



Backup and Restore Guide for Cisco Unified Communications Domain Manager 8.1.3

First Published: January 29, 2014

Last Modified: January 29, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED 'AS IS' WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Contents

| | |
|---------------------------------------------------|----|
| Overview | 4 |
| Typographic Conventions | 4 |
| Backup | 5 |
| Pre-requisites | 5 |
| Manual Backup | 7 |
| Automated Backups | 8 |
| Setting the time of day for backups | 8 |
| Setting the days of the week for backups | 8 |
| Email Notifications | 9 |
| SNMP Trap Notifications | 9 |
| Remote Copy Destination | 9 |
| Backup Retention | 9 |
| Backup maintenance | 10 |
| Restore | 11 |
| Copy Backup from Original Server to Target Server | 12 |
| Support | 13 |

Overview

This document explains the backup and restore processes on the platform.

This system supports various deployments/solutions including HCS and Large Enterprise (LE).

This document describes the product in general and is not specific to a particular deployment/solution. Information may vary slightly depending on the installation environment.

Typographic Conventions

The following typographic conventions are used in this document:

| Item | Character format | Example |
|---------------------------------------------------|------------------|------------------------------------------------------------------------------|
| Buttons | Bold | Click the Enter button. |
| Checkboxes | <i>italic</i> | Select the <i>Country</i> checkbox. |
| Dialog boxes menu items, tab names, radio buttons | <i>italic</i> | Select the <i>Configuration</i> option, or select the <i>Parameters</i> tab. |



CHAPTER 1

Backup

[Pre-requisites](#) 5

[Manual Backup](#) 7

[Automated Backups](#) 8

[Setting the time of day for backups](#) 8

[Setting the days of the week for backups](#) 8

[Email Notifications](#) 9

[SNMP Trap Notifications](#) 9

[Remote Copy Destination](#) 9

[Backup Retention](#) 9

Backups can be made in two ways:

- Manual backups
- Automated backups

The backup system saves a copy of the database, shared file system and certain configuration files. The shared file system contains the bulk load sheets, branding and themes.

The configuration data cannot be restored without the help of support, although the original system configuration can be imported to new deployments and the system restored.

Pre-requisites

The default system is deployed without a disk for backup usage.

The backups are stored on the system volume, *which is not recommended*.

Refer to the table below as a sizing guide for an additional backup volume:

| System Size | Backup Retention | Backup Volume Size |
|-------------------------------|----------------------|--------------------|
| Large (100000+ devices) | High (keep 7 copies) | 250 GB |
| Large (100000+ devices) | Low (keep 2 copies) | 100+ GB |
| Medium (10000-100000 devices) | High (keep 7 copies) | 200+ GB |
| Medium (10000-100000 devices) | Low (keep 2 copies) | 50+ GB |

Use the following procedure to add a backup volume:

Procedure

Add the disk to the system using the VMWare Vsphere client

- Step 1** Login to the VMWare Vsphere client.
 - Step 2** Choose the CUCDM node.
 - Step 3** Right click node, and choose *Edit settings...*
 - Step 4** Click **Add...**
 - Step 5** Choose *Hard Disk* and click **Next**.
 - Step 6** Keep on *Create a new virtual disk* and click **Next**.
 - Step 7** Choose the Size applicable to customer, select the *Thick Provisioned Lazy Zeroed* radio button, then click **Next**.
 - Step 8** Keep *Virtual Device Node* as is, click **Next**.
 - Step 9** Review changes, and click **Finish**.
 - Step 10** Click **OK** when complete.
-

Procedure

Add a disk to the CUCDM system

Caution: Applying changes may cause services to restart.

