Unified CCX Disaster Recovery Administration

This guide provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup and restore related tasks. This guide serves as a reference and procedural guide that is intended for users of Cisco Unified Contact Center Express 9.0(1)

• Legal Information, page 26

Disaster Recovery System

Cisco Disaster Recovery System (Cisco DRS), which can be invoked from Cisco Unified Contact Center Express Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified Contact Center Express (Unified CCX) cluster. Cisco DRS allows you to perform regularly scheduled automatic or user-invoked data backups and to restore data after a failure.

In case of high availability (HA), Cisco DRS performs a cluster-level backup, which means that it collects backups for all servers in a Unified CCX cluster to a central location and archives the backup data to physical storage device.

Cisco DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. Cisco DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure Cisco DRS backup device and schedule.

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

Caution Before you restore Unified CCX, ensure that the Unified CCX version that is installed on the server matches the version of the backup file that you want to restore. Cisco DRS supports only matching versions of Unified CCX for restore. For example, Cisco DRS does not allow a restore from version 8.5(1).1000-1 to version 9.0(1).1000-1, or from version 8.5(2).1000-1 to version 9.0(1).1000-2.

Caution Before you restore Unified CCX, make sure 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.

Cisco DRS 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.

Cisco DRS contains two key components, 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 immediately after installation on the server and in case of HA setup it is activated on all nodes in the cluster.

Note In Release 9.0(1), Cisco DRS uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Unified CCX publisher and subscriber nodes. Cisco 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 Cisco 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, see the certificate management help pages in the Cisco Unified Communications Manager Security Guide available here:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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

Quick-reference tables for backup and restore procedures

The following tables provide a quick reference for the backup and restore procedures.

Note Cisco 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 Cisco 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 Cisco DRS.

Table 1: Major Steps for Performing a Backup Procedure

Action	Reference
Create backup devices to map to a remote storage location or a locally attached tape drive.	Manage backup devices, on page 7
Create and edit backup schedules. **Note** Either a manual or a scheduled backup backs up one or both the nodes in a cluster.	Create backup schedules, on page 9
Enable and disable backup schedules.	Manage backup schedules, on page 10
Optionally, run a manual backup.	Start manual backup, on page 11
Check the status of the current backup job while a backup is running.	Backup status, on page 12

Action	Reference
View the history of the recent backup jobs that you have performed.	View backup history, on page 22

Restore quick reference

Table 2 provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a restore procedure by using Cisco DRS.

Note Cisco DRS 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 follow the steps in Table 1, for information on data migration from a Windows-based platform to a Linux-based platform, see the Upgrading to Cisco Unified Contact Center Express, Release 9.0(1) available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html

Table 2: Major Steps for Performing a Restore Procedure

Action	Reference
Choose Storage Location—You must first choose the storage location from which you want to restore a backup file.	Restore scenarios, on page 12
Choose the Backup File—From a list of available files, choose the backup file that you want to restore.	Restore scenarios, on page 12
Choose Nodes—Choose all nodes/servers.	Restore scenarios, on page 12
Choose Data Source—When you restore a first node (publisher), restore Cisco Unified CCX data from a good subsequent node (subscriber) to ensure that you are using current data.	Restore scenarios, on page 12
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	View restore status, on page 21
View the history of the recent restore jobs that you have performed.	View restore history, on page 22

Features and components

Cisco DRS can back up and restore the following components.

