



Backing Up and Restoring a Cisco Unity System

Backup and Restore: Introduction

This chapter explains in general terms how to use third-party backup and restore software or the Cisco Unity Disaster Recovery Tools (also known as DiRT) to back up and restore Cisco Unity data.

When you back up and restore a Cisco Unity server (and one or more Exchange servers) you need to consider the same issues involved in backing up and restoring any other system. (Note that the service packs, Engineering Specials, and Service Releases that are installed on the Cisco Unity server are not significant to the backup and restore process.)



Caution

To back up SQL Server/MSDE data, you need to use the SQL Server agent for your backup software, which allows you to back up open SQL Server/MSDE database files. If you are backing up Exchange data as part of the Cisco Unity backup, you also need to use the Exchange agent for your backup software, which allows you to back up open Exchange database files.

Refer to the following for a list of backup and restore software qualified for use with Cisco Unity, and for the Cisco Unity backup software support policy:

- For the Cisco Unity server—The “Supported Backup Software” section of the *Cisco Unity System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.
- For the Cisco Unity Bridge server—The “Supported Backup Software” section of the *Cisco Unity Bridge System Requirements, and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.

Data That May Be Lost Even If Backups Are Done Properly

If a hard disk in the Cisco Unity server fails, or if the server itself fails or is lost in a disaster, you may still lose some data even with a well-designed and well-executed backup and recovery plan. This section describes the data that may be lost if a hard disk fails, or if a server fails or is lost; the information applies both to backups done with third-party backup and restore software and to backups done with the Cisco Unity Disaster Recovery Tools. See the following sections:

- [Data That May Be Lost If a Hard Disk in a RAID Fails, page 4-2](#)
- [Data That May Be Lost If a Non-RAID Hard Disk Fails, page 4-2](#)
- [Data That May Be Lost If a Server Is Stolen or Destroyed, page 4-3](#)

Data That May Be Lost If a Hard Disk in a RAID Fails

No data is lost if only one disk in the RAID fails, as long as a supported fault-tolerant RAID configuration is implemented. (Cisco Unity does not support non-fault tolerant RAID configurations, in which data could be lost if a single disk failed.) However, if the failure occurs in a RAID 1 array composed of only two disks, there is no fault tolerance until the failed disk has been replaced and the data has been re-mirrored. If the failure occurs in a RAID 5 array, fault tolerance is maintained, but the loss of a disk will cause performance to be severely affected until the failed disk is replaced.

We recommend replacing a defective disk in a RAID with a blank disk to repair the RAID. Replacing disks in a RAID for any other reason is not recommended.

Some sites with multiple RAID 1 arrays use broken mirrors as a form of backup with fallback, by removing one drive before an upgrade or other major procedure so that in the event of a problem, the system could theoretically be restored by using that drive. However, there are serious issues with this approach:

- The capability to use broken mirrors is dependant on the server and RAID configuration. RAID 5 and RAID 10 arrays cannot readily be broken for purposes of data backup.
- Breaking a two-disk RAID 1 mirror leaves the system in a non fault-tolerant state until the mirror is reestablished.
- There is no systematic way to easily and completely stop all application data prior to breaking mirrors, though this is necessary to ensure that all related metadata across multiple arrays is simultaneously and correctly split.
- Broken mirrors may not recover data as expected if used as the only backup and restore method. Re-establishment of multiple RAID arrays in a fallback scenario carries with it a certain amount of risk, and may not be successful, even when the process is tested by using the exact hardware, software, and tools before implementation in a production environment.

Therefore, we do not recommend the use of make/break mirror splits as a form of system backup and recovery.

**Note**

Breaking a two-disk RAID 1 as described in this section is not the same as performing a traditional mirror split. A traditional mirror split involves breaking the relationship between multiple fault-tolerant RAIDs, as in the case of mirrors of multiple mirrors or arrays. Cisco does not provide a traditional mirror split RAID configuration for Cisco Unity servers.

Data That May Be Lost If a Non-RAID Hard Disk Fails

If a non-RAID hard disk fails, you may lose some data if database files and logs are stored on the same hard disk, as follows:

- If the Exchange 5.5 directory or the Active Directory database is stored only on the failed hard disk, you lose all changes to the directory that were made since the last backup (for example, new subscribers, changes to existing subscribers, and deletions of subscribers).
- If both the Cisco Unity SQL Server database and log files are stored on the failed hard disk, you lose all changes to Cisco Unity configuration data that were made since the last backup (for example, call handlers and templates).
- If Cisco Unity is installed on the failed hard disk, you lose changes to greetings and recorded names that were made since the last backup.

- If Cisco Unity is installed on the failed hard disk and if any voice messages were in the Unity Message Repository (UMR) when the hard disk failed (because, for example, the network connection to the partner Exchange server was down), you lose those messages.
- If Windows 2000 Server is installed on the failed hard disk, you lose changes to the registry that were made since the last backup, including some Cisco Unity configuration settings.
- If Cisco Unity subscribers are homed on the failed hard disk on the Cisco Unity server, you lose all changes to the message store for those subscribers that were made since the last backup (for example, new messages, changes to existing messages, and deletions of messages). If messages are not backed up, you lose all messages for those subscribers.
- If the server is backed up by using the Disaster Recovery Tools, refer to the Disaster Recovery Tools Help for a short list of Cisco Unity data that is not saved and is therefore not recoverable (for example, some configuration information and diagnostic and report logs).

Data That May Be Lost If a Server Is Stolen or Destroyed

If the Cisco Unity server is stolen or destroyed and if it contained more than one hard disk, the data loss may be much greater than the data loss caused by failure of a hard disk.

- If the message store directory database is stored only on the Cisco Unity server, you lose all changes to the directory that were made since the last backup (for example, new subscribers, changes to existing subscribers, and deletions of subscribers).
- You lose all changes to Cisco Unity configuration data that were made since the last backup (for example, call handlers, templates, and other data stored in the Cisco Unity SQL Server databases).
- You lose changes to greetings and recorded names that were made since the last backup.
- If any voice messages were in the Unity Message Repository (UMR) (because, for example, the network connection to the partner Exchange server was down), you lose those messages.
- You lose changes to the registry that were made since the last backup, including some Cisco Unity configuration settings.
- If Cisco Unity subscribers are homed on the Cisco Unity server, you lose all changes to the message store for those subscribers that were made since the last backup (for example, new messages, changes to existing messages, and deletions of messages). If messages are not backed up, you lose all messages for those subscribers.
- If the server is backed up by using the Disaster Recovery Tools, refer to the Disaster Recovery Tools Help for a short list of Cisco Unity data that is not saved and is therefore not recoverable (for example, some configuration information and diagnostic and report logs).

Deciding Which Backup and Restore Software to Use

There are many third-party backup and restore software packages—which are sometimes referred to as data protection software packages—available for backing up all of the data on the Cisco Unity server, including SQL Server/MSDE, and Exchange databases and transaction logs.

The Cisco Unity Disaster Recovery Tools are included with Cisco Unity. The Disaster Recovery Tools are used when migrating Cisco Unity from one server to another, but can also be used to back up and restore Cisco Unity data and, optionally, Exchange messages.

We recommend that you use a third-party backup and restore software package to back up a Cisco Unity server rather than the Disaster Recovery Tools. When using the Disaster Recovery Tools:

- Restoring the system may be significantly slower than with third-party software.
- Only the Cisco Unity data is backed up, not the entire server.
- Backup of Exchange messages is problematic (see [Table 4-1](#) for details).

