Pillar Axiom

NDMP Integration Guide

ORACLE

PILLAR AXIOM

Part Number: 4420-00093-0500
Pillar Axiom release 4.2
2011 October

Table of Contents

List of Tables

CHAPTER 1

Introduction to NDMP Integration

Audience

This document is targeted to backup administrators, network administrators, system administrators, and others who install and configure Oracle's Pillar Axiom systems.

We assume that you have the necessary skills and experience in:

- Operating computer hardware.
- Network Data Management Protocol (NDMP) theory and practice.
- Configuring your selected data management application (DMA).
- Configuring your tape storage device.
- Configuring the virtual network interface (VIF) on Pillar Axiom storage systems.

About NDMP-Based Backup System Configuration

Network Data Management Protocol (NDMP) is an industry-standard protocol that allows for the use of third-party backup applications to manage the backup and recovery of customer data. An NDMP user account, password, and access port are configured through the Pilot. Pillar Axiom systems support NDMP version 4. Refer to http://www.ndmp.org/info/faq.shtml for details.

NDMP-based backup and restore operations can be integrated into your existing backup and recovery system. When you do this, you can completely automate the backup and restore operations.

The Pillar Axiom system supports:

- CommVault Galaxy
- Symantec Veritas NetBackup
- EMC NetWorker
- BakBone NetVault: BackUp
- Oracle Secure Backup

Note: Refer to the *Pillar Axiom Support and Interoperability Guide* for more details on the supported versions of the above mentioned backup and recovery software.

To automate backup tasks, create schedules for backup operations through your data management application (DMA). Refer to the documentation of your DMA for details. Pillar Axiom systems allow up to ten distinct NDMP operations at the same time. That is, a total of ten concurrent backups or restores is allowed. For example, five backups and five restores can be run concurrently.

Pillar Axiom systems allow up to 250 user-defined Snap FS snapshots for each filesystem. Because each block-level or file-level backup requires one free available filesystem snapshot to succeed, no more than 249 snapshots of a given filesystem can be used for a backup. If 250 or more snapshots exist in the filesystem prior to the backup, the backup will fail.

Important! Due to the sensitivity of tape libraries and tape backup, do not run administrative tasks on the Fibre Channel (FC) switch to which the tape device is attached, while a backup or restore is in progress. This could cause timeouts or failures.

Important! You can use a maximum limit of eight logical units (LUNs) with the FC type NDMP adapter. The value of the LUN must be a number between 0 and 7. A LUN number over this value does not work on the Pillar Axiom system.

DMA Technical Support Information

If you have difficulties with your data management application (DMA), ensure you have the following information available before you contact the Pillar World Wide Customer Support Center.

Table 1 Required support information

Value	Description
	Name and manufacturer of the DMA and its version number.
	IP address of the Pillar Axiom Pilot.
	NDMP user account name created on the Pillar Axiom system for your DMA.
	NDMP user account password created on the Pillar Axiom system for your DMA.
	TCP port assigned to the NDMP daemon.
	Name of the filesystem and the name of the File Server with which the NDMP attributes are associated.
	Device name of the tape device.
	Slammer name and the control unit (CU) number to which the tape device is directly attached.
	Type of NDMP adapter: SCSI or Fibre Channel (FC).
	LUN number and the name of FC attached tapes.
	Type of tapes are native SCSI with an FC converter between them and the Pillar Axiom or not.
	Network address and hostname of the DMA system(s).

Pillar Contacts

Table 2 Contacts at Pillar Data Systems

For help with...	Contact...
Error messages, usage questions, and other support issues	US and Canada: 877-4PILLAR (1-877-474-5527) Europe: +800 PILLAR FS (+800 74 55 27 37) Asia Pacific: +1-408-518-4515 South Africa: +0 800 980 400 Have your system serial number ready. support@pillardata.com Pillar Customer Support (http://support-portal.pillardata.com/csportal/login.seam)
Training (custom or packaged)	Training and Education (http://www.pillardata.com/support-education/training/)
Professional services and inquiries	globalsolutions@pillardata.com Global Solutions (http://www.pillardata.com/support/professional-services/)
Sales and general contact information	Company contacts (http://www.pillardata.com/company/contact)
Documentation improvements and resources	docs@pillardata.com Technical documents (http://www.pillardata.com/techdocs) (Log in with your username and password, and select Documents.)

