Backup and Restore

Backup and Restore

Cisco Finesse uses the backup and restore tools that are provided by the common Cisco Unified Communications platform services for complete data backup-and-restore capabilities. Cisco DRS allows you to perform regularly scheduled automatic or user-invoked data backups and to restore data if the system fails.

To access the Disaster Recovery System (DRS) application, direct your browser to the following URL: https://*Finesse Server IP*:8443/drf, where *Finesse Server IP* is the IP address of your Finesse server.

Note Cisco Finesse does not support One-Step Restore with the DRS application.

In the case of high availability (HA), Cisco DRS performs a cluster-level backup, which means that it collects backups for all servers to Cisco Finesse and archives the backup data to a remote SFTP server.

DRS backs up and restores 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 the SSL-based communication between the Primary Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber nodes. Cisco DRS uses the IPSec certificates for its Public/Private Key encryption. 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 information about the certificate management, see, *Cisco Unified Communications Manager Security Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Important Considerations

Following are the important considerations when you perform the 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 Cisco Finesse. If different nodes are running different versions, you will have a certificate mismatch and your backup or restore fails.
- Before you restore Cisco Finesse, 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 Cisco Finesse, ensure that the 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 Cisco Finesse. 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 Cisco Finesse 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.

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.

Primary and Local Agents

The system automatically starts the Primary Agent service on each node of the cluster, but it is functional only on the first node. Both servers in the Cisco Finesse 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.

Primary Agent Duties

The Primary Agent (PA) performs the following duties:

- Stores system-wide component registration information.
- Maintains a complete set of scheduled tasks in an XML file. The PA updates this file when it receives updates of schedules from the user interface. The PA sends tasks (that can be run) to the applicable Local Agents, as scheduled. Local Agents run 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 the schedules that are run, and performing system restoration.
- Stores backup data on a remote network location.

Local Agent Duties

In the Cisco Finesse 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 Primary Agent and the Local Agent for authentication and encryption of data between the 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:

- Create and manage backup devices
- Create and manage backup schedules
- Perform manual backup and check backup status
- Estimate size of backup tar file
- 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.

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Backup Device**.

Step 3 Click **Add New** to add a new device or click the device name to edit settings of an existing backup device.

Step 4 Enter the backup device name and select destination. For more details on the field description, see the detailed online help provided with the DRS application.

Step 5 Click **Save**.

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.

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Scheduler**.

Step 3 Click **Add New** to add a new schedule or click the schedule name to edit settings of an existing backup schedule.

Step 4 Enter the backup schedule name, select the backup device, and select feature as **`Finesse`**.

Step 5 Enter the backup date and frequency details as required. For more details on the field description, see the detailed online help provided with the DRS application.

Step 6 Click **Save**.

Step 7 Select a schedule from the **Schedule List** and then click **Enable Selected Schedules**.

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 Cisco Finesse 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 a.m. and Shrink-repack on Sunday at 3:00 a.m..

Perform Manual Backup

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Manual Backup**.

Step 3 Select a backup device and feature as **`Finesse`**.

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

Note Click **Estimate Size** to get the approximate size of the disk space that the backup file consumes on the SFTP server.

To perform backup tasks on virtual machines, see *Unified Communications VMware Requirements*, at:https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html.

Check Backup Status

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Current Status** to check the backup status.

Caution The backup to the remote server to be completed within 20 hours otherwise the backup session times out and you will have to start the fresh backup.

Restore the Nodes in HA Setup with Rebuild

In a high availability (HA) setup, if a hard-drive failure or other critical hardware or software failure occurs, you may need to rebuild the primary and the secondary Finesse nodes (publisher and subscriber node). Perform the following steps to restore the Finesse nodes to its last backed up state.

Caution Cisco Finesse data can only be retrieved from the backup file. The recent Finesse configuration data, which is not backed up, must be manually configured in the Cisco Finesse administration console after the restore.

Step 1 Perform a fresh installation of Finesse. Make sure to install the same version of Finesse, using the same administrator credentials, network configuration, and security password that you used for the initial installation.

Step 2 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 3 From the Restore menu, select **Restore Wizard**.

Step 4 Select a backup device. Choose the location where your backup is stored.

Step 5 Select the backup file and feature as **`Finesse`**.

Step 6 When prompted to choose the nodes, either choose both nodes or choose each node to individually restore them.

Step 7 After the restore process is complete, restart the node.

Step 8 Run the following command on the primary Finesse server:

utils dbreplication stop all

Step 9 Run the following CLI command on the primary Finesse server to set up replication:

utils dbreplication reset all

Note The dbreplication reset command can take some time to complete.

Run the CLI command **utils dbreplication runtimestate** on the primary Finesse node. If the RTMT counter value for replication status is 2 on all nodes, replication is functioning properly.

Note After the installation is complete, check that the dbreplication is functioning and allowing the data to propagate from the primary to the secondary node. However, if you need to restore third-party gadgets to the secondary node, you must either upload them again or run the restore process on the secondary node.

Always check the dbreplication status after any restore, using the CLI command **utils dbreplication runtimestate**.