RMA Procedures for Cisco VCS and TelePresence Conductor Appliances

Reference Guide

Cisco VCS
Cisco TelePresence Conductor

D14887.07

June 2014

Contents

Introduction

This document describes the troubleshooting and information gathering procedures that should be followed if you are considering returning a Cisco TelePresence Video Communication Server (VCS) or a Cisco TelePresence Conductor (TelePresence Conductor) through the Return Material Authorization (RMA) process.

Note: This document does not apply to CE Series appliances. This document applies only to legacy appliances - these are identifiable as having an LCD panel, keypad and a black faceplate.

If you have a CE Series appliance, see *Cisco UCS C220 Server Installation and Service Guide* instead for basic information about that appliance and then follow your standard support process according to your service contract.

It is important to provide the required information to the Cisco support engineers when you request an RMA. You do not need to wait for a support engineer to contact you; you can update your support ticket with the appropriate information at any time.

Troubleshooting suspected hardware issues

System will not power up, or boot up, or is constantly rebooting, or booting the wrong image

The VCS/TelePresence Conductor system will not power up or boot up or keeps rebooting:

- Are any LEDs/LCD display on?
  - If yes, the device is powering on, but it might not be booting:
    - Are any devices connected to the USB ports of the system (especially USB KVM)?
      - If yes, remove them and try powering down and up the system again:
        - If the system still fails to boot, connect to the serial console, and collect as much of the output for the boot up as possible, and attach that to the support ticket. (See Console access [p.16] for information on how to connect to the system with a serial connection.)
    - Are any devices connected to the serial ports of the system?
      - If yes, remove them and try powering down and up the system again:
        - If the system still fails to boot, connect to the serial console, and collect as much of the output for the boot up as possible, and attach that to the support ticket. (See Console access [p.16] for information on how to connect to the system with a serial connection.)
  - If no (there are no LEDs/LCD on) try changing the power outlet the system is plugged into, and the power lead that is being used. Make sure the power and soft-switch on the back of the unit are both in the correct position and have been pressed as appropriate. Check the power cable is working correctly by plugging it into something else.
- If the box keeps rebooting, but is up for a little while, try and collect a sensors log, see Logs and evidence [p.9] for further information.
- If the system still fails to boot, then raise a support ticket with a list of the steps carried out to check the system.

System is reporting a fan failure

The system reports that a fan has failed:

Collect the proof of failure from the system as shown in Logs and evidence [p.9]

- Alarms and Warnings

Raise a support ticket with the collected information attached.

Suspected hard disk issues

The administrator thinks that there is a hard disk failure.

Is the hard disk described as being “unmounted”?

- If yes, please collect as much of the following as possible, as documented in Logs and evidence [p.9]:
  - Physical evidence – showing the message seen on the LCD
  - smartctl
  - DMI code
  - Alarms and warnings

  Raise a support ticket with the collected information attached.

- If no (the disk is not described as “unmounted”) investigate why the administrator thinks there is a problem with the hard disk. The following can provide good evidence of issues with the disk, see Logs and evidence [p.9] for more details:
  - Physical evidence
  - smartctl
  - DMI code
  - Alarms and warnings
  - System snapshot

  There may be disk related error messages in the standard Linux logs, such as dmesg or /var/log/messages.
  Raise a support ticket with the collected information attached.
  A few examples of the type of error log which might be seen are given below:

