



# Explorer Controller Backup and Restore User Guide for EC 8.0 and DTACS 5.0



## Please Read

### Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

# Notices

## Trademark Acknowledgments

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](http://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)

## Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

## Copyright

© 2018 Cisco and/or its affiliates. All rights reserved.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

# Contents

<b>About This Guide</b>	<b>v</b>
<b>Chapter 1 Hardware Compatibility</b>	<b>1</b>
Hardware Platform Compatibility.....	2
Supported External Backup Devices .....	3
<b>Chapter 2 Backup Recommendations</b>	<b>5</b>
System Backup Frequency.....	6
Prepare for the Backup .....	8
<b>Chapter 3 Backup and Restore Using Cloning</b>	<b>11</b>
Backing Up Full Systems Using Cloning.....	12
Restoring a System From a Cloned VM .....	16
<b>Chapter 4 Backup and Restore to an NFS Mount</b>	<b>21</b>
Back Up the Database and Key Files to an NFS-Mounted Directory .....	22
Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs .....	24
Restoring the Database and Key Files to an Existing VM.....	27
<b>Chapter 5 Customer Information</b>	<b>31</b>
<b>Appendix A Modify the Root crontab File for Automating Backups</b>	<b>33</b>
Configuring the Database and Key Files Backup cron Script.....	34
Modify the Root crontab File.....	35
<b>Index</b>	<b>37</b>



## About This Guide

### Purpose

This guide provides a full set of backup and restore procedures for the Cisco Explorer Controller (EC) and for the Cisco Digital Transport Adaptor Control System (DTACS) database, as well as for their respective key files.

### Scope

The procedures in this guide are for backing up and restoring the EC with an integrated Application Server and for the DTACS. The procedures are written using the vSphere v5.5 Web UI.

**Note:** System operators who support ECs with other application servers should contact their vendor for relevant backup and restore procedures for that application server.

### Audience

These backup and restore procedures are written for system operators who support the following Digital Broadband Delivery System (DBDS) System Releases (SRs):

- EC SR 8.0
- DTACS SR 5.0

### DBDS Maintenance ISO File

This guide refers to Version 8.0.x of the backup and restore scripts. These scripts are included with each EC and DTACS application. The backup and restore scripts are installed in the `/opt/cisco/backup_restore` directory as a part of the **CSCObackup-restore-8.0.\*** RPM. You can confirm the version by running the `rpm -qa | grep -i backup command`.

### Document Version

This is the first formal release of this document.



# 1

---

## Hardware Compatibility

### Introduction

This chapter lists the hardware platforms with which the backup and restore scripts are compatible.

### In This Chapter

- Hardware Platform Compatibility..... 2
- Supported External Backup Devices ..... 3

## Hardware Platform Compatibility

Version 8.0.x of the backup and restore scripts, which are part of the NextX 8.0 repositories (repos), have been tested and verified against the following hardware platforms:

- UCS C240 M3
- UCS C240 M4

## Supported External Backup Devices

Version 8.0.x of the backup and restore scripts have been tested and verified using the following external storage devices:

- Network File System (NFS)-mounted file systems
- Network-attached storage (NAS) drive, NFS-mounted



# 2

---

## Backup Recommendations

### Introduction

This chapter provides recommendations for the frequency with which system operators should back up their system data. By performing regular backups, system operators are assured that their valuable data will not be lost should they ever experience a failure of a major component of their system.

If you are using the vSphere Web client or the vSphere client, you should clone the VM to a network-accessible device. If you are using an ESXi client, you must execute a database and key files backup.

All backups should be saved to a network-accessible device that is NFS-mounted and that has root access.

### In This Chapter

- System Backup Frequency..... 6
- Prepare for the Backup ..... 8

## System Backup Frequency

You can ensure the integrity of your data only by adhering to a regular schedule of full system or database and key files backups. The recommendations in this section provide some guidance regarding how often you should do a system backup. Adjust these recommendations, if necessary, according to the size of the system and how often the data changes.

### Full System Backup

File system backups are no longer supported in EC SR 8.0 or in DTACS 5.0. Going forward, cloning the VM replaces a full filesystem backup. This creates filesystem, database and key files backups. The VM can be cloned while it is running or while it is shutdown.

#### Important:

- Cloning a VM requires vSphere Web UI or vSphere client.
- If you are using an ESXi client, you cannot clone a VM. In this case, you must build a new VM and install the appropriate application (for example, EC, DTACS). Then you must restore the most recent database and key files backup.

You should perform a VM clone in the following situations:

- Before making any substantial modifications to the system.
- Before upgrading to new system software.  
**Note:** The clone just before the upgrade can be used in case there is a catastrophic failure of the upgrade.
- Immediately after the acceptance sign-off of an installation or upgrade.
- Monthly or quarterly.

### Informix Database and Key Files Backup

**Note:** Key files and database backups are supported by using the backupDBKF script.

The Informix database and key files contain all headend configuration information, as well as data needed to provision and authorize Digital Home Communication Terminals (DHCTs). Therefore, you should perform a complete backup of the Informix database and key files in the following situations:

- Daily (for system updates)
- Before and after a channel lineup change
- Before and after a major system configuration change

When executing the backupDBKF script, default key files are backed up. To add additional files to key file backup list, update the `/opt/cisco/backup_restore/KeyFiles_templates/KeyFiles.include` file.

