



Backup and Restore User Guide for EC 9.0 and DTACS 5.2

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.

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

© 2018-2019 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

About This Guide	v
Chapter 1 Hardware Compatibility	1
Hardware Platform Compatibility	2
Supported External Backup Devices.....	3
Chapter 2 Backup Recommendations	5
System Backup Frequency	6
Prepare for the Backup.....	8
Chapter 3 Backup and Restore Using Cloning	9
Backing Up Full Systems Using Cloning.....	10
Restoring a System From a Cloned VM.....	13
Chapter 4 Backup and Restore to an NFS Mount	17
Backing Up the Database and Key Files to an NFS-Mounted Directory	18
Restoring the Database and Key Files to an Existing VM.....	21
Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs.....	24
Chapter 5 Customer Information	27
Appendix A Modify the root crontab File for Automating Backups	29
Configuring the Database and Key Files Backup cron Script.....	30
Modify the Root crontab File.....	31
Index	33

About This Guide

Purpose

This guide provides a full set of backup and restore procedures for the Cisco Explorer Controller (EC) System Release (SR) 9.0 and for the Cisco Digital Transport Adaptor Control System (DTACS) SR 5.2 database, as well as for their respective key files.

Scope

The procedures in this guide are for backing up and restoring the EC and DTACS systems. All examples within the documentation use vSphere Web UI version 6.0.

Note: System operators who support ECs using third-party 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) products:

- EC 9.0
- DTACS 5.2

Backup and Restore Scripts

This guide refers to version 9.0.6 of the backup and restore scripts. These scripts are included with each EC and DTACS installation. The backup and restore scripts are installed in the `/opt/cisco/backup_restore` directory as a part of the `CSCObakup-restore-9.0.*` rpm. You can confirm the version by running the `rpm -qa | grep -i backup` command.

Revision History

Revision Date	Modification
20190405	Minor updates
20180829	Updated for release
20180129	Initial draft

About This Guide

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 9.0 of the backup and restore scripts, which are part of the NextX 9.0 repositories (repos), have been tested and verified against the following hardware platforms:

- UCS C240 M3
- UCS C240 M4

Supported External Backup Devices

Version 9.0 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.

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 not* supported in EC 9.0 or in DTACS 5.2 as cloning the VM replaces a full file system backup. This creates a file system, database and key files backup. The VM can be cloned while it is running or while it is shutdown.

A VM clone should be executed 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 the 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 the vSphere Web UI. Refer to *Full System Backup* (on page 6) for details.

NFS-Mounted Directory Requirements

Network file systems (NFS) 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

Complete the following steps to record information that will be useful for any backup or restore operation, and especially useful when backing up or restoring across the network.

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

```
[admin@ecnextx90/dtacs52 ~]$ ifconfig -a
```
- 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/DTACS system via cloning.

Important: Skip this chapter and go to *Backup and Restore to an NFS Mount* (on page 17) if you prefer not to use the cloning feature.

In This Chapter

- Backing Up Full Systems Using Cloning..... 10
- Restoring a System From a Cloned VM..... 13

Backing Up Full Systems Using Cloning

This section provides instructions to complete a full system backup by cloning the active, *primary* EC/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 EC/DTACS 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 10).

■ 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 12).

Cloning When the VM is Shutdown

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

- 1 As **dncs** user on the *primary* EC/DTACS server, enter the following commands to stop system processes.

EC:

```
[dncs@ecnextx90 ~]$ appStop  
[dncs@ecnextx90 ~]$ appKill  
[dncs@ecnextx90 ~]$ dncsStop  
[dncs@ecnextx90 ~]$ dncsKill
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStop  
[dncs@dtacs52 ~]$ dtacsKill
```

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

```
[admin@ecnextx90/dtacs52 ~]$ sudo shutdown -h now
```

- 4 From the vSphere Web UI, right-click the *primary* EC/DTACS VM and select **Clone > Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
- 5 From the **Enter a name for the virtual machine** text box, enter a name for the cloned VM.
Note: You can simply add the current date to the end of the name to differentiate the two VMs (for example, ecnextx90_20190329).
- 6 Click **Next**.
- 7 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 on the same resource as the VM you are cloning.
- 8 Once the compatibility check succeeds, click **Next**. The Select storage window appears.
- 9 Ensure the following settings exist and then click **Next**.
 - The "Select virtual disk format" field is set to **Same format as source**.
 - The correct NFS share is selected.
- 10 Click **Next** again.
- 11 Review the settings and then click **Finish**.
- 12 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
- 13 When the VM clone completes, select and right-click the *primary* VM and select **Power > Power On**.
- 14 As **dncs** user, enter the following commands to start the system processes.
EC:

```
[dncs@ecnextx90 ~]$ dncsStart  
[dncs@ecnextx90 ~]$ appStart
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStart
```
- 15 Verify system functionality.

