Appendix A Commonly Asked Questions

Overview

The purpose of this section is to answer frequently asked questions that are not directly addressed in the descriptions of Backup Director concepts, procedures, and parameters. NetWare 4.x issues are addressed separately.

Contents

General

What are TSA.TMP files?*

TSA*.TMP files are temporary files created by TSAs and are normally deleted by the TSA after Backup Director disconnects. They remain on disk due to abnormal termination of a TSA operation.

- TSA*.TMP files may be manually deleted.
- Setting the rules at the root of the volume to Backup/Exclude for the

wild card name TSA*.TMP will prevent Backup Director from attempting to backup these files.

What are some causes of database corruption?

Recurring database corruptions are usually a sign of an environmental problem such as a faulty network interface card or cable. If corruptions continually occur, test the network using a network analyzing tool (sometimes referred to as a “sniffer” or “lanalyzer”) to locate the problem.

Whenever there is a loss of the data stream from the backup source location to the backup device during a backup operation, database corruption may occur.

This can be due to lost connections across the system, other NLM's initiating conflicts with Backup Director, and intermittent hardware problems. Substituting known working devices for suspect devices can narrow the search for the problem source.

VLM shells prior to version 1.10 and NETX shells prior to 3.31 have been known to cause database corruptions and should be upgraded.

Environmental conditions within the work place (and even strong magnetic and static fields behind walls of adjoining offices) can add to the possibility of corruptions. It is important to properly shield hardware and terminate the SCSI bus at both ends.

How can I optimize Backup Director performance?

Operating system settings, hardware on the system, the complexity and depth of directory structures, and Backup Director configuration settings all affect performance.

Operating system settings: The *Installation Guide* contains a “*Server Tuning*” section with detailed information on settings such as Packet Receive Buffers, Directory Cache, and Total Cache Buffers.

Hardware: Often, adding memory to the server will help improve performance, as the settings for various options can then be given a broader range to handle peak loads on the system. Replacing 16-bit controller cards with 32-bit cards, using compression backup devices, compressing files prior to backup, and using computers with higher speed CPUs can increase performance.

Backup Director Configuration: Backup Director default settings are sufficient for most environments, so little customization is needed. However, the rules, rotation schedules, and backup choices can be customized to optimize Backup Director for specific needs.

Configuring automatic backups to execute at non-peak memory utilization times is important, so that other applications do not compete with Backup Director demands.

Installation

How do I relocate my Backup Director installation?

To relocate the Backup Director installation:

- At the target location, specify the same directory path as the original installation directory.

- Be sure that the configured auto login user exists on the target server.
- Be sure that the target server/volume supports the same name spaces as the original installation server/volume.

See also: “*Moving a Backup Director Installation*” in Chapter 6 of this guide.

Why can't I configure my backup device?

Check for each of the following:

> **Termination**–Ensure that the backup device is properly terminated and/or try a different termination cap.

> **Device Drivers**–Ensure that the correct Palindrome supported device drivers are loaded. Both the SCSI hardware driver and the ASPI module (for example, ASPITRAN or CPQASPI) must be loaded. Download TSTDRVR.ASC from the Palindrome BBS for a list of supported device drivers.

> **SCSI ID conflict**–Use Device Manager to “Scan for Devices”. If there is a SCSI conflict, scanning will show the same device multiple times. Be sure that the device has a unique SCSI ID.

> **Supported Devices**–Ensure that the host adapter and backup device are supported and have a proper firmware and associated EE Code (must support SCSI-2 command set). Download CDL40.ASC from the Palindrome BBS for the latest list of supported devices.

> **Servers with more than 16MB of RAM**–If the server has more than 16MB of RAM and the installation is using a host adapter that cannot access more than 16MB of RAM, be sure to use the “LOAD PALSDRV ABOVE16MEG” statement.

Why do I see PLSM-53 errors when adding resources to the Protected Resource list?

Check the following:

> Be sure the proper TSA is loaded on the server being added to the list.

> For 4.x servers in a different tree than the installation server, be sure the configured auto login user has been created within the bindery context for those servers.

> Ensure that the configured auto login user does not have concurrent connection restrictions.

> If upgrading from TSA's dated June 1994 or earlier, be sure to re-select each resource on the Protected Resource List so that each resource will be associated with the upgraded TSA.

See also: “*Renaming Resources*” in Chapter 8 of this guide.

Backup

What are the requirements for protecting 4.x servers?