[Table 4-1](#) highlights the major differences between third-party backup and restore software packages and the Cisco Unity Disaster Recovery Tools, in the following categories:

- [Data Restoration Time, page 4-4](#)
- [Data That Can Be Backed Up and Restored, page 4-5](#)
- [Backing Up a Failover System, page 4-5](#)
- [Backing Up Exchange Messages, page 4-5](#)
- [Backing Up the Cisco Unity Bridge, page 4-5](#)
- [Versions of Cisco Unity Supported, page 4-6](#)
- [Cost of the Tools, page 4-6](#)

Table 4-1 *Third-Party Backup and Restore Software vs. the Cisco Unity Disaster Recovery Tools*

Category	Third-Party Backup and Restore Software	Cisco Unity Disaster Recovery Tools
Data Restoration Time	If you back up all of the data on a Cisco Unity server by using third-party backup and restore software, and you later need to replace a non-RAID hard disk or the entire server, you can typically restore all data in a few hours.	If you back up all Cisco Unity data by using the Disaster Recovery Tools, and you later need to replace a non-RAID hard disk or the entire server, you will need to reinstall all of the software that had been installed on the failed disk or server and then restore the Cisco Unity data. This entire process is likely to take about a day.

Table 4-1 Third-Party Backup and Restore Software vs. the Cisco Unity Disaster Recovery Tools (continued)


Category	Third-Party Backup and Restore Software	Cisco Unity Disaster Recovery Tools
Data That Can Be Backed Up and Restored	Third-party backup and restore software can back up every byte of data on a Cisco Unity server, so you can use this backup to restore all data from a failed non-RAID hard disk or to restore the entire contents of a failed server.	<p>The Disaster Recovery Tools back up all Cisco Unity data and, optionally, Exchange messages. (Note that we do not recommend you use the Disaster Recovery Tools to back up Exchange messages. See the “Backing Up Exchange Messages” section on page 4-5 for details.) To restore data that you backed up by using the Disaster Recovery Tools, you will need to reinstall all software on the failed hard disk or server, then restore Cisco Unity data. If you did not back up Exchange messages by using the Disaster Recovery Tools, you also need a separate backup of the Exchange message database.</p> <p>Directory data also appears in the Cisco Unity SQL Server database, and Cisco Unity includes a utility for synchronizing the SQL Server database and the directory. Therefore, even though the Disaster Recovery Tools do not back up the directory files, if the directory is stored on the Cisco Unity server and if you use the Disaster Recovery Tools to back up your data, you can restore the message store directory after you restore Cisco Unity data. Note that only the Cisco Unity subscriber and distribution list information is backed up and subsequently able to be restored to the directory.</p> <p> Caution The synchronization process is extremely time consuming and could add several hours to the recovery process.</p>
Backing Up a Failover System	Recommended.	Supported.
Backing Up Exchange Messages	When you back up Exchange messages by using third-party backup and restore software, the backup of the message database is the same size as the database itself, because third-party backup and restore software backs up the database in one piece.	<p>We do not recommend using Disaster Recovery Tools to back up Exchange messages, other than when you are migrating systems to a new directory or configuration. If you are upgrading from Exchange 5.5 to Exchange 2000/2003 or moving directories, forests, or entire networks, this is the only viable option for moving messages.</p> <p>Note that only Cisco Unity subscriber messages are backed up. Messages for non-subscribers (for example, e-mail accounts on the Exchange server) are not backed up.</p>
Backing Up the Cisco Unity Bridge	You must use third-party backup and restore software to back up data on the Cisco Unity Bridge server.	Not supported.

Table 4-1 *Third-Party Backup and Restore Software vs. the Cisco Unity Disaster Recovery Tools (continued)*

Category	Third-Party Backup and Restore Software	Cisco Unity Disaster Recovery Tools
Versions of Cisco Unity Supported	The use of third-party backup and restore software is supported with Cisco Unity version 2.4(6) and later.	The use of the Disaster Recovery Tools is supported with Cisco Unity version 3.1(1) and later.
Cost of the Tools	If you choose to use third-party backup and restore software and you do not already own the software, you customarily purchase the base software, the associated agent for SQL Server. If you are backing up Exchange data as part of the Cisco Unity backup, you also purchase the associated agent for Exchange. We recommend that you contact the product manufacturer for this information during deployment planning.	The Disaster Recovery Tools are included with Cisco Unity.

Preparing to Back Up and Restore a Cisco Unity Server

To ensure that you will be able to recover all data in the event of a hardware failure or the catastrophic loss of the Cisco Unity server, do the tasks described in the following sections:

- [Optimizing the Location of Database and Log Files on a Multi-Array Cisco Unity Server, page 4-6](#)
- [Documenting the Cisco Unity Installation, page 4-7](#)
- [Monitoring Hard Disks, page 4-7](#)
- [Maintaining an Inventory of Spare Hard Disks and Servers, page 4-8](#)
- [Storing Backup Tapes and Software Required to Reinstall Cisco Unity, page 4-8](#)
- [Installing a Tape Drive, page 4-8](#)
- [Scheduling SQL Server/MSDE Database Backups \(SQL Server Nightly and Weekly Jobs\), page 4-8](#)

Keep in mind that a successful recovery requires an understanding of your site service level agreement for allowable system downtime and your recovery time objective. The recovery time objective should be considered to be in the range of at least several hours, and should be set after completing regular recovery and disaster recovery tests that simulate real-world data loss scenarios, including full and partial data recovery, hardware replacement, and bare-metal disaster recovery. Managing to your site service level agreement for system downtime should include limiting mailbox size, which in turn limits the message store size to one that can be restored within allowable timeframes. Familiarity with procedures for each recovery scenario will also contribute to meeting service level agreement and recovery time objectives.

Optimizing the Location of Database and Log Files on a Multi-Array Cisco Unity Server

To improve performance and to safeguard data if a hard disk fails, the *Cisco Unity Installation Guide* includes information on the hard disk or partition on which to install Windows 2000 Server, Cisco Unity, SQL Server, Exchange, and other required software on supported Cisco Unity servers. In addition, the

Cisco Unity Installation Guide includes instructions for moving databases and transaction logs to different hard disks or partitions. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

Documenting the Cisco Unity Installation

Make a list of the following information, and keep this information up to date when you upgrade Cisco Unity or install new service packs or hot fixes. We also recommend that you keep this information for the partner Exchange server. Put the lists where you can find them quickly in an emergency:

- Specifications on the servers, including:
 - The amount of RAM
 - The processor type and speed
 - The voice card model, if applicable
 - The tape drive brand and model, if applicable
 - The sizes of the hard disks
- The computer (NetBIOS) name
- If you are not using DHCP, the IP address, subnet mask, and default gateway of the server, and the IP addresses of the preferred and alternate DNS servers
- The domain that the server belongs to, if the server is not a domain controller
- The RAID configuration
- Details on hard disk partitions, including volume names and partition size
- A list of software installed on each partition, including exact version numbers (note that backups can only be used to recover data for the exact version of Cisco Unity that was backed up)
- A list of databases and log files stored on each partition
- Contact information for hardware and software vendors

Monitoring Hard Disks

We recommend that you monitor the hard disks in the Cisco Unity server to verify that they are functioning, and to be alerted as soon as possible if they fail. For each server that has been qualified for use as a Cisco Unity server, a monitoring application (for example, Compaq InsightManager, Dell OpenManage IT Assistant and Server Administrator, and IBM Director) is available that you can use to monitor the health of hard disks and other server components. These applications have been qualified for limited use on the Cisco Unity server—they are qualified only for remotely restarting the server. However, some sites have been using other features without encountering any problems.

For more information on monitoring Cisco Unity, see the “[Performance Monitoring](#)” chapter.

Maintaining an Inventory of Spare Hard Disks and Servers

Not all RAID disks are compatible with one another, and only selected servers have been qualified for use as Cisco Unity servers. If you have spare servers that you can cannibalize for parts or that you can convert to a Cisco Unity server in an emergency, you need not maintain an inventory of spare hardware. Or you may want to keep spare parts and even a spare server on hand to speed recovery. Cisco also offers disk and memory field replacement units (FRUs) for its MCS servers.

For detailed information, refer to the *Cisco Unity Supported Platforms List*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

Storing Backup Tapes and Software Required to Reinstall Cisco Unity

We recommend that you store backup tapes at a location separate from your Cisco Unity installation, but preferably near by.

When selecting a fireproof safe or vault for archiving backup media, the most important factor is the internal temperature specification. We strongly recommend consulting with your archival or fire protection vendor for detailed recommendations and safety standards.

