Disaster Recovery System Administration Guide for Cisco Unified Communications Manager Release 8.6(1)

May 24, 2011

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:

- What is the Disaster Recovery System?, page 2
- Quick-Reference Tables for Backup and Restore Procedures, page 3
- Supported Features and Components, page 5
- System Requirements, page 5
- How to Access the Disaster Recovery System, page 6
- Master Agent Duties and Activation, page 6
- Local Agents, page 7
- Managing Backup Devices, page 7
- Creating and Editing Backup Schedules, page 9
- Enabling, Disabling, and Deleting Schedules, page 10
- Starting a Manual Backup, page 11
- Checking Backup Status, page 11
- Restore Scenarios, page 12
- Viewing the Restore Status, page 21
- Viewing the Backup and Restore History, page 21
- Trace Files, page 22
- Command Line Interface, page 23

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

- Alarms and Messages, page 24
- Related Documentation, page 26
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 26

What is the Disaster Recovery System?

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device.

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 Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager 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 of Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, 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.

When performing a system data restoration, you can choose which nodes in the cluster 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.

The system automatically activates both the Master Agent and the Local Agent on all nodes in the cluster.

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 The Disaster Recovery Systemuses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. 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. For more details, refer to the certificate management help pages in the *Cisco Unified Communications Manager Security Guide*s.

Note The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. 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, refer to the *Data Migration Assistant User Guide*.

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

Caution When you restore your data, the hostname, server IP address, and the deployment type must be the same as it was during the backup. DRS does not restore across different hostnames, IP addresses and deployment types.

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 platform backup/restore. 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, that you must perform to do a backup procedure by using 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" section on page 7
Create and edit backup schedules to back up data on a schedule. **Note** Either a manual or a scheduled backup backs up the whole cluster.	"Creating and Editing Backup Schedules" section on page 9

Table 1 Major Steps for Performing a Backup Procedure (continued)

Action	Reference
Enable and disable backup schedules to back up data.	"Enabling, Disabling, and Deleting Schedules" section on page 10
Optionally, run a manual backup.	"Starting a Manual Backup" section on page 11
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 11

Restore Quick Reference

Table 2 provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a restore procedure by using the Disaster Recovery System.

Note The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. 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, refer to the *Data Migration Assistant User Guide* before following the steps in Table 1.

Table 2 Major Steps for Performing a Restore Procedure

Action	Reference
Choose Storage Location—You must first choose the storage location from which you want to restore a backup file.	"Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)" section on page 13
Choose the Backup File—From a list of available files, choose the backup file that you want to restore.	"Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)" section on page 13
Choose Features—From the list of available features, choose the features that you want to restore.	"Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)" section on page 13
Choose Nodes—If the feature was backed up from multiple nodes, you must choose the nodes that you want to restore.	"Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)" section on page 13
Choose Data Source—When you restore a first node (publisher), restore Cisco Unified Communications Manager data from a good subsequent node (subscriber) to ensure that you are using current data.	"Restoring the First Node only (Rebuilding the Publisher Alone)" section on page 15
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 21

Supported Features and Components

Disaster Recovery System can back up and restore the following components. The system backs up all of its components automatically.

- Cisco Unified Communications Manager database (CCMDB), includes Cisco Unified Communications Manager/CDR Analysis and Reporting/Call Detail Records)
- Platform
- Music On Hold (MOH) Audio Files
- BAT Bulk Provisioning Service (BPS)
- CCM Preference Files (CCMPREFS)
- TFTP Phone device files (TFTP)
- SNMP Syslog Component (SYSLOGAGT SNMP)
- SNMP CDP Subagent (CDPAGT SNMP)
- Trace Collection Tool (TCT)
- Cluster Manager (CLM)
- Cisco Extended Functions (CEF)

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 specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, 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/)

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

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party 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 Unified Communications Manager 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 Unified Communications Manager 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 first node.

The system automatically starts the Master Agent service on the first node of the cluster and it is functional only on the first node. The Master Agents on the subsequent nodes are never activated and do not perform any function.

Duties That the Master Agent Performs

The Master Agent (MA) performs the following duties:

- The MA stores system-wide 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 status of executed schedules, and performing system restoration.
- The MA stores backup data on a locally attached tape drive or a remote network location.

Local Agents

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

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

Note By default, a Local Agent automatically gets activated on each node of the cluster.

Duties That Local Agents Perform

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

In a cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

Note The Disaster Recovery Systemuses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. 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 23.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

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 Be aware that you cannot span tapes or store more than one backup per tape.

  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. DRS only supports SFTP servers that are configured with an IPv4 address or hostname/Fully Qualified Domain Name (FQDN). 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.

  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 23.

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.

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

Perform the following steps to manage backup schedules:

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

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.

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

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.

Note Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

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 23.

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

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 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.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Navigate to **Backup > Manual Backup**. The Manual Backup window displays.

Step 4 Select a backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area.

Step 6 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 21.

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 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Navigate to **Backup > Current Status**. The Backup Status window displays.

Step 4 To view the backup log file, click the log filename link.

