PowerKEY iDNCS Backup and Restore

User Guide

Please Read

Important

Please 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

Contents

About This Guide

Purpose

This guide provides a full set of backup and restore procedures for the iDNCS databases, as well as for their respective key files and file systems.

Scope

The procedures in this guide are for backing up and restoring the iDNCS.

Audience

These backup and restore procedures are written for operators who support the following PowerKEY iDNCS System Releases (SRs):

- SR i4.5.0.0 and later

Field service and software installation engineers may also find the information in this guide useful as they assist system operators in installing, troubleshooting, and maintaining their systems.

DBDS Maintenance ISO File

This guide refers to Version 6.4.xx of the backup and restore scripts. These scripts will be included with each SR i4.5.x.x ISO image. Check with Cisco Services if you are unsure of the version of backup and restore scripts that are contained on iDNCS ISO.

Document Version

This is the first formal release of this document.

1

Release Notes

Introduction

This chapter lists any bug report (BR) IDs that were implemented during the development and testing of the backup and restore procedures covered in this guide, as well as the hardware platforms with which the backup and restore scripts are compatible.

In This Chapter

Hardware Platform Compatibility

Version 6.0.x of the backup and restore scripts, which is part of the iDNCS installation or upgrade ISO, has been tested against the following hardware platforms.

- Oracle M3000
- Oracle T5-2

Supported External Backup Devices

Version 6.0.x of the backup and restore scripts have been tested using the following external storage devices:

- LTO 4 tape drive
- NAS Drive NFS-mounted
- Network File System (NFS)-mounted file systems

Note: For additional information, see ***Storage Requirements*** (on page 39).

Bug Report IDs

There are no known Bug Reports (BR) against this version of the Backup/Restore package.

2

Backup Recommendations

Introduction

This chapter provides recommendations for the frequency with which system operators should back up the data of their DBDS. 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 DBDS system.

This release does not support backup and restore operations to or from tape devices. File system and database backups should be performed to the following devices:

- The database and key files can be backed up to an internal file system with sufficient space, or to an external disk device directly connected to the hardware platform.
  Note: If you back up the database to an internal file system, be sure to copy the backup to an external storage device as soon as possible.
- The file system should be backed up to network-accessible devices. Network devices must be NFS-mounted.

In This Chapter

System Backup Frequency

System operators can ensure the integrity of their data only by adhering to a regular schedule of database and file system backups. The recommendations in this section provide some guidance regarding the frequency with which system backups should occur. Adjust these recommendations, if necessary, according to the size of the system and the frequency with which the data changes.

Full System Backup

A full system backup refers to a backup of the file systems and the database.

System operators should perform a complete system backup prior to making any substantial modification to the system.

In addition, system operators should perform a complete system backup just prior to upgrading to new system software, as well as immediately after the acceptance sign-off. The backup just prior to the upgrade can be used in case there is a catastrophic failure of the upgrade.

Informix Database and Key Files Backup

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). System operators should perform a complete backup of the Informix database once a day. In addition, system operators should perform a complete backup of the database immediately before and after a channel lineup change or a major system configuration change.

Note: Beginning with BR 6.0.x, you can now back up the database to a file without stopping system components. Even though you are no longer required to stop system components to perform a database backup to a file system, our engineers highly recommend that you schedule backups during periods of lowest system activity.

File System Backup

System operators should perform a complete backup of the DBDS file systems once a week.

Note: You can now back up the file system of the DBDS without shutting down the system components. Our engineers highly recommend that you schedule your file system backups for periods of lowest system activity.

NFS-Mounted Directory Requirements

Network file systems must meet the following requirements in order to be used for file system and database backups:

- Must be accessible from the DBDS 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.

Considerations About the Backup Procedures

System Shutdown No Longer Required for Backups

System operators no longer have to shut down their system in order to back up the DBDS. The backup procedures reflect this change.