**Note:** Database and key files can be backed up without stopping system components. Even though you are not required to stop system components to perform a database backup, we strongly recommend that you schedule this backup during periods of lowest system activity.

### File System Backup

**Important:** File system backups are not supported.

To backup a file system, you must perform a full system backup by cloning your active VM using only the vSphere Web UI or vSphere client. Refer to *Full System Backup* (on page 6) for details.

**Note:** If you are using an ESXi client, you cannot clone a VM. In this case, the user must deploy a new VM, install the appropriate application (for example, EC, DTACS), and then restore the most recent database and key files backup.

### NFS-Mounted Directory Requirements

Network file systems must meet the following requirements to be used for database and key files backups:

- Must be accessible through the `/net/[remotehost]/[path_to_NFS_directory]` directory structure.
- The NFS directory must already exist.
- The root user must be able to write to, and change ownership of, the backup directory.

**Important:** Procedures for setting up NFS shared directories are beyond the scope of this document. See your system administrator, if necessary, for help in setting up the NFS shares.

## Prepare for the Backup

### Recording Network Configuration Information

Recording the following information will be useful for any backup or restore operation, and is especially useful when backing up or restoring across the network.

- 1 As **admin** user, type the following command on the server you are backing up to record network information.

```
[admin@vodwater ~]$ ifconfig -a
```

**Result:** Output similar to the following appears:

```
eth0      Link encap:Ethernet  HWaddr 00:50:56:8B:70:B9
          inet addr:10.90.45.16  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::250:56ff:fe8b:70b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64884651 errors:0 dropped:0 overruns:0 frame:0
          TX packets:202417 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4192859450 (3.9 GiB)  TX bytes:13692906 (13.0 MiB)

eth1      Link encap:Ethernet  HWaddr 00:50:56:8B:6C:94
          inet addr:204.3.1.49  Bcast:204.3.1.63  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth2      Link encap:Ethernet  HWaddr 00:50:56:8B:27:50
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth3      Link encap:Ethernet  HWaddr 00:50:56:8B:05:5C
          inet addr:204.3.3.50  Bcast:204.3.3.63  Mask:255.255.255.240
          inet6 addr: fe80::250:56ff:fe8b:55c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31021329 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19399834 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21774492321 (20.2 GiB)  TX bytes:2014244343 (1.8 GiB)
```

```

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:75837596 errors:0 dropped:0 overruns:0 frame:0
            TX packets:75837596 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:9326919264 (8.6 GiB)  TX bytes:9326919264 (8.6 GiB)

lo:1       Link encap:Local Loopback
            inet addr:127.0.0.2  Mask:255.0.0.0
            UP LOOPBACK RUNNING  MTU:65536  Metric:1

```

- 2 Record the network interfaces and their IP addresses.
- 3 Cross-reference the output you recorded with what is stored in the `/etc/hosts` file.  
**Note:** The data should match. If it does not, resolve the mismatch or call Cisco Services for assistance.

## Backing Up Unique Key Files

Default key files are included in the `/opt/cisco/backup_restore/KeyFiles_templates/KeyFiles.include` file. This file is used, by default, during the execution of the `backupDBKF` script.

If you have unique key files that you want backed up, add the absolute path for each key file to the end of the `KeyFiles.include` file. This includes adding the user home directories and third-party configurations as they are not included as default key files. It also includes the files that are synced between hosts when RepDB is enabled.

### Notes:

- You **MUST** manually add an entry in the `KeyFiles.include` file for each user created with the `useradmin` tool.
- If these users or third-party configurations are not added to the file, they will not be backed up.



# 3

---

## Backup and Restore Using Cloning

This chapter describes the procedures to backup and restore a complete EC or DTACS system via cloning.

**Important:** Skip this chapter and go to *Backup and Restore to an NFS Mount* (on page 21) for the following situations:

- If you are using an ESXi client because cloning is only supported with the vSphere Web UI or vSphere client.
- If you are using vSphere Web UI or vSphere client but prefer not to use the cloning feature.

### In This Chapter

- Backing Up Full Systems Using Cloning..... 12
- Restoring a System From a Cloned VM ..... 16

## Backing Up Full Systems Using Cloning

**Important:** If you are using an ESXi client, you cannot clone your EC or DTACS VM. Go to *Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs* (on page 24).

This section provides instructions to complete a full system backup by cloning the active, *primary* EC or DTACS server to a different ESXi host. Review the following two methods to determine how you will clone the *primary* VM.

**Note:** Cisco recommends cloning the VM during a maintenance window.

### ■ Cloning When the VM is Shutdown

- Cloning occurs during a maintenance window.
- Billing transactions and all system updates are suspended during the cloning process.
- Go to *Cloning When the VM is Shutdown* (on page 12).

### ■ Cloning While the VM is Running

- Cloning may cause performance issues depending on the size of the system.
- Cloning occurs during a maintenance window.
- The primary server will process transactions without the interruption of interactive services.
- Go to *Cloning While the VM is Running* (on page 14).

## Cloning When the VM is Shutdown

Complete the following procedure on the *primary* EC or DTACS server to create a clone of the active server. The clone will become a full system backup of the active system.