- Step 1** Log in to the system as the usmcli user.
 - Step 2** In the console go into enable mode.
 - Step 3** In the enable menu go into the system menu.
 - Step 4** Run the diskadd command.
 - Step 5** Choose the disk you would like to use.
 - Step 6** Choose *Use this as a backup volume*.
-

Example:

```
Welcome to the CLI management console

Documented commands (type help <topic>):
=====
[enable]      health      history      ping        exit

=>> en

Documented commands (type help <topic>):
=====
[autoregister]  [backup]      [configuration]  [destinations]
[dhcp]          [dr]          [logging]        [network]
```

```

[snmp]
health

[software]
history

[system]
exit

[webservices]

!!! Warnings exist - please run 'health'

=># system

Documented commands (type help <topic>):
=====
cleanup          cleardown        diskadd          diskshow        history
monitor          password         reboot          reinitialize    shutdown
startall         stopall         time            tune            exit

!!! Warnings exist - please run 'health'

=>[system] # diskadd

Reconfiguring lvm
Reconfigure completed.

Which unused storage device do you want to use:
[ 1 ] /dev/sdc with size 199Gb and no partition

Select one of the above options; <ENTER> to quit... 1

How should the disk /dev/sdc be used?
[ 1 ] Use this as a data disk for system services
[ 2 ] Use this to extend the swap space
[ 3 ] Use this as a backup volume

Select one of the above options; <ENTER> to quit... 3

```

Manual Backup

Procedure

To perform a manual backup follow these steps:

- Step 1** Login to the system as the usmcli user.
- Step 2** In the console go into enable mode.
- Step 3** In the enable menu go into the backup menu.
- Step 4** Run the backup command.

Manual backups created will be indicated by the word "manual" in the backup file name to distinguish them from automated backups.

Note

If a backup could not complete successfully, it will contain the word "partial" in the name. These backups should not be used to restore a system and cueddm support should be contacted immediately.

Example:

```

Welcome to the CLI management console

Documented commands (type help <topic>):
=====

[enable] exit health help history ping

```

```
=>> enable

Documented commands (type help <topic>):

=====

[autoregister]  [destinations]  [logging]  [software]  exit  history
[backup]        [dhcp]          [network]  [system]    health
[configuration] [dr]            [snmp]     [webservices] help

=># backup

Documented commands (type help <topic>):

=====

apply backup delete exit help history list restore set show

=>[backup] # backup

Running database backup...

File in /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-manual-2011-12-30-12-22.tar.gz

Backup completed and saved to /srv/CUCDM/pgsql/pgsql/backup

=>[backup] #
```

Automated Backups

Procedure

To set the time and days that the scheduled backups are performed:

- Step 1** Login as the usmcli user.
 - Step 2** In the console go into enable mode.
 - Step 3** In the enable menu go into the Backup menu.
 - Step 4** In the backup menu enter the command `show` to see the configuration settings.
 - Step 5** Use the `set` command to change the backup configuration (see below).
 - Step 6** Use the `apply` command to save and apply the new settings.
-

Setting the time of day for backups

In the backup menu, the scheduled time for backup can be changed with the `set` command.

```
set sched_time hh:mm
```

Here *hh* is hours between 0 and 23 and *mm* is minutes between 0 and 59. A colon ":" must be present between hours and minutes. The time specified should be in UTC timezone.

Setting the days of the week for backups

The day of the week for scheduled backups can be changed with the `set` command in the backup menu.

```
set sched_days a,b,c
```


Here *a, b, c* are numbers between 0 and 6 (0 is Sunday, 1 is Monday, 2 is Tuesday, 3 is Wednesday, 4 is Thursday, 5 is Friday and 6 is Saturday.) Numbers must be separated with a comma ",".

Note

Old backup files are deleted after the scheduled backup to prevent disk space from filling up.

Email Notifications

An email notification can optionally be sent whenever a backup is made. In the backup menu, the email notification group can be changed with the `set` command.

```
set email name
```

Here *name* should correspond to an email group. Email groups can be managed through the Destinations menu.

SNMP Trap Notifications

An optional SNMP trap can be generated when a backup is made, allowing remote management. The Backup subsystem uses the system wide SNMP trap destinations. The SNMP trap destinations can be changed from the trap submenu in the SNMP menu.

