Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x

Revised May 2009

The *Disaster Recovery System Administration Guide for Cisco Unity Connection* provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup-related tasks and restore-related tasks.

This guide contains the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What is the Disaster Recovery System?

Revised May 2009

The Disaster Recovery System (DRS), which can be invoked from Cisco Unity Connection Administration, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

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

Caution Before you restore Cisco Unity Connection, ensure that the Cisco Unity Connection version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unity Connection for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(**1**).1000-1 to version 6.1(**2**).1000-1, or from version 6.1.(2).1000-**1** to version 6.1(2).1000-**2**.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a physical tape drive or remote SFTP server.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with Local Agents.

Note In version 7.1(2), when a Cisco Unity Connection cluster is configured, the Disaster Recovery System uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber servers. DRS makes use of the IPSec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, then you must ensure that you upload the IPSEC certificate to the IPSEC-trust.

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

Quick-Reference Tables for Backup and Restore Procedures

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

Note DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. These backup device settings and schedule settings get restored as a part of the platform backup/restore. After the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

Backup Quick Reference

Table 1 provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a backup procedure by using the Disaster Recovery System.

Table 1 Major Steps for Performing a Backup Procedure

Action	Reference
Create backup devices on which to back up data.	"Managing Backup Devices" section on page 5
Note Create and edit backup schedules to back up data on a schedule.	"Creating and Editing Backup Schedules" section on page 7
Enable and disable backup schedules to back up data.	"Enabling, Disabling, and Deleting Schedules" section on page 8
Optionally, run a manual backup.	"Starting a Manual Backup" section on page 9
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	"Checking Backup Status" section on page 9

Restore Quick Reference

Revised May 2009

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

Table 2 Major Steps for Performing a Restore Procedure

Action	Reference
Choose Storage Location—You must first choose the storage location from which you want to restore a backup file.	"Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server" section on page 10
Choose the Backup File—From a list of available files, choose the backup file that you want to restore.	"Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server" section on page 10
Choose Features—From the list of available features, choose the features that you want to restore.	"Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server" section on page 10
Choose Nodes—Choose all nodes/servers.	"Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server" section on page 10
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	"Viewing the Restore Status" section on page 12

System Requirements

Revised May 2009

To back up data to a remote device on the network, you must have an SFTP server that is configured. Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unity Connection. For information on which vendors have certified their products with your version of Cisco Unity Connection, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

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

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

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

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

How to Access the Disaster Recovery System

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

Note You set the Administrator username and password during Cisco Unity Connection installation, and you can change the Administrator password or set up a new Administrator account by using the Command Line Interface (CLI). See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* for more information. The guide is available on Cisco.com at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Master Agent Duties and Activation

The system automatically activates the Master Agent (MA) on the server.

Duties That the Master Agent Performs

Revised May 2009

The Master Agent (MA) performs the following duties:

- The MA stores systemwide component registration information.
- The MA maintains a complete set of scheduled tasks in an XML file. The MA updates this file when it receives updates of schedules from the user interface. The MA sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the MA through the Disaster Recovery System user interface to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.
- The MA stores backup data on a locally attached tape drive or a remote network location.

Local Agents

The server has a Local Agent to perform backup and restore functions.

Duties That Local Agents Perform

Revised May 2009

The Local Agent runs backup and restore scripts on the server.

Note In version 7.1(2), when a Cisco Unity Connection cluster is configured, the Disaster Recovery System uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber servers. DRS makes use of the IPSec certificates for its Public/Private Key encryption. This certificate exchange gets handled internally; you do not need to make any configuration changes to accommodate this exchange.

Managing Backup Devices

Revised May 2009

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

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

Note When a Cisco Unity Connection cluster is configured, we recommend that you back up the publisher server and, optionally, the subscriber server.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

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

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

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

The Backup Device window displays.

Step 6 Enter the backup device name in the **Backup device name** field.

Note The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-) and underscores (_). Do not use any other characters.

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

- **Tape Device**—Stores the backup file on a locally attached tape drive. Choose the appropriate tape device from the list.

  Note the following considerations:

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

- **Network Directory**—Stores the backup file on a network drive that is accessed through an SFTP connection. Enter the following required information:

  - **Server name**: Name or IP address of the network server
  - **Path name**: Path name for the directory where you want to store the backup file
  - **User name**: Valid username for an account on the remote system
  - **Password**: Valid password for the account on the remote system
  - **Number of backups to store on Network Directory**: The number of backups to store on this network directory.