Cloning While the VM is Running

Complete the following procedure on the *primary* EC/DTACS 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/DTACS server and select **Clone > 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.

Note: You can simply add the current date to the end of the name to differentiate the two VMs (for example, ecnextx90_20190329).

- 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 on the same resource as the VM from which you are cloning.

- 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 **Same format as source**.
 - The correct NFS share is selected.
- 7 Click **Next** again. The Select clone options window displays.
- 8 Click **Next**. The Customize vApp properties window displays.

Important: Do not update any fields in this window as the ifcfg-ens192 configuration file overrides these properties.

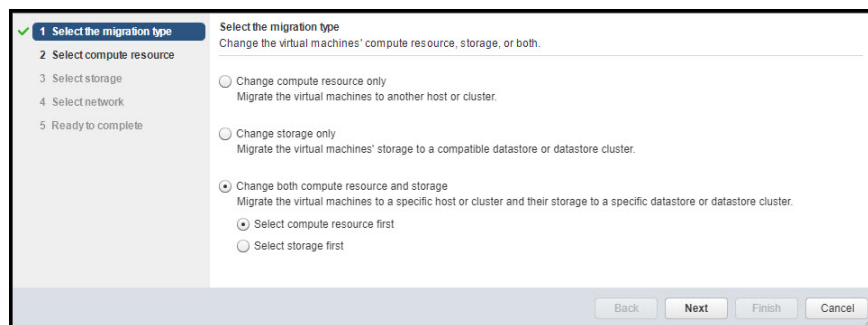
Click **Next**. The Ready to complete window displays.

- 9 Review the settings and then click **Finish**.
- 10 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 restore an EC/DTACS system from a cloned VM.

- 1 Do you want to keep the inoperable EC/DTACS 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/DTACS server and select **Power > Power Off**.
- 3 Monitor the **Recent Tasks** area until the task successfully completes.
- 4 Right-click the inoperable server and select **Delete from Disk**.
- 5 Repeat Steps 2 through 4 on the *secondary* (inoperable) server. Then go to Step 16.
- 6 Right-click the inoperable VM and select **Migrate**. The Select the migration type view displays.



- 7 Select **Change both compute resource and storage**.
- 8 Maintain the **Select compute resource first** selection and then click **Next**. The Select compute resource view displays.
- 9 Select the destination compute resource. A compatibility check is executed.
- 10 When the "compatibility check succeeded" message appears, click **Next**. The Select storage window opens.
- 11 Select the appropriate datastore storage device (for example, Guest-LUN) and then ensure that the **Select virtual disk format** is set to **Same format as source**.
- 12 Click **Next**. The Select network window opens.
- 13 If needed, update the destination network for each source network. Click **Next**. The Ready to Complete window opens.
- 14 Review the settings and click **Finish**.

Chapter 3 Backup and Restore Using Cloning

- 15 Monitor the **Recent Tasks** area until the VM is successfully migrated.
- 16 From the vSphere Web UI, right-click the EC/DTACS VM clone and select **Power > Power On**.
- 17 From a terminal window, login as **admin** user.
- 18 Enter the following command to verify if system processes or the InitD process is running.

```
[admin@ecnextx90/dtacs52 ~]$ pgrep -fl dvs | grep -i init
```

- 19 Are system and/or initD processes running?
 - If **yes**, go to the next step.
 - If **no**, go to Step 21.
- 20 As **dncs** user, enter the appropriate commands, as needed, to stop processes.

EC:

```
[dncs@ecnextx90 ~]$ appStop
[dncs@ecnextx90 ~]$ dncsStop
[dncs@ecnextx90 ~]$ appKill
[dncs@ecnextx90 ~]$ dncsKill
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStop
[dncs@dtacs52 ~]$ dtacsKill
```

- 21 As **root** user, enter the appropriate command to source the environment.

EC:

```
[root@ecnextx90 ~]# . /dvs/dncs/bin/dncsSetup
```

DTACS:

```
[root@dtacs52 ~]# . /dvs/dtacs/bin/dtacsSetup
```

- 22 Enter the following command to determine if any active sessions are running on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# showActiveSessions
```

- 23 Are active sessions present on the system?
 - If **no**, go to the Step 25.
 - If **yes**, enter the following command and then go to the next step.