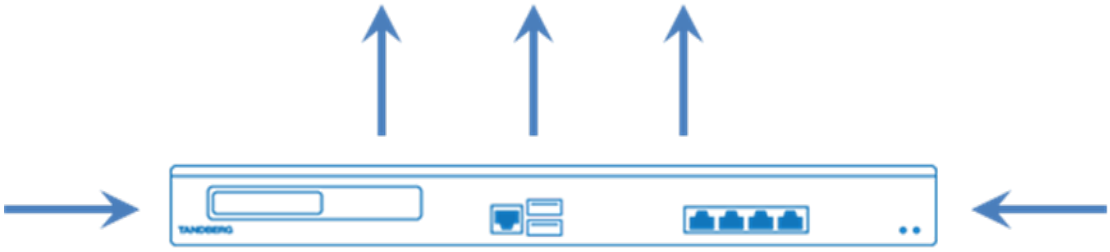
```
ata4.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata4.00: cmd c8/00:00:81:53:2a/00:00:00:00:00/e1 tag 0 dma 131072 in
         res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
ata4.00: status: { DRDY }
ata4: hard resetting link
ata4: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
ata4.00: configured for UDMA/133
ata4.00: device reported invalid CHS sector 0
ata4: EH complete
e2fsck 1.41.9 (22-Aug-2009)
ata4.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata4.00: cmd c8/00:c0:a1:53:2a/00:00:00:00:00/e1 tag 0 dma 98304 in
         res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
ata4.00: status: { DRDY }
ata4: hard resetting link
ata4: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
ata4.00: configured for UDMA/133
ata4.00: device reported invalid CHS sector 0
ata4: EH complete
ata4.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata4.00: cmd c8/00:d0:91:54:2a/00:00:00:00:00/e1 tag 0 dma 106496 in
         res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
ata4.00: status: { DRDY }
ata4: hard resetting link
ata4: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
ata4.00: configured for UDMA/133
ata4.00: device reported invalid CHS sector 0
ata4: EH complete
ata4: limiting SATA link speed to 1.5 Gbps
ata4.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata4.00: cmd c8/00:d0:91:54:2a/00:00:00:00:00/e1 tag 0 dma 106496 in
         res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
ata4.00: status: { DRDY }
ata4: hard resetting link
ata4: SATA link up 1.5 Gbps (SStatus 113 SControl 310)
ata4.00: configured for UDMA/133
ata4.00: device reported invalid CHS sector 0
ata4: EH complete
ata4.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata4.00: cmd c8/00:d0:91:54:2a/00:00:00:00:00/e1 tag 0 dma 106496 in
         res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
ata4.00: status: { DRDY }
ata4: hard resetting link
ata4: SATA link up 1.5 Gbps (SStatus 113 SControl 310)
```

```
ata4.00: configured for UDMA/133
ata4.00: device reported invalid CHS sector 0
ata4: EH complete

ata4: link is slow to respond, please be patient (ready=0)
ata4: SRST failed (errno=-16)
ata4: link is slow to respond, please be patient (ready=0)
ata4: SRST failed (errno=-16)
ata4: link is slow to respond, please be patient (ready=0)
ata4: SRST failed (errno=-16)
ata4: limiting SATA link speed to 1.5 Gbps
ata4: SRST failed (errno=-16)
ata4: reset failed, giving up

kernel: irq 19: nobody cared (try booting with the "irqpoll" option)
kernel: Pid: 0, comm: swapper Not tainted 2.6.31.12 #1
kernel: Call Trace:
kernel:  <IRQ>  [<ffffffff810743d6>] __report_bad_irq+0x26/0xa0
kernel:  [<ffffffff810745dc>] note_interrupt+0x18c/0x1d0
kernel:  [<ffffffff81074db5>] handle_fasteoi_irq+0xb5/0xe0
kernel:  [<ffffffff8100e35d>] handle_irq+0x1d/0x30
kernel:  [<ffffffff8100d887>] do_IRQ+0x67/0xe0
kernel:  [<ffffffff8100bcd3>] ret_from_intr+0x0/0xa
kernel:  <EOI>  [<ffffffff81012c03>] ? mwait_idle+0x63/0x80
kernel:  [<ffffffff8100a500>] ? enter_idle+0x20/0x30
kernel:  [<ffffffff8100a574>] ? cpu_idle+0x64/0xb0
kernel:  [<ffffffff81399d05>] ? rest_init+0x65/0x70
kernel:  [<ffffffff816c250a>] ? start_kernel+0x33c/0x348
kernel:  [<ffffffff816c1b75>] ? x86_64_start_reservations+0x125/0x129
kernel:  [<ffffffff816c1c5d>] ? x86_64_start_kernel+0xe4/0xeb
kernel: handlers:
kernel: [<ffffffff81254260>] (ata_sff_interrupt+0x0/0x110)
kernel: [<ffffffff81254260>] (ata_sff_interrupt+0x0/0x110)
kernel: [<ffffffff81280ba0>] (usb_hcd_irq+0x0/0x70)
kernel: Disabling IRQ #19
```

High temperature warning/alarm

The VCS/TelePresence Conductor reports that it has a high temperature alarm:

- The unit has side air intakes and rear air exhaust. A check should be made to ensure there is sufficient ventilation, particularly at the sides. Even if the sides look OK another device (e.g. a CODIAN MCU) may be exhausting directly into the unit's air intake.



- Codian MCU airflow is from right to left, so be especially careful if racking them to the right of a VCS/TelePresence Conductor.
- Occasionally the thermistor temperature sensor may report a spurious reading. Acknowledge any alarm and monitor the system for further occurrences.
- Collect the proof of failure from the system as shown in Logs and evidence [p.9]
  - Alarms and warnings
  - Physical evidence

  Raise a support ticket with the collected information attached.

Front panel buttons unresponsive

Certain versions of the front panel, especially early Cisco branded panels have problems with the contacts for the buttons on the front panel. This is resolved in newer versions of the front panel, and does not affect day-to-day operation of the system.

- Collect evidence of there being a problem (see Logs and evidence [p.9]):
  - DMI code

If the front panel is unresponsive, a serial connection can be used to the appliance for initial configuration. See Console access [p.16] for information on how to connect to the appliance with a serial connection.

Network adapter issues

The administrator reports that there are problems with the network adapter and/or the LAN link is down.

Verify that different LAN cables and ports on the switch/router that the appliance is connected to have been tried.

Collect evidence of there being a problem (see Logs and evidence [p.9]):

- ifconfig output
- ethtool statistics dump
- Board test
- Physical evidence
- Alarms and warnings
- System snapshot

Raise a support ticket with the collected information attached.

Serial port displays an unexpected login prompt (VCS only)

When a Cisco VCS boots up you typically see something like:

```
tandberg login: root
Password:
```

However during startup, a message from the Fusion MPT SAS driver may collide with the login prompt. In this case the following output will appear:

```
tandberg login: Fusion MPT misc device (ioctl) driver 3.04.14
mptctl: Registered with Fusion MPT base driver
mptctl: /dev/mptctl @ (major,minor=10,220)
```

This issue is due to a software issue which Cisco are aware of, and should not result in an RMA. The issue is fixed in X6.0 and later versions of code.

TANDBERG application / tsh will not start (VCS only)

When trying to log in as admin to a console session (SSH, telnet, serial or KVM), a message “unable to connect to tsh” or “/tmp/hwfail exists: TANDBERG application startup inhibited” is seen:

- Does the file /tmp/hwfail exist?
  - If yes, collect the following from Logs and evidence [p.9]:
    - System snapshot from root shell
    - DMI Code
    - Board Test
    - Physical Evidence
- When typing “tsh” or logging in as admin, is a message saying “cannot connect to tsh” seen?
  - Check that the system has a release key: “cat /tandberg/etc/rk” and that it is valid for the system’s serial number and the software level that is installed.
  - If there are still problems with the application not starting, collect the information as follows:
    - System snapshot from root shell
    - DMI Code
    - Board Test
    - Physical Evidence

Raise a support ticket with the collected information attached.

Note that the TelePresence Conductor has no tsh equivalent.

'preboot agent installation failure' message seen in boot log

A 'preboot agent installation failure' message can appear in the boot log if there is not a serial connection to the VCS during boot up.

This is not a problem and should not result in an RMA.

Logs and evidence

This section describes methods to take logs, snapshots and gather other evidence.

System snapshot (from web)

The system snapshot process creates a file archive of various system files which can be downloaded to the administrator's PC.

To initiate a system snapshot in X6.1 or XC1.1 and earlier:

1. Go to **Maintenance > System snapshot**.
2. Click **Create full snapshot**.
3. Wait for the archive to be created (this can take some time; there are a lot of files).
4. A file download dialogue should appear so that the file can be downloaded to the local pc (make sure the PC has enough disk space).