If you use the Disaster Recovery Tools to back up Cisco Unity and you need to recover data, you will need to reinstall the software that was installed on the failed hard disk or server before you can begin the recovery process. Store the compact discs for Cisco Unity and related software (Windows 2000 Server, SQL Server 2000, device drivers, and so on), plus a Windows 2000 Server emergency repair disk, in a safe place where you can quickly retrieve them if necessary.



Caution

Store all software in a safe place regardless of the backup software you are using. For example, you may not be aware that a backup failed, and you may need to reinstall all software even if you are using third-party backup and restore software to do full backups.

Installing a Tape Drive

If the Cisco Unity server is not connected to the network, install a tape drive in the server. If the server is connected to the network, you can install the tape drive or another backup device almost anywhere, though the server used for backup must have a Fast Ethernet or Gigabit Ethernet connection path to the Cisco Unity server.

Scheduling SQL Server/MSDE Database Backups (SQL Server Nightly and Weekly Jobs)

By default, a differential backup of the Cisco Unity SQL Server/MSDE database occurs daily, Monday through Saturday, at 2:00 a.m., and a full backup occurs every Sunday at 3:00 a.m. Do the following procedure to confirm that the SQL Server/MSDE database backup does not overlap the backup of the Cisco Unity server.

To Confirm or Change the Scheduled Time of the Cisco Unity SQL Server/MSDE Database Backup

Step 1 On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.

- Step 2** In the left pane, expand **Microsoft SQL Servers > SQL Server Group > <ServerName> > Management > SQL Server Agent**, and click **Jobs**.
- Step 3** In the right pane, right-click **SqlNightlyBackupJob**, and click **Properties**.
- Step 4** Click the **Schedules** tab.
- Step 5** To change the schedule, click **Edit**.
- Step 6** In the Edit Job Schedule dialog box, click **Change**.
- Step 7** In the Edit Recurring Job Schedule dialog box, change the schedule as applicable.
- Step 8** Click **OK** three times to save your changes.
- Step 9** Repeat [Step 3](#) through [Step 8](#) for **SqlWeeklyBackupJob**.
-

Backing Up the Cisco Unity Server by Using Third-Party Software

The following sections provide detailed information about using third-party backup and restore software to back up the Cisco Unity server:

- [General Requirements for Using Third-Party Backup and Restore Software, page 4-9](#)
- [Installing Third-Party Backup and Restore Software, page 4-10](#)
- [Choosing a Backup Method and a Media Rotation Method, page 4-10](#)
- [Ensuring That Exchange Transaction Logs Are Not Overwritten, page 4-11](#)
- [Additional Information About Backing Up the Exchange Databases and Mailboxes, page 4-11](#)
- [Backing Up the Cisco Unity Server: Third-Party Software, page 4-12](#)
- [Backing Up Separate Message Store Servers, page 4-12](#)
- [Backing Up a Cisco Unity Bridge Server: Third-Party Software, page 4-12](#)
- [Backing Up Cisco Unity Servers Configured for Failover, page 4-13](#)
- [Scheduling Backups: Third-Party Software, page 4-14](#)

General Requirements for Using Third-Party Backup and Restore Software

- A supported version of the third-party backup and restore software. Refer to the “Supported Backup Software” section of the *Cisco Unity System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm. Use of third-party backup and restore software not specifically listed as supported is addressed in the “Support Policy for Backup Software” section of the *Cisco Unity System Requirements, and Supported Hardware and Software* document.
- Third-party backup and restore software Agent for Exchange Server (if Exchange is installed on the Cisco Unity server or if you want to back up the Exchange and Cisco Unity servers together).
- Third-party backup and restore software Agent for SQL Server (also required for MSDE).
- A backup device (for example, a tape drive) and backup media (for example, tapes) compatible with the backup device.

In addition, note the following:

- If the backup device is not installed on the Cisco Unity server, the third-party backup and restore software remote access agent is required.
- Do not use the third-party backup and restore software open file feature, as it is suitable only for simple file system open file operations. The open file feature cannot reliably back up all application data.
- Do not attempt to back up a corrupted Cisco Unity database. A backup of a corrupted database cannot be used to restore a Cisco Unity server.

Installing Third-Party Backup and Restore Software

Install third-party backup and restore software and the third-party backup and restore software agents for Microsoft SQL Server (also required for MSDE) and for Exchange on the server on which the tape drive or other backup device is installed. If the backup device is not installed on the Cisco Unity server, install the third-party backup and restore software remote access agent for Windows NT/2000 on the Cisco Unity server. You may need to reboot the server after you install the software. For more information, refer to the manufacturer documentation.

Choosing a Backup Method and a Media Rotation Method

Third-party backup and restore software offers a number of backup methods, including backing up all files (full or normal backups), and various methods of backing up files that have changed since the last backup (differential and incremental backups). Full or normal backups include all specified files, regardless of when they were last modified or backed up. Differential backups include all files that changed since the last full backup. Incremental backups include only the files that changed since the last backup of any kind. As you choose a backup method, keep in mind how your choice affects the restore process:

- If you always do full backups, you will need to restore only the most recent full backup to completely restore the system.
- If you do both full backups and differential backups, you only need to restore the most recent full backup plus the most recent differential backup.
- If you do both full backups and incremental backups, you need to restore the most recent full backup plus all subsequent incremental backups. The more incremental backups you have done since the last full backup, the longer it will take you to get Cisco Unity working again.



Note

Incremental backup is the only partial backup method that resets the archive bit (an NTFS file attribute). Differential backups do not reset the archive bit, so all files that have changed since the last full backup are backed up, not just those that have changed since the last incremental backup. Differential backups may take longer than incremental backups. However, having a differential backup will save time in the event of a restore, because you will need to restore only the last full and the last differential backups.

Third-party software documentation typically includes a definition of backup methods offered and information on how to choose among them according to your circumstances. We recommend that you read the documentation prior to choosing a backup method.

Closely tied with the backup method is the media rotation method. When you choose a media rotation method, do the following:

- Choose the backup method to use each day (for example, differential backups Monday through Thursday and full backups on Friday).
- Determine how much backup media (for example, number of tapes) are required each day for the selected backup method (for example, one tape each day for the differential backups, three tapes on Friday for the full backup).
- Choose how often the backup media are rotated out of the backup device and taken to an offsite storage location.

Ensuring That Exchange Transaction Logs Are Not Overwritten

When a new message arrives, it is saved in a transaction log and then is copied from the log to the message store when system resources are available. If the message store is corrupted or destroyed, you can restore the last backup of the message store and then apply the contents of the transaction log to the restored message store (if the transaction log was stored in a different location than the message store and therefore was not destroyed along with the message store).

After you back up the message store by using Exchange-aware backup software, the backup software clears the transaction logs. At this point, the backup reflects the current state of the message store, so the transaction logs are no longer required to restore the message store.

You can configure logging in one of two ways: either the existing logs are regularly overwritten, or the existing logs are never overwritten. Overwriting the existing logs is known as circular logging.



Caution

If you turn circular logging on, the newest transaction log entries (which contain the newest messages) overwrite the oldest log entries (the oldest messages). When log entries are overwritten, you cannot use the transaction logs to restore messages that were received after the last backup. If disk space is very low and if the system is very busy, the overwriting of older messages can begin in less than a day of logging.

We strongly recommend that you do the following:

- Turn circular logging off.
Note that circular logging is turned off by default in Exchange 2000 and 2003, but is turned on by default in Exchange 5.5.
- Use Exchange-aware backup software to back up the message store.
- Carefully watch the amount of available space on the hard disk or in the partition where logs are stored, and free up disk space when the amount of available space gets too low.

Additional Information About Backing Up the Exchange Databases and Mailboxes

When you select the information store and the directory store databases for backup, mailboxes and messages are included in the backup. You can also select one or more messages, mailboxes, or folders for backup without selecting the databases.

However, we recommend that you do not back up mailboxes separately from the databases without running a test backup to determine the performance impact. Mailbox backups will generally take longer than database backups, and mailbox backups will be as large as or larger than the database backups.