```
[root@ecnextx90/dtacs52 ~]# killActiveSessions
```

- 24 Repeat Step 22.
- 25 Enter the following command to see if RepDB is enabled.

```
[root@ecnextx90/dtacs52 ~]# onstat -g dri
```

- 26 Is RepDB enabled?
 - If **yes**, go the next step.
 - If **no**, go to Step 29.

- 27 Enter the following command to disable RepDB.

```
[root@ecnextx90/dtacs52 ~]# /opt/cisco/repdb/RepDb -d
```

- 28 Repeat Step 25 to verify that RepDB is now disabled.

- 29 Enter the following command to restore the latest database and key files backup from your NFS device. The database restore begins, and when complete, the key files are restored.

Command Syntax:

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

Example:

```
[root@ecnextx90/dtacs52 ~]#  
/opt/cisco/backup_restore/restoreDBKF -v  
/shared/nextx90/DBKF/SR9.0
```

Example Output:

```
Beginning restore of database.  
opt_backup_uri          /shared/nextx90/DBKF/SR9.0  
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 00:14:39 --  
19978028 Kbytes  
Checking repdb type...  
0  
  
...  
Checking Session Count...  
INFORMIXDIR            /opt/cisco/informix/server  
INFORMIXSERVER         localhostdbserver  
PATH  
/bin:/sbin:/usr/sbin:/usr/bin:/opt/cisco/informix/server/bin  
Looking for ecnextx90_12.10.FC8W1_L0.gz on file:///shared/nextx90/DBKF/SR9.0  
Restoring from URI  
file:///shared/nextx90/DBKF/SR9.0/ecnextx90_12.10.FC8W1_L0.gz  
restoreDatabase(15014) +-pstree(15032)  
                    ^-tee(15031)  
PROCESS:                tee , PID: 15031  
  
...  
Creating /opt/cisco/informix/server/etc/onconfig.tape...  
Matched TAPEDEV Line: TAPEDEV /dev/null  
Modified TAPEDEV Line: TAPEDEV STDIO  
.  
.
```

Chapter 3 Backup and Restore Using Cloning

```
Program over.
ontape -r restore of localhostdbserver finished at: Weds Mar 27 19:40:37 2019
Waiting for Informix engine to be Quiescent...
Pruning unused zero size chunks...
Shutting down Informix engine..
Bringing Informix engine back On-Line...
Successfully restored the database.
tee
Finished restore of database.
Beginning restore of KeyFiles.
Looking for KeyFiles.tar.gz on file:///shared/nextx90/DBKF/SR9.0
opt_backup_uri: file:///shared/nextx90/DBKF/SR9.0
Restoring Key Files from KeyFiles.tar.gz...
/bin/cat /shared/nextx90/DBKF/SR9.0/KeyFiles.tar.gz | gzip -dc | /bin/tar xfv
- -C
.
.
var/lib/tftpboot/pcg_t1
var/log/dnscsLog
Successfully restored the Key Files.
```

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

- **restoreDatabaseLog**
- **restoreKeyFilesLog**

31 Enter the following commands to start the tomcat and httpd services on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# systemctl restart tomcat
[root@ecnextx90/dtacs52 ~]# systemctl restart httpd-dnscsws
[root@ecnextx90/dtacs52 ~]# systemctl restart httpd
```

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

```
[root@ecnextx90/dtacs52 ~]# rm /etc/no_system_start
```

33 When prompted to confirm the deletion, type **y** and press **Enter**.

34 As **dnscs** user, enter the appropriate commands to start system processes.

EC:

```
[dnscs@ecnextx90 ~]$ dnscsStart
[dnscs@ecnextx90 ~]$ appStart
```

DTACS:

```
[dnscs@dtacs52 ~]$ dtacsStart
```

35 Log into the EC/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 one of the listed documents to create a *secondary* server and to enable RepDb.

- *SR 9.0 Installation and Migration Guide*
- *DTACS 5.2 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. Backups should be done daily or weekly.