- Cluster configurations and applications profile in the data repository

- Workflow scripts that are already uploaded in the data repository
- Platform
- Databases (such as db_cra, db_cra_repository, and FCRasSvr database)
- Configuration data (such as open LDAP and flat files)
- Recording files
- JTAPI configuration (jtapi.ini)
- Trace Collection Tool (TCT)
- User prompts, grammars, and documents
- CUIC_CONFIG configuration (such as configuration property files, security configuration, and Unified Intelligence Center tomcat server.xml)

System requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured and accessible from the Unified CCX node on which you intend to run the backup. Cisco allows you to use any SFTP server product, but recommends SFTP products that have been certified with Cisco through the Interoperability Verification Testing (IVT) process. Cisco Developer Network (CDN) partners, such as GlobalSCAPE, certify their products with specified version of Unified CCX. For information on which vendors have certified their products with your version of Unified CCX, refer to the following URL:

https://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

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 (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

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

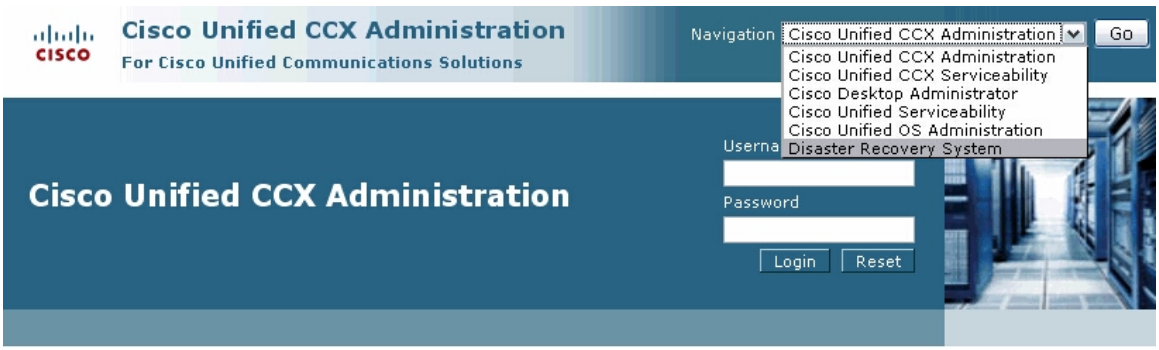
Note For issues with third-party products that have not been certified through the IVT process, contact the third-party vendor for support.

Note While a backup or restore is running, you cannot perform any Operating System (OS) Administration tasks because Cisco DRS blocks all OS Administration requests by locking the platform API. However, this does not block most CLI commands as only the CLI-based upgrade commands use the Platform API locking package.

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

Access Disaster Recovery System

To access Cisco DRS, choose **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window. Log in to the Disaster Recovery System by using the same Platform Administrator username and password that you use for Cisco Unified Operating System Administration.



Note You set the Platform Administrator username and password during Unified CCX installation, and you can change the Platform Administrator password or set up a new Platform Administrator account by using the Command Line Interface (CLI). For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions available here:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Master Agent duties and activation

The system automatically activates the Master Agent service on each node of the cluster, but the Master Agent is functional only on the first node. However, the Master Agent on the second node remains non-functional.

Master Agent duties

The Master Agent (MA) performs the following duties:

- The MA stores systemwide 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 can access the MA through Cisco DRS 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

Each server in a Cisco Unified Contact Center Express cluster, including the server that contains the Master Agent, must have its own Local Agent to perform the backup and restore functions for its server.

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

Local Agent duties

In a Unified CCX cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

Note In Release 9.0(1), Cisco DRS uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Unified CCX publisher and subscriber nodes. Cisco DRS makes use of the IPSec certificates for its Public/Private Key encryption. This certificate exchange gets handled internally; you do not need to make any configuration changes to accommodate this exchange.

Manage backup devices

Before using Cisco DRS, you must configure the locations where you want the backup files to be stored. You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select Disaster Recovery System from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 3 Navigate to **Backup** > **Backup Device**. The Backup Device List window displays.

Step 4 To configure a new backup device, click **Add New**.

Step 5 To edit a backup device, select it in the Backup Device list. Then, click **Edit Selected**.
The Backup Device window displays.

