Cisco Unified Communications Manager System Issues

This section covers solutions for the following most common issues that relate to a Cisco Unified Communications Manager system.

- Cisco Unified Communications Manager System Not Responding, page 3-1
- Database Replication, page 3-7
- LDAP Authentication Fails, page 3-12
- Issues with LDAP Over SSL, page 3-13
- Open LDAP Cannot Verify the Certificate to Connect to the LDAP Server, page 3-14
- Slow Server Response, page 3-15
- JTAPI Subsystem Startup Problems, page 3-15
- Security Issues, page 3-19
- Performing Failed RAID Disk Replacement, page 3-26

Cisco Unified Communications Manager System Not Responding

This section covers the following issues for a Cisco Unified Communications Manager system that is not responding:

- Cisco Unified Communications Manager System Stops Responding, page 3-2
- Cisco Unified Communications Manager Administration Does Not Display, page 3-3
- Error When Attempting to Access Cisco Unified Communications Manager Administration, page 3-3
- Error When Attempting to Access Cisco Unified Communications Manager Administration on a Subsequent Node, page 3-3
- You Are Not Authorized to View, page 3-4
- Problems Displaying or Adding Users with Cisco Unified Communications Manager, page 3-4
- Name to Address Resolution Failing, page 3-5
- Port 80 Blocked Between Your Browser and the Cisco Unified Communications Manager Server, page 3-5
Cisco Unified Communications Manager System Stops Responding

Symptom
The Cisco Unified Communications Manager system does not respond.

When the Cisco CallManager service stops responding, the following message displays in the System Event log:

The Cisco CallManager service terminated unexpectedly. It has done this 1 time. The following corrective action will be taken in 60000 ms. Restart the service.

Other messages you may see in this situation:
Timeout 3000 milliseconds waiting for Cisco CallManager service to connect.

The Cisco Communications Manager failed to start due to the following error:
The service did not respond to the start or control request in a timely fashion.

At this time, when devices such as the Cisco Unified IP Phones and gateways unregister from the Cisco Unified Communications Manager, users receive delayed dial tone, and/or the Cisco Unified Communications Manager server freezes due to high CPU usage. For event log messages that are not included here, view the Cisco Unified Communications Manager Event Logs.

Possible Cause
The Cisco CallManager service can stop responding because the service does not have enough resources such as CPU or memory to function. Generally, the CPU utilization in the server is 100 percent at that time.

Recommended Action
Depending on what type of interruption you experience, you will need to gather different data that will help determine the root cause of the interruption.

Use the following procedure if a lack of resources interruption occurs.

Procedure

Step 1 Collect Cisco CallManager traces 15 minutes before and after the interruption.
Step 2 Collect SDL traces 15 minutes before and after the interruption.
Step 3 Collect perfmon traces if available.
Step 4 If the traces are not available, start collecting the perfmon traces and track memory and CPU usage for each process that is running on the server. These will help in the event of another lack of resources interruption.
Cisco Unified Communications Manager System Not Responding

Cisco Unified Communications Manager Administration Does Not Display

**Symptom**
Cisco Unified Communications Manager Administration does not display.

**Possible Cause**
The Cisco CallManager service stopped.

**Recommended Action**
Verify that the Cisco CallManager service is active and running on the server, as described in “Verify Cisco Unified Communications Manager Services Are Running” section on page 2-23 or in the Cisco Unified Serviceability Administration Guide.

Error When Attempting to Access Cisco Unified Communications Manager Administration

**Symptom**
An error message displays when you are trying to access Cisco Unified Communications Manager Administration.

**Possible Cause**
The services did not start automatically as expected. One of the services stopping represents the most frequent reason for Cisco Unified Communications Manager Administration not displaying.

**Recommended Action**
Try starting the other services.

Error When Attempting to Access Cisco Unified Communications Manager Administration on a Subsequent Node

**Symptom**
An error message displays when you are trying to access the Cisco Unified Communications Manager Administration.

**Possible Cause**
If the IP address of the first Cisco Unified Communications Manager node gets changed while a subsequent node is offline, you may not be able to log in to Cisco Unified Communications Manager Administration on the subsequent node.

**Recommended Action**
If this occurs, follow the procedure for changing the IP address on a subsequent Cisco Unified Communications Manager node in the document, Changing the IP Address and Host Name for Cisco Unified Communications Manager.
You Are Not Authorized to View

Symptom
When you access Cisco Unified Communications Manager Administration, one of the following messages displays.

- You Are Not Authorized to View This Page
- You do not have permission to view this directory or page using the credentials you supplied.
- Server Application Error. The server has encountered an error while loading an application during the processing of your request. Please refer to the event log for more detailed information. Please contact the server administrator for assistance.
- Error: Access is Denied.

Possible Cause
Unknown

Recommended Action
Contact TAC for further assistance.

Problems Displaying or Adding Users with Cisco Unified Communications Manager

Symptom
You cannot add a user or conduct a search in Cisco Unified Communications Manager Administration.

Possible Cause
You may encounter the following problems if you are working with Cisco Unified Communications Manager that is installed on a server that has a special character (such as an underscore) in its hostname or Microsoft Internet Explorer 5.5 with SP2 and a Q313675 patch or above.

- When you conduct a basic search and click submit, the same page redisplay.
- When you try to insert a new user, the following message displays.

The following error occurred while trying to execute the command.
Sorry, your session object has timed out.
Click here to Begin a New Search

Recommended Action
You may not be able to add a user or do a search on Cisco Unified Communications Manager Administration, if your Cisco Unified Communications Manager hostname contains any special characters such as underscore or period (for example, Call_Manager). Domain Name System (DNS)-supported characters include all letters (A-Z, a-z), numbers (0-9), and hyphen (-); any special characters are not allowed. If the Q313675 patch is installed on your browser, make sure that the URL does not contain any non-DNS supported characters.

For more information about the Q313675 patch, refer to MS01-058: File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6.

To resolve this problem, you have the following options:
Name to Address Resolution Failing

Symptom
One of the following messages displays when you try to access the following URL:
http://your-cm-server-name/ccmadmin
- Internet Explorer—This page cannot be displayed
- Netscape—Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same URL by using the Cisco Communications Manager IP address (http://10.48.23.2/ccmadmin) instead of the name, the window displays.