In This Chapter

- Backing Up the Database and Key Files to an NFS-Mounted Directory 18
- Restoring the Database and Key Files to an Existing VM..... 21
- Restoring the Database and Key Files After a Catastrophic Failure to the Primary and Secondary VMs..... 24

Backing 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 have access and write privileges to the NFS 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 EC/DTACS 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 **admin** user, enter the following command to open the **KeyFiles.include** file in a text editor.

```
[admin@ecnextx90/dtacs52 ~]$ 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/nextx90/DBKF/SR9.0.
- 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@ecnextx90/dtacs52 ~]$ sudo mkdir  
/shared/nextx90/DBKF/SR9.0
```

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

- 6 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@ecnextx90/dtacs52 ~]$ sudo  
/opt/cisco/backup_restore/backupDBKF -v -B  
/backups/nextx90/DBKF/SR9.0
```

Example Output:

```
target_uri      file:///shared/nextx90/DBKF/SR9.0/ecnextx90_12.10.FC8W1_L0.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/nextx90/DBKF/SR9.0  
Hostname:     ecnextx90  
INFORMIXSERVER: localhostdbserver  
B/R Version:  UNKNOWN  
Date:        Weds Mar 27 16:42:35 2018 (1517244155)
```

```
.  
.  
ontape backup of localhostdbserver started at: Weds Mar 27 16:42:35 2018  
onmode -c; /usr/bin/env ONCONFIG=onconfig.tape ontape -s -L 0 -t STDIO -d -v  
| gzip -c | /usr/bin/curl --verbose --show-error --fail --insecure --tcp-  
nodelay --buffer --upload-file -  
file:///shared/nextx90/DBKF/SR9.0/ecnextx90_12.10.FC8W1_L0.gz
```

```
.  
.  
Successfully completed the Database backup..
```

```
Generating a list of files to be backed up...
```

```
List of files in %key_files:  
/disk1/appdata/cmd2000_netlogs  
/disk1/dvs/appFiles  
/disk1/dvs/backups  
/disk1/dvs/dvsFiles
```

```
.  
.  
/var/lib/tftpboot/pcg_t1  
/var/log/dnscsLog
```

```
Successfully backed up the Key Files.
```

Chapter 4 Backup and Restore to an NFS Mount

- 7 Review the following files in the **/var/log** directory to search for errors or warnings.
 - **backupDatabaseLog**
 - **backupKeyFilesLog**

Restoring the Database and Key Files to an Existing VM

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

```
[root@ecnextx90/dtacs52 ~]# /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/DTACS server.
- 4 Enter the following commands on the *primary* EC/DTACS server to verify that the database is ONLINE.

EC:

```
[root@ecnextx90 ~]# . /dvs/dncs/bin/dncsSetup
```

```
[root@ecnextx90 ~]# onstat -g dri
```

DTACS:

```
[root@dtacs52 ~]# . /dvs/dtacs/bin/dtacsSetup
```

```
[root@dtacs52 ~]# onstat -g dri
```

- 5 Repeat Step 4 on the *secondary* EC/DTACS server.
- 6 Type the following command on the *primary* server to see if system processes are running.

```
[root@ecnextx90/dtacs52 ~]# pgrep -fl dvs
```

- 7 Did the output from Step 6 show that the system or InitD processes are running?

- If **yes**, as **dncs** user, type the appropriate commands to stop the processes.

EC:

```
[dncs@ecnextx90 ~]$ appStop
```

```
[dncs@ecnextx90 ~]$ appKill
```

```
[dncs@ecnextx90 ~]$ dncsStop
```

```
[dncs@ecnextx90 ~]$ dncsKill
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStop
```

```
[dncs@dtacs52 ~]$ dtacsKill
```

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

- 8 Return to the **root** terminal session and enter the following commands to stop tomcat and httpd services.

```
[root@ecnextx90/dtacs52 ~]# systemctl stop tomcat
```

```
[root@ecnextx90/dtacs52 ~]# systemctl stop httpd-dncsws
```

```
[root@ecnextx90/dtacs52 ~]# systemctl stop httpd
```

Chapter 4 Backup and Restore to an NFS Mount

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

Note: The environment variables should still be sourced. If they are not, source them before running this command.

```
[root@ecnextx90/dtacs52 ~]# showActiveSessions
```

- 10 Do active sessions exist on the system?

- If **yes**, type `killActiveSessions` and press **Enter**. Then go to the next step.
- If **no**, go to Step 12.

- 11 Repeat Step 9 to verify that there are no active sessions present.

- 12 Enter the following command to restore the database and keyfiles. 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/ecnextx90/DBKF/SR9.0`.

Command Syntax:

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

Example:

```
[root@ecnextx90/dtacs52 ~]#  
/opt/cisco/backup_restore/restoreDBKF -v -B  
/shared/nextx90/DBKF/SR9.0
```

- 13 When the restore completes, review the following logs in the `/var/log` directory for any warnings or errors.

- `restoreDatabaseLog`
- `restoreKeyFilesLog`

- 14 Enter the following commands to start the tomcat and httpd services on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# systemctl start tomcat  
[root@ecnextx90/dtacs52 ~]# systemctl start httpd-dnscsws  
[root@ecnextx90/dtacs52 ~]# systemctl start httpd
```

- 15 Enter the following command to delete `/etc/no_system_start` file on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# rm /etc/no_system_start
```

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

- 17 As `dncs` user, enter the appropriate commands to start system processes.

