Disaster Recovery System Administration Guide for Cisco Unity Connection Release 10.x

Published November, 2013

This guide provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup-related tasks and restore-related tasks. This guide serves as a reference and procedural guide that is intended for users of Cisco Unified Communications Manager and other Cisco IP telephony applications.

This document includes the following topics:

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

What is the Disaster Recovery System?

The Disaster Recovery System (DRS), which can be invoked from, Cisco Unity Connection Administration provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

Caution Before you restore, ensure that the version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1.(2).1000-1 to version 6.1(2).1000-2

Caution Before you restore or Cisco Unity Connection, ensure that the hostname, IP address, version, and deployment type of the restore matches the hostname, IP address, version, and deployment type of the backup file that you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a physical tape drive or remote SFTP server.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with Local Agents.

Caution DRS encryption depends on the cluster security password. If you change this security password through the Command Line Interface or a fresh install, then it is recommended that you take a fresh backup immediately or remember the old security password.

Note When a Cisco Unity Connection cluster is configured, The Disaster Recovery System uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber servers. DRS makes use of the IPSec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore (hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, then you must ensure that you upload the IPSEC certificate to the IPSEC-trust.

Caution Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Task Lists for Backing Up and Restoring Cisco Unity Connection

The following tables list the tasks for backing up and restoring the Cisco Unity Connection.

Note DRS backs up and restores the backup device settings and backup schedule settings, so you do not need to reconfigure DRS settings after a restore.

Task List for Backing Up Cisco Unity Connection

Table 1 provides a task list for backing up Cisco Unity Connection by using the Disaster Recovery System.

Table 1 Task List for Backing Up Cisco Unity Connection

Action	Reference
Create backup devices on which to back up data.	"Managing Backup Devices" section on page 5
Create and edit backup schedules to back up data on a schedule.	"Creating and Editing Backup Schedules" section on page 7
Enable and disable backup schedules to back up data.	"Enabling, Disabling, and Deleting Schedules" section on page 9
Optionally, run a manual backup.	"Starting a Manual Backup" section on page 9
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	"Checking Backup Status" section on page 10

Task List for Restoring Cisco Unity Connection

Table 2 provides a task list for restoring Cisco Unity Connection by using the Disaster Recovery System.

Table 2 Task List for Restoring Cisco Unity Connection

Action	Reference
Choose the storage location, backup file, features, and nodes.	"Restoring or Replacing Cisco Unity Connection Servers" section on page 11
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	"Viewing the Restore Status" section on page 14

System Requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured. Cisco allows you to use any SFTP server product, but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with the specified version of .

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Cisco does not support using the SFTP product FreeFTPd. This is because of the 1 GB file size limit of this SFTP product.

Note For issues with third-party products, contact the corresponding vendor for support

Note While a backup or restore is running, you cannot perform any OS Administration tasks because Disaster Recovery System blocks all OS Administration requests by locking the platform API. However, this does not block most CLI commands as only the CLI-based upgrade commands use the Platform API locking package.

Tip Schedule backups during periods when you expect less network traffic.

Note Be aware that if you migrate to an HP DL380-G6 server (software-only), you will not be able to install older versions of Cisco Unified Communications Manager (5.x and 6.x) on the new server. Therefore, to be able to run a DRS backup, you must install the older version of Cisco Unified Communications Manager on your old publisher (which may no longer be supported). Once this backup has been completed, you will be able to restore it on your HP DL380-G6 (software-only) publisher.

How to Access the Disaster Recovery System

To access the Disaster Recovery System, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unity Connection Administration window. Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Note You set the Administrator username and password during Cisco Unity Connection installation, and you can change the Administrator password or set up a new Administrator account by using the Command Line Interface (CLI). Refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* for more information.

Master Agent Duties and Activation

The system automatically activates the Master Agent (MA) on the server.