### 1 Are you cloning an EC VM?

- If **yes**, as **dncs** user, enter the following commands to stop EC system processes.

```
[dncs@vodwater ~]$ appStop  
[dncs@vodwater ~]$ appKill  
[dncs@vodwater ~]$ dncsStop  
[dncs@vodwater ~]$ dncsKill
```

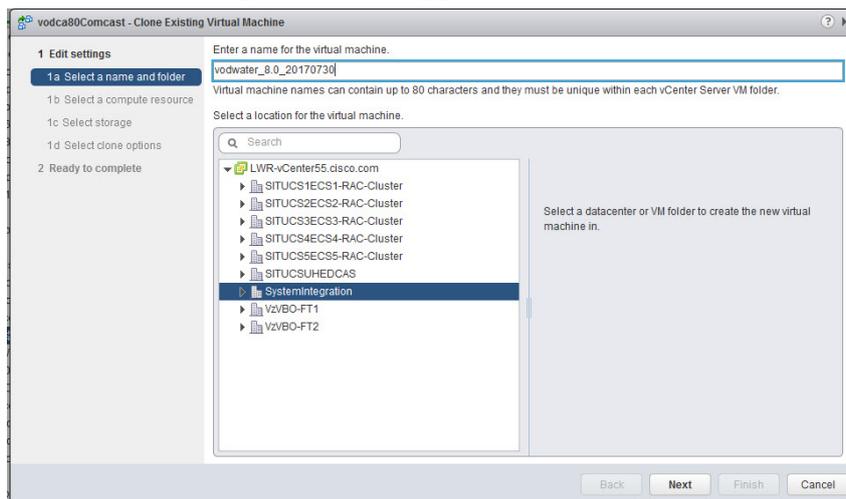
- If **no** and you are cloning a *DTACS* VM, as **dncs** user, enter the following commands to stop *DTACS* system processes.

```
[dncs@dtacs ~]$ dtacsStop
[dncs@dtacs ~]$ dtacsKill
```

- 2 Stop all billing transactions and updates to the *primary* EC or *DTACS* server.
- 3 As **admin** user, type the following command to shutdown the *primary* EC or *DTACS* server.
 

```
[admin@vodwater ~]$ sudo shutdown -h now
```
- 4 From the vSphere Web UI, right-click the *primary* EC or *DTACS* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
- 5 Right-click the *primary* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
- 6 From the **Enter a name for the virtual machine** text box, enter a name for the cloned VM.

**Note:** In this example, we have appended the date to the end of the name.



- 7 Click **Next**.
- 8 Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.
 

**Note:** The compute resource should not be the same resource as the VM you are cloning from.
- 9 Once the compatibility check succeeds, click **Next**. The Select storage window appears.
- 10 Ensure the following settings exist and then click **Next**.
  - The "Select virtual disk format" field is set to **Thin Provision**.
  - The correct NFS share is selected.
- 11 Click **Next** again.
- 12 Review the settings and then click **Finish**.

## Chapter 3 Backup and Restore Using Cloning

- 13 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
- 14 When the VM clone completes, select and right-click the *primary* VM and select **Power On**.
- 15 From a terminal window, login as an administrative user (for example, **ecadmin** or **dtacsadmin**).
- 16 Change to **dncs** user, enter the following commands to start the system processes for the appropriate system.

**EC:**

```
[dncs@vodwater ~]$ dncsStart
```

```
[dncs@vodwater ~]$ appStart
```

**DTACS:**

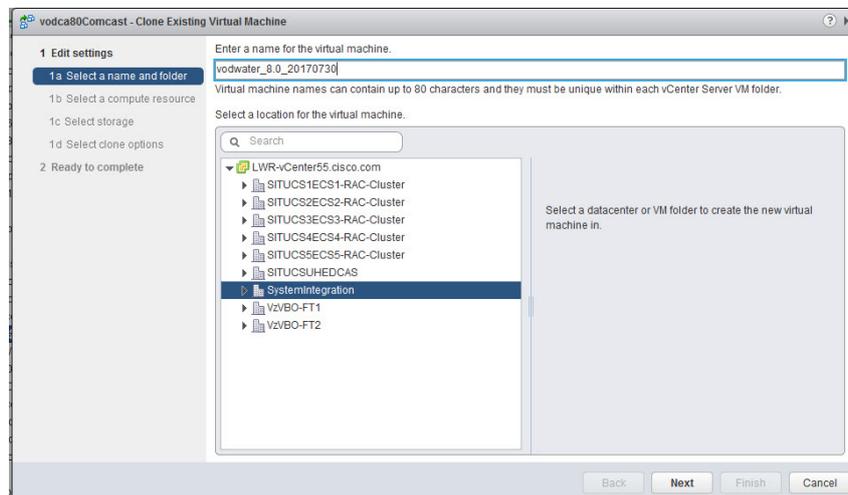
```
[dncs@dtacs_50 ~]$ dtacsStart
```

- 17 Verify system functionality.

## Cloning While the VM is Running

Complete the following procedure on the *primary* server to create a clone of the active server. The clone will become a full system backup of the active system.

- 1 From the vSphere Web UI, right-click the *primary* EC or DTACS server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
- 2 From the **Enter a name for the virtual machine** text box, enter a name for the cloned VM.