Possible Cause
The name that you entered as “your-cm-server-name” maps to the wrong IP address in DNS or hosts file.

Recommended Action
If you have configured the use of DNS, check in the DNS to see whether the entry for the your-cm-server-name has the correct IP address of the Cisco Unified Communications Manager server. If it is not correct, change it.
If you are not using DNS, your local machine will check in the “hosts” file to see whether an entry exists for the your-cm-server-name and an IP address that is associated to it. Open the file and add the Cisco Unified Communications Manager server name and the IP address. You can find the “hosts” file at C:\WINNT\system32\drivers\etc\hosts.

Port 80 Blocked Between Your Browser and the Cisco Unified Communications Manager Server

Symptom
One of the following messages displays when a firewall blocks the port that is used by the web server or the http traffic:
- Internet Explorer—This page cannot be displayed
- Netscape—There was no response. The server could be down or is not responding

Possible Cause
For security reasons, the system blocked the http access from your local network to the server network.
Cisco Troubleshooting Guide

Chapter 3    Cisco Unified Communications Manager System Issues

Cisco Unified Communications Manager System Not Responding

Recommended Action

1. Verify whether other types of traffic to the Cisco Unified Communications Manager server, such as ping or Telnet, are allowed. If any are successful, it will show that http access to the Cisco Unified Communications Manager web server has been blocked from your remote network.

2. Check the security policies with your network administrator.

3. Try again from the same network where the server is located.

Improper Network Setting Exists in the Remote Machine

Symptom

No connectivity exists, or no connectivity exists to other devices in the same network as the Cisco Unified Communications Manager.

When you attempt the same action from other remote machines, Cisco Unified Communications Manager Administration displays.

Possible Cause

Improper network configuration settings on a station or on the default gateway can cause a web page not to display because partial or no connectivity to that network exists.

Recommended Action

1. Try pinging the IP address of the Cisco Unified Communications Manager server and other devices to confirm that you cannot connect.

2. If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity. Refer to the appropriate hardware documentation for detailed information.

   If you are using TCP-IP over a LAN to connect, continue with the following steps to verify the network settings on the remote station.

3. Choose Start > Setting > Network and Dial-up connections.

4. Choose Local Area Connection, then Properties.

   The list of communication protocols displays as checked.

5. Choose Internet Protocol (TCP-IP) and click Properties again.

6. Depending on your network, choose either Obtain an ip address automatically or set manually your address, mask and default Gateway.

   The possibility exists that a browser-specific setting could be improperly configured.

7. Choose the Internet Explorer browser Tools > Internet Options.

8. Choose the Connections tab and then verify the LAN settings or the dial-up settings.

   By default, the LAN settings and the dial-up settings do not get configured. The generic network setting from Windows gets used.

9. If the connectivity is failing only to the Cisco Unified Communications Manager network, a routing issue probably exists in the network. Contact the network administrator to verify the routing that is configured in your default gateway.
If you cannot browse from the remote server after following this procedure, contact TAC to have the issue investigated in more detail.

# Database Replication

This section covers the following database replication issues for a Cisco Unified Communications Manager system:

- Replication Fails Between the Publisher and the Subscriber Server, page 3-7
- Database Replication Does Not Occur When Connectivity Is Restored on Lost Node, page 3-10
- Database Tables Out of Sync Do Not Trigger Alert, page 3-11
- Resetting Database Replication When You Are Reverting to an Older Product Release, page 3-11

## Replication Fails Between the Publisher and the Subscriber Server

Replicating the database represents a core function of Cisco Unified Communications Manager clusters. The server with the master copy of the database acts as the publisher (first node), while the servers that replicate the database comprise subscribers (subsequent nodes).

**Tip**

Before you install Cisco Unified Communications Manager on the subscriber server, you must add the subscriber to the Server Configuration window in Cisco Unified Communications Manager Administration to ensure that the subscriber replicates the database that exists on the publisher database server. After you add the subscriber server to the Server Configuration window and then install Cisco Unified Communications Manager on the subscriber, the subscriber receives a copy of the database that exists on the publisher server.

### Symptom

Changes that are made on the publisher server do not get reflected on phones that are registered with the subscriber server.

### Possible Cause

Replication fails between the publisher and subscriber servers.

### Recommended Action

Verify and, if necessary, repair database replication, as described in the following procedure:

### Procedure

#### Step 1

Verify database replication. You can use the CLI, Cisco Unified Reporting, or RTMT to verify database replication.

- To verify by using the CLI, see **Step 2**.
- To verify by using Cisco Unified Reporting, see **Step 3**.
• To verify by using RTMT, see Step 4.

**Step 2**

To verify database replication by using the CLI, access the CLI and issue the following command to check replication on each node. You will need to run this CLI command on each node to check its replication status. Also, after a subscriber is installed, depending on the number of subscribers, it may take a considerable amount of time to archive a status of 2:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—This value indicates that replication did not start. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—This value indicates that replicates have been created, but their count is incorrect.
- 2—This value indicates that replication is good.
- 3—This value indicates that replication is bad in the cluster.
- 4—This value indicates that replication setup did not succeed.

**Step 3**

To verify database replication by using Cisco Unified Reporting, perform the following tasks.

a. From the Navigation drop-down list box in the upper, right corner in Cisco Unified Communications Manager Administration, choose Cisco Unified Reporting.

b. After Cisco Unified Reporting displays, click System Reports.

c. Generate and view the Unified CM Database Status report, which provides debugging information for database replication.

Once you have generated the report, open it and look at the Unified CM Database Status. It gives the RTMT replication counters for all servers in the cluster. All servers should have a replicate state of 2, and all servers should have the same number of replicates created.

If you see any servers whose replicate states are not equal to 2 in the above status check, inspect the “Replication Server List” on this report. It shows which servers are connected and communicating with each node. Each server should show itself as local (in its list) and the other servers as active connected. If you see any servers as dropped, it usually means there is a communication problem between the nodes.

d. If you want to do so, generate and view the Unified CM Database Status report, which provides a snapshot of the health of the Cisco Unified Communications Manager database.

**Step 4**

To verify database replication by using RTMT, perform the following tasks:

a. Open the Cisco Unified Real-Time Monitoring Tool (RTMT).

b. Click the CallManager tab.

c. Click Database Summary. The Replication Status pane displays.

The following list shows the possible values for the Replication Status pane:
0—This value indicates that replication has not started. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.

1—This value indicates that replicates have been created, but their count is incorrect.

2—This value indicates that replication is good.

3—This value indicates that replication is bad in the cluster.

4—This value indicates that replication setup did not succeed.

d. To view the Replicate_State performance monitoring counter, choose System > Performance > Open Performance Monitoring. Double-click the publisher database server (first node) to expand the performance monitors. Click Number of Replicates Created and State of Replication. Double-click Replicate_State. Click ReplicateCount from the Object Instances window and click Add.

Tip To view the definition of the counter, right click the counter name and choose Counter Description.

Step 5 If all the servers have a good RTMT status, but you suspect the databases are not in sync, you can run the CLI command `utils dbreplication status`

(If any of the servers showed an RTMT status of 4, proceed to Step 6)

This status command can be run on all servers by using `utils dbreplication status all` or on one subscriber by using `utils dbreplication status <hostname>`

The status report will tell you if any tables are suspect. If there are suspect tables, you will want to do a replication repair CLI command to sync the data from the publisher server to the subscriber servers.

The replication repair can be done on all subscriber servers (using the all parameter) or on just one subscriber server by using the following:

```
utils dbreplication repair usage:utils dbreplication repair [nodename]|all
```

After running the replication repair, which can take several minutes, you can run another status command to verify that all tables are now in sync.

If tables are in sync after running the repair, you are successful in fixing replication.

Note Only do Step 6 if one of the servers showed an RTMT status of 4, or had a status of 0 for more than four hours.

Step 6 Generate and view the Unified CM Database Status report, which provides debugging information for database replication. For each subscriber server that has a bad RTMT status, check that the hosts, rhosts, sqlhosts, and services files have the appropriate information.

Generate and view the Unified CM Cluster Overview report. Verify that the subscriber servers have the
same version, verify that connectivity is good, and verify that time delay is within tolerances.

If the preceding conditions are acceptable, do the following to reset replication on that subscriber server:

a. At the subscriber server, perform the CLI command `utils dbreplication stop`
   Do this for all subscriber servers that have an RTMT value of 4

b. At the publisher server, perform the CLI command `utils dbreplication stop`

c. At the publisher server, perform the CLI command `utils dbreplication reset <hostname>`
   where `<hostname>` is the hostname of the subscriber server that needs to be reset. If all subscriber servers need to be reset, use command `utils dbreplication reset all`

For More Information

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Reporting Administration Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions*

**Database Replication Does Not Occur When Connectivity Is Restored on Lost Node**

**Symptom**

Database replication does not occur when connectivity is restored on lost node recovery. You can verify the state of replication by using the methods given in the topic *Replication Fails Between the Publisher and the Subscriber Server*, page 3-7. Only use the following procedure if you have already tried to reset replication on the node, and have been unsuccessful.

**Possible Cause**

The CDR check remains stuck in a loop, due to a delete on device table.

**Recommended Action**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Run <code>utils dbreplication stop</code> on the affected subscribers. You can run them all at once.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Wait until Step 1 completes, then, run <code>utils dbreplication stop</code> on the affected publisher server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Run <code>utils dbreplication clusterreset</code> from the affected publisher server. When you run the command, the log name gets listed in the log file. Watch this file to monitor the process status. The path to the follows: /var/log/active/cm/trace/dbl/sdi</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the affected publisher, run <code>utils dbreplication reset all</code>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Stop and restart all the services on all the subscriber servers [or restart/reboot all the systems (subscriber servers)] in the cluster to get the service changes. Do this only after <code>utils dbreplication status</code> shows Status 2.</td>
</tr>
</tbody>
</table>
Database Tables Out of Sync Do Not Trigger Alert

**Note**
“Out of sync” means that two servers in the cluster do not contain the same information in a specific database table.

**Symptom**
On Cisco Unified Communications Manager Version 6.x or later, the symptoms include unexpected call processing behaviors. Calls do not get routed or handled as expected. The symptoms may occur on either the publisher or on the subscriber servers.

On Cisco Unified Communications Manager Version 5.x, the symptoms include unexpected call processing behaviors. Calls do not get routed or handled as expected but only when the publisher server is offline.

If you see this symptom and you run `utils dbreplication status` at the CLI, it reports *Out of sync*. If *Out of sync* does not display, be aware that this is not the problem.

**Possible Cause**
Database tables remain out of sync between nodes. Replication alerts only indicate failure in the replication process and do not indicate when database tables are out of sync. Normally, if replication is working, tables should remain in sync. Instances can occur in which replication appears to be working, but database tables are “Out of sync”.

**Recommended Action**

**Step 1**
Reset cluster replication by using CLI commands. Ensure servers in the cluster are online with full IP connectivity for this to work. Confirm that all servers in the cluster are online by using platform CLIs and Cisco Unified Reporting.

**Step 2**
If the servers are in Replication State 2, run the following command on the publisher server:
`utils dbreplication repair server name`

If the servers are not in Replication State 2, run the following command on all subscriber servers:
`utils dbreplication stop`

Then, run the following commands on the publisher server:
`utils dbreplication stop`
then
`utils dbreplication reset all`

**Resetting Database Replication When You Are Reverting to an Older Product Release**

If you revert the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command `utils dbreplication reset` all on the publisher server.
When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message reminding you about the requirement to reset database replication if you are reverting to an older product release.

**utils dbreplication clusterreset**

This command resets database replication on an entire cluster.

**Command Syntax**

```
utils dbreplication clusterreset
```

**Usage Guidelines**

Before you run this command, run the command `utils dbreplication stop` first on all subscribers servers, and then on the publisher server.

**Requirements**

Command privilege level: 0
Allowed during upgrade: Yes

**utils dbreplication dropadmindb**

This command drops the Informix syscdr database on any server in the cluster.

**Command Syntax**

```
utils dbreplication dropadmindb
```

**Usage Guidelines**

You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

**Requirements**

Command privilege level: 0
Allowed during upgrade: Yes

**LDAP Authentication Fails**

This section describes a common issue when LDAP authentication failure occurs.

