



# Cisco VSM Operations Manager High Availability Troubleshooting Guide

---

**Revised: May 26, 2021**

Review the following information for workarounds and solutions to Cisco Video Surveillance Operations Manager high availability (HA) issues:

- [Requirements, page 2](#)
- [Known Limitations in VSOM-HA Functionality, page 4](#)
- [Deleting VSOM-HA Manually from CLI, page 4](#)
- [Database Replication Failures, page 7](#)
- [File Replication Failures, page 12](#)
- [Network Connectivity Loss Results in a Split Brain Scenario, page 13](#)
- [Troubleshooting Errors During a Force Failover, page 13](#)
  - [Summary of Force Failover Errors and Workarounds, page 14](#)
  - [Resolving a “Server Unreachable” Error During Force Failover, page 14](#)
  - [Force Failover During a Software Upgrade on the Secondary Server, page 15](#)
- [Virtual IP Login Failure, page 16](#)
- [Unmanaged Split Brain Scenario, page 16](#)
- [Useful Command Line Tools for HA Troubleshooting, page 18](#)



**Note**

---

For more information including configuration and management instructions, see the “Operations Manager High Availability” section of the [Cisco Video Surveillance Operations Manager User Guide](#).

---



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Requirements

Before you configure Operations Manager HA, verify that the following requirements are met.



**Note**

The **VSOM High Availability** configuration page appears only if the server is a stand-alone Operations Manager and is running a supported OS (such as RHEL 6.4).

**Table 1-1 Requirements**

Requirements	Requirement Complete? (✓)
<p>To configure Operations Manager HA, admins must belong to a User Group with permissions for <i>Servers &amp; Encoders</i>.</p> <p>See the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for more information.</p>	<input type="checkbox"/>
<p>Two standalone physical or virtual servers must be installed on the network.</p> <ul style="list-style-type: none"> <li>– Supported physical servers: CPS-UCS-1RU-K9 or CPS-UCS-2RU-K9</li> <li>– Supported virtual machines: VMs deployed using the Cisco VSM release 7.5 or 7.6 OVA templates.</li> </ul> <p><b>Note</b> Any data on the server used as the Secondary server will be deleted and replaced with the data from the Primary server.</p>	<input type="checkbox"/>
<p>We recommend two CPS-UCS-2RU-K9 servers for best performance.</p> <ul style="list-style-type: none"> <li>• Performance issues can occur using the CPS-UCS-1RU-K9 servers for Operations Manager HA since performance issues (such as slowness) may occur.</li> <li>• Do not mix a CPS-UCS-2RU-K9 server with a CPS-UCS-1RU-K9 server.</li> </ul>	<input type="checkbox"/>
<p>Additional server requirements and recommendations:</p> <ul style="list-style-type: none"> <li>• Stand-alone servers—Only stand-alone physical or virtual servers are supported in an HA configuration. The Operations Manager servers can not be co-located with other server services, such as a Media Server.</li> <li>• Operating system—Red Hat 6.4 64 bit OS only (SUSE and Red Hat 5.8 are NOT supported).</li> <li>• We recommend that both servers have the same hardware specifications such as processor, hard disk storage, and other attributes. For example, two CPS-UCS-2RU-K9 servers.</li> <li>• We do not recommend using Cisco UCS E-series platform servers for Operations Manager HA.</li> <li>• Both servers used for HA must be fully up and running prior to configuring HA or replacing the Secondary server. Verify that there are no pending jobs (of any kind) in the Secondary server.</li> </ul>	<input type="checkbox"/>
<p>Split Brain recovery support:</p> <ul style="list-style-type: none"> <li>• At least one Media Server must be added to the Split Brain Configuration to support recovery if communication between the Primary and Secondary server is lost.</li> <li>• See <a href="#">Unmanaged Split Brain Scenario, page 16</a> for more information.</li> </ul>	<input type="checkbox"/>

