CLI Commands and Disaster Recovery System

CLI Commands on Cisco Prime Collaboration Deployment

The main functions of Cisco Prime Collaboration Deployment (such as creating migration, upgrade, and other tasks) are supported through the Cisco Prime Collaboration Deployment GUI interface. You can use the GUI interface to create a specific task and schedule the time to perform the task. The GUI interface also reports the status of tasks.

For other operations, such as upgrading the software on the Cisco Prime Collaboration Deployment server and performing a DRS backup, use the Cisco Prime Collaboration Deployment CLI, which is similar to the CLI on Cisco Unified Communications Manager Release 10.x.

Use the CLI on Cisco Prime Collaboration Deployment to perform the following tasks:

- View or get log files
- Administer a DRS backup device, and perform a data backup or restore
- Upgrade the Cisco Prime Collaboration Deployment software
- Change the hostname, IP address, or password on the Cisco Prime Collaboration Deployment
- Perform diagnostic commands on the Cisco Prime Collaboration Deployment system

The most common CLI operations and commands are for viewing logs and performing DRS backups.

Getting Cisco Prime Collaboration Deployment Logs

When you troubleshoot problems on the Cisco Prime Collaboration Deployment server, it is often necessary to view the main application log.

CLI command: **file get activelog tomcat/logs/ucmap/log4j/***

The Cisco Prime Collaboration Deployment main application log contains the following information:

- Representational state transfer (REST) requests from the browser
- Simple Object Access Protocol (SOAP) requests to UC servers
- Database requests
- Scheduler events (scheduled, started, failed, and so on)
- Specific job events (tasks, task actions, and nodes)
- Exceptions and errors

DRS on Cisco Prime Collaboration Deployment

The Disaster Recovery System (DRS) can be administered and invoked from the Cisco Prime Collaboration Deployment CLI. DRS allows you to perform user-invoked data backups of the data on your Cisco Prime Collaboration Deployment (the server clusters you have discovered, and scheduled and completed tasks). You can also choose to set up regularly scheduled automatic backups. The DRS feature has the following functions:

- CLI commands for performing backup and restore tasks
- The ability to schedule backups ahead of time, or run backups manually immediately
- The ability to archive backups to a remote SFTP server

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup and restore.

Important While you restore your data, the hostname, server IP address, and Cisco Prime Collaboration Deployment software version on the machine to which you are restoring the data must be the same as they were on the server on which you performed the backup.

DRS CLI Commands

Below is a list of the CLI commands that you can use to configure and perform backup and restore operations through DRS.

- **utils disaster_recovery status <operation>** (An example of **operation** is Backup or Restore).
- **utils disaster_recovery device list**
- **utils disaster_recovery device add**
- **utils disaster_recovery device delete**
- **utils disaster_recovery schedule add**
- **utils disaster_recovery schedule delete**
- **utils disaster_recovery schedule enable**
- **utils disaster_recovery schedule disable**
- **utils disaster_recovery schedule list**
- **utils disaster_recovery backup** —Starts a manual backup by using the features that are configured in the DRS interface.
- **utils disaster_recovery restore** —Starts a restore, and requires parameters for backup location, filename, and features to restore.
- **utils disaster_recovery show_backupfiles**—Shows existing backup files.
- **utils disaster_recovery cancel_backup**
- **utils disaster_recovery show_registration**
- **utils disaster_recovery show_registration SERVER**—Shows the features that you need to back up. For example, if you want to back up Cisco Prime Collaboration Deployment, choose `PCD` from the feature list.

For more information, see the DRS documentation for Cisco Unified Communications Manager, at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Create a DRS Backup of the Server

Before you begin

If you are using a location on your network to back up your Cisco Prime Collaboration Deployment, ensure the following points:

1. You must have access to an SFTP server to configure a network storage location. The Disaster Recovery system supports only SFTP servers that are configured with an IPv4 address or hostname/FQDN.
2. The account that you use to access the SFTP server must have write permission for the selected path.