CHAPTER 2

Overview of the Pillar Axiom System Configuration for NDMP Support

About Block-Level Backup Configuration

The Pillar Axiom system supports both file-level and block-level Network Data Management Protocol (NDMP) backup.

File-level backup is a file-by-file backup, and it requires no special configuration. Block-level backup is a volume-level backup that reads the entire filesystem data from its underlying block device and writes the data to the tape device. Block level backup has specific configuration requirements that depend on the version of your Pillar Axiom system.

Refer to the *Pillar Axiom Administrator's Guide* for details.

About Block-Level Backup Configuration for Pillar Axiom Releases 3.0 or Earlier

Block-level backups require additional temporary free storage equal to the size of the entire size of the filesystem being backed up, plus some extra processing space. The storage for this block backup can be the low or high priority storage that is available on the Pillar Axiom system using a volume copy. Allocate one GB of space, plus an additional GB for each TB to be used as processing space. For example, for a 10 TB filesystem (10,000 GB), allocate a total of 20,011 GB. This amount of free storage includes:

- 10 TB for the original filesystem
- 10 TB for the backup space
- 11 GB for processing space

Important! Before you restore a block-level backup image, be certain that the target filesystem is offline.

About Block-Level Backup Configuration for Pillar Axiom Releases 3.1 and 3.2

A block-level backup requires an amount of Clone FS storage to be allocated to the filesystem being archived. The amount of allocated storage should be proportional to the amount of data written to the filesystem during the course of the backup. For example, a 10 GB filesystem that has a 2 GB rate of change during the course of the backup must have at least 2 GB dedicated to Clone FS storage, or the backup fails.

Tip: If you do not know the rate of change for your filesystem, we recommend a Clone FS storage allocation that equals ten percent of the filesystem.

About Block-Level Backup Configuration for Pillar Axiom Releases 3.3 or Later

In releases 3.3 or later, block-level as well as file-level backups are based on Snap FS snapshots.

Block-level backup does not require additional Pillar Axiom storage or Clone FS repository storage.

Releases 4.x support ten concurrent NDMP processes (as opposed to releases 3.x that support only five concurrent backup and restore operations). The ten concurrent backup or restore operations are taken from the same pool of resources as NAS replications. Hence, if you run five NDMP backup operations, you can run only five NAS replications.

About Block-Level Restore Configuration

The Pillar Axiom system supports both file-level and block-level NDMP restore.

File-level restore operations restore specified files, and they do not require special configuration.

Block-level restore operations can only restore the entire filesystem, providing superior performance to file-level backups. Block-level restore operations have specific configuration requirements that depend on the version of your Pillar Axiom system.

Backup images made with previous Pillar Axiom releases can be restored in later releases.

About Block-Level Restore Configuration for Pillar Axiom Releases 3.0 or Earlier

When a filesystem is block-level restored, the capacities of the newly restored filesystem reflect that of the restored filesystem. For example, using the values in the following table, if `src_fs` is restored over `rest_fs` the final capacities of the filesystem would be a capacity of 10 GB and a maximum capacity of 20 GB, losing the 40 GB capacity of `rest_fs`.

Important! If the source filesystem size is larger than the target's maximum capacity or current capacity, the restore fails.

Table 3 Example block-level restore values for Pillar Axiom releases 3.0 and earlier

Value	Source filesystem	Target filesystem	Result of restore
Name	src_fs	rest_fs	rest_fs
Current capacity	10 GB	20 GB	10 GB
Maximum capacity	20 GB	40 GB	20 GB

About Block-Level Restore Configuration for Pillar Axiom Releases 3.1 and 3.2

When a filesystem is block-level restored, the target filesystem expands its current capacity if the source filesystem's current capacity is larger than the current capacity of the target. For example, using the values in the following table, if `src_fs` is restored over `rest_fs`, the current capacity of the target filesystem expands to 20 GB.

