IBM System Storage N series

Clustered Data ONTAP 8.2 Data Protection Tape Backup and Recovery Guide

SC27-6274-01

Contents

Preface

About this guide

This document applies to IBM N series systems running Data ONTAP, including systems with gateway functionality. If the terms *Cluster-Mode* or *clustered Data ONTAP* are used in this document, they refer to the Data ONTAP features and functionality designed for clusters, which are different from 7-Mode and prior Data ONTAP 7.1, 7.2, and 7.3 release families.

In this document, the term *gateway* describes IBM N series storage systems that have been ordered with gateway functionality. Gateways support various types of storage, and they are used with third-party disk storage systems—for example, disk storage systems from IBM, HP®, Hitachi Data Systems®, and EMC®. In this case, disk storage for customer data and the RAID controller functionality is provided by the back-end disk storage system. A gateway might also be used with disk storage expansion units specifically designed for the IBM N series models.

The term *filer* describes IBM N series storage systems that either contain internal disk storage or attach to disk storage expansion units specifically designed for the IBM N series storage systems. Filer storage systems do not support using third-party disk storage systems.

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in *Websites* on page 7).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:
  www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web

content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:

www.ibm.com/storage/support/nseries/

This web page also provides links to AutoSupport information as well as other important N series product resources.

- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:

  www.ibm.com/systems/storage/network/interophome.html
- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:

  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in *Websites* on page 7) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in *Websites* on page 7).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in *Websites* on page 7).

Note: If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by email to *starpubs@us.ibm.com*.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Tape backup of FlexVol volumes

Data ONTAP supports tape backup and restore through the Network Data Management Protocol (NDMP). NDMP allows you to back up storage systems directly to tape, resulting in efficient use of network bandwidth. Clustered Data ONTAP supports dump engine for tape backup.

Dump is a Snapshot copy-based backup to tape, in which your file system data is backed up to tape. The Data ONTAP dump engine backs up files, directories, and the applicable access control list (ACL) information to tape. You can back up an entire volume, an entire qtree, or a subtree that is neither an entire volume nor an entire qtree. Dump supports level-0, differential, and incremental backups.

You can perform a dump backup or restore by using NDMP-compliant backup applications. Starting with Data ONTAP 8.2, only NDMP version 4 is supported.

Related concepts

Understanding NDMP for FlexVol volumes on page 29
Understanding dump engine for FlexVol volumes on page 54

Performing tape backup and restore of FlexVol volumes

You can perform tape backup and restore operations by using an NDMP-enabled backup application.

About this task

The tape backup and restore workflow provides an overview of tasks that are involved in performing tape backup and restore operations. To perform a backup and restore operation, see the backup application documentation.

Steps

1. Set up a tape library configuration by choosing an NDMP-supported tape topology.
2. Enable NDMP services on your storage system.

   You can enable the NDMP services either at the node level or at the Storage Virtual Machine (SVM) level. This depends upon the NDMP mode in which you choose to perform a tape backup and restore operation.
3. Use NDMP options to manage NDMP on your storage system.

   You can use NDMP options either at the node level or at the SVM level. This depends upon the NDMP mode in which you choose to perform a tape backup and restore operation. You can modify the NDMP options at the node level by using the `options` command and at the SVM

level by using the `vserver services ndmp modify` command. For more information about these commands, see the man pages.

4. Perform a tape backup or restore operation by using an NDMP-enabled backup application.

   Clustered Data ONTAP supports dump engine for tape backup and restore. For more information about using the backup application (also called Data Management Applications or DMAs) to perform backup or restore operations, see your backup application documentation.

Related concepts

Understanding dump engine for FlexVol volumes on page 54

Related references

Common NDMP tape backup topologies on page 42

Where to find information about Infinite Volume tape backup and restore

Information about tape backup and restore of Infinite Volumes is available in the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Understanding tape drives

You must use a qualified tape drive that has been tested and found to work properly on a storage system. You can follow tape aliasing and also enable tape reservations to ensure that only one storage system accesses a tape drive at any particular time.

What qualified tape drives are

A qualified tape drive is a tape drive that has been tested and found to work properly on storage systems.

You can add support for tape drives to existing Data ONTAP releases by using the tape configuration file. You can download the tape configuration file from the N series support website (accessed and navigated as described in *Websites* on page 7). You can view the instructions required to download the tape configuration file, add support to Data ONTAP for a tape drive that was qualified after the release of the Data ONTAP version, and view the current list of supported tape drives at the N series support website (accessed and navigated as described in *Websites* on page 7).

Only qualified tape drives are listed in the tape qualification list. The tape libraries are not listed. For example, the tape library IBM TS3500 is not listed. However, the IBM LTO 4 tape drives that the IBM TS3500 contains are listed.

You can view information about qualified and nonqualified tape drives, tape libraries, and tape drive connections to the storage system.

Related tasks

Using a nonqualified tape drive on page 24

Related references

Commands for viewing tape drive information on page 23
Commands for verifying tape library connections on page 27

Related information

IBM N series Interoperability Matrices website: www.ibm.com/systems/storage/network/interophome.html

Format of the tape configuration file

The tape configuration file format consists of fields such as vendor ID, product ID, and details of compression types for a tape drive. This file also consists of optional fields for enabling the autoload feature of a tape drive and changing the command timeout values of a tape drive.

The following table displays the format of the tape configuration file:

Item	Size	Description
vendor_id (string)	up to 8 bytes	The vendor ID as reported by the `SCSI Inquiry` command.
product_id (string)	up to 16 bytes	The product ID as reported by the `SCSI Inquiry` command.
id_match_size (number)		The number of bytes of the product ID to be used for matching to detect the tape drive to be identified, beginning with the first character of the product ID in the Inquiry data.
vendor_pretty (string)	up to 16 bytes	If this parameter is present, it is specified by the string displayed by the nodeshell command, `sysconfig -v` , or `sysconfig -t`; otherwise, INQ_VENDOR_ID is displayed.
product_pretty (string)	up to 16 bytes	If this parameter is present, it is specified by the string displayed by the nodeshell command, `sysconfig -v`, or `sysconfig -t`; otherwise, INQ_PRODUCT_ID is displayed.

Note: The *vendor_pretty* and *product_pretty* fields are optional, but if one of these fields has a value, the other must also have a value.

The following table explains the description, density code, and compression algorithm for the various compression types such as, `l`, `m`, `h`, and `a`:

Item	Size	Description
`{l | m | h | a}_description=(string)`	up to 16 bytes	The string to print for the nodeshell command, `sysconfig -t` that describes characteristics of the particular density setting.
`{l | m | h | a}_density=(hex codes)`		The density code to be set in the SCSI mode page block descriptor corresponding to the desired density code for l, m, h, or a.

Item	Size	Description
`{l | m | h | a}_algorithm=(hex codes)`		The compression algorithm to be set in the SCSI Compression Mode Page corresponding to the density code and the desired density characteristic.

The following table describes the optional fields available in the tape configuration file:

Field	Description
`autoload=(Boolean yes/no)`	This field is set to `yes` if the tape drive has an automatic loading feature; that is, after tape cartridge is inserted, the tape drive becomes ready without the need to execute a `SCSI load` (start/stop unit) command. The default for this field is `no`.
`cmd_timeout_0x`	Individual timeout value. Use this field only if you want to specify a different timeout value from the one being used as a default by the tape driver. The sample file lists the default SCSI command timeout values used by the tape drive. The timeout value can be expressed in minutes (m), seconds (s), or milliseconds (ms). **Note:** You should change this field only with guidance from technical support.

To download and view the tape configuration file, go to the N series support website (accessed and navigated as described in *Websites* on page 7).

Example of a tape configuration file format

The tape configuration file format for the HP LTO5 ULTRIUM tape drive is as follows:

vendor_id="HP"

product_id="Ultrium 5-SCSI"

id_match_size=9

vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3(ro)/4 4/800GB"

l_density=0x00

l_algorithm=0x00

m_description="LTO-3(ro)/4 8/1600GB cmp"

m_density=0x00

m_algorithm=0x01

h_description="LTO-5 1600GB"

h_density=0x58

h_algorithm=0x00

a_description="LTO-5 3200GB cmp"

a_density=0x58

a_algorithm=0x01

autoload="yes"

Related information

IBM N series Interoperability Matrices website: www.ibm.com/systems/storage/network/interophome.html

How the storage system qualifies a new tape drive dynamically

The storage system qualifies a tape drive dynamically by matching its vendor ID and product ID with the information contained in the tape qualification table.

When you connect a tape drive to the storage system, the storage system looks for a vendor ID and product ID match between information obtained during the tape discovery process and information contained in the internal tape qualification table. If the storage system discovers a match, it marks the tape drive as qualified and can access the tape drive. If the storage system cannot find a match, the tape drive remains in the unqualified state and is not accessed.

What tape devices are

A tape device is a representation of a tape drive. It is a specific combination of rewind type and compression capability of a tape drive.

A tape device is created for each combination of rewind type and compression capability. Therefore, a tape drive or tape library can have several tape devices associated with it. You must specify a tape device to move, write, or read tapes.

When you install a tape drive or tape library on a storage system, Data ONTAP creates tape devices associated with the tape drive or tape library.

Data ONTAP detects tape drives and tape libraries and assigns logical numbers and tape devices to them. Data ONTAP detects the Fibre Channel, SAS, and parallel SCSI tape drives and libraries when

they are connected to the interface ports. Data ONTAP detects these drives when their interfaces are enabled.

Tape device name format

Each tape device has an associated name that appears in a defined format. The format includes information about the type of device, rewind type, alias, and compression type.

The format of a tape device name is as follows:

[*remote_host:*]*rewind_type* st *alias_number compression_type*

remote_host is optional. You specify a remote host storage system if you want to use a tape drive attached to that host. You must follow the remote host name with a colon (:).

rewind_type is the rewind type.

The following list describes the various rewind type values:

r Data ONTAP rewinds the tape after it finishes writing the tape file.

nr Data ONTAP does not rewind the tape after it finishes writing the tape file. Use this rewind type when you want to write multiple tape files on the same tape.

ur This is the unload/reload rewind type. When you use this rewind type, the tape library unloads the tape when it reaches the end of a tape file, and then loads the next tape, if there is one.

Use this rewind type only under the following circumstances:

- The tape drive associated with this device is in a tape library or is in a medium changer that is in the library mode.
- The tape drive associated with this device is attached to a storage system.
- Sufficient tapes for the operation that you are performing are available in the library tape sequence defined for this tape drive.