Step 6 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 7 Choose one of the following backup devices and enter the appropriate field values in the Select Destination area:

a) **Tape Device**—Stores the backup file on a locally attached tape drive. Choose the appropriate tape device from the list. Note the following considerations:

- You cannot use more than one tape for a single backup. If you have more data than will fit on a tape, either you must store backups on a network directory, or you must back up components on one tape and back up mailbox stores on one or more additional tapes.
- You cannot store more than one backup on a tape; each backup overwrites the data from the previous backup, so you only have the data from the most recent backup. If you want to create more than one backup for a server (components in one backup, mailbox stores in another backup, for example), you must use separate tapes. Otherwise, you will only have the portion of the data that you backed up last.

Note You cannot span tapes or store more than one backup per tape.

Support for tape devices to store backup files is not available for systems running Unified CCX in a VM environment.

b) **Network Directory**—Stores the backup file on a network drive that is accessed through an SFTP connection. Cisco DRS only supports SFTP servers that are configured with an IPv4 address or hostname/Fully Qualified Domain Name (FQDN). 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. This field displays 2 by default.

Note You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

Step 8 To update these settings, click **Save**. The Update Successful Status appears.

Note After you click the Save button, the Cisco DRS Master Agent validates the selected backup device. If the user name, password, server name, or directory path is invalid, the save will fail.

Step 9 To delete a backup device, select it in the Backup Device list. Then, click **Delete Selected**.

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

Create backup schedules

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

Note You can list and add backup schedules through the Command Line Interface. For more information on CLI commands for DRS, refer to the Command line interface, on page 23.

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.

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

Perform the following steps to manage backup schedules:

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System 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.

Step 6 Select the backup device in the Select Backup Device area.
You must back up the database and recorded names. Backing up messages is optional.

Step 7 Select the feature UCCX.

Step 8 Choose the date and time when you want the backup to begin in the Start Backup at area. Note the following:

a) Schedule backups during off-peak hours to avoid affecting system performance.

b) Do not schedule a backup to run while the Update Database Statistics task is running. By default, this task runs daily at 2:00 am.

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 If you plan to schedule a backup on a two-node deployment, ensure that both the servers in the cluster are running the same version of Unified CCX 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**.

Manage backup schedules

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified 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 performed on an SFTP device.

Note 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. Also, this procedure does not estimate the size of a backup performed on a tape device.

Note If no backup history exists for one or more of the selected features, Unified CCX cannot estimate the size of the backup tar.

Procedure

Step 1 Sign 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 2 Select the **Backup > Manual Backup** menu.

Step 3 In te **Select Features** area of the Manual Backup window, select the features to back up.

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

Start manual backup

Follow this procedure to start a manual backup.

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.

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Cisco DRS by using the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 3 Navigate to **Backup** > **Manual Backup**. The Manual Backup window displays.

Step 4 Select a backup device in the **Select Backup Device** area.
You must back up the database and recorded names. Backing up messages is optional.

Step 5 Select the feature UCCX.

Step 6 To start the manual backup, click **Start Backup**.

Note Click **Estimate Size** button to know the approximate size of the disk space consumed on the SFTP server once backup is performed. The size estimation is done based on the previous history of backup performed on the server.

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 22.

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.

Note Typically, when the backup is complete, the Successful Backup Status displays.

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 3 Navigate to **Backup** > **Current Status**. The Backup Status window displays.

Note You can also use a CLI command to check the backup status. See the Command line interface, on page 23 for details.

Step 4 To view the backup log file, click the log filename link.

Step 5 To cancel the current backup, click **Cancel Backup**.

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

Restore scenarios

When performing a system data restoration, you can choose which node in the cluster you want to restore considering both stand alone (SA) and high availability (HA).

Note Do not attempt a restore when there is a version mismatch between the nodes of UCCX.

Caution Before you restore Unified CCX, ensure that the Unified CCX version that is installed on the server matches the version of the backup file that you want to restore. Cisco DRS supports only matching versions of Unified CCX for restore. For example, Cisco DRS does not allow a restore from version 8.5(1).1000-1 to version 9.0(1).1000-1, or from version 8.5(1).1000-2 to version 9.0(1).1000-1. (The last parts of the version number change when you install a service release or an engineering special.) In essence, the product version needs to match, end-to-end, for Cisco DRS to run a successful Unified CCX database restore.