To initiate a system snapshot in X7.0 or XC1.2 and later:

1. Go to **Maintenance > Diagnostics > System snapshot**.
2. Click **Create full snapshot**.
3. Wait for the archive to be created (this can take some time; there are a lot of files).
4. A file download dialogue should appear so that the file can be downloaded to the local pc (make sure the PC has enough disk space).

Taking a snapshot reserves system resources. On a very busy system it may be advisable to initiate snapshot at a "low traffic" period (although, do not leave it too long after the event you want to analyze).

The system stores only 1 snapshot archive (**.tar.gz**) on disk at any one time (the most recent) – in **/mnt/harddisk/snapshot**.

System snapshot (from root shell)

The system snapshot process creates a file archive of various system files which can be downloaded to the administrator's PC.

To initiate a system snapshot:

1. Log in to the system as root.
2. Type `snapshot.sh`
3. Wait for the archive to be created (this can take some time; there are a lot of files — wait for the file to change from a .tar file to a .tar.gz file).
4. When the snapshot has been generated it will be available to scp from here: **/mnt/harddisk/snapshot/** (it is a **tar.gz** archive).

Taking a snapshot reserves system resources. On a very busy system it may be advisable to initiate snapshot at a "low traffic" period (although, do not leave it too long after the event you want to analyze).

The system stores only 1 snapshot archive (**.tar.gz**) on disk at any one time (the most recent) – in **/mnt/harddisk/snapshot**.

Crash logs

Every time there is an application fail an incident report is written to disk, into the **/tandberg/crash/**directory.

Incident reports are included in the snapshot archive.

The Cisco support engineers host an externally routable server, onto which the VCS/TelePresence Conductor can be configured to post incident reports. If administrators are willing to configure the system to post incident reports it will speed up notification of application failures.

The automatic uploading of crash reports to the ACR (automated crash report) server is configured on the **Maintenance > Incident reporting > Configuration** page (in X7.0 / XC1.1 and later this is **Maintenance > Diagnostics > Incident reporting > Configuration**).

- The incident reports sending mode needs to be set to *On* (it is *Off* by default).
- The incident reports URL needs to be set to https://cc-reports.cisco.com/submitapplicationerror/ (The legacy URL https://vcser.tandberg.com/submitapplicationerror/ will also reach the incident reporting server).
- Following an 'incident' (crash) an incident report is posted to this URL using HTTPS (system source port 4000-4999).

It might not be the whole application crashing; ACRs can also be generated by subcomponents in the system.

If crash reporting cannot be turned on for any reason, or the system does not have routable access to the server, any ACRs generated can be separately copied off the system, and then attached to a support ticket. The Cisco support engineers can then manually upload the ACRs to the reporting server for investigation. Be aware that in most cases a system snapshot is also required to understand the origin of the issue.

Incident reports can be viewed and copied off the system from the **Maintenance > Incident reporting > View** page (in X7.0 / XC1.1 and later this is **Maintenance > Diagnostics > Incident reporting > View**).

Sensor logs

The appliance hardware includes a number of sensors, the values of which can be read by the Linux OS. These can be retrieved by typing **`sensors`** at the command prompt. The output can then be attached to the Support ticket.

```
~ # sensors
acpitz-virtual-0
Adapter: Virtual device

it8712.7-isa-0290
Adapter: ISA adapter
VCore:       +1.22 V  (min =  +0.83 V, max =  +1.39 V)
DDR 1.8V:    +1.78 V  (min =  +1.62 V, max =  +1.98 V)
VCC 3.3V:    +3.31 V  (min =  +3.14 V, max =  +3.47 V)
VCC 5V:      +5.00 V  (min =  +4.76 V, max =  +5.24 V)
+12V:       +12.22 V  (min =  +9.60 V, max = +14.40 V)
VCC 1.5V:    +1.49 V  (min =  +1.42 V, max =  +1.57 V)
VBat:        +3.26 V  (min =  +2.99 V)
Fan 1:       9375 RPM  (min = 7670 RPM, div = 8)
Fan 2:       9375 RPM  (min = 7670 RPM, div = 8)
Fan 3:       10546 RPM  (min = 7670 RPM, div = 8)
```

```
Sys Temp1:    +18.0 C  (high = +45.0 C)                  sensor = thermistor
Sys Temp2:    +20.0 C  (high = +45.0 C)                  sensor = thermistor
CPU Temp:     +18.0 C  (high = +50.0 C)                  sensor = thermal diode

coretemp-isa-0000
Adapter: ISA adapter
Core 0:       +35.0 C  (high = +78.0 C, crit = +100.0 C)

coretemp-isa-0001
Adapter: ISA adapter
Core 1:       +32.0 C  (high = +78.0 C, crit = +100.0 C)
```