Important: Even though you are no longer required to shut down the system components, our engineers highly recommend that you schedule all your file system backups for periods of lowest system activity.

Prepare for the Backup

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. Type the following command in an xterm window on the server you are backing up and then press **Enter**.

   `ifconfig -a`

   Result: Output similar to the following appears.

```
bash-3.2# ifconfig -a
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu
8232 index 1
        inet 127.0.0.1 netmask ff000000
ixgbe0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
2
        inet 192.168.1.1 netmask ffffff00 broadcast 192.168.1.255
        ether 0:10:e0:57:47:8e
ixgbe1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
3
        inet 10.253.0.1 netmask ffffc000 broadcast 10.253.63.255
        ether 0:10:e0:57:47:8f
ixgbe2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
4
        inet 192.168.100.102 netmask ffffff00 broadcast 192.168.100.255
        ether 0:10:e0:57:47:90
ixgbe3: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
5
        inet 10.78.203.178 netmask ff000000 broadcast 10.255.255.255
        ether 0:10:e0:57:47:91
```

2. Note the dncsatm and the network interfaces and record the information.

   Example: These interfaces are noted by ixgbe0 and ixgbe1 in the example from Step 1.

3. Cross-reference your data from Steps 1 and 2 with what is contained in the /etc/hosts file.

   Note: The data should match. If it does not, resolve the mismatch or call Cisco Services for assistance.

3

Back Up the System to an NFS-Mounted Directory

Introduction

Use the procedures in this chapter to back up the file system and database to an NFS-mounted directory.

In This Chapter

Back Up the File System to an NFS-Mounted Directory

The file system can be backed up to a directory that is located on an NFS-mounted file system. You must be able to access the NFS directory through the /net/[remotehost]/[path_to_NFS_directory] directory structure. In addition, you must have write-access to the directory or the backup will fail.

Note: 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.

Important: All commands in this procedure must be executed as **root** user. We recommend creating an FS (for file system), and DBKF (for database and key files) directory in the NFS directory path.

Example:

- /net/192.0.2.1/backups/pepe/FS
- /net/192.0.2.1/backups/pepe/DBKF

1 Ensure that you have write-access to the NFS-mounted file system and backup directory.

2 To back up a file system over NFS, type the following command and press **Enter**.

```
/usr/local/backup_restore/backupFileSystems –v –B
/net/[remotehost]/[path_to_NFS_directory/[hostname]/FS
```

Notes:

- The [remotehost] should be replaced with the actual hostname or IP address of the remote computer system which is exporting (or shares) the file system into which you will write the backup.
- The *-B* option allows you to define a backup directory path.
- The [path_to_NFS_directory] represents the directory path on the remote host which will hold the backup files.
- The [hostname] should be replaced with the hostname of the system you are backing up.
- This can be a very lengthy command. Type to the end of the command before you press **Enter**. The command is likely to wrap to the following line.

Example:

```
/usr/local/backup_restore/backupFileSystems –v –B
/net/192.0.2.1/backups/pepe/FS
```

3 Record the exact path to the file system backup.

Notes:

- The path should be the path you used with the backup command.
- You can back up the file system to the same path multiple times. Each new backup archive creates its own date/time directory in the path. The directory name consists of the hostname, date, and time of the backup.

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. You must be able to access the NFS directory through the /net/[remotehost]/[path_to_NFS_directory] directory structure. In addition, you must have write-access to the directory or the backup will fail.

Note: 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.

Important: All commands in this procedure must be executed as **root** user.