**Symptom**

Login fails for end users. Authentication times out before the user can log in.

**Possible Cause**

You misconfigured the LDAP Port in the LDAP Authentication window in Cisco Unified Communications Manager Administration.
Recommended Action
How your corporate directory is configured determines which port number to enter in the LDAP Port field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

Example: LDAP Port For When the LDAP Server Is Not a Global Catalog Server
- 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Example: LDAP Port For When the LDAP Server Is a Global Catalog Server
- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Tip Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

Issues with LDAP Over SSL

This section describes a common issue when you use LDAP over SSL.

Symptom
LDAP over SSL does not work.

Possible Causes
In most cases, problems with LDAP over SSL involve invalid, wrong, or incomplete certificates (chains) on the Cisco Unified Communications Manager server.

Explanation
In some cases, you may use multiple certificates for SSL. In most cases, uploading the AD root certificate as a directory trust is the only certificate that you need to make LDAP over SSL work. However, if a different directory trust certificate is uploaded, that is, one other than a root certificate, that other certificate must be verified to a higher level certificate, such as a root certificate. In this case, a certificate chain is created because more than one extra certificate is involved. For example, you may have the following certificates in your certificate chain:

- Root Certificate—The top-level CA certificate in the trust chain which will have similar issuer and the subject name.
- Intermediate Certificate—The CA certificate that is part of the trust chain (other than the top level). This follows the hierarchy starting from root till the last intermediate.
- Leaf Certificate—The certificate issued to the service/server which is signed by the immediate intermediate.

For example, your company has two certificates and a root certificate in your certificate chain. The following example shows the contents of a certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    77:a2:0f:36:7c:07:12:9c:41:a0:84:5f:c3:0c:64:64
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: DC=com, DC=DOMAIN3, CN=jim
  Validity
    Not Before: Apr 13 14:17:51 2009 GMT
    Not After: Apr 13 14:26:17 2014 GMT
  Subject: DC=com, DC=DOMAIN3, CN=jim

Recommended Action
If you have a two node chain, the chain contains the root and leaf certificate. In this case, uploading the root certificate to the directory trust is all you need to do.

If you have more than a two node chain, the chain contains the root, leaf, and intermediate certificates. In this case, the root certificate and all the intermediate certificates, excluding the leaf certificate, needs to be uploaded to the directory trust.

At the highest level in the certificate chain, that is, for the root certificate, check to make sure that the Issuer field matches the Subject field. If the Issuer field and Subject field do not match, the certificate is not a root certificate; it is an intermediate certificate. In this case, identify the complete chain from root to the last intermediate certificate, and upload the complete chain to the directory trust store.

In addition, check the Validity field to ensure the certificate has not expired. If the intermediate is expired, get the new chain from the certificate authority, along with the new leaf that is signed by using the new chain. If only the leaf certificate is expired, get a new signed certificate.

Open LDAP Cannot Verify the Certificate to Connect to the LDAP Server

Symptoms
End user authentication via CTI/JTAPI clients fails, but user authentication to Unified CM works.

Possible Causes
Open LDAP cannot verify the certificate to connect to the LDAP server.

Explanation
Certificates are issued with a Fully Qualified Domain Name (FQDN). The Open LDAP verification process matches the FQDN with the server that is being accessed. Because the uploaded certificate uses FQDN and the web form is using IP Address, Open LDAP cannot connect to the server.

Recommended Actions
- If possible, use DNS.
During the Certificate Signing Request (CSR) process, ensure that you provide the FQDN as part of subject CN. Using this CSR when a self signed certificate or CA certificate is obtained, the Common Name will contain the same FQDN. Hence, no issues should occur when LDAP authentication is enabled for applications, such as CTI, CTL, and so on, with the trust certificate imported to the directory-trust.

- If you are not using DNS, enter an IP Address in the LDAP Authentication Configuration window in Cisco Unified Communications Manager Administration. Then, add the following line of text in /etc/openldap/ldap.conf:

  ```
  TLS_REQCERT never
  ```

  You must have a remote account to update the file, which prevents the Open LDAP library from verifying that certificate from the server. However, subsequent communication still occurs over SSL.

### Slow Server Response

This section addresses a problem that relates to a slow response from the server due to mismatched duplex port settings.

**Symptom**
Slow response from the server occurs.

**Possible Cause**
Slow response could result if the duplex setting of the switch does not match the duplex port setting on the Cisco Unified Communications Manager server.

**Recommended Action**
1. For optimal performance, set both switch and server to **100/Full**.
   Cisco does not recommend using the Auto setting on either the switch or the server.
2. You must restart the Cisco Unified Communications Manager server for this change to take effect.

### JTAPI Subsystem Startup Problems

The JTAPI (Java Telephony API) subsystem represents a very important component of the Cisco Customer Response Solutions (CRS) platform. JTAPI communicates with the Cisco Unified Communications Manager and has responsibility for telephony call control. The CRS platform hosts telephony applications, such as Cisco Unified Auto-Attendant, Cisco IP ICD, and Cisco Unified IP-IVR. Although this section is not specific to any of these applications, keep in mind that the JTAPI subsystem is an underlying component that all of them use.

Before starting the troubleshooting process, ensure that the software versions that you are using are compatible. To verify compatibility, read the Cisco Unified Communications Manager Release Notes for the version of Cisco Unified Communications Manager that you are using.

To check the version of CRS, log in to AppAdmin by entering http://servername/appadmin, where `servername` specifies the name of the server on which CRS is installed. Find the current version in the lower-right corner of the main menu.
JTAPI Subsystem is OUT_OF_SERVICE

Symptom
The JTAPI subsystem does not start.

Possible Cause
One of the following exceptions displays in the trace file:

- MIVR-SS_TEL-4-ModuleRunTimeFailure
- MIVR-SS_TEL-1-ModuleRunTimeFailure

MIVR-SS_TEL-4-ModuleRunTimeFailure

Search for the MIVR-SS_TEL-1-ModuleRunTimeFailure string in the trace file. At the end of the line, an exception reason displays.

