ONTAP® 9

Data Protection Tape Backup and Recovery Guide

January 2019 | 215-11155_G0
doccomments@netapp.com

Updated for ONTAP 9.5

NetApp®

Contents

Tape backup of FlexVol volumes

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

You can perform a dump or SMTape backup or restore by using NDMP-compliant backup applications. Only NDMP version 4 is supported.

Tape backup using dump

Dump is a Snapshot copy based backup in which your file system data is backed up to tape. The 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 not an entire volume or an entire qtree. Dump supports baseline, differential, and incremental backups.

Tape backup using SMTape

SMTape is a Snapshot copy based disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the qtree or subtree level. SMTape supports baseline, differential, and incremental backups.

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 the tasks that are involved in performing tape backup and restore operations. For detailed information about performing 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 on the NDMP mode in which you choose to perform the 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 on the NDMP mode in which you choose to perform the tape backup and restore operation.

   You can modify the NDMP options at the node level by using the `system services ndmp modify` 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.

   ONTAP supports both dump and SMTape engines 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 52

Related references

Common NDMP tape backup topologies on page 41

Use cases for choosing a tape backup engine

ONTAP supports two backup engines: SMTape and dump. You should be aware of the use cases for the SMTape and dump backup engines to help you choose the backup engine to perform tape backup and restore operations.

Dump can be used in the following cases:

- Direct Access Recovery (DAR) of files and directories
- Backup of a subset of subdirectories or files in a specific path
- Excluding specific files and directories during backups
- Preserving backup for long durations

SMTape can be used in the following cases:

- Disaster recovery solution
- Preserving deduplication savings and deduplication settings on the backed up data during a restore operation
- Backup of large volumes

Where to find information about Infinite Volume tape backup and restore

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

Infinite volumes management

Managing tape drives

You can verify tape library connections and view tape drive information before 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 managing tape drives, media changers, and tape drive operations

There are commands for viewing information about tape drives and media changers in a cluster, bringing a tape drive online and taking it offline, modifying the tape drive cartridge position, setting and clearing tape drive alias name, and resetting a tape drive. You can also view and reset tape drive statistics.

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

If you want to...	Use this command...
Bring a tape drive online	`storage tape online`
Clear an alias name for tape drive or media changer	`storage tape alias clear`
Enable or disable a tape trace operation for a tape drive	`storage tape trace`
Modify the tape drive cartridge position	`storage tape position`
Reset a tape drive	`storage tape reset` **Note:** This command is available only at the advanced privilege level.
Set an alias name for tape drive or media changer	`storage tape alias set`
Take a tape drive offline	`storage tape offline`
View information about all tape drives and media changers	`storage tape show`
View information about tape drives attached to the cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
View information about media changers attached to the cluster	`storage tape show-media-changer`
View error information about tape drives attached to the cluster	`storage tape show-errors`

If you want to...	Use this command...
View all ONTAP qualified and supported tape drives attached to each node in the cluster	`storage tape show-supported-status`
View aliases of all tape drives and media changers attached to each node in the cluster	`storage tape alias show`
Reset the statistics reading of a tape drive to zero	`storage stats tape zero` *`tape_name`* You must use this command at the nodeshell.
View tape drives supported by ONTAP	`storage show tape supported [-v]` You must use this command at the nodeshell. You can use the `-v` option to view more details about each tape drive.
View tape device statistics to understand tape performance and check usage pattern	`storage stats tape` *`tape_name`* You must use this command at the nodeshell.

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

Using a nonqualified tape drive

You can use a nonqualified tape drive on a storage system if it can emulate a qualified tape drive. It is then treated like a qualified tape drive. To use a nonqualified tape drive, you must first determine whether it emulates any of the qualified tape drives.

About this task

A nonqualified tape drive is one that is attached to the storage system, but not supported or recognized by ONTAP.

Steps

1. View the nonqualified tape drives attached to a storage system by using the `storage tape show-supported-status` command.

   #### Example

   The following command displays tape drives attached to the storage system and the support and qualification status of each tape drive. The nonqualified tape drives are also listed. "*`tape_drive_vendor_name`*" is a nonqualified tape drive attached to the storage system, but not supported by ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                Is
          Tape Drive            Supported  Support Status
          --------------------  ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Emulate the qualified tape drive.

NetApp Downloads: Tape Device Configuration Files

Related concepts

What qualified tape drives are on page 15

Assigning tape aliases

For easy device identification, you can assign tape aliases to a tape drive or medium changer. Aliases provide a correspondence between the logical names of backup devices and a name permanently assigned to the tape drive or medium changer.

Step

1. Assign an alias to a tape drive or medium changer by using the `storage tape alias set` command.

   For more information about this command, see the man pages.

   You can view the serial number (SN) information about the tape drives by using the `system node hardware tape drive show` command and about tape libraries by using the `system node hardware tape library show` commands.

Example

The following command sets an alias name to a tape drive with serial number SN[123456]L4 attached to the node, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3 -
mapping SN[123456]L4
```

Example

The following command sets an alias name to a media changer with serial number SN[65432] attached to the node, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1 -
mapping SN[65432]
```

Related concepts

What tape aliasing is on page 19

Related tasks

Removing tape aliases on page 12

Removing tape aliases

You can remove aliases by using the `storage tape alias clear` command when persistent aliases are no longer required for a tape drive or medium changer.

Step

1. Remove an alias from a tape drive or medium changer by using the `storage tape alias clear` command.

   For more information about this command, see the man pages.