Step 5 To cancel the current backup, click **Cancel Backup**.

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

Restore Scenarios

Caution Be aware that DRS encryption depends on the cluster security password. If you have changed the security password between the backup and this restore, DRS will ask for the old security password. Therefore, to use such old backups, you must remember the old security password or take a backup immediately after the security password change/reset.

Caution Do not make any configuration changes to Cisco Unified Communications Manager during a restore. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option windows.

Do not perform any configuration tasks until the restore completes on all servers in the cluster, and until you have verified that database replication is functioning.

Note When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and host name that the old server used.

For more information about replacing a server, refer to the *Replacing a Single Server or Cluster for Cisco Unified Communications Manager* guide.

Tip Beginning with Cisco Unified Communications Manager Release 8.0(1), there is only one upgrade scenario in which 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*.

Note Restoring subscribers in a cluster is important, as many components (for example, SERVM and TCT) do not get configuration data from the database.

You can restore Cisco Unified Communications Manager in the following scenarios:

- Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild), page 13
- Restoring the First Node only (Rebuilding the Publisher Alone), page 15
- Restoring the Entire Cluster, page 17
- Restoring Subsequent Cluster Nodes (With or Without Rebuild), page 19

Note At the final stage of a restore operation, DRS sends a registration request for all successfully restored components. Therefore, after the completion of the restore operation, all successfully restored components are registered to DRS.

Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)

Note Use this procedure only if you are restoring the node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure. If you intend to rebuild the publisher server, read the "Restoring the First Node only (Rebuilding the Publisher Alone)" section on page 15. If you intend to rebuild the entire cluster, read the "Restoring the Entire Cluster" section on page 17.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager 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 of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 7.0(**1**).1000-1 to version 7.1(**2**).1000-1, or from version 7.1(2).1000-**1** to version 7.1(2).1000-**2**. (The last parts of the version number change when you install a service release or an engineering special.) In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unified Communications Manager database restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore. DRS does not restore across different hostnames, IP addresses and deployment types.

The Restore Wizard walks you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

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 Choose the features that you want to restore.

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

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 get prompted to choose the node to restore, choose the appropriate node.

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 9, 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 will ERROR out the component that failed the integrity check and move to restore the next .tar file (that is, the next component).

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

Note If you choose the first node to restore the data, DRS automatically restores the Cisco Unified Communications Manager database on the subsequent nodes. Read "Restoring the First Node only (Rebuilding the Publisher Alone)" section on page 15 for more details.

Step 12 Your data gets restored on the node that you chose. To view the status of the restore, see the "Viewing the Restore Status" section on page 21.

Step 13 Restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

Note Cisco recommends that you do not restart the first node until the subsequent nodes are restored and restarted. See Steps 14 through 16 of the "Restoring Subsequent Cluster Nodes (With or Without Rebuild)" section on page 19 for details.

Note Even if you are restoring only to the first node, you must restart all nodes in the cluster. Make sure that you restart the subsequent nodes before you restart the first node.

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

Restoring the First Node only (Rebuilding the Publisher Alone)

Follow this procedure to restore the first node (publisher) server in the cluster.

Procedure

Note Cisco recommends that you perform a fresh installation of Cisco Unified Communications Manager on the first node. For more information on installing Cisco Unified Communications Manager, see *Installing Cisco Unified Communications Manager*.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager 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 of Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore. DRS does not restore across different hostnames, IP addresses and deployment types.

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Configure the backup device. For more information, see Managing Backup Devices, page 7.

Step 4 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 5 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 6 Click **Next**. The Restore Wizard Step 2 window displays.

Step 7 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 8 Click **Next**. The Restore Wizard Step 3 window displays.

Step 9 Choose the features that you want to restore.

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

Step 10 Click **Next**. The Restore Wizard Step 4 window displays.

Step 11 When you get prompted to choose 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 12 (Optional) If you want to, you may select which subsequent (subscriber) node to use to restore the Cisco Unified Communications Manager database from. Use the drop-down list box to select the node that you want to use. DRS will first load all other information from the back up and then pull the latest database from the selected node.This will help to ensure that to ensure that all nodes are using current data.

Note If you use this option, initially you will restore only the data on the first node (publisher). However, when you perform the procedure in Step 15 and restore the subsequent cluster nodes, you will perform database replication and fully synchronize all nodes' databases.

Step 13 To start restoring the data, click **Restore**.

Step 14 Your data gets restored on the publisher node. To view the status of the restore, see the "Viewing the Restore Status" section on page 21.

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

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.

Step 15 When the restore status indicates 100 percent, continue with the "Restoring Subsequent Cluster Nodes (With or Without Rebuild)" section on page 19.

Note Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

Restoring the Entire Cluster

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. Follow these steps to restore an entire cluster:

Tip 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 the following procedure.

Note You can restore the whole cluster as a single operation after you rebuild the publisher server and the subscriber servers, or to revert to a known good configuration. You do not need to restore the first node and the subsequent nodes in two separate operations.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Note Before you restore a cluster, make sure that all nodes in the cluster are up and communicating with the first node. You must perform a fresh install for the nodes that are down or not communicating with first node at the time of the restore.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Configure the backup device. For more information, see Managing Backup Devices, page 7.

