Backing Up and Restoring Cisco Unity Connection Components

You must take the backup of Cisco Unity Connection components to avoid loosing any data or messages. The following are the tools supported for taking the backup or restoring the Unity Connection components:

- About Cobras, on page 1
- About Disaster Recovery System, on page 1
- About System Restore Tool, on page 8

About Cobras

Cisco Unified Backup and Restore Application Suite (COBRAS) is an application used to migrate data and messages. You can take the backup using Export tool and restore the backup data using Import tool.

For more information, download the latest version of COBRAS, and view the training videos and Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

About Disaster Recovery System

The Disaster Recovery System (DRS) is web application that enables you to take the full backup of Unity Connection server components to remote locations using File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP).

You can take the backup of the following Unity Connection server components:

- Unity Connection configuration database
- Mailbox messages
- User greetings and recorded names
- Other server and platform components

DRS also provides a restore wizard that enables you to restore the Unity Connection server components from a backup file stored on an FTP or SFTP server.

Note You must configure the Unity Connection server with the settings similar to the server of which backup was taken before you can restore the software components.

All the tasks related to Cisco Unified Operating System Administration web interface remain in the locked state when Disaster Recovery System backup or restore is running. This is because DRS locks the operating system platform API. All the Command Line Interface (CLI) commands continue to work except for the CLI based upgrade command since the platform API is locked.

The Disaster Recovery System contains two key components:

- Master Agent (MA)
- Local Agent (LA)

The Master Agent coordinates the backup and restore activities with Local Agents. The system automatically activates both the Master Agent and the Local Agent on all the servers in the cluster.

Disaster Recovery System backup tasks can be configured from web interface or Command Line Interface (CLI) but configuring from web interface is more preferable. For information on configuring backup tasks using CLI, see the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Components Supported for DRS Backup

You can take the backup specific Unity Connection components. The components are listed under Select Features:

- CUC: Other Unity Connection server and platform components.
- CONNECTION_GREETINGS_VOICENAMES: All user greetings and recorded names.
- CONNECTION_DATABASE: Unity Connection configuration database.
- CONNECTION_MESSAGES_<MAILBOXSTORENAME>: All messages in the named mailbox store.
- CONNECTION_HTML_NOTIFICATION: All HTML notification messages.

Note Selecting the CONNECTION_GREETINGS_VOICENAMES or CONNECTION_HTML_NOTIFICATION component automatically includes the CONNECTION_DATABASE component.

You should take the backup of all the server components when you are taking the backup for the first time, changing the backup device, upgrading the Unity Connection server to higher releases, migrating from physical server to virtual machine, or re-installing the server.

Backup Files in DRS

DRS stores the backup of all the server software components in multiple .tar files based on the component selected.

The .tar backup file includes an XML file called drfComponent.xml that contains a catalog of all the component files stored during the backup operation. When DRS performs the next backup operation, it uses the contents of this catalog to determine:

- Whether the number of.tar backup files should exceed the total number of backups you defined for the backup device.
- The .tar backup file to erase.

Caution DRS encrypts the .tar backup files using the security password configured during the installation of Unity Connection server. If you decide to change this password, perform a full DRS backup immediately. You must use the same security password on the replacement server when performing a restore

operation.

Configuring DRS Backup

Note In a cluster deployment, you need to take the backup of publisher server only

Step 1 Set up and configure the FTP or SFTP server(s) used for storing the backups.

A number of SFTP applications, such as Free FTP and Core FTP mini SFTP server are available that can be used to store and retrieve the backups.

To configure the FTP or SFTP server, you must define the directory that stores the backup and create an account that DRS can use to store and retrieve the backups.

Note Make sure there is enough capacity in the directory for the required number and size of backups. Keep in mind that the size of the backups increase as the organization grows.

Step 2 Configure a backup device in DRS.

Each DRS backup device consists of the backup location, the FTP or SFTP account credentials, and the total number of backups that can be stored at the backup location. When the total number of allowed backups is reached, DRS overwrites the oldest backup on the server.

Follow the given steps to configure a backup device:

- Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.
- Select Backup> Backup Device. The Backup Device window displays. Select Add New.
- Enter the backup device name, network configuration information and the number of backups to store on network directory.
- Select Save to create the backup device.

Note Depending on the backup policy and organization, it is advisable to create multiple backup devices for redundancy. If the organization consists of multiple locations, each location should have its own set of backup devices

Caution Do not use the same network location/directory for different backup devices. Backup files for each Unity Connection server must be stored in a directory dedicated to that server.