1 Make sure that you have write-access to the NFS-mounted file system and backup directory.

2 To back up the database and key files, type the following command and press **Enter**.

```
/usr/local/backup_restore/backupDBKF –v –B
/net/[remotehost]/[path_to_NFS_directory/[hostname]/DBKF/[Date
]
```

Notes:

- The [remotehost] should be replaced with the actual hostname or IP address of the remote computer system which is exporting (or shares) the file system into which you will write the backup.
- The [path_to_NFS_directory] represents the directory path on the remote host which holds the database backup.
- The [hostname] should be replaced with the hostname of the system you are backing up.
- The [Date] should be replaced with a date and timestamp which reflects the time that the backup was executed
- This can be a very lengthy command. Type to the end of the command before you press **Enter**. The command is likely to wrap to the following line.

Example:

```
/usr/local/backup_restore/backupDBKF –v –B
/net/192.0.2.1/backups/pepe/DBKF/2013-08-01T12:00:00
```

3 Write down the exact path to the database and key files backup.

Notes:

- The path should be the path you used with the backup command.
- Each new database and key file backup will overwrite any existing database and key file backup in the path. The use of a date stamp in the path will allow you to store multiple copies of backups.
- The DBKF backup will create a gzip file containing the backup. The file name will be of the form: <hostname>_11.70.FC4_L0.gz.

  Example: Using Step 2 as an example, the path to this backup is:

  `/net/192.0.2.1/backups/pepe/DBKF/2013_0801T12:00:00/conan_11.70.FC4_L0.gz`
- The script also creates a file containing the default key files in the same path. The file name will be KeyFiles.tar.gz.

4

Restore the System from an NFS-Mounted Directory

Introduction

Use the procedures in this chapter to restore the file system and database from an NFS-mounted directory

In This Chapter

Restore the DBDS File System from an NFS-Mounted Directory

The following steps describe how to restore the DBDS file system from a specified backup directory on the network.

Important:

- All commands in this procedure must be executed as **root** user.
- You need the following information to configure the network interface:
  - The interface name to the NFS-mounted storage
  - The IP address for this interface
  - The netmask for this interface
  - If the NFS server is on a separate subnet, you will also need to create a route to that subnet

Note: Use the information you recorded in ***Prepare for the Backup*** (on page 10).

1. Ensure that the server is in OK> prompt and the SRDVD is inserted on DVD drive.
2. From Console connection execute the following command:

   ok> boot cdrom -SAshell

3 The DNCS server boots into the solairs SAshell Environment.

4 Type the following command and press **Enter** to configure the network interface.

`ifconfig [interface] plumb [IP address] netmask [netmask] up`

Notes:

- Replace [interface] with the actual interface to be configured
- Replace [IP address] with the actual IP address to the NFS storage
- Replace [netmask] with the actual netmask for the interface

Example: **`ifconfig bge2 plumb 192.0.2.32 netmask 255.255.254.0 up`**

5 Ping the IP address of the NFS server to which you backed up this system.

6 Was the ping successful?

- If **yes**, go to Step 6.
- If **no**, is the NFS server on a separate subnet.
  - If **yes**, type the following command and press **Enter** to add a router to the subnet. Then, repeat Steps 5 and 6.

    `route add [subnet] [gateway]`

    Example: `route add 10.100.0.0 192.0.2.1`
  - If **no**, repeat Steps 12 and 13. If you are still unable to ping the IP of the NFS server, contact your Network Administrator.

7 Type the appropriate command and press **Enter**. The NFS shared directory mounts.

- NFS mount command: **`mount [IP address]:/backups /mnt`**
- NAS drive command: **`mount -o vers=3 [IP address]:/backups /mnt`**

Examples:

- **NFS mount — `mount 192.0.2.3:/backups /mnt`**
- **NAS drive — `mount -o vers=3 192.0.2.5:/backups /mnt`**

8 Type the following command and press **Enter** to verify that the backup directory is present in the NFS mount.

`ls /mnt/[hostname]/FS`

Example: `ls /mnt/pepe/FS`

Result: You should see any and all previous backups for this system.

9 Does the output from Step 15 show the expected file system backups?

- If **yes**, continue with Step 17 to restore the DBDS file system.
- If **no**, contact Cisco Services for assistance.