You can also back up your Cisco Prime Collaboration Deployment to a local disk; however, this method is not recommended, because of the amount of space that is required on the Cisco Prime Collaboration Deployment disk to store the backup files.

Procedure

Step 1 Add the backup device.

Run the following command: **utils disaster_recovery device add network**

Example:

utils disaster_recovery device add network

Step 2 To verify that the device was set up correctly, run the following CLI command: **disaster_recovery device list**.

Step 3 Run a backup using the following command:

utils disaster_recovery backup network PCD device_name where device_name is the name of the backup device that was defined in Step 1.

Example:

utils disaster_recovery backup network PCD device1

Step 4 Check the status of the backup using the following CLI command:

utils disaster_recovery status backup.

Use this command to see the status of your backup. The backup is complete when Percentage Complete is 100, and all components show "SUCCESS."

Important Notes on Backup and Restore

Note When you restore your Cisco Prime Collaboration Deployment data, ensure that the Cisco Prime Collaboration Deployment software version that is installed on your server matches the version of the backup file that you want to restore.

Note When you perform a DRS restore operation to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present before you perform a restore operation.

Note We recommend that you perform a fresh installation of Cisco Prime Collaboration Deployment on your virtual machine before you restore the data.

Restore a Backup to Cisco Prime Collaboration Deployment

Note This procedure is optional.

Procedure

Step 1 Because a fresh install of the VM is recommended before the restore, you will need to add a backup device, so the system can retrieve the files from there. Configure the backup device by using the **utils disaster_recovery device add network** command.

Example:

utils disaster_recovery device add network device1 /backupdir/pcdbk 10.94.155.76 adminname 2

Specify the device from which you want to restore a backup file.

Step 2 List the backup files by using the following CLI command: **utils disaster_recovery show_backupfiles**

Example:

admin: utils disaster_recovery show_backupfiles device1

The **show_backupfiles command** shows which backups are available to be restored. Backups are named by date and the time the backup was performed.

Step 3 Start the restore operation by running the following CLI command: **utils disaster_recovery restore network**

Example:

admin:utils disaster_recovery restore network b7k-vmb031 2013-10-30-15-40-54 device1

When you are prompted to enter the features to restore, enter **PCD**.

Enter the comma separated features you wish to restore. Valid features for server B7K-VMB031 are PCD:PCD.

Step 4 Check the status of the restore by using the following CLI command: **utils disaster_recovery status restore**.

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

Do not administer any data on the Cisco Prime Collaboration Deployment server until the command shows as one hundred percent complete. This can take several minutes, depending on the amount of data that is being restored.

What to do next

After you restore your data, perform a system restart on the Cisco Prime Collaboration Deployment server to initialize the database.

The Cisco Prime Collaboration Deployment server will lose contact with ESXi hosts during the reinstallation. You may have to add ESXi hosts back into Cisco Prime Collaboration Deployment after a restore operation.

CLI Commands for TLS Minimum Version Configuration

For the minimum TLS version support control feature, following CLI commands have been added.

set tls min-version

This command sets the minimum version of Transport Layer Security (TLS) protocol.

Note

- After you set the minimum TLS version, the system reboots.
- Configure the minimum TLS version for each node.

set tls min-version *tls minVersion*

Syntax Description

Parameters	Description
tls minVersion	Type one of the following options to set it as the minimum TLS version: • 1.0 • 1.1 • 1.2

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager and IM and Presence Service on Cisco Unified Communications Manager

Example

```
admin: set tls min-version 1.2

This command will result in setting minimum TLS version to 1.2 on all the secure interfaces.
If you have custom applications that makes secure connection to the system, please ensure
they support the TLS version you have chosen to configure.
Also, please refer to the Cisco Unified Reporting Administration Guide to ensure the
endpoints in your deployment supports this feature.

********************************************************************************************

Warning: This will set the minimum TLS to 1.2 and the server will reboot.

********************************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.2

The system will reboot in few minutes.
```

show tls min-version

This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

show tls min-version

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager and IM and Presence Service on Cisco Unified Communications Manager

Example

```
admin:show tls min-version
Configured TLS minimum version: 1.0
```