Important! If the source filesystem size or current capacity is larger than the target's maximum capacity, the restore fails.

Table 4 Example block-level restore values for Pillar Axiom releases 3.1 and 3.2

Value	Source filesystem	Target filesystem	Result of restore
Name	src_fs	rest_fs	rest_fs
Current capacity	10 GB	20 GB	20 GB
Maximum capacity	25 GB	40 GB	40 GB

About Block-Level Restore Configuration for Pillar Axiom Releases 3.3 or Later

The Pillar Axiom system does not preserve snapshot names when they are restored. Snapshots are renamed according to the timestamps they had when they were taken.

You will need to put restored filesystems online manually using the Pillar Axiom Storage Services Manager. Refer to the *Pillar Axiom Administrator's Guide* for details.

Pillar Axiom System Configuration Tips

The following items are general notes and tips for configuring a Pillar Axiom system to interact with a data management application (DMA).

- For small NDMP installations that include two to four tape drives, zone a tape library to a single Slammer control unit (CU). If the CU to which the tape library is assigned is offline for an extended period of time, the tape library can be easily rezoned to the other CU.
- For large NDMP installations with over four tape drives, create multiple virtual tape libraries. Zone each library and its tape devices to separate CUs to balance the I/O operations across multiple CUs.
- The Slammer CU on which NDMP runs depends on the type of backup being performed.
- For local NDMP backup and recovery, a SCSI or Fibre Channel (FC) interface module is required on the Slammer. Note the following:
    - One SCSI card is allowed for each Pillar Axiom system.
    - Only one FC card for each CU is allowed.
    - Only one FC attached library for each CU is allowed.
    - Tape devices within a library cannot be visible on different CUs at the same time.
    - Only eight LUNs can be zoned to a Pillar Axiom system.
- The Pillar Axiom system uses point-in-time Volume Copies (prior to release 3.1), Clone FS (releases 3.1 and 3.2), or Snap FS (releases 3.3 or later) to support NDMP block-level backup requests against non-WORM filesystems. However, when using an NDMP Volume Copy, there is an additional space limitation above the amount required for filesystem-based NDMP backups.
- During the NDMP backup process, the system creates a snapshot of the filesystem before archiving it. The NDMP backup appears in the list of snapshots until the backup is complete. If you delete the NDMP snapshot while the backup is in progress, the associated NDMP session fails. Wait for the system to remove the snapshot when the NDMP session is complete. Do not delete the snapshot manually.
- In releases 3.3 and later, filesystem snapshots deleted during the course of a block-level backup will not be part of the backup image. A subsequent

restore will not contain any snapshots that were deleted, but it will contain all other snapshots in the filesystem prior to the start of the backup.

- Updating system software may cause tape drives or libraries attached to a Pillar Axiom system to go offline. For example, Symantec NetBackup may mark the Pillar Axiom tape devices offline if they become temporarily unavailable during an upgrade. In this case, use the administrative tools provided by your DMA to bring the tape devices back online. If you need assistance, contact the Pillar World Wide Customer Support Center.

Related concepts

- *About Block-Level Backup Configuration*

Related references

- *Pillar Axiom Configuration Requirements for NDMP*

About NDMP Backup Operations on Full Filesystems

When an NDMP file-level or block-level (Pillar Axiom releases 3.3 or later), backup operation begins, the system takes an immediate Snap FS of the filesystem. This Snap FS is the NDMP data source for the backup. At the end of the backup operation, the system deletes the Snap FS. Working from this Snap FS allows clients to use the filesystem during the NDMP backup operation.

Snap FS is defined as:

> A point-in-time, read-only snapshot of a filesystem, which can be used later to restore the filesystem. A Snap FS has no Quality of Service (QoS) parameters. It consumes storage capacity from the filesystem itself. A Snap FS can be scheduled to occur at any time.

