Configure Cisco Emergency Responder Disaster Recovery System

Disaster Recovery System overview

The Disaster Recovery System (DRS), which can be invoked from the main Cisco Emergency Responder web interface, provides full data backup and restore capabilities for all servers in an Emergency Responder server group. The Disaster Recovery System allows you to perform a regularly scheduled automatic or user-invoked data backup. DRS supports multiple backup schedules.

The Cisco Disaster Recovery System performs a server group-level backup, which means that it collects backups for all servers in an Emergency Responder server group to a central location and archives the backup data to physical storage device.

Cisco Emergency Responder provides DRS Email Alerts to System Administrators with status and description of any successes or failures.

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.

When performing a system data restoration, you can choose which servers in the server group that you want to restore.

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

Note The tape device must be attached to the Publisher.

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

The system automatically activates both the Master Agent and the Local Agent on all servers in the server group.

Note The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. A restore must run on the same product version as the backup. For information about data migration from a Windows-based platform to a Linux-based platform, see the Data Migration Assistant User Guide before performing the following the steps.

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

Backup and restore procedures

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

Perform backup procedure

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

Procedure

Step 1 Create backup devices on which to back up data.
For more information, see Add backup devices, on page 5.

Step 2 Create and edit backup schedules to back up data on a schedule.
Note Either a manual or a scheduled backup backs up the server group.
For more information, see Create and edit backup schedules, on page 6.

Step 3 Enable and disable backup schedules to back up data.
For more information, see Manage backup schedules, on page 7.

Step 4 (Optional) Run a manual backup.
For more information, see Start manual backup, on page 7.

Step 5 Check the status of the backup.
While a backup is running, you can check the status of the current backup job. For more information, see Check backup status, on page 8.

Perform restore procedure

The following procedure provides a quick, high-level reference to the major steps, in chronological order, that you must follow to perform a restore procedure using the Disaster Recovery System.

Procedure

Step 1 Choose storage location.
You must first choose the storage location from which you want to restore a backup file.

Step 2 Choose the backup file.
From a list of available files, choose the backup file that you want to restore.

Step 3 Choose features.
From the list of available features, choose the features that you want to restore.

Step 4 Choose server.
If the feature was backed up from multiple servers, you must choose the servers that you want to restore.

Step 5 Check the status of the restore.
While the restore process is running, you can check the status of the current restore job.

Related Topics

Restore backup file, on page 8
View Restore Status, on page 12

Supported features and components

For your Emergency Responder release, you can back up and restore Emergency Responder.

When you choose a feature for backup, the system backs up all of its subcomponents automatically.

System requirements

Make sure that the current version of Emergency Responder is running on all servers in the server group.

To back up data to a remote device on the network, you must have an SFTP server configured. Cisco tests and recommends the following SFTP servers, but you may use any SFTP server:

- Open SSH (for Unix systems)
- Cygwin
- freeFTPD
- Titan

Note Cisco does not support third-party software. Contact the SFTP vendor for support issues.

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, a backup or restore does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Access Disaster Recovery System

To access the Disaster Recovery System, select **Disaster Recover System** from the pull-down **Navigation** menu on the main Emergency Responder web interface. Log in to the Disaster Recovery System by using the same Administrator username and password that you use for the Cisco Unified OS Administration web interface.

Note You set the Administrator username and password during Emergency Responder installation, and you can change the Administrator password or set up a new Administrator account by using the CLI. See set password.

Master Agent duties and activation

The system automatically activates the Master Agent on all servers in the server group, but only the Master Agent running on the publisher server is fully active.

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 the Emergency Responder database. When it receives updates 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 scheduling backups, adding a new backup task for a specific server or a defined server group, updating or reviewing an existing entry, displaying status of executed tasks, and performing system restoration.
- The MA stores backup sets on a locally attached tape drive or a remote network location.

Local Agents

Each server in an Emergency Responder server group, including the server that contains the Master Agent, must have its own Local Agent to perform backup and restore functions for its server.

Note By default, a Local Agent automatically gets activated on each server in the server group.

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

Add backup devices

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

Procedure

Step 1 Select **Backup > Backup Device** from the main **Disaster Recovery System** web page.
The **Backup Device List** page appears.

Step 2 Click **Add New** to configure a new backup device. To edit a backup device, select it in the **Backup Device** list and click **Edit Selected**.
The **Backup Device** window appears.

Step 3 In the **Backup device name** field, enter the backup device name.

Note The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-), and underscores (_). No other characters are allowed.