Caution Be aware that Cisco DRS encryption depends on the cluster security password. if you have changed the security password between the backup and this restore, Cisco 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 or reset.

Note If there is no backup available, then you may not be able to run the restore activity on any of the nodes through Cisco DRS framework.

Caution After you restore a node using any of the restore scenarios, reboot the node, and then perform the Data Resync manually by logging in to the web interface of Cisco Unified CCX Administration.

You can restore either the SA or an HA setups of Unified CCX in the following scenarios:

- Restore SA setup (with rebuild), on page 13
- Restore SA or HA setup (without rebuild), on page 15
- Restore publisher node in HA setup (with rebuild), on page 16
- Restore subscriber node in HA setup (with rebuild), on page 18
- Restore both nodes in HA setup (with rebuild), on page 20

Restore SA setup (with rebuild)

You can restore an SA setup (with rebuild) if:

- There is a hard drive failure and you have a valid backup taken before the failure. Follow this procedure to restore the node.
- The server hardware is to be replaced. Take a backup of Unified CCX when running in the old server hardware that is to be replaced. Note the backup device details before you bring down the Unified CCX setup. Follow this procedure to bring up a new server.

Tip If you are doing any other type of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform the following procedure.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration and security password used earlier) on the node prior to restoring it.
For more information on installing Unified CCX, see Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Navigate to Cisco Unified CCX Administration. Choose **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 3 Log in to the Disaster Recovery System by using the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 4 Configure the backup device. For more information, see Manage backup devices, on page 7.

Step 5 Navigate to **Restore** > **Restore Wizard**.
The Restore Wizard Step 1 window displays.

Step 6 In the Select Backup Device area, choose the backup device from which to restore.

Step 7 Click **Next**.
The Restore Wizard Step 2 window displays.

Step 8 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 9 Click **Next**.
The Restore Wizard Step 3 window displays.

Step 10 Select the feature UCCX.

Step 11 Click **Next**.
The Restore Wizard Step 4 window displays.

Step 12 In **File Integrity Check** field, select the check box if you want to perform the file integrity check using SHA1 Message digest.
A warning appears. This step is, however, optional.

Note If you select the Perform file integrity check using SHA1 Message Digest checkbox, Cisco 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).

Step 13 Click **OK** to proceed.

Step 14 In Select the Servers to be restored for each Feature field, select the node that you want to restore.

Step 15 To start restoring the data, click **Restore**.

Note Restoring the node restores the whole Unified CCX database. This may take up to several hours based on the size of database that is being restored.

Step 16 Your data gets restored on the node. To view the status of the restore, see the View restore status, on page 21.

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

Step 17 Restart the server when the restore is successful and the status shows 100 per cent.
For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Note If you have done some configuration or hardware changes while performing fresh installation in Step 1 that might impact the License MAC, then rehost your license again using the license rehosting mechanism.

For more information on the licensing rehosting mechanism, see Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Restore SA or HA setup (without rebuild)

Use this procedure if you are simply restoring an SA or HA setup of Unified CCX to the last known good configuration, without reinstalling Unified CCX on any of the nodes. Do not use this after a hard drive failure or other hardware failure. If you intend to rebuild an SA setup, see the Restore SA setup (with rebuild), on page 13. For an HA setup with rebuild, see the following sections.

Note Before you restore a cluster, make sure that the second node in the cluster is up and communicating with the first node. Run the CLI command **utils network connectivity** to know if second node is communicating with the first node.

You must carry out a fresh installation for the second node that is neither up nor communicating with the first node at the time of the restore.

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

Caution You should not perform the restore activity of a SA backup in a HA setup; otherwise the cluster will break and the second node will become an orphan.

To perform a restore, use the procedure that follows.