Example

The following command removes the aliases of all tape drives by specifying the scope of the alias clear operation to **`tape`**:

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope
tape
```

After you finish

If you are performing a tape backup or restore operation using NDMP, then after you remove an alias from a tape drive or medium changer, you must assign a new alias name to the tape drive or medium changer to continue access to the tape device.

Related concepts

What tape aliasing is on page 19

Related tasks

Assigning tape aliases on page 12

Enabling or disabling tape reservations

You can control how 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 21

Commands for verifying tape library connections

You can view information about the connection path 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 while troubleshooting path-related errors or if 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...
View information about a tape library in a cluster	`system node hardware tape library show`
View path information for a tape library	`storage tape library path show`
View path information for a tape library for every initiator port	`storage tape library path show-by-initiator`
View connectivity information between a storage tape library and cluster	`storage tape library config show`

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

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 qualify tape drives for existing ONTAP releases by using the tape configuration file.

Related tasks

Using a nonqualified tape drive on page 11

Related references

Commands for managing tape drives, media changers, and tape drive operations on page 10
Commands for verifying tape library connections on page 13

Related information

NetApp Downloads: Tape Device Configuration Files

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 command, `storage tape show -device-names`; 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 command, `storage tape show -device-names`; 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 24 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.
`{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. You must 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.

You can download and view the tape configuration file from the NetApp Support Site.

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

NetApp Downloads: Tape Device Configuration Files

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, it looks for a vendor ID and product ID match between the information obtained during tape discovery and the information 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, ONTAP creates tape devices associated with the tape drive or tape library.

ONTAP detects tape drives and tape libraries and assigns logical numbers and tape devices to them. ONTAP detects the Fibre Channel, SAS, and parallel SCSI tape drives and libraries when they are connected to the interface ports. 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:

rewind_type `st` *alias_number compression_type*

rewind_type is the rewind type.

The following list describes the various rewind type values:

r

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

nr

ONTAP does not rewind the tape after it finishes writing the tape file. You must 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.

You must 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 ONTAP assigns to the tape drive. When ONTAP detects a new tape drive, 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.

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

ONTAP supports a maximum of 64 simultaneous tape drive connections, 16 medium changers, and 16 bridge or router devices for each storage system (per node) 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 58

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 ONTAP assigns to tape drives and tape libraries based on the SCSI-2/3 adapter or switch (specific location) they are connected to 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. 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. 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 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, 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 two paths from the storage system to access the tape drives in a tape library. If one path fails, the storage system can use the other paths to access the tape drives without having to immediately repair the failed path. This ensures that tape operations can be restarted.

You must consider the following 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.

- A maximum of two paths can be configured from the storage system to access the tape drives in a tape library.

- Multipath tape access supports load balancing. Load balancing is disabled by default.

In the following example, the storage system accesses LUN group 0 through two initiator paths: 0b and 0d. In both 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 tape 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 you add tape drives and libraries to storage systems

You can add tape drives and libraries to storage system dynamically (without taking the storage system 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 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 interface error recovery procedures, reservations can be lost. If this occurs, 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.

Transferring data using ndmpcopy

The ndmpcopy command transfers data between storage systems that support NDMP v4. You can perform both full and incremental data transfers. Incremental transfers are limited to a maximum of two levels (one full and up to two incremental backups). You can transfer full or partial volumes, qtrees, directories, or individual files.

About this task

You can run ndmpcopy at the command line of the source and destination storage systems, or a storage system that is neither the source nor the destination of the data transfer. You can also run ndmpcopy on a single storage system that is both the source and the destination of the data transfer.

You can use IPv4 or IPv6 addresses of the source and destination storage systems in the ndmpcopy command. The path format is */vserver_name/volume_name [path]*.

Steps

1. Enable NDMP service on the source and destination storage systems:

If you are performing data transfer at the source or destination in...	Use the following command...
SVM-scoped NDMP mode	**vserver services ndmp on** **Note:** For NDMP authentication in the admin SVM, the user account is admin and the user role is admin or backup. In the data SVM, the user account is vsadmin and the user role is vsadmin or vsadmin-backup role.
Node-scoped NDMP mode	**system services ndmp on**

2. Transfer data within a storage system or between storage systems using ndmpcopy command at the nodeshell:

   ndmpcopy [options]*source_IP*:*source_path* *destination_IP*:*destination_path* [-mcs {*inet*|*inet6*}][-mcd {*inet*|*inet6*}][-md {*inet*|*inet6*}]

   Note: DNS names are not supported in ndmpcopy. You must provide the IP address of the source and the destination. The loopback address (127.0.0.1) is not supported for the source IP address or the destination IP address.

   - The ndmpcopy command determines the address mode for control connections as follows:
     - The address mode for control connection corresponds to the IP address provided.
     - You can override these rules by using the -mcs and -mcd options.
   - If the source or the destination is the ONTAP system, then depending on the NDMP mode (node-scoped or SVM-scoped), use an IP address that allows access to the target volume.
   - *source_path* and *destination_path* are the absolute path names till the granular level of volume, qtree, directory or file.
   - -mcs specifies the preferred addressing mode for the control connection to the source storage system.
     inet indicates an IPv4 address mode and *inet6* indicates an IPv6 address mode.

- `-mcd` specifies the preferred addressing mode for the control connection to the destination storage system.
  `inet` indicates an IPv4 address mode and *`inet6`* indicates an IPv6 address mode.
- `-md` specifies the preferred addressing mode for data transfers between the source and the destination storage systems.
  `inet` indicates an IPv4 address mode and *`inet6`* indicates an IPv6 address mode.
  If you do not use the `-md` option in the `ndmpcopy` command, the addressing mode for the data connection is determined as follows:
  - If either of the addresses specified for the control connections is an IPv6 address, the address mode for the data connection is IPv6.
  - If both the addresses specified for the control connections are IPv4 addresses, the `ndmpcopy` command first attempts an IPv6 address mode for the data connection.
    If that fails, the command uses an IPv4 address mode.

Note: An IPv6 address, if specified, must be enclosed within square brackets.

Example

This sample command migrates data from a source path (*`source_path`*) to a destination path (*`destination_path`*).

```
>ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol> 192.0.2.131:/
<dst_svm>/<dst_vol>
```

Example

This sample command explicitly sets the control connections and the data connection to use IPv6 address mode:

```
>ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Options for the ndmpcopy command

You should understand the options available for the `ndmpcopy` command to successfully transfer data.

The following table lists the available options. For more information, see the `ndmpcopy` man pages available through the nodeshell.