- 3 Click **Next**.
- 4 Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.  
**Important:** The compute resource should not be the same resource as the VM you are cloning from.
- 5 Once the compatibility check succeeds, click **Next**. The Select storage window appears.
- 6 Ensure the following settings exist and then click **Next**.
  - The "Select virtual disk format" field is set to **Thin Provision**.
  - The correct NFS share is selected.
- 7 Click **Next** again.
- 8 Review the settings and then click **Finish**.
- 9 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.

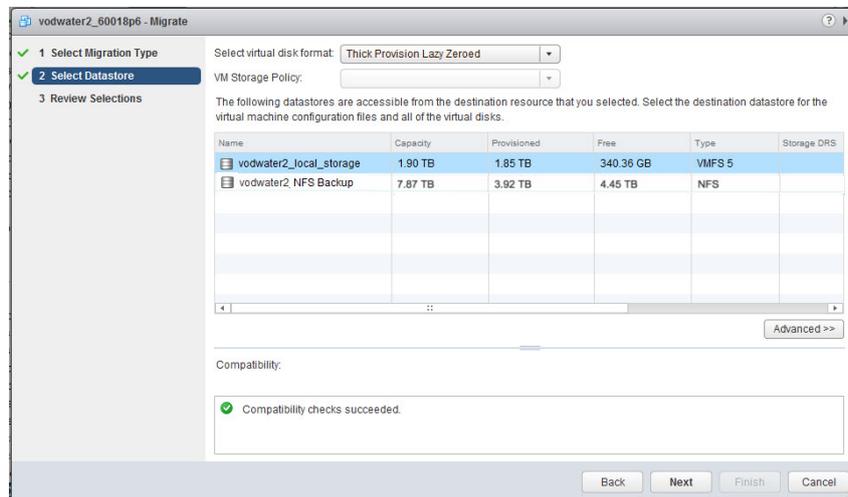
## Restoring a System From a Cloned VM

Complete the following procedure to migrate a cloned VM from the storage device to the ESXi host.

- 1 Do you want to keep the inoperable VM(s) for future troubleshooting?
 

**Important:** You must have enough space on the EXSi host to keep the VM(s) along with the new cloned VMs. If you do not, you must delete the inoperable VMs.

  - If **no**, go to the next step.
  - If **yes**, go to Step 6.
- 2 From the vSphere Web UI, right-click the inoperable *primary* EC or DTACS server and select **All vCenter Actions > Power > Power Off**.
- 3 Monitor the **Recent Tasks** area until the task successfully completes.
- 4 Right-click the inoperable server and select **All vCenter Actions > Delete from Disk**.
- 5 Repeat Steps 2 through 4 on the *secondary* (inoperable) server.
- 6 Right-click the cloned VM and select **Migrate**.
- 7 Select **Change datastore** and click **Next**.
- 8 Select the local datastore for the ESXi host and then click the **Select virtual disk format** dropdown menu.
- 9 Select **Thick Provision Lazy Zeroed** and then click **Next**.



- 10 Review the selections and click **Finish**.
- 11 Monitor the **Recent Tasks** area until the task successfully completes.
- 12 Right-click the EC or DTACS VM and select **Open Console**.
- 13 Login as **admin** user.

- 14 Enter the following command to delete the **70-persistent-net.rules** file.

```
[admin@vodwater ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

- 15 Enter the following command to reboot the VM.

```
[admin@vodwater ~]$ sudo reboot
```

- 16 From a terminal window, log into the VM as **admin** user.

- 17 Enter the following command to delete the **tomcat.pid** file.

```
[admin@vodwater ~]$ sudo rm /var/run/tomcat.pid
```

- 18 Enter the following commands to stop the tomcat and httpd services.

```
[admin@vodwater ~]$ sudo service tomcat stop
[admin@vodwater ~]$ sudo service httpd-dnscs stop
[admin@vodwater ~]$ sudo service httpd stop
```

- 19 Enter the following command to verify if system processes are running.

```
[admin@vodwater ~]$ pgrep -fl dvs
```

- 20 Are system and/or initD processes running?

- If **yes**, go to the next step.
- If **no**, go to Step 22.

- 21 As **dncs** user on the EC or DTACS system, enter the appropriate commands to stop system processes.

**EC:**

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ dnscsStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dnscsKill
```

**Note:** If you are using a third-party application server, refer to the appropriate documentation to stop its services.

**DTACS:**

```
[dncs@dtacs_50 ~]$ dtacsStop
[dncs@dtacs_50 ~]$ dtacsKill
```

- 22 As **root** user on the EC or DTACS system, enter the appropriate command to source the environment.

**EC:**

```
[root@vodwater ~]# . /dvs/dnscs/bin/dnscsSetup
```

**DTACS:**

```
[root@dtacs_50 ~]# . /dvs/dtacs/bin/dtacsSetup
```

- 23 Enter the following command to kill any active sessions.

```
[root@vodwater ~]# killActiveSessions
```

### Chapter 3 Backup and Restore Using Cloning

24 Enter the following command to see if RepDB is enabled.

```
[root@vodwater ~]# onstat -g dri
```

25 Is RepDb enabled?

- If **yes**, go the next step.
- If **no**, go to Step 29.