The Master Agent (MA) performs the following duties:

- The MA stores systemwide component registration information.
- The MA maintains a complete set of scheduled tasks in an XML file. The MA updates this file when it receives updates of schedules from the user interface. The MA sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the MA through the Disaster Recovery System user interface to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying the status of executing schedules, and performing system restoration.
- The MA stores backup data to a locally attached tape drive or a remote network location.

Local Agents

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

The Local Agent runs backup and restore scripts on the server.

Note When a Cisco Unity Connection cluster is configured, the Disaster Recovery System uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber servers. DRS makes use of the IPSec certificates for its Public/Private Key encryption. This certificate exchange gets handled internally; you do not need to make any configuration changes to accommodate this exchange.

Managing Backup Devices

Before using the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

Note You can add, delete, and list devices through the Command Line Interface. For more information on CLI commands for DRS, refer to the "Command Line Interface" section on page 17.

Procedure

Step 1 In case of Unity Connection, log in to the Cisco Unity Connection Administration, select **Disaster Recovery System** from the Navigation window, and click **Go**.

Note When a Cisco Unity Connection cluster is configured, we recommend that you back up the publisher server and, optionally, the subscriber server.

The Disaster Recovery System Logon window displays.

Step 2 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Backup Device**. The Backup Device List window displays.

Step 4 To configure a new backup device, click **Add New**.

Step 5 To edit a backup device, select it in the Backup Device list. Then, click **Edit Selected**.

The Backup Device window displays.

Step 6 Enter the backup device name in the **Backup device name** field.

Note The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-) and underscores (_). Do not use any other characters.

Step 7 Choose one of the following backup devices and enter the appropriate field values in the Select Destination area:

- **Tape Device**—Stores the backup file on a locally attached tape drive. Choose the appropriate tape device from the list. Note the following considerations:
  - You cannot use more than one tape for a single backup. If you have more data than will fit on a tape, either you must store backups on a network directory, or you must back up components on one tape and backup mailbox stores on one or more additional tape.
  - You cannot store more than one backup on a tape; each backup overwrites the data from the previous backup, so you only have the data from the most recent backup. If you want to create more than one backup for a server (components in one backup, mailbox stores in another backup, for example), you must use separate tapes. Otherwise, you will only have the portion of the data that you backed up last.

  Note Be aware that if you are logged in through a VMware virtual machine, you cannot back up on a tape. This is because the tape device option is disabled for VMware users.

- **Network Directory**—Stores the backup file on a network drive that is accessed through an SFTP connection. Enter the following required information:
  - **Server name**: Name or IP address of the network server
  - **Path name**: Path name for the directory where you want to store the backup file
  - **User name**: Valid username for an account on the remote system
  - **Password**: Valid password for the account on the remote system
  - **Number of backups to store on Network Directory**: The number of backups to store on this network directory.

    If you are backing up more than one Unity Connection server, we recommend that you create a separate directory on the network drive for each Connection server. In addition, if you are using DRS to back up other applications (Cisco Unified Communications Manager, Cisco Unified Presence), we recommend that you create a separate directory for each of the other servers. The value that you specify here applies to all of the backups in the directory, not just the backups for one server. For example, suppose you want to retain three backups for a Unity Connection server and three backups for a Cisco Unified Communications Manager server. If you specify the same network directory for both servers, and if you specify three as the number of backups

to store in the directory on both servers, only the most recent three backups will appear in the directory. If the last three backups were of the Unity Connection server, you will not have any Cisco Unified Communications Manager backups at all.

Specify a value high enough to ensure that the backups you want to keep are not overwritten. For example, if you configure DRS so a full backup of a Connection server requires three separate backups (components, MailboxStore1, and MailboxStore2) and if you want to retain the two most recent full backups, choose 6 here. Choosing a lower number will cause the Disaster Recovery System to overwrite backups that you want to retain.

The location you specified in the Path Name field must have enough space for the number of backups you specify here plus one. When the network drive contains the maximum number of backups that you want to store, DRS saves the newest backup to that location before deleting the oldest backup.