Note: If you record a tape using a no-rewind device, you must rewind the tape before you read it.

st is the standard designation for a tape drive.

alias_number is the alias that Data ONTAP assigns to the tape drive. When Data ONTAP detects a new tape drive, Data ONTAP assigns an alias to the tape drive.

compression_type is a drive-specific code for the density of data on the tape and the type of compression.

The following list describes the various values for *compression_type*:

a Highest compression

h High compression

m Medium compression

l Low compression

Examples

- `nrst0a` specifies a no-rewind device on tape drive 0 using the highest compression.
- `remfiler:nrst0a` specifies a no-rewind device on tape drive 0 on the remote host remfiler that uses the highest compression.

Attention: When using the urst device with the `dump` or `restore` command, ensure that you use tape libraries and that there are sufficient tapes in the library sequence. Otherwise, the tape drives involved terminate the command sequence or overwrite the same tape multiple times.

Example of a listing of tape devices

The following example shows the tape devices associated with HP Ultrium 2-SCSI:

```
Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
   rst0l  -  rewind device,        format is: HP (200GB)
   nrst0l -  no rewind device,     format is: HP (200GB)
   urst0l -  unload/reload device, format is: HP (200GB)
   rst0m  -  rewind device,        format is: HP (200GB)
   nrst0m -  no rewind device,     format is: HP (200GB)
   urst0m -  unload/reload device, format is: HP (200GB)
   rst0h  -  rewind device,        format is: HP (200GB)
   nrst0h -  no rewind device,     format is: HP (200GB)
   urst0h -  unload/reload device, format is: HP (200GB)
   rst0a  -  rewind device,        format is: HP (400GB w/comp)
   nrst0a -  no rewind device,     format is: HP (400GB w/comp)
   urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

The following list describes the abbreviations in the preceding example:

- GB—Gigabytes; this is the capacity of the tape.
- w/comp—With compression; this shows the tape capacity with compression.

Supported number of simultaneous tape devices

Data ONTAP supports a maximum of 64 simultaneous tape drive connections, 16 medium changers, and 16 bridge or router devices for each storage system in any mix of Fibre Channel, SCSI, or SAS attachments.

Tape drives or medium changers can be devices in physical or virtual tape libraries or stand-alone devices.

Note: Although a storage system can detect 64 tape drive connections, the maximum number of backup and restore sessions that can be performed simultaneously depends upon the scalability limits of the backup engine.

Related concepts

Scalability limits for dump backup and restore sessions on page 59

What tape aliasing is

Aliasing simplifies the process of device identification. Aliasing binds a physical path name (PPN) or a serial number (SN) of a tape or a medium changer to a persistent, but modifiable alias name.

The following table describes how tape aliasing enables you to ensure that a tape drive (or tape library or medium changer) is always associated with a single alias name:

Scenario	Reassigning of the alias
When the system reboots	The tape drive is automatically reassigned its previous alias.
When a tape device moves to another port	The alias can be adjusted to point to the new address.
When more than one system uses a particular tape device	The user can set the alias to be the same for all the systems.

Note: When you upgrade from Data ONTAP 8.1.x to Data ONTAP 8.2.x, the tape alias feature of Data ONTAP 8.2.x modifies the existing tape alias names. In such a case you might have to update the tape alias names in the backup application.

Assigning tape aliases provides a correspondence between the logical names of backup devices (for example, st0 or mc1) and a name permanently assigned to a port, a tape drive, or a medium changer.

Note: st0 and st00 are different logical names.

Note: Logical names and serial numbers are used only to access a device. After the device is accessed, it returns all error messages by using the physical path name.

There are two types of names available for aliasing: physical path name and serial number.

What physical path names are

Physical path names (PPNs) are the numerical address sequences that Data ONTAP assigns to tape drives and tape libraries based on the SCSI-2/3 adapter or switch (specific location) they are connected to, on the storage system. PPNs are also known as electrical names.

PPNs of direct-attached devices use the following format:

host_adapter.*device_id_lun*

Note: The LUN value is displayed only for tape and medium changer devices whose LUN values are not zero; that is, if the LUN value is zero the *lun* part of the PPN is not displayed.

For example, the PPN 8.6 indicates that the host adapter number is 8, the device ID is 6, and the logical unit number (LUN) is 0.

SAS tape devices are also direct-attached devices. For example, the PPN 5c.4 indicates that in a storage system, the SAS HBA is connected in slot 5, SAS tape is connected to port C of the SAS HBA, and the device ID is 4.

PPNs of Fibre Channel switch-attached devices use the following format:

switch:port_id.*device_id_lun*

For example, the PPN MY_SWITCH:5.3L2 indicates that the tape drive connected to port 5 of a switch called MY_SWITCH is set with device ID 3 and has the LUN 2.

The LUN (logical unit number) is determined by the drive itself. Fibre Channel, SCSI tape drives and libraries, and disks have PPNs.

PPNs of tape drives and libraries do not change unless the name of the switch changes, the tape drive or library moves, or the tape drive or library is reconfigured. PPNs remain unchanged after reboot.

For example, if a tape drive named MY_SWITCH:5.3L2 is removed and a new tape drive with the same device ID and LUN is connected to port 5 of the switch MY_SWITCH, the new tape drive would be accessible by using MY_SWITCH:5.3L2.

What serial numbers are

A serial number (SN) is a unique identifier for a tape drive or a medium changer. Starting with Data ONTAP 8.2, Data ONTAP generates aliases based on SN instead of the WWN.

Since the SN is a unique identifier for a tape drive or a medium changer, the alias remains the same regardless of the multiple connection paths to the tape drive or medium changer. This helps storage systems to track the same tape drive or medium changer in a tape library configuration.

The SN of a tape drive or a medium changer does not change even if you rename the Fibre Channel switch to which the tape drive or medium changer is connected. However, in a tape library if you replace an existing tape drive with a new one, then Data ONTAP generates new aliases because the SN of the tape drive changes. Also, if you move an existing tape drive to a new slot in a tape library or remap the tape drive's LUN, Data ONTAP generates a new alias for that tape drive.

Attention: You must update the backup applications with the newly generated aliases.

The SN of a tape device uses the following format: `SN[`*xxxxxxxxxx*`]L[`*X*`]`

x is an alphanumeric character and L*X* is the LUN of the tape device. If the LUN is 0, the L*X* part of the string is not displayed.

Each SN consists of up to 32 characters; the format for the SN is not case-sensitive.

Considerations when configuring multipath tape access

You can configure multiple paths from the storage system to access tape drives in a tape library. If one path fails, then the storage system can use the other paths to access tape drives without having to immediately repair the failed path. This ensures that tape operations can be restarted.

You must take into account a list of considerations when configuring multipath tape access from your storage system:

- In tape libraries that support LUN mapping, for multipath access to a LUN group, LUN mapping must be symmetrical on each path.

  Tape drives and media changers are assigned to LUN groups (set of LUNs that share the same initiator path set) in a tape library. All tape drives of a LUN group must be available for backup and restore operations on all multiple paths.
- Maximum of two paths can be configured from the storage system to access tape drives in a tape library.
- Multipath tape access does not support load balancing.

In the following example, the storage system accesses LUN group 0 through two initiator paths: 0b and 0d. On both of these paths, the LUN group has the same LUN number, 0 and LUN count, 5. The storage system accesses LUN group 1 through only one initiator path, 3d.

```
STSW-3070-2_cluster::> storage library config show

Node                     LUN Group   LUN Count  Library Name  Library Target Port  Initiator
------------------------ ----------- ---------- ------------- -------------------- -----
STSW-3070-2_cluster-01        0      5          IBM 3573-TL_1  510a09800000412d     0b
                                                                                    0d
                              1      2          IBM 3573-TL_2  50050763124b4d6f     3d