Option	Description
`-sa` *username*:[*password*]	This option sets the source authentication user name and password for connecting to the source storage system. This is a mandatory option. For a user without admin privilege, you must specify the user's system-generated NDMP-specific password. The system-generated password is mandatory for both admin and non-admin users.
`-da` *username*:[*password*]	This option sets the destination authentication user name and password for connecting to the destination storage system. This is a mandatory option.
`-st` {**md5**|**text**}	This option sets the source authentication type to be used when connecting to the source storage system. This is a mandatory option and therefore the user should provide either the **text** or **md5** option.
`-dt` {**md5**|**text**}	This option sets the destination authentication type to be used when connecting to the destination storage system.
`-l`	This option sets the dump level used for the transfer to the specified value of level. Valid values are **0**, **1**, to **9**, where **0** indicates a full transfer and **1** to **9** specifies an incremental transfer. The default is **0**.
`-i`	This option enables the incremental transfer forever. It is mandatory to run a base-level `ndmpcopy` using the `-l` option with the **0** value before doing the first incremental transfer using the `-i` option.
`-d`	This option enables generation of ndmpcopy debug log messages. The ndmpcopy debug log files are located in the `/mroot/etc/log` root volume. The ndmpcopy debug log file names are in the `ndmpcopy.`*yyyymmdd* format.
`-f`	This option enables the forced mode. This mode enables system files to be overwritten in the `/etc` directory on the root of the 7-Mode volume.
`-h`	This option prints the help message.

Option	Description
`-p`	This option prompts you to enter the password for source and destination authorization. This password overrides the password specified for `-sa` and `-da` options. **Note:** You can use this option only when the command is running in an interactive console.
`-exclude`	This option excludes specified files or directories from the path specified for data transfer. The value can be a comma-separated list of directory or file names such as `*.pst` or `*.txt`.

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 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.

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 have 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 ONTAP for authenticating NDMP access to a storage system are: plaintext and challenge.

NDMP does not support backup and restore of Infinite Volumes.

Related concepts

Environment variables supported by ONTAP on page 29

About NDMP modes of operation

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 8.2 to Data ONTAP 8.3, the NDMP mode of operation used in 8.2 will continue to be retained post the upgrade from 8.2 to 8.3.

If you install a new cluster with Data ONTAP 8.2 or later, 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 44
Managing SVM-scoped NDMP mode for FlexVol volumes on page 46

Related references

Commands for managing node-scoped NDMP mode on page 44

What node-scoped NDMP mode is

In the node-scoped NDMP mode, you can perform tape backup and restore operations at the node level. The NDMP mode of operation used in Data ONTAP 8.2 will continue to be retained post the upgrade from 8.2 to 8.3.

In the node-scoped NDMP 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.

Note: This mode is deprecated and will be removed in a future major release.

Related concepts

Managing node-scoped NDMP mode for FlexVol volumes on page 44

What SVM-scoped NDMP mode is

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 the 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. The connection can be established on a LIF only if the NDMP service is enabled on the SVM that owns this LIF.

A data LIF belongs to the data SVM and the intercluster LIF, node-management LIF, and cluster-management LIF belong to the admin SVM.

In the SVM-scoped NDMP mode, the availability of volumes and tape devices for backup and restore operations depends on 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 the 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 46

Considerations when using NDMP

You must take into account a number of considerations when starting the NDMP service on your storage system.

- Each node supports a maximum of 16 concurrent backups, restores, or combination of the two using connected tape drives.
- 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.

  Note: SMTape does not support file history.

  If your data protection is configured for 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 whether it is possible to disable NDMP file history generation.
- Firewall policy for NDMP is enabled by default on all LIF types.
- In node-scoped NDMP mode, backing up a FlexVol volume requires that you 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 a LIF that is not configured for failover. If a data LIF fails over during an NDMP operation, the NDMP operation fails and must be run again.
- In node-scoped NDMP mode and storage virtual machine (SVM) scoped NDMP mode with no CAB extension support, the NDMP data connection uses the same LIF as the NDMP control connection.

- During LIF migration, ongoing backup and restore operations are disrupted.
  You must initiate the backup and restore operations after the LIF migration.
- The NDMP backup path is of the format */vserver_name/volume_name/path_name*.
  path_name is optional, and specifies the path of the directory, file, or Snapshot copy.
- When a SnapMirror destination is backed up to tape by using the dump engine, only the data in the volume is backed up.
  However, if a SnapMirror destination is backed up to tape using SMTape, then the metadata is also 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, but the associated SnapMirror relationships are not restored.

Related concepts

What Cluster Aware Backup extension does on page 47

Related information

ONTAP concepts
System administration

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 ONTAP

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system. 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 tables list the environment variables whose behavior is common to dump and SMTape and those variables that are supported only for dump and SMTape. These tables also contain descriptions of how the environment variables that are supported by ONTAP work if they are used:

Note: In most cases, variables that have the value, **`Y`** also accept **`T`** and **`N`** also accept **`F`**.

Environment variables supported for dump and SMTape

Environment variable	Valid values	Default	Description
DEBUG	**Y** or **N**	**N**	Specifies that debugging information is printed.
FILESYSTEM	*string*	**none**	Specifies the path name of the root of the data that is being backed up.
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. 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.
PATHNAME_SEPARATOR	*return_value*	**none**	Specifies the path name separator character. This character depends on the file system being backed up. For ONTAP, the character "/" is assigned to this variable. The NDMP server sets this variable before starting a tape backup operation.
TYPE	**dump** or **smtape**	**dump**	Specifies the type of backup supported to perform tape backup and restore operations.
VERBOSE	**Y** or **N**	**N**	Increases the log messages while performing a tape backup or restore operation.

Environment variables supported for dump

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 communicate to 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. After 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.
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 specifies the file or directory names and the positioning information.

Environment variable	Valid values	Default	Description
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.
ENHANCED_DAR_ENABLED	**Y** or **N**	**N**	Specifies whether enhanced DAR functionality is enabled. 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: • ONTAP 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 rules apply while specifying names in the exclude list: • The exact name of the file or directory must be used. • The asterisk (*), a wildcard character, 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 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**.
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).

