CHAPTER 4

Backup and Restore for Cisco HCM-F

The Disaster Recovery System (DRS), which you invoke from the command line interface (CLI) on the Cisco HCM-F platform, provides data backup and restore capabilities for the Cisco HCM-F. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups. The Disaster Recovery System includes the following capabilities:

- A command line interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.

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.

This chapter contains information on the following topics:

Backed Up and Restored Data for Cisco HCM-F

The Disaster Recovery System backs up and restores all configuration for Cisco HCM-F and all data that is stored in the Shared Data Repository. In addition, DRS restores its own settings (backup device settings and schedule settings) as part of the backup/restore process. 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 the DRS backup device and schedule.

Quick-Reference Tables for Backup and Restore Procedures

The following tables provide a quick reference for the backup and restore procedures.

Note DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. These backup device settings and schedule settings get restored as a part of the restore process. After the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

Backup Quick Reference

Table 1 provides a quick, high-level reference to the major steps, in chronological order, for backups through the Disaster Recovery System.

Table 1 Major Steps for Performing a Backup Procedure

Action	Reference
Create backup devices on which to back up data.	Managing Backup Devices, page 4-4
Create backup schedules to back up data on a schedule.	Creating Backup Schedules, page 4-6
Enable and disable backup schedules to back up data.	Enabling, Disabling, and Deleting Schedules, page 4-6
Optionally, run a manual backup.	Starting a Manual Backup, page 4-7
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	Checking Backup Status, page 4-7

Restore Quick Reference

Table 2 provides a quick, high-level reference to the major steps, in chronological order, for restores through the Disaster Recovery System.

Table 2 Major Steps for Performing a Restore Procedure

Action	Reference
Restore a backup file from a local or network directory.	Restoring Cisco HCM-F, page 4-8
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, page 4-10

System Requirements

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

Note While a backup or restore is running, the command line interface may block you from running some commands, including commands that support upgrades.

Archive backups to a local drive or remote SFTP server. The Disaster Recovery System does not support tape drives for backup and restore on the Cisco HCM-F platform. You must choose a local device if you do not have outgoing SFTP access to the Cisco HCM-F platform. If you store backup files to a local device, DRS stores the backup files in the /common/adminsftp/backup directory. You must manually move local backup files from the Cisco HCM-F platform by opening an SFTP client and connecting to the Cisco HCM-F platform by using the adminsftp user and the administrator password that you set up during installation.

To back up data to a remote device on the network or to move a local backup to another location, 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 specified versions. For information on which vendors have certified their products with your version, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

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/)

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

How to Access the Disaster Recovery System

To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform. To log in to the CLI, you must enter the administrator username and password (from the Cisco HCM-F installation, unless you changed it after installation).

Master Agent Duties and Activation

The system automatically activates the Master Agent on the Cisco HCM-F platform. The Master Agent performs the following duties:

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

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 create local or network backup devices. If you create a local backup device, Disaster Recovery System stores the backup files in the a preconfigured directory on the Cisco HCM-F platform. You must manually move local backup files from the Cisco HCM-F platform by opening an SFTP client and connecting to the Cisco HCM-F platform by using the adminsftp user and the administrator password that you set up during Cisco HCM-F installation.

Note The system automatically deletes local backup files that are more than one week old. When you perform a backup. a warning message displays that indicates that local backup files get deleted after one week.

You can estimate the size of the .tar file that the backup creates by entering **utils disaster_recovery estimate_tar_size**.

You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 To create a local device, enter **utils disaster_recovery device local** ***device_name number of backups***

where

device_name equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters. By default, DRS stores backup files for local devices in the /common/adminsftp/backup directory.

number of backups equals the number of backups that are retained for the backup server. When the backup reaches the limit, the oldest backup files on the backup server are deleted and the new backup files are added.

Step 3 To create a network device so that you can store backup files on a network drive that is accessed through an SFTP connection, enter **utils disaster_recovery device add network** ***device_name path server_name username number_of_backups***

where

device_name equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters.

path equals the path name for the directory where you want to store the backup file

server_name equals the name or IP address of the network server

username equals a valid username for an account on the remote system

number of backups equals the number of backups allowed for this device

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.

Note The DRS Master Agent validates the selected backup device. If the username, password, server name, or directory path is invalid, the command fails.

Step 4 To display a list of backup devices, enter **utils disaster_recovery** ***device list***.

The device name, device type, and device path for each backup device displays.

Step 5 To delete a backup device, enter **utils disaster_recovery device delete** ***device_name***, where *device_name* equals the name of the device that you want to delete.

Note You cannot delete a backup device that is configured as the backup device in a backup schedule. You must first delete the schedule which uses this device name, and then delete this device.

Creating 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.

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

To view a history of backups, enter **utils disaster_recovery history Backup**. The results of all backups display.

Perform the following steps to create backup schedules:

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery schedule add** ***schedulename devicename featurelist datetime frequency***

where

schedulename equals the name of the schedule

devicename equals the location where Disaster Recovery System stores the backup files

featurelist equals HCS

datetime specifies the time and date when Disaster Recovery System performs the backup. The format is *yyyy/mm/dd-hh:mm*. Enter the time based on a 24-hour clock.

frequency equals how often Disaster Recovery System performs the backup. Options are once, daily, weekly, and monthly.