Note You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

Step 8 To update these settings, click **Save**.

Note After you click the **Save** button, the DRS Master Agent validates the selected backup device. If the user name, password, server name, or directory path is invalid, the save will fail.

Step 9 To delete a backup device, select it in the Backup Device list. Then, click **Delete Selected**.

Note You cannot delete a backup device that is configured as the backup device in a backup schedule.

Creating and Editing Backup Schedules

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Note You can list and add backup schedules through the Command Line Interface. For more information on CLI commands for DRS, refer to the "Command Line Interface" section on page 17.

Note Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change/reset.

Perform the following steps to manage backup schedules:

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Scheduler**.

The Schedule List window displays.

Step 4 Do one of the following steps to add a new schedule or edit an existing schedule

a. To create a new schedule, click **Add New**.

b. To configure an existing schedule, click its name in the **Schedule List** column.

The scheduler window displays.

Step 5 Enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 6 Select the backup device in the **Select Backup Device** area.

Step 7 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Always choose to back up the following features:

- Recorded greetings and voice names (CONNECTION_GREETINGS_VOICENAMES).
- The database (CONNECTION_DATABASE).
- Other Connection-specific data (CUC).

Backing up messages (CONNECTION_MESSAGES_<database name>) is optional.

Step 8 Choose the date and time when you want the backup to begin in the **Start Backup at** area. Note the following:

- Schedule backups during off-peak hours to avoid affecting system performance.
- Do not schedule a backup to run while the Update Database Statistics task is running. By default, this task runs daily at 3:30 am.

Step 9 Choose the frequency at which you want the backup to occur in the **Frequency** area: Once, Daily, Weekly, or Monthly. If you choose Weekly, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to Weekly, occurring Tuesday through Saturday, click **Set Default**.

Step 10 To update these settings, click **Save**.

Step 11 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Step 12 To disable the schedule, click **Disable Schedule**.

Enabling, Disabling, and Deleting Schedules

Procedure

Note You can enable, disable, and delete backup schedules through the Command Line Interface. For more information on CLI commands for DRS, refer to the "Command Line Interface" section on page 17.

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Scheduler**.

The Schedule List window displays.

Step 4 Check the check boxes next to the schedules that you want to modify.

- To select all schedules, click **Select All**.
- To clear all check boxes, click **Clear All**.

Step 5 To enable the selected schedules, click **Enable Selected Schedules**.

Step 6 To disable the selected schedules, click **Disable Selected Schedules**.

Step 7 To delete the selected schedules, click **Delete Selected**.

Starting a Manual Backup

Follow this procedure to start a manual backup.

Note Be aware that your backup .tar files are encrypted with a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change/reset.

Procedure

Step 8 In case of Unity Connection, log in to the Cisco Unity Connection Administration, select **Disaster Recovery System** from the Navigation window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 9 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 10 Navigate to **Backup > Manual Backup**. The Manual Backup window displays.

Step 11 Select a backup device in the **Select Backup Device** area.

Step 12 Select the features to back up in the **Select Features** area.

Always choose to back up the following features:

- Recorded greetings and voice names (CONNECTION_GREETINGS_VOICENAMES).
- The database (CONNECTION_DATABASE).
- Other Unity Connection-specific data (CUC).

Backing up messages (CONNECTION_MESSAGES_<database name>) is optional.

Step 13 To start the manual backup, click **Start Backup**.

Checking Backup Status

You can check the status of the current backup job and cancel the current backup job. To view the backup history, see the "Viewing the Backup and Restore History" section on page 14.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Checking the Status of the Current Backup Job

Perform the following steps to check the status of the current backup job.

Procedure

Step 14 In case of Unity Connection, log in tothe Cisco Unity Connection Administration, select **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 15 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 16 Navigate to **Backup > Current Status**. The Backup Status window displays.

Step 17 To view the backup log file, click the log filename link.