If the filesystem is full, a file-level backup operation may fail or it may be impossible to delete files from the original filesystem during the backup operation. This is because the data from those files would need to be stored in the backup image Snap FS.

Note: This behavior does not occur during block-level backups on Pillar Axiom systems prior to release 3.3 because those earlier releases did not use Snap FS for block-level backups.

To prevent the file-level backup operation from failing, you can increase the space allocated to the filesystem to allow any data that is modified or deleted during backup operations to be safely stored in the Snap FS created for the backup. If it becomes necessary to recover space, delete any unnecessary Snap FS instances and wait for the space to become available. If there are no Snap FS instances, delete at least 16 KB of data prior to running the backup.

Refer to the *Pillar Axiom Administrator's Guide* for details.

Pillar Axiom Configuration Requirements for NDMP

This table contains the Pillar Axiom configuration requirements for successfully integrating the Pillar Axiom system into an NDMP environment.

Table 5 Pillar Axiom Storage Services Manager requirements for NDMP

Requirement	Description
File Server	The NDMP subsystem uses the networking configuration from a single Pillar Axiom File Server, which can be selected by means of the Pillar Axiom Storage Services Manager GUI. A File Server must be defined in the NDMP configuration portion of the GUI.
NDMP command interface	The NDMP command and response interface on a Pillar Axiom system is the Pilot management interface. Data movement is performed over the data path interfaces provided by the Slammer. Be sure that any external NDMP backup servers are able to reach the Pilot management IP addresses. Use the IP or hostname of the Pilot when adding a Pillar Axiom system to the configuration of a third-party backup application (DMA).
Virtual network interface (VIF)	Only one VIF is required. For local backups, the networking configuration must be on the Slammer control unit (CU) to which the tape devices are attached. The tape menu in the GUI lists the CU as a control unit number. Refer to the *Pillar Axiom Administrator's Guide* for details. There are two ways to ensure there is networking on the CU with the tape devices: • Create the File Server on the CU with the tape devices (or move the File Server once it has been created). • Create a second VIF on the CU to which the tape devices are attached. **Note:** You must use the same File Server that is listed in the NDMP configuration.

CHAPTER 3

Overview of Data Management Application Configuration

Data Management Application Configuration Tips

The following items are general notes and tips for configuring a data management application (DMA) so it integrates successfully with the Pillar Axiom system.

- If you want to work with a tape library, a tape autoloader, or a standalone tape drive that is directly attached to a Slammer for backup and restore operations, specify the name of that device in the DMA configuration procedures.
- If you rename a filesystem, you must update the filesystem name in your DMA to the filesystem's new name. The next backup will be a full backup, even if an incremental backup is scheduled.
- Fibre Channel (FC) tape devices must have a LUN ID set between 0 and 7 (for each SCSI target ID) in order to be recognized by the Pillar Axiom system.
- Your FC switch zone must contain only switch ports, Pillar Axiom system ports, and tape library ports. Otherwise, non-tape devices might appear in the Pillar Axiom Storage Services Manager.
- Backup and restore operations are sensitive to fabric and SCSI bus noise. If you are using the QLogic QLA2340 HBA card, maintain low FC switch management activity while performing a backup or restore. FC switch management activities may cause backups and restores to fail due to port logouts.
- If you are using the Adaptec SCSI Card 29160, verify that the SCSI bus is properly terminated and you are using the recommended cable lengths.
- The maximum number of LUNs that can be zoned to a single FC NDMP card is eight LUNs for each target. The LUN ID must be between 0 and 7. It is possible to see more than eight drives because the system can allocate different target numbers randomly.

About the Exclude Backup Feature

Many data management applications (DMA) support a feature that excludes listed files or directories from the backup session. Usually called the Exclude Backup feature, it is also known as an *include/exclude backup* feature. Pillar Axiom systems running version 3.2 or later fully support this feature.

Note: All access to the Exclude Backup feature is specific to your DMA. If your DMA does not support the Exclude Backup feature, the option is ignored. Refer to your DMA documentation for information.