NetWare 4.x server resources are added to the Protected Resource List similarly to any other server's resources.

- Load the appropriate TSA for the server being added to the Protected Resource List (for example, TSA3.1x, TSA410)
- Unique to 4.x servers is a Network Directory Services (NDS). To protect this resource, load TSANDS on one of the servers in the NDS tree. To backup the NDS in full, add “Full_Directory_Backup” to the Protected Resource List.
- If protecting 4.x servers not part of the installation server's NDS tree, create an auto login user on each of these servers. Add this user to the default bindery context for each server and assign the user supervisory object rights to the “.[Root]” object within the NDS tree.

See also: *Installation Guide*

What is the difference between NDS “Full Directory Backup” and “.[Root]”?

There is no difference currently. It is recommended that the user select “Full Directory Backup” so that as enhancements (such as the ability to backup schema information) are added to TSANDS, this additional data will be protected without the need to modify the Protected Resource List.

Currently TSANDS only backs up NDS objects and associated data. It is anticipated that schema, but not partition information, will be backed up with future TSA releases.

How do I perform full backups on specific days?

For a complete “snapshot” of the system, custom jobs can be scheduled to run periodically (daily, if desired) and these custom sessions can (optionally) be tracked within the File History Database.

Note that with both the Tower of Hanoi and Grandfather/Father/Son rotations, full backups automatically occur every rotation day. In addition, the system administrator can configure for full backups on non-rotation days.

What causes backups to run slowly?

The following are some common causes of slow backups:

- Using the job status window to monitor jobs in progress can adversely affect performance. Monitoring is only recommended for specific purposes and for short periods.
- The number of directories on a volume, and the amount of server memory allocated to access those directories, are closely related. The default settings are often too low for good performance. A formula for computing the Minimum Directory Cache Buffers setting is available in the “*Server Tuning*” section of the *Installation Guide*.

Why do scheduled automatic backups not execute?

There are a number of items that may affect the execution of automatic backup operations. Be sure:

> There is a job queue.

> PALJSRVR (the Job Server) is loaded on the server. To load PALJSRVR, at the server console prompt, type:

LOAD PALJSRVR /I<<*installation path*>>

where <<installation path>> is the volume and directory of your installation directory (for example, VOL1:\PAL).

> Eligible media is loaded.

> The configured auto login user has supervisory rights.

> There are no NLMs loaded that conflict with Backup Director NLMs.

> There is sufficient memory to execute the operation.

Why are some files skipped during a backup operation?

Depending upon the backup operation running, Backup Director will not copy files (with the default settings) when:

- Rules are defined that exclude those files from all backups
- The files are opened by another application unshareably
- The files have invalid characters within the file name
- The files have no date or an invalid date

Restore

What is the best way to recover from a corrupted or missing System Control Database (files ASDB.PAC and ASNX.PAC)?

To restore the latest System Control Database, use Palindrome Control Console at the server (PAL.NLM). Select “Recover System Control Database” and specify the location of the System Control Database.

If the latest System Control Database is not available on backup media, then restore the next most recent set. If the latest System Control Database is not restored, File History Databases for the same backup date for **all** resources on the Protected Resource List must also be restored−so that both databases are synchronized. This method is the second choice because some file history information may be lost.

Why aren't some files restored during a restore operation?

The following are some reasons that files are not restored:

- The file is already on disk and the **Overwrite** parameter for replacing existing files is set to **Never** (a file on disk is never replaced) or **Older** (a file on disk is never replaced with an older version from media).
- The file does not exist in the File History Database.
- The System Control Database and the File History Database(s) are not synchronized. This can result from restoring an older System Control Database without restoring File History Databases from the same date or earlier.
- A TZ (Time Zone) variable has been set.

Use of the TZ variable can cause a date/time mismatch between the file versions in the File History Database and the files on media. Palindrome does not recommend using the TZ variable.

To restore specific versions of files that were backed up when a TZ variable was set, journal the media containing the file in Media Manager, and tag the version to restore.

How do I restore an object in an NDS tree?

Single objects can be restored by tagging them using File Manager. Due to NDS limitations, however, linkages with other objects (rights to use printers, file trustee information, etc.) do not get restored with single object restores.

To restore user objects in an NDS tree where users access only services within their own container, **restore the the entire container** in which they are defined.

Media Scheduling

How can I predict how many tapes (media) I will need for backups?

The number of media required varies depending upon combinations of the following:

- The rotation pattern configured.