Step 4 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 You cannot span tapes or store more than one backup per tape.
- **Network Directory—**Stores the backup file on a networked 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.

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

Step 5 Click **Save** to update these settings, .
Note For network directory backups, after you click the Save button, the DRS Master Agent validates the selected SFTP server. If the user name, password, server name, or directory path is invalid, the save fails.

Step 6 To delete a backup device, select it in the Backup Device list and **Delete Selected**.
Note You cannot delete a backup device that is configured as the backup device in a backup schedule.

Create and edit 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.

Procedure

Step 1 Select **Backup > Scheduler** from the main Disaster Recovery System web page.
The Schedule List window appears.

Step 2 Do one of the following steps to add a new schedule or edit an existing schedule:

- Click **Add New** to create a new schedule.
- Click a name in the **Schedule List** column to configure an existing schedule.

The scheduler window appears.

Step 3 Enter a schedule name in the **Schedule Name** field.
Note You cannot change the name of the default schedule.

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

Step 5 Select the features to back up in the **Select Feature**s area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 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 occurs.

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

Step 8 Click **Save** to update these settings.

Step 9 Click **Enable Schedule** to enable the schedule.
The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the server group are running the same version of Emergency Responder and are reachable through the network. Servers that are not running at the time of the scheduled backup are not backed up.

Step 10 Click **Disable Schedule** to disable the schedule.

Manage backup schedules

Procedure

Step 1 Select **Backup > Scheduler** from the main **Disaster Recovery System** web page.
The **Schedule List** window appears.

Step 2 Select the check boxes next to the schedules that you want to modify:

- Click **Select All** to select all schedules.
- Click **Clear All** To uncheck all check boxes.

Step 3 Click **Enable Selected Schedules** to enable the selected schedules.

Step 4 Click **Disable Selected Schedules** to disable the selected schedules.

Step 5 Click **Delete Selected** to delete the selected schedules.

Start manual backup

Procedure

Step 1 Select **Backup > Manual Backup** from the main **Disaster Recovery System** web page.

The **Manual Backup** page appears.

Step 2 Select a backup device in the **Select Backup Device** area.

Step 3 Select the features to back up in the **Select Features** area.

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

Check backup status

You can check the status of the current backup job and cancel the current backup job. To view the backup history, see Backup and Restore history, on page 12.

Procedure

Step 1 Select **Backup > Current Status** from the main **Disaster Recovery System** web page.
The **Backup Status** page appears.

Step 2 Click the log filename link to view the backup log file.

Step 3 Click **Cancel Backup** to cancel the current backup.
The backup is cancelled after the current component has completed its backup operation.

Restore backup file

Disaster Recovery System adheres to strict version checking and allows restore only for matching versions of Emergency Responder.

The Restore Wizard leads you through the steps that are required to restore a backup.

Tip To restore all servers in a server group, see Restore entire server group, on page 9.

Caution Before you restore Emergency Responder, ensure that the Emergency Responder 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 Emergency Responder for restore.

The product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Emergency Responder database restore.

Procedure

Step 1 Select **Restore > Restore Wizard** from the main **Disaster Recovery System** web page.

The first page of the **Restore Wizard (Step1 Restore—Choose Backup Device)** appears.

Step 2 Choose the backup device to restore in the **Select Backup Device** area.

Step 3 Click **Next**.
The Step 2 Restore—Choose the Backup Tar File page appears.

Step 4 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 5 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 6 Choose the features that you want to restore.
Note Only the features that were backed up to the chosen file are displayed.

Step 7 Click **Next**.
The Step 4 Restore—Final Warning for Restore page appears.

Step 8 Click **Restore** to start restoring the data, .
You are prompted to choose the server to restore.

Step 9 Choose the appropriate server.
Caution After you choose the server that you want restored, any existing data on that server will be overwritten.
Your data is restored on the server that you chose. To view the status of the restore, see View Restore Status, on page 12.

Step 10 Restart the server.
Note The system can require one hour or more to restore depending on the size of your database and the chosen components.

Restore entire server group

If a major failure or a hardware upgrade occurs, you may need to restore all the servers in the server group.

Note Before you restore a server group, make sure that the subscriber server in the server group is up and communicating with the publisher server. You must carry out a fresh install for the subscriber server that is down or not communicating with publisher server at the time of the restore.

Procedure

Step 1 Restore both Emergency Responder Publisher and Subscriber at the same time by selecting both the servers using Restore wizard.

Step 2 Restart Publisher.