3 entries were displayed
```

For more information, see the man pages.

How to add tape drives and libraries to storage systems

You can add tape drives and libraries to storage systems dynamically (without taking the storage systems offline).

When you add a new medium changer, the storage system detects its presence and adds it to the configuration. If the medium changer is already referenced in the alias information, no new logical names are created. If the library is not referenced, the storage system creates a new alias for the medium changer.

In a tape library configuration, you must configure a tape drive or medium changer on LUN 0 of a target port for Data ONTAP to discover all medium changers and tape drives on that target port.

What tape reservations are

Multiple storage systems can share access to tape drives, medium changers, bridges, or tape libraries. Tape reservations ensure that only one storage system accesses a device at any particular time by enabling either the SCSI Reserve/Release mechanism or SCSI Persistent Reservations for all tape drives, medium changers, bridges, and tape libraries.

Note: All the systems that share devices in a library, whether switches are involved or not, must use the same reservation method.

The SCSI Reserve/Release mechanism for reserving devices works well under normal conditions. However, during the interface error recovery procedures, the reservations can be lost. If this happens, initiators other than the reserved owner can access the device.

Reservations made with SCSI Persistent Reservations are not affected by error recovery mechanisms, such as loop reset or target reset; however, not all devices implement SCSI Persistent Reservations correctly.

Managing tape drives

You can verify tape library connections and view tape drive information prior to performing a tape backup or restore operation. You can use a nonqualified tape drive by emulating this to a qualified tape drive. You can also assign and remove tape aliases in addition to viewing existing aliases.

When you back up data to tape, the data is stored in tape files. File marks separate the tape files, and the files have no names. You specify a tape file by its position on the tape. You write a tape file by using a tape device. When you read the tape file, you must specify a device that has the same compression type that you used to write that tape file.

Commands for viewing tape drive information

You can view information about tape drives to help you perform a tape backup and restore operation, use tape drives supported by Data ONTAP, understand tape drive performance, and be aware of the existing tape aliases.

You can view the following tape drive information:

- Node to which the tape drive is attached
- Device ID
- NDMP path
- Tape drive description
- Tape drives supported by Data ONTAP
- Tape drive statistics
- Existing aliases of tape drives

To use some of the commands listed in the following table, you need to access the nodeshell. You can access the nodeshell by using the `system node run` command.

If you want to...	Use this command...
View information about tape drives in a cluster	`system node hardware tape drive show`
View tape drives supported by Data ONTAP	`storage show tape supported [-v]` **Note:** You must use this command at the nodeshell. You can use the `-v` option to view more details about each tape drive.

If you want to...	Use this command...
View tape device statistics to understand tape performance and check usage pattern. You can reset the statistics reading and restart the process of displaying the statistics whenever you want.	`storage stats tape tape_name` **Note:** You must use this command at the nodeshell.
View existing aliases of tape drives	`storage alias` **Note:** You must use this command at the nodeshell.

For more information about these commands, see the man pages.

Using a nonqualified tape drive

To use a nonqualified tape drive, you must first determine whether it emulates any of the qualified tape drives.

About this task

You can use a nonqualified tape drive (one that is not on the list of qualified tape drives) on a storage system if it can emulate a qualified tape drive. It is then treated as though it were a qualified tape drive.

To use some of the commands, you need to access the nodeshell. You can access the nodeshell by using the `system node run` command. For more information about this command, see the man pages.

Steps

1. If the storage system has accessed the tape drive through the `mt` command, go directly to Step 3. If the storage system has not accessed the tape drive through the `mt` command, go to Step 2.
2. To access the tape drive, enter the following command at the nodeshell:

   `mt -f` *`device`* `status`

   `device` is any device that contains the tape drive number that you think is assigned to the tape drive.

   Example

   `mt -f nrst1a status`
3. Enter the following command at the nodeshell:

   `sysconfig -t`

If the storage system has registered a tape drive as emulating a qualified tape drive, it displays a message similar to the following:
`Tape drive (6.5) DLT9000 emulates Digital DLT7000`

If the storage system has not registered a tape drive as emulating a qualified tape drive, it displays a message similar to the following:
`Tape drive (6.5) DLTXXXX (Non-qualified tape drive)`

To emulate a qualified tape drive, go to the N series support website (accessed and navigated as described in *Websites* on page 7).

Related concepts

What qualified tape drives are on page 13

Related information

IBM N series Interoperability Matrices website: www.ibm.com/systems/storage/network/interophome.html

Assigning tape aliases

You can assign tape aliases to provide a correspondence between the logical names of backup devices and a name permanently assigned to a port, a tape drive, or a medium changer.

About this task

To use the following command, you need to access the nodeshell. You can access the nodeshell by using the `system node run` command. For more information about this command, see the man pages.

Step

1. To assign an alias to a tape drive or medium changer, enter the following command at the nodeshell:

   `storage alias [`*`alias`* **`{`*`PPN`* **`|` *`SN`*`}]`**

   `alias` is the logical name of the tape drive or medium changer to which you want to add the alias.

   `PPN` is the physical path name to which you want to assign the tape drive or medium changer.

   `SN` is the unique identifier of a tape drive or medium changer.

   Note: You can view the PPN and SN information about the tape drives and tape libraries by using `system node hardware tape drive show` and `system node hardware tape library show` commands respectively.

Examples

`storage alias st0 MY_SWITCH:5.3L3`

The tape device st0 is assigned to the physical path name MY_SWITCH:5.3L3.

`storage alias mc80 SN[HU106150D4]`

The medium changer alias mc80 is mapped to its serial number SN[HU106150D4] on LUN 0.

Related concepts

What tape aliasing is on page 19

Related tasks

Removing tape aliases on page 26

Removing tape aliases

You can remove aliases from tape drives, medium changers, or both, using the `storage unalias` command.

About this task

To use the following command, you need to access the nodeshell. You can access the nodeshell by using the `system node run` command. For more information about this command, see the man pages.

Step

1. To remove an alias from a tape drive or medium changer, enter the following command at the nodeshell:

   `storage unalias {`*`alias`*` | -a | -m | -t}`

   `alias` is the logical name of the tape drive or medium changer from which you want to remove the alias.

   `-a` removes all aliases.

   `-m` removes the aliases from all medium changers.

   `-t` removes the aliases from all tape drives.

Examples

`storage unalias st0`

`storage unalias mc80`

Related concepts

What tape aliasing is on page 19

Related tasks

Assigning tape aliases on page 25

Enabling or disabling tape reservations

You can control how Data ONTAP manages tape device reservations by using the `tape.reservations` option. By default, tape reservation is turned off.

About this task

Enabling the tape reservations option can cause problems if tape drives, medium changers, bridges, or libraries do not work properly. If tape commands report that the device is reserved when no other storage systems are using the device, this option should be disabled.

Step

1. To use either the SCSI Reserve/Release mechanism or SCSI Persistent Reservations or to disable tape reservations, enter the following command at the clustershell:
   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` selects the SCSI Reserve/Release mechanism.

   `persistent` selects SCSI Persistent Reservations.

   `off` disables tape reservations.

Related concepts

What tape reservations are on page 22

Commands for verifying tape library connections

You can view information about the path connected between a storage system and a tape library configuration attached to the storage system. You can use this information to verify the connection path to the tape library configuration or for troubleshooting issues related to the connection paths.

You can view the following tape library details to verify the tape library connections after adding or creating a new tape library or after restoring a failed path in a single-path or multipath access to a tape library. You can also use this information during troubleshooting of path-related errors or if the access to a tape library fails.

- Node to which the tape library is attached

- Device ID
- NDMP path
- Tape library name
- Target port and initiator port IDs
- Single-path or multipath access to a tape library for every target or FC initiator port
- Path-related data integrity details such as "Path Errors" and "Path Qual"
- LUN groups and LUN counts

If you want to...	Use this command...
Display information about a tape library in a cluster	`system node hardware tape library show`
Display information about tape library paths for every target port	`storage library path show` **Note:** If you want to display information related to "Path Errors" and "Path Qual", you must use the `-detail` option along with this command.
Display information about tape library paths for every initiator port	`storage library path show-by-initiator`
Display information about LUN groups and LUN counts in a tape library	`storage library config show`

For more information about these commands, refer to the man pages.

Understanding NDMP for FlexVol volumes

The Network Data Management Protocol (NDMP) is a standardized protocol for controlling backup, recovery, and other types of data transfer between primary and secondary storage devices, such as storage systems and tape libraries.

By enabling NDMP protocol support on a storage system, you enable that storage system to communicate with NDMP-enabled network-attached backup applications (also called *Data Management Applications* or *DMAs*), data servers, and tape servers participating in backup or recovery operations. All network communications occur over TCPIP or TCP/IPv6 network. NDMP also provides low-level control of tape drives and medium changers.

Starting with Data ONTAP 8.2, you can perform tape backup and restore operations in either node-scoped NDMP mode or Storage Virtual Machine (SVM)-scoped NDMP mode.

You must be aware of the considerations that you need to take into account while using NDMP, list of environment variables, and supported NDMP tape backup topologies. You can also enable or disable the enhanced DAR functionality. The two authentication methods supported by Data ONTAP for authenticating NDMP access to a storage system are: plaintext and challenge.

NDMP does not support backup and restore of Infinite Volumes.

About NDMP modes of operation

Starting with Data ONTAP 8.2, you can choose to perform tape backup and restore operations either at the node level as you have been doing until now or at the Storage Virtual Machine (SVM) level. To perform these operations successfully at the SVM level, NDMP service must be enabled on the SVM.

If you upgrade from Data ONTAP 8.1 to Data ONTAP 8.2, NDMP continues to follow node-scoped behavior. You must explicitly disable node-scoped NDMP mode to perform tape backup and restore operations in the SVM-scoped NDMP mode.

If you install a new Data ONTAP 8.2 cluster, NDMP is in the SVM-scoped NDMP mode by default. To perform tape backup and restore operations in the node-scoped NDMP mode, you must explicitly enable the node-scoped NDMP mode.

Related concepts

Managing node-scoped NDMP mode for FlexVol volumes on page 45
Managing SVM-scoped NDMP mode for FlexVol volumes on page 47

Related references

Commands for managing node-scoped NDMP mode on page 45

What node-scoped NDMP mode is

In the node-scoped NDMP mode, you can perform tape backup and restore operations at the node level. If you upgrade from 8.1 to 8.2, NDMP continues to follow the node-scoped behavior.

In this mode, you can perform tape backup and restore operations on a node that owns the volume. To perform these operations, you must establish NDMP control connections on a LIF hosted on the node that owns the volume or tape devices.

Related concepts

Managing node-scoped NDMP mode for FlexVol volumes on page 45

What SVM-scoped NDMP mode is

