Backup and Restore

Cisco Disaster Recovery System (Cisco DRS), which you can access from Cisco Unified Contact Center Express Administration, provides complete 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 in the case of a system failure.

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 using platform administrator credentials.

Cisco DRS will 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`)
- Finesse components
- Socket.IO Server Configuration Files

In the 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 a remote SFTP server.

DRS will back up and restore its own settings, that is, backup device settings (saved in file `drfDevice.xml`) and schedule settings (saved in file `drfSchedule.xml`) as part of the platform component. Once a server is restored with these files, you do not need to reconfigure DRS backup device and schedule settings.

Note Cisco DRS uses 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:

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

Important Considerations

Following are the important considerations when you perform backup and restore procedures:

- Before you run 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 have a certificate mismatch and your backup or restore will fail.
- Before you restore Unified CCX, make sure that the hostname, IP address, DNS configuration, version, and deployment type matches the hostname, IP address, DNS configuration, version, and deployment type of the backup file that you want to restore.
- 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 restore only for matching versions of Unified CCX. For example, Cisco DRS does not allow you to 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.
- Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.
- After you use the recovery disk to bring a server with a corrupted file system into a bootable and semi-functional state, rebuild the server.

Note If you do not rebuild the server, you may notice missing directories, lost permissions, or corrupted soft links.

SFTP 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 to run the backup. Cisco allows you to use any SFTP server 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 a specified version of Unified CCX. For information about which vendors have certified their products with your version of Unified CCX, see 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 (see http://sshwindows.sourceforge.net/)
- Cygwin (see http://www.cygwin.com/)
- Titan (see http://www.titanftp.com/)

Cisco does not support use of the SFTP product freeFTPD, because it has a 1-GB file-size limit.

Note

- For issues with third-party products that have not been certified through the IVT process, contact the third-party vendor for support.
- While a backup or restore is running, you cannot perform any Operating System (OS) Administration tasks because Cisco DRS blocks all OS Administration requests. However, you can use CLI commands to back up or restore the system.

Master and Local Agents

The system automatically starts the Master Agent service on each node of the cluster, but it is functional only on the first node. Both servers in a Unified CCX cluster must have Local Agent running to perform the backup and restore functions.

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

Master Agent Duties

The Master Agent (MA) performs the following duties:

- Stores system-wide component registration information.
- 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.
- Lets you 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.
- Stores backup data on a remote network location.

Local Agent Duties

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

Note 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 uses IPSec certificates for its Public/Private Key encryption. This certificate exchange is handled internally; you do not need to make any configuration changes to accommodate this exchange.

Backup Tasks

You can perform the following backup tasks using Cisco DRS:

- Manage backup devices
- Create backup schedules
- Manage backup schedules
- Estimate size of backup tar file
- Perform manual backup
- Check backup status
- View history of last 20 backups

Manage Backup Devices

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

Procedure

Step 1 On **Disaster Recovery System** page, choose **Backup** > **Backup Device**.

Step 2 Click appropriate button to add a new device or to edit settings of an existing backup device.

Step 3 Enter the backup device name and choose the backup device type.

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

Manage Backup Schedules

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

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

Procedure

Step 1 On the **Disaster Recovery System** page, choose **Backup** > **Scheduler**.

Step 2 Click the appropriate button to add a new schedule or to edit settings of an existing backup schedule.

Step 3 Fill out the form and enable the backup schedule.

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 communicating in the network. Servers that are not communicating at the time of the scheduled backup will not be backed up.
- Do not schedule a backup to run while the **Update Database Statistics** task is running. By default, this task is set to run every Saturday at 3:00 am and Shrink-repack on Sunday at 3:00 am.

Perform Manual Backup

Procedure

Step 1 On the **Disaster Recovery System** page, choose **Backup** > **Manual Backup**.

Step 2 Select a backup device and start the backup.

Step 3 Click **Estimate Size** to get the approximate size of the disk space that the backup file will consume on the SFTP server.