10 Type CD /tmp/cdrom/sai/backup_restore and then press Enter. The

/tmp/cdrom/sai/backup_restore directory becomes the working directory

11 To restore the file system from the network location, type the following command and then press **Enter**.

`./restoreFileSystems -v -B /mnt/[file_system_archive]`

Example: **`./restoreFileSystems -v -B /mnt/pepe/FS/pepe_2012-12-11-16T15:39:19`**

Note: The restoration begins. Depending upon the size of the system, this could take an hour or more.

Result: A **Successfully restored all UFS filesystems** message appears.

12 When the restoration is complete, type the following command and press **Enter**.

`shutdown -y -g0 -i6`

Result: The server Reboots.

13 After the boot, log in as **root** user.

14 Go to ***Restore the Database and Key Files from an NFS-Mounted Directory*** (on page 22).

Restore the Database and Key Files from an NFS-Mounted Directory

Complete the following steps to restore the database and key files from a specified backup directory on the network after performing a file system restore.

1. Log into the DNCS as **root** user,
2. Type the following command and press **Enter**.
   pgrep -fl dvs
3. Does the output from Step 2 show that the dncsInitd and/or appInitd processes are running?
   - If **yes**, change to **dncs** user and type the following commands, pressing **Enter** after each, to stop the processes.
     dncsKill
     appKill
   - If **no**, go to Step 4.
4. As **root** user, type the following commands, and press **Enter** after each, to stop the http and the apache-tomcat services.
   svcadm disable http
   svcadm disable http-dncsws
   svcadm disable apache-tomcat
5. Type **onstat -** and press **Enter** to see if Informix is online.
6. Is Informix online?
   - If **yes**, go to Step 9.
   - If **no**, skip to Step 12.
7. Type the following command and press **Enter** to see if any active sessions are present.
   showActiveSessions
8. Do active sessions exist on the system?
   - If **yes**, type **killActiveSessions** and press **Enter**.
   - If **no**, go to Step 12.
9. Repeat Steps 9 and 10 to verify that there are no active database sessions.
10. Type the following command and press **Enter** to change to, and verify access to, the NFS share where the database backup is located.
    cd /net/[remotehost]/[path_to_NFS_DBKF_backup]
    Example: cd /net/192.0.2.3/backups/pepe/DBKF/2013_08-01T12:00:00

11 Are you restoring a DBKFcron.sh backup?

- If **yes**, type the following command and press **Enter** to untar the DBKF-#.tar file.

  Note: Substitute the number that pertains to the particular backup instance that you are restoring for "#".

  ```
  tar Exvf DBKF-#.tar
  ```

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

12 As **root** user, type the following command and then press **Enter** to format the database spaces.

```
/export/home/informix/libexec/formatDbSpace
```

Note: Formatting the database spaces will take 15 minutes or more depending on the system build. Do not proceed to Step 15 until formatDbSpace has completed.

13 To restore the database and key files from the network location, type the following command and then press **Enter**.

```
/usr/local/backup_restore/restoreDBKF –v –B
/net/[remotehost]/[path_to_NFS_databaseDBKF_backup]
```

Example: `/usr/local/backup_restore/restoreDBKF –v –B /net/192.0.2.3/backups/pepe/DBKF/2013_08-01T12:00:00`

Important: This lengthy command must be typed to the end before you press **Enter**.

Notes:

- The [remotehost] represents the hostname of the remote computer which is exporting (or holds) the database and keyfiles into which you will restore.
- The [path_to_NFS_directory] represents the directory path on the remote host which holds the backup files.

Result: A **Successfully restored the database** message appears.

14 When the database restoration completes, type the following commands, and press **Enter** after each, to restart the http and apache-tomcat services.

```
svcadm enable http
svcadm enable http-dncsws
svcadm enable apache-tomcat
```

15 Go to *Restarting System Components* (on page 31).

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

Stopping System Components

In This Appendix

Introduction

Use the procedures in this appendix to stop the system components.