  The default Tower of Hanoi rotation pattern, which rotates media weekly, requires a minimum of one media in each of five media sets (more if the data to copy to media exceeds one media per backup).

  The GFS (Grandfather/Father/Son) rotation pattern is based upon sets of daily media, weekly media, and monthly media. Seven media sets are required for daily media sets. Using the default settings, a total of 23 media sets will be requested. If copied data will not fit on one media per set, then additional media (but not media sets) will be needed.

- The storage capacity of the media relative to the amount of data to be copied to media.
- The types of backup being performed (full, incremental, or differential operations).
- The setting of the **Preserve Backups** parameter. The longer the time period that you preserve these sessions, the more media the program will require. The program cannot overwrite any backup session on the managed media until the most recent session is eligible for overwriting.

How do I know ahead of time what backup media will be needed?

View the Next Required Media window to find out which media will be needed to continue an incomplete automatic job, for the next automatic backup operation, or the next rotation day.

What happens when a tape (media) fills during a backup?

If a media fills during a backup operation, Backup Director automatically continues writing on the next eligible media. If no other eligible media is available within the backup device, Backup Director logs or displays message indicating that the backup could not complete and to insert an eligible media.

NetWare 4.x

Bindery Emulation

For more information on bindery emulation, see chapter 2 of the Installation Guide.

Due to a NetWare limitation, if you are protecting 4.x servers that are not part of your installation server's NDS tree, you must enable bindery emulation on each of those servers and create the auto login user on each of those servers in the the proper bindery context for that server.

Backup Director follows the default methods of NetWare, whereby it uses NDS logins for servers within the same tree and bindery logins for servers outside of the current NDS tree.

Compressed Files

Backup Director protects NetWare 4.x compressed volumes. You can back up these volumes as compressed or uncompressed by toggling the **Retain File System Compression** option in Configuration Manager (select Configure/*Operation* and then the Advanced tab). When you turn on this option, compressed data cannot be restored to a volume that does not support compression.

If you turn off this option, the compressed data is backed up uncompressed on media (this affects performance). Note that if you choose this option, you **cannot restore** the data in compressed format, only uncompressed.

Generally, the option should only be used if there is a likelihood that you need to restore data to a volume that does not support NetWare 4.x compression (for example, a NetWare 3.11 or a workstation volume).

SYSCON

Avoid using SYSCON to administer NetWare 4.x servers and especially do not use SYSCON to create user objects. If you use SYSCON to create a user on a 4.x server and have to restore, neither the login script nor directory or file trustees will be restored for the user.

If use NWADMIN to create the user objects, they are restored completely.

Read Fault Emulation

Be sure to set **Read Fault Emulation** to ON on all 4.x servers.

Protecting NetWare Directory Services

Backup Director uses the NetWare Directory Services Target Service Agent provided by

Novell, Inc., to back up the NDS database. You should use TSANDS.NLM that ships with the current version of Backup Director (or a newer version). Do **not** use the version TSA_NDS.NLM that shipped with NetWare 4.01.

TSANDS backs up the entire NDS database for a Directory tree from a single point, regardless of the number of partitions that exist. A Directory tree need only be added once to the Protected Resource List.

If performance becomes an issue while backing up the NDS database, you may consider storing a replica of each partition on the server where TSANDS is loaded.

NDS Database Replication

Although Palindrome provides comprehensive backup of NDS, Palindrome strongly recommends that you have at least two replicas of each partition of your Directory tree.

Replicating the NDS database among multiple servers has several benefits:

- It provides faster access to NDS information for users across a wide area network data link.
- It eliminates a single point of failure. If a disk crashes or a server goes down, a replica on another server can continue to authenticate users to use the network and to provide information on objects in that partition.
- It allows a partition that becomes corrupted to be recreated from a replica.

Partition Loss

It is important to note that the loss of an NDS partition can have far-reaching consequences. Not only is the NDS data contained in that partition lost, but subsequent partitions are also lost.

For example, if the Root partition is not replicated and is lost, the entire NDS database is destroyed. Furthermore, loss of the NDS database invalidates the file system trustee information on all servers in the Directory tree. It is also not currently possible to back up the NDS database once a portion of it is off line.

Reinstallation

Should you ever need to re-install NetWare Directory Services, you should call the new Directory tree by the same name as the tree it is replacing. You must add servers to the same container objects as before.