To perform backup tasks on virtual machines, see *Unified Communications VMware Requirements*, available here:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

Check Backup Status

On the **Disaster Recovery System** page, choose **Backup** > **Current Status** to check the backup status.

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.

Restore Scenarios

You can choose to restore any node in the cluster.

Note

- Do not attempt a restore when there is a version mismatch between the Unified CCX nodes.
- If no backup is available, you may not be able to run the restore activity on any of the nodes through Cisco DRS.
- If restore is performed without rebuild, both the nodes have to be restored.
- **One-Step Restore** option is not supported in 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, remember the old security password or perform a fresh backup immediately after you reset or change the password.
- 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.) The product versions need to match, end-to-end, for Cisco DRS to run a successful Unified CCX database restore.
- After you restore a node, reboot the node, and then perform the Data Resync manually by logging in to the web interface of **Cisco Unified CCX Administration**.
- The backup process does not back up the passwords that you set for Wallboard and Recording SFTP external database users. After data is restored, passwords revert to the original default value. If you set passwords for external database users, you must manually reset them from the **Password Management** window.

Restore SA or HA Setup (Without Rebuild)

Perform this procedure if you are 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 perform this procedure after a hard drive failure or other hardware failure.

Note Before you restore a cluster, make sure that the second node in the cluster is functional and is 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 if it is not functional or if it is not communicating with the first node at the time of the restore.

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 be an orphan.

Procedure

Step 1 In the **Disaster Recovery System** page, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process. You can select a single node or both nodes while performing restore.

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

Step 2 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 *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Step 3 After you restart the SA server or HA cluster, perform the data resync by choosing **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from **Cisco Unified CCX Administration** web interface.

Restore SA Setup (with Rebuild)

You can restore a SA setup (with rebuild) in the following cases:

- The hard drive fails, and you have a valid backup that was taken before the hard drive failure.
- The server hardware is to be replaced. Take a backup of Unified CCX when it is running in the old server hardware that is to be replaced. Note the backup device details before you shut down the Unified CCX setup.
- To correct a virtual machine with unaligned partitions, you will need to perform a manual backup first and follow the procedure by performing a fresh installation using the latest OVF Template from Unified Contact Center Express Virtual Machine Templates

Tip If you are performing 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 that you used earlier) on the node before you restore it.

Step 2 In the **Disaster Recovery System** page, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process.

Note
- There is no need to perform initial configuration in the **Unified CCX Administration** page for any restore with rebuild scenarios.
- To view the current license package, go to **System > Licensing > Display License**.

Step 3 Restart the server when the restore is successful and perform data resync manually using **Unified CCX Administration** page.

Note
- Apply the same license type on node the backup was taken to restore.
- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Standard, Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.

For more information on the license rehosting mechanism, see the *Cisco Unified Contact Center Express Install and Upgrade Guide*, available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Restore Only First 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 first node, then perform the following procedure to recover the publisher node to the last backed up state of the publisher.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration, and security password that you used earlier) on the node before you restore it.

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.

Note To view the current license package, go to **System > Licensing > Display License**.

Step 3 After the restore process is successful, run the following CLI command from the second node.

```
utils uccx setuppubrestore
```

Step 4 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
```

Step 5 Restart both the nodes and run the following CLI command on the Publisher node to set up replication:

```
utils uccx dbreplication reset
```

Step 6 To set up replication for the Cisco Finesse database:

a) Run the following CLI command on the Subscriber node:

```
utils dbreplication stop
```

b) Run the following CLI command on the Publisher node:

```
utils dbreplication reset all
```

Caution

- Apply the same license type on node the backup was taken to restore.
- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Standard, Enhanced, Premium, IP IVR) as the license contained within the backup that was restored.

For more information on the licensing rehosting mechanism, see *Cisco Unified Contact Center Express Install and Upgrade Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Restore Second 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, 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 server 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 second node, then perform the following procedure to recover the second node to the last backed up state of the second node.

Procedure

Step 1 Perform a fresh installation of the same version of Unified CCX (using the same administrator credentials, network configuration, and security password that you used earlier) on the node before you restore it.

Step 2 In the **Disaster Recovery System** web interface, choose **Restore** > **Restore Wizard**.

Follow the on-screen instructions in the wizard to complete the restore process.

Note When you are prompted to choose the nodes to restore, choose only the second node.

Step 3 Restart the server when the restore status is 100 per cent.

For more information on restarting, see *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_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 first 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.
- To correct a virtual machine with unaligned partitions, you need to perform a manual backup first and follow the procedure by performing a fresh installation using the latest OVF Template from Unified Contact Center Express Virtual Machine Templates to restore both the nodes, starting with the first node.

Caution Set up a new cluster if you do not have a valid backup for the first node.

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 *Cisco Unified Contact Center Express Install and Upgrade Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 2 Restore only the first node by following the procedure in Restore Only First Node in HA Setup (with Rebuild), on page 8.

Note To view the current license package, go to **System > Licensing > Display License**.

Step 3 Restart the first node.

For more information on restarting, see the *Cisco Unified Operating System Administration Guide* available here: https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_%20list.html.

Caution
- Apply the same license type on node the backup was taken to restore and should be applied for first node only.
- If the License MAC has changed during the rebuild, the UCCX license will need to be rehosted. When applying the new license after the restore process has completed, apply a rehosted license with the same package (Standard, Enhanced, Premium, IP IVR) as the license contained within the backup that was restored. For more information on the licensing rehosting mechanism, see the Installing Cisco Unified Contact Center Express available here: https://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).

Step 5 Restore only the second node by following the procedure in Restore Second Node in HA Setup (with Rebuild), on page 9.

Step 6 Restart the second node. Your data is restored on both the nodes of the cluster.

Trace Files

The trace files for the Master Agent, the user interface, each Local Agent, and the JSch (Java Secure Channel) library are found in 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 user interface, 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 Command Line Interface, on page 11.

Command Line Interface

Cisco DRS also provides command-line access to few backup and restore tasks, as listed in the following table:

Table 1: 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
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

Cisco DRS (DRF) displays alarms for errors that can occur during a backup or restore procedure. The Cisco DRS alarms can be found detailed in the *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager and IM & Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 2: Disaster Recovery System Alarms

Alarm Name	Description
DRFBackupDeviceError	Cisco DRS backup process encountered errors while it was accessing the device.

Alarm Name	Description
DRFBackupFailure	Cisco DRS backup process encountered errors.
DRFBackupInProgress	Cisco DRS cannot start new backup while another backup is still running.
DRFInternalProcessFailure	Cisco DRS internal process encountered an error.
DRFLA2MAFailure	Cisco DRS Local Agent cannot connect to Master Agent.
DRFLocalAgentStartFailure	Cisco DRS Local Agent might be down.
DRFMA2LAFailure	Cisco DRS Master Agent cannot connect to Local Agent.
DRFMABackupComponentFailure	Cisco DRS requested that a component back up its data; however, an error occurred during the backup process, and the backup of the component failed.
DRFMABackupNodeDisconnect	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	Cisco DRS requested that a component restore its data; however, an error occurred during the restore process, and the component was not restored.
DRFMARestoreNodeDisconnect	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	Cisco DRS Master Agent might be down.
DRFNoRegisteredComponent	Cisco DRS backup failed because no registered components are available.
DRFNoRegisteredFeature	No feature was selected for backup.
DRFRestoreDeviceError	Cisco DRS restore process cannot read from device.
DRFRestoreFailure	Cisco DRS restore process encountered errors.
DRFSftpFailure	Errors exist in Cisco DRS SFTP operation.
DRFSecurityViolation	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. DRF Local Agent cannot connect to Master Agent.

Alarm Name	Description
DRFUnknownClient	The DRF Master Agent on the first node received a client connection request from an unknown server outside the cluster. The request was rejected.
DRFLocalDeviceError	DRF is unable to access local device.
DRFBackupCompleted	DRF backed up successfully.
DRFRestoreCompleted	DRF restored successfully.
DRFNoBackupTaken	DRF did not find a valid backup of the current system after an upgrade or migration or fresh install.