Remote Copy Destination

Once a backup is made, the backup file can optionally be copied to a remote server. In the backup menu the remote copy destination can be changed with the `set` command.

```
set remote_dest name
```

Here *name* should correspond to a SFTP or FTP destination. Remote copy destinations can be managed through the Destinations menu as follows:

1. In the destinations menu, use the command "add sftp" to add a new sftp destination.
2. Provide a name for the destination, eg. remotebackups
3. Set the various options, e.g username, path, password, and hostname.
4. Once the changes are applied, the new destination can be used in the backup menu as the `remote_dest`

Backup Retention

There are two settings to manage the retention of backup files (i.e. removing old backup files ensuring that the filesystem does not become full).

1. Number - The amount of backup files to keep; if there are more backup files on the system than specified amount, the oldest files will be removed.
2. Retention_days - The amount of days to keep backup files; files older than the specified number of days will be removed.



CHAPTER 2

Backup maintenance

The number of backups that are retained are controlled via the `retention_days` and `number` options in the backup menu. The number of backups that are kept are naturally subject to sufficient disk space being available to store all backups.

Backups may be deleted via the CLI menu by using the `delete` command in the backup menu. A list of current backups will be presented, and the selected backup will be deleted.

Backups may also be accessed and deleted via the sftp server on the host with the username `sftp` in the backups directory. The sftp server can be used to retrieve backups from the server for storage offsite. Also note that the `remote_dest` option can be used to automatically copy backups offsite when automated backups are scheduled

Note that it is highly recommended that a separate backup disk be provisioned on the system. This will prevent backups from being deleted accidentally, as backups are otherwise stored on the database volume. This backup volume can be added via the `diskadd` command in the system menu - see the CLI guide for further information. It is recommended that this backup volume be at least 100Gb, or 5 times the size of the database so that sufficient space is available to make multiple database backups.



CHAPTER 3

Restore

Copy Backup from Original Server to Target Server 12

In order to restore a system, the target system should have the same physical configuration as the system that has been backed up - i.e. same disk space allocated, memory, etc. The restore process will only restore the database and the shared filesystem. In order to restore the configuration files, either setup the target machine by importing the configuration file via the install wizard, or contact customer support.

Note

The restore process is destructive - all data in the database of the restore machine will be lost and overwritten from the backup file.

Procedure

To restore the backup, follow these instructions:

- Step 1** Login to the system as the usmcli user.
- Step 2** In the console go into enable mode.
- Step 3** In the enable menu go into the backup menu
- Step 4** Run the `list` command to display the available backups.

Note

The backup file name needs to contain "ucdm-backup" for it to show up in the list of available db backup files.

- Step 5** Run the `restore` command with number that corresponds with the backup you wish to restore.
-

Once the process is done a success message will be displayed (see example).

Example:

```
Welcome to the CLI management console
Documented commands (type help <topic>):
=====
[enable]  exit  health  help  history  ping
=>> enable
```

```
Documented commands (type help <topic>):
=====

[autoregister]  [destinations]  [logging]  [software]  exit  history
[backup]        [dhcp]          [network]  [system]    health
[configuration] [dr]            [snmp]     [webservices] help

=># backup

Documented commands (type help <topic>):
=====

apply  backup  delete  exit  help  history  list  restore  set  show

=>[backup] # list

Backup file

[ 1 ] /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-auto-2011-12-30-12-00.tar.gz
[ 2 ] /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-auto-2012-01-01-12-00.tar.gz
[ 3 ] /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-auto-2012-01-02-12-00.tar.gz
[ 4 ] /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-manual-2011-12-30-09-12.tar.gz
[ 5 ] /srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-manual-2011-12-30-09-13.tar.gz

=>backup # restore 4

Restore backup:
/srv/CUCDM/pgsql/pgsql/backup/ucdm-backup-manual-2011-12-30-09-12.tar.gz

This operation will destroy ALL data in the database.
Are you sure you want to continue? [y/N] y

Database restore completed successfully

=>backup #
```

Copy Backup from Original Server to Target Server

If the backup is used to restore a different target machine, the backup file can be copied from the server that was backed up to the target server via SFTP as the usmcli user.



CHAPTER 4

Support

For support related queries, please contact your dedicated customer support person.