Disaster Recovery System

Backup and Restore Overview

The Disaster Recovery System (DRS) provides full data backup for all servers in a Cisco Unified Intelligence Center cluster. It 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 Intelligence Center cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up 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.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.

Backup Prerequisites

To back up data to a remote device on the network, you must have an SFTP server that is configured. You can use an SFTP server product that is certified with Cisco Technology Partners. Technology partners 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.

Ensure that all cluster nodes are running the same version of Cisco Unified intelligence Center. If different nodes are running different versions, the certificates will not match and your backup or restore could fail.

Note 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. Additionally, 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 Unified Communications Manager for which versions are 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 1GB 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**

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

Backup Procedure Taskflow

Configure backup devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.
- Ensure that the username, password, server name, and directory path are valid as the DRS Primary Agent validates the configuration of the backup device.

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

Procedure

Step 1 From Disaster Recovery System, select **Backup** > **Backup Device**.

Step 2 In the **Backup Device List** window, do either of the following:

- To configure a new device, click **Add New**.
- To edit an existing backup device, enter the search criteria, click Find, and **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 3 Enter a backup name in the **Backup Device Name** field.

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

Step 4 In the **Select Destination** area, under **Network Directory** perform the following:

- In the **Host name/IP Address** field, enter the hostname or IP address for the network server.
- In the **Path name** field, enter the directory path where you want to store the backup file.
- In the **User name** field, enter a valid username.
- In the **Password** field, enter a valid password.
- From the **Number of backups to store on Network Directory** drop-down list, choose the required number of backups.

Step 5 Click **Save**.

What to do next

Estimate Size of Backup Tar, on page 6

Configure a Schedule Backup

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

Caution Schedule backups during off-peak hours to avoid service interruptions.

Before you begin

Configure backup devices

Procedure

Step 1 From the Disaster Recovery System, choose **Backup Scheduler**.

Step 2 In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.

- To create a new schedule, click **Add New**.
- To configure an existing schedule, click the name in the Schedule List column.

Step 3 In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

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

Step 5 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and 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 8 To update these settings, click **Save**.

Step 9 Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

Step 10 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 Intelligence Center and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

What to do next

(Optional) View Current Backup Status

Start a Manual Backup

Before you begin

- Ensure that all cluster nodes have the same installed version of Cisco Unified Intelligence Center.
- Ensure that there is adequate space in the remote server.
- Ensure that there are no network interruptions.
- Configure backup devices
- Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change/reset.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

What to do next

(Optional) View Current Backup Status

View Current Backup 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 From the Disaster Recovery System, select **Backup** > **Current Status**.

Step 2 To view the backup log file, click the log filename link.

Step 3 To cancel the current backup, click **Cancel Backup**.

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

What to do next

View Backup History, on page 7

Estimate Size of Backup Tar

Cisco Unified Intelligence Center will estimate the size of the backup tar, only if a backup history exists for one more selected features.

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.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Select Features** area, select the features to back up.

Step 3 Click **Estimate Size** to view the estimated size of backup for the selected features.

What to do next

View Backup History, on page 7

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **History**.

Step 2 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.