Step 3 Restart the Subscriber after the publisher is back online.
Note You must restore both the servers in the server group at the same time.
The following sections provide the procedures for restoring servers in a server group.

Restore Publisher server

Caution Before you restore Emergency Responder, ensure that the Emergency Responder 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 Emergency Responder for restore.

Procedure

Step 1 Perform a fresh installation of Cisco Emergency Responder on the Publisher server. See the Install Emergency Responder Publisher procedure for more information.

Step 2 From the main Disaster Recovery System web page, select **Restore > Restore Wizard**.
The first page of the **Restore Wizard (Step 1 Restore—Choose Backup Device)** appears.

Step 3 Choose the backup device from which to restore in the **Select Backup Device** area.

Step 4 Click **Next**.
The **Step 2 Restore—Choose the Backup Tar File** page appears.

Step 5 Choose the backup file that you want to restore.
Note The backup filename indicates the date and time that the backup file was created.

Step 6 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 7 Choose the features that you want to restore.
Note Only the features that were backed up to the chosen file are displayed.

Step 8 Click **Next**.
The **Step 4 Restore—Final Warning for Restore** page appears.

Step 9 Click **Restore** to start restoring the data.

Step 10 Choose only the Publisher when you are prompted to choose the server to restore.

Step 11 Your data is restored on the publisher server. To view the status of the restore, see View Restore Status, on page 12.
Note During the restore process, do not perform any tasks with Emergency Responder Administration or User Pages.

Step 12 Restart the server.
Note Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

Step 13 After the publisher server restarts, continue with the Restore Subscriber server, on page 11.

Restore Subscriber server

Caution When restoring a server group, you must restore the publisher server before you restore the subscriber server.

Before You Begin

Before you restore Emergency Responder, ensure that the Emergency Responder 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 Emergency Responder for restore.

Procedure

Step 1 Perform a fresh installation of Cisco Emergency Responder on the Subscriber server. See Install Emergency Responder Subscriber for more information.

Step 2 Select **Restore > Restore Wizard** from the main **Disaster Recovery System** web page.
The first page of the **Restore Wizard (Step 1 Restore—Choose Backup Device)** appears.

Step 3 Choose the backup device in the **Select Backup Device** area.

Step 4 Click **Next**.
The **Step 2 Restore—Choose the Backup Tar File** page appears.

Step 5 Choose the backup file that you want to restore.

Caution To restore the subscriber server in the server group, you must choose the same backup file that you used to restore the Publisher.

Step 6 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 7 Choose the features that you want to restore.

Note Only the features that were backed up to the chosen file are displayed.

Step 8 Click **Next**.
The **Step 4 Restore—Final Warning for Restore** page appears.

Step 9 Click **Restore** to start restoring the data.

Step 10 Choose only the Subscriber when you are prompted to choose the servers to restore.

Step 11 Your data is restored on the subscriber server. To view the status of the restore, see View Restore Status, on page 12.

Step 12 Restart the server.

Note The system can require one hour or more to restore depending on the size of your database and the components that you choose to restore.

Step 13 When the subscriber has rebooted and is running the restored version of Emergency Responder, reboot the publisher.

Step 14 Check the Replication Status value on all nodes by using the **utils dbreplication status** CLI command as described in the utils dbreplication status. The value on each node should equal two.

Tip If replication does not set up properly, use the **utils dbreplication reset** CLI command as described in the utils dbreplication reset.

View Restore Status

Procedure

Step 1 From the main **Disaster Recovery System** web page, select **Restore > Status**.
The **Restore Status** page appears. 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 2 Click the **log filename** link to view the restore log file.

Backup and Restore history

The following sections describe how you can see the last 20 backup and restore jobs.

View Backup History

Procedure

Step 1 Select **Backup > History** from the main **Disaster Recovery System** web page.
The Backup History page appears.

Step 2 From the **Backup History** page, 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** page displays only the last 20 backup jobs.

View Restore History

Procedure

Step 1 Select **Restore > History** from the main **Disaster Recovery System** web page.
The **Restore History** page appears.

Step 2 From the **Restore History** page, 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** page displays only the last 20 restore jobs.

Trace files

Trace files for the Master Agent, the GUI, and each Local Agent are written to the following locations:

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

You can view trace files by using the CLI. For more information, see CLI

Use the CLI for backup and restore

The Disaster Recovery System also provides command-line access to a subset of backup and restore functions, as shown in Table 1: Disaster Recovery System CLI, on page 13. For detailed information about these commands and for information about using the CLI, see CLI.

Table 1: Disaster Recovery System CLI

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 servers 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.