Stop System Components

Follow these instructions to stop the system components.

1 If applicable, from an xterm window on the DBDS where you are logged in as **dncs** user, use the siteCmd command to access the RNCS (or LIONN) and complete the following steps.

   a Type the following command and press **Enter**. The RNCS processes stop.

   ```
   siteCmd [lionn hostname] lionnStop
   ```

   b Type the following command and press **Enter**. The initd process on the LIONN shut down.

   ```
   siteCmd [lionn hostname] lionnKill
   ```

   c Type the following command and press **Enter** to determine if the processes have stopped. The processes are stopped when there are no processes listed in the output.

   ```
   siteCmd [lionn hostname] pgrep -fl dvs
   ```

   d From a **root** xterm window, type the following commands, pressing **Enter** after each, to disable the RNCS cron jobs.

   ```
   ssh –X dncs@[lionn hostname]
   su -
   svcadm –v disable –s cron
   exit
   ```

2 From an xterm window on the DBDS where you are logged in as **dncs** user, complete these instructions.

   e Type the following command and press **Enter**. The DBDS processes stop.

   ```
   dncsStop
   ```

   f Type the following command and press **Enter**. The initd process on the DBDS is shut down.

   ```
   dncsKill
   ```

g Type the following command and press **Enter** to determine if the processes have stopped. The processes are stopped when there are no processes listed in the output.

```
pgrep -fl dvs
```

h From the **root** xterm window, type the following command and press **Enter** to disable cron jobs.

```
svcadm –v disable –s cron
```

3 Close all GUIs and WUIs.

B

Restarting System Components

In This Appendix

Introduction

Use the procedures in this appendix to restart the system components.

Restart System Components

Restarting the DBDS

1. From an xterm window on a remote system, log onto the DBDS as an administrative user.
   `ssh –X [adminstrator account]@[VM IP address]`
   Example: `ssh –X ciscousr@192.0.2.35`
2. Type the following command and press **Enter** to change to **root** user.
   `sux – root`
3. Type the **root** password and press **Enter**.
4. Type the following command and press **Enter** to change to the dncs role.
   `sux - dncs`
   Note: Type the dncs user password when prompted.
5. Change to dncs user and type the following command.
   `dncsStart`
6. From the **dncs** xterm window on the DBDS, type the following command and press **Enter**. The dncsControl utility window opens.
   `dncsControl`
7. Type **2** (for Startup / Shutdown Single Element Group) and then press **Enter**. The dncsControl window updates to list the available applications for Startup/Shutdown.
8. Type **1** (for dncs) and press **Enter**. The dncsControl window updates to list the goal states.
9. Type **e** (for Display Groups) and press **Enter**. The dncsControl window updates to list the status of all of the processes and servers running on the DBDS.
10. Wait for the dncsControl window to list the current status (Present State) of all processes and servers as **running**.
    Notes:
    - The dncsControl window updates automatically every few seconds, or you can press **Enter** to force an update.
    - The indicators on the dncsControl window all become green when the processes and servers have restarted.

C

Modify the Root crontab File for Automating Backups

In This Appendix

Introduction

In version 6.0.44 and higher of the backup and restore, there are scripts available to assist in automating backups:

- /usr/local/backup_restore/DBKFcron.sh
- /usr/local/backup_restore/FScron.sh

These scripts may be run from the crontab file. Prior to enabling these on your system, you may wish to change the default behavior of the scripts.

Configure the Database and Key Files Backup cron Script

1. Use a text editor to open the /usr/local/backup_restore/DBKFcron.sh file.
2. Insert the path to your backups storage area into the 'nfspath' variable.
3. Insert the hostname of your server into the 'your iDNCS' variable, or use the default.