Backing up individual mailboxes should not be used as a substitute for backups of the entire information store database. For a full recovery of an Exchange server, you will need a backup of the information store database.

Note that the Exchange .edb and .log files are backed up only when the Exchange databases are backed up.

Backing Up the Cisco Unity Server: Third-Party Software

Note the following stipulations for backing up the Cisco Unity server. For more information, refer to the third-party backup and restore software Help.

- Back up all data on all drives on the Cisco Unity server. Having backups of all data will reduce the amount of time required to get Cisco Unity running again if a non-RAID hard disk fails or if the Cisco Unity server is stolen or destroyed. Refer to the third-party backup and restore software documentation for detailed instructions on backing up data for your configuration.
- Do online backups only. If you are using third-party backup and restore software, the online backup requirement means that you need to purchase and use the third-party backup and restore software agents for Exchange and for SQL Server, which allow you to back up open database files. Do not use the third-party backup and restore software open file feature for backing up open files. (Note that offline backups are supported for the Cisco Unity Bridge. See the [“Backing Up a Cisco Unity Bridge Server: Third-Party Software”](#) section on page 4-12.)
- Configure the third-party software to verify the backup, which ensures that the backup tape or other media can be read after the backup is finished.
- Back up all data on the Cisco Unity server both before and after you install or upgrade any software on the server.

Note that backing up Cisco Unity does not require custom settings in third-party backup and restore software. For information on any special backup requirements associated with third-party software that is installed on the Cisco Unity server (for example, virus-scanning software), refer to the manufacturer documentation.

Backing Up Separate Message Store Servers

If Cisco Unity is configured for Voice Messaging Only and if Exchange is installed on a separate server, back up the separate Exchange server by using the recommendations in the third-party backup and restore software documentation.

If Cisco Unity is configured for Unified Messaging, back up the Exchange servers on which Cisco Unity subscribers are homed by using the same backup procedures that you use to back up all Exchange data.

Backing up an Exchange server that includes Cisco Unity voice messages (and, for Exchange 5.5, directory information) does not require any custom settings in third-party backup and restore software.

Backing Up a Cisco Unity Bridge Server: Third-Party Software

Use third-party backup and restore software to back up data on the Cisco Unity Bridge server. The Disaster Recovery Tools are not supported for use with the Bridge.

Both offline and online backups are supported for the Cisco Unity Bridge server. When backing up the Bridge server, you need to back up only the configuration files.

Do one of the following procedures, as applicable to your site:

- [To Do an Online Backup of the Bridge server by Using Third-Party Backup and Restore Software, page 4-13](#)
- [To Do an Offline Backup of the Configuration Files on the Bridge Server, page 4-13](#)

To Do an Online Backup of the Bridge server by Using Third-Party Backup and Restore Software

- Step 1** Do the backup of the configuration files during off-peak hours if possible. No unique software agents are required.

For detailed instructions, refer to the manufacturer documentation or Help.

To Do an Offline Backup of the Configuration Files on the Bridge Server

- Step 1** On the Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:

- Digital Networking
- Unity Bridge

Any calls that are in progress are allowed to finish before the services are stopped.

- Step 2** Back up the following directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)



Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

- Step 3** On the Windows Start menu, click **Programs > Administrative Tools > Services**, and start the following services:

- Digital Networking
- Unity Bridge

- Step 4** Close the Services window.
-

Backing Up Cisco Unity Servers Configured for Failover

The procedure for backing up a secondary (failover) server is the same procedure used to back up the primary server. Choose either third-party backup and restore software or the Cisco Unity Disaster Recovery Tools, and refer to Help for detailed instructions for doing backups. In a failover configuration, neither the primary nor the secondary server backup includes messages, which are held on a separate

message store server. Consequently, backing up data on the secondary server does not replace a comprehensive strategy for backing up and restoring messages on other servers that are part of the Cisco Unity system.

Note that a backup of the primary server has SQL replication links that will be broken if this data is restored to a new server, thus requiring an extra procedure to clean up the broken SQL links.

Backup data produced by using third-party backup and restore software is typically associated with the specific server that the data was backed up from, unless a virtual server name is used. If a secondary server backup occurs after a primary server fails over, the data in the secondary server backup will be associated with the primary server. You may be required to recover data associated with the primary server.

We recommend that you set up regularly scheduled backups of both primary and secondary servers. Do not make changes in the Cisco Unity Administrator, or record greetings or subscriber names, while backups are being created. For additional details on scheduling backups, see the [“Scheduling Backups: Third-Party Software”](#) section on page 4-14 or the [“Scheduling Backups: Cisco Unity Disaster Recovery Tools”](#) section on page 4-15, as applicable.

Scheduling Backups: Third-Party Software

Third-party backup and restore software generally includes options for scheduling backups to occur automatically at a specified time. Select a time when the Cisco Unity server is processing a low volume of calls (for example, after the end of the regular business day), and when there are no other processes running (for example, do not schedule a backup concurrently with running a virus scan or generating reports). If you are using the Cisco Unity Bridge or AMIS, schedule backups for a time that will not overlap with message delivery.

Depending on how much data needs to be backed up, and in a failover configuration, whether you are backing up all data on the primary and secondary servers, the backup could take several hours. When scheduling backups, allow enough time for the backup to finish before the beginning of the next business day, at which time Cisco Unity again becomes busy answering calls.



Caution

If the Cisco Unity server is scheduled to reboot periodically, ensure that the reboot does not occur during the time when the server is being backed up. If the server reboots during a backup, the backup will not be complete.

Backing Up Cisco Unity Data by Using the Cisco Unity Disaster Recovery Tools

The Cisco Unity Disaster Recovery Tools are available in the Cisco Unity Tools Depot, which you can access from the Cisco Unity Tools Depot icon on the Windows desktop. For detailed instructions on using the Cisco Unity Disaster Recovery Tools to back up Cisco Unity data, including a link to downloadable training videos, refer to the Disaster Recovery Tools Help.

Cisco Unity must be running before you can use the Disaster Recovery Tools to back up or restore data. Do not shut down Cisco Unity or other software on the Cisco Unity server before you do a backup.

The following sections provide information about using the Cisco Unity Disaster Recovery Tools to back up the Cisco Unity server:

- [Requirements for Using the Cisco Unity Disaster Recovery Tools, page 4-15](#)

- [Obtaining the Latest Version of the Cisco Unity Disaster Recovery Tools, page 4-15](#)
- [Scheduling Backups: Cisco Unity Disaster Recovery Tools, page 4-15](#)

Requirements for Using the Cisco Unity Disaster Recovery Tools

- Cisco Unity version 3.1(1) or later.
- Use the most recent version of the tools, available at http://www.CiscoUnityTools.com/App_DisasterRecoveryTools.htm.
- The installation disks for all of the software on the failed hard disk or server. The Disaster Recovery Tools back up only data, not applications, so you need to reinstall all of the software before you can restore Cisco Unity data.
- To restore data on a Cisco Unity version 4.0 or later system, you need either the current Cisco Unity license file(s) (if you are not replacing the Cisco Unity server) or new license files (if you are replacing the Cisco Unity server). The license files are associated with the MAC address on the server, and a new server will have a new MAC address, which requires an updated license file.
- You can restore a Cisco Unity backup onto a clean install of the same version of Cisco Unity that is connected to a different version of Microsoft Exchange than what was in use when the backup was made. For example, migrating from Exchange 5.5 to Exchange 2000 or 2003, on or off-box, is supported.
- Restoring a Cisco Unity backup after changing from one message store to another is not supported.



Caution

Do not attempt to back up a corrupted Cisco Unity database. A backup of a corrupted database cannot be used to restore a Cisco Unity server.

Obtaining the Latest Version of the Cisco Unity Disaster Recovery Tools

The Disaster Recovery Tools are shipped with Cisco Unity. Updates to the Disaster Recovery Tools are periodically made available for download from the Cisco Unity Tools website at http://www.CiscoUnityTools.com/App_DisasterRecoveryTools.htm.