**Table 1-1 Requirements**

Requirements	Requirement Complete? (✓)
<p>Network requirements:</p> <ul style="list-style-type: none"> <li>• Subnet—Both servers must be in the same network subnet. This ensures connectivity and data synchronization between the servers.</li> <li>• NIC port—Both servers must be connected to the network using the same NIC port: for example, Eth0. Only a single Ethernet port can be active (either Eth0 or Eth1).</li> <li>• Three IP addresses/hostnames are required:               <ul style="list-style-type: none"> <li>– An IP address/hostname for the Primary server Ethernet (NIC) port.</li> <li>– An IP address/hostname for the Secondary server Ethernet (NIC) port.</li> <li>– A virtual IP address that is shared by both servers.</li> </ul> </li> </ul> <p><b>Note</b> End-users should always use the virtual IP address to access the Operations Manager since it will still work even in a failover occurs. Users should never use the server Ethernet port (NIC) address since connectivity can be lost if the server is unreachable.</p>	<input type="checkbox"/>
<p>Security certificate requirements:</p> <p>By default, all Cisco VSM server include a self-signed certificate. Using the self-signed certificate on the Operations Manager server causes a security warning to appear when users log in the Operation Manager. To avoid this, you can create and install a web server certificate for the Operations Manager servers. The certificate must point to the HA virtual IP address and be installed on both Operations Manager servers (Primary and Secondary) used in the HA configuration.</p> <p>For more information:</p> <ul style="list-style-type: none"> <li>• See the “Operations Manager High Availability” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a>.</li> <li>• <a href="#">Cisco Video Surveillance Management Console Administration Guide</a> for instructions to install the certificate.</li> <li>• <a href="#">Resolving a “Server Unreachable” Error During Force Failover, page 14</a></li> </ul>	<input type="checkbox"/>
<p>Network Time Protocol (NTP) server:</p> <p>All servers must be configured with the same NTP configuration to ensure the time settings are accurate and identical.</p> <p>See the “NTP Information” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for more information.</p>	<input type="checkbox"/>
<p>Passwords:</p> <ul style="list-style-type: none"> <li>• The Management Console password for Operations Manager each server. This is the <i>localadmin</i> password used to access the Cisco VSM Management Console, and is set during the initial server setup.</li> <li>• The admin password used to access the browser-based Operations Manager interface.</li> </ul>	<input type="checkbox"/>

## Known Limitations in VSOM-HA Functionality

While using the VSOM-HA functionality, the following issues may occur causing inaccessibility to VSOM or the system to be in Critical Alert state. If so, disable VSOM-HA functionality.

**Table 2** Known Limitation of Using HA Functionality

Limitation	Summary	CDET
DP Replication Issues	<p>It has been observed that MYSQL replication failure generates a critical alert and stops the data replication process. VSOM server then goes into critical state. In this situation, even though HA functionality is in place, but since data replication has stopped, it can have adverse effects on the system once failover happens. This is because data has not been replicated on the secondary server due to replication issues.</p> <p>When replication fails, the only option is <b>Replace HA</b>. This reinitializes the HA functionality. This process totally depends on the DB size. The larger the DB size, the more time it takes to complete <b>Replace HA</b> jobs.</p>	CSCvx95597
DB Size Issues	<p>DB size plays a role in DB replication failure The MySQL thread that updates and copies the data remotely during replication becomes slower depending on the size of the DB. Customers with larger data sets are consistently facing DB replication issues and the recovery path depends on DB size.</p>	CSCvx95597
User unable to view Live/recorded streams if both Primary and Secondary VSOM servers switch to standby	<p>If both primary and secondary VSOM servers switch to standby mode, user is unable to login to VIP, primary server IP, or secondary server IP to view live/recorded streams.</p> <p>System assigns VIP only to server with Primary mode. If both servers are in standby mode, VIP is inaccessible to users. Per design, system does not allow user to login to VSOM-UI using server's IP address if server is in standby mode.</p> <p>System prompts user: Operation failed: Invalid access, server is in standby mode. Must login with Virtual IP 10.xx.xx.xx to access system.</p>	CSCvx98695
VIP not accessible	<p>Sometimes, VIP running on Primary server becomes unavailable and pacemaker goes to "STOPPED" state. Bringing up the system in stable state again is a challenging task. Often, it can only be achieved by breaking the HA and reinstalling it.</p>	CSCvx99103

## Deleting VSOM-HA Manually from CLI

### Issue

User is unable to delete VSOM-HA from VSOM-UI and needs to delete VSOM-HA manually from CLI.

### Purpose

- To freshly Re-Add VSOM-HA again
- To discontinue using VSOM-HA and use a stand alone VSOM server

### Recovery

Perform the steps below on the primary VSOM.

- 
- Step 1** Update vsomservice table, set NULL for haConfig\_OBJECTID for every related row.
- ```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysql--defaults-file=/usr/BWhttpd/vsom_be/db/db.cnf vsom -e "UPDATE vsomservice SET haConfig_OBJECTID=NULL;
```
- Step 2** Set SYSTEM\_CREATED to false in 'server' table for secondary VSOM server.
- ```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysql--defaults-file=/usr/BWhttpd/vsom_be/db/db.cnf vsom -e "UPDATE server SET system_created=false where name='<secondary_server>';"
```
- Step 3** Delete all rows from haserverstate table.
- ```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysql--defaults-file=/usr/BWhttpd/vsom_be/db/db.cnf vsom -e "DELETE FROM haserverstate;"
```
- Step 4** Delete all rows from haconfig table.
- ```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysql--defaults-file=/usr/BWhttpd/vsom_be/db/db.cnf vsom -e "DELETE FROM haconfig;"
```
- Step 5** Delete all rows from hasplitbrainserver table.
- ```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysql--defaults-file=/usr/BWhttpd/vsom_be/db/db.cnf vsom -e "DELETE FROM hasplitbrainserver;"
```
- Step 6** Delete /root/.ssh/known\_hosts file.
- ```
rm -f /root/.ssh/*
```
- Step 7** Stop the pacemaker service.
- ```
sudo service pacemaker stop (On RHEL 6 system )
sudo systemctl stop pacemaker (On RHEL 7 system)
```

Perform the steps below on the secondary VSOM.