   Note: The *your iDNCS* variable is set to 'uname -n'. This will set the your iDNCS variable to the current hostname of the system. You may leave it set this way or change it to a name of your choice.
4. Insert the number of backups to maintain into the 'num_to_keep' variable, or use the default.
5. Save and close the file.

Result: This results in backups written to /<path_to_storage>/<hostname>/DBKF/DBKF-#.tar, where '#' is the backup number. At most, 'num_to_keep' backups will be stored. When that number is reached, older backups are deleted.

Configure the File System Backup cron Script

1. Use a text editor to open the /usr/local/backup_restore/FScron.sh file.
2. Insert the path to your backups storage area into the 'nfspath' variable.
3. Insert the hostname of your server into the 'your iDNCS' variable, or use the default.

   Note: The *your iDNCS* variable is set to 'uname -n'. This will set the your iDNCS variable to the current hostname of the system. You may leave it set this way or change it to a name of your choice.
4. Insert the number of backups to keep into the 'num_to_keep' variable, or use the default.
5. Save and close the file.

Result: This results in backups written to /<path_to_storage>/<hostname>/FS/FS-#.tar, where '#' is the backup number. At most, 'num_to_keep' backups will be stored. After that number is reached, older backups are deleted.

Modify the Root crontab File

The following are sample crontab entries that demonstrate automating nightly backups of the file systems, database, and key files.

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

```
# Backup Database and KeyFiles
[minutes] [hours] * * *   /usr/local/backup_restore/DBKFcron.sh
# Backup FileSystems
[minutes] [hours] * * *   /usr/local/backup_restore/FScron.sh
```

D

Storage Requirements

In This Appendix

Introduction

System Release i4.5 has a new backup and restore utility to go along with the new T5-2 hardware platform that does not include a tape drive. This appendix explains some of the terms used to describe different types of storage, what is supported for backup/restore, and how to size the storage that is needed for backing up an iDNCS.

SR i4.5 Storage Requirements

The computing industry has many acronyms for storage interfaces (IDE, ATA, PATA, SATA, SCSI, FC, and others). Some are even acronyms of acronyms (SAS: Serial Attached SCSI). These acronyms represent specific physical interfaces to storage and 'command sets' that are used to read and write to or from that storage. This appendix will not try to explain these interfaces, but instead discuss broader categories of how a computer accesses these interfaces.

How computers access storage generally falls into one of three categories: Direct Attached Storage (DAS), Storage Attached Network (SAN), and Network Attached Storage (NAS). Each of these terms is explained in the following sections.

Direct Attached Storage (DAS) or Direct Attached Storage Device (DASD)

Direct attached storage refers to a storage device that is directly connected to the computer with whatever interface is on the device. In this situation, the storage device is under the control of the computer. Examples of DAS range from a single ATA disk drive connected to a PC, to a SCSI tape drive inside or nearby a server, to a separate enclosure of disks connected to the computer via a SCSI or Fibre Channel (FC) cable. If the computer is connected to a network, the storage could be offered to other computers on the network and would appear to those other computers as NAS.

Storage Area Network (SAN)

Storage area network (SAN) is a dedicated network built for sharing storage devices among multiple computers. Typically a SAN is built with Fibre Channel interfaces on computers, and storage devices with one or more Fibre Channel switches. SAN networks are generally built to provide 'block level' access to storage. Disk space on a storage device is configured into pieces that are presented to the network as a Logical Unit Number (LUN). A SAN switch is configured to control what computer is able to access which LUN. Computers or hosts access these LUNs using a Fibre Channel host bus adapter (HBA). While a disk array is connected to the SAN via a Fibre Channel interface, what interface the disks use inside the array can vary. Traditionally, disks in a Fibre Channel array have Fibre Channel interfaces themselves, but many arrays today that have external Fibre Channel interfaces use SAS or SATA interface disks internally.

