



# Troubleshooting Procedures for Cisco TelePresence Video Communication Server

## Reference Guide

---

Cisco VCS X8.2

D14889.03

June 2014

# Contents

<b>Introduction .....</b>	<b>3</b>
<b>Alarms .....</b>	<b>3</b>
<b>VCS logs.....</b>	<b>4</b>
Event Log .....	4
Configuration Log .....	4
Network Log .....	4
<b>Call and search history .....</b>	<b>5</b>
Calls.....	5
Search history.....	5
<b>Diagnostic logging .....</b>	<b>6</b>
Advanced logging levels.....	6
<b>NTP server .....</b>	<b>7</b>
<b>Additional information .....</b>	<b>8</b>
Memory usage.....	8
<b>Document revision history .....</b>	<b>9</b>

## 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](#).

Alarms								You are here: <a href="#">Status</a> > <a href="#">Alarms</a>	
Alarm	Description	State	Severity	Peer	Action	First raised	Last raised	ID	
<input type="checkbox"/> Configuration warning	Expected default link between the Default Subzone and the Cluster Subzone is missing	Raised	Warning	This system	<a href="#">View instructions on configuring default links</a>	2013-02-26 10:57:29	2013-02-26 10:57:29	<a href="#">45006</a>	
<input type="checkbox"/> Insecure password in use	The root user's password is hashed using MD5, which is not secure enough	Raised	Warning	This system	<a href="#">View instructions on changing the root password</a>	2013-02-26 10:57:26	2013-02-26 10:57:26	<a href="#">40028</a>	

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 ([Maintenance > 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 is active logging. The administrator can start and stop the logs as required. During logging you can 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. You can also take a tcpdump while logging is in progress.

## Enabling diagnostic logging

Go to **Maintenance > Diagnostics > Diagnostic logging**. Optionally, select **Take tcpdump while logging**, and then click **Start new log** to start the logging. The relevant system modules will have their log levels automatically set to "debug". Note, this raises an alarm to indicate that the VCS is running with a higher log level than normal. This alarm will clear 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 in to 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**. If appropriate, click **Download tcpdump** to also download the tcpdump file to your local file system.

**Diagnostic logging** You are here: [Maintenance](#) > [Diagnostics](#) > Diagnostic logging

**Logging status**

Started logging at	Friday 4th of October 2013 09:56:13 AM
Stopped logging at	Friday 4th of October 2013 10:01:05 AM
Marker	<input type="text"/> ⓘ
	<input type="button" value="Add marker"/>
Take tcpdump while logging	<input type="checkbox"/> ⓘ

## Advanced logging levels

If instructed by the support organization, you can more finely tune the log levels before starting diagnostic logging (via the **Maintenance > Diagnostics > Advanced > Network log configuration** and **Maintenance > Diagnostics > Advanced > Support log configuration** pages).

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.

## 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-cl-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>.

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.

## Additional information

### Memory usage

From software version X8, VCS memory usage (as reported via the root top command, for example) shows higher allocations of virtual memory than when compared to previous software versions. This is due to new multi-threaded architectures introduced in X8.

However, this has not affected physical memory usage which is broadly similar to previous software versions.



## Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
3	June 2014	Updated for X8.2.
2	December 2013	Updated for X8.1.
1	September 2011	Initial release.

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.