- 
- Step 1** Stop the pacemaker service.
- ```
sudo service pacemaker stop (On RHEL 6 system )
sudo systemctl stop pacemaker (On RHEL 7 system)
```
- Step 2** Stop the VSM software and rebuild VSOM database by performing the steps below:
- a. Remove the VSOM database files, everything in /usr/BWhttpd/vsom\_be/db/mysql/data/ but leave the data/ directory.  

```
# rm -rf /usr/BWhttpd/vsom_be/db/mysql/data/*
```
  - b. Start the VSOM database to create the default database.  

```
# /usr/BWhttpd/bin/init_vsom_mysql start
```
  - c. Create a new Operations Manager database and CDAF database to restore its configuration.  

```
# /usr/BWhttpd/vsom_be/db/database_create.sh
```

```
# /usr/BWhttpd/cdaf_be/db/database_create.sh
```

Perform the steps below on the VSOM-UI.

- 
- Step 1** Login in to the Primary VSOM-UI and delete the Secondary VSOM from the server tab.  
Now, the environment has only a standalone VSOM. VSOM-HA can be enabled back from primary VSOM-UI, if customer requires High Availability environment.



**Note**

---

Whenever VSOM-HA is enabled or “Replace HA” is performed, DB and file replication between the Primary and Secondary starts. This takes time to complete, depending on the number of devices configured and other parameters.

---

## The HA Configuration Job Does Not Complete

### Issue

While configuring Operations Manager HA or replacing the HA Secondary server, the sub job that updates the Secondary server may not complete and cause the job to remain in Pending/Running state.

### Root Cause

This can happen if the Secondary server is in any of the following states:


- The Secondary server is being rebooted.
- The Secondary server was recently rebooted but is not fully up.
- The Secondary server has a Pending or In-progress job. This can be any job but examples include synchronization, device configuration, or template configuration.

### Recovery

To clear the job and complete the HA configuration, do one or more of the following:

- 
- Step 1** Verify that there are no configuration or other tasks being performed on the Secondary server, and that the Secondary server does not have any Pending jobs.
- a. Login to the Secondary server Operations Manager interface.
  - b. Click **System Settings > Jobs**.
  - c. Verify that there are no Pending jobs in the Secondary server.
- Step 2** Restart the services on the Primary server:
- a. Log in the Primary server Management Console interface.
  - b. Click **Restart Services** at the top right corner of the page.
  - c. Follow the on-screen prompts and wait for the operation to complete (the login screen will reappear when services are fully restarted).

See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.

- Step 3** Verify that the HA job is cleared on the Primary server.
- Login to the Primary server Operations Manager interface.
  - Click **System Settings > Jobs**.
  - Verify that the previously stuck Operations Manager HA job is marked *Failed*.
- Step 4** Replace the HA configuration:
- Select **System Settings > Servers**.
  - Select the **Primary** server from the list.
  - Select the **VSOM High Availability** tab.
  - Click the pencil icon in the top right to turn maintenance mode ON.
    - The icon is grey  when maintenance mode is ON.
  - Select **Device Settings > Replace HA Configuration**.
  - Click **OK** and wait for the job to complete.
- See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
- Step 5** Log in to the Operations Manager using the virtual IP address or hostname to verify that the HA setup was successful.
- 

## Database Replication Failures

Some events on either server in an HA configuration can cause database replication failures, where the data on the Primary server is different than the data on the Secondary server.

Events that can cause this include server reboots, power failures, database crashes, or a database going down on either of the participating servers.

Refer to the following topics for information to determine the cause of the failure and recover the database.

- [Determining if a Database Replication Error Occurred, page 7](#)
- [Manually Running the restoreDBReplication.sh Script in case of MYSQL Errors, page 9](#)
- [Detecting if the Database Crashed, page 11](#)
- [Recovering the Database, page 11](#)

### Determining if a Database Replication Error Occurred

To detect if a database replication issue occurred, run the following command. If the fields `LAST_SQL_ERRNO` or `LAST_SQL_ERROR` fields have a value in the response, the database replication is stuck (the query is in the response).