Step 18 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

How a Restore Affects Cisco Unity Connection Voice Messages

If you back up Unity Connection, create one or more new mailbox stores, and then restore without backing up the new mailbox stores, the new mailbox stores are deleted.

If you back up and restore only the Unity Connection directory, without also backing up and restoring Unity Connection voice messages, some user folders may be deleted, depending on whether the associated features are in use for those users:

- The drafts folder is created the first time a user saves a draft message after the feature is configured. (You must either configure Unity Connection to automatically save draft messages when users are disconnected or hang up, or configure Connection to allow users to save draft messages.)
- The future delivery folder is created the first time a user marks a message for future delivery. (Future delivery is not configurable.)
- The sent items folder, which allows users to recall messages they have already sent, is created the first time a user sends a voice message after the message recall is configured. (In Cisco Unity Connection Administration, you must change the value of the Sent Messages: Retention Period (in Days) setting on the System Settings > Advanced > Messaging page to a value greater than zero.)

If the folders contain any messages, the messages are moved to the undeliverable messages folder.

Restoring or Replacing Cisco Unity Connection Servers

If you are restoring Cisco Unity Connection data on an existing server or on both servers in a Cisco Unity Connection cluster, do the procedure in this section.

If you are replacing a Cisco Unity Connection server or replacing the hard disks in a Unity Connection server, including one or both servers in a Cisco Unity Connection cluster, start with the applicable task list in the "Replacing Cisco Unity Connection 10.x Servers or Hard Disks" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html. Each task list will redirect you to the procedure in this section to restore data.

Note Cisco Unity Connection does not support restoring or replacing clone cluster. Also, pre-configured backup devices must be created before restoring Unity Connection servers.

Procedure

Step 1 If you reinstalled software on the server or on a Cisco Unity Connection cluster, do the following steps, as applicable:

a. Confirm that the IP address and host name of the server match the IP address and host name when the server was backed up. Otherwise, the restore will fail.

In addition, when Cisco Unity Connection is running on a virtual machine, confirm that the following settings match the values when the server was backed up. The settings are used to create the license MAC value of the Connection virtual machine, and if you change any of them, you must get new license files for the virtual machine.

- Time zone
- NTP server
- NIC speed and duplex settings
- DHCP settings
- Primary DNS settings
- SMTP hostname

- X.509 Certificate information (Organization, Unit, Location, State, and Country)

b. Confirm that the Cisco Unity Connection version that is installed on the server exactly matches the Connection version that was installed when you made the backup.

For example, the Disaster Recovery System does not allow a restore from version 8.5(**1**).1000-1 to version 8.5(**2**).1000-1, or from version 8.5(2).1000-**1** to version 8.5(2).1000-**2**. (The last parts of the version number change when you install a service release or an engineering special.)

c. Confirm that you have the security password that was in effect when the Cisco Unity Connection server was backed up.

DRS encrypts backed-up data by using the security password as the encryption key. If you changed the security password after the last backup, DRS will ask for the old security password.

d. Reinstall the licenses that were originally installed on the server.

e. If any Unity Connection languages were previously installed, reinstall the same languages.

Step 2 On the Cisco Unity Connection server, sign in to Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 4 Choose the backup device from which to restore in the **Select Backup Device** area. Then, click **Next**.

The Restore Wizard Step 2 window displays.

Step 5 Choose the backup file that you want to restore.

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

Step 6 Click **Next**. The Restore Wizard Step 3 window displays.

Step 7 Always choose to restore the following features:

- Recorded greetings and voice names (CONNECTION_GREETINGS_VOICENAMES).
- The database (CONNECTION_DATABASE): Restoring messages (CONNECTION_MESSAGES_<database name>) is optional.
- Other Unity Connection-specific data (CUC).

Note The only features listed are the features that were included in the backup.

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

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

Note The file integrity check is optional and is only required in the case of SFTP backups. You do not need to run a file integrity check when restoring from tape and local device backups.