Download both the Disaster Recovery Backup and the Disaster Recovery Restore Tools. Install the new version of the tools in the existing directories. By default, these directories are `CommServer\Utilities\DisasterRecoveryBackup` and `CommServer\Utilities\DisasterRecoveryRestore`, and are on the hard disk on which Cisco Unity is installed.

Scheduling Backups: Cisco Unity Disaster Recovery Tools

The Disaster Recovery Tools include options for scheduling backups to occur automatically at a specified time. Select a time when the Cisco Unity server is not busy, for example, when the call volume is low and when no other processes such as virus-scanning or reports are running.

Before using the Disaster Recovery Tools to schedule regular backups of Cisco Unity data, do one successful manual backup. This helps ensure that you will find any problems before you start doing scheduled backups (for example, determining that the account under which the Disaster Recovery Tools runs has insufficient permissions).

**Caution**

If the Cisco Unity server is scheduled to restart periodically, ensure that the restart does not occur during the time when the server is being backed up. If the server reboots during a backup, the backup will not be complete.

Testing Backup and Restore

We recommend that you thoroughly test backing up and restoring your Cisco Unity servers in a test environment before using the backup and restore software on a production system.

To ensure that your backups can be used to successfully restore a failed non-RAID hard disk (if the server contains non-RAID disks) or a server, do the following procedure.

To Test Backup and Restore of the Cisco Unity Server

- Step 1** Back up the Cisco Unity server, and note the amount of time required for the backup.
- Step 2** For a configuration in which Exchange is installed on a separate server, back up the Exchange server.
- Step 3** Verify that the schedule you set in the third-party backup and restore software or in the Disaster Recovery Tools allows sufficient time for the backup to complete before the next business day, and that the backup medium has sufficient storage space.

**Note**

If this is a new installation with little data in the SQL Server and in the Exchange databases, subsequent backups will probably be much larger and take significantly longer after the server has been in service for a while.

If you are using third-party backup and restore software, refer to the manufacturer documentation for backup performance optimization information.

- Step 4** Check the event log for backup-related errors.
- Step 5** To test restoring data in the event of a failed non-RAID hard disk, replace a hard disk in the Cisco Unity server (and in the separate Exchange server, if applicable) and restore data by following the steps in the applicable section:
 - [Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using Third-Party Backup and Restore Software, page 4-17](#)
 - [Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-18](#)
- Step 6** Verify that Cisco Unity is answering calls and taking messages.
- Step 7** To test restoring data in the event of a catastrophically failed server, do the following sub-steps:
 - a. Disconnect the existing Cisco Unity server from the network.
 - b. Select a test server that has the same hard disk configuration as the Cisco Unity server.
 - c. Restore data onto the test server by following the steps in the applicable section:
 - [Replacing a Failed Cisco Unity Server and Restoring Data by Using Third-Party Backup and Restore Software, page 4-20](#)

- [Replacing a Failed Cisco Unity Server and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-20](#)
 - [Replacing a Failed Cisco Unity Bridge Server and Restoring the Bridge Configuration Files, page 4-21](#)
 - [Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using Third-Party Backup and Restore Software, page 4-22](#)
 - [Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-28](#)
- d. Verify that the test server is answering calls and taking messages.
 - e. Disconnect the test server from the network and reconnect the Cisco Unity server.
-

Replacing a Failed Hard Disk and Restoring Data

Use the procedure in the applicable section:

- [Replacing a Failed Hard Disk in a RAID, page 4-17](#)
- [Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using Third-Party Backup and Restore Software, page 4-17](#)
- [Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-18](#)

Replacing a Failed Hard Disk in a RAID

If a hard disk in a RAID fails, all you need to do is replace the disk. The RAID controller automatically ensures that the correct data is restored to the new hard disk.

To Replace a Failed Hard Disk in a RAID

-
- Step 1** If you do not already have a new, blank hard disk that is compatible with the other disks in the RAID, get one from the server manufacturer or the vendor from whom you purchased the server.
 - Step 2** When the new hard disk is available, follow the manufacturer instructions to remove the failed disk from the server.
 - Step 3** Insert the new hard disk in the server.
-

Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using Third-Party Backup and Restore Software

To Replace a Failed Non-RAID Hard Disk and Restore Data by Using Third-Party Backup and Restore Software

-
- Step 1** Exit the Cisco Unity software, and then shut down the server.

- Step 2** Disconnect the server from the network.
- Step 3** Replace the hard disk according to the instructions provided by the manufacturer.
- Step 4** If the server contains only one hard disk, install Windows 2000 Server on the new hard disk by following the instructions in the *Cisco Unity Installation Guide*. Configure the server as a workgroup. Do not join a domain. Do not install Active Directory at this time. These configured attributes will return when the restoration is complete.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 5** Install onto the new hard disk the third-party backup and restore software that was installed on the failed hard disk, including the agents for SQL Server, Exchange, or the remote access agent for Windows NT/2000, as applicable.

If the server contains more than one hard disk, you can install the software and agents on the new disk, or on any other hard disk in the server.

- Step 6** Restore the remaining contents of the disk from the backup medium by following the instructions in the manufacturer documentation.



Caution If Active Directory, Microsoft SQL Server, MSDE, or Exchange were installed on the failed hard disk, carefully follow the manufacturer instructions for restoring those applications and their data.

- Step 7** Reconnect the server to the network.

Replacing a Failed Non-RAID Hard Disk and Restoring Data by Using the Cisco Unity Disaster Recovery Tools

If the hard disk that failed was the hard disk that contained Cisco Unity, and if you used the Cisco Unity Disaster Recovery Tools to back up the Cisco Unity data (and possibly the Exchange data) on the disk, reinstall all software that was installed on the hard disk that failed. Depending on how many hard disks are installed in the server and how software was divided among them, this may include, in addition to Cisco Unity:

- Windows 2000 Server
- Exchange 2000 or 2003, or Exchange 5.5
- SQL Server 2000 or MSDE 2000
- The service packs and other software required by your version of Cisco Unity

To Replace a Failed Non-RAID Hard Disk and Restore Data by Using the Cisco Unity Disaster Recovery Tools

- Step 1** If the server is running, exit the Cisco Unity software, and then shut down the server.
- Step 2** Disconnect the server from the network.
- Step 3** Replace the hard disk according to the instructions provided by the manufacturer.

- Step 4** Follow the instructions in the *Cisco Unity Installation Guide* to reinstall all of the software that was installed on the failed hard disk. Take note of the following:
- If Cisco Unity was installed on the failed hard disk, you must reinstall the exact version of Cisco Unity that was installed before the hard disk failed.
 - If the failed hard disk contained only some of the software that is required on a Cisco Unity server (for example, only Windows 2000 Server and the Cisco Unity software), reinstall only that software on the new hard disk.
 - Do not do the procedures from the *Cisco Unity Installation Guide* for customizing the Cisco Unity system.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 5** If you reinstalled Exchange 5.5 on the failed hard disk in [Step 4](#), disable circular logging. (In Exchange 2000 and 2003, circular logging is disabled by default.)
- Step 6** Reconnect the server to the network.
- Step 7** Confirm that Cisco Unity is up and running. (Note that successfully creating or importing a test subscriber using the Cisco Unity Administrator, leaving a message for the subscriber, confirming that their MWI goes on, retrieving the message, and then deleting the subscriber, confirms that the basic Cisco Unity functionality is working.)
- Step 8** If Cisco Unity was installed on the failed hard disk, restore Cisco Unity data by using the Disaster Recovery Tools. For information on using the Disaster Recovery Tools to recover data, refer to the Disaster Recovery Tools Help.

Replacing a Failed Cisco Unity Server and Restoring Data

If you are replacing a failed Cisco Unity server, and restoring data, use the procedure in the applicable section:

- [Replacing a Failed Cisco Unity Server and Restoring Data by Using Third-Party Backup and Restore Software, page 4-20](#)
- [Replacing a Failed Cisco Unity Server and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-20](#)

If you are replacing a failed Cisco Unity Bridge server, or Cisco Unity with Failover, use the procedures in the applicable section:

- [Replacing a Failed Cisco Unity Bridge Server and Restoring the Bridge Configuration Files, page 4-21](#)
- [Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using Third-Party Backup and Restore Software, page 4-22](#)
- [Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using the Cisco Unity Disaster Recovery Tools, page 4-28](#)

For information specific to doing authoritative restores of Active Directory, see the “[Authoritative Restores of Active Directory](#)” section on page 4-29.

