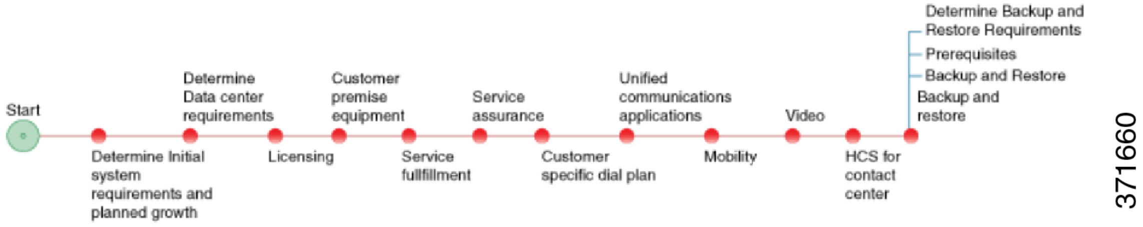
Backup and Restore

Prerequisites

Before you plan the backup and restore processes for your Cisco HCS installation, make sure that you:

- Review and have access to the *Cisco Hosted Collaboration Solution Release 14 Solution Reference Network Design Guide*.
- Review and have access to the *Cisco Hosted Collaboration Solution Release 14 Maintain and Operate Guide*.
- Complete the actions outlined in previous sections of this guide including:
    - Initial system requirements and planned growth
    - Data center requirements
    - Service fulfilment requirements
    - Service assurance requirements
    - Customer specific dial plan
    - Unified Communications Applications
    - Mobility
    - Video
    - HCS for Contact Center

Backup and Restore Workflow


Start
Determine Initial system requirements and planned growth
Determine Data center requirements
Licensing
Customer premise equipment
Service fullfillment
Service assurance
Customer specific dial plan
Unified communications applications
Mobility
Video
HCS for contact center
Backup and restore
Determine Backup and Restore Requirements
Prerequisites
Backup and Restore
371660

Determine Backup and Restore Requirements

Procedure

Step 1 Determine which backup and replication technologies you will use in your system. You may have the following options:

- Consolidated Backup, which is the least expensive option but with the slowest recovery time.
- High availability storage networks--A storage area network (SAN) can overcome local server failures by providing access to a standby or clustered server system to ensure continuous operation.
- Remote point-in-time update replication--Point-in-time update replication copies the changes made to data in another building or city. The system can replicate changes at scheduled times during the day or whenever changes occur. With no latency limitations to overcome, this technology accommodates any distance requirements. It offers faster recovery times than tape backup, but it cannot guarantee zero data loss.
- Synchronous disk replication--Suitable for applications that require the fastest recovery with zero data loss. This method synchronously copies all disk writes to a remote site across a high-performance network before a transaction is acknowledged, eliminating any transaction loss. This technology is sensitive to network latency, which limits the practical distance between sites.
- Asynchronous replication--Offers significantly lower data loss than point-in-time update replication and reduces bandwidth costs compared to synchronous replication. Asynchronous replication allows the primary and remote copies to be out of synchronization by a range of seconds to minutes.

Step 2 Include these operational parameters in your planning:

- Backup frequency--Depends on the frequency of changes in the network. Changes may include platform configurations or user data provisioning activities. Schedule additional backups before any major configuration and software updates.
- Disk space requirements--Calculated by multiplying the frequency of backups and disk space requirements per backup by the number of backups the service provider maintains per UC cluster, as specified in the Service Level Agreement (SLA).

- Backup and restore duration--Depends directly on the amount of disk space required for the backup or restore and the network bandwidth. Frequent backups and restores can adversely affect network traffic performance.
- Input/output operations per second (IOPS)--Used to determine backup demands on the system. The higher the IOPS, the faster that the backups are completed.

Step 3 Determine your FTP server usage. We recommend that you have a dedicated FTP server (or dedicated servers) per UC cluster. Schedule HCS component backups so that they do not overwhelm FTP server input/output operations per second (IOPS) capabilities and available bandwidth.

Step 4 Plan to use the Cisco Disaster Recovery System (DRS) for the Unified Communications applications. Be aware of the following when using DRS:

- Use DRS in coresident mode to back up and restore Unified Communications Manager and Cisco Unity Connection. In the current DRS release, IM and Presence Service servers must be backed up and restored separately.
- Each backup of a UC application is considered as one backup.
- DRS does not delete or overwrite phone images if DRS is used with upgrades, so disk space requirements will vary with each Unified Communications Manager upgrade.
- Consider scheduling backup and restoration tasks during off peak hours.

Step 5 Plan to use Platform Manager in conjunction with DRS for these applications: Cisco Unified Communications Manager IM and Presence Service, Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Contact Center.

Be aware of the following when using DRS:

- When setting up server groups, all of the servers in a particular group must have the same product. For example, you cannot mix Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service nodes in the same server group.
- After you schedule backups on your servers and configure all of your servers and server groups within Platform Manager, you can manage and monitor backup tasks of your system using the Backup Schedule feature to perform DRS backups on groups of servers.

Step 6 You may also use virtual machine (VM) backups. Full VM backups include both the binaries and configuration data, while DRS backs up only the configuration data of the application. For information on how to perform a full VM backup, refer tohttp://www.VMware.com .

VM backup options consist of the following:

- A crash-consistent backup includes an entire virtual machine while it is running, and there is no shutdown of the application for the backup.
- An application-consistent backup includes an entire virtual machine when the VM is powered off, or if the application can and does quiesce before the backup.
- A full VM backup is any backup done on a full virtual machine. It might be crash-consistent or application-consistent.
- The VMware Data Recovery (VDR) feature backs up entire virtual machines, in other words, a full VM backup.

Note Full VM backups are not a replacement for Cisco DRS and are not supported as backup of the application, only as a method to recover the VM quickly without having to deploy from ISO or Template. Customers must take DRS backups to protect and restore the configuration and data within the application.

Step 7 Consider these disk and time requirements for backups:

- Network and data center element backups require 1 to 10 kilobytes of disk space per device.
- Assuming appropriate bandwidth availability (10/100 Mbit/sec or higher), a network and data center element restore can take from 3 to 15 seconds.

Step 8 If using Micro Node deployment, plan for the following:

- Dedicate one or more C-series servers to host FTP servers, using the C-series server disk (local storage) for backup.
- Provide for offsite backup to address Data Center loss.
- You can back up multiple applications to the same FTP server, but do not store a backup on the same server (disk) that hosts the application or component itself.

Backup Strategy

You need to develop a Backup and Restore plan to match your implementation by reviewing the components in your implementation to identify the backup requirements and sequence for backups. Refer to the *Cisco Hosted Collaboration Solution Release 14 Maintain and Operate Guide* to identify the components that are backed up occasionally and those that are backed up daily.

Procedure

Step 1 Group the components in your deployment under the following groups:

- Data Center Infrastructure Components
- Aggregation / Shared Component Elements
- Cisco HCS Service Fulfillment
- Cisco HCS Service Assurance
- Cisco UC Applications
- Endpoints
- SRST and Voice Gateways Components
- Cisco HCS for Contact Center Components
- Third Party Applications

The components in each group have similar backup requirements.

Step 2 Review the component tables in the *Cisco Hosted Collaboration Solution Release 14 Maintain and Operate Guide* to identify and record the backup requirements for the components in your installation.

Step 3 For components that require occasional backup, identify the backup mechanism you will use.

Step 4 For components that require frequent (daily) backup, identify the backup mechanism you will use.