26 Enter the following command to disable RepDB.

```
[root@vodwater ~]# /opt/cisco/repdb/repDb -d
```

27 When RepDB is successfully disabled, enter the following command to deconfigure RepDB.

```
[root@vodwater ~]# /opt/cisco/repdb/setupRepDbEnv -D
```

28 Repeat Step 24 to verify that RepDB is now disabled.

29 As **admin** user, enter the following command to restore the latest database and key files backup from your NFS device. The database restore begins, and when completed, the key files are restored as well.

#### Command Syntax:

```
sudo /opt/cisco/backup_restore/restoreDBKF -v -B  
[path_to_NFS_DBKF_backup]
```

#### Example:

```
[admin@vodwater ~]$ sudo /opt/cisco/backup_restore/restoreDBKF  
-v -B /shared/vodwater/DBKF/80016
```

```
Beginning restore of database.  
  
opt_backup_uri      /shared/conan/DBKF/80016  
opt_local_tape  
opt_remote_tape  
opt_fake_backup     0  
opt_physical_restore 0  
opt_primary_host  
opt_compress        0  
opt_bzip2           0  
opt_parallel        0  
opt_skip_hpn        0  
opt_interactive     0  
opt_check_database  0  
opt_verbose         1  
  
Checking ontape...  
Checking Repdb...  
  
IBM InFormix Dynamic Server Version 12.10.FC8W1 -- On-Line -- Up 01:15:24 -- 20024824 Kbytes
```

```
var/lib/tftpboot/gqam...  
var/lib/tftpboot/caqam...  
var/lib/tftpboot/aeisf 12  
var/lib/tftpboot/D9485_REL_4P_1_2_22-G.bin.signed  
var/lib/tftpboot/SA-PCG-MIB.my  
var/lib/tftpboot/gqam.config  
var/lib/tftpboot/nc.config  
var/lib/tftpboot/B603_G14  
var/log/dnscsLog  
Successfully restored the Key Files.
```

- 30 Review the following logs in the `/var/log` directory for any warnings or errors.
  - `restoreDatabaseLog`
  - `restoreDatabaseKeyFilesLog`
- 31 Enter the following commands to start the tomcat and httpd services.

```
[admin@vodwater ~]$ sudo service tomcat start
[admin@vodwater ~]$ sudo service httpd-dnscsws start
[admin@vodwater ~]$ sudo service httpd start
```
- 32 Enter the following command to delete `/etc/no_system_start` file.

```
[admin@vodwater ~]$ sudo rm /etc/no_system_start
```
- 33 When prompted to confirm the deletion, type **y** and press **Enter**.
- 34 As **dncs** user on the EC or DTACS, enter the appropriate command(s) to start the system processes.

**EC:**

```
[dncs@vodwater ~]$ dncsStart
[dncs@vodwater ~]$ appStart
```

**Note:** If you are using a third-party application server, refer to the appropriate documentation to start its services.

**DTACS:**

```
[dncs@dtacs_50 ~]$ dtacsStart
```
- 35 As an administrative user, (for example, `ecadmin` or `dtacsadmin`), log into the EC or DTACS Web UI to verify that processes are green.
- 36 Verify system functionality.
- 37 Refer to the chapter, *Configure and Operate the Replicated Database* in the appropriate document to create a secondary server and to enable RepDb.
  - *SR 8.0 Installation and Migration Guide*
  - *DTACS 5.0 Installation and Migration Guide*



# 4

---

## Backup and Restore to an NFS Mount

This chapter includes the procedures to execute a database and key file backup of your system. This should be done daily or weekly.

### In This Chapter

- Back Up the Database and Key Files to an NFS-Mounted Directory ..... 22
- Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs ..... 24
- Restoring the Database and Key Files to an Existing VM..... 27

## Back Up the Database and Key Files to an NFS-Mounted Directory

The database and key files can be backed up to a directory that is located on an NFS-mounted file system. To successfully back up your system to an NFS-mount, you must be able to access the NFS directory and you must have write-access to the directory.

**Note:** The procedures for setting up the NFS are beyond the scope of this document. See your system administrator, if necessary, for help in setting up the NFS.

Complete the following steps to backup the database and key files to an NFS mount.

- 1 Do you have unique files you want to add to the KeyFiles backup list?

**Important:** If the sync list for RepDB includes files that are not included in the default KeyFiles.include list, you *must add the absolute path to each of these files to the KeyFiles.include file.*

- If **yes**, go to the next step.

- If **no**, go to Step 5.

- 2 As **root** user, open the following file in a text editor.

```
[admin@vodwater ~]$ sudo vi /opt/cisco/backup_restore/KeyFiles_templates/KeyFiles.include
```

- 3 Go to the end of the file and add the absolute path to *each* unique file you want to backup.
- 4 Save and close the file.
- 5 Create a new directory on the NFS mount where you want to backup the database and key files.

**Notes:**

- In this procedure, the NFS mount is /shared and the full directory path for the backup is /shared/vodwater/DBKF/80016.
- Each new database and key file backup will overwrite any existing database and key file backup in the path. Therefore, any future updates should be saved to a unique directory on the NFS-mounted device.

**Example:**

```
[admin@vodwater ~]$ sudo mkdir /shared/vodwater/DBKF/SR80016
```

## NFS-Mounted Directory

- Enter the following command to back up the database and key files to the NFS-mounted directory. The database backup begins, and when it completes, the key file backup begins.