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

Step 10 When you are prompted to choose the node to restore, choose the same features that you selected in Step 7, and click **Next**.

Caution Existing data for the selected features is overwritten.

Step 11 To start restoring the data, click **Restore**.

Note If you selected the **Perform file integrity check using SHA1 Message Digest** checkbox in Step 7, DRS runs a file integrity check on each file when you click **Restore**. If the system finds discrepancies in any .tar file during the check, the restore process generate ERROR out for the component that failed the integrity check and move to restore the next .tar file (that is, the next component).

Step 12 To view the status of the restore, see the "Viewing the Restore Status" section on page 14.

Step 13 Restart the server. For more information on restarting, see the "System Restart" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/os_administration/guide/10xcucosagx.html.

Step 14 If you are restoring a Unity Connection standalone server, skip to Step 15.

If you are restoring a Unity Connection cluster, force Unity Connection to copy the data from the publisher to the subscriber server:

a. After the publisher server has finished restarting, log on to the command line interface for the subscriber server.

b. On the command line, run the following command to force Unity Connection to copy data from the publisher server to the subscriber server:

```
utils cuc cluster overwritedb
```

c. Check the status of the Unity Connection cluster on the subscriber server. On the command line, run the following command:

```
show cuc cluster status
```

d. Log on to the command line interface for the publisher server.

e. Check the status of the Unity Connection cluster on the publisher server. At the command line, run the following command:

```
show cuc cluster status
```

Step 15 During off-peak hours, re-synchronize message-waiting indicators for each phone system:

a. In Cisco Unity Connection Administration, expand Telephony Integrations, and click Phone System.

b. Click the name of the first phone system.

c. For Synchronize All MWIs on This Phone System, click Run.

d. Repeat Step a. through Step c. for the remaining phone systems.

Step 16 If you replace the servers with supported virtual machines, return to the applicable task list in the "Replacing Cisco Unity Connection 10.x Servers or Hard Disks" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html.

Viewing the Restore Status

To check the status of the current restore job, perform the following steps:

Procedure

Step 17 In case of Unity Connection, log in to the Cisco Unity Connection Administration, select **Disaster Recovery System** from the Navigation menu, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 18 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 19 Navigate to **Restore >Status**. The Restore Status window displays.

The Status column in the Restore Status window shows the status of the restoration in progress, including the percentage of completion of the restore procedure.

Step 20 To view the restore log file, click the log filename link.

Viewing the Backup and Restore History

Using the following procedures, you can see the last 20 backup and restore jobs:

- Backup History
- Restore History

Backup History

Perform the following steps to view the backup history.

Procedure

Step 21 In case of Unity Connection, log in to the Cisco Unity Connection Administration, select **Disaster Recovery System** from the Navigation menu, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 22 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 23 Navigate to **Backup > History**. The Backup History window displays.

Step 24 From the Backup History window, you can view the backups that you have performed, including file name, backup device, completion date, result, and features that are backed up.

Note The Backup History window displays only the last 20 backup jobs.

Restore History

Perform the following steps to view the restore history.

Procedure

Step 25 In case of Unity Connection, log in to the Cisco Unity Connection Administration, select **Disaster Recovery System** from the Navigation list, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 26 Log into the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 27 Navigate to **Restore > History**. The Restore History window displays.

Step 28 From the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

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

Backup and Restore in HTTPS Networking

In an HTTPS network, if the data rollback/restore is done on a particular Unity Connection location in the network, then the location first tries to update its network directory information from other locations and then provides the directory information feed to the other directly connected locations. This process helps in saving the time required to replicate the updated information in the entire network. For more information on HTTPS networking, refer to the *HTTPS Networking Guide Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/https_networking/guide/10xcuchttpsnetx.html.

After the restore/rollback is complete on a location in a network, the replication set of the location gets changed. If the replication set of a location gets changed, the Feeder on the location sends its directory information to the requesting location in the network only in either of the following situations:

- If the restored location has synchronized with all the directly connected locations after the replication set has changed irrespective of the status of synchronization whether successful or failed.
- If two hours have passed after the Feeder has detected the change in the replication set of the restored location.