Environment variable	Valid values	Default	Description
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 enough volume space or inodes are not 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 volume space or inodes are not available.
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 that 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. **Note:** The `NDMP dump` command sets `IGNORE_CTIME` to **`false`** by default. Setting it to **`true`** can result in the following data loss: **1.** If `IGNORE_CTIME` is set to true with a volume level incremental `ndmpcopy`, it results in the deleting of files, which are moved across qtrees on source. **2.** If `IGNORE_CTIME` is set to true during a volume level incremental dump, it results in the deleting of files, which are moved across qtrees on source during incremental restore. To avoid this problem, `IGNORE_CTIME` must be set to false during volume level `NDMP dumps` or `ndmpcopy`.
IGNORE_QTREES	**Y** or **N**	**N**	Specifies that the restore operation does not restore qtree information from backed-up qtrees.

Environment variable	Valid values	Default	Description
LEVEL	**0-31**	**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.
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.
NO_ACLS	**Y** or **N**	**N**	Specifies that ACLs must 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 must 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 NON_QUOTA_TREE to **Y** simultaneously.
NOWRITE	**Y** or **N**	**N**	Specifies that the restore operation must not write data to the disk. This variable is used for debugging.

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 set to **N** or the RECOVER_FULL_PATHS variable is set to **Y**, the recovery path must end with the original path. **Note:** If the RECURSIVE variable is disabled and if there is more than one recovery path, all of 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 because all of 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 the 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 set to **Y**, the 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.
UPDATE	**Y** or **N**	**Y**	Updates the metadata information to enable LEVEL based incremental backup.

Environment variables supported for SMTape

Environment variable	Valid values	Default	Description
BASE_DATE	*DUMP_DATE*	**-1**	Specifies the start date for incremental backups. *BASE_DATE* is a string representation of the reference Snapshot identifiers. Using the *BASE_DATE* string, SMTape locates the reference Snapshot copy. *BASE_DATE* is not required for baseline backups. For an incremental backup, the value of the *DUMP_DATE* variable from the previous baseline or incremental backup is assigned to the *BASE_DATE* variable. The backup application assigns the *DUMP_DATE* value from a previous SMTape baseline or incremental backup.

Environment variable	Valid values	Default	Description
DUMP_DATE	*return_value*	**none**	At the end of an SMTape backup, DUMP_DATE contains a string identifier that identifies the Snapshot copy used for that backup. This Snapshot copy could be used as the reference Snapshot copy for a subsequent incremental backup. The resulting value of DUMP_DATE is used as the BASE_DATE value for subsequent incremental backups.
SMTAPE_BACKUP_SET_ID	**string**	**none**	Identifies the sequence of incremental backups associated with the baseline backup. Backup set ID is a 128-bit unique ID that is generated during a baseline backup. The backup application assigns this ID as the input to the *SMTAPE_BACKUP_SET_ID* variable during an incremental backup.
SMTAPE_SNAPSHOT_NAME	Any valid Snapshot copy that is available in the volume	**Invalid**	When the SMTAPE_SNAPSHOT_NAME variable is set to a Snapshot copy, that Snapshot copy and its older Snapshot copies are backed up to tape. For incremental backup, this variable specifies incremental Snapshot copy. The BASE_DATE variable provides the baseline Snapshot copy.
SMTAPE_DELETE_SNAPSHOT	**Y** or **N**	**N**	For a Snapshot copy created automatically by SMTape, when the SMTAPE_DELETE_SNAPSHOT variable is set to **Y**, then after the backup operation is complete, SMTape deletes this Snapshot copy. However, a Snapshot copy created by the backup application will not be deleted.

Environment variable	Valid values	Default	Description
SMTAPE_BREAK_MIRROR	**Y** or **N**	**N**	When the SMTAPE_BREAK_MIRROR variable is set to **Y**, the volume of type **DP** is changed to a **RW** volume after a successful restore.

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. 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 45
User authentication in the SVM-scoped NDMP mode on page 50

NDMP extensions supported by ONTAP

NDMP v4 provides a mechanism for creating NDMP v4 protocol extensions without modifying the core NDMP v4 protocol. You should be aware of the NDMP v4 extensions that are supported by ONTAP.

The following NDMP v4 extensions are supported by ONTAP:

- Cluster Aware Backup (CAB)

  Note: This extension is supported only in the SVM-scoped NDMP mode.

- Connection Address Extension (CAE) for IPv6 support
- Extension class 0x2050
  This extension supports restartable backup operations and Snapshot Management Extensions.

  Note: The `NDMP_SNAP_RECOVER` message, which is part of the Snapshot Management Extensions, is used to initiate a recovery operation and to transfer the recovered data from a local Snapshot copy to a local file system location. In ONTAP, this message allows the recovery of volumes and regular files only.

  The `NDMP_SNAP_DIR_LIST` message enables you to browse through the Snapshot copies of a volume. If a nondisruptive operation takes place while a browsing operation is in progress, the backup application must reinitiate the browsing operation.

NDMP restartable backup extension for a dump supported by ONTAP

You can use the NDMP restartable backup extension (RBE) functionality to restart a backup from a known checkpoint in the data stream before the failure.

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.

The limits mentioned in the following table are for the NDMP server. The limits mentioned in the section “Scalability limits for dump backup and restore sessions” are for the dump and restore session.

Scalability limits for dump backup and restore sessions on page 58

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 the node level by using NDMP options and commands. You can modify the NDMP options by using the `options` command. You must use NDMP-specific credentials to access a storage system to perform tape backup and restore operations.

For more information about the `options` command, see the man pages.

Related concepts

What node-scoped NDMP mode is on page 27

Related references

Commands for managing node-scoped NDMP mode on page 44

Commands for managing node-scoped NDMP mode

You can use the `system services ndmp` commands to manage NDMP at a node level. Some of these commands are deprecated and will be removed in a future major release.