**Note:** This could take up to an hour or more depending on the size of your database.

**Command Syntax:**

```
sudo /opt/cisco/backup_restore/backupDBKF -v -B
[path_to_NFS_directory]
```

**Example:**

```
[admin@vodwater SR80016]$ sudo
/opt/cisco/backup_restore/backupDBKF -v -B
/shared/vodwater/SR80016
```

```
Beginning backup of database.
target_uri      file:///shared/vodwater/SR80016/vodwater_12.10.FC8W1_I0.gz
check_database  False
username
password        <unset>
compression:
  method        gzip -c
  extension     .gz
  multithread   False
INFORMIXDIR    /opt/cisco/informix/server
INFORMIXSERVER localhostdbserver
PATH           /bin:/sbin:/usr/sbin:/usr/bin:/opt/cisco/informix/server/bin

-----
Database Backup Information
-----
Command Used:  /opt/cisco/backup_restore/backupDatabase -v -B /shared/vodwater/SR80016
Hostname:     vodwater
INFORMIXSERVER: localhostdbserver
B/R Version:  UNKNOWN
Date:        Tue Jul 25 15:33:32 2017 (1501011212)

Output from 'ifconfig -a':
eth0      Link encap:Ethernet  HWaddr 00:50:56:8B:60:FF
          inet 10.90.47.248  Bcast:10.90.47.255  Mask:255.252.0

/var/lib/tftpboot/ae1s
/var/lib/tftpboot/D9485_REL_4r_1_x_22-G.bin.signed
/var/lib/tftpboot/SA-PCG-MIB.my
/var/lib/tftpboot/gqam.config
/var/lib/tftpboot/nc.config
/var/lib/tftpboot/B603_G14
/var/log/gnacsLog
Successfully backed up the Key Files.
```

- Review the following files in the `/var/log` directory to search for errors or warnings. You can also verify that the keyfiles were backed up the `backupKeyFilesLog` file.

- `backupDatabaseLog`
- `backupKeyFilesLog`

## Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs

**Important:** This procedure assumes that you do not have a clone of your system.

Complete the following procedure if there is a catastrophic failure to your system and you must deploy and install the applications on a new VM.

- 1 From the appropriate installation and migration guide, complete the procedures in the following chapters.
  - **SR 8.0 Installation and Migration Guide**
    - Deploy the EC Virtual Machine
    - Preparing the System for the Installation or Migration
    - SR 8.0 Application Installation
  - **DTACS 5.0 Installation and Migration Guide**
    - Deploy the DTACS Virtual Machine
    - Preparing the System for the Installation or Migration
    - DTACS 5.0 Installation
- 2 As **dncs** user, enter the following command to verify that system processes are not running.

```
[dncs@vodwater ~]$ ps -ef | grep dvs
```
- 3 Are system processes running?
  - If **yes**, enter the following commands for the system you are restoring to stop and kill all processes.

**EC:**

```
[dncs@vodwater ~]$ appStop  
[dncs@vodwater ~]$ appKill  
[dncs@vodwater ~]$ dncsStop  
[dncs@vodwater ~]$ dncsKill
```

**DTACS:**

```
[dncs@dtacs_50 ~]$ dtacsStop  
[dncs@dtacs_50 ~]$ dtacsKill
```
  - If **no**, go to the next step.

## Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs

- 4 As **admin** user, enter the following commands to stop tomcat and httpd services.

```
[admin@vodwater ~]$ sudo service tomcat stop
[admin@vodwater ~]$ sudo service httpd-dnscs stop
[admin@vodwater ~]$ sudo service httpd stop
```

- 5 Enter the following command to restore the database and keyfiles to the new VM. The database restore begins, and when complete, the key files are restored.

**Note:** In this procedure, the NFS mount is /shared and the full directory path for the backup is /shared/vodwater/DBKF/80016.

### Command Syntax:

```
sudo /opt/cisco/backup_restore/restoreDBKF -v -B
[path_to_NFS_DBKF_backup]
```

### Example:

```
[admin@vodwater ~]$ sudo /opt/cisco/backup_restore/restoreDBKF
-v -B /shared/vodwater/DBKF/80016
```



```
Beginning restore of database.
opt_backup_uri      /shared/conan/DBKF/80016
opt_local_tape
opt_remote_tape
opt_fake_backup     0
opt_physical_restore 0
opt_primary_host
opt_compress        0
opt_bzip2           0
opt_parallel        0
opt_skip_hpn        0
opt_interactive     0
opt_check_database  0
opt_verbose         1

Checking ontape...
Checking Repdb...

IBM Informix Dynamic Server Version 12.10.FC8W1 -- On-Line -- Up 01:15:24 -- 20024824 Kbytes

/var/lib/tftpboot/qp
var/lib/tftpboot/caqam_bob
var/lib/tftpboot/aeisf_12
var/lib/tftpboot/D9485_REL_4P_1_2_22-G.bin.signed
var/lib/tftpboot/SA-PCG-MIB.my
var/lib/tftpboot/gqam.config
var/lib/tftpboot/nc.config
var/lib/tftpboot/B603_G14
var/log/dnscsLog
Successfully restored the Key Files.
```

- 6 Review the following logs in the /var/log directory for any warnings or errors.