For information specific to recovery of a Microsoft SQL server, see the “Additional Information About SQL Server Recovery” section on page 4-30.

Replacing a Failed Cisco Unity Server and Restoring Data by Using Third-Party Backup and Restore Software

To Replace a Failed Cisco Unity Server and Restore Data by Using Third-Party Backup and Restore Software

Step 1 Set up the new Cisco Unity server (install voice cards if applicable, and plug everything in) by using the instructions in the “Setting Up the Hardware” chapter of the *Cisco Unity Installation Guide*.

If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server, and install the associated driver.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

Step 2 Install Windows 2000 Server on the new server by using the instructions in the *Cisco Unity Installation Guide*.

Configure the server as a workgroup. Do not join a domain. Do not install Active Directory at this time. These configured attributes will return, if applicable, when the restoration is complete.

Step 3 Install new Cisco Unity license files.



Note For information about obtaining or updating license files, refer to the *White Paper: Licensing for Cisco Unity (All Versions)*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpapr/licenses.htm.

Step 4 Restore the remaining contents of the server from the backup medium by following the instructions in the third-party software documentation.



Caution If Active Directory, Microsoft SQL Server, MSDE, Domino, or Exchange were installed on the failed server, carefully follow the instructions for restoring those applications and their data.

Replacing a Failed Cisco Unity Server and Restoring Data by Using the Cisco Unity Disaster Recovery Tools

If you used the Cisco Unity Disaster Recovery Tools to back up the Cisco Unity data (and possibly the Exchange or Domino data) on the disk, you need to reinstall all of the software that was installed on the Cisco Unity server at the time of the failure.

To Replace a Failed Cisco Unity Server and Restore Data by Using the Cisco Unity Disaster Recovery Tools

- Step 1** Follow the instructions in the Cisco Unity Installation Guide to set up the new Cisco Unity server and reinstall all software, including replacement Cisco Unity license files.



Caution You must reinstall the exact version of Cisco Unity that was installed before the server failed.

If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server, and install the associated driver.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 2** If you installed Exchange 5.5 on the Cisco Unity server in [Step 1](#), disable circular logging. (In Exchange 2000 and 2003, circular logging is already disabled by default.)
- Step 3** Confirm that Cisco Unity is up and running. (Note that successfully creating or importing a test subscriber using the Cisco Unity Administrator, leaving a message for the subscriber, confirming that their MWI goes on, retrieving the message, and then deleting the subscriber, confirms that the basic Cisco Unity functionality is working.)
- Step 4** Restore Cisco Unity data by using the Disaster Recovery Tools. For information on using the Disaster Recovery Tools to recover data, refer to the Disaster Recovery Tools Help.

Replacing a Failed Cisco Unity Bridge Server and Restoring the Bridge Configuration Files

When replacing a failed Bridge server, you install the Bridge software and then restore the configuration files.

To Replace a Failed Bridge Server and Restore the Bridge Configuration Files

- Step 1** Install the new Bridge server according to the instructions in the “Overview of Mandatory Tasks for Installing the Cisco Unity Bridge” chapter of *Cisco Unity Bridge Installation Guide, Release 3.0*, which is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/big30/index.htm.
- Step 2** After the post-installation restart, on the Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:
- Digital Networking
 - Unity Bridge
- Step 3** Restore the following directories from the backup medium:
- SN (include all files and subdirectories)
 - Starfish\Db\StarFish.mdb
 - VPIM\Vpim.cfg

- VPI\M\Propagation (include all files and subdirectories)



Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

- Step 4** On the Windows Start menu, click **Programs > Administrative Tools > Services**, and start the following services:
- Digital Networking
 - Unity Bridge
- Step 5** Close the Services window.

Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using Third-Party Backup and Restore Software

This section describes how to replace a failed server and restore data, when failover is configured, according to the following scenarios:

- Restoring the primary server from a backup of the primary server
- Restoring the secondary server from a backup of the secondary server
- Restoring the secondary server from a backup of the primary server

When failover is configured, server backups include replicated and non-replicated data. For example, replicated data includes SQL and Cisco Unity data; non-replicated data includes Cisco Unity software patches (Engineering Specials) and changes to server registry settings.

When restored, the primary and secondary servers are restored to the point at which the server backup that was used for the restoration was made. Changes made to Cisco Unity after the backup and prior to the restoration will be lost.

Note that if you restart the primary and secondary servers while automatic failover and failback are disabled, both servers start as inactive, and therefore Cisco Unity is unable to take calls.

Do the procedures in one of the following sections, according to the needs of your site:

- [Replacing Only a Failed Primary Server and Restoring Data by Using Third-Party Backup and Restore Software, page 4-23](#)
- [Replacing Only a Failed Secondary Server and Restoring Data by Using Third-Party Backup and Restore Software, page 4-25](#)
- [Replacing Both Failed Primary and Secondary Servers at the Same Time and Restoring Data by Using Third-Party Backup and Restore Software, page 4-26](#)

The scope of this document is limited to the replacement and restoration of one or both of the primary and secondary servers in a failover configuration. Converting a secondary server into a primary server and the primary server into a secondary server as a part of the restoration process is not a supported recovery strategy. For information on converting a single remaining server to a regular server without failover, refer to the “Converting the Primary Server to a Permanent Regular Cisco Unity Server Without Failover” section in the “Replacing or Converting a Cisco Unity Server” chapter of the *Cisco Unity Reconfiguration and Upgrade Guide*, available at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/rug/ex/index.htm. You can use your third-party backup in place of the Disaster Recovery Tool backup specified in these procedures.

Replacing Only a Failed Primary Server and Restoring Data by Using Third-Party Backup and Restore Software

Use the following procedures to replace the primary Cisco Unity server in a failover configuration and restore data, when the secondary server is active and the primary server is unable to function. In this circumstance, the replacement primary server will have the IP address and server name of the original primary server. Changes made after the last backup, while the secondary server is active and the primary server is off line, are not replicated to the primary server. Therefore, the system will be restored to the point at which the last primary server backup was made. The Cisco Unity data and SQL Server database from the restored primary server will then be replicated to the secondary server.

Note that an interruption of the voice messaging service occurs during the final steps of the following procedures. During the interruption of service, callers and subscribers will not be able to record or listen to voice messages.

To Stop Data Replication on the Secondary Server

-
- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
 - Step 2** Click **Configure**.
 - Step 3** In the Failback Type field of the Failover Configuration dialog box, click **Manual**.
 - Step 4** Click **OK** to close the Failover Configuration dialog box.
 - Step 5** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 6** In the right pane, double-click **AvCsNodeMgr**.
 - Step 7** On the General tab, click **Stop**.
 - Step 8** In the Startup Type list, click **Disabled**.
 - Step 9** Click **OK**.
 - Step 10** Close the Services window.

**Caution**

When the Node Manager service is disabled, changes made to Cisco Unity files in the Localize\DefaultConfiguration, Localize\Prompts, and Support directories from this point on will not be replicated to the primary server. However, files in the UnityMTA and Stream Files directories are replicated when normal failover operation resumes.

To Replace a Failed Primary Server, Restore Data by Using Third-Party Backup and Restore Software, and Reconfigure Failover

-
- Step 1** On the primary server, if the server is running, exit the Cisco Unity software, and then shut down the server.
 - Step 2** Disconnect the primary server from the network.
 - Step 3** Set up the new Cisco Unity server (install voice cards if applicable, and plug everything in) by using the instructions in the “Setting Up the Hardware” chapter of the *Cisco Unity Installation Guide*.

If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server, and install the associated driver.

**Note**

The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

Step 4 Install Windows 2000 Server on the new server by using the instructions in the *Cisco Unity Installation Guide*.

Step 5 Install new Cisco Unity license files.

**Note**

For information about obtaining or updating license files, refer to the *White Paper: Licensing for Cisco Unity (All Versions)*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitapr/licenses.htm.