DMI code

In the event of an issue, the DMI code can provide the Cisco support engineers with a useful reference code indicating any Engineering Change Requests that have been applied to the system in question.

Run the command **`cat /sys/class/dmi/id/chassis_version`** from a root console session and add the resulting output or include the **dmidecode.txt** file from the system snapshot to the support ticket.

Board test

Run the command **`boarddetect`** from a root console session and add the resulting output to the support ticket.

smartctl

The Linux OS includes a hard disk checker which looks at the hard disk SMART data.

This can be run by typing **`smartctl -all /dev/sdb2`** at the command prompt from a root console session. The output can then be attached to the support ticket.

```
~ # smartctl --all /dev/sdb2
smartctl 5.39.1 2010-01-28 r3054 [x86_64-pc-linux-gnu] (local build)
Copyright (C) 2002-10 by Bruce Allen, http://smartmontools.sourceforge.net

=== START OF INFORMATION SECTION ===
Model Family:     Seagate Barracuda 7200.10 family
Device Model:     ST3250410AS
Serial Number:    9RY29MGL
Firmware Version: 3.AAC
User Capacity:    250,059,350,016 bytes
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   7
ATA Standard is:  Exact ATA specification draft version not indicated
Local Time is:    Mon Apr  4 16:10:02 2011 GMT
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

General SMART Values:
```

```
Offline data collection status:  (0x82) Offline data collection activity
                                        was completed without error.
                                        Auto Offline Data Collection: Enabled.
Self-test execution status:      (   0) The previous self-test routine completed
                                        without error or no self-test has ever
                                        been run.
Total time to complete Offline
data collection:                 ( 430) seconds.
Offline data collection
capabilities:                    (0x5b) SMART execute Offline immediate.
                                        Auto Offline data collection on/off support.
                                        Suspend Offline collection upon new
                                        command.
                                        Offline surface scan supported.
                                        Self-test supported.
                                        No Conveyance Self-test supported.
                                        Selective Self-test supported.
SMART capabilities:            (0x0003) Saves SMART data before entering
                                        power-saving mode.
                                        Supports SMART auto save timer.
Error logging capability:        (0x01) Error logging supported.
                                        General Purpose Logging supported.
Short self-test routine
recommended polling time:        (   1) minutes.
Extended self-test routine
recommended polling time:        (  64) minutes.
SCT capabilities:              (0x0001) SCT Status supported.

SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RA
W_VALUE
  1 Raw_Read_Error_Rate     0x000f   111   092   006    Pre-fail  Always       -       35
118725
  3 Spin_Up_Time            0x0003   097   097   000    Pre-fail  Always       -       0
  4 Start_Stop_Count        0x0032   099   099   020    Old_age   Always       -       10
76
  5 Reallocated_Sector_Ct   0x0033   100   100   036    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000f   084   060   030    Pre-fail  Always       -       31
3078675
  9 Power_On_Hours          0x0032   073   073   000    Old_age   Always       -       23
803
 10 Spin_Retry_Count        0x0013   100   100   097    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   099   099   020    Old_age   Always       -       10
78
187 Reported_Uncorrect      0x0032   100   100   000    Old_age   Always       -       0
189 High_Fly_Writes         0x003a   100   100   000    Old_age   Always       -       0
190 Airflow_Temperature_Cel 0x0022   074   068   045    Old_age   Always       -       26
(Lifetime Min/Max 24/32)
194 Temperature_Celsius     0x0022   026   040   000    Old_age   Always       -       26
(0 12 0 0)
195 Hardware_ECC_Recovered  0x001a   081   051   000    Old_age   Always       -       14
9212051
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   200   200   000    Old_age   Always       -       0
200 Multi_Zone_Error_Rate   0x0000   100   253   000    Old_age   Offline      -       0
202 Data_Address_Mark_Errs  0x0032   100   253   000    Old_age   Always       -       0
```

```
SMART Error Log Version: 1
No Errors Logged

SMART Self-test log structure revision number 1

SMART Selective self-test log data structure revision number 1
 SPAN  MIN_LBA  MAX_LBA  CURRENT_TEST_STATUS
    1        0        0  Not_testing
    2        0        0  Not_testing
    3        0        0  Not_testing
    4        0        0  Not_testing
    5        0        0  Not_testing
Selective self-test flags (0x0):
  After scanning selected spans, do NOT read-scan remainder of disk.
If Selective self-test is pending on power-up, resume after 0 minute delay.
```

