# Restore the System


- Restore Overview, on page 1
- Restore Prerequisites, on page 2
- Restore Task Flow, on page 3
- Data Authentication, on page 11
- Alarms and Messages, on page 13
- Restore Interactions and Restrictions, on page 16
- Troubleshooting, on page 17


# Restore Overview

The Disaster Recovery System (DRS) provides a wizard to walk you through the process of restoring your system.

The backup files are encrypted and only the DRS system can open them to restore the data. The Disaster Recovery System includes the following capabilities:

- A user interface for performing restore tasks.
- A distributed system architecture for performing restore functions.

## Master Agent

The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the publisher node. The Master Agents on the subscriber nodes do not perform any functions.

## Local Agents

The server has a Local Agent to perform backup and restore functions.

Each node in a Cisco Unified Communications Manager cluster, including the node that contains the Master Agent, must have its own Local Agent to perform backup and restore functions.

**Note** By default, a Local Agent automatically gets started on each node of the cluster, including IM and Presence nodes.

# Restore Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail.
- Make sure that the IP address, hostname, DNS configuration and deployment type for the server matches the IP address, hostname, DNS configuration and deployment type that are stored on the backup file.
- If you have changed the cluster security password since the backup was run, make sure that you have a record of the old password, or the restore will fail.
- If IPsec policy is enabled in a cluster, ensure to disable it before starting the restore operation.

### Re-enable SAML SSO after Restore

**Important** This section is applicable for Release 12.5(1)SU7 only.

After restoring the system using DRS, SAML SSO can be disabled on any of the nodes in the cluster intermittently. To re-enable SAML SSO on the affected nodes, you must perform the following:

1. From Cisco Unified CM Administration, choose **System** > **SAML Single Sign On**.
2. Click **Run SSO Test**.
3. After you see the **"SSO Test Succeeded!"** message, close the browser window; click **Finish**.

**Note** Cisco Tomcat restarts during SAML SSO re-enabling process. It will not have any impact on the nodes where SAML SSO is already enabled.

# Restore Task Flow

During the restore process, do not perform any tasks with Cisco Unified Communications Manager OS Administration or Cisco Unified IM and Presence OS Administration.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Restore the First Node Only, on page 3 | (Optional) Use this procedure only to restore the first publisher node in the cluster. |
| **Step 2** | Restore Subsequent Cluster Node, on page 5 | (Optional) Use this procedure to restore the subscriber nodes in a cluster. |
| **Step 3** | Restore Cluster in One Step After Publisher Rebuilds, on page 7 | (Optional) Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt. |
| **Step 4** | Restore Entire Cluster, on page 8 | (Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you may need to rebuild all nodes in the cluster. |
| **Step 5** | Restore Node Or Cluster to Last Known Good Configuration, on page 9 | (Optional) Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure. |
| **Step 6** | Restart a Node, on page 10 | Use this procedure to restart a node. |
| **Step 7** | Check Restore Job Status, on page 11 | (Optional) Use this procedure to check the restore job status. |
| **Step 8** | View Restore History, on page 11 | (Optional) Use this procedure to view the restore history. |

# Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

### Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

### Procedure

**Step 1** From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

**Step 2** In the **Restore Wizard Step 1** window, **Select Backup Device** area, select the appropriate backup device to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file you want to restore.

**Note**
The backup filename indicates the date and time that the system created the backup file.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, click **Next**.

**Step 7** Choose the features that you want to restore.

**Note**
The features that you have selected for backup will be displayed.

**Step 8** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 9** Select the Perform file integrity check using the SHA1 Message Digest checkbox if you want to run a file integrity check.

**Note**
The file integrity check is optional and is only needed in the case of SFTP backups.

Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which slows down the restore process.

We can use SHA-1 for message digest verification in FIPS mode as well. SHA-1 is allowed for all non-digital signature uses in the hash functions applications like HMAC and Random Bit Generation that are not used for digital signatures. For instance, SHA-1 can still be used to compute a checksum. Only for signature generation and verification, we can't use SHA-1.