The following list gives the most common errors:

- Unable to create provider—bad login or password
- Unable to create provider—Connection refused
- Unable to create provider—login=
- Unable to create provider—hostname
- Unable to create provider—Operation timed out
- Unable to create provider—null

Unable to create provider—bad login or password

Possible Cause
Administrator entered an incorrect user name or password in the JTAPI configuration.

Full Text of Error Message

%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time failure in JTAPI subsystem: Module=JTAPI Subsystem,Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT, Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable to create provider -- bad login or password.

Recommended Action
Verify that the user name and password are correct. Try logging into the Cisco Unified CM User window (http://servername/ccmuser) on the Cisco Unified Communications Manager to ensure that the Cisco Unified Communications Manager cannot authenticate correctly.
Unable to create provider—Connection refused

Possible Cause
The Cisco Unified Communications Manager refused the JTAPI connection to the Cisco Unified Communications Manager.

Full Text of Error Message
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- Connection refused
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Connection refused

Recommended Action
Verify that the CTI Manager service is running in the Cisco Unified Serviceability Control Center.

Unable to create provider—login=

Possible Cause
Nothing has been configured in the JTAPI configuration window.

Full Text of Error Message
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- login=
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=

Recommended Action
Configure a JTAPI provider in the JTAPI configuration window on the CRS server.

Unable to create provider—hostname

Possible Cause
The CRS engine cannot resolve the host name of the Cisco Unified Communications Manager.

Full Text of Error Message
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- dgrant-mcs7835.cisco.com
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com

Recommended Action
Verify that DNS resolution is working correctly from the CRS engine. Try using an IP address instead of the DNS name.
### Unable to create provider—Operation timed out

**Possible Cause**
The CRS engine does not have IP connectivity with the Cisco Unified Communications Manager.

**Full Text of Error Message**

```plaintext
101: Mar 24 11:37:42.153 PST
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem, Failure Cause=7, Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
```

**Recommended Action**
Check the IP address that is configured for the JTAPI provider on the CRS server. Check the default gateway configuration on the CRS server and the Cisco Unified Communications Manager. Make sure no IP routing problems exist. Test connectivity by pinging the Cisco Unified Communications Manager from the CRS server.

### Unable to create provider—null

**Possible Cause**
No JTAPI provider IP address or host name get configured, or the JTAPI client is not using the correct version.

**Full Text of Error Message**

```plaintext
102: Mar 24 11:37:42.168 PST
%MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- null
```

**Recommended Action**
Verify that a host name or IP address is configured in the JTAPI configuration. If the JTAPI version is incorrect, download the JTAPI client from the Cisco Unified Communications Manager Plugins window and install it on the CRS server.

### MIVR-SS_TEL-1-ModuleRunTimeFailure

**Symptom**
This exception usually occurs when the JTAPI subsystem cannot initialize any ports.

**Possible Cause**
The CRS server can communicate with the Cisco Unified Communications Manager, but cannot initialize any CTI ports or CTI route points through JTAPI. This error occurs if the CTI ports and CTI route points are not associated with the JTAPI user.
Full Text of Error Message
255: Mar 23 10:05:35.271 PST%MIVR-SS_TEL-1-ModuleRunTimeFailure:
Real-time failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7, Failure Module=JTAPI_SS, Exception=null

Recommended Action
Check the JTAPI user on the Cisco Unified Communications Manager and verify that CTI ports and CTI route points that are configured on the CRS server associate with the user.

JTAPI Subsystem is in PARTIAL_SERVICE

Symptom
The following exception displays in the trace file:
MIVR-SS_TEL-3-UNABLE_REGISTER_CTI_PORT

Possible Cause
The JTAPI subsystem cannot initialize one or more CTI ports or route points.

Full Text of Error Message
1683: Mar 24 11:27:51.716 PST%MIVR-SS_TEL-3-UNABLE_REGISTER_CTI_PORT:
Unable to register CTI Port: CTI Port=4503,
Exception=com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
1684: Mar 24 11:27:51.716 PST%MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.

Recommended Action
The message in the trace tells you which CTI port or route point cannot be initialized. Verify that this device exists in the Cisco Unified Communications Manager configuration and also associates with the JTAPI user on the Cisco Unified Communications Manager.

Security Issues
This section provides information about security-related measurements and general guidelines for troubleshooting security-related problems. This section contains information on the following topics:

- Security Alarms, page 3-20
- Security Performance Monitor Counters, page 3-20
- Reviewing Security Log and Trace Files, page 3-21
- Troubleshooting Certificates, page 3-22
- Troubleshooting CTL Security Tokens, page 3-22
- Troubleshooting CAPF, page 3-23
- Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways, page 3-24
This section does not describe how to reset the Cisco Unified IP Phone if it has been corrupted by bad loads, security bugs, and so on. For information on resetting the phone, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that matches the model of the phone.

For information about how to delete the CTL file from Cisco Unified IP Phone models 7970, 7960, and 7940 only, see the Cisco Unified Communications Manager Security Guide or the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that matches the model of the phone.

Security Alarms

Cisco Unified Serviceability generates security-related alarms for X.509 name mismatches, authentication errors, and encryption errors. Cisco Unified Serviceability provides the alarm definitions.

Alarms may get generated on the phone for TFTP server and CTL file errors. For alarms that get generated on the phone, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager for your phone model and type (SCCP or SIP).

Security Performance Monitor Counters

Performance monitor counters monitor the number of authenticated phones that register with Cisco Unified Communications Manager, the number of authenticated calls that are completed, and the number of authenticated calls that are active at any time. Table 3-1 lists the performance counters that apply to security features.
Table 3-1  Security Performance Counters