ifconfig output

Some appliances may suffer a loss of a physical network port. This can be checked by using a root console session and running the command "ifconfig -a | grep eth". Four interfaces should be listed:

```
~ # ifconfig -a | grep eth
eth0      Link encap:Ethernet  HWaddr 00:10:F3:1E:D4:90
eth1      Link encap:Ethernet  HWaddr 00:10:F3:1E:D4:91
eth2      Link encap:Ethernet  HWaddr 00:10:F3:1E:D4:92
eth3      Link encap:Ethernet  HWaddr 00:10:F3:1E:D4:93
```

If fewer than four are listed, this appliance may have a hardware issue, although reboots may sometimes also resolve this.

ethtool statistics dump

The Linux OS includes a tool for dumping Ethernet adapter statistics.

From a root console session, run “ethtool –S eth0” for the main network adapter used by the appliance or “ethtool –S eth1” if the issue is with a LAN 2 port.

```
~ # ethtool -S eth0
NIC statistics:
     rx_packets: 49308441
     tx_packets: 13055377
     rx_bytes: 10446941316
     tx_bytes: 8354830356
     rx_broadcast: 36524340
     tx_broadcast: 129146
     rx_multicast: 5884
     tx_multicast: 79
     rx_errors: 0
     tx_errors: 0
     tx_dropped: 0
     multicast: 5884
     collisions: 0
     rx_length_errors: 0
     rx_over_errors: 0
```

```
rx_crc_errors: 0
rx_frame_errors: 0
rx_no_buffer_count: 0
rx_missed_errors: 0
tx_aborted_errors: 0
tx_carrier_errors: 0
tx_fifo_errors: 0
tx_heartbeat_errors: 0
tx_window_errors: 0
tx_abort_late_coll: 0
tx_deferred_ok: 0
tx_single_coll_ok: 0
tx_multi_coll_ok: 0
tx_timeout_count: 0
tx_restart_queue: 0
rx_long_length_errors: 0
rx_short_length_errors: 0
rx_align_errors: 0
tx_tcp_seg_good: 115846
tx_tcp_seg_failed: 0
rx_flow_control_xon: 465
rx_flow_control_xoff: 465
tx_flow_control_xon: 0
tx_flow_control_xoff: 0
rx_long_byte_count: 10446941316
rx_csum_offload_good: 12205535
rx_csum_offload_errors: 0
rx_header_split: 0
alloc_rx_buff_failed: 0
tx_smbus: 0
rx_smbus: 0
dropped_smbus: 0
rx_dma_failed: 0
tx_dma_failed: 0
```

Checking for viruses

You can use the **`ps aux`** command from a root console session, to search for the presence of viruses.