**Step 10** Select the node to restore.

**Step 11** Click **Restore** to restore the data.

**Step 12** Click **Next**.

**Step 13** When you are prompted to select the nodes to restore, choose only the first node (the publisher).

**Caution**
Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

**Step 14** (Optional) From the **Select Server Name** drop-down list, select the subscriber node from which you want to restore the publisher database. Ensure that the subscriber node that you chose is in-service and connected to the cluster.
The Disaster Recovery System restores all non database information from the backup file and pulls the latest database from the chosen subscriber node.

**Note**

This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 14 and restart the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

**Step 15** Click **Restore**.

**Step 16** Your data is restored on the publisher node. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

**Note**
Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

**Step 17** When the **Percentage Complete** field on the **Restore Status** window, shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

**Note**
If you are restoring a Cisco Unified Communications Manager node only, the Cisco Unified Communications Manager and IM and Presence Service cluster must be restarted.

If you are restoring an IM and Presence Service Publisher node only, the IM and Presence Service cluster must be restarted.

### What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 11
- To restart a node, see Restart a Node, on page 10

# Restore Subsequent Cluster Node

This procedure is applicable to the Cisco Unified Communications Manager subscriber (subsequent) nodes only. The first Cisco Unified Communications Manager node installed is the publisher node. All other Cisco Unified Communications Manager nodes, and all IM and Presence Service nodes are subscriber nodes.

Follow this procedure to restore one or more Cisco Unified Communications Manager subscriber nodes in the cluster.

### Before you begin

Before you perform a restore operation, ensure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore. Disaster Recovery System does not restore across different hostnames, IP addresses, DNS configurations and deployment types.

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. Disaster Recovery System supports only matching software versions for restore operations. If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

### Procedure

**Step 1** From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

**Step 2** In the **Restore Wizard Step 1** window, **Select Backup Device** area, choose the backup device from which to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, select the features that you want to restore.

**Note**
Only the features that were backed up to the file that you chose display.

**Step 7** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 8** In the **Restore Wizard Step 4** window, when you are prompted to choose the nodes to restore, select only the subsequent nodes.

**Step 9** Click **Restore**.

**Step 10** Your data is restored on the subsequent nodes. For more information about how to view the status of the restore, see the What to Do Next section.

**Note**
During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

**Step 11** When the **Percentage Complete** field on the **Restore Status** window shows 100%, restart the secondary servers you just restored. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

**Note**
If the IM and Presence Service first node is restored. Ensure to restart the IM and Presence Service first node before you restart the IM and Presence Service subsequent nodes.

### What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 11
- To restart a node, see Restart a Node, on page 10

# Restore Cluster in One Step After Publisher Rebuilds

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt or freshly installed.

### Procedure

**Step 1** From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

**Step 2** In the **Restore Wizard Step 1** window **Select Backup Device** area, choose the backup device from which to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

The backup filename indicates the date and time that the system created the backup file.

Choose only the backup file of the cluster from which you want to restore the entire cluster.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, select the features that you want to restore.

The screen displays only those features that were saved to the backup file.

**Step 7** Click **Next**.

**Step 8** In the **Restore Wizard Step 4** window, click **One-Step Restore**.

This option appears on **Restore Wizard Step 4** window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes. For more information, see Restore the First Node Only, on page 3 and Restore Subsequent Cluster Node, on page 5.

**Note**
If a status message indicates that *Publisher has failed to become cluster aware. Cannot start one-step restore*, you need to restore the publisher node and then the subscriber node. See the Related topics for more information.

This option allows the publisher to become cluster aware and will take five minutes to do so. Once you click on this option, a status message displays as “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period”.

After the delay, if the publisher becomes cluster aware, a status message displays as “Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster”.

After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 3 and Restore Subsequent Cluster Node, on page 5.

**Step 9** When you are prompted to choose the nodes to restore, choose all the nodes in the cluster.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

**Step 10** Click **Restore**.
Your data is restored on all the nodes of the cluster.

**Step 11** When the **Percentage Complete** field on the **Restore Status window** shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

### What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 11
- To restart a node, see Restart a Node, on page 10

# Restore Entire Cluster

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you have to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster.

If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform this procedure.