Step 3 Configure the backup process

After creating the backup device, you can

- Configure a backup schedule using Configuring a Backup Schedule, on page 4
- Configure a manual backup using Configuring a Manual Backup, on page 5

Configuring a Backup Schedule

You can create a different backup schedule for each backup device you created. Backup schedule can be configured to run the backup at different times. It is recommended to take multiple schedules, each stored on a different network location.

In most of the cases, you should set a schedule that performs a nightly backup during a defined maintenance window when there is the least amount of server and network traffic.

You can configure up to ten backup schedules, each has its own backup device, features, and components.

Note Disabling the schedule allows you to prevent the scheduled backups from running without deleting the schedule entirely.

To Configure a Backup Schedule for Each Backup Device in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> Scheduler**. The Schedule List window displays.

Step 3 On the **Schedule List** window, select **Add New** to create a new backup schedule. The Scheduler window displays.

Step 4 On the Scheduler window, the following information are mentioned to configure a schedule:

- **Schedule Name**: Specify a schedule name.
- **Select Backup Device**: Specify the backup device for which you want to create a schedule.
- **Select Features**: Specify the Unity Connection components you want to backup.
- **Starts Backup a**t: Specify the starting date and time of the schedule.
- **Frequency**: Specify the daily, weekly, or monthly cycles of the schedule.

Step 5 Select **Save** to apply the backup schedule.

Note If you select the Set Default option in the toolbar enables you to configure the backup schedule to perform weekly backups on Tuesday through Saturday.

Configuring a Manual Backup

You can run a manual backup for all components each time you create or change the configuration of a backup device.

Note Make sure to select all the components listed for backup.

The amount of time required to complete the backup depends on the size of the database and the number of components selected for backup. The maximum time taken for backup to complete is 20 hours or it gets time out.

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> Manual Backup**. The Manual Backup window displays.

Step 3 On the Manual Backup window,

- **Select Backup Device:** Specify the backup device to be used for backup.
- **Select Features:** Specify the Unity Connection components you want to backup.

Step 4 Select **Start Backup** to start the manual backup.

DRS generates a log file for each component after completing its backup. If an error occurred, you can open the component's log file to identify the specific error.

Viewing the Backup Status

To View the Backup Status in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

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

Step 3 The **Backup Status** window displays the current status of the components selected for backup.

Step 4 You can select Cancel Backup to cancel the backup after the backup of the current component completes.

Viewing the Backup History

To View the Backup History in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> History**. The Backup History window displays.

Step 3 On the **Backup History** window you can view the backup history after running a manual backup, to ensure it completed successfully.

Step 4 You can select Cancel Backup to cancel the backup after the backup of the current component completes.

Configuring DRS Restore

In case of Unity Connection cluster, you take the backup of publisher server only. Therefore, you need to restore only on the publisher server.

To Restore the Software Components on Unity Connection

Step 1 Install a new Unity Connection server.

The new server must be installed with exactly the same software and patches as the server being removed from service, and must be configured with the same hostname, IP address, and deployment type (standalone server or cluster pair). For example, the Disaster Recovery System does not allow a restore from version 8.5(1).1000-1 to version 8.5(2).1000-1, or from version 8.5(2).1000-1 to version 8.5(2).1000-2. (The last parts of the version number change when you install a service release or an engineering special.)

Step 2 Follow the given steps after reinstalling Unity Connection:

a) Confirm that the IP address and hostname of the server matches the IP address and hostname of the server as it was before taking the backup.

b) Confirm that the following settings match the values when taking the server backups:

- Time zone
- NTP server
- NIC speed and duplex settings
- DHCP settings
- Primary DNS settings
- SMTP hostname
- X.509 Certificate information (Organization, Unit, Location, State, and Country)

c) Confirm that the security password of the server matches the security password of the server as it was before taking the backup.

DRS encrypts the backup data using security password as the encryption key. If you change the security password of the Unity Connection server after the last backup was taken, you need to enter the old security password during the restore process.

d) If any Unity Connection languages were previously installed, reinstall the same languages on the server.

Step 3 On the new server, log in to Disaster Recovery System (DRS) and recreate the backup device used to store the backups from the server removed from service.

Step 4 Follow the given steps to run the restore operation in DRS:

a) Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

b) Run the **Restore Wizard**.