Network Attached Storage (NAS)

NAS refers to storage that is shared between computers on a LAN or a WAN interface. Where a SAN is specifically built for moving blocks of data between computers and storage, NAS takes a general purpose network and adds storage traffic into the mix. Access to NAS storage can be either 'block level' or 'file level', based on what protocol is used over the network. iSCSI is an example of a 'block level' protocol, and NFS is an example of a 'file level' protocol.

Backup/restore in System Release 6.0 supports backups and restorations to and from a network file system (NFS). A NAS device or an NFS server on the network can provide the required NFS share. The rest of this appendix describes how these choices are used and how to determine the amount of storage needed to accommodate the backup needs. When discussing storage options there are three factors that must be considered: cost, speed, and reliability. These factors are discussed with each option.

For protection from all failure scenarios, a highly-available NAS backup is desired. NAS can be placed in a separate facility from the iDNCS, and backup/restore utilities can access the storage via a NFS mount-point provided by the NAS device. What type of NAS storage is selected depends on how the factors interact at each site. With NAS, all of the trade-offs on cost, speed, and reliability come into play. NAS can be provided by anything from a small two-drive desktop enclosure, all the way to a portion of a large EMC or NetApp storage array.

Disk vs. Tape Backup

The reasons for backing up data to disk instead of tape include:

- Disk backups are faster; disk transfer rates are generally faster than tape, resulting in shorter backup windows
- Disk access is faster. There are no 'seek delays' for finding data and it is faster to restore data
- Disks, especially disks that are protected using RAID, are more reliable when compared to tapes. There are no tapes to manage.

Sizing Backup Storage Requirements

A formula that can be used to calculate how much disk space is needed for storing backups is as follows:

*Required Total Storage = [(size of Informix database backup + size of key files backup) * number of copies + (size of file system dumps) * number of copies] * growth factor*

The size of each backup type can be obtained as follows:

Size of Informix Database Backup

The 'onstat -d' command reports disk space allocated in the Informix database. The number of bytes used in the database is not readily apparent and a little math is needed to calculate it.

1. Obtain the pages in use in each DBspace by subtracting the 'free' column from the 'size' column.
2. Add up all the pages in use.
3. Multiply the total pages in use by the page size (2K) of the DBspaces.

Example:

```
# onstat -d

IBM Informix Dynamic Server Version 11.70.FC4 -- On-Line -- Up 16:47:08 --
7759872 Kbytes

Dbspaces

address          number   flags      fchunk   nchunks  pgsize   flags
owner    name

27984b028        1        0x40001    1        1        2048     N  BA
informix rootdbs

283993028        2        0x40001    2        1        2048     N  B
informix physdbs

2839931d0        3        0x40001    3        1        2048     N  B
informix logspace

283993378        4        0x42001    4        1        2048     N TBA
informix tempspace1

283993520        5        0x48001    5        1        2048     N SBA
informix sbspace1

2839936c8        6        0x40001    6        1        2048     N  BA
informix dataspace1

283993870        7        0x40001    7        1        2048     N  BA
informix dataspace2

 7 active, 2047 maximum
```

```
Chunks

address          chunk/dbs     offset     size       free       bpages
flags pathname

27984b1d0        1      1      0          1048576    1038183
PO-B-D /export/home/informix/sai/dsk/dncsDbServer_rootdbs_p_1

283993a18        2      2      0          2097152    0
PO-B-D /export/home/informix/sai/dsk/dncsDbServer_physdbs_p_1

283993c18        3      3      0          4194304    51
PO-B-D /export/home/informix/sai/dsk/dncsDbServer_logspace_p_1

283993e18        4      4      0          2097152    2097099
PO-B-- /export/home/informix/sai/dsk/dncsDbServer_tempspace1_p_1

283995028        5      5      0          2097152    1955929    1955929
POSB-D /export/home/informix/sai/dsk/dncsDbServer_sbspace1_p_1

                                  Metadata 141170     105048     141170

283995228        6      6      0          10485760   3055441
PO-B-D /export/home/informix/sai/dsk/dncsDbServer_dataspace1_p_1

283995428        7      7      0          2621440    637897
PO-B-D /export/home/informix/sai/dsk/dncsDbServer_dataspace2_p_1

 7 active, 32766 maximum


size = [(1048576 - 1038183) + (2097152 - 0) + (4194304 - 51) + (2097152 -
2097099) + (2097152 - 1955929) + (10485760 - 3055441) + (2621440 - 637897) ]
* 2048 = 32185888768 (approx. 32GB)
```

