Cisco Unified Communications Manager System Issues

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

Cisco Unified Communications Manager System Not Responding

This section covers issues related to a Unified Communications Manager system that is not responding.

Related Topics

Cisco Unified Communications Manager System Stops Responding, on page 2
Cisco Unified Communications Manager Administration Does Not Display, on page 3
Error When Attempting to Access Cisco Unified Communications Manager Administration, on page 3
Error When Attempting to Access Cisco Unified Communications Manager Administration on a Subsequent Node, on page 3
You Are Not Authorized to View, on page 4
Problems Displaying or Adding Users with Cisco Unified Communications Manager, on page 4
Name to Address Resolution Failing, on page 5
Port 80 Blocked Between Your Browser and the Cisco Unified Communications Manager Server, on page 6
Improper Network Setting Exists in the Remote Machine, on page 6
Slow Server Response

Cisco Unified Communications Manager System Stops Responding

Symptom

The Unified Communications Managersystem 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 Unified Communications Manager, users receive delayed dial tone, and/or the Unified Communications Managerserver freezes due to high CPU usage. For event log messages that are not included here, view the 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

1. Collect Cisco CallManager traces 15 minutes before and after the interruption.
2. Collect SDL traces 15 minutes before and after the interruption.
3. Collect perfmon traces if available.
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 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. See related topics or the *Cisco Unified Serviceability Administration Guide*.

Related Topics

Verify Cisco Unified Communications Manager Services Are Running

Error When Attempting to Access Cisco Unified Communications Manager Administration

Symptom

An error message displays when you are trying to access Unified Communications Manager.

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 Unified Communications Manager Administration.

Possible Cause

If the IP address of the first 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 Unified Communications Manager node in the document, *Changing the IP Address and Host Name for Unified Communications Manager*.

You Are Not Authorized to View

Symptom

When you access 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 Unified Communications Manager.

Possible Cause

You may encounter the following problems if you are working with 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 redisplays.
- 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 Unified Communications Manager Administration, if your 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:

- Access Cisco Unified Communications Manager Administration by using the IP address of the server.
- Do not use non-DNS characters in the Server Name.
- Use the localhost or IP address in the URL.

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 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 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.

Recommended Action

1. Verify whether other types of traffic to the Unified Communications Manager server, such as ping or Telnet, are allowed. If any are successful, it will show that http access to the 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 Unified Communications Manager.

When you attempt the same action from other remote machines, 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 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 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.

Note If you cannot browse from the remote server after following this procedure, contact TAC to have the issue investigated in more detail.

Manage Impact of Cisco RAID Operations

Cisco Redundant Array of Independent Disks (RAID) Controller conducts background operations such as Consistency Check (CC), Background Initialization (BGI), Rebuild (RBLD), Volume Expansion & Reconstruction (RLM) and Patrol Real (PR).

These background operations are expected to limit their impact to I/O operations. However, there have been cases of higher impact during some of the operations like Format or similar input output operations. In these cases, both the I/O operation and the background operations may consume large amount of CPU resources. It is recommended that CC and Patrol Read jobs are scheduled when the load is relatively less. If there are CallManager servers where huge load is running at the same time, it is recommend that you limit possible concurrent background operations and other intensive I/O operations of CallManager.

Database Replication

This section covers database replication issues for aUnified Communications Manager system.

Related Topics

Replication Fails Between the Publisher and the Subscriber Server, on page 8
Database Replication Does Not Occur When Connectivity Is Restored on Lost Node, on page 11
Database Tables Out of Sync Do Not Trigger Alert, on page 11
Resetting Database Replication When You Are Reverting to an Older Product Release, on page 12

Replication Fails Between the Publisher and the Subscriber Server

Replicating the database represents a core function of 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 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 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

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 2, on page 8 .
   - To verify by using Cisco Unified Reporting, see 3, on page 9 .
   - To verify by using RTMT, see 4, on page 9 .
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"