### Procedure

**Step 1** From Disaster Recovery System, select **Restore** > **Restore Wizard**.

**Step 2** In the **Select Backup Device** area, select the appropriate backup device to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file you want to restore.

**Note**
The backup filename indicates the date and time that the system created the backup file.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, click **Next**.

**Step 7** In the **Restore Wizard Step 4** window, select all the nodes when prompted to choose restore nodes.

**Step 8** Click **Restore** to restore the data.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database.

Data is restored on the all the nodes.

**Note**
During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

**Step 9** Restart the server once the restoration process is completed. See the What to Do Next section for more information about how to restart the server.

**Note**
Make sure that you restart the first node before you restart the subsequent nodes.

After the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

**Step 10** Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

**Note**
Database replication on the subsequent nodes may take enough time to complete after the subsequent node restarts, depending on the size of the cluster.

**Tip**
If replication does not set up properly, use the "utils dbreplication rebuild" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

### What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 11
- To restart a node, see Restart a Node, on page 10

# Restore Node Or Cluster to Last Known Good Configuration

Follow this procedure to restore node or cluster to last known good configuration.

### Before you begin

- Ensure that the restore file contains the hostname, IP address, DNS configuration, and deployment type that is configured in the backup file.
- Ensure that the Cisco Unified Communications Manager version installed on the server matches the version of the backup file that you want to restore.
- Ensure this procedure is used only to restore node to a last known good configuration.

### Procedure

**Step 1** From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

**Step 2** In the **Select Backup Device** area, select the appropriate backup device to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file you want to restore.

**Note**

The backup filename indicates the date and time that the system created the backup file.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, click **Next**.

**Step 7** Select the appropriate node, when prompted to choose restore nodes.
Data is restored on the chosen nodes.

**Step 8** Restart all nodes in the cluster. Restart the first Cisco Unified Communications Manager node before restarting the subsequent Cisco Unified Communications Manager nodes. If the cluster also has Cisco IM and Presence nodes, restart the first Cisco IM and Presence node before restarting the subsequent IM and Presence nodes. See the What to Do Next section for more information.

# Restart a Node

You must restart a node after you restore data.

If you are restoring a publisher node (first node), you must restart the publisher node first. Restart subscriber nodes only after the publisher node has restarted and is successfully running the restored version of the software.

**Note** Do not restart IM and Presence subscriber nodes if the CUCM publisher node is offline. In such cases, the node services will fail to start because the subscriber node is unable to connect to the CUCM publisher.

**Caution** This procedure causes the system to restart and become temporarily out of service.

Perform this procedure on every node in the cluster that you need to restart.

### Procedure

**Step 1** From Cisco Unified OS Administration, select **Settings** > **Version**.

**Step 2** To restart the node, click **Restart**.

**Step 3** Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the **utils dbreplication runtimestate** CLI command. The value on each node should be equal 2. See Cisco Unified Communications (CallManager) Command References for more information about CLI commands.

If replication does not set up properly, use the **utils dbreplication reset** CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*.

**Note**
Database replication on the subsequent nodes may take several hours to complete after the subsequent nodes restart, depending on the size of the cluster.

### What to do next

(Optional) To view the status of the restore, see Check Restore Job Status, on page 11.

## Check Restore Job Status

Follow this procedure to check the restore job status.

### Procedure

**Step 1** From the Disaster Recovery System, select **Restore** > **Current Status**.

**Step 2** In the **Restore Status** window, click the log filename link to view the restore status.

## View Restore History

Perform the following steps to view the restore history.

### Procedure

**Step 1** From Disaster Recovery System, choose **Restore** > **History**.

**Step 2** From the **Restore History** window, you can view the restores that you have performed, including filename, backup device, completion date, result, version, features that were restored, and failed features.

The **Restore History** window displays only the last 20 restore jobs.

# Data Authentication

## Trace Files

The following trace file locations are used during troubleshooting or while collecting the logs.