- restoreDatabaseLog
- restoreDatabaseKeyFilesLog

- 7 Enter the following commands to start the tomcat and httpd services.

```
[admin@vodwater ~]$ sudo tomcat start
[admin@vodwater ~]$ sudo service httpd-dnscs start
[admin@vodwater ~]$ sudo service httpd start
```

## Chapter 4 Backup and Restore to an NFS Mount

- 8 Enter the following command to delete the `/etc/no_system_start` file.  

```
[admin@vodwater ~]$ sudo rm /etc/no_system_start
```
- 9 When prompted to confirm the deletion, type **y** and press **Enter**.
- 10 As **dncs** user, enter the following commands to start system processes.  
**EC:**  

```
[dncs@vodwater ~]$ dncsStart  
[dncs@vodwater ~]$ appStart
```

**DTACS:**  

```
[dncs@dtacs_50 ~]$ dtacsStart
```
- 11 Log into the Web UI and verify that processes are green.
- 12 Verify system functionality.
- 13 Refer to the chapter, *Configure and Operate the Replicated Database* in the appropriate document to create a secondary server and to enable RepDb.
  - *SR 8.0 Installation and Migration Guide*
  - *DTACS 5.0 Installation and Migration Guide*

## Restoring the Database and Key Files to an Existing VM

- 1 As **root** user on the *primary* EC or DTACS server, enter the following command to disable RepDB.

```
[root@vodwater ~]# /opt/cisco/repdb/RepDb -d
```

- 2 When prompted to confirm disabling RepDb, type **y** and press **Enter**.
- 3 Repeat Steps 1 through 2 on the *secondary* EC or DTACS server.
- 4 Enter the following command on the *primary* and the *secondary* EC or DTACS server to verify that the database for each server is ONLINE.

```
[root@vodwater ~]# onstat -g dri
```

- 5 Type the following command to see if system processes are running.

```
[root@vodwater ~]# pgrep -fl dvs
```

- 6 Does the output from Step 5 show that the system or Initd processes are running?

- If **yes**, as **dncs** user on the EC or DTACS server, type the appropriate commands to stop the system processes.

### EC:

```
[dncs@vodwater ~]$ appStop
[dncs@vodwater ~]$ appKill
[dncs@vodwater ~]$ dncsStop
[dncs@vodwater ~]$ dncsKill
```

### DTACS:

```
[dncs@dtacs_50 ~]$ dtacsStop
[dncs@dtacs_50 ~]$ dtacsKill
```

- If **no**, go to the next step.

- 7 As **admin** user, enter the following command to see if the OAM process is running.

```
[admin@vodwater ~]$ pgrep -fl oam
```

- 8 Is OAM running?

- If **yes**, enter the following command to stop the OAM process.

```
[admin@vodwater ~]$ sudo /etc/init.d/oammgrctrl stop
```

- If **no**, continue with the next step.

## Chapter 4 Backup and Restore to an NFS Mount

- 9 Enter the following commands to stop tomcat and httpd services.

```
[admin@vodwater ~]$ sudo service tomcat stop
[admin@vodwater ~]$ sudo service httpd-dnscws stop
[admin@vodwater ~]$ sudo service httpd stop
```

- 10 As **root** user, enter the appropriate command to source the EC or DTACS environment.

**EC:**

```
[root@vodwater ~]# . /dvs/dnscs/bin/dnscsSetup
```

**DTACS:**

```
[root@dtacs_50 ~]# . /dvs/dtacs/bin/dtacsSetup
```

- 11 Enter the following command to see if any active sessions are present on the system.

```
[root@vodwater ~]# showActiveSessions
```

- 12 Do active sessions exist on the system?

- If **yes**, type `killActiveSessions` and press **Enter**.
- If **no**, go to the next step.

- 13 Repeat Step 11 to verify that there are no active sessions are present.

- 14 As **admin** user, enter the following command to restore the database and keyfiles. The database restore begins, and when completed, the key files are restored as well.

**Note:** In this procedure, the NFS mount is `/shared` and the full directory path for the backup is `/shared/vodwater/DBKF/80016`.

**Command Syntax:**

```
sudo /opt/cisco/backup_restore/restoreDBKF -v -B
[path_to_NFS_DBKF_backup]
```

**Example:**

```
[admin@vodwater ~]$ sudo /opt/cisco/backup_restore/restoreDBKF
-v -B /shared/vodwater/DBKF/80016
```

```
Beginning restore of database.
opt_backup_uri      /shared/conan/DBKF/80016
opt_local_tape
opt_remote_tape
opt_fake_backup     0
opt_physical_restore 0
opt_primary_host
opt_compress        0
opt_bzip2           0
opt_parallel        0
opt_skip_hpn        0
opt_interactive     0
opt_check_database  0
opt_verbose         1

Checking ontape...
Checking Repdb...

IBM Informix Dynamic Server Version 12.10.FC8W1 -- On-Line -- Up 01:15:24 -- 20024824 Kbytes

var/lib/tftpboot/qaqam_bob
var/lib/tftpboot/aeisf_12
var/lib/tftpboot/D9485_REL_4P_1_2_22-G.bin.signed
var/lib/tftpboot/SA-PCG-MIB.my
var/lib/tftpboot/gqam.config
var/lib/tftpboot/nc.config
var/lib/tftpboot/B603_G14
var/log/dnscsLog
Successfully restored the Key Files.
```

- 15 Review the following logs in the `/var/log` directory for any warnings or errors.