Step 4 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 5 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 6 Click **Next**. The Restore Wizard Step 2 window displays.

Step 7 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 8 Click **Next**. The Restore Wizard Step 3 window displays.

Step 9 Choose the features that you want to restore.

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

Step 10 Click **Next**. The Restore Wizard Step 4 window displays.

Step 11 When you get prompted to choose the nodes to restore, choose all the nodes in the cluster.

Note 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.

Note If a subsequent node is down or not connected to the cluster during the cluster restore, the database component restore will skip that node and proceed with the next one. You must perform a fresh install of Cisco Unified Communications Manager on these subsequent nodes.

Step 12 Your data gets restored on all the nodes of the cluster. To view the status of the restore, see the "Viewing the Restore Status" section on page 21.

Step 13 Restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

Note 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 14 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, begin rebooting the subsequent nodes in the cluster.

Step 15 When all the subsequent nodes have rebooted and are running the restored version of Cisco Unified Communications Manager, reboot the first node.

Note Database replication on the subsequent nodes may take an hour or more to complete after the publisher reboots, depending on the size of the cluster.

Step 16 Check the Replication Status value on all nodes by using the utils dbreplication status CLI command as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*. The value on each node should equal 2.

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

Restoring Subsequent Cluster Nodes (With or Without Rebuild)

Follow this procedure to restore subsequent nodes in the cluster.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Procedure

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager 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 of Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore. DRS does not restore across different hostnames, IP addresses and deployment types.

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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 If you are restoring the subsequent nodes after a rebuild, you must configure the backup device. For more information, see Managing Backup Devices, page 6.

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

Step 4 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 5 Click **Next**. The Restore Wizard Step 2 window displays.

Step 6 Choose the backup file that you want to restore.

Caution If you restored the first node earlier, you must choose the same backup file that you used to restore the first node to restore subsequent nodes in the cluster.

Step 7 Click **Next**. The Restore Wizard Step 3 window displays.

Step 8 Choose the features that you want to restore.

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

Step 9 Click **Next**. The Restore Wizard Step 4 window displays.

Step 10 When you get prompted to choose the nodes to restore, choose only the subsequent nodes.

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

Step 12 Your data gets restored on the subsequent nodes. To view the status of the restore, see the "Viewing the Restore Status" section on page 21.

Step 13 Restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

Note Database replication on the subsequent nodes may take an hour or more to complete after the publisher reboots, depending on the size of the cluster.

Step 14 Check the Replication Status value on all nodes by using the utils dbreplication status CLI command as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*. The value on each node should equal 2.

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

Viewing the Restore Status

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

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 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 4 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 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Navigate to **Backup > History**. The Backup History window displays.

Step 4 From the Backup History window, you can view the backups that you have performed, including filename, backup device, completion date, result, backup type, version, features that are backed up, and features that failed to back up.

Note The Features Backed Up window displays features that were backed up successfully or with a warning. The Failed Features window displays features that failed to backup or cancelled during a backup.

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

Restore History

Perform the following steps to view the restore history.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 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.

Step 3 Navigate to **Restore > History**. The Restore History window displays.

Step 4 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 features that failed to restore.

Note The Features Restored window displays features that restored successfully or with a warning. The Failed Features window displays features that failed to restore successfully.

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

Trace Files

In this release of the Disaster Recovery System, trace files for the Master Agent, the GUI, each Local Agent, and the Maverick SSH 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 Maverick, find the trace file at *platform/drf/trace/drfConfLib0**

Note Starting with Cisco Unified Communications Manager Release 8.6(1), DRS captures complete component logs for one backup and one restore operation; however, the DRS GUI continues to displays only 1 MB log files. You can locate these files under platform/drf/fulllog/.

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 **Note** Disaster Recovery System allows only an input parameter of the hostname of the server.
utils disaster_recovery maverick	Enables/Disables Maverick SSH 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 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

Table 3 Disaster Recovery System Command Line Interface (continued)

Command	Description
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, component registration, and deregistration 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 Unified Communications Manager node, the node disconnected before the backup operation completed.

Table 4 Disaster Recovery System Alarms and Messages (continued)

Alarm Name	Description	Explanation
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 Unified Communications Manager 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.	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 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. DRF Network Message has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing on the node. 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 Upgarde/Migration or Fresh Install.
DRFComponentRegistered	DRF successfully registered the requested component.	DRF successfully registered the requested component.
DRFRegistrationFailure	DRF registration operation failed.	DRF registration operation failed.
DRFComponentDeRegistered	DRF successfully deregistered the requested component.	DRF successfully deregistered the requested component.
DRFDeRegistrationFailure	DRF deregistration request for a component failed.	DRF deregistration request for a component failed.

Related Documentation

Refer to the *Cisco Unified Communications Manager Documentation Guide* to learn about the documentation for Cisco Unified Communications Manager.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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.