#### Example Output

For example, the replication errors in the following output are shown in red:

```
mysql> show slave status\G
***** 1. row *****
Slave_IO_State: Waiting for Primary to send event
Primary_Host: 172.28.0.64
Primary_User: vsomrepl
```

```

        Primary_Port: 6611
        Connect_Retry: 60
        Primary_Log_File: vsom-mysql-bin.000001
        Read_Primary_Log_Pos: 29020815
        Relay_Log_File: mysql-relay-bin.000004
        Relay_Log_Pos: 2462282
        Relay_Primary_Log_File: vsom-mysql-bin.000001
        Slave_IO_Running: Yes
        Slave_SQL_Running: No
        Replicate_Do_DB:
        Replicate_Ignore_DB:
        Replicate_Do_Table:
        Replicate_Ignore_Table:
        vsom.qrtz_trigger_listeners,vsom.qrtz_calendars,vsom.qrtz_fired_triggers,vsom.qrtz_job
        _details,vsom.qrtz_scheduler_state,vsom.qrtz_job_listeners,vsom.qrtz_triggers,vsom.qrt
        z_locks,vsom.qrtz_paused_trigger_grps
        Replicate_Wild_Do_Table:
        Replicate_Wild_Ignore_Table:
        Last_Errno: 1032
        Last_Error: Could not execute Delete_rows event on table
        vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error
        HA_ERR_KEY_NOT_FOUND; the event's Primary log vsom-mysql-bin.000001, end_log_pos
        23237993
        Skip_Counter: 0
        Exec_Primary_Log_Pos: 23237346
        Relay_Log_Space: 8246408
        Until_Condition: None
        Until_Log_File:
        Until_Log_Pos: 0
        Primary_SSL_Allowed: No
        Primary_SSL_CA_File:
        Primary_SSL_CA_Path:
        Primary_SSL_Cert:
        Primary_SSL_Cipher:
        Primary_SSL_Key:
        Seconds_Behind_Primary: NULL
        Primary_SSL_Verify_Server_Cert: No
        Last_IO_Errno: 0
        Last_IO_Error:
        Last_SQL_Errno: 1032
        Last_SQL_Error: Could not execute Delete_rows event on table
        vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error
        HA_ERR_KEY_NOT_FOUND; the event's Primary log vsom-mysql-bin.000001, end_log_pos
        23237993
        Replicate_Ignore_Server_Ids:
        Primary_Server_Id: 2
        Primary_UUID: f55e65d2-5261-11e4-a165-005056ae786a
        Primary_Info_File: /mysql/data/vsom/mysql/data/Primary.info
        SQL_Delay: 0
        SQL_Remaining_Delay: NULL
        Slave_SQL_Running_State:
        Primary_Retry_Count: 86400
        Primary_Bind:
        Last_IO_Error_Timestamp:
        Last_SQL_Error_Timestamp: 141012 17:47:50
        Primary_SSL_Crl:
        Primary_SSL_Crpath:
        Retrieved_Gtid_Set:
        Executed_Gtid_Set:
        Auto_Position: 0
1 row in set (0.00 sec)

```



## Procedure

For example, complete this procedure to detect which database replication query is stuck in the following error:

```
Could not execute Delete_rows event on table vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error HA_ERR_KEY_NOT_FOUND; the event's Primary log vsom-mysql-bin.000001, end_log_pos 23237993'
```

**Step 1** Decrypt the binary error log file.

**Step 2** Look in the Primary log file for the *end\_log\_pos* entry in the [Example Output, page 7](#).

**Step 3** Enter the following command on the Primary log file on the Secondary server.

For example, if an HA deployment includes server 50 and server 51, and the issue was seen on server 51, go to the Secondary server 50 and enter the following command on the Primary log file. In the example error message above it is *vsom-mysql-bin.000001*:

```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysqlbinlog -r /tmp/error_log.sql  
--base64-output=DECODE-ROWS --verbose  
/mysql/data/vsom/mysql/data/vsom-mysql-bin.000001
```

- Notice that the command was storing the parsed output in the */tmp/error\_log.sql* file.
- Open the parsed log file *error\_log.sql* and search for log position seen in above error 23237993.
- Check the query seen at the log position which gives the ASCII format of the original query that is being executed and is stuck.

## Manually Running the restoreDBReplication.sh Script in case of MYSQL Errors

Using the *restoreDBReplication.sh* script will correct a DB replication issue only if replication failed because of MySQL error 1032, 1062 or 1517. If the script is executed in case of MySQL error other than 1032, 1062 or 1517, there will not be any adverse effect on the system. There may be downtime of the application because the script will stop tomcat service during execution. The script will work on VSM 7.11 and later.



### Note

The script must be executed on the Primary server using the following script location:

```
/usr/BWhttpd/vsom_be/ha/restoreDBReplication.sh
```

### Command:

```
restoreDBReplication.sh [-m masterIp] [-s slaveIp] [-p slave root password]
```

Once executed on the Primary server, Primary server will trigger the same execution on the Secondary server. The script executes the following:

- Puts pacemaker in MaintenanceMode
- Stops tomcat service
- Takes DB dump if DB replication is not running.
- Takes backup of current MySQL DB config file. Location of current MySQL DB config file:

```
/usr/BWhttpd/vsom_be/db/mysql/my.cnf
```

- Creates 2 copies of original my.cnf file under location /usr/BWhttpd/vsom\_be/ha:  
my\_original.cnf : It is created to restore original configuration.  
my\_temp.cnf : It is a modified file which contains changes to skip specified MySQL errors.
- Copy my\_temp.cnf to /usr/BWhttpd/vsom\_be/db/mysql/my.cnf and restart vsom mysql service.
- Once execution is done, restore original DB configuration from my\_original.cnf and restart vsom mysql service.

Once Primary is done with execution, it will wait for Secondary server to finish execution. When both Primary and Secondary servers are done with execution, below steps will be performed:

- 
- Step 1** Release pacemaker MaintenanceMode on Primary.
  - Step 2** Start tomcat on Primary.
  - Step 3** Release pacemaker MaintenanceMode on Secondary.
  - Step 4** Start tomcat on Secondary.

**Important Files and Locations on Primary Server:**

- Execution of the script will be logged in a file:  
/usr/BWhttpd/tomcat/logs/vsom\_be/restore\_db\_replication.log<UTCTIMESTAMP>\_DB.dmp
- MySQL DB config backup file: /usr/BWhttpd/vsom\_be/ha/my\_original.cnf
- Primary DB replication status file: /usr/BWhttpd/vsom\_be/ha/replicationStatus.txt
- Secondary DB replication status file: /usr/BWhttpd/vsom\_be/ha/slaveReplicationStatus.txt

**Important Files and Locations on Secondary Server:**

- Execution of the script will be logged in a file:  
/usr/BWhttpd/tomcat/logs/vsom\_be/restore\_db\_replication.log<UTCTIMESTAMP>\_DB.dmp
- MySQL DB config backup file: /usr/BWhttpd/vsom\_be/ha/my\_original.cnf



**Note**

After running the script, if DB Replication is still not running either on Primary or Secondary server, do the following:

1. Restore DB using DB dump–taken during script execution. This is available here:  
/usr/BWhttpd/vsom\_be/ha/
2. Perform Replace HA config.

**Frequently Asked Questions**

Q: When the script starts, if DB replication is currently running, does it exit with an error?

A: If DB replication is currently running, script will exit with message “DB replication is already running. There is no need to restore DB replication. Hence exiting...”

Q: What if someone kills the script Ctrl-C or reboots the server, how does someone recover the system?

A: If someone kills the script Ctrl-C or reboots the server, use Replace HA config to recover the system.

Q: Should I clean up the DB dump if everything was OK?

A: Yes. Currently, script does not clean DB dump. It may be required to restore/look at the DB at some point in the future, if critical data is lost.

## Detecting if the Database Crashed

To determine if the database crashed, verify the `/usr/BWhttpd/vsom_be/mysql.log` and look for errors such as the following (in red):

```
2014-11-06 13:46:40 2859 [Note] Error reading relay log event: slave SQL thread was
killed
2014-11-06 13:46:40 2859 [ERROR] Error reading packet from server: Lost connection to
MySQL server during query ( server_errno=2013)
2014-11-06 13:46:40 2859 [Note] Slave I/O thread killed while reading event
2014-11-06 13:46:40 2859 [Note] Slave I/O thread exiting, read up to log
'vsom-mysql-bin.000023', position 580246
2014-10-24 15:34:39 13859 [Note] InnoDB: Not using CPU crc32 instructions
2014-10-24 15:34:39 13859 [Note] InnoDB: Initializing buffer pool, size = 64.0M
2014-10-24 15:34:39 13859 [Note] InnoDB: Completed initialization of buffer pool
2014-10-24 15:34:39 13859 [Note] InnoDB: Highest supported file format is Barracuda.
2014-10-24 15:34:39 13859 [Note] InnoDB: The log sequence numbers 46653980 and
46653980 in ibdata files do not match the log sequence number 197868345 in the
ib_logfiles!
2014-10-24 15:34:39 13859 [Note] InnoDB: Database was not shutdown normally!
```

## Recovering the Database

### If a Database Replication Error Occurred

If the SQL that was stuck is of no significance, log in to the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**. This process clears the replication error by replacing the Secondary data with the Primary data.

### If the Database Crashed

- 
- Step 1** Restart Cisco services using the following commands:
- ```
service cisco stop
service cisco start
```
- Step 2** Ensure the database is fully up, by checking Cisco service status:
- ```
service cisco status
```
- Step 3** If the VSOM database service is still not coming up, check the `/usr/BWhttpd/vsom_be/mysql.log`:
- If the log states that the slave thread was killed, fix the issue by logging into the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**.
  - if the *ibdata files* do not match the log sequence number, force recover the database as recommended by Oracle Support team in [this link](http://dev.mysql.com/doc/refman/5.6/en/forcing-innodb-recovery.html) and restart Cisco services:  
<http://dev.mysql.com/doc/refman/5.6/en/forcing-innodb-recovery.html>

- 
- Step 4** If all services are up and running, a database replication issue occurred. Recover the database by logging into the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**.
- 


## File Replication Failures

If a database or file replication issue is displayed in the server Status page, double-click the alert to view the events that describe why file replication is failing. The following can cause these errors:

### Password Change

The *localadmin* password for the Secondary server is not valid. For example, the password was changed on the Secondary server but was not updated on the **VSOM HA Configuration** page.

To resolve this problem:

- 
- Step 1** Log in to the Operations Manager using the virtual IP address / hostname.
- Step 2** Click the pencil icon in the top right to turn maintenance mode ON.
- The icon is grey  when maintenance mode is ON.
- Step 3** Select **System Settings > Servers**.
- Step 4** Select the **Primary** server from the list.
- Step 5** Select the **VSOM High Availability** tab.
- Step 6** Enter the new Secondary server password.
- Step 7** Click **Save**.
- 

### The Remote Host Identification (Hostkeys) for the Secondary Server Changed

The Hostkeys for the Secondary server can change if the server IP address is changed when the server is reinstalled or replaced. If this occurs:

- 
- Step 1** Log in to the Primary server using an SSH client.
- Step 2** SSH to the Secondary server to verify that the following error is displayed. For example:

```
[root@psbu-server-qaha]# ssh localadmin@psbu-server-qa2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d3:b5:e3:0d:fc:0b:ab:6a:c6:c4:b2:3e:17:21:7b:c9.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:8
RSA host key for psbu-server-qa2 has changed and you have requested strict checking.
```

Host key verification failed.

**Step 3** If this message appears, edit the known hosts using the following command:

- `vi /root/.ssh/known_hosts`

**Step 4** Delete the host key entry of the Secondary server and save the changes.

**Step 5** Verify that the database or file replication error is resolved. Wait at least one minute since health monitoring jobs are updated each minute.

- a. Log in to the Operations Manager using the virtual IP address / hostname.
  - b. Select **System Settings > Servers**.
  - c. Select the **Primary** server from the list.
  - d. Select the Status tab.
  - e. Verify that the issue is clear.
- 

## Network Connectivity Loss Results in a Split Brain Scenario

If communication between the Primary and Secondary servers is lost, both servers will try to independently assume the Primary role. This is called a “Split Brain” scenario.

Cisco VSM will automatically detect a Split Brain scenario and direct all traffic to the server that was Primary at the time of communication loss. The Secondary server is put in standby and a Health alert is sent.



### Note

This recovery process requires that at least one Media Server be added to the HA “Split Brain Configuration. See the “Operations Manager High Availability” section of the [Cisco Video Surveillance Operations Manager User Guide](#).

---

Since there can be a delay up to 90 seconds for the issue to be detected, users may still be able to log in to the wrong server. During this time, it is possible that user traffic will go to both servers.

If this occurs, refer to the “Operations Manager High Availability” section of the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

## Troubleshooting Errors During a Force Failover

If a force failover does not complete or encounters errors, review the following information and workarounds.

- [Summary of Force Failover Errors and Workarounds, page 14](#)
- [Resolving a “Server Unreachable” Error During Force Failover, page 14](#)
- [Force Failover During a Software Upgrade on the Secondary Server, page 15](#)

## Summary of Force Failover Errors and Workarounds

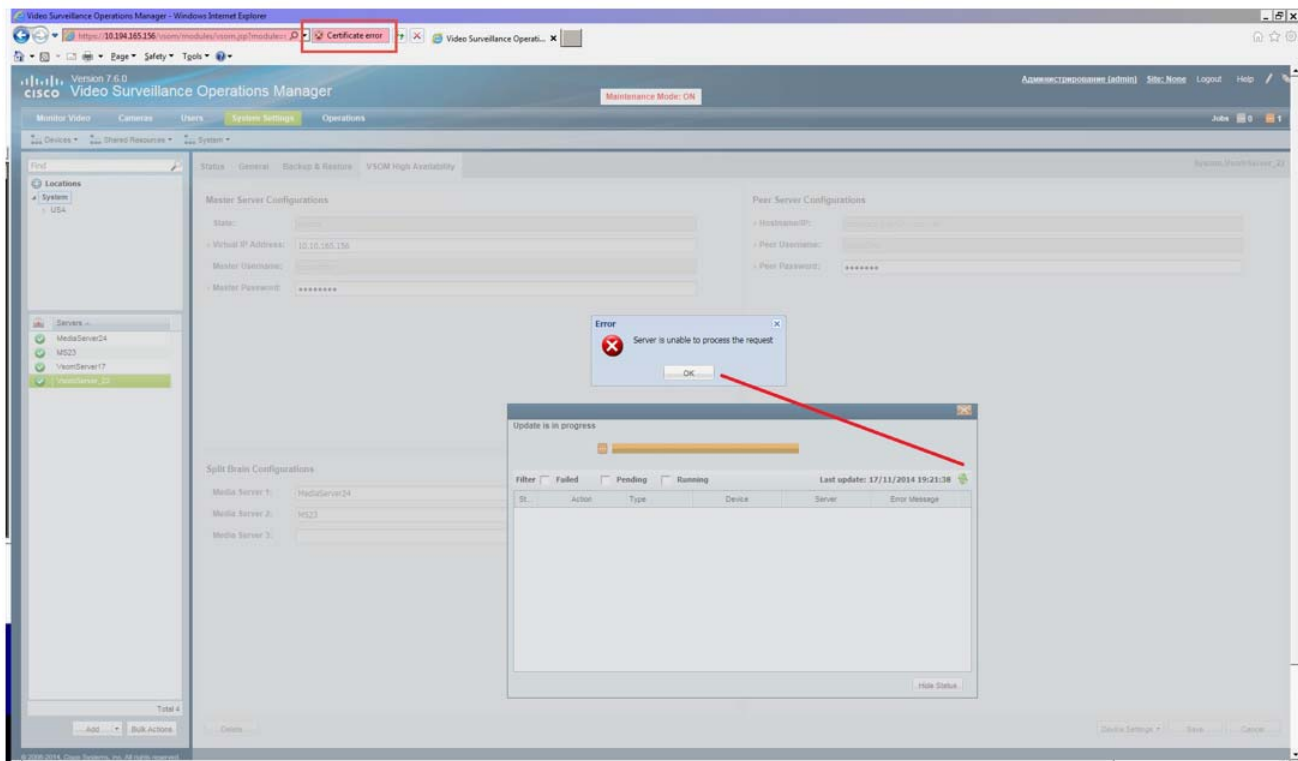
**Table 1-3**      *Troubleshooting Force Failover*