            ==>query class: - Perf class (Number of Replicates Created and
State of Replication) has instances and values: ReplicateCount -> Number of
Replicates Created = 344 ReplicateCount -> Replicate_State = 2
```

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.

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 Unified Communications Manager database.

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.
   - 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** .

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.

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. See the related topics for methods to verify the state of replication if replication fails. 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

1. Run **utils dbreplication stop** on the affected subscribers. You can run them all at once.
2. Wait until step 1 completes, then run **utils dbreplication stop** on the affected publisher server.
3. Run **utils dbreplication clusterreset** 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`
4. From the affected publisher, run **utils dbreplication reset all**.
5. 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 **utils dbreplication status** shows Status 2.

Related Topics

Replication Fails Between the Publisher and the Subscriber Server, on page 8

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 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 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 dbrepication 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

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*.
2. If the servers are in Replication State 2, run the following command on the publisher server:
3. **utils dbreplication repair** *server name*
4. If the servers are not in Replication State 2,
5. run the following command on all subscriber servers:
6. **utils dbreplication stop**
7. Then, run the following commands on the publisher server:
8. **utils dbreplication stop**
9. then
10. **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 Cause

In most cases, problems with LDAP over SSL involve invalid, wrong, or incomplete certificates (chains) on the 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

Symptom

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

Possible Cause

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 Action

- 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 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.

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 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 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

Related Topics

MIVR-SS_TEL-4-ModuleRunTimeFailure, on page 17
MIVR-SS_TEL-1-ModuleRunTimeFailure, on page 19

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:

Related Topics

Unable to Create Provider–Bad Login or Password, on page 17
Unable to Create Provider-Connection Refused, on page 17
Unable to Create Provider–Login= , on page 18
Unable to Create Provider–Hostname, on page 18
Unable to Create Provider–Operation Timed Out , on page 19
Unable to Create Provider–Null , on page 19

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-timefailure 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.
%MIVR-SS_TEL-7-
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 Unified CM User window (`http://servername/ccmuser`) on the Unified CM to ensure that the Unified CM cannot authenticate correctly.

Unable to Create Provider-Connection Refused

Possible Cause

The Unified Communications Manager refused the JTAPI connection to the Unified Communications Manager.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure 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-timefailure 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 Unified Communications Manager.

Full Text of Error Message

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure 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 Unified Communications Manager.

Full Text of Error Message

```
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
102: Mar 24 11:37:42.168 PST%MIVR-SS_TEL-7-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 Unified Communications Manager. Make sure no IP routing problems exist. Test connectivity by pinging the 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

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
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 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 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 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_CTIPORT

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_CTIPORT:
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 Unified Communications Manager configuration and also associates with the JTAPI user on the Unified Communications Manager.

Security Issues

This section provides information about security-related measurements and general guidelines for troubleshooting security-related problems.

Note 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 7960, and 7940 only, see the System Configuration Guide for Cisco Unified Communications Manager or the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* that matches the model of the phone.

Related Topics

Security Alarms, on page 21
Security Performance Monitor Counters, on page 21
Reviewing Security Log and Trace Files, on page 22
Troubleshooting Certificates, on page 23
Troubleshooting CTL Security Tokens, on page 24
Troubleshooting CAPF, on page 26
Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways, on page 27

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 Unified Communications Manager, the number of authenticated calls that are completed, and the number of authenticated calls that are active at any time. The following table lists the performance counters that apply to security features.

Table 1: Security Performance Counters

Object	Counters
Unified Communications Manager	AuthenticatedCallsActive AuthenticatedCallsCompleted AuthenticatedPartiallyRegisteredPhone AuthenticatedRegisteredPhones EncryptedCallsActive EncryptedCallsCompleted EncryptedPartiallyRegisteredPhones EncryptedRegisteredPhones SIPLineServerAuthorizationChallenges SIPLineServerAuthorizationFailures SIPTrunkServerAuthenticationChallenges SIPTrunkServerAuthenticationFailures SIPTrunkApplicationAuthorization SIPTrunkApplicationAuthorizationFailures TLSConnectedSIPTrunk
SIP Stack	StatusCodes4xxIns StatusCodes4xxOuts For example: 401 Unauthorized (HTTP authentication required) 403 Forbidden 405 Method Not Allowed 407 Proxy Authentication Required
TFTP Server	BuildSignCount EncryptCount

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

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

Note For devices that support encryption, the SRTP keying material does not display in the trace file.

You can use the trace collection feature of Cisco Unified Real-Time Monitoring Tool or CLI commands to find, view, and manipulate log and trace files.

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 tomcat**. For information about how to use the GUI or CLI to manage certificates, refer to Administration Guide for Cisco Unified Communications Manager and the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Troubleshooting Ciphers

The Cipher Management page has no default values. Instead, the Cipher Management feature takes effect only when you configure Ciphers.

For information about Ciphers, see Security Guide for Cisco Unified Communications Manager

This section provides information to help you troubleshoot problems with Unified Communications Manager Ciphers:

Troubleshooting DRS and CDR Functionality

Symptom

Breakage to DRS and CDR functionality.

Possible Cause

Configuring `hmac-sha2-512` in SSH MAC interface affects the DRS and CDR functionality.