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco CCX 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 Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 3 Navigate to **Restore** > **Restore Wizard**.

The Restore Wizard Step 1 window displays.

Step 4 In the Select Backup Device area, choose the backup device from which to restore.

Step 5 Click **Next**.
The Restore Wizard Step 2 window displays.

Step 6 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 7 Click **Next.**
The Restore Wizard Step 3 window displays.

Step 8 Select the feature UCCX.

Step 9 Click **Next.**.
The Restore Wizard Step 4 window displays

Step 10 In **File Integrity Check** field, select the check box if you want to perform the file integrity check using SHA1 Message digest.
A warning appears. This step is however optional.

Note If you select the Perform file integrity check using SHA1 Message Digest checkbox, Cisco 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).

Step 11 Click **OK** to proceed.

Step 12 In **Select the Servers to be restored for each Feature** field, select the node(s) that you want to restore.

Note In Select the Servers to be restored for each Feature field, select both the nodes in case of an HA setup.

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

Step 14 Your data gets restored on the node. To view the status of the restore, see View restore status, on page 21.

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

Step 15 Restart the SA server or the HA cluster when the restore is successful and the status shows 100 per cent. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Step 16 After you restart the SA server or HA cluster, perform the data resync by choosing **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from the Web interface of the Cisco Unified CCX Administration.

Note Restoring the node restores the entire Unified CCX database. This may take up to several hours based on the size of database that is being restored.

Restore publisher node in HA setup (with rebuild)

In a high availability (HA) setup, if there is a hard-drive failure or any other critical hardware or software failure which needs rebuild of the Publisher (first) node, then do the following procedure to recover the publisher node to the last backed up state of the publisher. Run the following procedure if you have a valid backup taken before the failure of the node.

Caution Be aware that one-step restore feature is not supported for Unified CCX.

Caution Be aware that your backup .tar files are encrypted by a randomly generated password. Unified CCX 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, Cisco DRS will prompt you for the old security password. Therefore, to use old backups, Cisco recommends that you remember the old security password or perform a fresh backup immediately after you reset or change the password.

Procedure

Step 1 Perform a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password used earlier) on the node prior to restoring it.
For more information on installing Unified CCX, see the Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Navigate to Cisco Unified Contact Center Express Administration, select **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 3 Log in to the Disaster Recovery System by using the same Platform Administrator username and password that you use to login to Cisco Unified Operating System Administration.

Step 4 Configure the backup device. For more information, see Manage backup devices, on page 7.

Step 5 Navigate to **Restore** > **Restore Wizard**.
The Restore Wizard Step 1 window displays.

Step 6 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 7 Click **Next.**
The Restore Wizard Step 2 window displays.

Step 8 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 9 Click **Next**.
The Restore Wizard Step 3 window displays.

Step 10 Select the feature UCCX.

Step 11 Click **Next.**
The Restore Wizard Step 4 window displays.

Step 12 When you are prompted to choose the nodes to restore, choose only the first node (the publisher).
Caution Do not select the second (subscriber) node in this condition as this action will result in failure of the restore attempt.

Step 13 To start restoring the data, click **Restore**.
Note During the restore process, do not perform any tasks with Cisco Unified CCX Administration or User Options.

Restoring the first node may take up to several hours based on the size of database that is being restored. Depending on the size of your database that you choose to restore, the system can require one hour or more to restore.

Note Based on the requirements, you have the option to either retrieve the existing publisher node data from the Cisco DRS backup to be available on all the nodes in the cluster or retrieve the more recent data (if available) from the subscriber node to be available in the cluster.

Step 14 Run the following CLI command from the Subscriber node after the restore process is successful (restore status indicates 100 per cent) to initiate restoring the Publisher node only (with rebuild).

```
utils uccx setuppubrestore
```

Step 15 Run the following CLI command on the target node; that is, if you want to retrieve the publisher node's data, then run this command on the subscriber node, but if you want to retrieve the subscriber node's data (which is more up-to-date), then run this command on the publisher node.

```
utils uccx database forcedatasync
```

Warning In any case, you must execute this command on either of the nodes after restoring the publisher node.