Issue	Workaround
A “Server Unreachable” error appears	<a href="#">Resolving a “Server Unreachable” Error During Force Failover, page 14</a>
Errors during a software upgrade	<a href="#">Force Failover During a Software Upgrade on the Secondary Server, page 15</a>
The Secondary server is not reachable	Check the Secondary server’s Status tab to see if the server is reachable.
The <i>pacemaker</i> service is not running	Go to the Secondary server <b>Status &gt; Status History</b> tab to see if there is a issue “HA Functionality is not available at this time.Pacemaker service is not running”.  To resolve the issue select <b>Device Settings &gt; Replace HA Configuration</b> to bring up the pacemaker service on the Secondary server.
The system is in a Split Brain state	To resolve this, go to <b>Server &gt; VSOM High Availability</b> and select <b>Device Settings &gt; Clear Split Brain Issues</b> . See <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> .

## Resolving a “Server Unreachable” Error During Force Failover

If the default self-signed certificates are used on the Primary and Secondary servers, a “Server unreachable” error may occur when performing a force failover ([Figure 1-1](#)).

**Figure 1-1**      *Certificate Error*



To temporarily address this issue, refresh the browser page to remove the error and continue.

To resolve the issue, obtain and install a signed certificate issued by a Certification Authority.

1. Obtain a signed certificate by a Certification Authority. This certificate should contain the host name mapped to the virtual IP. For example: *vsom-server3*.
2. Install the certificate on both the Primary and Secondary servers using the Cisco Video Surveillance Management Console. For example *vsom-server1* and *vsom-server2*.
3. Wait for the services to be restarted.
4. Log in again to the Operation Manager using the virtual IP address. The certificate error should not appear.

For more information, see the following:

- [Requirements, page 2](#)
- [Cisco Video Surveillance Operations Manager User Guide](#)
- [Cisco Video Surveillance Management Console Administration Guide](#)—for instructions to install the certificate.

## Force Failover During a Software Upgrade on the Secondary Server

If you perform a force failover while a software upgrade is in process on the Secondary server (for example, the Secondary server has not fully initialized after the upgrade), the virtual IP address/hostname can be lost.

If this happens, error messages may appear when a user attempts to log in using the Operations Manager virtual IP address. Messages include: “Invalid access, server is in standby mode” or “Must login with Virtual IP [*IP address*] to access system”. This is because both the Primary and Secondary servers are in standby state.

### Recovery

To resolve this issue, you must manually release *standby* mode on the original Primary server.

- 
- Step 1** To determine the Primary server, query the following database with the following SQL from either server:
- ```
select peerserverip from haconfig where state = 2
```
- Step 2** Log in to the Primary server from the command prompt.
- ```
crm_node -n
```
- Step 3** This provides the node name of the server.
- Step 4** Release standby mode using the following command:
- ```
crm_standby -D -N server-name [node name collected from above command]
```
- For example: **crm\_standby -D -N vsm-server**
- Step 5** After releasing the Standby mode, the server should automatically acquire the virtual IP address.
- Step 6** Log back in to the Operations Manager using the virtual IP address or hostname.
- Step 7** Go to the Primary server and select **Force Fail Over** to proceed with rest of the software upgrade process.
-

## Virtual IP Login Failure

If users are not able to login using the virtual IP address or hostname, do the following:

Determine the following

- The pacemaker service may be down or crashed.
  - Check the status by entering **service pacemaker status** on both the servers.
  - Run the command **crm\_mon -1** to list node status information on both the servers.
- The virtual IP address is not assigned to either of the participating Operations Manager servers:
  - Enter the command **ifconfig** on both servers. If either server returns **NO eth0:0** or **eth1:0**, then neither server acquired the virtual IP address.

If a software upgrade was not being performed, log in to the Primary server using the server's actual IP/Hostname and select **Replace HA Configuration**. Otherwise, try one of the following:

### Software Upgrade Issue

If a force fail over was issued before a software upgrade was complete, see [Force Failover During a Software Upgrade on the Secondary Server, page 15](#).