Trace files for the Master Agent, the GUI, each Local Agent, and the JSch library get written to the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drfMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the GUI, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platform/drf/trace/drfJSch*

For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

# Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in the following table. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide* for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

***Table 1: Disaster Recovery System Command Line Interface***

| Command | Description |
|---|---|
| utils disaster_recovery estimate_tar_size | Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list |
| utils disaster_recovery backup | Starts a manual backup by using the features that are configured in the Disaster Recovery System interface |
| utils disaster_recovery jschLogs | Enables or disables JSch library logging |
| utils disaster_recovery restore | Starts a restore and requires parameters for backup location, filename, features, and nodes to restore |
| utils disaster_recovery status | Displays the status of ongoing backup or restore job |
| utils disaster_recovery show_backupfiles | Displays existing backup files |
| utils disaster_recovery cancel_backup | Cancels an ongoing backup job |
| utils disaster_recovery show_registration | Displays the currently configured registration |
| utils disaster_recovery device add | Adds the network device |
| utils disaster_recovery device delete | Deletes the device |
| utils disaster_recovery device list | Lists all the devices |
| utils disaster_recovery schedule add | Adds a schedule |
| utils disaster_recovery schedule delete | Deletes a schedule |
| utils disaster_recovery schedule disable | Disables a schedule |

| Command | Description |
|---|---|
| utils disaster_recovery schedule enable | Enables a schedule |
| utils disaster_recovery schedule list | Lists all the schedules |
| utils disaster_recovery backup | Starts a manual backup by using the features that are configured in the Disaster Recovery System interface. |
| utils disaster_recovery restore | Starts a restore and requires parameters for backup location, filename, features, and nodes to restore. |
| utils disaster_recovery status | Displays the status of ongoing backup or restore job. |
| utils disaster_recovery show_backupfiles | Displays existing backup files. |
| utils disaster_recovery cancel_backup | Cancels an ongoing backup job. |
| utils disaster_recovery show_registration | Displays the currently configured registration. |

# Alarms and Messages

## Alarms and Messages

The Disaster Recovery System issues alarms for various errors that could occur during a backup or restore procedure. The following table provides a list of Cisco Disaster Recovery System alarms.

***Table 2: Disaster Recovery System Alarms and Messages***

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFBackupDeviceError | DRF backup process has problems accessing device. | DRS backup process encoun while it was accessing devic |
| DRFBackupFailure | Cisco DRF Backup process failed. | DRS backup process encoun |
| DRFBackupInProgress | New backup cannot start while another backup is still running | DRS cannot start new backup backup is still running. |
| DRFInternalProcessFailure | DRF internal process encountered an error. | DRS internal process encoun |
| DRFLA2MAFailure | DRF Local Agent cannot connect to Master Agent. | DRS Local Agent cannot con Agent. |
| DRFLocalAgentStartFailure | DRF Local Agent does not start. | DRS Local Agent might be |

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFMA2LAFailure | DRF Master Agent does not connect to Local Agent. | DRS Master Agent cannot conne Agent. |
| DRFMABackupComponentFailure | DRF cannot back up at least one component. | DRS requested a component to b data; however, an error occurred backup process, and the compone get backed up. |
| DRFMABackupNodeDisconnect | The node that is being backed up disconnected from the Master Agent prior to being fully backed up. | While the DRS Master Agent wa a backup operation on a Cisco U Communications Manager node, disconnected before the backup completed. |
| DRFMARestoreComponentFailure | DRF cannot restore at least one component. | DRS requested a component to r data; however, an error occurred restore process, and the compone get restored. |
| DRFMARestoreNodeDisconnect | The node that is being restored disconnected from the Master Agent prior to being fully restored. | While the DRS Master Agent wa a restore operation on a Cisco U Communications Manager node, disconnected before the restore o completed. |
| DRFMasterAgentStartFailure | DRF Master Agent did not start. | DRS Master Agent might be dow |
| DRFNoRegisteredComponent | No registered components are available, so backup failed. | DRS backup failed because no r components are available. |
| DRFNoRegisteredFeature | No feature got selected for backup. | No feature got selected for backu |
| DRFRestoreDeviceError | DRF restore process has problems accessing device. | DRS restore process cannot read device. |
| DRFRestoreFailure | DRF restore process failed. | DRS restore process encountered |
| DRFSftpFailure | DRF SFTP operation has errors. | Errors exist in DRS SFTP opera |
| DRFSecurityViolation | DRF system detected a malicious pattern that could result in a security violation. | The DRF Network Message con malicious pattern that could resu security violation like code injec directory traversal. DRF Networl has been blocked. |
| DRFTruststoreMissing | The IPsec truststore is missing on the node. | The IPsec truststore is missing or DRF Local Agent cannot connect Agent. |