Step 16 Restart both the nodes and run the following CLI command on the Publisher node to set up replication:

```
utils uccx dbreplication reset
```

For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Caution If you have done some configuration or hardware changes while performing fresh installation in Step 1 that might impact the License MAC, then rehost your license again using the license rehosting mechanism before running the CLI command `utils uccx dbreplication reset`.

For more information on the licensing rehosting mechanism, see the Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 17 Your data gets restored on the publisher node. To view the status of the restore, see the View restore status, on page 21.

Restore subscriber node in HA setup (with rebuild)

Caution In case the second node crashes and there is no backup available, you may not be able to restore anything. However, to recover the second node in this case, delete the second node from the first node, add the second node details again, and then rebuild the second node. The recording and monitoring data which was present in the box cannot be recovered since there is no backup.

In a high availability (HA) setup , if there is a hard-drive failure or any other critical hardware or Software failure which needs rebuild of the Subscriber (second) node, then follow the below procedure to recover the subscriber node to the last backed up state of the subscriber. Run the below procedure if you have a valid backup taken before the failure of the node.

Procedure

Step 1 Perform a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password used earlier) on the node prior to restoring it.
For more information on installing Cisco Unified Contact Center Express, see the Installing Cisco Unified Contact Center Express guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Navigate to Cisco Unified Contact Center Express Administration, select **Disaster Recovery System** from the Navigation drop-down list box in the upper-right corner of the Cisco Unified Contact Center Express Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 3 Log in to the Disaster Recovery System by using the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System Administration.

Step 4 Configure the backup device.
For more information, see Manage backup devices, on page 7.

Step 5 Navigate to **Restore** > **Restore Wizard**.
The Restore Wizard Step 1 window displays.

Step 6 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 7 Click **Next.**
The Restore Wizard Step 2 window displays.

Step 8 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 9 Click **Next.**
The Restore Wizard Step 3 window displays.

Step 10 Select the feature UCCX.

Step 11 Click **Next.**
The Restore Wizard Step 4 window displays.

Step 12 When you get prompted to choose the nodes to restore, choose only the second node (the subscriber).

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

Step 14 Your data gets restored on the second node.
To view the status of the restore, see View restore status, on page 21.

Step 15 Restart the server when the restore status is 100 per cent.
For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Restore both nodes in HA setup (with rebuild)

In a high availability (HA) setup, if a major hard drive failure occurs on both the nodes in the cluster, or in the event of a hard drive migration or replacement, you may need to rebuild both the nodes.

- In case of a hard drive failure if you have taken a valid backup before the failure, follow this procedure to restore both the nodes, starting with the publisher node.
- In case of server hardware replacement, take a backup of Unified CCX when running in the old server hardware that is to be replaced. Note the backup device details before you bring down the Unified CCX setup. Follow this procedure to bring up a new server.

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

Caution If you do not have a valid backup for the publisher node, you may not be able to restore anything as all of your data will be lost from both the nodes. In such a case, set up a new cluster.

Procedure

Step 1 Rebuild the first node by performing a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password being used before the failure).
For more information on installing Cisco Unified Contact Center Express, see the Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Restore only the first node by following Step 1 through Step 13 of the Restore publisher node in HA setup (with rebuild), on page 16.

Step 3 Restart the first node.
For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Caution If you have done some configuration or hardware changes during the fresh installation of first node in Step 1 that might impact the License MAC, then rehost your license again using the license rehosting mechanism. For more information on the licensing rehosting mechanism, see the Installing Cisco Unified Contact Center Express available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 4 Rebuild the second node by performing a fresh installation of the same version of Cisco Unified Contact Center Express (using the same administrator credentials, network configuration and security password being used before the failure).
For more information on installing Cisco Unified Contact Center Express, refer to Installing Cisco Unified Contact Center Express.

