Cisco Unified Communications Manager 7.x/8.x: Troubleshoot Backup Issue

Document ID: 111796

Contents

Introduction

Cisco Unified Communications Manager backups are not running as scheduled. All Disaster Recovery Framework (DRF) services are down, and no new devices, schedules, or statuses can be viewed from the DRF console. This document discusses how to troubleshoot this issue.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Unified Communications Manager 7.1(3)/8.x .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem

Cisco Unified Communications Manager backups are not running as scheduled. All Disaster Recovery Framework (DRF) services are down, and no new devices, schedules, or statuses can be viewed from the DRF console. Also, when you access the DRF admin pages, this error message is received:

```
Status:  Local Agent is not responding.
This may be due to Master or Local Agent being down.
```

This RTMT alert is received during the backup failure:

```
CiscoDRFFailure Reason : Master Agent was unable to send a
backup/restore request to the local agent.
Node [ELS−PUB1] is not connected.
AppID : Cisco DRF Master
ClusterID : NodeID: ELS−pub1 .
The alarm is generated on Tue Nov 24 02:00:04 PST 2009
```

Solution

First, verify if the Certificate Serial Number in the keystore of Publisher is present in the Truststore of all Subscribers. Complete these steps:

1. Log on to CUCM OS Administration page of Publisher server of the cluster setup. Choose **Security > Certificate Management**. The Certificate List window displays.
2. You can use the **Find** controls in order to filter the certificate.
3. Click on the **ipsec.pem** file and check the serial number of the certificate.
4. Log on to CUCM OS Administration page of each node of the cluster. Choose **Security > Certificate Management**. The Certificate List window displays.
5. You can use the **Find** controls in order to filter the certificate.
6. Click on **ipsec−trust.pem** file with the file name of hostname of the publisher and check the serial number of the certificate.
7. Certificate Serial Number should be same on all the nodes of the cluster. If Serial Number of any node is mismatched, complete these steps.

    a. Log on to CUCM OS Admin page of affected node.
    b. Choose **Security > Certificate Management**. The Certificate List window displays.

c. You can use the Find controls in order to filter the certificate.
d. Click on **ipsec.pem** file and download that certificate.
e. Find the existing **ipsec−trust** with the filename of the hostname of the publisher,click on the file name and **Delete**.
f. Upload the downloaded **ipsec.pem** file with the caption **ipsec−trust**.
g. Restart the **DRF Master Agent(MA)/DRF Local Agent (LA)**.

Error: Cannot write: Broken pipe

DRF backup failed with this error message:

```
/bin/tar: −: Cannot write: Broken pipe
/bin/tar: Error is not recoverable: exiting now
CCMDB Backup failed, unable to tar data to master agent
Restoring CAR services ...
```

This issue is documented in Cisco bug ID CSCte62205 (registered customers only)

As a workaround try one of these steps:

1. Disable **client alive messages** on the Open SSH server
2. Set the **ClientAliveCountMax** and **ClientAliveInterval** to a high enough count / interval so the server does not timeout the connection to CUCM during the backup.
3. Restart the DRF Master Agent(MA)/DRF Local Agent (LA).

DRS Hangs During CCMDB Backup

Problem

DRS hangs during CCMDB backup if there are large number of CDR/CMR files accumulated in the Preserve folder. This issue is documented in Cisco bug ID CSCsl16967 (registered customers only) .

Note: If you stop CAR service, it does not stop the accumulation of flat CDR files.

Solution

Complete these steps in order to resolve this issue:

1. Complete these steps in order to clean up the CDR files temporarily so that DRS can proceed:

    a. Stop the CDR Agent service on all servers in the cluster, so that no new CDR files are pushed to the publisher.
    b. Run this command in order to verify that all files have been pushed to the billing server(s):

    ```
    file list activelog /cm/cdr_repository/destination/*
    ```
2. Complete these steps in order to verify that there are no symbolic links in any of the subfolders:

    a. Stop CDR Repository Manager, CAR Scheduler, and CAR Web Service on the publisher.
    b. Use this command in order to remove all the files under /var/log/active/cm/cdr_repository/preserve/<*date*> that have been accumulated:

    ```
    file delete activelog /cm/cdr_repository/preserve/* noconfirm
    ```
    c. Use this command in order to remove all the symbolic links under

/var/log/active/cm/cdr_repository/car/<*date*>:

```
file delete activelog /cm/cdr_repository/car/* noconfirm
```

   d. Restart CDR Repository Manager, CAR Scheduler, and CAR Web Services on the publisher.

3. Complete these steps in order to stop further accumulation of CDR files:

   Note: In order to stop further accumulation of CDR files, you must start the CAR Scheduler service, set the loader to schedule continuous loading, and load CDR only.

   a. If it is not yet created, create a ccmadmin account in user group management on the ccmadmin page.
   b. Log in to CAR, and go to **System** > **Scheduler** > **CDR Load**.
   c. Check the **Continuous Loading 24/7** and the **Load CDR only** check boxes, and click **Update**.
   d. Choose **System** > **Database** > **Configure Automatic Database Purge**.
   e. Enter **1** for Min Age of Call Detail Records and Max Age of Call Detail Records, and click **Update**.
   f. Choose **Report Config** > **Automatic Generation/Alert**.
   g. For each report, choose **Disabled**, and click **Update**.
4. Restart the CDR Agent service on all the servers.

Error: The system is currently locked by another process. Please try again later

DRS Backups stop to execute automatically and when you attempt a manual backup, you get the `Backup operation currently in progress. Please wait and try after sometime` error message. When you try to install a new version or a COP file, you get the `The system is currently locked by another process. Please try again later` error message. This issue occurs if DRF is scheduled to backup the CUCM server automatically. This is documented by Cisco bug ID CSCsr87199 (registered customers only) .