TSANDS Limitations

Novell releases updates to TSAs periodically. These updates can be obtained from Novell via the NOVLIB forum on Compuserve. Once updates have been certified by Palindrome, they will also be made available on the Palindrome BBS.

Palindrome has seen the following limitations with the current NDS Target Service Agent (TSANDS.NLM [dated 10/21/94]):

Partition Information is Not Saved

You must repartition and/or replicate the database manually during a restore operation.

Because of this limitation, when restoring **large** NDS databases:

> First restore containers only

> Secondly, partition and replicate as necessary.

> Thirdly, restore the data.

Schema Information is Not Saved

Applications that modify the NDS schema may need to be re-installed if data is restored into a new NDS database as opposed to an existing NDS database. This is because only the default schema is available whenever NDS is installed.

NOTE: Palindrome recommends that you add "<<tree>>/Full Directory Backup" to the Protected Resource List, rather than "<<tree>>/Root". This ensures that schema information will also be backed up once this capability is added to TSANDS by Novell.

Bindery Emulation login scripts are not saved.

Login scripts created via the NetWare 3.x SYSCON utility for users who log in via bindery emulation are stored as files in the appropriate MAIL directory, rather than as a property of the User object (as is the case with the login script for a user who logs into NDS).

While these login files are backed up, the directories in which they reside are based on a user identification number under the SYS:MAIL directory that becomes invalid once NetWare Directory Services is removed from a server.

Single Point Backup

Currently, Palindrome recommends that the entire NDS database be backed up from a single point using a single NetWare Directory Services Target Service Agent (TSANDS.NLM). This presents several problems:

- It may take considerable time for portions of the tree that may exist on the other side of a WAN link. In this case, a local replica of the remote partition might be useful.
- Multiple system administrators may be responsible for different portions of the NDS tree. To avoid this problem you should consider two alternatives:

1. make one administrator responsible for backups of the NDS database, or

2. allow each administrator rights to back up the entire NDS database (i.e., backup NDS multiple times from multiple Backup Director installations).

Future releases of Backup Director will be enhanced to back up portions of the NDS database.

Off-line Partitions

The NDS database cannot be backed up if any partitions are off-line. If a server that contains a Master replica is off line and there is no other replica of the partition on any other server, TSANDS terminates with the following error:

> **NWSMTSReadDataSet: -626 All referrals have failed. Directory Object Name <<container object>> (FFFDFEAE)**
>
> where <<container object>> is the full name of the root object of the partition that is missing. If this partition is needed, you must wait until it is back on line before attempting another back up of the NDS database. Consider replicating the partition once it is again available so as to avoid a reoccurrence of this problem.

Restore Limitations

Rights to Other Objects Not Restored

It is possible to restore a single object once it has been deleted. Note, however, that restoring a single object does not restore that object's rights to other objects, nor are directory and file rights of the deleted object restored.

For example, if a User object is deleted, then later restored, the User object and data associated with that object are restored (i.e., the user's name, location, telephone number, login script and other properties are restored). However, rights to other objects must be restored manually (i.e., the groups to which the user belonged, the printers that the user had rights to use, the files and directories the user could access or owned, etc.).

You can restore directory trustees in Resource Manager using Operations/*Restore Directory Structure*.

Palindrome recommends that when designing your NDS tree, objects that users have rights to are in the same container that the user is defined in. Then when restoring a single object, restore all objects in a single container to ensure all objects associated with that object are restored.

Printer Information

Printers are likely to need re-configuring after restoring an NDS database. Not all of the information relating the Print Servers, Print Queues and Printers is restored properly.

NDS Recovery Techniques

Whenever a problem with NDS is encountered, a multi-step approach should be taken before attempting to re-install NetWare Directory Services.

Palindrome strongly recommends that you familiarize yourself with all of these steps by studying the NetWare 4.x documentation *before* you have a need to restore NDS.

Repairing the NDS Database

DSREPAIR is a server utility that checks and repairs the NDS database similar to the way VREPAIR checks and repairs volumes. It is important to ensure that the NDS database is not corrupted before trying to restore data into it.

You can use DSREPAIR to repair the NDS partitions and replicas that reside on a particular server. If the problem persists after running DSREPAIR, run the utility again on any other servers that contain the same partition replicas. To repair the entire NDS database, you must run the utility on each server that contains a part of the NDS database.