<table>
<thead>
<tr>
<th>Object</th>
<th>Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>AuthenticatedCallsActive</td>
</tr>
<tr>
<td></td>
<td>AuthenticatedCallsCompleted</td>
</tr>
<tr>
<td></td>
<td>AuthenticatedPartiallyRegisteredPhone</td>
</tr>
<tr>
<td></td>
<td>AuthenticatedRegisteredPhones</td>
</tr>
<tr>
<td></td>
<td>EncryptedCallsActive</td>
</tr>
<tr>
<td></td>
<td>Encrypted Calls Completed</td>
</tr>
<tr>
<td></td>
<td>EncryptedPartiallyRegisteredPhones</td>
</tr>
<tr>
<td></td>
<td>EncryptedRegisteredPhones</td>
</tr>
<tr>
<td></td>
<td>SIPLineServerAuthorizationChallenges</td>
</tr>
<tr>
<td></td>
<td>SIPLineServerAuthorizationFailures</td>
</tr>
<tr>
<td></td>
<td>SIPTrunkServerAuthenticationChallenges</td>
</tr>
<tr>
<td></td>
<td>SIPTrunkServerAuthenticationFailures</td>
</tr>
<tr>
<td></td>
<td>SIPTrunkApplicationAuthorization</td>
</tr>
<tr>
<td></td>
<td>SIPTrunk Application Authorization Failures</td>
</tr>
<tr>
<td></td>
<td>TLSConnectedSIPTrunk</td>
</tr>
<tr>
<td>SIP Stack</td>
<td>StatusCodes4xxIns</td>
</tr>
<tr>
<td></td>
<td>StatusCodes4xxOuts</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>401 Unauthorized (HTTP authentication required)</td>
</tr>
<tr>
<td></td>
<td>403 Forbidden</td>
</tr>
<tr>
<td></td>
<td>405 Method Not Allowed</td>
</tr>
<tr>
<td></td>
<td>407 Proxy Authentication Required</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>BuildSignCount</td>
</tr>
<tr>
<td></td>
<td>EncryptCount</td>
</tr>
</tbody>
</table>

Refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for accessing performance monitors in RTMT, configuring perfmon logs, and for more details about counters.

The CLI command `show perf` displays performance monitoring information. For information about using the CLI interface, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

**Reviewing Security Log and Trace Files**

Cisco Unified Communications Manager stores log and trace files in multiple directories (cm/log, cm/trace, tomcat/logs, tomcat/logs/security, and so on).
Troubleshooting Certificates

The certificate management tool in Cisco Unified Communications Platform Administration allows you to display certificates, delete and regenerate certificates, monitor certificate expirations, and download and upload certificates and CTL files (for example, to upload updated CTL files to Unity). The CLI allows you to list and view self-signed and trusted certificates and to regenerate self-signed certificates.

The CLI commands `show cert`, `show web-security`, `set cert regen`, and `set web-security` allow you to manage certificates at the CLI interface; for example, `set cert regen tomatc`. For information about how to use the GUI or CLI to manage certificates, refer to Cisco Unified Communications Operating System Administration Guide and the Command Line Interface Reference Guide for Cisco Unified Solutions.

Troubleshooting CTL Security Tokens

The section contains information on the following topics:

- Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password, page 3-22
- Troubleshooting If You Lose One Security Token (Etoken), page 3-22

If you lose all security tokens (etokens), contact Cisco TAC for further assistance.

Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password

Each security token contains a retry counter, which specifies the number of consecutive attempts to log in to the etoken Password window. The retry counter value for the security token equals 15. If the number of consecutive attempts exceeds the counter value, that is, 16 unsuccessful consecutive attempts occur, a message indicates that the security token is locked and unusable. You cannot re-enable a locked security token.

Obtain additional security token(s) and configure the CTL file, as described in the Cisco Unified Communications Manager Security Guide. If necessary, purchase new security token(s) to configure the file.

After you successfully enter the password, the counter resets to zero.

Troubleshooting If You Lose One Security Token (Etoken)

If you lose one security token, perform the following procedure:
Procedure

Step 1  Purchase a new security token.

Step 2  Using a token that signed the CTL file, update the CTL file by performing the following tasks:
   a.  Add the new token to the CTL file.
   b.  Delete the lost token from the CTL file.

For more information on how to perform these tasks, see the Cisco Unified Communications Manager Security Guide.

Step 3  Reset all phones, as described in the Cisco Unified Communications Manager Security Guide.

Troubleshooting CAPF

This section contains information on the following topics:

- Troubleshooting the Authentication String on the Phone, page 3-23
- Troubleshooting If the Locally Significant Certificate Validation Fails, page 3-24
- Verifying That the CAPF Certificate Is Installed on All Servers in the Cluster, page 3-24
- Verifying That a Locally Significant Certificate Exists on the Phone, page 3-24
- Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone, page 3-24
- CAPF Error Codes, page 3-25

Troubleshooting the Authentication String on the Phone

If you incorrectly enter the authentication string on the phone, a message displays on the phone. Enter the correct authentication string on the phone.

Tip

Verify that the phone is registered to the Cisco Unified Communications Manager. If the phone is not registered to the Cisco Unified Communications Manager, you cannot enter the authentication string on the phone.

Verify that the device security mode for the phone equals nonsecure.

Verify authentication mode in the security profile that is applied to the phone is set to By Authentication String.

CAPF limits the number of consecutive attempts in which you can enter the authentication string on the phone. If you have not entered the correct authentication string after 10 attempts, wait at least 10 minutes before you attempt to enter the correct string again.
Troubleshooting If the Locally Significant Certificate Validation Fails

On the phone, the locally significant certificate validation may fail if the certificate is not the version that CAPF issued, the certificate has expired, the CAPF certificate does not exist on all servers in the cluster, the CAPF certificate does not exist in the CAPF directory, the phone is not registered to Cisco Unified Communications Manager, and so on. If the locally significant certificate validation fails, review the SDL trace files and the CAPF trace files for errors.

Verifying That the CAPF Certificate Is Installed on All Servers in the Cluster

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific for CAPF. The CAPF certificate, which the Cisco CTL client copies to all servers in the cluster, uses the .0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI or use the CLI:

- In DER encoded format—CAPF.cer
- In PEM encoded format—.0 extension file that contains the same common name string as the CAPF.cer

Verifying That a Locally Significant Certificate Exists on the Phone

You can verify that the locally significant certificate is installed on the phone at the Model Information or Security Configuration phone menus and by viewing the LSC setting. Refer to the Cisco Unified IP Phone Administration Guide for your phone model and type (SCCP or SIP) for additional information.

Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone

You can verify that a MIC exists in the phone at the Model Information or Security Configuration phone menus and by viewing the MIC setting. Refer to the Cisco Unified IP Phone Administration Guide for your phone model and type (SCCP or SIP) for additional information.

Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways

This section contains information on the following topics:

- Using Packet Capturing, page 3-24

Using Packet Capturing

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable SRTP encryption, you must use Cisco Unified Communications Manager Administration to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Cisco Unified Communications Manager and the device [Cisco Unified IP Phone (SCCP and SIP), Cisco IOS MGCP gateway, H.323 gateway, H.323/H.245/H.225 trunk, or SIP trunk].

Note

SIP trunks do not support SRTP.

- Capture the SRTP packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

For information about using or configuring packet capturing and about analyzing captured packets for SRTP-encrypted calls (and for all other call types), see the “Packet Capture” section on page 2-7.

Tip
Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

By using the Bulk Administration Tool that is compatible with this Cisco Unified Communications Manager release, you can configure the packet capture mode for phones. For information about how to perform this task, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

Tip
Performing this task in Cisco Unified Communications Manager Bulk Administration may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

### CAPF Error Codes

The following table contains CAPF error codes that may appear in CAPF log files and the corresponding corrective actions for those codes:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CAPF_OP_SUCCESS /*Success */</td>
<td>No correction action required.</td>
</tr>
<tr>
<td>1</td>
<td>CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */</td>
<td>Install a certificate on the phone. For more information, refer to the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>2</td>
<td>CAPF_OP_FAIL /<em>Fail</em>/</td>
<td>No corrective action available.</td>
</tr>
<tr>
<td>3</td>
<td>CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */</td>
<td>Enter the correct authentication string on phone. For more information, refer to the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>4</td>
<td>CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */</td>
<td>Update the locally significant certificate (LSC) on the phone. For more information, refer to the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>
Performing Failed RAID Disk Replacement

This section provides information about performing a failed disk replacement and the general guidelines for troubleshooting Redundant Array of Inexpensive Disks (RAID) rebuild functionality. This section contains information about the following topics:

- Performing Failed RAID Disk Replacement with Single Restart
- Performing Failed RAID Disk Replacement with Single Restart for Linux Software RAID
- Performing Failed RAID Disk Replacement Without Restart

The MCS servers use the RAID drive to protect from any data loss when the hard disk fails or runs into some issue.

To replace a failed disk using the RAID rebuild procedures, your system must operate with at least two hard disks.

For systems that operate with only one hard disk, RAID mirror does not apply, and disk failure will result in complete data loss. Recovery on such servers would require replacing the single failed disk with a replacement new disk and then subsequent DRS restoration. For such servers, Cisco highly recommends that you preconfigure DRS and schedule daily backups. This would provide maximum data recovery in the case of any such catastrophic failures.

For information on DRS, refer to the Disaster Recovery Administration Guide.

Limitations

Before you begin, you must understand the following limitations about RAID rebuild:

- These procedures apply to the Cisco Unified Communications Manager 7.1(2) release and later releases.
- These RAID rebuild procedures strictly do not apply to the following server models that have only one single physical disk:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */</td>
<td>This code indicates that the manufacture-installed certificate (MIC) has been invalidated. You must install a LSC. For more information, refer to the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>6</td>
<td>CAPF_OP_FAIL_INVALID_CREDENTIALS, /* Invalid credential */</td>
<td>Enter correct credentials.</td>
</tr>
<tr>
<td>7</td>
<td>CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure */</td>
<td>No corrective action available.</td>
</tr>
<tr>
<td>8</td>
<td>CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */</td>
<td>Reschedule the operation.</td>
</tr>
<tr>
<td>11</td>
<td>CAPF_OP_FAIL_LATE_REQUEST, /* User Initiated Request Late */</td>
<td>Reschedule the CAPF operation.</td>
</tr>
</tbody>
</table>

Table 3-2 CAPF Error Codes (continued)
Performing Failed RAID Disk Replacement

- MCS-7815-I3
- MCS-7816-H3
- MCS-7816-I3
- MCS-7816-I4

- The RAID rebuild will have Input/Output (I/O) performance impact; so, be sure to schedule the failed disk replacement and rebuild operations only during off-peak hours or in a maintenance window.

- Failed disk replacement instructions only get supported for the RAIDed server configuration as mentioned in each section and apply only when one of the RAIDed disks fails.

An SNMP or an RTMT trap or a disk LED status (on supported servers only) usually detects this failure. You can manually check the status of RAIDed drives by using the CLI command `show hardware`, as mentioned in the procedures.

---

**Warning**

The following procedures do not apply and are not supported if you attempt disk replacement for a disk that is not detected as failed per the following procedures.

For convenience, RAID rebuild procedures get categorized for various server types based on the server model numbers. Depending on the server model number, you can choose the corresponding procedure and replace the failed disk.

The following table contains the categorization of each server type that corresponds to the number of system restarts that are required during each procedure.

### Table 3-3 Server Categorization with Restart Type

<table>
<thead>
<tr>
<th>Required Restart Type</th>
<th>Server Model</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Restart</td>
<td>MCS-7825-H4</td>
<td>Performing Failed RAID Disk Replacement with Single Restart</td>
</tr>
<tr>
<td></td>
<td>MCS-7825-I3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7825-I4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7828-I3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7825-H3</td>
<td>Performing Failed RAID Disk Replacement with Single Restart</td>
</tr>
<tr>
<td></td>
<td>MCS-7828-H3</td>
<td></td>
</tr>
<tr>
<td>No Restart</td>
<td>MCS-7835-H2</td>
<td>Performing Failed RAID Disk Replacement Without Restart</td>
</tr>
<tr>
<td></td>
<td>MCS-7835-I2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7845-H2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7845-I2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7835-I3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS-7845-I3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DL-380-G6</td>
<td></td>
</tr>
</tbody>
</table>
Performing Failed RAID Disk Replacement with Single Restart

Perform the following procedure to replace a failed RAID disk for these specific servers:

- MCS-7825-H4
- MCS-7825-I3
- MCS-7825-I4
- MCS-7828-I3

**Step 1**
Log in to the console as an Administrator and enter the CLI command, `show hardware`.

**Step 2**
Check the status of the logical drives. Perform one of the following:
- If the logical drive status is OK or Optimal, you need not perform any further action.
- If the logical drive status is not OK, check the physical disk status, as described in Step 3.