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFUnknownClient | DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected. | The DRF Master Agent on the a Client connection request f unknown server outside the c request has been rejected. |
| DRFBackupCompleted | DRF backup completed successfully. | DRF backup completed succ |
| DRFRestoreCompleted | DRF restore completed successfully. | DRF restore completed succ |
| DRFNoBackupTaken | DRF did not find a valid backup of the current system. | DRF did not find a valid bac current system after an Upgra or Fresh Install. |
| DRFComponentRegistered | DRF successfully registered the requested component. | DRF successfully registered component. |
| DRFRegistrationFailure | DRF Registration operation failed. | DRF Registration operation component due to some inter |
| DRFComponentDeRegistered | DRF successfully deregistered the requested component. | DRF successfully deregistered component. |
| DRFDeRegistrationFailure | DRF deregistration request for a component failed. | DRF deregistration request fo failed. |
| DRFFailure | DRF Backup or Restore process has failed. | DRF Backup or Restore proc encountered errors. |
| DRFRestoreInternalError | DRF Restore operation has encountered an error. Restore cancelled internally. | DRF Restore operation has e error. Restore cancelled inter |
| DRFLogDirAccessFailure | DRF could not access the log directory. | DRF could not access the log |
| DRFDeRegisteredServer | DRF automatically de-registered all the components for the server. | The server may have been di from the Unified Communicat cluster. |
| DRFSchedulerDisabled | DRF Scheduler is disabled because no configured features are available for backup. | DRF Scheduler is disabled b configured features are availa |
| DRFSchedulerUpdated | DRF Scheduled backup configuration is updated automatically due to feature de-registration. | DRF Scheduled backup conf updated automatically due to de-registration |

# Restore Interactions and Restrictions

## Restore Restrictions

The following restrictions apply to using Disaster Recovery System to restore Cisco Unified Communications Manager or IM and Presence Service

***Table 3: Restore Restrictions***

| Restriction | Description |
|---|---|
| Export Restricted | You can restore the DRS backup from a restricted version only to a restricted version and the backup from an unrestricted version can be restored only to an unrestricted version. Note that if you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software |
| Platform Migrations | You cannot use the Disaster Recovery System to migrate data between platforms (for example, from Windows to Linux or from Linux to Windows). A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, see the *Data Migration Assistant User Guide*. |
| HW Replacement and Migrations | When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore.<br>For more information about replacing a server, refer to the *Replacing a Single Server or Cluster for Cisco Unified Communications Manager guide*.<br>In addition, you must run the Certificate Trust List (CTL) client after a hardware replacement. You must run the CTL client if you do not restore the subsequent node (subscriber) servers. In other cases, DRS backs up the certificates that you need. For more information, see the "Installing the CTL Client" and "Configuring the CTL Client " procedures in the *Cisco Unified Communications Manager Security Guide*. |
| Extension Mobility Cross Cluster | Extension Mobility Cross Cluster users who are logged in to a remote cluster at backup shall remain logged in after restore. |

**Note** DRS backup/restore is a high CPU-oriented process. Smart Licence Manager is one of the components that are backed-up and restored. During this process Smart License Manger service is restarted. You can expect high resource utilization so recommended to schedule the process during maintenance period.

After successfully restoring the Cisco Unified Communications server components, register the Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. If the product is already registered before taking the backup, then reregister the product for updating the license information.

For more information on how to register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite, see the *System Configuration Guide for Cisco Unified Communications Manager* for your release.

# Troubleshooting

## DRS Restore to Smaller Virtual Machine Fails

### Problem

A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

### Cause

This failure occurs when you migrate from a larger disk size to a smaller disk size.

### Solution

Deploy a VM for the restore from an OVA template that has 2 virtual disks.