### Recovery for Pacemaker Down

---

- Step 1** If the pacemaker is down, restart the pacemaker service using the command:
- ```
service pacemaker start
```
- Step 2** If the pacemaker does not come up clean, run the script:
- ```
/usr/BWhttpd/vsom_be/ha/recoverPacemaker.sh
```
- Step 3** Restart the pacemaker service:
- ```
service pacemaker start
```
- 

## Unmanaged Split Brain Scenario

If network connectivity is lost between the Primary and Secondary server, both servers can assume the Primary role and acquire the virtual IP address.

If connectivity is restored between the servers, user traffic can be sent to both servers.

### Root Causes

This scenario can be caused by the following:

- The Primary server is disconnected from the rest of the world, but the Secondary server can see all other servers (including the Media Servers used for HA storage).
- The Primary server has communication with all servers except the Secondary server, and the Secondary server loses network communication with the rest of the world.
- No Media Servers are configured for HA storage, so the system cannot resolve the split brain.
- Media Servers are configured for HA storage but the connectivity issue was shorter than a minute.



---

### Validate

If an unmanaged split brain scenario occurs, the virtual IP address is configured on both servers. Enter the **ifconfig** command on both servers to view the IP address on each server and verify that both servers are using the virtual IP address.

For example, if the Eth0 interface was used, the virtual IP address is displayed under the eth0:0 entry. If the eth1 interface was used for HA configuration, the virtual IP address is displayed under eth1:0.

### Recovery: Method 1

After network connectivity between the Operation Manager HA servers is restored, log in to the Operation Manager browser-based interface to replace the HA configuration.

- 
- Step 1** Log in to the Operation Manager for either server using the physical IP address.
  - Step 2** Select **Device Settings > Replace HA Configuration**.
  - Step 3** If the issue is still not resolved, delete the HA Configuration and reconfigure Operation Manager HA:
    - a. Delete the HA Configuration.
    - b. Re-configure Operations Manager HA.
- See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
- 

### Recovery: Method 2

The following alternative method can also be performed to manually resolve the issues.

- 
- Step 1** Enter the command **ifconfig** on both servers to determine if both servers are configured with the virtual IP address.
    - For example, if the Eth0 interface was used, the virtual IP address will appear under the eth0:0 entry.
  - Step 2** Verify that the Cisco service is up on both servers.
  - Step 3** Bring the Cisco service back up on both servers, if necessary.
  - Step 4** Stop the pacemaker service on both servers.
  - Step 5** Start the pacemaker service on the original Primary server.
  - Step 6** When the pacemaker service starts, enter the command **ifconfig** to verify it has the virtual IP address.
  - Step 7** Log in to the Operation Manager using the virtual IP address or hostname.
  - Step 8** View the server status.
  - Step 9** If the database replication issue is not automatically released, go to the **VSOM High Availability** tab and select **Device Settings > Replace HA Configuration**.
-

## Useful Command Line Tools for HA Troubleshooting

**Table 1-4 CLI Monitoring Tools**

CLI	Description
<code>service pacemaker status</code>	Displays if pacemaker service is running or not. For example: <i>pacemakerd (pid 2583) is running...</i>
<code>crm_mon -l</code>	Lists the participating servers along with where the resources are running. For example:  Last updated: Mon Nov 17 10:47:23 2014 Last change: Thu Nov 13 16:11:23 2014 via crm_attribute on vsm7-55 Stack: cman Current DC: vsm7-54 - partition with quorum Version: 1.1.10-14.el6-368c726 2 Nodes configured 2 Resources configured  Online: [ vsm7-54 vsm7-55 ]  Resource Group: group1 <b>ClusterIP</b> (ocf::heartbeat:IPaddr2): <b>Started</b> auto-vsm7-54 <b>vsom</b> (lsb:vsomha): <b>Started</b> vsm7-54
<code>crm_node -n</code>	Get node name as seen by the pacemaker on local server
<code>crm_mon --failcounts</code>	Resource current failure status and limits
<code>crm_standby -v true [nodename]</code>	To force the server to pacemaker standby state (useful for upgrades and backup restores). For example:  <code>crm_standby -v true vsm7-server</code>
<code>crm_standby -D -N [nodename]</code>	Release the server from standby mode. For example:  <code>crm_standby -D -N vsm7-server</code>

# Related Documentation

See the following locations for the most current information and documentation:

## **HA Configuration, Management and Monitoring**

See the “Operations Manager High Availability” section of the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

## **Cisco Video Surveillance 7 Documentation Roadmap**

Descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

<http://www.cisco.com/go/physicalsecurity/vsm/roadmap>

## **Cisco Physical Security Product Information:**

[www.cisco.com/go/physicalsecurity/](http://www.cisco.com/go/physicalsecurity/)

## **Cisco Video Surveillance Manager Documentation Website**

[www.cisco.com/go/physicalsecurity/vsm/docs](http://www.cisco.com/go/physicalsecurity/vsm/docs)

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [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. (1721R)

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.

*Troubleshooting Operations Manager High Availability, Release 7.6*  
© 2021 Cisco Systems, Inc. All rights reserved.