When performing a backup operation using DMA backup software, you may perform a file-based backup by specifying a list of directory paths and files. However, if there is a directory that does not need to be archived, it is cumbersome to include 99% of the files in a directory (that may be multiple layers deep) just to exclude that directory. Therefore, the Exclude Backup feature allows you to specify specific directory paths that are ignored by the DMA.

For example, to skip a sandbox directory on a server, use the full path `/server/share/directory/sandbox/` in the exclude string.

Related references

- *Exclude Backup Feature Requirements*

Exclude Backup Feature Requirements

The Exclude Backup feature requires an exclude string containing the data objects to be ignored by the Data Management Application (DMA). The following describes the special requirements of the Exclude Backup feature. Refer to your DMA documentation for information.

The DMA interprets an exclude string that defines the directories and files to be excluded from the backup process.

- An empty exclude string signifies that there is nothing to be excluded in the backup session.
- The maximum length of the exclude string is 20,480 bytes.
- The exclude string may contain multiple paths, and each path must be separated by a comma.
- If an exclude path ends in a filename, then this one file is excluded from the backup session.
- If an exclude path ends in directory name, then that directory name, the entire directory contents, and any sub-directories are excluded from the backup session.
- Multiple contiguous forward slashes are treated as a single forward slash.
- If a path ends in a forward slash, it is considered a directory name. That directory name, the entire directory contents, and any sub-directories are excluded from the backup session.
- If an exclude path specified is too long, or matches part of a path and filename, it is backed up as normal.

Note: File pathnames that are longer than 5120 characters are not excluded from the backup. The files are archived normally.

The Pillar Axiom NDMP server validates all files and paths in the exclude string. The following table contains information about special characters used in exclude strings.

Table 6 Special characters for an exclude string

Character	Description
\	The escape character is a backslash (\). If an escape or asterisk character is actually part of the filename or directory name, the escape character must be preceded by another escape character. • Two consecutive backslashes are collapsed to make one backslash. • A single backslash followed by an asterisk converts to a single asterisk.
,	If the comma character is to be part of a filename, it must be preceded with the escape character (backslash). For example, the file `blue,red.tmp` should be specified as `blue\,red.tmp`.
/	Every path must be specified relative to the backup root directory. If a path is not preceded with a forward slash then the system assumes that a forward slash is there.
*	The asterisk is treated as a wildcard character. If an asterisk is at the end of the path, or the characters “*.*” are encountered in the path, no subsequent part of the path will be evaluated. For example, in the path string `/level1dir/level2dir/*.*` the directory `level2dir`, all file contents, and any sub-directories are excluded from the backup session. To exclude an entire directory and all contents, add /* or /*.* after the directory name.

CHAPTER 4

Configure Data Management Applications

Configure the NDMP User Account

The backup administrator, by means of the data management application (DMA) software, creates a schedule of backup tasks. The DMA software uses the information contained in the schedule to automatically issue commands to the NDMP server on the Pilot to initialize and control backup and restore operations. To issue these commands, the DMA first logs in to the Pillar Axiom system using a pre-defined Pillar Axiom user account. To permit this login, enable NDMP on your Pillar Axiom system and configure the user account.

1. Log in to the Pillar Axiom Storage Services Manager.
2. Click the **System** icon in the top context pane.
3. Click the **NDMP Backup Settings** link in the left navigation pane.
4. Select **Modify NDMP Backup Settings** from the **Actions** drop-down list.
5. Select the **Enable NDMP** option.
6. Enter values for the NDMP port, user name, and File Server fields.

   The File Server value is the name of the File Server through which backups are performed.

   Note: The NDMP user account has permission only to perform NDMP backup and restore operations.
7. (Optional) Click **Change Password**.

   Note: We recommend that you modify the password for the NDMP user account for greater security.
8. Enter between six and eight characters for the NDMP user account password, and click **OK**.
9. Click **OK** to save the NDMP settings.

