Disaster Recovery System Overview

Disaster Recovery System

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, or from any IM and Presence Service node, 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.

When you perform 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.
- Archived backups to a 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 starts the Master Agent on the publisher node, and starts the Local Agent on all cluster nodes.

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, Call Detail Records Analysis and Reporting, and 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)
- Reporter

In addition, the Disaster Recovery System backs up and restores the following components of the IM and Presence Service if you have IM and Presence nodes installed in the cluster:

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

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 at https://marketplace.cisco.com.

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 on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
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 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

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

For Cygwin to function properly as your backup SFTP server, you must add the following lines to the `sshd_config` file:

The cipher key: ciphers aes128-cbc

The Unified Communications Algorithm: KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

Note For details on how to set up third-party SFTP products, contact the third-party vendor for support.

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.

Master Agent

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

Local Agents

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

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

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

Log In to Disaster Recovery System

Use the following procedure to access the Disaster Recovery System on Cisco Unified Communications Manager (Unified Communications Manager) nodes, or on IM and Presence nodes. If you are already signed in to the administration software for the node, you must sign out before you begin this procedure.

Procedure

	Command or Action	Purpose
Step 1	Log in to the Disaster Recovery System for the type of node that you are using: • If you are configuring backup and restore operations for Unified Communications Manager nodes, select **Navigation** > **Disaster Recovery System** from the Cisco Unified Communications Manager Administration window and click **Go**. • If you are configuring backup and restore operations 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**.	If you are already signed into the administration interface for the node, you must sign out of the application before you use the Disaster Recovery System.
Step 2	Enter the same Administrator username and password that you use to access the Operating System Administration interface for the node.	You set the Administrator username and password during the installation, and you can change the Administrator password or set up a new Administrator account using the Command Line Interface (CLI). Refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* for more information.