Solution

Reset DRF Master Agent in order to resolve the issue.

Backup Fails with Winsock Error

With CUCM 8.x, the backup failed with the `Winsock Error 10054/10035/10053` error message.

Solution

Make sure that the firewall is disabled on the remote backup device and perform the backup again.

DRF Backup Does Not Backup Certificates

With CUCM 8.x, on a bridge upgrade restored server, the ITL file does not have a valid signer. Phones do not have https services if the publisher is the TFTP server. On a migration to UCS, or any new hardware where a backup and restore is performed, phones do not accept configuration files and changes from the new cluster without the manual deletion of the existing ITL from the phones.

When you restore from a disaster recovery situation, phones no longer recognize their configuration or ITL files after the DRS restore if the restored server was the TFTP server. Phones may not recognize configuration changes or upgrades until their existing ITL is deleted and replaced with the newly generated ITL.

Also, when you issue the **show itl** CLI command on the servers, this error message appears:

```
This etoken was not used to sign the ITL file.
Verification of the ITL file failed.
Error parsing the ITL file
```

This issue is documented by Cisco bug ID CSCtn50405 (registered customers only) .

Solution

After a disaster recovery or hardware migration situation, complete these steps.

1. Regenerate the CallManager.pem file (only on the restored server) to sync the CallManager.pem file on the file system to the one in the database.
2. Restart TVS and TFTP.
3. For a single node cluster, or only one TFTP server, delete the ITL file manually from all phones in the cluster.
4. For a Multi node cluster, phones should automatically use TVS of alternate CallManager Group Servers in order to authenticate the new ITL file. Alternatively phones can be pointed to another TFTP server in the cluster.

After a bridge upgrade, complete these steps.

1. Regenerate the CallManager.pem file (only on the restored server) to sync the CallManager.pem file on the file system to the one in the database.
2. Restart TVS and TFTP.
3. The phones need to be reset in order to download the new ITL file, but should not need to have the ITL file deleted as they never would have had a valid ITL file to download so far.

Error Message: bad decrypt 16404:error

With CUCM 8.x, DRS restore fails for the TFTP components with this error message

```
error:06065064:digital envelope routines:EVP_DecryptFinal:bad
decrypt:evp_enc.c:438:
```

Solution

This error message is an indication of the IP Address or Hostname Mismatch. Make sure that the CUCM server has the same IP Address and Hostname as on the MCS servers from where the backup is located. If the hostname is not the same as the backup server, you need to modify the hostname in order to be the same as the backup server and run the restore again.

Error on the backup page on CUCM

Problem

When you navigate to the backup page, the `Local Agent is not responding. This may be due to Master or Local Agent being down` error message appears. This also happens while you attempt to add a back−up device.

Solution

Complete these steps in order to resolve this issue:

1. Login to the CUCM OS Admin page.
2. Choose **Security > Certificate Management**.
3. Check the serial number for **ipsec.pem** file.
4. Ensure that the serial number matches the **ipsec−trust.pem** file for the subscribers.
5. Restart the Cisco DRF MAster and DRF Local service in the Publisher.
6. Activate the **TFTP** service.

Unable to Add Backup Device

Problem

You are unable to add Backup Device on the CUCM DRS page.

Solution

In order to resolve this issue, you need to add the Cisco−recommended SFTP server as the Backup Device. You can use any one of these SFTP servers:

- Open SSH for Unix systems
- Cygwin
- Titan
- GlobalSCAPE EFT Server formerly known as GlobalSCAPE's Secure FTP Server

Cisco recommends SFTP products that are certified with Cisco through the Cisco Technology Developer Partner program (CTDP).

Refer to Configure Backup Server for Cisco Unified Communications Manager for more information.

Unable to Restore CUCM 8.x Server

Problem

This error message appears when you try to restore CUCM 8.5:

```
digital envelope routines:EVP_DecryptFinal:bad
decrypt:evp_enc.c:438:
```

Solution

This error occurs if DNS was configured when the backup was taken, but it was not configured when the restore is being done. In order to resolve this issue, complete the steps:

1. Configure DNS before you perform the restore.
2. Ensure that the FQDN of the server is resolvable by DNS.

   Note: This is documented in the Cisco bug ID CSCtk05743 (registered customers only)

Unable to restore CUCM 8.5

Problem

Unable to restore a 8.5. server, giving the following error:

```
digital envelope routines:EVP_DecryptFinal:bad
decrypt:evp_enc.c:438:
```

Solution

This issue may occur if there is any mismatch of IP / Hostname / Security password. However, in this case all are matched.

The issue is in relation to the **DNS / Domain information** not being configured on the server to match. This will occur if DNS was configured when the backup was taken, but it was not configured when the restore is being done.

To resolve this issue configure DNS before performing the restore. Ensure that the FQDN of the server is resolvable by DNS.

Note: This is documented in the Cisco Bug ID: CSCtk05743 (registered customers only)

Related Information

- **Cisco Unified Communications Manager (CallManager) Frequently Asked Questions**
- **IBM 7816−I4 782x−I4 filesystem errors**
- **Cisco Unified Communications Operating System Administration Guide, Release 7.1(2) − Security**
- **Callmanager 5.x: Delete and Regenerate a Security Certificate**
- **Cisco Unified Communications Manager (CallManager) Backup Error − Failed to Retrieve Destination Details**
- **Configure Backup Server for Cisco Unified Communications Manager**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony** ↗
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map