- `restoreDatabaseLog`
- `restoreDatabaseKeyFilesLog`

- 16 Enter the following commands to start the tomcat and httpd services.

```
[admin@vodwater ~]$ sudo service tomcat start
[admin@vodwater ~]$ sudo service httpd-dnscsws start
[admin@vodwater ~]$ sudo service httpd start
```

- 17 Enter the following command to delete `/etc/no_system_start` file.

```
[admin@vodwater ~]$ sudo rm /etc/no_system_start
```

- 18 When prompted to confirm the deletion, type `y` and press **Enter**.

- 19 As `dncs` user, enter the appropriate command(s) to start system processes.

**EC:**

```
[dncs@vodwater ~]$ dnscsStart
[dncs@vodwater ~]$ appStart
```

**DTACS:**

```
[dncs@dtacs_50 ~]$ dtacsStart
```

#### Chapter 4 Backup and Restore to an NFS Mount

- 20 Log into the EC or DTACS Web UI and verify that processes are green.
- 21 Refer to the chapter, *Configure and Operate the Replicated Database* in the appropriate document to enable RepDb.
  - *SR 8.0 Installation and Migration Guide*
  - *DTACS 5.0 Installation and Migration Guide*
- 22 Verify system and RepDB functionality.

# 5

---

## Customer Information

### **If You Have Questions**

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.



# A

## Modify the Root crontab File for Automating Backups

### Introduction

In EC SR 8.0 and DTACS SR 5.0, the CSCObackup-restore package includes the following script to assist in automating backups:

- /opt/cisco/backup\_restore/DBKFcron.sh

You can run this script from the crontab file. Before you run this on your system, you may wish to change the default behavior of the script.

### In This Appendix

- Configuring the Database and Key Files Backup cron Script..... 34
- Modify the Root crontab File..... 35

## Configuring the Database and Key Files Backup cron Script

- 1 As **admin** user on the EC or DTACS system, type the following command to change to the **/opt/cisco/backup\_restore** directory.  

```
[admin@vodwater ~]$ cd /opt/cisco/backup_restore
```
- 2 Type the following command and press **Enter** to copy the **DBKFcron.sh** script to **DBKFcron\_orig.sh**.  

```
[admin@vodwater backup_restore]$ sudo cp -p DBKFcron.sh DBKFcron_orig.sh
```
- 3 Enter the following command to open the **DBKFcron.sh** file in a text editor.  

```
[admin@vodwater backup_restore]$ sudo vi DBKFcron.sh
```
- 4 Go to the **nfspath** entry and update the value with the path to your backup storage device.
- 5 Go to the **yourEC** entry and update the value to the hostname of your server.  
**Note:** The default *yourEC* variable is set to 'uname -n'. This sets the *yourEC* variable to the current hostname of the system. You may leave it set this way or change it to a name of your choice.
- 6 In the **num\_to\_keep** entry, keep the default value or update the value to the number of backups you want to maintain.
- 7 Save and close the file.  
**Result:** Backups are written to  
`/[path_to_storage]/[hostname]/DBKF/DBKF-#.tar`, where '#' is the backup number. At most, the number of backups that are stored is defined by the 'num\_to\_keep' value. When that number is reached, older backups are deleted.
- 8 Enter the following command to ensure that the **crond** service is running.  

```
[admin@vodwater backup_restore]$ sudo service crond status
```

## Modify the Root crontab File

The following is a sample crontab entry that demonstrates automating nightly backups of the database and key files.

Append the following lines to the root user crontab file. Substitute the appropriate values for [minutes] and [hours]."

```
# Backup Database and KeyFiles  
[minutes] [hours] * * * /opt/cisco/backup_restore/DBKFcron.sh
```

**Example:**

```
# Backup Database and KeyFiles  
0 1 * * * /opt/cisco/backup_restore/backup_restore/DBKFcron.sh
```

**Note:** This example backs up the database and key files every night at 01:00 (1 am).



# Index

---

## **B**

- Back Up the Database and Key Files to an NFS-Mounted Directory • 22
- Backing Up Full Systems Using Cloning • 12
- Backing Up Unique Key Files • 9
- Backup and Restore to an NFS Mount • 21
- Backup and Restore Using Cloning • 11
- Backup Recommendations • 5

## **C**

- Cloning When the VM is Shutdown • 12
- Cloning While the VM is Running • 14
- Configuring the Database and Key Files Backup cron Script • 34
- Customer Information • 31

## **F**

- File System Backup • 7
- Full System Backup • 6

## **H**

- Hardware Compatibility • 1
- Hardware Platform Compatibility • 2

## **I**

- Informix Database and Key Files Backup • 6

## **M**

- Modify the Root crontab File • 35

## **N**

- NFS-Mounted Directory Requirements • 7

## **P**

- Prepare for the Backup • 8

## **R**

- Recording Network Configuration Information • 8
- Restoring a System From a Cloned VM • 16

- Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs • 24

- Restoring the Database and Key Files to an Existing VM • 27

## **S**

- Supported External Backup Devices • 3
- System Backup Frequency • 6



**Americas Headquarters**

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

<http://www.cisco.com>

Tel: 408 526-4000

800 553-6387

Fax: 408 527-0883

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2018 Cisco and/or its affiliates. All rights reserved.

January 2018

Part Number TP-00138-01