Configuring Ciphers

- `aes128-gcm@openssh.com`
- `aes256-gcm@openssh.com`

in **SSH Cipher's** field or configuring only `ecdh-sha2-nistp256` algorithm in "SSH KEX" breaks the DRS and CDR functionalities.

Recommended Action

1. From Cisco Unified OS Administration, choose **Security** > **Cipher Management**
2. Remove or Delete the above mentioned ciphers if they are already configured and **Save** the settings.

3. Reboot the server for the changes to take effect.

Troubleshooting CTL Security Tokens

The section contains information about troubleshooting CTL security tokens.

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

Note These troubleshooting steps are not required if you manage cluster security through the CLI command set **utils ctl**.

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 Security Guide for Cisco Unified Communications Manager. If necessary, purchase new security token(s) to configure the file.

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

Troubleshooting If You Lose One Security Token (Etoken)

Note This procedure is not required if you manage cluster security through the CLI command set **utils ctl**.

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

Procedure

1. Purchase a new security token.
2. Using a token that signed the CTL file, update the CTL file by performing the following tasks:
3. Add the new token to the CTL file.
4. Delete the lost token from the CTL file.

   For more information on how to perform these tasks, see the Security Guide for Cisco Unified Communications Manager.
5. Reset all phones, as described in the Security Guide for Cisco Unified Communications Manager.

Troubleshooting If You Lose All Security Tokens (Etoken)

Perform the following procedure if you lose the security tokens and you need to update the CTL file.

Tip Perform the following procedure during a scheduled maintenance window, because you must reboot all servers in the cluster for the changes to take effect.

Procedure

Step 1 On every Unified Communications Manager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists from the OS SSH command line.

file list tftp *CTLFile.tlv*

Step 2 Delete CTLFile.tlv.

file delete tftp *CTLFile.tlv*

Step 3 Repeat step 1 and step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 By using the Cisco CTL client, create the CTL File, as described in "Installing the Cisco CTL Client" and "Configuring the Cisco CTL Client".

Tip If the clusterwide security mode is in mixed mode, the Cisco CTL client displays the message No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click OK; then, choose Set CallManager Cluster to Mixed Mode and complete the CTL file configuration.

Step 6 Reboot all the servers in the cluster.

Step 7 After you create the CTL file on all the servers and reboot all servers in the cluster, delete the CTL file from the phone, as described in "Deleting the CTL File on the Cisco Unified IP Phone".

Troubleshooting ITL Files

Symptom

Error parsing the ITL File

Possible Cause

A Corrupt **ITLFile.tlv** or **ITLEXTFile.tlv**

Recommended Action

1. From Cisco Unified OS Administration, choose **Software Upgrade** > **TFTP File Management**
2. Search for **itlfileflags.txt** and select the file.

3. Click Delete Selected to delete the selected file.
4. Restart the TFTP service.

Enter the command **show itl** in Command Line Interface to confirm ITL status after applying actions.

Troubleshooting CAPF

This section contains information about troubleshooting CAPF.

Related Topics

Troubleshooting the Authentication String on the Phone, on page 26
Troubleshooting If the Locally Significant Certificate Validation Fails, on page 26
Verifying That the CAPF Certificate Is Installed on All Servers in the Cluster, on page 26
Verifying That a Locally Significant Certificate Exists on the Phone, on page 27
Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone, on page 27
CAPF Error Codes, on page 28

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 Unified Communications Manager. If the phone is not registered to the 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 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 about troubleshooting encryption for phones and Cisco IOS MGCP Gateways.

Related Topics

Using Packet Capturing, on page 27

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 Assistant to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between 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 topics related to packet capture.

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 Unified Communications Manager release, you can configure the packet capture mode for phones. For information about how to perform this task, refer to the Bulk Administration Guide for Cisco Unified Communications Manager.

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

Related Topics

Packet Capture

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 2: CAPF Error Codes

Error Code	Description	Corrective Ac
0	CAPF_OP_SUCCESS /*Success */	No correction required.
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	Install a certif phone. For mo information, s Guide for Cis Communicati Manager.
2	CAPF_OP_FAIL /* Fail */	No corrective available.
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	Enter the corr authentication phone. For mo information, s Guide for Cis Communicati Manager.
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	Update the lo significant ce (LSC) on the more informa Security Guid Unified Comm Manager.

Error Code	Description	Corrective
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	This code the manuf certificate invalidate install a L informatio Guide for Communi Manager.
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	Enter corr
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	No correc available.
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	Reschedul
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	Reschedul operation.