Step 6 Restore the remaining contents of the server from the most recent primary server backup by following the instructions in the third-party software documentation.

**Caution**

If Active Directory, Microsoft SQL Server, MSDE, Domino, or Exchange were installed on the failed server, carefully follow the instructions for restoring those applications and their data.

Step 7 Continue with the “[To Repair Broken SQL Replication Links After Restoring Data From a Primary Server Backup](#)” procedure on page 4-24.

To Repair Broken SQL Replication Links After Restoring Data From a Primary Server Backup

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.
- Step 2** In the left pane, expand **Microsoft SQL Servers > SQL Server Group > <Server Name>**.
- Step 3** Right-click the **Replication** directory, and click **Configure Publishing, Subscribers, and Distribution**. A wizard opens.
- Step 4** On the Welcome page, click **Next**.
- Step 5** On the Select Distributor page, click **Next**.
- Step 6** On the Snapshot Folder page, click **Next**.
- Step 7** On the Customize the Configuration page, click **Next**.
- Step 8** On the Completing page, click **Finish**.
- Step 9** Right-click the **Replication** directory, and click **Disable Publishing**. A wizard opens.
- Step 10** On the Welcome page, click **Next**.
- Step 11** On the Disable Publishing page, click **Next**.
- Step 12** On the Completing page, click **Finish**.
- Step 13** On the SQL Enterprise Manager dialog box, click **Console > Exit**.
- Step 14** On the primary server, disable automatic failover and failback.
- Step 15** On the primary server, run the failover configuration wizard to enable automatic failover and failback.

- Step 16** On the secondary server, run the failover configuration wizard to enable automatic failover and failback.



Note Refer to the *Cisco Unity Failover Configuration and Administration Guide* for detailed configuration instructions. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fail401/ex/index.htm.

Replacing Only a Failed Secondary Server and Restoring Data by Using Third-Party Backup and Restore Software

Use the following procedures to replace the secondary Cisco Unity server in a failover configuration, when the primary server is active and the secondary server is unable to function. In this circumstance, the replacement secondary server will have the IP address and server name of the original secondary server. After the secondary server is restored, the Cisco Unity data and SQL Server database from the primary server will be automatically replicated to the secondary server.

Note that an interruption of the voice messaging service occurs during the final steps of the following procedures. During the interruption of service, callers and subscribers will not be able to record or listen to voice messages.

To Stop Data Replication on the Primary Server

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Configure**.
- Step 3** In the Failback Type field of the Failover Configuration dialog box, click **Manual**.
- Step 4** Click **OK** to close the Failover Configuration dialog box.
- Step 5** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 6** In the right pane, double-click **AvCsNodeMgr**.
- Step 7** On the General tab, click **Stop**.
- Step 8** In the Startup Type list, click **Disabled**.
- Step 9** Click **OK**.
- Step 10** Close the Services window.



Caution When the Node Manager service is disabled, changes made to Cisco Unity files in the Localize\DefaultConfiguration, Localize\Prompts, and Support directories from this point on will not be replicated to the secondary server. However, files in the UnityMTA and Stream Files directories are replicated when normal failover operation resumes.

To Replace a Failed Secondary Server, Restore Data by Using Third-Party Backup and Restore Software, and Reconfigure Failover

-
- Step 1** On the secondary server, if the server is running, exit the Cisco Unity software, and then shut down the server.
- Step 2** Disconnect the secondary server from the network.
- Step 3** Set up the new Cisco Unity server (install voice cards if applicable, and plug everything in) by using the instructions in the “Setting Up the Hardware” chapter of the *Cisco Unity Installation Guide*.
- If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server, and install the associated driver.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 4** Install Windows 2000 Server on the new server by using the instructions in the *Cisco Unity Installation Guide*.
- Step 5** Restore the remaining contents of the server from the most recent secondary server backup by following the instructions in the third-party software documentation.



Caution If Active Directory, Microsoft SQL Server, MSDE, or Exchange were installed on the failed server, carefully follow the instructions for restoring those applications and their data.

- Step 6** On the secondary server, disable automatic failover and failback.
- Step 7** On the primary server, run the failover configuration wizard to enable automatic failover and failback.
- Step 8** On the secondary server, run the failover configuration wizard to enable automatic failover and failback.



Note Refer to the *Cisco Unity Failover Configuration and Administration Guide* for detailed configuration instructions. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fail401/ex/index.htm.

Replacing Both Failed Primary and Secondary Servers at the Same Time and Restoring Data by Using Third-Party Backup and Restore Software

Use the following procedure to replace both the primary server and the secondary servers in a failover configuration, at the same time. In this circumstance, both servers keep their original IP addresses and server names.

In order to do the following procedure, you must have a recent backup of both servers. Also note that the voice messaging service does not function while you replace the primary and secondary servers. During the interruption of service, callers and subscribers will not be able to record or listen to voice messages.

To Replace Both Failed Servers, Restore Data by Using Third-Party Backup and Restore Software, and Reconfigure Failover

- Step 1** If either or both of the servers are running, exit the Cisco Unity software, and then shut down the server(s).
- Step 2** Disconnect both servers from the network.
- Step 3** Set up the new Cisco Unity servers (install voice cards if applicable, and plug everything in) by using the instructions in the “Setting Up the Hardware” chapter of the *Cisco Unity Installation Guide*.
- If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server, and install the associated driver.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 4** Install Windows 2000 Server on the new servers by using the instructions in the *Cisco Unity Installation Guide*.
- Step 5** On the primary server, install new Cisco Unity license files.



Note For information about obtaining or updating license files, refer to the *White Paper: Licensing for Cisco Unity (All Versions)*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpaper/licenses.htm.

- Step 6** Restore the remaining contents of each server from the backup of that server by following the instructions in the third-party software documentation.



Caution If Active Directory, Microsoft SQL Server, MSDE, or Exchange were installed on the failed server, carefully follow the instructions for restoring those applications and their data.

- Step 7** On both servers, disable automatic failover and failback.
- Step 8** On the primary server, run the failover configuration wizard to enable automatic failover and failback.
- Step 9** On the secondary server, run the failover configuration wizard to enable automatic failover and failback.



Note Refer to the *Cisco Unity Failover Configuration and Administration Guide* for detailed configuration instructions. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fai401/ex/index.htm.

Replacing Failed Cisco Unity Servers Configured for Failover and Restoring Data by Using the Cisco Unity Disaster Recovery Tools

You can use the Cisco Unity Disaster Recovery Tools to restore one or both Cisco Unity servers configured for failover, by using the most recent backup from either the primary or the secondary server in the following scenarios:

- Restoring the primary server from a backup of the primary server
- Restoring the secondary server from a backup of the secondary server
- Restoring the secondary server from a backup of the primary server
- Restoring the primary server from a backup of the secondary server

When failover is configured, server backups include replicated and non-replicated data. For example, replicated data includes SQL and Cisco Unity data; non-replicated data includes Cisco Unity software patches (Engineering Specials) and changes to server registry settings.

When restored, the primary and secondary servers are restored to the point at which the server backup that was used for the restoration was made. Changes made to Cisco Unity after the backup and prior to the restoration will be lost.

Note that if you restart the primary and secondary servers while automatic failover and failback are disabled, both servers start as inactive, and therefore Cisco Unity is unable to take calls.

If you restore a server by using backup data from the primary server, an additional procedure must be done to repair broken SQL replication links.

To Replace One or Both Failed Cisco Unity Servers and Restore Data by Using the Cisco Unity Disaster Recovery Tools

-
- Step 1** If either of the servers is active, stop data replication on the active server. (See the “[To Stop Data Replication on the Secondary Server](#)” procedure on page 4-23, or the “[To Stop Data Replication on the Primary Server](#)” procedure on page 4-25, as applicable.)
- Step 2** If either or both of the servers are running, exit the Cisco Unity software, and then shut down the server(s).
- Step 3** Disconnect the failed server(s) from the network.
- Step 4** Follow the instructions in the *Cisco Unity Installation Guide* to set up the new Cisco Unity server(s) and reinstall all software, including replacement Cisco Unity license files.