Starting with Data ONTAP 8.2, you can perform tape backup and restore operations at the Storage Virtual Machine (SVM) level successfully if the NDMP service is enabled on the SVM. You can back up and restore all volumes hosted across different nodes in an SVM of a cluster if the backup application supports the CAB extension.

An NDMP control connection can be established on different LIF types. In the SVM-scoped NDMP mode, these LIFs belong to either the data SVM or admin SVM. Data LIF belongs to the data SVM and the intercluster LIF, node-management LIF, and cluster-management LIF belong to the admin SVM. The NDMP control connection can be established on a LIF only if the NDMP service is enabled on the SVM that owns this LIF.

In the SVM context, the availability of volumes and tape devices for backup and restore operations depends upon the LIF type on which the NDMP control connection is established and the status of the CAB extension. If your backup application supports the CAB extension and a volume and tape device share the same affinity, then the backup application can perform a local backup or restore operation instead of a three-way backup or restore operation.

Related concepts

Managing SVM-scoped NDMP mode for FlexVol volumes on page 47

Considerations when using NDMP

You have to take into account a list of considerations when starting the NDMP service on your storage system.

- NDMP services can generate file history data at the request of NDMP backup applications.
  File history is used by backup applications to enable optimized recovery of selected subsets of data from a backup image. File history generation and processing might be time-consuming and CPU-intensive for both the storage system and the backup application.

If your data protection needs are limited to disaster recovery, where the entire backup image will be recovered, you can disable file history generation to reduce backup time. See your backup application documentation to determine if it is possible to disable NDMP file history generation.

- Firewall policy for NDMP is enabled by default on all LIF types.

  For information about managing firewall service and policies, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.
- In the node-scoped NDMP mode, to back up a FlexVol volume you must use the backup application to initiate a backup on a node that owns the volume.

  However, you cannot back up a node root volume.
- You can perform NDMP backup from any LIF as permitted by the firewall policies. If you use a data LIF, you must select one that is not configured for failover. If a data LIF fails over during an NDMP operation, the NDMP operation fails and must be reexecuted.
- In the node-scoped NDMP mode, NDMP data connection uses the same LIF as the NDMP control connection.
- NDMP backup path is of the format `/vserver_name/volume_name/path_name`, where `path_name` is the path of the directory, file, or Snapshot copy.
- When using `ndmpcopy` command for transferring data between a storage system running Data ONTAP operating in 7-Mode and a storage system running clustered Data ONTAP:
  - The `ndmpcopy` command must be initiated from a storage system running Data ONTAP operating in 7-Mode
  - In the node-scoped mode, the destination IP address is the address of a LIF on the node on which the target volume is located
  - Destination path is of the format `/vserver_name/volume_name`

  Note: You should not use the `ndmpcopy` command for restoring a LUN between a storage system running Data ONTAP operating in 7-Mode and a storage system running clustered Data ONTAP because the LUN is restored as a file on the destination storage system.

  For the syntax and examples of the `ndmpcopy` command, see the *Data Protection Tape Backup and Recovery Guide for 7-Mode*.
- When a SnapMirror destination is backed up to tape, only the data on the volume is backed up.

  The SnapMirror relationships and the associated metadata are not backed up to tape. Therefore, during restore, only the data on that volume is restored and the associated SnapMirror relationships are not restored.

Related concepts

Tape backup and restore between Data ONTAP operating in 7-Mode and clustered Data ONTAP on page 60

What environment variables do

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system.

For example, if a user specifies that a backup application should back up `/vserver1/vol1/dir1`, the backup application sets the FILESYSTEM environment variable to `/vserver1/vol1/dir1`. Similarly, if a user specifies that a backup should be a level 1 backup, the backup application sets the LEVEL environment variable to 1 (one).

Note: The setting and examining of environment variables are typically transparent to backup administrators; that is, the backup application sets them automatically.

A backup administrator rarely specifies environment variables; however, you might want to change the value of an environment variable from that set by the backup application to characterize or work around a functional or performance problem. For example, an administrator might want to temporarily disable file history generation to determine if the backup application's processing of file history information is contributing to performance issues or functional problems.

Many backup applications provide a means to override or modify environment variables or to specify additional environment variables. For information, see your backup application documentation.

Environment variables supported by Data ONTAP

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system. Data ONTAP supports environment variables, which have an associated default value. However, you can manually modify these default values.

If you manually modify the values set by the backup application, the application might behave unpredictably. This is because the backup or restore operations might not be doing what the backup application expected them to do. But in some cases, judicious modification might help in identifying or working around problems.

The following table contains descriptions of what the environment variables supported by Data ONTAP do if they are used:

Note: In most cases, variables that have `Y` or `N` values also accept `T` or `F` values, respectively.

Environment variable	Valid values	Default	Description
ACL_START	*return_only*	none	Created by the backup operation, the ACL_START variable is an offset value used by a direct access restore or restartable NDMP backup operation. The offset value is the byte offset in the dump file where the ACL data (Pass V) begins and is returned at the end of a backup. For a direct access restore operation to correctly restore backed up data, the ACL_START value must be passed to the restore operation when it begins. An NDMP restartable backup operation uses the ACL_START value to tell the backup application where the nonrestartable portion of the backup stream begins.
BASE_DATE	`0`,`-1`, or *DUMP_DATE* value	`-1`	Specifies the start date for incremental backups. When set to -1, the BASE_DATE incremental specifier is disabled. When set to 0 on a level 0 backup, incremental backups are enabled. Subsequent to the initial backup, the value of the DUMP_DATE variable from the previous incremental backup is assigned to the BASE_DATE variable. These variables are an alternative to the LEVEL/UPDATE based incremental backups.
DEBUG	`Y` or `N`	`N`	Specifies that debugging information is printed.

Environment variable	Valid values	Default	Description
DIRECT	`Y` or `N`	`N`	Specifies that a restore should fast-forward directly to the location on the tape where the file data resides instead of scanning the entire tape. For direct access recovery to work, the backup application must provide positioning information. If this variable is set to Y, the backup application will specify the file or directory names and the positioning information.
DMP_NAME	*`string`*	none	Specifies the name for a multiple subtree backup. This variable is mandatory for multiple subtree backups.
DUMP_DATE	*`return_value`*	none	You do not change this variable directly. It is created by the backup if the BASE_DATE variable is set to a value other than -1. The DUMP_DATE variable is derived by prepending the 32-bit level value to a 32-bit time value computed by the dump software. The level is incremented from the last level value passed into the BASE_DATE variable. The resulting value is used as the BASE_DATE value on a subsequent incremental backup.

Environment variable	Valid values	Default	Description
ENHANCED_DAR_ENABLED	`Y` or `N`	`N`	Specifies if enhanced DAR functionality is instantiated. Enhanced DAR functionality supports directory DAR, and DAR of files with NT Streams. It provides performance improvements. Enhanced DAR during restore is possible only if the following conditions are met: • Data ONTAP 8.0 or later supports enhanced DAR • File history is enabled (HIST=Y) during the backup • The `ndmpd.offset_map.enable` option is set to `on` • ENHANCED_DAR_ENABLED variable is set to "Y" during restore

Environment variable	Valid values	Default	Description
EXCLUDE	*pattern_string*	none	Specifies files or directories that are excluded when backing up data. The exclude list is a comma-separated list of file or directory names. If the name of a file or directory matches one of the names in the list, it is excluded from the backup. The following are rules for specifying names in the exclude list: • The exact name of the file or directory must be used. • An asterisk (*) is a wildcard character. The asterisk must be either the first or the last character of the string. Each string can have up to two asterisks. • A comma in a file or directory name must be preceded with a backslash. • The exclude list can contain up to 32 names. **Note:** Files or directories specified to be excluded for backup are not excluded if you set the NON_QUOTA_TREE to `Y` simultaneously.
EXTRACT	`Y`, `N`, or `E`	`N`	Specifies that subtrees of a backed-up data set are to be restored. The backup application specifies the names of the subtrees to be extracted. If a file specified matches a directory whose contents were backed up, the directory is recursively extracted. To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to `E`.

Environment variable	Valid values	Default	Description
EXTRACT_ACL	`Y` or `N`	`Y`	Specifies that ACLs from the backed up file are restored on a restore operation. The default is to restore ACLs when restoring data, except for DARs (DIRECT=Y).
FILESYSTEM	*`string`*	none	Specifies the path name of the root of the data that is being backed up.
FORCE	`Y` or `N`	`N`	Determines if the restore operation must check for volume space and inode availability on the destination volume. Setting this variable to `Y` causes the restore operation to skip checks for volume space and inode availability on the destination path. If there is not enough volume space or inodes available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when there is no more volume space or inodes left.
HIST	`Y` or `N`	`N`	Specifies that file history information is sent to the backup application. Most commercial backup applications set the HIST variable to Y. If you want to increase the speed of a backup operation, or you want to troubleshoot a problem with the file history collection, you can set this variable to N. **Note:** You should not set the HIST variable to Y if the backup application does not support file history.

Environment variable	Valid values	Default	Description
IGNORE_CTIME	`Y` or `N`	`N`	Specifies that a file is not incrementally backed up if only its ctime value has changed since the previous incremental backup. Some applications, such as virus scanning software, change the ctime value of a file within the inode, even though the file or its attributes have not changed. As a result, an incremental backup might back up files which have not changed. The IGNORE_CTIME variable should be specified only if incremental backups are taking an unacceptable amount of time or space because the ctime value was modified.
IGNORE_QTREES	`Y` or `N`	`N`	Specifies that the restore operation does not restore qtree information from backed up qtrees.
LEVEL	`0-9`	`0`	Specifies the backup level. Level 0 copies the entire data set. Incremental backup levels, specified by values above 0, copy all files new or modified since the last incremental backup. For example, a level 1 backs up new or modified files since the level 0 backup, a level 2 backs up new or modified files since the level 1 backup, and so on.
LIST	`Y` or `N`	`N`	Lists the backed-up file names and inode numbers without actually restoring the data.
LIST_QTREES	`Y` or `N`	`N`	Lists the backed-up qtrees without actually restoring the data.

Environment variable	Valid values	Default	Description
MULTI_SUBTREE_ NAMES	*string*	none	Specifies that the backup is a multiple subtree backup. Multiple subtrees are specified in the string which is a newline-separated, null-terminated list of subtree names. Subtrees are specified by path names relative to their common root directory, which must be specified as the last element of the list. If you use this variable, you must also use the DMP_NAME variable.
NDMP_UNICODE_ FH	`Y` or `N`	`N`	Specifies that a Unicode name is included in addition to the NFS name of the file in the file history information. This option is not used by most backup applications and should not be set unless the backup application is designed to receive these additional file names. The HIST variable must also be set.
NDMP_VERSION	*return_only*	none	You should not modify the NDMP_VERSION variable. Created by the backup operation, the NDMP_VERSION variable returns the NDMP version. Data ONTAP sets the NDMP_VERSION variable during a backup for internal use and to pass to a backup application for informational purposes. The NDMP version of an NDMP session is not set with this variable.
NO_ACLS	`Y` or `N`	`N`	Specifies that ACLs not be copied when backing up data.

Environment variable	Valid values	Default	Description
NON_QUOTA_TREE	`Y` or `N`	`N`	Specifies that files and directories in qtrees be ignored when backing up data. When set to `Y`, items in qtrees in the data set specified by the FILESYSTEM variable are not backed up. This variable has an effect only if the FILESYSTEM variable specifies an entire volume. The NON_QUOTA_TREE variable only works on a level-0 backup and does not work if the MULTI_SUBTREE_NAMES variable is specified. **Note:** Files or directories specified to be excluded for backup are not excluded if you set the NON_QUOTA_TREE to `Y` simultaneously.
NOWRITE	`Y` or `N`	`N`	Specifies that the restore operation not write data to the disk. This variable is used for debugging.
PATHNAME_SEPARATOR	*`return_value`*	none	Specifies the pathname separator character. This character depends upon the file system being backed up. For Data ONTAP, the character "/" is assigned to this variable. NDMP server sets this variable prior to starting a tape backup operation.

Environment variable	Valid values	Default	Description
RECURSIVE	`Y` or `N`	`Y`	Specifies that directory entries during a DAR restore be expanded. The DIRECT and ENHANCED_DAR_ENABLED environment variables must be enabled (set to `Y`) as well. If the RECURSIVE variable is disabled (set to `N`), only the permissions and ACLs for all the directories in the original source path are restored from tape, not the contents of the directories. If the RECURSIVE variable is `N` or the RECOVER_FULL_PATHS variable is `Y`, the recovery path must end with the original path. **Note:** If the RECURSIVE variable is disabled and if there are more than one recovery path, all the recovery paths must be contained within the longest of the recovery paths. Otherwise, an error message is displayed. For example, the following are valid recovery paths as all the recovery paths are within foo/dir1/deepdir/myfile: • /foo • /foo/dir • /foo/dir1/deepdir • /foo/dir1/deepdir/myfile The following are invalid recovery paths: • /foo • /foo/dir • /foo/dir1/myfile • /foo/dir2 • /foo/dir2/myfile

Environment variable	Valid values	Default	Description
RECOVER_FULL_PATHS	`Y` or `N`	`N`	Specifies that full recovery path will have their permissions and ACLs restored after the DAR. DIRECT and ENHANCED_DAR_ENABLED must be enabled (set to `Y`) as well. If RECOVER_FULL_PATHS is `Y`, recovery path must end with the original path. If directories already exist on the destination volume, their permissions and ACLs will not be restored from tape.
TYPE	`dump`	`dump`	Specifies the type of backup supported to perform tape backup and restore operations.
UPDATE	`Y` or `N`	`Y`	Updates the metadata information to enable LEVEL based incremental backup.
VERBOSE	`Y` or `N`	`N`	Increases the log messages while performing a tape backup or restore operation.

Common NDMP tape backup topologies

NDMP supports a number of topologies and configurations between backup applications and storage systems or other NDMP servers providing data (file systems) and tape services.

Storage system-to-local-tape

In the simplest configuration, a backup application backs up data from a storage system to a tape subsystem attached to the storage system. The NDMP control connection exists across the network boundary. The NDMP data connection that exists within the storage system between the data and tape services is called an NDMP local configuration.

Storage system-to-tape attached to another storage system

A backup application can also back up data from a storage system to a tape library (a medium changer with one or more tape drives) attached to another storage system. In this case, the NDMP data connection between the data and tape services is provided by a TCP or TCP/IPv6 network connection. This is called an NDMP three-way storage system-to-storage system configuration.

Storage system-to-network-attached tape library

NDMP-enabled tape libraries provide a variation of the three-way configuration. In this case, the tape library attaches directly to the TCP/IP network and communicates with the backup application and the storage system through an internal NDMP server.

Storage system-to-data server-to-tape or data server-to-storage system-to-tape

NDMP also supports storage system-to-data-server and data-server-to-storage system three-way configurations, although these variants are less widely deployed. Storage system-to-server allows storage system data to be backed up to a tape library attached to the backup application host or to another data server system. The server-to-storage system configuration allows server data to be backed up to a storage system-attached tape library.

Supported NDMP authentication methods

You can specify an authentication method to allow NDMP connection requests. Data ONTAP supports two methods for authenticating NDMP access to a storage system: plaintext and challenge.

In node-scoped NDMP mode, both challenge and plaintext are enabled by default. However, you cannot disable challenge. You can enable and disable plaintext. In the plaintext authentication method, the login password is transmitted as clear text.

In the Storage Virtual Machine (SVM)-scoped NDMP mode, by default the authentication method is challenge. Unlike the node-scoped NDMP mode, in this mode you can enable and disable both plaintext and challenge authentication methods.

Related concepts

User authentication in a node-scoped NDMP mode on page 46
User authentication in the SVM-scoped NDMP mode on page 52

NDMP extensions supported by Data ONTAP

NDMP v4 provides a mechanism for creating NDMP v4 protocol extensions without requiring modifications to the core NDMP v4 protocol.

The following are the NDMP v4 extensions supported by Data ONTAP:

- CAB (Cluster Aware Backup)

  Note: This extension is supported only in the Storage Virtual Machine (SVM)-scoped NDMP mode.

- CAE (Connection Address Extension) for IPv6 support

What enhanced DAR functionality is

You can use the enhanced direct access recovery (DAR) functionality for directory DAR and DAR of files and NT streams. By default, enhanced DAR functionality is enabled.

Enabling enhanced DAR functionality might impact the backup performance because an offset map has to be created and written onto tape. You can enable or disable enhanced DAR in both the node-scoped and Storage Virtual Machine (SVM)-scoped NDMP modes.

Scalability limits for NDMP sessions

You must be aware of the maximum number of NDMP sessions that can be established simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

System memory of a storage system	Maximum number of NDMP sessions
Less than 16 GB	8
Greater than or equal to 16 GB but less than 24 GB	20
Greater than or equal to 24 GB	36

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

Managing node-scoped NDMP mode for FlexVol volumes

You can manage NDMP at a node level by using NDMP options and commands. You can modify the NDMP `options` by using the options command. For more information about this command, see the man pages. You must use NDMP specific credentials to access a storage system to perform tape backup and restore operations.

Related concepts

What node-scoped NDMP mode is on page 30

Related references

Commands for managing node-scoped NDMP mode on page 45

Commands for managing node-scoped NDMP mode

You can use the `system services ndmp` commands to manage NDMP at a node level.

You can use the following NDMP commands only at the advanced privilege level:

- `system services ndmp terminate`
- `system services ndmp start`
- `system services ndmp stop`
- `system services ndmp log start`
- `system services ndmp log stop`

If you want to...	Use this command...
Enable NDMP service	`system services ndmp on`
Disable NDMP service	`system services ndmp off`
Display NDMP configuration	`system services ndmp show`
Modify NDMP configuration	`system services ndmp modify`
Display default NDMP version	`system services ndmp version`
Display all NDMP sessions	`system services ndmp status`
Display detailed information about all NDMP sessions	`system services ndmp probe`

If you want to...	Use this command...
Terminate all NDMP sessions	`system services ndmp kill-all`
Change the NDMP password	`system services ndmp password`
Enable node-scoped NDMP mode	`system services ndmp node-scope-mode on`
Disable node-scoped NDMP mode	`system services ndmp node-scope-mode off`
Display node-scoped NDMP mode status	`system services ndmp node-scope-mode status`
Forcefully terminate all NDMP sessions	`system services ndmp terminate`
Start the NDMP service daemon	`system services ndmp start`
Stop the NDMP service daemon	`system services ndmp stop`
Start logging for the specified NDMP session	`system services ndmp log start`
Stop logging for the specified NDMP session	`system services ndmp log stop`

For more information about these commands, see the man pages for the `system services ndmp` commands.

User authentication in a node-scoped NDMP mode

In the node-scoped NDMP mode, you must use NDMP specific credentials to access a storage system in order to perform tape backup and restore operations.

The default user ID is “root”. Before using NDMP on a node, you must ensure that you change the default NDMP password associated with the NDMP user. You can also change the default NDMP user ID.

Related references

Commands for managing node-scoped NDMP mode on page 45

Managing SVM-scoped NDMP mode for FlexVol volumes

You can manage NDMP on a per SVM basis by using the NDMP options and commands. You can modify the NDMP options by using the `vserver services ndmp modify` command. For more information about this command, see the man pages. In the SVM-scoped NDMP mode, user authentication is integrated with the role-based access control mechanism.

You can add NDMP in the allowed or disallowed protocols list by using the `vserver modify` command. By default, NDMP is in the allowed protocols list. If NDMP is added to the disallowed protocols list, NDMP sessions cannot be established. For more information about the allowed and disallowed protocols list, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

You can control the LIF type on which an NDMP data connection is established by using the `-preferred-interface-role` option. During an NDMP data connection establishment, NDMP chooses an IP address that belongs to the LIF type as specified by this option. If the IP addresses do not belong to any of these LIF types, then the NDMP data connection cannot be established. For more information about the `-preferred-interface-role` option, see the man pages.

Related concepts

What Cluster Aware Backup extension does on page 49
What SVM-scoped NDMP mode is on page 30

Related references

Commands for managing SVM-scoped NDMP mode on page 48

Related information

Documentation on the N series support website: www.ibm.com/storage/support/nseries

Commands for managing SVM-scoped NDMP mode

You can use the `vserver services ndmp` commands to manage NDMP per Storage Virtual Machine (SVM, formerly known as Vserver) basis.

If you want to...	Use this command...
Enable NDMP service	`vserver services ndmp on` **Note:** You must ensure that NDMP service is always enabled on all nodes in a cluster. You can enable NDMP service on a node by using the `system services ndmp on` command. By default, NDMP service is always enabled on a node.
Disable NDMP service	`vserver services ndmp off`
Display NDMP configuration	`vserver services ndmp show`
Modify NDMP configuration	`vserver services ndmp modify`
Display default NDMP version	`vserver services ndmp version`
Display all NDMP sessions	`vserver services ndmp status`
Display detailed information about all NDMP sessions	`vserver services ndmp probe`
Terminate a specified NDMP session	`vserver services ndmp kill`
Terminate all NDMP sessions	`vserver services ndmp kill-all`
Generate the NDMP password	`vserver services ndmp generate-password`
Start logging for the specified NDMP session	`vserver services ndmp log start` **Note:** This command is available at the advanced privilege level.
Stop logging for the specified NDMP session	`vserver services ndmp log stop` **Note:** This command is available at the advanced privilege level.

For more information about these commands, see the man pages for the `vserver services ndmp` commands.

What Cluster Aware Backup extension does

CAB (Cluster Aware Backup) is an NDMP v4 protocol extension. This extension enables the NDMP server to establish a data connection on a node that owns a volume. This also enables the backup application to determine if volumes and tape devices are located on the same node in a cluster.

To enable the NDMP server to identify the node that owns a volume and to establish a data connection on such a node, the backup application must support the CAB extension. CAB extension requires the backup application to inform the NDMP server about the volume to be backed up or restored prior to establishing the data connection. This allows the NDMP server to determine the node that hosts the volume and appropriately establish the data connection.

With the CAB extension supported by the backup application, the NDMP server provides affinity information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and tape device are located on the same node in a cluster.

Availability of volumes and tape devices for backup and restore on different LIF types

You can configure a backup application to establish an NDMP control connection on any of the LIF types in a cluster. In the Storage Virtual Machine (SVM)-scoped NDMP mode, you can determine the availability of volumes and tape devices for backup and restore operations depending upon these LIF types and the status of the CAB extension.

The following tables show the availability of volumes and tape devices for NDMP control connection LIF types and the status of the CAB extension:

Availability of volumes and tape devices when CAB extension is not supported by the backup application

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	Only volumes that belong to the SVM hosted by a node that hosts the data LIF	None

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Cluster-management LIF	All volumes hosted by a node that hosts the cluster-management LIF	None
Intercluster LIF	All volumes hosted by a node that hosts the intercluster LIF	Tape devices connected to the node hosting the intercluster LIF

Availability of volumes and tape devices when CAB extension is supported by the backup application

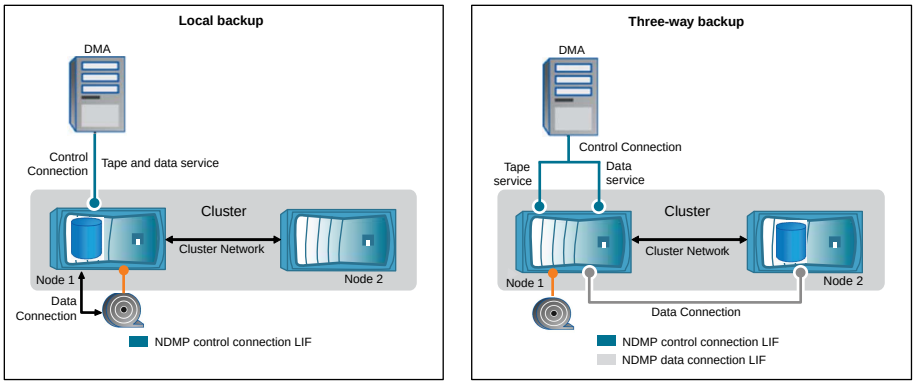
NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM that hosts the data LIF	None
Cluster-management LIF	All volumes in the cluster	All tape devices in the cluster
Intercluster LIF	All volumes in the cluster	All tape devices in the cluster

What affinity information is

With the backup application being CAB aware, the NDMP server provides unique location information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and a tape device share the same affinity.

If the NDMP control connection is established on a node management LIF, cluster management LIF, or an intercluster LIF, the backup application can use the affinity information to determine if a volume and tape device are located on the same node and then perform either a local or a three-way backup or restore operation. If the NDMP control connection is established on a data LIF, then the backup application always performs a three-way backup.

Local NDMP backup and Three-way NDMP backup



Using the affinity information about volumes and tape devices, the DMA (backup application) performs a local NDMP backup on the volume and tape device located on Node 1 in the cluster. If the volume moves from Node 1 to Node 2, affinity information about the volume and tape device changes. Hence, for a subsequent backup the DMA performs a three-way NDMP backup operation. This ensures continuity of the backup policy for the volume irrespective of the node to which the volume is moved to.

Related concepts

What Cluster Aware Backup extension does on page 49

NDMP data connection types

In the Storage Virtual Machine (SVM)-scoped NDMP mode, the supported NDMP data connection types depend on the NDMP control connection LIF type and the status of the CAB extension. This NDMP data connection type indicates whether you can perform a local or a three-way NDMP backup or restore operation.

You can perform a three-way NDMP backup or restore operation over a TCP or TCP/IPv6 network. The following tables show the NDMP data connection types based on the NDMP control connection LIF type and the status of the CAB extension.

NDMP data connection type when CAB extension is not supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	TCP, TCP/IPv6

NDMP control connection LIF type	NDMP data connection type
Intercluster LIF	LOCAL, TCP, TCP/IPv6

NDMP data connection type when CAB extension is supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	LOCAL, TCP, TCP/IPv6
Intercluster LIF	LOCAL, TCP, TCP/IPv6

Note: In Data ONTAP 8.2, you cannot configure intercluster LIFs with IPv6 addresses. For more information about IPv6 and intercluster LIF, see *Clustered Data ONTAP Network Management Guide*.

Related concepts

What Cluster Aware Backup extension does on page 49

User authentication in the SVM-scoped NDMP mode

In the Storage Virtual Machine (SVM)-scoped NDMP mode, NDMP user authentication is integrated with the role-based access control mechanism. In the SVM context, the NDMP user must belong to either the "vsadmin" or "vsadmin-backup" role. In a cluster context, the NDMP user must belong to either the "admin" or "backup" role.

In this mode, you must generate an NDMP password for a given user account, which is created through role-based access control mechanism. Cluster users in an admin or backup role can access a node-management LIF, cluster-management LIF, or an intercluster LIF. Users in a vsadmin-backup or vsadmin role can access only the data LIF. Hence, depending upon the role of a user, the availability of volumes and tape devices for backup and restore operations vary.

This mode also supports user authentication for NIS and LDAP users. Hence, NIS and LDAP users can access multiple SVMs with a common userid and password. However, NDMP authentication does not support Active Directory users.

In this mode, a user account must be associated with the SSH application and the authentication method "User password".

For more information about role-based access control, see *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Related references

Commands for managing SVM-scoped NDMP mode on page 48

Generating an NDMP-specific password for NDMP users

In the Storage Virtual Machine (SVM)-scoped NDMP mode, you must generate a password for a specific user ID. The generated password is based on the actual login password for the NDMP user. If the actual login password changes, you must generate the NDMP-specific password again.

Steps

1. Use the `vserver services ndmp generate-password` command to generate an NDMP-specific password.

   You can use this password in any current or future NDMP operation that requires password input.

   Note: From the Storage Virtual Machine (SVM, formerly known as Vserver) context, you can generate NDMP passwords for users belonging only to that SVM.

   Example

   The following example shows how to generate an NDMP-specific password for a user ID user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. If you change the password to your regular storage system account, repeat this procedure to obtain your new NDMP-specific password.

Understanding dump engine for FlexVol volumes

Dump is a Snapshot copy-based backup and recovery solution from Data ONTAP that helps you to back up files and directories from a Snapshot copy to a tape device and restore the backed up data to a storage system.

You can back up your file system data, such as directories, files, and their associated security settings to a tape device by using the dump backup. You can back up an entire volume, an entire qtree, or a subtree that is neither an entire volume nor an entire qtree.

Dump does not support backup and restore of Infinite Volumes.

You can perform a dump backup or restore by using NDMP-compliant backup applications.

When you perform a dump backup, you can specify the Snapshot copy to be used for a backup. If you do not specify a Snapshot copy for the backup, the dump engine creates a Snapshot copy for the backup. After the backup operation is completed, the dump engine deletes this Snapshot copy.

You can perform level-0, incremental, or differential backups to tape by using the dump engine.

Note: After reverting to Data ONTAP 8.1.x, to perform an incremental backup operation you must first perform a baseline backup operation.

How a dump backup works

A dump backup writes file system data from disk to tape using a predefined process.

You can back up a volume, a qtree, or a subtree that is neither an entire volume nor an entire qtree.

The following table describes the process that Data ONTAP uses to back up the object indicated by the dump path:

Stage	Action
1	For less than full volume or full qtree backups, Data ONTAP traverses directories to identify the files to be backed up. If you are backing up an entire volume or qtree, Data ONTAP combines this stage with Stage 2.
2	For a full volume or full qtree backup, Data ONTAP identifies the directories in the volumes or qtrees to be backed up.
3	Data ONTAP writes the directories to tape.
4	Data ONTAP writes the files to tape.
5	Data ONTAP writes the ACL information (if applicable) to tape.

The dump backup uses a Snapshot copy of your data for the backup. Therefore, you do not have to take the storage system or volume offline before initiating the backup.

The dump backup names each Snapshot copy it creates as `snapshot_for_backup.`*n*, where *n* is an integer starting at 0. Each time the dump backup creates a Snapshot copy, it increments the integer by 1. The storage system resets the integer to 0 when it is rebooted. After the backup operation is completed, the dump engine deletes this Snapshot copy.

When Data ONTAP performs multiple dump backups simultaneously, the dump engine creates multiple Snapshot copies. For example, if Data ONTAP is running two dump backups simultaneously, you find the following Snapshot copies in the volumes from which data is being backed up: `snapshot_for_backup.0` and `snapshot_for_backup.1`

Note: When you are backing up from a Snapshot copy, the dump engine does not create an additional Snapshot copy.

What the dump engine backs up

The dump engine can back up a file, directory, qtree, or an entire volume to a tape.

In addition to backing up data in files, the dump engine can back up the following information about each file, as applicable:

- UNIX GID, owner UID, and file permissions
- UNIX access, creation, and modification time
- File type
- File size
- DOS name, DOS attributes, and creation time
- Access Control Lists (ACLs) with 1024 Access Control Entries (ACEs)

  Note: If you restore ACLs backed up from storage systems running Data ONTAP 8.2 to storage systems running Data ONTAP 8.1.x and earlier that have an ACE limit lower than 1024, a default ACL is restored.
- Qtree information
- Junction paths

  Junction paths are backed up as symbolic links.
- LUN and LUN clones

  You can back up only an entire LUN object; you cannot back up a single file within the LUN object. Similarly, you can restore an entire LUN object but not a single file within the LUN.

  Note: The dump engine backs up LUN clones as independent LUNs.

When you back up a SnapVault secondary volume or a volume SnapMirror destination to tape, only the data on the volume is backed up. The associated metadata is not backed up. Therefore, when you try to restore the volume, only the data on that volume is restored. Information about the volume SnapMirror relationships is not available in the backup and therefore is not restored.

If you dump a file that has only Windows NT permissions and restore it to a UNIX-style qtree or volume, the file gets the default UNIX permissions for that qtree or volume.

If you dump a file that has only UNIX permissions and restore it to an NTFS-style qtree or volume, the file gets the default Windows permissions for that qtree or volume.

Other dumps and restores preserve permissions.

What increment chains are

An increment chain consists of a series of incremental backups of the same path. Because you can specify any level of backup at any time, you must understand increment chains to be able to perform backups and restores effectively. You can perform nine levels of incremental backup operations.

There are two types of increment chains:

- A consecutive increment chain is a sequence of incremental backups that starts with level 0 and is raised by 1 at each subsequent backup.
- A nonconsecutive increment chain is one in which incremental backups skip levels or have levels that are out of sequence, such as 0, 2, 3, 1, 4, or more commonly, 0, 1, 1, 1 or 0, 1, 2, 1, 2.

Incremental backups base themselves on the most recent lower-level backup. For example, the sequence of backup levels 0, 2, 3, 1, 4 gives two increment chains: 0, 2, 3 and 0, 1, 4. The following table explains the bases of the incremental backups:

Back-up order	Increment level	Increment chain	Base	Files backed up
1	0	Both	Files on the storage system	All files in the back up path
2	2	0, 2, 3	The level-0 backup	Files in the backup path created since the level-0 backup
3	3	0, 2, 3	The level-2 backup	Files in the backup path created since the level-2 backup
4	1	0, 1, 4	The level-0 backup, because that is the most recent level that is lower than the level-1 backup	Files in the backup path created since the level-0 backup, including files that are in the level-2 and level-3 backups

Back-up order	Increment level	Increment chain	Base	Files backed up
5	4	0, 1, 4	The level-1 backup, because it is both of a lower level and more recent than the level-0, level-2, or level-3 backups	Files created since the level-1 backup

What the blocking factor is

A tape block is 1,024 bytes of data. During a tape backup or restore, you can specify the number of tape blocks that are transferred in each read/write operation. This number is called the blocking factor.

You can use a blocking factor from 4 to 256. If you plan to restore a backup to a system other than the system that did the backup, the restore system must support the blocking factor that you used for the backup. For example, if you use a blocking factor of 128, the system on which you restore that backup must support a blocking factor of 128.

During an NDMP backup, the MOVER_RECORD_SIZE determines the blocking factor. Data ONTAP allows a maximum value of 256 KB for MOVER_RECORD_SIZE.

How a dump restore works

A dump restore writes file system data from tape to disk using a predefined process.

The process in the following table shows how the dump restore works:

Stage	Action
1	Data ONTAP catalogs the files that need to be extracted from the tape.
2	Data ONTAP creates directories and empty files.
3	Data ONTAP reads a file from tape, writes it to disk, and sets the permissions (including ACLs) on it.
4	Data ONTAP repeats stages 2 and 3 until all the specified files are copied from the tape.

What the dump engine restores

The dump engine enables you to recover all the information that you backed up.

Starting with Data ONTAP 8.2, you can restore data to an online mapped LUN. However, host applications cannot access this LUN until the restore operation is complete. After the restore operation is complete, the host cache of the LUN data should be flushed to guarantee coherency with the restored data.

The dump engine can recover the following data:

- Contents of files and directories
- UNIX file permissions
- ACLs

  If you restore a file that has only UNIX file permissions into an NTFS qtree or volume, the file has no Windows NT ACLs. The storage system uses only the UNIX file permissions on this file until you create a Windows NT ACL on it.

  Note: If you restore ACLs backed up from storage systems running Data ONTAP 8.2 to storage systems running Data ONTAP 8.1.x and earlier that have an ACE limit lower than 1024, a default ACL is restored.
- Qtree information

  Qtree information is used only if a qtree is restored to the root of a volume. Qtree information is not used if a qtree is restored to a lower directory, such as `/vs1/vol1/subdir/lowerdir`, and it ceases to be a qtree.
- All other file and directory attributes
- Windows NT streams
- LUNs
  - A LUN must be restored to a volume level or a qtree level for it to remain as a LUN. If it is restored to a directory, it is restored as a file because it does not contain any valid metadata.
  - A 7-Mode LUN is restored as a regular file on a clustered Data ONTAP volume.
- A 7-Mode volume can be restored to a clustered Data ONTAP volume.
- The destination volume for a restore operation might have files with mandatory or advisory locks. While performing restore operation to such a destination volume, the dump engine ignores these locks.

Considerations before restoring data

You can restore the backed up data to its original path or to a different destination. If you are restoring the backed up data to a different destination, you must prepare the destination for the restore.

Before restoring data either to its original path or to a different destination, you must have the following information and meet the following requirements:

- The level of the restore
- The path into which you are restoring the data
- The blocking factor used during the backup
- If you are doing an incremental restore, all tapes must be in the backup chain.
- A tape drive that is available and compatible with the tape to be restored from.

Before restoring data to a different destination, you must perform the following operations:

- If you are restoring a volume, you must create a new volume.
- If you are restoring a qtree or a directory, you must rename or move files that are likely to have the same names as files you are restoring.

  Attention: If a restored file has the same name as an existing file, the existing file is overwritten by the restored file. However, the directories are not overwritten.

To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to E.

Required space on the destination storage system

You need about 100 MB more space on the destination storage system than the amount of data to be restored.

Attention: The restore operation command terminates if it runs out of space.

Scalability limits for dump backup and restore sessions

You must be aware of the maximum number of dump backup and restore sessions that can be performed simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

System memory of a storage system	Total number of dump backup and restore sessions
Less than 16 GB	4

System memory of a storage system	Total number of dump backup and restore sessions
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

Note: If you use `ndmpcopy` command to copy data within storage systems, two sessions are established: dump backup and dump restore.

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

Tape backup and restore between Data ONTAP operating in 7-Mode and clustered Data ONTAP

You can restore data backed up from a storage system operating in 7-Mode or running clustered Data ONTAP to a storage system either operating in 7-Mode or running clustered Data ONTAP.

The following tape backup and restore operations are supported between Data ONTAP operating in 7-Mode and clustered Data ONTAP:

- Backing up a 7-Mode volume to a tape drive connected to a storage system running clustered Data ONTAP
- Backing up a clustered Data ONTAP volume to a tape drive connected to a 7-Mode system
- Restoring backed up data of a 7-Mode volume from a tape drive connected to a storage system running clustered Data ONTAP
- Restoring backed up data of a clustered Data ONTAP volume from a tape drive connected to a 7-Mode system
- Restoring a 7-Mode volume to a clustered Data ONTAP volume

  Note: A 7-Mode LUN is restored as a regular file on a clustered Data ONTAP volume.
- Restoring a clustered Data ONTAP volume to a 7-Mode volume

  Note: A clustered Data ONTAP LUN is restored as a regular file on a 7-Mode volume.

How dump backs up data from a SnapVault secondary volume

You can perform tape backup operations on data that is mirrored on the SnapVault secondary volume. You can back up only the data that is mirrored on the SnapVault secondary volume to tape, but not the SnapVault relationship metadata.

When you break the data protection mirror relationship (`snapmirror break`) or when a SnapMirror resynchronization occurs, you must always perform a baseline backup.

For more information about SnapVault secondary volumes, see *Clustered Data ONTAP Data Protection Guide*

Related information

Documentation on the N series support website: www.ibm.com/storage/support/nseries

How dump works with SFO and ARL

Storage Failover (SFO) and Aggregate Relocate (ARL) allow an aggregate to be relocated from one node to another in a cluster. The `-override-vetoes` option determines the behavior of dump engine during an SFO or ARL operation.

When a dump backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated SFO or ARL operation is stopped. However, if the `–override-vetoes` option is set to `true` then the SFO or ARL operation is continued and the dump backup or restore operation is aborted. When an SFO or ARL operation is automatically initiated by the storage system, an active dump backup or restore operation is always aborted. Dump backup and restore operations are not restartable after SFO or ARL operations are complete.

The following table describes the behavior of dump backup and restore operations after the SFO and ARL operation:

If you are performing dump backup and restore operations in the...	**Then...**
Storage Virtual Machine (SVM)-scoped NDMP mode when CAB extension is supported by the backup application	You can continue performing incremental dump backup and restore operations without reconfiguring backup policies.

If you are performing dump backup and restore operations in the...	Then...
SVM-scoped NDMP mode when CAB extension is not supported by the backup application	You can continue performing incremental dump backup and restore operations if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Else, after the SFO and ARL operation, you must perform a baseline backup prior to performing the incremental backup operation. **Note:** For SFO operations, the LIF configured in the backup policy must migrate to the partner node. For more information about what LIFs can be migrated, see the *Clustered Data ONTAP Network Management Guide*.
Node-scoped NDMP mode	

For more information about the SFO operations, see the *Clustered Data ONTAP High-Availability Configuration Guide* and for more information about ARL operations, see the *Clustered Data ONTAP Physical Storage Management Guide*.

Related information

Documentation on the N series support website: www.ibm.com/storage/support/nseries

How dump works with volume move

Starting with Data ONTAP 8.2, tape backup and restore operations and volume move can run in parallel until the final cutover phase is attempted by the storage system. After this phase, new tape backup and restore operations are not allowed on the volume that is being moved. However, the current operations continue running until completion.

The following table describes the behavior of tape backup and restore operations after the volume move operation:

If you are performing tape backup and restore operations in the...	Then...
Storage Virtual Machine (SVM)-scoped NDMP mode when CAB extension is supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.

If you are performing tape backup and restore operations in the...	Then...
SVM-scoped NDMP mode when CAB extension is not supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Else, after the volume move, you must perform a baseline backup prior to performing the incremental backup operation. For more information about what LIFs can be migrated, see the *Clustered Data ONTAP Network Management Guide*.
Node-scoped NDMP mode	

Note: When a volume move occurs, if the volume belonging to a different SVM on the destination node has the same name as that of the moved volume, then you cannot perform incremental backup operations of the moved volume.

Related information

Documentation on the N series support website: www.ibm.com/storage/support/nseries

How dump works when volume access type changes

Whenever a SnapMirror destination volume or a SnapVault secondary volume changes state from read/write to read-only or from read-only to read/write, you must perform a baseline tape backup or restore operation.

SnapMirror destination and SnapVault secondary volumes are read-only volumes. If you perform tape backup and restore operations on such volumes, you must perform a baseline backup or restore operation whenever the volume changes state from read-only to read/write or read/write to read-only.

For more information about when a SnapMirror destination volume or a SnapVault secondary volume changes state, see the *Clustered Data ONTAP Data Protection Guide*.

Monitoring tape backup and restore operations for FlexVol volumes

You can view the event log files to monitor the tape backup and restore operations. Data ONTAP automatically logs significant dump and restore events and the times at which they occur in a log file named `backup` in the controller's `/etc/log/` directory. By default, event logging is set to `on`.

You might want to view event log files for the following reasons:

- To find out whether a nightly backup was successful
- To gather statistics on backup operations
- To use information contained in past event log files to help diagnose problems with dump and restore operations

Once every week, the event log files are rotated. The `/etc/log/backup` file is renamed to `/etc/log/backup.0`, the `/etc/log/backup.0` file is renamed to `/etc/log/backup.1`, and so on. The system saves the log files for up to six weeks; therefore, you can have up to seven message files (`/etc/log/backup.[0-5]` and the current `/etc/log/backup` file).

Accessing the event log files

You can access the event log files for tape backup and restore operations at the `/etc/log/` directory by using the `rdfile` command at the nodeshell. You can view these event log files to monitor tape backup and restore operations.

Steps

1. To access the nodeshell, enter the following command:

   `node run -node` *`node_name`*

   `node_name` is the name of the node.

2. To access the event log files for tape backup and restore operations, enter the following command:

   `rdfile /etc/log/backup`

   With additional configurations, you can also use a web browser to access these log files. For more information about accessing a node's log files by using a web browser, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

What the dump and restore event log message format is

For each dump and restore event, a message is written to the backup log file.

The format of the dump and restore event log message is as follows:

type timestamp identifier event (*event_info*)

The following list describes the fields in the event log message format:

- Each log message begins with one of the type indicators described in the following table:

Type	Description
log	Logging event
dmp	Dump event
rst	Restore event

- *timestamp* shows the date and time of the event.
- The *identifier* field for a dump event includes the dump path and the unique ID for the dump. The *identifier* field for a restore event uses only the restore destination path name as a unique identifier. Logging-related event messages do not include an *identifier* field.

What logging events are

The event field of a message that begins with a log specifies the beginning of a logging or the end of a logging.

It contains one of the events shown in the following table:

Event	Description
Start_Logging	Indicates the beginning of logging or that logging has been turned back on after being disabled.
Stop_Logging	Indicates that logging has been turned off.

What dump events are

The event field for a dump event contains an event type followed by event-specific information within parentheses.

The following table describes the events, their descriptions, and the related event information that might be recorded for a dump operation:

Event	Description	Event information
Start	NDMP dump is started	Dump level and the type of dump
End	Dumps completed successfully	Amount of data processed
Abort	The operation is cancelled	Amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name
Phase-change	A dump is entering a new processing phase	The new phase name
Error	A dump has encountered an unexpected event	Error message
Snapshot	A Snapshot copy is created or located	The name and time of the Snapshot copy
Base_dump	A base dump entry in the internal metafile has been located	The level and time of the base dump (for incremental dumps only)

What restore events are

The event field for a restore event contains an event type followed by event-specific information in parentheses.

The following table provides information about the events, their descriptions, and the related event information that can be recorded for a restore operation:

Event	Description	Event information
Start	NDMP restore is started	Restore level and the type of restore
End	Restores completed successfully	Number of files and amount of data processed
Abort	The operation is cancelled	Number of files and amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name

Event	Description	Event information
Phase-change	Restore is entering a new processing phase	The new phase name
Error	Restore encounters an unexpected event	Error message

Enabling or disabling event logging

You can turn the event logging on or off.

Step

1. To enable or disable event logging, enter the following command at the clustershell:

   `options -option-name backup.log.enable -option-value {on | off}`

   `on` turns event logging on.

   `off` turns event logging off.

   Note: Event logging is turned on by default.

Error messages for tape backup and restore of FlexVol volumes

You might encounter an error message when performing a dump backup or restore operation due to various reasons.

Backup and restore error messages

You might encounter an error message while performing a tape backup or restore.

Resource limitation: no available thread

Message	`Resource limitation: no available thread`
Cause	The maximum number of active local tape I/O threads is currently in use. You can have a maximum of 16 active local tape drives.
Corrective action	Wait for some tape jobs to finish before starting a new backup or restore job.

Tape reservation preempted

Message	`Tape reservation preempted`
Cause	The tape drive is in use by another operation or the tape has been closed prematurely.
Corrective action	Ensure that the tape drive is not in use by another operation and that the DMA application has not aborted the job and then retry.

Could not initialize media

Message	`Could not initialize media`
Cause	You might get this error for one of the following reasons: • The tape drive used for the backup is corrupt or damaged. • The tape does not contain the complete backup or is corrupt. • The maximum number of active local tape I/O threads is currently in use. You can have a maximum of 16 active local tape drives.
Corrective action	• If the tape drive is corrupt or damaged, retry the operation with a valid tape drive.

- If the tape does not contain the complete backup or is corrupt, you cannot perform the restore operation.
- If tape resources are not available, wait for some of the backup or restore jobs to finish and then retry the operation.

Too many active dumps/restores currently in progress

Message	`Too many active dumps/restores currently in progress`
Cause	A maximum number of backup and/or restore jobs are already running.
Corrective action	Retry the operation after some of the currently running jobs have finished.

Media error on tape write

Message	`Media error on tape write`
Cause	The tape used for the backup is corrupted.
Corrective action	Replace the tape and retry the backup job.

Tape write failed

Message	`Tape write failed`
Cause	The tape used for the backup is corrupted.
Corrective action	Replace the tape and retry the backup job.

Tape write failed - new tape encountered media error

Message	`Tape write failed - new tape encountered media error`
Cause	The tape used for the backup is corrupted.
Corrective action	Replace the tape and retry the backup.

Tape write failed - new tape is broken or write protected

Message	`Tape write failed - new tape is broken or write protected`
Cause	The tape used for the backup is corrupted or write-protected.
Corrective action	Replace the tape and retry the backup.

Tape write failed - new tape is already at the end of media

Message	`Tape write failed - new tape is already at the end of media`

Cause	There is not enough space on the tape to complete the backup.
Corrective action	Replace the tape and retry the backup.

Tape write error

Message	`Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning`
Cause	The tape capacity is insufficient to contain the backup data.
Corrective action	Use tapes with larger capacity and retry the backup job.

Media error on tape read

Message	`Media error on tape read`
Cause	The tape from which data is being restored is corrupted and might not contain the complete backup data.
Corrective action	If you are sure that the tape has the complete backup, retry the restore operation. If the tape does not contain the complete backup, you cannot perform the restore operation.

Tape read error

Message	`Tape read error`
Cause	The tape drive is damaged or the tape does not contain the complete backup.
Corrective action	If the tape drive is damaged, use another tape drive. If the tape does not contain the complete backup, you cannot restore the data.

Already at the end of tape

Message	`Already at the end of tape`
Cause	The tape does not contain any data or must be rewound.
Corrective action	If the tape does not contain data, use the tape that contains the backup and retry the restore job. Otherwise, rewind the tape and retry the restore job.

Tape record size is too small. Try a larger size.

Message	`Tape record size is too small. Try a larger size.`

Cause	The blocking factor specified for the restore operation is smaller than the blocking factor that was used during the backup.
Corrective action	Use the same blocking factor that was specified during the backup.

Tape record size should be block_size1 and not block_size2

Message	`Tape record size should be block_size1 and not block_size2`
Cause	The blocking factor specified for the local restore is incorrect.
Corrective action	Retry the restore job with *`block_size1`* as the blocking factor.

Tape record size must be in the range between 4KB and 256KB

Message	`Tape record size must be in the range between 4KB and 256KB`
Cause	The blocking factor specified for the backup or restore operation is not within the permitted range.
Corrective action	Specify a blocking factor in the range of 4 KB to 256 KB.

NDMP error messages

You might encounter an error message while performing a tape backup or restore using NDMP-enabled commercial backup applications.

Network communication error

Message	`Network communication error`
Cause	Communication to a remote tape in an NDMP three-way connection has failed.
Corrective action	Check the network connection to the remote mover.

Message from Read Socket: error_string

Message	`Message from Read Socket: error_string`
Cause	Restore communication from the remote tape in NDMP 3-way connection has errors.
Corrective action	Check the network connection to the remote mover.

Message from Write Dirnet: error_string

Message	`Message from Write Dirnet: error_string`

Cause	Backup communication to a remote tape in an NDMP three-way connection has an error.
Corrective action	Check the network connection to the remote mover.

Read Socket received EOF

Message	`Read Socket received EOF`
Cause	Attempt to communicate with a remote tape in an NDMP three-way connection has reached the End Of File mark. You might be attempting a three-way restore from a backup image with a larger block size.
Corrective action	Specify the correct block size and retry the restore operation.

ndmpd invalid version number: version_number

Message	`ndmpd invalid version number: version_number`
Cause	The NDMP version specified is not supported by the storage system.
Corrective action	Specify NDMP version 4.

ndmpd session session_ID not active

Message	`ndmpd session session_ID not active`
Cause	The NDMP session might not exist.
Corrective action	Use the `ndmpd status` command to view the active NDMP sessions.

Could not obtain vol ref for Volume volume_name

Message	`Could not obtain vol ref for Volume vol_name`
Cause	The volume reference could not be obtained because the volume might be in use by other operations.
Corrective action	Retry the operation later.

Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for ["IPv6"|"IPv4"] control connections

Message	`Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for ["IPv6"|"IPv4"] control connections`

Cause	In node-scoped NDMP mode, the NDMP data connection established must be of the same network address type (IPv4 or IPv6) as the NDMP control connection.
Corrective action	Contact your backup application vendor.

DATA LISTEN: CAB_DATA_CONN_PREPARE not sent or addr type mismatch

Message	`DATA LISTEN: CAB_DATA_CONN_PREPARE not sent or addr type mismatch`
Cause	The backup application has not negotiated the CAB extension, yet has sent the CAB message. Or, the backup application has negotiated the CAB extension, but sends the incorrect CAB message.
Corrective action	Disable the CAB extension using the backup application by contacting your backup application vendor.

DATA CONNECT: CAB_DATA_CONN_PREPARE not sent or addr type mismatch

Message	`DATA CONNECT: CAB_DATA_CONN_PREPARE not sent or addr type mismatch`
Cause	The backup application has not negotiated the CAB extension, yet has sent the CAB message. Or, the backup application has negotiated the CAB extension, but sends the incorrect CAB message.
Corrective action	Disable the CAB extension using the backup application by contacting your backup application vendor.

Error:show failed: Cannot get password for user '<username>'

Message	`Error: show failed: Cannot get password for user '<username>'`
Cause	Incomplete user account configuration for NDMP
Corrective action	Ensure that the user account is associated with the SSH access method and the authentication method is user password.

Dump error messages

You might encounter an error message while performing a tape backup or restore using the dump engine.

Destination volume is read-only

Message	`Destination volume is read-only`
Cause	The path to which the restore operation is attempted to is read-only.
Corrective action	Try restoring the data to a different location.

Destination qtree is read-only

Message	`Destination qtree is read-only`
Cause	The qtree to which the restore is attempted to is read-only.
Corrective action	Try restoring the data to a different location.

Dumps temporarily disabled on volume, try again

Message	`Dumps temporarily disabled on volume, try again`
Cause	Volume movement is in progress.
Corrective action	Wait for volume movement operation to complete and then perform the backup operation again.

No files were created

Message	`No files were created`
Cause	A directory DAR was attempted without enabling the enhanced DAR functionality.
Corrective action	Enable the enhanced DAR functionality and retry the DAR.

Restore of the file <file name> failed

Message	`Restore of the file` *`file name`* `failed`
Cause	When a DAR (Direct Access Recovery) of a file whose file name is the same as that of a LUN on the destination volume is performed, then the DAR fails.
Corrective action	Retry DAR of the file.

Truncation failed for src inode <inode number>...

Message	`Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.`
Cause	Inode of a file is deleted when the file is being restored.
Corrective action	Wait for the restore operation on a volume to complete before using that volume.

Unable to lock a snapshot needed by dump

Message	`Unable to lock a snapshot needed by dump`
Cause	The Snapshot copy specified for the backup is not available.
Corrective action	Retry the backup with a different Snapshot copy. Use the `snap list` command to see the list of available Snapshot copies.

Unable to locate bitmap files

Message	`Unable to locate bitmap files`
Cause	The bitmap files required for the backup operation might have been deleted. In this case, the backup cannot be restarted.
Corrective action	Perform the backup again.

Volume is temporarily in a transitional state

Message	`Volume is temporarily in a transitional state`
Cause	The volume being backed up is temporarily in an unmounted state.
Corrective action	Wait for some time and perform the backup again.

Copyright and trademark information

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP,

ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Index

R

S

T

V

NA 210-06391_A0, Printed in USA

SC27-6274-01