Backup Procedures

This chapter describes the process for running backups.

- Backup Quick Reference, page 1
- Backup Notes and Tips, page 2
- Set Up Backup Devices, page 3
- Create and Edit Backup Schedules, page 4
- Enable, Disable, and Delete Schedules, page 5
- Estimate Size of Backup tar, page 6
- Manual Backup, page 6
- Check Current Backup Job Status, page 7

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 3

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 4

Step 3 Enable and disable backup schedules to back up data.
Enable, Disable, and Delete Schedules, on page 5

Step 4 Estimate size of backup tar taken to SFTP device
Estimate Size of Backup tar, on page 6

Step 5 Optionally, run a manual backup.

Manual Backup, on page 6

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 7

Backup Notes and Tips

Before you run a backup, review the following notes and tips for information about backups.

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

Note DRS encryption depends on the cluster security password. If you change this security password through the CLI or a fresh install, Cisco recommends that you take a fresh backup immediately or remember the old security password.

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 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, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the certificate management help pages in the Cisco Unified Communications Manager security guides.

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

Note For Release 10.0(1) and later, archived backups to tape drives are not supported. If you upgrade from pre-10.0(1) release to 10.0(1), the devices and schedules that are configured with tape drives will be removed after the upgrade. You must add the network device if it is not already added and reconfigure the schedule to facilitate the backup post upgrade.

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 a Network Directory location. The Network Directory location must be accessible through an SFTP connection.
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

Complete this procedure to enable, disable or delete schedules.

You can enable, disable, and delete backup schedules through the CLI. For details, see the Command Line Interface section.

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

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 Navigate to **Backup** > **Scheduler**.
The Schedule List window displays.

Step 3 Check the check boxes next to the schedules that you want to modify.

- To select all schedules, click **Select All**.
- To clear all check boxes, click **Clear All**.

Step 4 To enable the selected schedules, click **Enable Selected Schedules**.

Step 5 To disable the selected schedules, click **Disable Selected Schedules**.

Step 6 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.

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.