Caution You must reinstall the exact version of Cisco Unity that was installed before the server failed.

If you backed up Cisco Unity by using a tape drive in the Cisco Unity server, install a tape drive in the new server(s), and install the associated driver.



Note The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst404/ex/index.htm.

- Step 5** If you installed Exchange 5.5 on the Cisco Unity server(s) in [Step 4](#), disable circular logging. (In Exchange 2000 and 2003, circular logging is already disabled by default.)

- Step 6** Restore Cisco Unity data from the backup of the secondary server by using the Disaster Recovery Tools. If you are restoring the server by using a backup of the primary server, skip the remaining steps in this procedure and continue with the “[To Repair Broken SQL Replication Links After Restoring Data From a Primary Server Backup](#)” procedure on page 4-24. Otherwise continue with [Step 7](#).
- Step 7** On the secondary server, disable automatic failover and failback.
- Step 8** On the primary server, run the failover configuration wizard to enable automatic failover and failback.
- Step 9** On the secondary server, run the failover configuration wizard to enable automatic failover and failback.

**Note**

Refer to the *Cisco Unity Failover Configuration and Administration Guide* for detailed configuration instructions. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/fail/fail401/ex/index.htm.

Authoritative Restores of Active Directory

To ensure that data appearing in both the Cisco Unity database and in Active Directory remains synchronized, Cisco Unity checks Active Directory at regular intervals for changes in both places, and updates the database with the new values. If critical Active Directory data has accidentally been deleted, and the deletion has been replicated to other domain controllers in the domain, you may need to do an authoritative restore. An authoritative restore gives the restored data the highest Update Sequence Numbers (USNs) in Active Directory, which ensures that the restored data is replicated to the other domain controllers. (In a non-authoritative restore, data retains its original USNs and is never replicated to other domain controllers.)

However, caution is required when choosing to do an authoritative restore. If the Active Directory data that you restore includes Cisco Unity data, some old data may overwrite new data, for example:

- Changes to subscriber data, such as extension numbers, made after the last backup of Active Directory may be lost.
- Subscriber accounts on Cisco Unity that were deleted after the last backup of Active Directory will reappear.

To help minimize the potential adverse effects, we recommend that you:

- Back up Active Directory frequently. Note that Active Directory is typically backed up as part of the third-party backup of the system state, when done on a domain controller.
- If an authoritative restore is required, always restore from the most recent backup.
- Restore only the objects or sub-trees affected, and document the restore.

For additional information on authoritative restores, refer to Knowledge Base articles 216243 and 241594 on the Microsoft Support website.

Additional Information About SQL Server Recovery

The Microsoft default recovery model for the Cisco Unity SQL Server UnityDB and ReportsDB databases is configured to Simple mode. Simple mode permits high performance bulk copy operations and allows the reclamation of log space to keep capacity requirements minimal, but can require that changes made since the last normal and differential incremental backups be manually re-established following successful recovery from those backups. The recovery model for Cisco Unity databases can be altered either to Full or Bulk-Logged, as applicable.

For additional information regarding backup Simple mode SQL Server databases, refer to Veritas Support Article 233717. For general information on recovery model selection criteria, refer to the Microsoft MSDN SQL Administration Guide.

Additionally, depending on your reason for doing a data restore, and on the version of Microsoft SQL Server used, the preparation and steps for restoring backups can vary. You may need to restore the entire server, including the desired Microsoft SQL Server databases, from full system backups, or to restore only the Microsoft SQL Server databases. In some cases you may be required to rebuild the Master database. For additional information on SQL Server Master database backup and rebuilding, refer to Microsoft Knowledge Base article 285288.

Troubleshooting Hardware and Software Problems by Using Backups

Table 4-2 lists some of the hardware and software problems that can occur on servers in a Cisco Unity environment, as well as possible solutions.

Table 4-2 Hardware or Software Problems That Can Require Recovery of Data

Problem	Possible Solution(s)
Deleted or corrupted file(s) on the Cisco Unity server	Restore individual files from a backup.
Deleted or corrupted file(s) on the Exchange server.	<ul style="list-style-type: none"> Restore individual files from a backup. Use the Win2K recovery process to restore and repair the operating system.
Deleted or corrupted file(s) on the SQL Server	<ul style="list-style-type: none"> Restore individual files from a backup. Use the Win2K recovery process to restore and repair the operating system.

Table 4-2 Hardware or Software Problems That Can Require Recovery of Data (continued)



Problem	Possible Solution(s)
System state errors: problems starting the server	<ul style="list-style-type: none"> • Restore individual files from a backup. • Use the Win2K recovery process to restore and repair the operating system. • Recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> – Replace the hard disk. – Recover the entire contents of the hard disk from a backup. – Restore Exchange and SQL Server from the logs. <p> Caution Exchange Server may not start if you attempt to restore both Microsoft Exchange Mailbox and Microsoft Exchange Server objects at the same time. Restoration of the mailbox objects fails because the Exchange services are down to perform a restore of the Exchange Server databases. Restoration of the mailbox objects may also fail if the restore of the Exchange mailbox items finishes before the restore of the Exchange databases begins, because the mailbox objects will be overwritten by the Exchange database restore.</p>
System state errors: blue screens (kernel-mode crash dumps commonly caused by bad drivers)	<ul style="list-style-type: none"> • Restore individual files from a backup. • Use the Win2K recovery process to restore and repair the operating system. • Recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> – Replace the hard disk. – Recover the entire contents of the hard disk from a backup. – Restore Exchange and SQL Server from the logs. <p> Caution Exchange Server may not start if you attempt to restore both Microsoft Exchange Mailbox and Microsoft Exchange Server objects at the same time. Restoration of the mailbox objects fails because the Exchange services are down to perform a restore of the Exchange Server databases. Restoration of the mailbox objects may also fail if the restore of the Exchange mailbox items finishes before the restore of the Exchange databases begins, because the mailbox objects will be overwritten by the Exchange database restore.</p>
Hard disk failure: RAID	Recover the contents of a hard disk by replacing the failed disk in a RAID.
Hard disk failure: non-RAID	Recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> • Replace the hard disk. • Recover the entire contents of the hard disk from a backup. • Restore Exchange (if present) and SQL Server from the logs.
Hardware failure: repairable without a manual restoration of the operating system	<ul style="list-style-type: none"> • Recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> – Replace the hard disk. – Recover the entire contents of the hard disk from a backup. – Restore Exchange (if present) and SQL Server from the logs. • Replace hardware, as applicable (for example, a faulty tape drive).

Table 4-2 Hardware or Software Problems That Can Require Recovery of Data (continued)

Problem	Possible Solution(s)
Hardware failure: irreparable or catastrophic	<ul style="list-style-type: none"> • If Exchange is installed on the Cisco Unity server, recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> – Replace the hard disk. – Reinstall Win2K. – Recover the entire contents of the hard disk from a backup. – Restore Exchange and SQL Server from the logs. • If Exchange is not installed on the Cisco Unity server, recover the contents of a hard disk by doing the following: <ul style="list-style-type: none"> – Replace the hard disk. – Recover the entire contents of the hard disk from a backup. – Restore Exchange and SQL Server from the logs. –
Exchange 2000 information store is dismounted because the backup process stopped responding	If the Exchange backup process fails to complete, and the number of transaction logs exceeds 1,088, Exchange will stop in order to preserve database integrity. The problem with the backup needs to be resolved before Exchange can be restarted. For more information, refer to Microsoft Knowledge Base article 812962, available on the Microsoft Support website.
Backup and restore activity logs indicate an error	<p>Both third-party backup and restore software products and the Disaster Recovery Tools can generate activity logs, provided that logging is enabled. Refer to the applicable Help for information on enabling logging options.</p> <p>If you find errors in the third-party software backup activity log, they can be related to the software attempting to back up open SQL Server/MSDE or Exchange database files. To resolve this problem, exclude the directories in which those files appear from the backup.</p> <p>SQLSyncSvr logs can also be helpful in diagnosing Disaster Recovery Tool restore problems.</p>