For example, to check for the 'war dialler', type:

`ps aux | grep svwar.py`

This will produce several output lines similar to this if the 'war dialler' is present:

```
9430 root 20 0 19020 4340 1880 R 1 0.1  0:00.01 python svwar.py -v -d users.txt <address>
```

The command should produce no output if the virus is not present.

These issues can be fixed by using the USB reinstall procedure (see Restoring default configuration (factory reset) [p.17]).

Alarms and warnings

Alarms and warnings are shown on the system web pages as well as when logging in to the CLI or running the “xstatus” command. They may also be displayed on the LCD panel.

Screen captures from the web interface or the output from “xstatus” should be provided, for example:

	Alarm	State	Severity	Peer	Action	ID
☐	Hardware failure - Fan 2 3013 RPM (min = 7670 RPM, div = 8) ALARM	Raised	Critical			d445eea4-d8fd-11de-8914-001d09a14174

Hardware

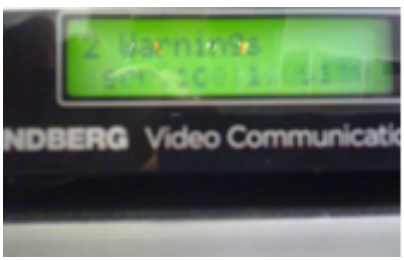
Fans	
Fan 1	9375 RPM (min = 7670 RPM, div = 8)
Fan 2	2909 RPM (min = 7670 RPM, div = 8) ALARM
Fan 3	9375 RPM (min = 7670 RPM, div = 8)

Physical evidence

Any camera phone videos of procedures being carried out or pictures of monitor output, the LEDs, LCD and network link light display, such as the following examples are very useful in helping find the root cause for an RMA:

Alarm LED lit:

LCD text:



Console access

To collect logs or other information when there are network problems or other issue preventing access to the VCS/TelePresence Conductor remotely, a serial console may be used. Connection should be made to the data port on the front of the appliance.

The settings below should be used for the console connection:

Setting	Value
Baud rate	115200 bits per second
Data bits	8
Parity	None
Stop bits	1
Flow control (hardware and software)	None

Restoring default configuration (factory reset)

Very rarely, it may become necessary to run the "factory-reset" script on your system. This reinstalls the software image and resets the configuration to the functional minimum.

Note: restoring default configuration causes the system to use its current default values, which may be different from the previously configured values, particularly if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring default configuration you may want to reset those port settings to match the expected behavior of your firewall.

Prerequisite files

The `factory-reset` procedure described below rebuilds the system based on the most recent successfully-installed software image. The files that are used for this reinstallation are stored in the **/mnt/harddisk/factory-reset/** folder on the system. These files are:

- A text file containing just the 16-character Release Key, named **rk**
- A file containing the software image in tar.gz format, named **tandberg-image.tar.gz**

In some cases (most commonly a fresh VM installation that has not been upgraded), these files will not be present on the system. If so, these files must first be put in place using SCP as root.

Performing a reset to default configuration

The following procedure must be performed from the serial console (or via a direct connection to the appliance with a keyboard and monitor). This is because the network settings will be rewritten, so any SSH session used to initiate the reset would be dropped and the output of the procedure would not be seen.

The process takes approximately 20 minutes.

1. Log in to the system as **root**.
2. Type `factory-reset`
3. Answer the questions as required:
   The recommended responses will reset the system completely to a factory default state.

Prompt	Recommended response
Keep option keys [YES/NO]?	YES
Keep IP configuration [YES/NO]?	YES
Keep ssh keys [YES/NO]?	YES
Keep ssl certificates and keys [YES/NO]?	YES
Keep root and admin passwords [YES/NO]?	YES
Save log files [YES/NO]?	YES
Replace hard disk [YES/NO]? (only applies to systems running on legacy appliance hardware)	NO

4. Finally, confirm that you want to proceed.

Resetting via USB stick

Cisco TAC may also suggest an alternative reset method. This involves downloading the software image onto a USB stick and then rebooting the system with the USB stick plugged in.

If you use this method you must clear down and rebuild the USB stick after use. Do not reset one system and then take the USB stick and re-use it on another system.