After a location is restored and restarted, all the locations directly connected with the restored location may fail to synchronize with the restored location if both of the situations mentioned above have not occurred.

The restored location relies on the remote locations for the re-synchronization to occur. This means that the remote location first sends request to the Feeder of the restored location, the restored location then sends the changed the replication set to the remote location and when the remote location detects the change in the replication set of the restored location, it triggers resynchronization towards a restored location.

Consider the following requirements while taking the backup/restore of a location in an HTTPS network:

- Locations should not be added or removed from the network after taking the backup and before restoring a particular location.
- Restoring more than one location in a network simultaneously is not supported in HTTPS networking. Therefore, make sure that a location is completely restored and its data is replicated throughout the network before restoring another location in the network.

Managing DRS Backup Remotely

The Disaster Recovery System (DRS), which provides full data backup, can be invoked remotely by using the following URL:

https://<UC Application>/platform-services/services/< MaintenanceService>?wsdl

where --

- <UC Application> specifies the name of the Cisco Unity Connection server.
- <MaintenanceService> specifies the operations for DRS backup. The following are the supported values of the < MaintenanceService> parameter:
  - scheduleBackup - scheduleBackup service updates an already scheduled DRS backup, which is to be run at a specified time in the future.
  - startBackup - startBackup service starts a DRS backup instantly.
  - getBackupProgress - getBackupProgress service returns the current status of an on-going DRS backup.

Trace Files

In this release of the Disaster Recovery System, trace files for the Master Agent, the GUI, and each Local Agent 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**

You can view trace files by using the Command Line Interface. See the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* for more information.

Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in Table 3. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions.*

Table 3 Disaster Recovery System Command Line Interface

Command	Description
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, file name, 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 show_tapeid	Displays the tape identification information
utils disaster_recovery device add	Adds the network or tape 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
utils disaster_recovery schedule enable	Enables a schedule
utils disaster_recovery schedule list	Lists all the schedules

Alarms and Messages

The Disaster Recovery System (DRS) issues alarms and other messages for various errors and other conditions that occur during a backup or restore procedure. Table 4 provides a list of Cisco DRS alarms.

Table 4 Disaster Recovery System Alarms and Messages

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encountered errors while it was accessing device.
DRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encountered errors.
DRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup while another backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encountered an error.
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot connect to Master Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be down.
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot connect to Local Agent.
DRFMABackupComponent Failure	DRF cannot back up at least one component.	DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not 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 was running a backup operation on a Cisco Unity Connection node, the node disconnected before the backup operation completed.
DRFMARestoreComponent Failure	DRF cannot restore at least one component.	DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation on a Cisco Unity Connection node, the node disconnected before the restore operation completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be down.
DRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no registered components are available.
DRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backup.
DRFRestoreDeviceError	DRF restore process has problems accessing device.	The DRS restore process cannot read from device.
DRFRestoreFailure	DRF restore process failed.	DRS restore process encountered errors.
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP operation.

Table 4 Disaster Recovery System Alarms and Messages (continued)

Alarm Name	Description	Explanation
DRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message contains a malicious pattern that could result in a security violation like code injection or directory traversal. The DRF Network Message has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing on the node. The DRF Local Agent cannot connect to Master Agent.
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 Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.
DRFLocalDeviceError	DRF is unable to access local device.	DRF is unable to access local device.
DRFBackupCompleted	DRF backup completed successfully.	DRF backup completed successfully.
DRFRestoreCompleted	DRF restore completed successfully.	DRF restore completed successfully.
DRFNoBackupTaken	DRF did not find a valid backup of the current system.	DRF did not find a valid backup of the current system after an Upgrade/Migration or Fresh Install.

Related Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 10.x*. The document is shipped with Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/roadmap/10xcucdg.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors

and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.