    If you are backing up more than one Cisco Unity Connection server, we recommend that you create a separate directory on the network drive for each Connection server. In addition, if you are using DRS to back up other applications (Cisco Unified Communications Manager, Cisco Unified Presence), we recommend that you create a separate directory for each of the other servers. The value that you specify here applies to all of the backups in the directory, not just the backups for one server. For example, suppose you want to retain three backups for a Connection server and three backups for a Cisco Unified Communications Manager server. If you specify the same network directory for both servers, and if you specify three as the number of backups to store in the directory on both servers, only the most recent three backups will appear in the directory. If the last three backups were of the Connection server, you will not have any Cisco Unified Communications Manager backups at all.

Specify a value high enough to ensure that the backups you want to keep are not overwritten. For example, if you configure DRS so a full backup of a Connection server requires three separate backups (components, MailboxStore1, and MailboxStore2) and if you want to retain the two most recent full backups, choose 6 here. Choosing a lower number will cause the Disaster Recovery System to overwrite backups that you want to retain.

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

Step 8 To update these settings, click **Save**.

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

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

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

Creating and Editing Backup Schedules

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

Perform the following steps to manage backup schedules.

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Scheduler**.

The Schedule List window displays.

Step 4 Do one of the following steps to add a new schedule or edit an existing schedule

a. To create a new schedule, click **Add New**.

b. To configure an existing schedule, click its name in the **Schedule List** column.

The scheduler window displays.

Step 5 Enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 6 Select the backup device in the **Select Backup Device** area.

Step 7 Select the features to back up in the **Select Features** area. You must choose at least one feature.

You must back up the database and recorded names. Backing up messages is optional.

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

- Schedule backups during off-peak hours to avoid affecting system performance.
- Do not schedule a backup to run while the Update Database Statistics task is running. By default, this task runs daily at 3:30 am.

Step 9 Choose the frequency at which you want the backup to occur in the **Frequency** area: Once, Daily, Weekly, or Monthly. If you choose Weekly, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to Weekly, occurring Tuesday through Saturday, click **Set Default**.

Step 10 To update these settings, click **Save**.

Step 11 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Step 12 To disable the schedule, click **Disable Schedule**.

Enabling, Disabling, and Deleting Schedules

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Scheduler**.

The Schedule List window displays.

Step 4 Check the check boxes next to the schedules that you want to modify.

- To select all schedules, click **Select All**.
- To clear all check boxes, click **Clear All**.

Step 5 To enable the selected schedules, click **Enable Selected Schedules**.

Step 6 To disable the selected schedules, click **Disable Selected Schedules**.

Step 7 To delete the selected schedules, click **Delete Selected**.

Starting a Manual Backup

Revised May 2009

Follow this procedure to start a manual backup. We recommend that you:

- Back up during off-peak hours to avoid affecting system performance.
- Not back up while the Update Database Statistics task is running. By default, this task runs daily at 3:30 am.

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

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

Step 4 Select a backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area.

You must back up the database and recorded names. Backing up messages is optional.

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

Checking Backup Status

Revised May 2009

You can check the status of the current backup job and cancel the current backup job. To view the backup history, see the "Viewing the Backup and Restore History" section on page 13.

⚠ **Caution** Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Checking the Status of the Current Backup Job

Perform the following steps to check the status of the current backup job.

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

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

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

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

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

Restore Scenarios

You can restore Cisco Unity Connection in the following scenarios:

- Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server, page 10
- Replacing Cisco Unity Connection Servers, page 12

Restoring a Server or Cluster to a Last Known Good Configuration Without Replacing the Server

Revised May 2009

Note Use this procedure only if you are restoring an existing server to a last known good configuration. Do not use this procedure to replace a server. (For information on how to replace a server, see the "Replacing Cisco Unity Connection 7.x Servers" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrugx.html.)

Caution Before you restore Cisco Unity Connection, ensure that the Cisco Unity Connection version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unity Connection for restore. For example, the Disaster Recovery System does not allow a restore from version 7.0(**1**).1000-1 to version 7.1(**2**).1000-1, or from version 7.1(2).1000-**1** to version 7.1(2).1000-**2**. (The last parts of the version number change when you install a service release or an engineering special.) In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unity Connection database restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unity Connection.

The Restore Wizard walks you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.

Procedure

Step 1 If you reinstalled software on the server, do the following steps, as applicable:

a. Confirm that the IP address and host name of the server match the IP address and host name when the server was backed up. Otherwise, the restore will fail.

b. Reinstall the licenses that were originally installed on the server.

c. If any Connection languages were previously installed, reinstall the same languages.

Step 2 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

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

Step 4 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 5 Choose the backup device from which to restore in the **Select Backup Device** area. Then, click **Next**.

The Restore Wizard Step 2 window displays.

Step 6 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

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

Step 8 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

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

Step 10 When you are prompted to choose the node to restore, choose the same features that you selected in Step 8, and click **Next**.