Rename a File Server for an NDMP Configuration

If you modify a File Server's name, you may need to update the NDMP configuration in the Pillar Axiom Storage Services Manager.

1. Launch the Pillar Axiom Storage Services Manager, and go to the **System > NDMP Backup Settings** page.
2. Select **Modify NDMP Backup Settings** from the **Actions** drop-down list.
3. If the File Server field displays **None**, select the File Server's new name from the drop-down list, and click **OK**.

About CommVault Galaxy and the Pillar Axiom System

CommVault Galaxy requires only the NDMP username and password, and the Pillar Axiom host name. There are no other special parameters to set.

Note: Any documentation from CommVault supersedes this document.

Make sure you have the username, password, and host name before beginning this task. Use the Galaxy configuration utility to set up the link to the Pillar Axiom system.

Important! Install Service Pack 4 if you are using Windows 2000.

Note: The Pillar Axiom system does not support the NDMP security extension.

Related tasks

- *Configure the NDMP User Account*

Configure Symantec Veritas NetBackup

These are the steps and parameters required for configuring Symantec Veritas NetBackup 6.0 to communicate with the Pillar Axiom system. After configuring Symantec NetBackup 6.0, you can perform data backup and restore operations in local and 3-way tape-attached environments.

To see the *Veritas NetBackup™ 3.4 – 6.0 Network Data Management Protocol Hardware Compatibility List*, go to the Symantec Veritas Web site (http://ftp.support.veritas.com/pub/support/products/NetBackup_DataCenter/251713.pdf).

Make sure you configure the NDMP user account before beginning this task.

For details on how to configure NetBackup, refer to the appropriate NetBackup documentation. Detailed instructions relating to specific tasks for NetBackup are outside the scope of this document. Any documentation from Symantec supersedes this document.

Note: The Pillar Axiom system does not support the NDMP security extension.

Use the NetBackup Device Configuration Wizard to create and configure a backup policy that uses the parameters defined below to access the Pillar Axiom File Server.

1. Specify the TYPE environment variable:

   Use *TYPE = file_dsif* for file-level backups or *TYPE = block_dsif* for block-level backups. Use the format:

   ```
   set TYPE = file_dsif
   ```

   or

   ```
   set TYPE = block_dsif
   ```

   Important! You must include the spaces; otherwise, Direct Access Recoveries (DAR) are not possible.

   Note: This TYPE variable must be listed prior to backup path variables or the TYPE variable is ignored.

2. Include the following environment variables in the **Backup Selections** section of the backup policy (optional):

   - *PILLAR_ACL*. Specifies whether access control lists (ACL) are backed up:
     - Y: Back up the ACLs (default).

- N: Do not back up the ACLs.

Use the format:

```
set PILLAR_ACL = Y
```

or

```
set PILLAR_ACL = N
```

Tip: If your environment is NFS-only, or if you have CIFS clients but do not care about ACLs, you can avoid backing up the ACLs by setting the PILLAR_ACL variable to N. Not backing up ACLs can provide a modest performance increase.

3 (Optional) If you are using Pillar Axiom releases 3.3 or later, you can also specify the following parameters in the **Backup Selections** section of the backup policy:

- *PILLAR_COMPRESS_DATA*. Specifies whether the Pillar Axiom system performs ZLIB compression prior to writing the data to tape or over the network. This may be useful if you are backing up data to a remote data server over a WAN.
  - N: Do not use data compression (default)
  - Y: Use data compression

  Use the format:

  ```
  set PILLAR_COMPRESS_DATA = Y
  ```

  or

  ```
  set PILLAR_COMPRESS_DATA = N
  ```

  Note: Setting this parameter provides software compression, not hardware compression.

- *PILLAR_RATE_LIMIT*. Specifies a limit for the amount of network bandwidth used by the backup, for three-way backup operations only. Backups to tape will ignore any rate limiting when doing local backups. Specify the maximum throughput allowed in Kb/s. For example, a value of 200 will limit the rate to 200 Kb/s. This limit is specific to the individual backup being run.
  - Zero or no value: No limit (default)
  - Non-zero value: Maximum throughput allowed in Kb/s

  Use the format:

  ```
  set PILLAR_RATE_LIMIT = n
  ```

where *n* is zero, no value, or the maximum throughput in Kb/s.

4 Specify the pathname as */fileserver-name/source-path*. The *source-path* value identifies the filesystem or file that is the source for the backup operation.

5 Specify an existing NDMP storage unit.

6 Specify the client name as *Pilot hostname* or *IP*.

7 For the client properties, specify **NDMP** as the hardware property and **NDMP** as the operating system property.

Related tasks

- *Configure the NDMP User Account*

Configure EMC NetWorker

These instructions allow EMC Networker 7.3 to communicate with the Pillar Axiom system. For EMC NetWorker to recognize the Pillar Axiom system, you must configure certain parameters within the EMC NetWorker software.

Make sure you configure the NDMP user account before beginning this task. For specific details on how to configure EMC NetWorker, refer to the appropriate NetWorker documentation. Detailed instructions relating to specific tasks for NetWorker are outside the scope of this document. Any documentation from EMC supersedes this document.

Note: The Pillar Axiom system does not support the NDMP security extension.

1. Enable and register the NDMP Client Connection.
2. Enable and register the Storage Node.
3. Install and configure the EMC SnapImage Module.
4. Configure the autochanger or tape device (a NetWorker Autochanger Module is required).

   Note: If you're using a tape autochanger, run the `jbconfig` tool from the command line on the NetWorker server to configure the autochanger for NDMP operations.
5. Configure the NetWorker server for NDMP operations.
6. To configure the Pillar Axiom NDMP server as a data source, use the NetWorker Administrator application to set these attributes:
   - Name of the Pillar Axiom system or the IP address of the Pilot
   - Name of the save set, the syntax of which is:

     / fileserver-name/ source-path

     The *source-path* value identifies the filesystem or file that is the source for the backup operation.
   - Name of the remote user, which is the name of the NDMP account
   - Password of the remote user, which is the NDMP account password
   - Backup command, the syntax of which is:

     `nsrndmp_save -T` *data-format*

This command tells NetWorker what format to use. The value for *data-format* can be either `file_dsif` (for file-based backups) or `block_dsif` (for block-based backups).

Note: If you want to perform a Direct Access Recovery (DAR), specify a data format of `file_dsif`.

- Application information (NDMP environment variables):
  - List of files that were backed up:

    `HIST=`*Y-or-N*

    For *Y-or-N*, a value of Y reports the list of files; a value of N reports no list.

    By default, the NDMP server sends a file history. If you do not want the NDMP server to send a file history, set HIST=N.

    Note: If you want to perform a DAR recovery, be sure the NDMP server sends a file history.

  - Direct backups:

    `DIRECT=`*Y-or-N*

    For *Y-or-N*, a value of Y causes the NDMP server to perform a direct backup. A value of N causes the NDMP server to perform a normal backup (default).

    EMC NetWorker requires that DIRECT be set explicitly.

- Pillar-specific environment variables:
  - PILLAR_ACL. Specifies whether access control lists (ACL) are backed up:
    - Y: Back up the ACLs (default)
    - N: Do not back up the ACLs

    Tip: If your environment is NFS-only or you have CIFS clients but do not care about ACLs, you do not need to back up ACLs. Not backing up ACLs provides a modest performance increase.

7 Use the NetWorker Administrator application to configure any Slammer-attached tape devices.

Refer to the appropriate DMA documentation.

8 Use the `jbconfig` utility to set these tape library attributes:

- Name of the Pillar Axiom system or the IP address of the Pilot

- Device name and IP address of the remote tape device. Use the following `jbconfig` command syntax:

  ```
  rd=IP-address:device-name
  ```

- Media type of the remote storage device
- NDMP = Yes, to mark it as an NDMP device
- Name of the remote user
- Password of the remote user

9 Use the NetWorker Administrator application, or the `jbconfig` utility, to set these attributes for a jukebox (autochanger) or other robotic storage device:

- Autodetected NDMP SCSI Jukebox Autochanger
- Name of the Pillar Axiom system or the IP address of the Pilot
- Name of the remote user
- Password of the remote user
- Name of the storage device

Tip: Run a test backup and restore operation to verify that your NetWorker configuration is correct.

Related tasks

- *Configure the NDMP User Account*

Configure BakBone NetVault: Backup

These instructions allow BakBone NetVault: Backup 7 to communicate with the Pillar Axiom system. The Pillar Axiom support pack must be successfully installed before the Pillar Axiom File Server can be recognized by the NetVault: Backup software.

Make sure you configure the NDMP user account before beginning this task. For specific details on how to configure NetVault: Backup, refer to the appropriate NetVault: Backup documentation. Detailed instructions relating to specific tasks for NetVault: Backup are outside the scope of this document. Any documentation from BakBone supersedes this document.

Note: The Pillar Axiom system does not support the NDMP security extension.

1. Obtain the support pack for the File Server from the Pillar World Wide Customer Support Center.

   Usually, this is a file called pchy200.npk.

   Important! If you are using the NDMP plugin 6.5 update 4 or later, the support pack is not required. Skip to Step 7.

2. Launch NetVault: Backup Configurator.
3. Open the Packages dialog and click **Install Software**.
4. Click **Browse** to navigate to the location of the pchy200.npk installation file.
5. Click on this file to select it, then click **Next**.

   When the installation has completed, a successful installation message appears in the Install Software dialog box.

6. Click **OK** to close this dialog box and complete the installation.
7. Launch NetVault and add the File Server to the NDMP client list in the backup window.

   Consult the NetVault documentation for complete instructions. You will need the following parameters:

   - File Server: Name of the File Server to which NetVault connects
   - IP Address: IP address or hostname of the Pilot
   - Port Number: The NDMP port used to connect to the Pillar Axiom File Server, typically 10000
   - Account: The NDMP username configured on the File Server

- Password: The NDMP password on the File Server

The files and filesystems on the Pillar Axiom system are now accessible to the NetVault: Backup Configurator.

Related tasks

- *Configure the NDMP User Account*

Configure Oracle Secure Backup

These instructions allow Oracle Secure Backup 10.1.0.3 to communicate with the Pillar Axiom system. For Oracle Secure Backup to recognize the Pillar Axiom system, you must configure certain parameters within the Oracle Secure Backup software.

Make sure you configure the NDMP user account before beginning this task.

For specific details on how to configure Oracle Secure Backup, refer to the appropriate Oracle Secure Backup documentation. Detailed instructions relating to specific tasks for Oracle Secure Backup are outside the scope of this document. Any documentation from Oracle supersedes this document.

Note: The Pillar Axiom system does not support the NDMP security extension.

The Pillar Axiom system uses the default options for creating a host for Oracle Secure Backup with only one exception: the Pillar Axiom system uses a unique parameter for the *-B* backup type option of `obtool`.

Note: The Oracle utility `obtool` is the primary command-line interface to Oracle Secure Backup. The `obtool` executable is located in the `bin` subdirectory of the Oracle Secure Backup home. Refer to the *Oracle Secure Backup Reference Guide* for details.

1. Create a host using `obtool` with the -B backup type option.

   For file-level backups use *-B file_dsif*. For block-level backups use *-B block_dsif*. For example, this command would be used to create a host for file-level backups:

   ```
   obtool mkhost -a ndmp -u username -p password -B file_dsif
   hostname
   ```

   Where:

   - *username* and *password* are the values you created when you configured the NDMP user account.
   - *hostname* is the Pillar Axiom system's hostname or IP address.

2. Verify the connection to the Pillar Axiom system with the command:

   ```
   obtool pinghost hostname
   ```

3. Set up your tape devices according to the manufacturer's instructions.

4 Use the `obtool pingdev` option to verify the connection to your tape devices with the command:

```
obtool pingdev your tape device
```

Related tasks

- *Configure the NDMP User Account*

Index