration and Maintenance > Diagnostics > Advanced > Support log configuration respectively).

Setting any of these log levels higher than their default will raise an alarm to indicate that the VCS is running with a higher log level than normal. These log levels are not reset after stopping the diagnostic log and so must be manually reset to their default level of *Info* after logging is complete.
**Wireshark**

You can take a TCPdump on the VCS which can then be copied off the system and analyzed in Wireshark or similar tools.

A packet capture of all the network traffic being received and sent via the VCS Ethernet interfaces can be saved to the VCS hard drive. The packet capture will include all network traffic (including RTP – if the media is routed via the VCS) seen by the VCS Ethernet interface.

*Note:* if TLS connections are used for SIP signaling, Wireshark will only show the TLS packets, it will not be able to decode the SIP traffic.

On VCS, log in as root and type:

```bash
mkdir /mnt/harddisk/traces
cd /mnt/harddisk/traces
```

Then to activate the trace type:

```bash
tcpdump -w trace.cap -s 0 -C 10
```

- `-w` instructs tcpdump to write the raw packets to file rather than parsing and printing them out. The raw packets are (initially) written to the specified file name (in this case `trace.cap`).
- `-s` sets snaplen to 0 (which instructs tcpdump to capture complete packets regardless of packet length).
- `-C` restricts the output file size to the number (following the option) in millions of bytes.

In the example above, after the initial output file has reached 10 million bytes in length (~10 MB) then a new output file is created and used. The file name will have an incremental index appended to it (`trace, trace2, trace3` and so on).

By default the tcpdump command (without the `-i` option specified) will collect packet data from the lowest available interface ID, that is eth0.

To stop the packet collection, press **Ctrl+C**

The capture files will be available in the following directory:

```
/mnt/harddisk/traces/
```

Use an application which can do SCP to copy them to a local machine (PC). For example, Winscp is a free SCP client for Windows.

If after the packet capture has been stopped, the OS reports that packets have been dropped during the capture (which could happen on very busy systems), make a note of it and let the support organization know, if the packet trace is to be sent on to them.
NTP server

To gather more information for problems with NTP on the VCS, log in as root and type:

```
ntpq
```

At the “ntpq>” prompt type “as”:

```
ntpq> as
```

Results such as the following should be seen:

```
ind assid status conf reach auth condition last_event cnt
```

```
1 7696 961d yes yes none sys.peer 1
```

If this returns a blank please check that DNS is configured.

Make a note of the number in the “assid” column for each entry and then type:

```
rv <assid number>
```

All the variables ntpq has associated with that NTP server will be printed and will look similar to the following:

```
ntpq> rv 7696
associd=7696 status=961d conf, reach, sel_sys.peer, 1 event, popcorn,
srcadr=adc-sjc2-c1-4-w.cisco.com, srcport=123, dstadr=10.50.152.92,
dstport=123, leap=00, stratum=4, precision=-6, rootdelay=269.989,
rootdisp=115.555, refid=72.163.56.103,
reftime=d21c2d01.11365bdc Thu, Sep 15 2011 7:51:29.067,
rec=d21c2d4c.d5627e75 Thu, Sep 15 2011 7:52:44.833, reach=377,
unreach=0, hmode=3, pmode=4, hpoll=10, ppoll=10, headway=0, flash=00 ok,
keyid=0, offset=27.581, delay=179.317, dispersion=15.669, jitter=7.882,
xleave=0.034,
filtdelay= 180.61  220.79  179.32  183.55  179.42  179.40  180.28  180.22,
filtoffset=  27.01    6.87   27.58   25.42   27.45   27.40   26.97   26.94,
filtdisp=  15.63  15.66  15.69  15.72  15.75  15.78  15.81  15.84
```

It is important to note the flash code if the VCS is failing to synchronize with the NTP server. The flash code details the reason for the NTP not synchronizing. A list of the flash codes and their meaning can be retrieved from [http://www.eecis.udel.edu/~mills/ntp/html/decode.html#flash](http://www.eecis.udel.edu/~mills/ntp/html/decode.html#flash).

In some instances, Windows NTP servers that use their own internal clock as a reference time can give a “peer_dist” flash code. This may be due to the localclockdispersion registry value (located at “HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config”) being set too high. NTPQ will not synchronize with a server if it believes the error value the NTP server has on its time is too high. Time servers referencing their own internal clocks should only be used if no other NTP server is available. In this case it is safe to reduce the dispersion to 0. In all other cases a properly referenced time server should be used.