For further information refer to the following Novell Documentation: “Repairing the NetWare Directory Services Database” in Chapter 4 of *Supervising the Network,* and “DSREPAIR” in Chapter 4 of *Utilities Reference.*

Replacing an NDS Replica with a New Copy

If your NDS database is replicated across multiple servers and you find users on only one server tend to experience problems, you may find it beneficial to replace the suspect replica with a fresh copy.

You can do this by deleting replicas that you suspect contain corrupt data and replacing them with a new copies of the Master replica.

If you suspect that the Master replica is corrupt, but that other replicas still contain valid data, you should first make one of the other replicas the new Master replica before proceeding with this operation. This method ensures that all other replicas contain the same data as the Master replica.

Restore the NDS Database into the Existing Directory Tree

When you restore data into an existing database, trustee ID information is maintained, thereby avoiding the need to re-synchronize the file system data with a new NDS database. It is worthwhile attempting to restore into an existing database first before taking more drastic measures (such as removing NDS from a server) since the procedure can be done fairly quickly.

The NDS database can be restored by tagging the NDS resource in Resource Manager and selecting Operations/*Restore*. Be sure to set the overwrite options to ALL in the restore dialog box.

Installing a New Directory Tree

If none of the above procedures is successful, or you need to recover from a situation where a partition has been lost that is not replicated, then you may need to re-install NetWare Directory Services on all of your servers. This procedure has far-reaching consequences.

Once NetWare Directory Services is removed from a server, that server's file system trustees are invalidated, even though the file system data is still valid. Thus, the trustee information on all NetWare volumes that were in the Directory tree must also be restored as part of this procedure.

To restore directory and file trustees, using Backup Director, you must use the Restore*/Directory Structure* and the Restore/*Data* options.

Re-installing NetWare Directory Services

1. Before removing NetWare Directory Services from a server it is recommended that all replicas be removed from the server. Replica management is done via the Partition Manager. Delete Read/Write and Read Only partitions from each server. Merge Master

Partitions into parents until only the Root partition remains on a single server.

2. Remove NetWare Directory Services from each server in the Directory tree. This is done using the INSTALL utility at each server containing a part of the NDS database. The order in which this is done can be important. You should remove NetWare Directory Services from the server containing the Root partition last.

3. Down and cold boot each server on which Directory Services was removed before reinstalling. For a cold boot, turn off the machines power, wait at least 30 seconds, then turn on the machines power.

4. Install NetWare Directory Services on one of the servers, specifying the same Directory tree name, Organization, and optional Organizational Unit(s) as before. This is done using the INSTALL utility at the server console.

5. Install NetWare Directory Services on each of the remaining servers that existed in the Directory tree prior to removing the NDS database. Ensure that the same Directory tree, Organization and Organizational Unit(s) are specified as existed prior to removing the NDS database.

6. Install mounted volumes into the NetWare Directory tree on each server using the INSTALL utility. (Newer versions of NetWare 4.x may install the mounted volumes for you as part of the previous step. Do not be alarmed if you receive a message stating that no volumes were found that needed installing into the Directory.

7. Run the DSREPAIR utility on each server. This operation removes old (obsolete) trustee IDs from the file system. Running the utility once should be sufficient. However, you may want to run it a second time to ensure that no more errors are found.

8. Recreate the Auto Login User object where it existed previously.

9. Repartition and replicate the NDS database as it was before, or at least to the extent necessary.

10. It should not be necessary to re-install Backup Director, however, you may have difficulty if some of the Backup Director files are no longer owned by the Auto Login User object, particularly if these files have no owner. Most important are the log files, database files, and lingering temporary files in and under the directory where Backup Director is installed.

11. Change the owner of the problem files using the FLAG utility. See “FLAG” in Chapter 3 of Novell's *Utilities Reference* manual.

12. Restore the NDS database data by tagging the NDS object in Resource Manager and selecting Operations/*Restore*. Select *Full Resource*. Set the overwrite parameter to **ALL**.

13. Check that the auto login user has sufficient file system rights to restore data. If you have granted the auto login user the Supervisor object right to the server object, these rights will have been restored automatically.

14. Reconstruct the trustee information on each server volume in the NDS tree by accessing Resource Manager and tagging each resource that is in the NDS tree.

15. For each server, select Operations/*Restore*. Choose *Directory Structure*. This restores directory trustees for each directory.

16. To restore file-level trustees, you have to restore all data to the volumes. For each server, select Operations/*Restore*. Choose *Data*. This restores all data on each of your volumes.