Caution Existing data for the selected features is overwritten.

Step 11 To start restoring the data, click **Restore**.

Step 12 To view the status of the restore, see the "Viewing the Restore Status" section on page 12.

Step 13 Restart the server. For more information on restarting, see the "System Restart" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/os_administration/guide/7xcucosagx.html.

Step 14 If a Connection is not configured as a cluster, skip to Step 15. If a Connection cluster is configured, force Connection to copy the data from the publisher to the subscriber server:

a. After the publisher server has finished restarting, log on to the command-line interface for the subscriber server.

b. At the command line, run the following command to force Connection to copy data from the publisher server to the subscriber server:

```
utils cuc cluster overwritedb
```

c. Check the status of the Connection cluster on the subscriber server. At the command line, run the following command:

```
show cuc cluster status
```

d. Log on to the command-line interface for the publisher server.

e. Check the status of the Connection cluster on the publisher server. At the command line, run the following command:

```
show cuc cluster status
```

Step 15 During off-peak hours, resynchronize message-waiting indicators for each phone system:

a. In Cisco Unity Connection Administration, expand Telephony Integrations, and click Phone System.

b. Click the name of the first phone system.

c. For Synchronize All MWIs on This Phone System, click Run.

d. Repeat Step a. through Step c. for the remaining phone systems.

Replacing Cisco Unity Connection Servers

Added May 2009

For information on how to replace Cisco Unity Connection servers, see the "Replacing Cisco Unity Connection 7.x Servers" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrugx.html.

Viewing the Restore Status

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

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore > Status**. The Restore Status window displays.

The Status column in the Restore Status window shows the status of the restoration in progress, including the percentage of completion of the restore procedure.

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

Viewing the Backup and Restore History

Using the following procedures, you can see the last 20 backup and restore jobs:

- Backup History
- Restore History

Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

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

Step 4 From the Backup History window, you can view the backups that you have performed, including filename, backup device, completion date, result, and features that are backed up.

Note The Backup History window displays only the last 20 backup jobs.

Restore History

Perform the following steps to view the restore history.

Procedure

Step 1 In Cisco Unity Connection Administration, in the Navigation list, click **Disaster Recovery System**, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore > History**. The Restore History window displays.

Step 4 From the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

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

Trace Files

In this release of the Disaster Recovery System, trace files for the Master Agent, the GUI, and each Local Agent get written to the following locations:

- For the Master Agent, find the trace file at *platform/drf/trace/drfMA0**
- For each Local Agent, find the trace file at *platform/drf/trace/drfLA0**
- For the GUI, find the trace file at *platform/drf/trace/drfConfLib0**

You can view trace files by using the command line interface. See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html for more information.

Command Line Interface

The Disaster Recovery System also provides command-line access to a subset of backup and restore functions, as shown in Table 3. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Table 3 Disaster Recovery System Command Line Interface

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery show_backupfiles	Displays existing backup files
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery show_tapeid	Displays the tape identification information

Error Messages

The Disaster Recovery System (DRS) issues alarms for various errors that could occur during a backup or restore procedure. Table 4 provides a list of Cisco DRS alarms.

Table 4 Disaster Recovery System Alarms

Alarm Name	Description	Explanation
CiscoDRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encountered errors while it was accessing device.
CiscoDRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encountered errors.
CiscoDRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup while another backup is still running.
CiscoDRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encountered an error.
CiscoDRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot connect to Master Agent.
CiscoDRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be down.
CiscoDRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot connect to Local Agent.
CiscoDRFMABackupComponent Failure	DRF cannot back up at least one component.	DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up.
CiscoDRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation on a Cisco Unity Connection node, the node disconnected before the backup operation completed.
CiscoDRFMARestoreComponent Failure	DRF cannot restore at least one component.	DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.
CiscoDRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation on a Cisco Unity Connection node, the node disconnected before the restore operation completed.
CiscoDRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be down.
CiscoDRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no registered components are available.
CiscoDRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backup.
CiscoDRFRestoreDeviceError	DRF restore process has problems accessing device.	DRS restore process cannot read from device.
CiscoDRFRestoreFailure	DRF restore process failed.	DRS restore process encountered errors.
CiscoDRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP operation.

Table 4 Disaster Recovery System Alarms (continued)

Alarm Name	Description	Explanation
CiscoDRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message contains a malicious pattern that could result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.
CiscoDRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing on the node. DRF Local Agent cannot connect to Master Agent.
CiscoDRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.

Related Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, refer to the *Documentation Guide for Cisco Unity Connection Release 7.x*. The document is shipped with Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/roadmap/7xcucdg.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.