Step 5 Restore only the second node by following Step 1 through Step 15 of the Restore subscriber node in HA setup (with rebuild), on page 18.

Step 6 Restart the second node if not done already. Your data gets restored on both the nodes of the cluster.
For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Note Depending on the size of your database that you choose to restore, the system may require a few hours to restore.

Replace server hardware

You can replace the server hardware in the following cases:

- To restore the hardware in case of a disaster or to replace the server for an SA setup, follow the steps in Restore SA setup (with rebuild).
- To replace only the Publisher server hardware in HA setup, follow the steps in Restore publisher node in HA setup (with rebuild).
- To replace only the Subscriber server hardware in HA setup, follow the steps in Restore subscriber node in HA setup (with rebuild)
- If the hard drive fails or you need to upgrade to new servers in HA setup, follow the steps in Restore both nodes in HA setup (with rebuild).

View restore status

To check the status of the current restore job, perform the following steps:

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System 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.

Note You can also use a CLI command to check the restore status. See the Command line interface, on page 23 for details.

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, on page 22
- View restore history, on page 22

View backup history

Perform the following steps to view the backup history.

Procedure

Step 1 Navigate to Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System 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, time, result, and feature that are backed up.

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 Cisco Unified CCX Administration, select **Disaster Recovery System** from the Navigation menu in the upper-right corner of the Cisco Unified CCX Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System with the same Platform Administrator username and password that you use to log in to Cisco Unified Operating System 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, and the feature that were restored.

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

Trace files

In this release of Cisco DRS, 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/drMA0*
- 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 platforms/drf/trace/drfJSch*

You can view trace files by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html

Command line interface

Cisco DRS 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 available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Table 3: Disaster Recovery System Command Line Interface Commands

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the feature that is configured in the Cisco DRS interface
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, feature, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery history	Displays the history of previous backup and restore operations
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

Command	Description
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
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

Cisco DRS issues alarms for various errors that could occur during a backup or restore procedure. Table 4 provides a list of Cisco DRS alarms.

Table 4: Disaster Recovery System Alarms

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	Cisco DRS backup process encountered errors while it was accessing device.
DRFBackupFailure	Cisco DRF Backup process failed.	Cisco DRS backup process encountered errors.
DRFBackupInProgress	New backup cannot start while another backup is still running.	Cisco DRS cannot start new backup while another backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	Cisco DRS internal process encountered an error.
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	Cisco DRS Local Agent cannot connect to Master Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	Cisco DRS Local Agent might be down.
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	Cisco DRS Master Agent cannot connect to Local Agent.

Alarm Name	Description	Explanation
DRFMABackupComponentFailure	DRF cannot back up at least one component.	Cisco DRS requested a component to back up its data; however, an error occurred during the backup process, and the backup of the component failed.
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the Cisco DRS Master Agent was running a backup operation on a Unified CCX node, the node disconnected before the backup operation completed.
DRFMARestoreComponentFailure	DRF cannot restore at least one component.	Cisco DRS requested a component to restore its data; however, an error occurred during the restore process, and the component was not restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the Cisco DRS Master Agent was running a restore operation on a Unified CCX node, the node disconnected before the restore operation completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	Cisco DRS Master Agent might be down.
DRFNoRegisteredComponent	No registered components are available, so backup failed.	Cisco 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.	Cisco DRS restore process cannot read from device.
DRFRestoreFailure	DRF restore process failed.	Cisco DRS restore process encountered errors.
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in Cisco 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 backed up successfully.	DRF backed up successfully.
DRFRestoreCompleted	DRF restored successfully.	DRF restored 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 Upgrade or Migration or Fresh Install.

Related documentation

- To learn more about Cisco Unified Contact Center Express documentation, see the following URL: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html.
- For a complete list of terms used in Cisco Unified CCX and Cisco Unified IP IVR, see the following URL: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_technical_reference_list.html.

Additional support and documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Legal Information