Size of Key Files Backup

A good approximation for key files is that they are about 30 percent of the size of the Informix database.

An alternative is to run database and key files backups to local file systems to determine the sizes.

Size of File System Dumps

The iDNCS uses the Solaris UFS file system, so disk space used by the file systems can be easily determined by summing the 'USED' columns in the output of the 'df -h' command.

Example:

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d500       7.9G   3.2G   4.6G    42%    /
/devices                 0K     0K     0K     0%    /devices
```

```
ctfs                    0K     0K     0K     0%    /system/contract
proc                    0K     0K     0K     0%    /proc
mnttab                  0K     0K     0K     0%    /etc/mnttab
swap                   21G   1.4M    21G     1%    /etc/svc/volatile
objfs                   0K     0K     0K     0%    /system/object
sharefs                 0K     0K     0K     0%    /etc/dfs/sharetab
/platform/sun4v/lib/libc_psr/libc_psr_hwcap3.so.1
                       7.9G   3.2G   4.6G    42%
/platform/sun4v/lib/libc_psr                        .so.1
/platform/sun4v/lib/sparcv9/libc_psr/libc_psr_hwcap3.so.1
                       7.9G   3.2G   4.6G    42%
/platform/sun4v/lib/sparcv9/                        libc_psr.so.1
fd                      0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d503        19G   1.0G    18G     6%    /var
swap                    21G   1.2M    21G     1%    /tmp
swap                    21G    40K    21G     1%    /var/run
/dev/md/dsk/d510       517G   104G   408G    21%    /disk1
/dev/md/dsk/d505       482G   4.9G   473G     2%    /export/home
/dev/md/dsk/d399       115G   1.3G   113G     2%    /disk2
/disk2/dvs/backups     115G   1.3G   113G     2%    /disk1/dvs/backups
/disk2/dvs/dncs/tmp    115G   1.3G   113G     2%    /disk1/dvs/dncs/tmp
```

Determining Growth Factor

A rule of thumb for file growth is to count on 20 percent to 30 percent growth per year. If you are trying to size backup storage for three years, count on needing between 175 percent to 225 percent of your initial space by the end of three years.

Number of Copies

This is a number that the site will have to determine based upon business needs, but should never be less than two. Having two copies gives the site a means to 'fence in' a maintenance activity with backup pre-maintenance and another immediately post-maintenance. Other factors to consider are:

- How long an error goes unnoticed and requires a restoration to something other than the most recent backup
- Data forensics; more copies allow you to find when a change was made to the system

Summary Example

The total disk space required for backups can be calculated, as follows:

Assumptions

- Database backup size = 20 GB
- Key files backup size = 6 GB
- File systems backup size = 40 GB
- Number of database + key file backups = 7 (daily backups)
- Number of file system backups = 4 (weekly backups)

Disk space required for database and key files backup for one month:

[(20 GB + 6 GB) * 7 days/week] * 4 weeks/month = 728 GB/month

Disk space required for file systems backup for one month:

[40 GB * 4 weeks/month] = 160 GB/month

Total disk space required per month for backups:

728 GB/month + 160 GB/month = 888 GB/month

If the site does not overwrite their backups, the total disk space required for a month:

888 GB/month * 12 = 10, 656 GB/year (10.656 TB/year)

However, most sites would want to overwrite their backups or preserve only a

subset of their backups.

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

January 2015