Step 3 To enable a schedule, enter **utils disaster_recovery schedule enable** ***schedulename***.

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

Note To disable or delete schedules, see the "Enabling, Disabling, and Deleting Schedules" section on page 4-6.

Enabling, Disabling, and Deleting Schedules

Follow this procedure to enable, disable, or delete backup schedules.

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 To view the list of backup schedules, enter **utils disaster_recovery schedule list**.

The CLI displays the device name and status for each schedule. The device name specifies where Disaster Recovery System stores the backup files.

Step 3 Perform one of the following tasks:

- To enable a schedule, enter **utils disaster_recovery schedule enable** ***schedulename***.
- To disable a schedule, enter **utils disaster_recovery schedule disable** ***schedulename***.
- To delete a schedule, enter **utils disaster_recovery schedule delete** ***schedulename***.

The schedules can be enabled, disabled, or deleted only one at a time.

Starting a Manual Backup

Follow this procedure to start a manual backup.

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery backup** ***type featurelist device_name***

where

type equals the location of the backup, either local or network

featurelist equals HCS

device_name equals the name of the backup device

Step 3 To view the status of the current backup, enter **utils disaster_recovery status backup**.

Step 4 To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

Checking Backup Status

You can check the status of the current backup job and cancel the current backup job. Perform the following steps to check the status of the current backup job:

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

Successful backups display a status of successful. To view a history of backups, enter **utils disaster_recovery history Backup**. The results of all backups display.

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 To view the status of the current backup, enter **utils disaster_recovery status backup**.

Step 3 To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

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

Displaying Backup Files

Using the following procedures, you can see the list of backup files that are stored to the local or network drives:

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 To view backup files, do one of the following:

- To view the list of backup files in the local directory (/common/adminsftp/backup), enter **utils disaster_recovery show_backupfiles local backup**.
- To view the list of backup files in the local restore directory (/common/adminsftp/restore), enter **utils disaster_recovery show_backupfiles local restore**.
- To view the list of backup files on a network drive, enter **utils disaster_recovery show_backupfiles network *path servername userid***.

where

path equals the path name for the directory where the backup file is stored

servername equals the name or IP address of the network server

userid equals a valid user ID for an account on the remote system

Restoring Cisco HCM-F

You can restore the data for Cisco HCM-F from a backup file in a network directory or in a local directory. Use one of the following procedures to restore the data for Cisco HCM-F:

Caution Before you restore Cisco HCM-F platform, ensure that the Cisco HCM-F version that is installed on the platform matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco HCM-F for restore. For example, the Disaster Recovery System does not allow a restore from Version 8.6(**2**)ES1.1000-1 to Version 8.6(**2**)ES1.1000-2. Essentially, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco HCM-F.

Caution After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

Procedure 1: Restoring from a Local Directory

Step 1 Copy the backup file to the Cisco HCM-F platform by opening an SFTP client, and connecting to the Cisco HCM-F platform by using the adminsftp user and the administrator password that you set up during installation. To do that, navigate to the backup directory by entering **cd backup**, and copy the backup file to the /common/adminsftp/restore directory.

Step 2 Access the Disaster Recovery System by starting an SSH session and logging in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 3 Enter **utils disaster_recovery restore local** ***restore_server tarfilename device_name***

where

restore_server equals the hostname of the server to be restored

tarfilename equals the name of the backup file to be restored without extension; for example, 2008-01-21-18-25-03

device_name equals the name of the backup device

Step 4 Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**.

Step 5 Restart the Cisco HCM-F platform.

Procedure2: Restoring from a Network Directory

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery restore network** ***restore_server tarfilename device_name***

where

restore_server equals the hostname of the server to be restored

tarfilename equals the name of the file to be restored without extension (for example, 2008-01-21-18-25-03)

device_name equals the name of the backup device

Caution After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

Step 3 Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**.

Step 4 Restart the Cisco HCM-F platform.

Viewing the Restore Status

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

Procedure

Step 1 To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.

The CLI admin prompt displays.

Step 2 To view information about the current restore job, enter **utils disaster_recovery status restore**. The status shows the restore percentage, log file location, timestamp, feature name, platform name, component name, and component status.

Error Messages

The Disaster Recovery System (DRS) issues alarms for various errors that can occur during a backup or restore procedure. Table 3 provides a list of Cisco DRS alarms.

Table 3 Disaster Recovery System Alarms

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 may be down.

Table 3 Disaster Recovery System Alarms (continued)

Alarm Name	Description	Explanation
DRFLocalDeviceError	DRF has problems accessing local device.	DRS encountered errors while it was accessing local device.
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, the Cisco HCM-F platform 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 the Cisco HCM-F platform, the platform disconnected before the restore operation completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent may 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.	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.
DRFSecurityViolation	DRF system detected a malicious pattern that can result in a security violation.	The DRF Network Message contains a malicious pattern that can result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.
DRFTruststoreMissing	The IPsec trust store is missing on the node.	The IPsec trust store is missing on the node. DRF Local Agent cannot connect to Master Agent.
DRFUnknownClient	DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected.	The DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected.