Disaster Recovery System Administration Guide for Cisco Unified Communications Manager and IM & Presence Service, Release 9.1(1)

First Published: December 20, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28671-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface vii

Purpose vii

Audience vii

Related Documents vii

Obtaining Documentation and Submitting a Service Request viii

Cisco Product Security Overview viii

PART I Disaster Recovery System Administration for Cisco Unified CM 1

CHAPTER 1 Cisco Unified CM Disaster Recovery System 3

Disaster Recovery System 3

Quick-Reference Tables for Backup and Restore Procedures 5

Backup Quick Reference 5

Restore Quick Reference 6

Supported Features and Components 6

System Requirements 7

Log In to Disaster Recovery System 9

Master Agent 9

Master Agent Functions 9

Local Agents 10

Local Agent Functions 10

Set Up Backup Devices 10

Create and Edit Backup Schedules 11

Enable, Disable, and Delete Schedules 13

Estimate Size of Backup tar 13

Manual Backup 14

Backup status 15

Check Current Backup Job Status 15
Restore Scenarios 15
Restore Node Or Cluster to Last Known Good Configuration 16
Restore the First Node Only 18
Restore Entire Cluster 20
Restore Subsequent Cluster Nodes 21
Restore Cluster in One Step After Publisher Rebuilds 22
Check Current Restore Job Status 24
Backup and Restore History 24
View Backup History 24
View Restore History 25
Trace Files 25
Command-Line Interface 26
Alarms and Messages 27

PART II Disaster Recovery System Administration for IM and Presence Service 31

CHAPTER 2 IM and Presence Disaster Recovery System 33
Disaster Recovery System 33
Features and components 33
System requirements 34
Access the Disaster Recovery System 34
Back up data in the Disaster Recovery System 34
Add backup devices 35
Create and edit backup schedules 36
Enable, disable, and delete schedules 38
Start manual backup 38
Check status of current backup job 40
Restore scenarios 40
Restore node or cluster to a good configuration 41
Restore publisher node 43
Restore subsequent cluster nodes 44
Restore entire cluster 45
Backup and restore history 47
View Restore Status 47

View Backup History 47
View Restore History 48
Data authentication and encryption 48
Trace files 49
Command Line Interface 49
Known issues 50
Restore to virtual machine fails 50
Alarms 50

Preface

- Purpose, page vii
- Audience, page vii
- Related Documents, page vii
- Obtaining Documentation and Submitting a Service Request, page viii
- Cisco Product Security Overview, page viii

Purpose

The *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager* 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, Cisco Unified Communications Manager IM and Presence Service, and other Cisco IP telephony applications.

Audience

The *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager* provides information to perform a system data restoration for network administrators who are responsible for managing and supporting Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.

Related Documents

See the *Cisco Unified Communications Manager Documentation Guide* to learn about the documentation for Cisco Unified Communications Manager and IM and Presence Service.

For the latest IM and Presence Service and Cisco Unified Communications Manager requirements, see the *Release Notes for Cisco Unified Communications Manager*.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco Product Security Overview

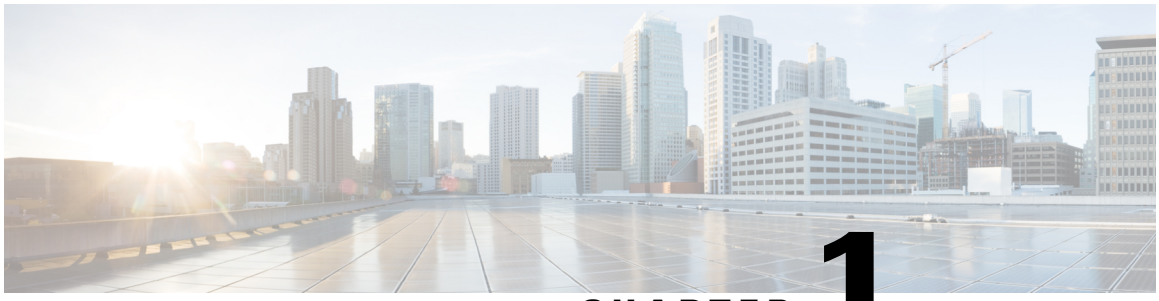
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors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

PART I

Disaster Recovery System Administration for Cisco Unified CM

- Cisco Unified CM Disaster Recovery System, page 3



CHAPTER 1

Cisco Unified CM Disaster Recovery System

- Disaster Recovery System, page 3
- Quick-Reference Tables for Backup and Restore Procedures , page 5
- Supported Features and Components, page 6
- System Requirements, page 7
- Log In to Disaster Recovery System, page 9
- Master Agent, page 9
- Local Agents, page 10
- Set Up Backup Devices, page 10
- Create and Edit Backup Schedules, page 11
- Enable, Disable, and Delete Schedules, page 13
- Estimate Size of Backup tar, page 13
- Manual Backup, page 14
- Backup status, page 15
- Restore Scenarios, page 15
- Check Current Restore Job Status, page 24
- Backup and Restore History, page 24
- Trace Files, page 25
- Command-Line Interface, page 26
- Alarms and Messages, page 27

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 the 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 8.6.1.20000-1 to version 8.6.2.20000-2, or from version 8.6.2.20000-2 to 8.6.2.21900-5.

Caution Before running a backup or restore, make sure that all cluster nodes are running the same version of Cisco Unified Communications Manager. If different nodes are running different versions of Cisco Unified Communications Manager, you will end up with a certificate mismatch and your backup or restore could fail.

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, DNS configuration, version, and deployment type of the restore matches the hostname, IP address, DNS configuration, 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 Guides.

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.

Procedure

Step 1 Create backup devices on which to back up data.
Set Up Backup Devices, on page 10

Step 2 Create and edit backup schedules to back up data on a schedule. Either a manual or a scheduled backup backs up the whole cluster.

Create and Edit Backup Schedules, on page 11

Step 3 Enable and disable backup schedules to back up data.
Enable, Disable, and Delete Schedules

Step 4 Estimate size of backup tar taken to SFTP device
Estimate Size of Backup tar, on page 13

Step 5 Optionally, run a manual backup.
Manual Backup, on page 14

Step 6 Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.
Check Current Backup Job Status, on page 15

Restore Quick Reference

The following procedure 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.

Procedure

Step 1 Choose Storage Location—You must first choose the storage location from which you want to restore a backup file.

Step 2 Choose the Backup File—From a list of available files, choose the backup file that you want to restore.

Step 3 Choose Features—From the list of available features, choose the features that you want to restore.

Step 4 Choose Nodes—If the feature was backed up from multiple nodes, you must choose the nodes that you want to restore.

Step 5 Start the Restore.

Step 6 Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.

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 Technology Partners. Technology partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, see the *Solutions Catalog* on the Cisco Developer Network.

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, contact GlobalSCAPE.

Note We recommend that you retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. As a best practice, perform a backup and restore on a standby or backup server.

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 1: SFTP Server Information

SFTP Server	Information
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade UCM for which versions compatible: https://marketplace.cisco.com

SFTP Server	Information
SFTP Server from another Third Party	These servers are third party provided, have limited Cisco testing, and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

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
- Cygwin
- Titan

For information on how to configure Cygwin for use with Cisco Unified Communications Manager, see http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/initial/configuration/ig.pdf.

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 Cisco Technology Developer Program 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, Disaster Recovery System does not block most CLI commands, because 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). After this backup is complete, you can restore it on your HP DL380-G6 (software-only) publisher.

Log In to 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 CLI. See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* for more information.

Master Agent

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

The system automatically starts the Master Agent (MA) on the publisher node. The Master Agent 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 remote network location.

Master Agent Functions

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

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

Local Agent Functions

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 System uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. This certificate exchange is handled internally. You do not need to make any configuration changes to accommodate this exchange.

Set Up Backup Devices

Before you use the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can configure up to ten backup devices. You can add, delete, and list devices through the CLI. Perform the following steps to configure backup devices.

Procedure

Step 1 Log in to the **Disaster Recovery System** with the same administrator username and password that you use for Cisco Unified OS Administration or IM and Presence OS Administration .

Step 2 Select **Backup** > **Backup Device**. The Backup Device List window displays.

Step 3 Do either of the following:

- To create a new backup device, click **Add New**.
- To edit an existing backup device, select the device in the Backup Device list and click **Edit Selected**.
- To delete a backup device, select it in the Backup Device list and click **Delete Selected**.

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

Step 4 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 5 In the Select Destination area, choose the location to which you want to save the backup file. The options are:

a) Tape Device—Stores the backup file on a locally attached tape drive. Choose the tape device from the list.

Note Be aware that you cannot span tapes or store more than one backup on a 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.

b) 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:

- Host name/IP address: Hostname 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 before you create the backup. The account that is used to access the SFTP server must have write permission for the selected path.

Step 6 Click **Save**.
The DRS Master Agent validates the selected backup device to ensure that the username, password, server name, and directory path are valid. If any of these values are invalid, the save operation fails.

Create and Edit Backup Schedules

You can create up to fourteen 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.

Note You can list and add backup schedules through the Command Line Interface.

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 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**. If you are creating and editing backup schedules for IM and Presence nodes, select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence 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 OS Administration. For Cisco Unified CM IM and Presence, log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified CM IM and Presence OS 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 or Cisco IM and Presence Service 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**.

Enable, Disable, and Delete Schedules

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, on page 26.

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

a) To select all schedules, click Select All.
b) 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.

Estimate Size of Backup tar

Follow this procedure to estimate the size of the backup tar that is performed on an SFTP device.

Note Be aware that the calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

Note Be aware that if no backup history exists for one or more of the selected features, Cisco Unified Communications Manager cannot estimate the size of the backup tar.

Procedure

Step 1 Log in to the Disaster Recovery System by using the same administrator username and password that you use for Cisco Unified OS Administration or IM and Presence OS Administration.

Step 2 Select the **Backup** > **Manual Backup** menu.
The Manual Backup window appears.

Step 3 In the Select Features area, select the features to back up.

Step 4 Click **Estimate Size** to get the estimated size of backup for the selected features.

Manual Backup

Follow this procedure to start a manual backup.

Note While a backup is running, you cannot perform any tasks in Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration because Disaster Recovery System locks the platform API to block all requests. However, Disaster Recovery System does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

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.

Note Before you run a backup, make sure that all cluster nodes are running the same version of Cisco Unified Communications Manager or Cisco Unified Communications Manager IM and Presence Service. If different nodes are running different versions, the certificates will not match and your backup could fail.

Procedure

Step 1 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified OS Administration or IM and Presence OS Administration.

Step 2 Navigate to **Backup** > **Manual Backup**. The Manual Backup window displays.

Step 3 In the Select Backup Device area, select a backup device.

Step 4 In the Select Features area, select the features to back up.

Step 5 Click **Start Backup** to start the manual backup.

Note Be aware that because of “no space in remote server” or “interruptions in network connectivity” or any other reason, the backup process could fail. If this happens, address the reasons that caused the backup to fail and then start a fresh backup.

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 Backup and Restore History, on page 24.

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.

Check Current Backup Job Status

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 and you must begin a fresh backup.

Procedure

Step 1 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified OS Administration or IM and Presence Administration.

Step 2 Select **Backup** > **Current Status**. The Backup Status window displays.

Step 3 To view the backup log file, click the log filename link.

Step 4 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.

Caution 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. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore.

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

Note Before running a DRS restore, make sure that all cluster nodes are running the same version of Cisco Unified Communications Manager. If different nodes are running different versions of Cisco Unified Communications Manager, you will end up with a certificate mismatch and your restore could fail.

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.

Tip For more information, see the “Installing the CTL Client” and “Configuring the CTL Client” procedures in the Cisco Unified Communications Manager Security Guide.

Restore Node Or Cluster to Last Known Good Configuration

Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure. If you intend to rebuild the publisher server, read the Restore the First Node Only, on page 18. If you intend to rebuild the entire cluster, read the Restore Entire Cluster, on page 20.

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

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

Procedure

Step 1 Choose **Restore** > **Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 2 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 3 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 4 Click Next. The Restore Wizard Step 3 window displays.

Step 5 Choose the features that you want to restore.

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

Step 6 Click **Next**. The Restore Wizard Step 4 window displays.

Step 7 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.

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 8 When you get prompted to choose the node to restore, choose the appropriate node.

Step 9 (Optional) If the node that you chose to restore is a publisher node, from the Select Server Name drop-down list box, choose the Cisco Unified Communications Manager subscriber node from which you want to restore the publisher database. The Disaster Recovery System restores all nondatabase information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component and if the node that you chose is a publisher node.

Note In order to resolve the hostname, you must first configure a DNS server on the publisher, or to navigate to **System** > **Server** on the publisher to add the subscriber for which the database is going to be restored from.

Step 10 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).

Note 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 Restore the First Node Only, on page 18 for more details.

Step 11 Your data gets restored on the node that you chose. To view the status of the restore, see the Check Current Restore Job Status, on page 24.

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

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 12 After the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

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

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

Step 13 Replication will setup automatically after a cluster reboot. Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

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

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

Restore the First Node Only

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

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

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.

Note 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 8.6.1.20000-1 to version 8.6.2.20000-2, or from version 8.6.2.20000-2 to 8.6.2.21900-5.

Procedure

Step 1 Choose **Restore** > **Restore Wizard**.
The **Restore Wizard Step 1** window displays.

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

Step 3 Click **Next**. The Restore Wizard Step 2 window displays.

Step 4 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 5 Click **Next**. The Restore Wizard Step 3 window displays.

Step 6 Choose the features that you want to restore.

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

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

Step 8 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 9 (Optional) From the Select Server Name drop-down list box, choose the subscriber node from which you want to restore the publisher database. The Disaster Recovery System restores all nondatabase information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 15 and restore the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Note Make sure the subscriber node that you chose is up and connected to the cluster. A subscriber node can be added manually to the cluster in Cisco Unified Communications Manager Administration (**System** > **Server**).

Step 10 To start restoring the data, click **Restore**.

Step 11 Your data gets restored on the publisher node.

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.

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 12 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, restart the server. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

Note Restart of all the nodes in the cluster is required in case of restoring only to the first node.

Note Ensure that you restart the first node before you restart the subsequent nodes.

Step 13 When the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

Step 14 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions. The value on each node should equal 2.

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

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

Restore 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.

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

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 Choose **Restore** > **Restore Wizard**.
The **Restore Wizard Step 1** window displays.

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

Step 3 Click **Next**.
The **Restore Wizard Step 2** window displays.

Step 4 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 5 Click **Next**.
The **Restore Wizard Step 3** window displays

Step 6 Click **Next**. The Restore Wizard Step 4 window displays.

Step 7 Choose all the nodes when prompted to choose restore nodes.

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

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

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 9 After the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, restart the server(s). For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

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

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

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

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

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

Restore Subsequent Cluster Nodes

Follow this procedure to restore one or more subsequent nodes in the cluster.

Before You Begin

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

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching software versions for restore operations.

If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

Procedure

Step 1 Click **Restore** > **Restore Wizard**. The Restore Wizard Step 1window displays.

Step 2 In the**Select Backup Device area** choose the backup device from which to restore.

Step 3 Click **Next**. The Restore Wizard Step 2 window displays.

Step 4 Choose the backup file that you want to restore.

Step 5 Click **Next**. The Restore Wizard Step 3 window displays.

Step 6 Choose the features that you want to restore.

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

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

Step 8 When you get prompted to choose the nodes to restore, choose only the subsequent nodes.

Step 9 Click **Restore**.

Step 10 Your data is restored on the subsequent nodes.

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

Step 11 After the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.

Restore Cluster in One Step After Publisher Rebuilds

Follow this procedure to restore the entire cluster in one step if the Publisher has already been rebuilt or fresh installed.

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*

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.

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

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.

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

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 Click **One-Step Restore**.

Note This option appears on Restore Wizard Step 4 window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes.

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

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

Note After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 18 and Restore Subsequent Cluster Nodes, on page 21.

Step 12 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.

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

Step 14 Your data gets restored on all the nodes of the cluster. To view the status of the restore, see Viewing the Restore Status, page 24.

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 15 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

Note Database replication on the subsequent nodes may take enough time to complete depending on the size of the cluster.

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

Step 16 If the database replication status is 2, restart the servers. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

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

Note When the subsequent nodes have restarted, and is running the restored version of Cisco Unified Communications Manager, restart the first node.

Check Current Restore Job 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. If you are checking the current restore job status for IM and Presence nodes, select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence 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. For Cisco Unified CM IM and Presence, log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified CM IM and Presence OS 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.

Backup and Restore History

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

View Backup History

Perform the following steps to view the backup history.

Note Backup files are encrypted and can be opened only by the system software.

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. If you are viewing backup history for IM and Presence nodes, select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence 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. For Cisco Unified CM IM and Presence, log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified CM IM and Presence OS 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, version, features that are backed up, and failed features.

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

View 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. If you are viewing restore history for IM and Presence nodes, select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence 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. For Cisco Unified CM IM and Presence, log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified CM IM and Presence OS 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 failed features.

Note 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 JSch library get written to the following locations:

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

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 2: Disaster Recovery System Command Line Interface

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

Command	Description
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 3: 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.
DRFMABackupComponentFailure	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.

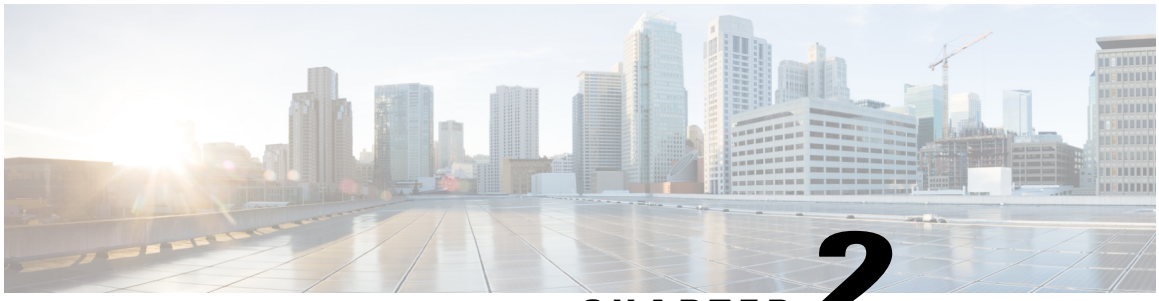
Alarm Name	Description	Explanation
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation on a Cisco Unified Communications Manager node, the node disconnected before the backup operation completed.
DRFMARestoreComponentFailure	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.

Alarm Name	Description	Explanation
DRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the 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.

PART II

Disaster Recovery System Administration for IM and Presence Service

- IM and Presence Disaster Recovery System, page 33



CHAPTER 2

IM and Presence Disaster Recovery System

- Disaster Recovery System, page 33
- Access the Disaster Recovery System , page 34
- Back up data in the Disaster Recovery System, page 34
- Restore scenarios, page 40
- Backup and restore history, page 47
- Data authentication and encryption, page 48
- Alarms, page 50

Disaster Recovery System

The IM and Presence Disaster Recovery System, which can be invoked from Cisco Unified CM IM and Presence Administration, provides full data backup and restoration capabilities for all servers in an IM and Presence cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

Features and components

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks. You can schedule backups of the IM and Presence database and can choose which nodes in the cluster you want to restore.
- A distributed system architecture for performing backup and restore functions. The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with all the Local Agents, which run backup and restore scripts on the server.
- Archive backups to a physical tape drive or remote SFTP server.

The Disaster Recovery System can back up and restore the following components:

- Trace Collection Tool (TCT)

- IM and Presence Preference Files (PREFS)
- IM and Presence Database (DB)
- XMPP Configuration Files (XCP)
- Syslog Component (SYSLOGAGT)
- Platform
- Reporter
- Cluster Manager (CLM)
- IM and Presence Configuration Files (CUP)

The Disaster Recovery System backs up all of its components automatically.

System requirements

To back up data to a remote device on the network, you must have configured an SFTP server. 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).

Access the Disaster Recovery System

Before You Begin

- If you are already signed into Cisco Unified CM IM and Presence Administration, you must sign out of the application before you use the Disaster Recovery System.
- Make sure that IM and Presence is running on all servers in the cluster.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Enter the same Administrator username and password that you use to access the Cisco Unified IM and Presence Operating System Administration.

Troubleshooting Tip

You set the Administrator username and password during IM and Presence installation, and you can change the Administrator password or set up a new Administrator account using the Command Line Interface (CLI).

Back up data in the Disaster Recovery System

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

Caution Always run the Post Install Setup wizard immediately after a fresh installation of the IM and Presence Service, and before you back up or restore your data in the Disaster Recovery System. The operation fails if you install IM and Presence and attempt to back up or restore data in the Disaster Recovery System before you run the Post Install wizard. For more information, see the *Installation Guide*.

Add backup devices

Before you use the Disaster Recovery System, you must create backup devices on which to back up data and configure the locations where you want the backup files to be stored. You can configure up to ten backup devices. You can add, delete, and list devices through the CLI.

Note The Disaster Recovery System restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. The Disaster Recovery System backs up and restores drfDevice.xml and drfSchedule.xml files. When the server restores these files, you do not need to reconfigure the Disaster Recovery System backup device and schedule.

Before You Begin

Make sure that you have access to an SFTP server to configure a network storage location. The Disaster Recovery System only supports SFTP servers that are configured with an IPv4 address or hostname/Fully Qualified Domain Name (FQDN). The account that you use to access the SFTP server must have write permission for the selected path.

Note If you sign in on a VMware virtual machine, you cannot back up on a tape because the system disables the tape device option for VMware users.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence main window.

Step 2 Select **Go**.

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration.

Step 4 Select **Backup** > **Backup Device**.

Step 5 Select **Add New** to configure a new backup device.

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

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

If you want to...	Action
Store the backup file on a locally attached tape drive	1 Select **Tape Device**. 2 Select the appropriate tape device from the **Device name** list box. You cannot span tapes or store more than one backup per tape.
Store the backup file on a networked drive that is accessed through an SFTP connection	1 Select **Network Directory**. 2 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.

Step 8 Select **Save** to allow the Disaster Recovery System Master Agent to validate the selected SFTP server.

What to Do Next

Create and edit backup schedules.

Related Topics

Create and edit backup schedules, on page 36

Create and edit backup schedules

You can create up to 10 backup schedules to back up the whole cluster. 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 Be aware that your backup .tar files are encrypted by a randomly generated password. IM and Presence uses the cluster security password to encrypt this password and save it along with the backup .tar files. If you change this security password through the Command Line Interface or a fresh install, the Disaster Recovery System will prompt you for the old security password. Therefore, to use old backups, we recommend that you remember the old security password or perform a fresh backup immediately after you reset or change the password.

Before You Begin

- Configure your backup devices. You can add, delete, and list devices through the Command Line Interface (CLI).
- Schedule backups during off-peak hours to avoid processing interruptions and impact to service.
- Make sure that all servers in the cluster are running the same version of IM and Presence and can be reached through the network. Servers that are not running at the time of the scheduled backup will not be backed up.

Note While a backup is running, you cannot perform any tasks in Cisco Unified IM and Presence Operating System Administration because Disaster Recovery System locks the platform API to block all requests to Cisco Unified IM and Presence Operating System Administration. However, this does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go**.

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration.

Step 4 Select **Backup** > **Scheduler**.

Step 5 Do one of the following steps to add a new schedule or edit an existing schedule:

a) Select **Add New** to create a new schedule.

b) Select a name in the **Schedule List** column to configure an existing schedule.

Step 6 Enter a schedule name in the **Schedule Name** field. You cannot change the name of the default schedule.

Step 7 Select the backup device in the **Select Backup Device** area.

Step 8 Select the features to back up in the **Select Features** area. You must select at least one feature, for example, CUP.

Step 9 Select the date and time when you want the backup to begin in the **Start Backup** at area.

Step 10 Select the frequency at which you want the backup to occur in the **Frequency** area: Once, Daily, Weekly, or Monthly.
If you choose to back up on a weekly basis, you can also select the days of the week when the backup will occur. To set the backup frequency to Weekly, occurring Tuesday through Saturday, select **Set Default**.

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

What to Do Next

Enable, disable and delete schedules

Related Topics

Enable, disable, and delete schedules, on page 38
Command Line Interface, on page 49
Add backup devices, on page 35

Enable, disable, and delete schedules

Complete this procedure to enable, disable or delete schedules.
You can also enable, disable, and delete backup schedules through the Command Line Interface (CLI).

Note You cannot delete a backup device if you configured it as the backup device in a backup schedule.

Procedure

Step 1 Select **Navigation** > **IM and Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration.

Step 4 Select **Backup** > **Scheduler**.

Step 5 Select the check boxes next to the schedules that you want to modify.

a) Select **Select All** to select all schedules.
b) Select **Clear All** to clear all check boxes.

Step 6 Select **Enable Selected Schedules** to enable the selected schedules.

Step 7 Select **Disable Selected Schedules** to disable the selected schedules.

Step 8 Select **Delete Selected** to delete the selected schedules.

What to Do Next

Check the status of the current backup job.

Related Topics

Check status of current backup job, on page 40
Start manual backup, on page 38
Command Line Interface, on page 49

Start manual backup

Complete the following procedure to start a manual backup. Optionally, you can run a manual backup to back up the whole cluster.

Caution Be aware that your backup .tar files are encrypted by a randomly generated password. IM and Presence uses the cluster security password to encrypt this password and save it along with the backup .tar files. If you change this security password through the Command Line Interface or a fresh install, the Disaster Recovery System will prompt you for the old security password. Therefore, to use old backups, we recommend that you remember the old security password or perform a fresh backup immediately after you reset or change the password.

Before You Begin

- Configure your backup devices.
- Schedule backups during off-peak hours to avoid processing interruptions and impact to service.
- Make sure that all servers in the cluster are running the same version of IM and Presence and can be reached through the network. Servers that are not running at the time of the scheduled backup will not be backed up.
- While a backup is running, you cannot perform any tasks in Cisco Unified IM and Presence Operating System Administration because Disaster Recovery System locks the platform API to block all requests to Cisco Unified IM and Presence Operating System Administration. However, this does not block most CLI commands as only the CLI-based upgrade commands use the Platform API locking package.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration window.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration.

Step 4 Select **Backup** > **Manual Backup**.

Step 5 Select a backup device in the **Select Backup Device** area.

Step 6 Select the features to back up in the **Select Features** area, for example, CUP.

Step 7 Select **Start Backup** to start the manual backup.

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

What to Do Next

Check the status of the current backup job.

Related Topics

Check status of current backup job, on page 40
Add backup devices, on page 35

Check status of current backup job

While a backup is running, you can check the status of the current backup job.

Before You Begin

Configure and schedule the backup job. 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.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper, right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go**.

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration.

Step 4 Select **Backup** > **Current Status**.

Step 5 Select the log filename hyperlink to view the backup log file.

Step 6 Perform one of the following actions if required:

a) Select **Cancel Backup** to cancel the current backup. The backup cancels after the current component completes its backup operation.

b) Select **Refresh**.

The **Result** column indicates the staging results of individual components. The **Status** column indicates the status of the entire backup.

Related Topics

Start manual backup, on page 38
Create and edit backup schedules, on page 36
Restore scenarios, on page 40

Restore scenarios

The Restore Wizard walks you through the steps that are required to restore a backup file:

- Select Storage Location—You must first select the storage location from which you want to restore a backup file.
- Select the Backup File—From a list of available files, you must select the backup file that you want to restore.
- Select Features—From the list of available features, you must select the features that you want to restore.
- Select Nodes—If the feature was backed up from multiple nodes, you must select the nodes that you want to restore.

Caution Always run the Post Install Setup wizard immediately after a fresh installation of the IM and Presence Service, and before you back up or restore your data in the Disaster Recovery System. The operation fails if you install IM and Presence and attempt to back up or restore data in the Disaster Recovery System before you run the Post Install wizard. For more information, see the *Installation Guide*.

Related Topics

Restore node or cluster to a good configuration, on page 41
Restore publisher node, on page 43
Restore subsequent cluster nodes, on page 44
Restore entire cluster, on page 45

Restore node or cluster to a good configuration

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, see the topic on restoring the first node on the publisher server. If you intend to rebuild the entire cluster, see the relevant topic.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Also, be aware that the File Integrity Check process consumes a lot of CPU and network bandwidth, which will considerably slow down the restore process.

Note The Disaster Recovery System does not migrate data from Windows to Linux. A restore must run on the same product version as the backup.

Before You Begin

- Make sure that the IM and Presence 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 IM and Presence for restore. For example, the Disaster Recovery System does not allow a restore from version 8.6.2.10000-44 to version 8.6.3.10000-20, or from version 8.6.3.10000-20 to version 8.6.3.20000-1. (The last parts of the version number change when you install a service release or an engineering special.)
- Make sure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore.

Caution After you select the node to which you want the data restored, the system overwrites any existing data on that server.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **Restore Wizard**.

Step 5 On the first screen of the Restore Wizard, select the backup device from which to restore.

Step 6 On the second screen of the Restore Wizard, select the backup file that you want to restore.
The backup filename indicates the date and time that the system created the backup file.

Step 7 On the third screen of the Restore Wizard, select the features that you want to restore.
Only the features that were backed up to the file that you select display.

Step 8 [Optional] Check Perform file integrity check using SHA1 Message Digest to run a File Integrity Check.
A file integrity check is optional and required only in the case of SFTP backups. You need not run an integrity check when restoring from Tape and Local device backups.

Step 9 Select **Restore** to start restoring the data.

- If you choose the first node to restore the data, the Disaster Recovery System automatically restores the IM and Presence database on the subsequent nodes.
- If you selected the Perform file integrity check using SHA1 Message Digest check box, the Disaster Recovery System runs the File Integrity Check on each file when you select Restore. If the system finds discrepancies in any .tar file during the check, it aborts the restore process immediately.

Caution After you select the node to which you want the data restored, the system overwrites any existing data on that server.

Step 10 Restart the server.
Even if you are restoring only to the first node, you must restart all nodes in the cluster.

Troubleshooting Tips

- If replication does not set up properly, use the `utils dbreplication status` CLI command to check the Replication Status value on all nodes. The value on each node should equal 2.
- 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 carry out a fresh install of IM and Presence on these subsequent nodes.
- During the restore process, do not perform any tasks with Cisco Unified CM IM and Presence Administration or IM and Presence User Pages.

What to Do Next

View the restore status.

Related Topics

Known issues, on page 50
Restore publisher node, on page 43
Restore entire cluster, on page 45

Restore publisher node

Restoring the first node restores the whole IM and Presence database to the cluster. This may take up to several hours based on number of nodes and size of database that you are restoring.

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.

Before You Begin

- Perform a fresh installation of IM and Presence on the first node or publisher server. For more information on installing IM and Presence, see the *Installation Guide for IM and Presence*.
- Make sure that the IM and Presence version that you 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 IM and Presence for restore. For example, the Disaster Recovery System does not allow a restore from version 8.6.2.10000-44 to version 8.6.3.10000-20, or from version 8.6.3.10000-20 to version 8.6.3.20000-1. (The last parts of the version number change when you install a service release or an engineering special.)
- Make sure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore.
- During the restore process, do not perform any tasks with Cisco Unified CM IM and Presence Administration or IM and Presence User Pages.

Caution Be aware that your backup .tar files are encrypted by a randomly generated password. IM and Presence uses the cluster security password to encrypt this password and save it along with the backup .tar files. If you change this security password between the backup and restore, the Disaster Recovery System will prompt you for the old security password. Therefore, to use old backups, we recommend that you remember the old security password or perform a fresh backup immediately after you reset or change the password.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **Restore Wizard**.

Step 5 On the first screen of the Restore Wizard, select the backup device from which to restore.

Step 6 On the second screen of the Restore Wizard, select the backup file that you want to restore.
The backup filename indicates the date and time that the system created the backup file.

Step 7 On the third screen of the Restore Wizard, select the features that you want to restore.
Only the features that were backed up to the file that you select display.

Step 8 On the final screen of the Restore Wizard, select **Restore** to start restoring the data
Select to restore your data to the first node only (the publisher).

Caution After you select the node to which you want the data restored, the system overwrites any existing data on that server.

Step 9 Restart all nodes in the cluster.

What to Do Next

Restore subsequent nodes in the cluster.

Related Topics

Known issues, on page 50
Restore node or cluster to a good configuration, on page 41
Restore entire cluster, on page 45
Backup and restore history, on page 47

Restore subsequent cluster nodes

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

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.

Before You Begin

- Restore the publisher node in the cluster.
- If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

- During the restore process, do not perform any tasks with Cisco Unified CM IM and Presence Administration or IM and Presence User Pages.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go**.

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **Restore Wizard**.

Step 5 On the first screen of the Restore Wizard, select the backup device from which to restore.

Step 6 On the second screen of the Restore Wizard, select the backup file that you want to restore.

Caution To restore subsequent nodes in the cluster, you must select the same backup file that you used to restore the first node.

Step 7 On the third screen of the Restore Wizard, select the features that you want to restore.
Only the features that were backed up to the file that you select display.

Step 8 On the final screen of the Restore Wizard, select **Restore** to start restoring the data
Select to restore only the subsequent nodes.

Caution After you select the node to which you want the data restored, the system overwrites any existing data on that server.

Step 9 Restart the server.

Step 10 Use the utils dbreplication status CLI command to check the Replication Status value on all nodes. The value on each node should equal 2.

What to Do Next

View the restore status.

Related Topics

Known issues, on page 50
Add backup devices, on page 35
Restore publisher node, on page 43
Restore node or cluster to a good configuration, on page 41
Restore entire cluster, on page 45

Restore 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. 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.

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 carry out a fresh install of IM and Presence on these subsequent nodes.

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.

Before You Begin

- Before you restore a cluster, make sure that all nodes in the cluster are up and communicating with the first node. You must carry out a fresh install for the nodes that are down or not communicating with first node at the time of the restore.
- 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.
- During the restore process, do not perform any tasks with Cisco Unified CM IM and Presence Administration or IM and Presence User Pages.

Procedure

Step 1 Select **Navigation** > **IM and Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **Restore Wizard**.

Step 5 On the first screen of the Restore Wizard, select the backup device from which to restore.

Step 6 On the second screen of the Restore Wizard, select the backup file that you want to restore.
The backup filename indicates the date and time that the system created the backup file.

Step 7 On the third screen of the Restore Wizard, select the features that you want to restore.
Only the features that were backed up to the file that you select display.

Step 8 On the final screen of the Restore Wizard, select **Restore** to start restoring the data
Select to restore all the nodes in the cluster.

Caution After you select the node to which you want the data restored, the system overwrites any existing data on that server.

Step 9 Use the utils dbreplication status CLI command to check the Replication Status value on all nodes. The value on each node should equal 2.

What to Do Next

View the restore status.

Related Topics

Known issues, on page 50

Restore publisher node, on page 43
Restore node or cluster to a good configuration, on page 41

Backup and restore history

Use these procedures to review the last 20 backup and restore jobs that you have performed.

View Restore Status

While the restore process is running, you can check the status of the current restore job.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **Status**.

Step 5 Select the log filename hyperlink to view the restore log file.

Step 6 Select **Refresh** if required.

Related Topics

Restore scenarios, on page 40
View Restore History, on page 48

View Backup History

From the **Backup History** window, you can view the backups that you have performed, including filename, storage location, completion date, result, and features that are backed up.

Note Backup files are encrypted and can only be opened by the system software.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Backup** > **History** to view the last 20 backup jobs.

Step 5 Select **Refresh** if required.

Related Topics

Back up data in the Disaster Recovery System, on page 34

View Restore History

You can check the status of the current backup job and cancel the current backup job. From the **Restore History** window, you can view the restore operations that you have performed, including filename, storage location, completion date, result, and the features that you restored.

Procedure

Step 1 Select **Navigation** > **IM and Presence Disaster Recovery System** from the menu in the upper right corner of Cisco Unified CM IM and Presence Administration.

Step 2 Select **Go.**

Step 3 Enter the same Administrator username and password that you use for the Cisco Unified IM and Presence Operating System Administration .

Step 4 Select **Restore** > **History** to view the last 20 restore jobs.

Step 5 Select **Refresh** if required.

Related Topics

Restore scenarios, on page 40
View Restore Status, on page 47

Data authentication and encryption

The system automatically activates both the Master Agent and the Local Agent on all nodes in the cluster. Each server in the IM and Presence 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 The Master Agent is functional only on the publisher node. The Master Agents on the subsequent nodes do not perform any functions.

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 IM and Presence cluster nodes. The Disaster Recovery System makes use of the IPSec certificates for its Public/Private Key encryption. IM and Presence handles this certificate exchange internally; you do not need to make any configuration changes to accommodate this exchange. However, be aware that if you delete the IPSEC truststore (hostname.pem) file from the Certificate Management pages in Cisco Unified IM and Presence Operating System Administration, the Disaster Recovery System will not work as expected. If you delete the IPSEC-trust file manually, make sure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the certificate management pages in the *Cisco Unified Operating System Administration Guide*.

Related Topics

Trace files, on page 49
Command Line Interface, on page 49
Known issues, on page 50
Alarms, on page 50

Trace files

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

- For the Master Agent: `platform/drf/trace/drfMA0*`
- For each Local Agent: `platform/drf/trace/drfLA0*`
- For the GUI: `platform/drf/trace/drfConfLib0*`

You can view trace files by using the Command Line Interface (CLI). See the *Cisco Unified Communications Operating System Maintenance Guide for IM and Presence* 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 the following table. For more information on these commands and on using the command line interface, see the *Cisco Unified Communications Operating System Administration Guide*.

Table 4: 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, filename, features, and nodes to restore.

Command	Description
`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.

Known issues

Restore to virtual machine fails

Problem

A database restore may fail if you restore an IM and Presence server, that was originally installed on an MCS physical server, to one of the small (500 or 2000 user) OVA deployment virtual machines.

Cause

This failure occurs when you migrate from a physical server with storage of 80GB or more to a virtual machine configuration that is designed for a smaller database (less than 80GB).

Solution

Redeploy the virtual machine with one of the larger user deployment sizes (5000 or 15000) because these deployment sizes are provisioned with two 80GB virtual disks which can accommodate the larger database from the physical server. This solution requires you to reinstall the base IM and Presence image because you cannot add storage after installation.

Alarms

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

Table 5: Disaster Recovery System Alarms

Alarm Name	Description	Explanation
CiscoDRFBackupCancelInternalError	DRF Backup operation has encountered an error. Backup cancelled internally.	DRF Backup operation has encountered an error. Backup cancelled internally.
CiscoDRFBackupDeviceError	DRF backup process has problems accessing device.	DRF backup process encountered errors while accessing device.
CiscoDRFBackupFailure	Cisco DRF Backup process failed.	DRF backup process encountered errors.
CiscoDRFFailure	DRF Backup or Restore process has failed.	DRF Backup or Restore process encountered errors.
CiscoDRFInternalProcessFailure	DRF internal process has encountered an error.	DRF internal process encountered an error.
CiscoDRFLA2MAFailure	DRF Local Agent is not able to connect to Master Agent.	DRF Local Agent cannot connect to Master Agent.
CiscoDRFLocalAgentStartFailure	DRF Local Agent was not able to start.	DRF Local Agent might be down.
CiscoDRFMA2LAFailure	DRF Master Agent is not able to connect to Local Agent.	DRF Master Agent cannot connect to Local Agent.
CiscoDRFMABackupComponentFailure	DRF was unable to backup at least one component.	DRF requested a component to back up its data; however, an error occurred during the backup process, and the component was not backed up.
CiscoDRFMABackupNodeDisconnect	The node being backed up disconnected from the Master Agent prior to being fully backed up.	The DRF Master Agent was running a backup operation on an IM and Presence node, and the node disconnected before the backup operation completed.
CiscoDRFMARestoreComponentFailure	DRF was unable to restore at least one component.	DRF requested a component to restore its data; however, an error occurred during the restore process, and the component was not restored.

Alarm Name	Description	Explanation
CiscoDRFMARestoreNodeDisconnect	The node being restored disconnected from the Master Agent prior to being fully restored.	The DRF Master Agent was running a restore operation on an IM and Presence node, and the node disconnected before the restore operation completed.
CiscoDRFMasterAgentStartFailure	DRF Master Agent was not able to start.	DRF Master Agent might be down.
CiscoDRFNoRegisteredComponent	No registered components available, backup failed.	DRF backup failed because no registered components are available.
CiscoDRFNoRegisteredFeature	No feature selected for backup.	No feature got selected for backup.
CiscoDRFRegistrationFailure	DRF Registration operation failed.	DRF Registration operation failed for a component due to some internal error.
CiscoDRFRestoreFailure	DRF restore process failed.	DRF restore process encountered errors.
CiscoDRFRestoreInternalError	DRF Restore operation has encountered an error. Restore cancelled internally.	DRF Restore operation has encountered an error. Restore cancelled internally.
CiscoDRFSftpFailure	DRF sftp operation has errors.	DRF SFTP operation has errors.
CiscoDRFTapeDeviceError	DRF is unable to access tape device.	DRF process encountered errors while accessing the tape device.

INDEX

A

Alarms and Messages 27

C

Checking Backup Status 15
Command Line Interface 26
Creating and Editing Backup Schedules 11

E

Enabling, Disabling, and Deleting Schedules 13

H

How to Access DRS 9

L

Local Agents 10

M

Managing Backup Devices 10
Master Agent Duties and Activation 9

Q

Quick-Reference Tables for Backup and Restore Procedures 5

R

Restore Scenarios 15

S

Starting a Manual Backup 14
Supported Features and Components 6
System Requirements 7

T

Trace Files 25

V

Viewing the Backup and Restore History 24
Viewing the Restore Status 24

W

What is the Disaster Recovery System? 3