EC:

```
[dncs@ecnextx90 ~]$ dncsStart  
[dncs@ecnextx90 ~]$ appStart
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStart
```

Restoring the Database and Key Files to an Existing VM

- 18 Log into the Web UI and verify that processes are green.
- 19 Refer to the chapter, *Configure and Operate the Replicated Database* in one of the listed documents to enable RepDB.
 - *SR 9.0 Installation and Migration Guide*
 - *DTACS 5.2 Installation and Migration Guide*
- 20 Verify system functionality.

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 9.0 Installation and Migration Guide**

- Chapter 3: Deploy the EC Virtual Machine
- Chapter 4: SR 9.0 Application Installation

- **DTACS 5.2 Installation and Migration Guide**

- Chapter 3: Deploy the EC Virtual Machine
- Chapter 4: DTACS 5.2 Installation

- 2 As **dncs** user, enter the following command to verify that system processes are not running.

```
[dncs@ecnextx90/dtacs52 ~]$ ps -ef | grep dvs
```

- 3 Are system processes running?

- If **yes**, enter the appropriate commands to stop and kill all processes.

EC:

```
[dncs@ecnextx90 ~]$ appStop  
[dncs@ecnextx90 ~]$ appKill  
[dncs@ecnextx90 ~]$ dncsStop  
[dncs@ecnextx90 ~]$ dncsKill
```

DTACS:

```
[dncs@dtacs52 ~]$ dtacsStop  
[dncs@dtacs52 ~]$ dtacsKill
```

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

- 4 As **root** user, enter the following commands to stop tomcat and httpd services on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# systemctl stop tomcat  
[root@ecnextx90/dtacs52 ~]# systemctl stop httpd-dnscsws  
[root@ecnextx90/dtacs52 ~]# systemctl stop httpd
```


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

- 5 Enter the following command to restore the database and keyfiles to the new EC/DTACS 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/nextx90/DBKF/SR9.0.

Command Syntax:

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

Example:

```
[root@ecnextx90/dtacs52 ~]#  
/opt/cisco/backup_restore/restoreDBKF -v -B  
/shared/nextx90/DBKF/SR9.0
```

- 6 When the restore completes, review the following logs in the **/var/log** directory for any warnings or errors.

- **restoreDatabaseLog**

- **restoreKeyFilesLog**

- 7 Enter the following commands to start the tomcat and httpd services on the EC/DTACS.

```
[root@ecnextx90/dtacs52 ~]# systemctl start tomcat  
[root@ecnextx90/dtacs52 ~]# systemctl httpd-dnscws  
[root@ecnextx90/dtacs52 ~]# systemctl start httpd
```

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

```
[root@ecnextx90/dtacs52 ~]# rm /etc/no_system_start
```

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

- 10 As **dncs** user, enter the appropriate commands to start system processes.

EC:

```
[dncs@ecnextx90 ~]$ dncsStart  
[dncs@ecnextx90 ~]$ appStart
```

DTACS:

```
[dncs@dtacs52 ~]$ 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 one of the listed documents to create a *secondary* server and to enable RepDB.

- *SR 9.0 Installation and Migration Guide*

- *DTACS 5.2 Installation and Migration Guide*

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 9.0 and DTACS 5.2, 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..... 30
- Modify the Root crontab File..... 31

Configuring the Database and Key Files Backup cron Script

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

```
[admin@ecnextx90/dtacs52 ~]$ cd /opt/cisco/backup_restore
```

- 2 Type the following command and press **Enter** to copy the DBKFcron.sh script to **DBKFcron_orig.sh**.

```
[admin@ecnextx90/dtacs52 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@ecnextx90/dtacs52 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 EC/DTACS 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@ecnextx90/dtacs52 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

- Backing Up Full Systems Using Cloning • 10
- Backing Up the Database and Key Files to an NFS-Mounted Directory • 18
- Backing Up Unique Key Files • 8
- Backup and Restore to an NFS Mount • 17
- Backup and Restore Using Cloning • 9
- Backup Recommendations • 5

C

- Cloning When the VM is Shutdown • 10
- Cloning While the VM is Running • 12
- Configuring the Database and Key Files Backup cron Script • 30
- Customer Information • 27

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 • 31

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 • 13

- 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 • 21

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.

© 2019 Cisco and/or its affiliates. All rights reserved.

April 2019