From the toolbar, select **Restore** > **Restore Wizard**.

c) Select the backup device you re-created and select **Next**.

d) Select the backup .tar file to restore the components and select **Next**.

Note DRS time stamps each backup file enabling you to easily select the backup file to use for a restore operation.

e) Select the software components to restore and select **Next**.

f) Select the specific server to restore each component.

Additionally, Unity Connection can perform a file integrity check as part of the restore operation. This is advisable to ensure that the files are valid and have not been corrupted during the backup or restore operations.

g) Select **Restore** to begin the restore of the selected .tar file to the server.

As with the restore operation, you can view the restore operation log file for each restored component.

Also as with a restore operation, the time it takes to restore depends on the size of the database and the components restored.

Step 5 Restart the new Unity Connection server. In case of a cluster server, reboot the publisher server.

Step 6 (Cluster only) Once the publisher reboots, run the following command on Command Line Interface (CLI) on the subscriber server to copy the data from the publisher to the subscriber server:

```
utils cuc cluster overwritedb
```

Step 7 (Cluster only) Run the following CLI command on either the publisher or subscriber server to check the status of the Unity Connection cluster:

```
show cuc cluster status
```

Verify that the status of publisher server is Primary and subscriber server is Secondary. Test and validate it before moving it back into production.

Viewing the Restore Status

To Check the Restore Status in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

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

The Status column in the **Restore Status** window shows the percentage of restore process completed.

Step 3 To view the restore log file, select the log filename link.

Viewing the Restore History

To View the Restore History in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Restore > History**. The Restore History window displays.

Step 3 On the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

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

About System Restore Tool

The System Restore Tool is a new tool introduced in Unity Connection that allows the administrator to take either manual backup or schedule backup at specified intervals of time. The tool creates restore points that the administrator can use to restore data. For example, if the database is corrupted, the data can be restored using restore points.

Types of System Restore Points

The administrator can create following types of restore points using System Restore Tool:

- **Recent**: Allows you to restore the data from the most recent backup stored on the server.
- **Daybefore**: Allows you to restore the data from the backup before the recent data backup stored on the server.
- **Temp**: Allows you to restore data from the manual backup created at a particular instance of time. The administrator can create the Temp restore point through the run cuc sysrestore backup_temp CLI command only. For more information on the CLI command, see the "run cuc sysrestore backup_temp section" of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at

Note Whenever the data backup is initiated, the data from Recent restore point is copied to Daybefore and current restore point is marked as Recent. This cycle continues with each scheduled backup, which helps in maintaining the integrity of the backup and consuming less space (less than 2GB) to store the restore points efficiently.

Creating a Restore Point task

Do the following tasks to create restore points using System Restore Tool.

1. Create a user with mailbox with an alias "system-backup-and-restore-admin" and assign him a corporate email id to receive the restore point creation alerts or failure notifications. For more information on how to create a user, see Users chapter of *System Administration Guide for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Note Skip this task, if such user already exists.

2. If you want to schedule automatic backup, enable the Create Backup Restore Point task to automate backup. See Enabling Create Backup Restore Point
3. If you want to create manual backup, run the run cuc sysrestore backup_tem CLI command.

Note In case of Unity Connection cluster, take backup of publisher and subscriber server separately.

Enabling Create Backup Restore Point

Do the following steps to enable the Create Backup Restore Point task for automatic backup.

Step 1 Sign in to Cisco Unity Connection Administration.
Step 2 Navigate to **Tools > Task Management** and select **Create Backup Restore Point**.
Step 3 Go to **Edit** and select **Task Schedules**.
Step 4 On the Task Schedules page, enter the required information to schedule the task.
Step 5 Click **Save** to apply the settings.

Restoring Data using Restore Points task

The administrator can restore data using restore points created through System Restore Tool.

Note During restore operation, the tool specifies the timestamp of the restore point, the count of the messages against the user aliases, and also lists the users which will be lost after restore operation. The user aliases that are reported to be lost after restore are the aliases created after the restore point creation.

To restore the data using restore points, run the following CLI command:

```
run cuc sysrestore restore_operation <restore mode> <restore point>
```

where,

- restore mode can be database, config, or both
- restore point can be Recent, Daybefore or Temp

Restore mode specifies the data that you want to restore. For example, if you specify database as restore mode, only database is restored.

Note If you specify config or both as restore mode, you need to restart the server to restore the data successfully.