**Step 3**
Enter the CLI command, `show hardware`, again and perform one of the following:
- If none of the physical disks displays the status as “Failed”, you need not perform any further action.
- If the logical drive status is not OK or Optimal, and any physical disk displays as “Failed”, identify the physical disk on the server as follows.

  The LED color of the failed disk will be in amber or red.

  **Note** You must perform step 2 to verify the logical RAID drive status and then perform step 3 to verify the physical disk status.

To replace the failed drive and rebuild the RAID, continue with Step 4.

**Step 4**
Perform a graceful shut down of the server by using the CLI command `utils system shutdown`.

**Step 5**
After the system is shut down, replace the empty slot on the failed disk with a new disk that is of the same type, of same manufacturer, and of the same size as that of the original disk. For example, Western Digital.

**Step 6**
Ensure the new replacement disk is inserted all the way in.

**Step 7**
Power up the system.

**Step 8**
During the system startup, if you view a message about RAID, accept the default option and continue with the system startup.

**Step 9**
After the system is up, log in to the CLI and enter the CLI command `show hardware`.

  In the show hardware command output, in the “Logical Drive” section, the “Current Operation” field will display “Rebuild”, and the “Percentage Complete” field will display the percentage complete for RAID rebuild.

  The Status on the new, replaced hard disk will display “Rebuilding” for the course of rebuilding. Rebuild will take between 1 to 2 hours to complete. This depends on the size of the disk.

  After the failed RAID disk replacement is complete, the status of both the logical drive and the new physical disk will display as “OK” and “Online”.

In the show hardware command output, in the “Logical Drive” section, the “Current Operation” field will display “Rebuild”, and the “Percentage Complete” field will display the percentage complete for RAID rebuild.

The Status on the new, replaced hard disk will display “Rebuilding” for the course of rebuilding. Rebuild will take between 1 to 2 hours to complete. This depends on the size of the disk.

After the failed RAID disk replacement is complete, the status of both the logical drive and the new physical disk will display as “OK” and “Online”.

The LED color of the failed disk will be in amber or red.
Performing Failed RAID Disk Replacement with Single Restart for Linux Software RAID

Perform the following procedure to replace a failed RAID disk for these specific servers:

- MCS-7825-H3
- MCS-7828-H3

**Step 1** Log in to the console as an administrator and enter the CLI command `show hardware`.

**Step 2** Check the status of the logical drives:
- If the logical drive state is active or clean, you need not perform any further action.
- If the logical drive state is degraded, check the physical disk status, as described in Step 3.

**Step 3** Enter the CLI command `show hardware`, again and check the physical disk status:
- If none of the physical disks displays the state as “Removed”, you need not perform any further action.
- If the logical drive state is degraded, and any physical disk displays the state as “Removed”, identify the physical disk on the server as follows—The LED color of the failed disk will be amber or red.

You must perform Step 2 to verify the logical RAID drive Status and then perform Step 3 to verify the physical disk status.

To replace the failed drive and rebuild the RAID, continue with Step 4.

**Step 4** Shut down the server using the CLI command `utils system shutdown`.

**Step 5** After the system shuts down, replace the faulty hard disk with a new disk that is of the same type and size as the original disk and that comes from the same manufacturer—for example, Western Digital.

**Step 6** Ensure that the new replacement disk is fully inserted.

**Step 7** Power up the system.

**Step 8** After the system is powered up, log in to the CLI and enter the CLI command `show hardware`.

In the `show hardware` command output, in the Logical Drive section, the Current Operation field will display Rebuild.

The status on the new, replaced hard disk will display spare rebuilding during the course of rebuilding.

Rebuilding will take 8 to 10 hours to complete. The duration depends on the size and I/O activity of the disk.

After the failed RAID disk replacement is complete, the status of both the logical drive and the new physical disk will display as clean and active.

**Warning** If the failed disk is the first disk in the array, then replace it with a blank new disk that does not contain any partitions. However, if you replace the failed disk with a disk that was previously configured using HP RAID, the system will not be able to boot and this will result in a kernel panic.
Performing Failed RAID Disk Replacement

Perform the following procedure to replace a failed RAID disk for these specific servers:

- MCS-7835-H2
- MCS-7835-I2
- MCS-7845-H2
- MCS-7845-I2
- MCS-7835-I3
- MCS-7845-I3
- DL-380-G6

Step 1 Log in to the console as an Administrator and enter the CLI command, `show hardware`.

Step 2 Check the status of the logical drives. Perform one of the following:

- If the logical drive status is OK or Optimal, you need not perform any further action.
- If the logical drive status is not OK, check the physical disk status, as described in Step 3.

Step 3 Enter the CLI command, `show hardware`, again and perform one of the following:

- If none of the physical disks displays the status as “Failed”, you need not perform any further action.
- If the logical drive status is not OK or Optimal, and any physical disk displays as “Failed”, identify the physical disk on the server as follows.

The LED color of the failed disk will be in amber or red.

**Note** You must perform step 2 to verify the logical RAID drive status and then perform step 3 to verify the physical disk status.

To replace the failed drive and rebuild the RAID, continue with Step 4.

Step 4 Pull the failed disk from the slot.

Step 5 Enter the `show hardware` CLI command to ensure that the current number of physical disks is reported.

It reports:

- On a 7835 class of server, only one physical disk in the `show hardware` CLI command output.
- On a 7845 class of server, only three physical disks in the `show hardware` CLI command output.

Step 6 Replace the empty slot on the failed disk with a new disk that is of the same type, of same manufacturer, and of the same size as that of the original disk. For example, Western Digital.

Step 7 Ensure the new replacement disk is inserted all the way in.

Step 8 Run the `show hardware` CLI command to ensure that the newly inserted physical disk has been detected.

It reports:

- On a 7835 class of server, only two physical disks in the `show hardware` CLI command output.
- On a 7845 class of server, only four physical disks in the `show hardware` CLI command output.

Step 9 If the correct disks are not reported, pull out the new disk and repeat from Step 5.
Step 10 Enter the CLI command `show hardware` to check the RAID status. It displays the rebuild percentage completion.

- Rebuild will take between 1 to 2 hours to complete. This depends on the size of the disk.
- After the failed RAID disk replacement is complete, the status of both the logical drive and the new physical disk will display as “OK” and “Online”.