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

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service 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 the default NDMP version	`system services ndmp version*`
Display NDMP service configuration	`system services ndmp service show`
Modify NDMP service configuration	`system services ndmp service modify`
Display all NDMP sessions	`system services ndmp status`
Display detailed information about all NDMP sessions	`system services ndmp probe`
Terminate the specified NDMP session	`system services ndmp kill`
Terminate all NDMP sessions	`system services ndmp kill-all`
Change the NDMP password	`system services ndmp password*`

If you want to...	Use this command...
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 the node-scoped NDMP mode status	`system services ndmp node-scope-mode status*`
Forcefully terminate all NDMP sessions	`system services ndmp service terminate`
Start the NDMP service daemon	`system services ndmp service start`
Stop the NDMP service daemon	`system services ndmp service 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*`

* These commands are deprecated and will be removed in a future major release.

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 44

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. 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.

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.

For more information about the `vserver services ndmp modify` command, see the man pages.

Related concepts

What Cluster Aware Backup extension does on page 47
What SVM-scoped NDMP mode is on page 28

Related references

Commands for managing SVM-scoped NDMP mode on page 46

Related information

ONTAP concepts
System administration

Commands for managing SVM-scoped NDMP mode

You can use the `vserver services ndmp` commands to manage NDMP on each storage virtual machine (SVM, formerly known as Vserver).

If you want to...	Use this command...
Enable NDMP service	`vserver services ndmp on` **Note:** NDMP service must always be 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`

If you want to...	Use this command...
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`
Display NDMP extension status	`vserver services ndmp extensions show` This command is available at the advanced privilege level.
Modify (enable or disable) NDMP extension status	`vserver services ndmp extensions modify` This command is available at the advanced privilege level.
Start logging for the specified NDMP session	`vserver services ndmp log start` This command is available at the advanced privilege level.
Stop logging for the specified NDMP session	`vserver services ndmp log stop` 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
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

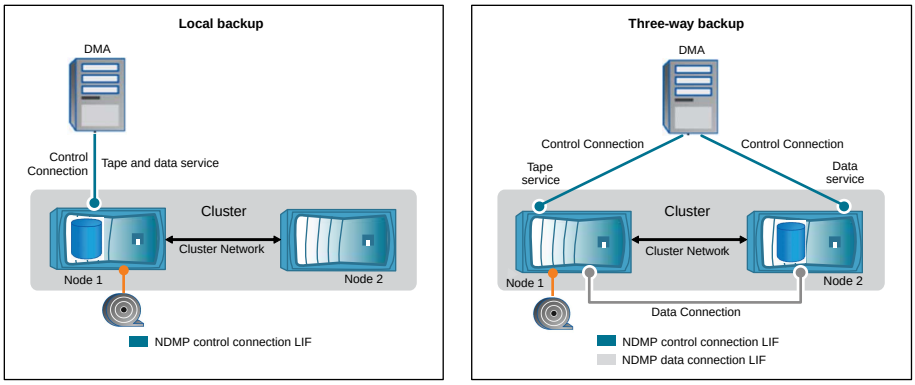
NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM that hosts the data LIF	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 47

NDMP server supports secure control connections in SVM-scoped mode

A secure control connection can be established between the Data Management Application (DMA) and NDMP server by using secure sockets (SSL/TLS) as the communication mechanism. This SSL communication is based on the server certificates. The NDMP server listens on port 30000 (assigned by IANA for “ndmps” service).

After establishing the connection from the client on this port, the standard SSL handshake ensues where the server presents the certificate to the client. When the client accepts the certificate, the SSL handshake is complete. After this process is complete, all of the communication between the client and the server is encrypted. The NDMP protocol workflow remains exactly as before. The secure NDMP connection requires server- side certificate authentication only. A DMA can choose to establish a connection either by connecting to the secure NDMP service or the standard NDMP service.

By default, secure NDMP service is disabled for a storage virtual machine (SVM). You can enable or disable the secure NDMP service on a given SVM by using the **`vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]`** command.

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 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

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
Intercluster LIF	LOCAL, TCP, TCP/IPv6

Related concepts

What Cluster Aware Backup extension does on page 47

Related information

Network and LIF management

User authentication in the SVM-scoped NDMP mode

In the storage virtual machine (SVM)-scoped NDMP mode, NDMP user authentication is integrated with role-based access control. In the SVM context, the NDMP user must have either the “vsadmin” or “vsadmin-backup” role. In a cluster context, the NDMP user must have either the “admin” or “backup” role.

Apart from these pre-defined roles, a user account associated with a custom role can also be used for NDMP authentication provided that the custom role has the “vserver services ndmp” folder in its command directory and the access level of the folder is not “none”. In this mode, you must generate an NDMP password for a given user account, which is created through role-based access control. Cluster users in an admin or backup role can access a node-management LIF, a cluster-management LIF, or an intercluster LIF. Users in a vsadmin-backup or vsadmin role can access only the data LIF for that SVM. Therefore, depending on 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. Therefore, NIS and LDAP users can access multiple SVMs with a common user ID 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 “User password” authentication method.

Related references

Commands for managing SVM-scoped NDMP mode on page 46

Related information

System administration
ONTAP concepts

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.

How tape backup and restore operations are affected during disaster recovery in MetroCluster configuration

You can perform tape backup and restore operations simultaneously during disaster recovery in a MetroCluster configuration. You must understand how these operations are affected during disaster recovery.

If tape backup and restore operations are performed on a volume of an SVM in a disaster recovery relationship, then you can continue performing incremental tape backup and restore operations after a switchover and switchback.

Understanding dump engine for FlexVol volumes

Dump is a Snapshot copy based backup and recovery solution from 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 a release earlier than Data ONTAP 8.3, you must perform a baseline backup operation before performing an incremental backup operation.

Related information

Upgrade, revert, or downgrade

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 ONTAP uses to back up the object indicated by the dump path:

Stage	Action
1	For less than full volume or full qtree backups, ONTAP traverses directories to identify the files to be backed up. If you are backing up an entire volume or qtree, ONTAP combines this stage with Stage 2.
2	For a full volume or full qtree backup, ONTAP identifies the directories in the volumes or qtrees to be backed up.
3	ONTAP writes the directories to tape.
4	ONTAP writes the files to tape.
5	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 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 integer is reset to 0 after the storage system is rebooted. After the backup operation is completed, the dump engine deletes this Snapshot copy.

When ONTAP performs multiple dump backups simultaneously, the dump engine creates multiple Snapshot copies. For example, if 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.

Types of data that the dump engine backs up

The dump engine enables you to back up data to tape to guard against disasters or controller disruptions. In addition to backing up data objects such as a files, directories, qtrees, or entire volumes, the dump engine can back up many types of information about each file. Knowing the types of data that the dump engine can back up and the restrictions to take into consideration can help you plan your approach to disaster recovery.

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 1,024 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 1,024, the default ACL is restored.

- Qtree information
- Junction paths
  Junction paths are backed up as symbolic links.
- LUN and LUN clones
  You can back up an entire LUN object; however, 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.

- VM-aligned files
  Backup of VM-aligned files is not supported in releases earlier than Data ONTAP 8.1.2.

Note: When a snapshot-backed LUN clone is transitioned from Data ONTAP operating in 7-Mode to ONTAP, it becomes an inconsistent LUN. The dump engine does not back up inconsistent LUNs.

When you restore data to a volume, client I/O is restricted on the LUNs being restored. The LUN restriction is removed only when the dump restore operation is complete. Similarly, during a SnapMirror single file or LUN restore operation, client I/O is restricted on both files and LUNs being restored. This restriction is removed only when the single file or LUN restore operation is complete. If a dump backup is performed on a volume on which a dump restore or SnapMirror single file or LUN restore operation is being performed, then the files or LUNs that have client I/O restriction are

not included in the backup. These files or LUNs are included in a subsequent backup operation if the client I/O restriction is removed.

Note: A LUN running on Data ONTAP 8.3 that is backed up to tape can be restored only to 8.3 and later releases and not to an earlier release. If the LUN is restored to an earlier release, then the LUN is restored as a file.

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.

You can back up VM-aligned files and the `vm-align-sector` option. For more information about VM-aligned files, see the *Logical Storage Management Guide*.

Logical storage management

What increment chains are

An increment chain is 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 32 levels of incremental backup operations.

There are two types of increment chains:

- A consecutive increment chain, which is a sequence of incremental backups that starts with level 0 and is raised by 1 at each subsequent backup.
- A nonconsecutive increment chain, where 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 are based on the most recent lower-level backup. For example, the sequence of backup levels 0, 2, 3, 1, 4 provides two increment chains: 0, 2, 3 and 0, 1, 4. The following table explains the bases of the incremental backups:

Backup order	Increment level	Increment chain	Base	Files backed up
1	0	Both	Files on the storage system	All files in the backup path
2	2	0, 2, 3	Level-0 backup	Files in the backup path created since the level-0 backup
3	3	0, 2, 3	Level-2 backup	Files in the backup path created since the level-2 backup
4	1	0, 1, 4	Level-0 backup, because this 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

Backup order	Increment level	Increment chain	Base	Files backed up
5	4	0, 1, 4	The level-1 backup, because it is a lower level and is 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. ONTAP allows a maximum value of 256 KB for MOVER_RECORD_SIZE.

When to restart a dump backup

A dump backup sometimes does not finish because of internal or external errors, such as tape write errors, power outages, accidental user interruptions, or internal inconsistency on the storage system. If your backup fails for one of these reasons, you can restart it.

You can choose to interrupt and restart a backup to avoid periods of heavy traffic on the storage system or to avoid competition for other limited resources on the storage system, such as a tape drive. You can interrupt a long backup and restart it later if a more urgent restore (or backup) requires the same tape drive. Restartable backups persist across reboots. You can restart an aborted backup to tape only if the following conditions are true:

- The aborted backup is in phase IV.
- All of the associated Snapshot copies that were locked by the dump command are available.
- The file history must be enabled.

When such a dump operation is aborted and left in a restartable state, the associated Snapshot copies are locked. These Snapshot copies are released after the backup context is deleted. You can view the list of backup contexts by using the `vserver services ndmp restartable backup show` command.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver vserver1 -
context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
           Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
```

```
                    Volume Name: /vserver1/vol1
            Is Cleanup Pending?: false
             Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                  Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
           Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

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

Types of data that the dump engine restores

When a disaster or controller disruption occurs, the dump engine provides multiple methods for you to recover all of the data that you backed up, from single files, to file attributes, to entire directories. Knowing the types of data that dump engine can restore and when to use which method of recovery can help minimize downtime.

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 provide 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 to 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 1,024, 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 LUN on an ONTAP volume.
- A 7-Mode volume can be restored to an ONTAP volume.
- VM-aligned files restored to a destination volume inherit the VM-align properties of the destination volume.

  Note: Restore of VM-aligned files to destination volumes in releases earlier than Data ONTAP 8.1.2 is not supported.
- 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 backed-up data to its original path or to a different destination. If you are restoring backed-up data to a different destination, you must prepare the destination for the restore operation.

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 to 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.

  Note: In ONTAP 9, qtree names support the Unicode format. The earlier releases of ONTAP do not support this format. If a qtree with Unicode names in ONTAP 9 is copied to an earlier release of ONTAP using the `ndmpcopy` command or through restoration from a backup image in a tape, the qtree is restored as a regular directory and not as a qtree with Unicode format.

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

Attention: The restore operation checks for volume space and inode availability on the destination volume when the restore operation starts. Setting the FORCE environment variable to **Y** causes the restore operation to skip the 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.

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.

The limits mentioned in the following table are for the dump or restore engine. The limits mentioned in the scalability limits for NDMP sessions are for the NDMP server, which are higher than the engine limits.

System memory of a storage system	Total number of dump backup and restore sessions
Less than 16 GB	4
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 NDMP sessions are established, one for dump backup and the other for 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.

Related references

Scalability limits for NDMP sessions on page 42

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

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

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

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

Notes:

- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- Restoring an ONTAP volume to a 7-Mode volume

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

Deleting restartable contexts

If you want to start a backup instead of restarting a context, you can delete the context.

About this task

You can delete a restartable context using the `vserver services ndmp restartable-backup delete` command by providing the SVM name and the context ID.

Step

1. Delete a restartable context:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context-id` *`context identifier`*

   .

Example

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver vserver1 -
context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

How dump works on 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, and 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.

How dump works with storage failover and ARL operations

Before you perform dump backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operations. The `-override-vetoes` option determines the behavior of dump engine during a storage failover or ARL operation.

When a dump backup or restore operation is running and the `-override-vetoes` option is set to **`false`**, a user-initiated storage failover or ARL operation is stopped. However, if the `–override-vetoes` option is set to **`true`**, then the storage failover or ARL operation is continued and the dump backup or restore operation is aborted. When a storage failover or ARL operation is automatically initiated by the storage system, an active dump backup or restore operation is always aborted. You cannot restart dump backup and restore operations even after storage failover or ARL operations complete.

Dump operations when CAB extension is supported

If the backup application supports CAB extension, you can continue performing incremental dump backup and restore operations without reconfiguring backup policies after a storage failover or ARL operation.

Dump operations when CAB extension is not supported

If the backup application does not support CAB extension, 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. Otherwise, after the storage failover and ARL operation, you must perform a baseline backup prior to performing the incremental backup operation.

Note: For storage failover operations, the LIF configured in the backup policy must be migrated to the partner node.

Related information

ONTAP concepts
High-availability configuration

How dump works with volume move

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 to run 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. Otherwise, after the volume move, you must perform a baseline backup before performing the incremental backup operation.
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

ONTAP concepts

How dump works when a FlexVol volume is full

Before performing an incremental dump backup operation, you must ensure that there is sufficient free space in the FlexVol volume.

If the operation fails, you must increase the free space in the Flex Vol volume either by increasing its size or deleting the Snapshot copies and then perform the incremental backup operation again.

How dump works when volume access type changes

When 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 from read/write to read-only.

Related information

ONTAP concepts

How dump works with SnapMirror single file or LUN restore

Before you perform dump backup or restore operations on a volume to which a single file or LUN is restored by using SnapMirror technology, you must understand how dump operations work with a single file or LUN restore operation.

During a SnapMirror single file or LUN restore operation, client I/O is restricted on the file or LUN being restored. When the single file or LUN restore operation finishes, the I/O restriction on the file or LUN is removed. If a dump backup is performed on a volume to which a single file or LUN is restored, then the file or LUN that has client I/O restriction is not included in the dump backup. In a subsequent backup operation, this file or LUN is backed up to tape after the I/O restriction is removed.

You cannot perform a dump restore and a SnapMirror single file or LUN restore operation simultaneously on the same volume.

How dump backup and restore operations are affected in MetroCluster configurations

Before you perform dump backup and restore operations in a MetroCluster configuration, you must understand how dump operations are affected when a switchover or switchback operation occurs.

Dump backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During a dump backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `override-vetoes` option is **`false`**, then the switchover is aborted and the backup or restore operation continues.
- If the value of the option is **`true`**, then the dump backup or restore operation is aborted and the switchover continues.

Dump backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and a dump backup or restore operation is initiated on cluster 2. The dump operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `override-vetoes` option is **`false`**, then the switchback is cancelled and the backup or restore operation continues.
- If the value of the option is **`true`**, then the backup or restore operation is aborted and the switchback continues.

Dump backup or restore operation initiated during a switchover or switchback

During a switchover from cluster 1 to cluster 2, if a dump backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback from cluster 2 to cluster 1, if a dump backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

Understanding SMTape engine for FlexVol volumes

SMTape is a disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the qtree or subtree level. SMTape supports baseline, differential, and incremental backups. SMTape does not require a license.

You can perform an SMTape backup and restore operation by using an NDMP-compliant backup application. You can choose SMTape to perform backup and restore operations only in the storage virtual machine (SVM) scoped NDMP mode.

Note: Reversion process is not supported when an SMTape backup or restore session is in progress. You must wait until the session finishes or you must abort the NDMP session.

Using SMTape, you can back up 255 Snapshot copies. For subsequent baseline, incremental, or differential backups, you must delete older backed-up Snapshot copies.

Before performing a baseline restore, the volume to which data is being restored must be of type **DP** and this volume must be in the restricted state. After a successful restore, this volume is automatically online. You can perform subsequent incremental or differential restores on this volume in the order in which the backups were performed.

Using Snapshot copies during SMTape backup

You should understand how Snapshot copies are used during an SMTape baseline backup and an incremental backup. There are also considerations to keep in mind while performing a backup using SMTape.

Baseline backup

While performing a baseline backup, you can specify the name of the Snapshot copy to be backed up to tape. If no Snapshot copy is specified, then depending on the access type of the volume (read/write or read-only), either a Snapshot copy is created automatically or existing Snapshot copies are used. When you specify a Snapshot copy for the backup, all the Snapshot copies older than the specified Snapshot copy are also backed up to tape.

If you do not specify a Snapshot copy for the backup, the following occurs:

- For a read/write volume, a Snapshot copy is created automatically.
  The newly created Snapshot copy and all the older Snapshot copies are backed up to tape.
- For a read-only volume, all the Snapshot copies, including the latest Snapshot copy, are backed up to tape.
  Any new Snapshot copies created after the backup is started are not backed up.

Incremental backup

For SMTape incremental or differential backup operations, the NDMP-compliant backup applications create and manage the Snapshot copies.

You must always specify a Snapshot copy while performing an incremental backup operation. For a successful incremental backup operation, the Snapshot copy backed up during the previous backup operation (baseline or incremental) must be on the volume from which the backup is performed. To ensure that you use this backed-up Snapshot copy, you must consider the Snapshot policy assigned on this volume while configuring the backup policy.

Considerations on SMTape backups on SnapMirror destinations

- A data protection mirror relationship creates temporary Snapshot copies on the destination volume for replication.
  You should not use these Snapshot copies for SMTape backup.
- If a SnapMirror update occurs on a destination volume in a data protection mirror relationship during an SMTape backup operation on the same volume, then the Snapshot copy that is backed up by SMTape must not be deleted on the source volume.
  During the backup operation, SMTape locks the Snapshot copy on the destination volume and if the corresponding Snapshot copy is deleted on the source volume, then the subsequent SnapMirror update operation fails.
- You should not use these Snapshot copies during incremental backup.

SMTape capabilities

SMTape capabilities such as backup of Snapshot copies, incremental and differential backups, preservation of deduplication and compression features on restored volumes, and tape seeding help you optimize your tape backup and restore operations.

SMTape provides the following capabilities:

- Provides a disaster recovery solution
- Enables incremental and differential backups
- Backs up Snapshot copies
- Enables backup and restore of deduplicated volumes and preserves deduplication on the restored volumes
- Backs up compressed volumes and preserves compression on the restored volumes
- Enables tape seeding

SMTape supports the blocking factor in multiples of 4 KB, in the range of 4 KB through 256 KB.

Note: You can restore data to volumes created across up to two major consecutive ONTAP releases only.

Features not supported in SMTape

SMTape does not support restartable backups and verification of backed-up files.

Scalability limits for SMTape backup and restore sessions

While performing SMTape backup and restore operations through NDMP or CLI (tape seeding), you must be aware of the maximum number of SMTape backup and restore sessions that can be performed simultaneously on storage systems with different system memory capacities. This maximum number depends on the system memory of a storage system.

Note: SMTape backup and restore sessions scalability limits are different from NDMP session limits and dump session limits.

System memory of the storage system	Total number of SMTape backup and restore sessions
Less than 16 GB	6
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

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.

Related concepts

Scalability limits for dump backup and restore sessions on page 58

Related references

Scalability limits for NDMP sessions on page 42

What tape seeding is

Tape seeding is an SMTape functionality that helps you initialize a destination FlexVol volume in a data protection mirror relationship.

Tape seeding enables you to establish a data protection mirror relationship between a source system and a destination system over a low-bandwidth connection.

Incremental mirroring of Snapshot copies from the source to the destination is feasible over a low bandwidth connection. However, an initial mirroring of the base Snapshot copy takes a long time over a low-bandwidth connection. In such cases, you can perform an SMTape backup of the source volume to a tape and use the tape to transfer the initial base Snapshot copy to the destination. You can then set up incremental SnapMirror updates to the destination system using the low-bandwidth connection.

Related information

ONTAP concepts

How SMTape works with storage failover and ARL operations

Before you perform SMTape backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operation. The `-override-vetoes` option determines the behavior of SMTape engine during a storage failover or ARL operation.

When an SMTape backup or restore operation is running and the `-override-vetoes` option is set to **`false`**, a user-initiated storage failover or ARL operation is stopped and the backup or restore operation complete. If the backup application supports CAB extension, then you can continue performing incremental SMTape backup and restore operations without reconfiguring backup policies. However, if the `–override-vetoes` option is set to **`true`**, then the storage failover or ARL operation is continued and the SMTape backup or restore operation is aborted.

Related information

Network and LIF management
High-availability configuration

How SMTape works with volume move

SMTape backup operations and volume move operations can run in parallel until the storage system attempts the final cutover phase. After this phase, new SMTape backup operations cannot run on the volume that is being moved. However, the current operations continue to run until completion.

Before the cutover phase for a volume is started, the volume move operation checks for active SMTape backup operations on the same volume. If there are active SMTape backup operations, then the volume move operation moves into a cutover deferred state and allows the SMTape backup operations to complete. After these backup operations are completed, you must manually restart the volume move operation.

If the backup application supports CAB extension, you can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.

Baseline restore and volume move operations cannot be performed simultaneously; however, incremental restore can run in parallel with volume move operations, with the behavior similar to that of SMTape backup operations during volume move operations.

Related information

ONTAP concepts

How SMTape works with volume rehost operations

Starting with ONTAP 9, SMTape operations cannot commence when a volume rehost operation is in progress on a volume. When a volume is involved in a volume rehost operation, SMTape sessions should not be started on that volume.

If any volume rehost operation is in progress, then SMTape backup or restore fails. If an SMTape backup or restore is in progress, then volume rehost operations fail with an appropriate error message. This condition applies to both NDMP-based and CLI-based backup or restore operations.

How NDMP backup policy are affected during ADB

When the automatic data balancer (ADB) is enabled, the balancer analyzes the usage statistics of aggregates to identify the aggregate that has exceeded the configured high-threshold usage percentage.

After identifying the aggregate that has exceeded the threshold, the balancer identifies a volume that can be moved to aggregates residing in another node in the cluster and attempts to move that volume. This situation affects the backup policy configured for this volume because if the data management application (DMA) is not CAB aware, then the user has to reconfigure the backup policy and run the baseline backup operation.

Note: If the DMA is CAB aware and the backup policy has been configured using specific interface, then the ADB is not affected.

How SMTape backup and restore operations are affected in MetroCluster configurations

Before you perform SMTape backup and restore operations in a MetroCluster configuration, you must understand how SMTape operations are affected when a switchover or switchback operation occurs.

SMTape backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During an SMTape backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `–override-vetoes` option is **`false`**, then the switchover process is aborted and the backup or restore operation continues.
- If the value of the option is **`true`**, then the SMTape backup or restore operation is aborted and the switchover process continues.

SMTape backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and an SMTape backup or restore operation is initiated on cluster 2. The SMTape operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `–override-vetoes` option is **`false`**, then the switchback process is aborted and the backup or restore operation continues.
- If the value of the option is **`true`**, then the backup or restore operation is aborted and the switchback process continues.

SMTape backup or restore operation initiated during a switchover or switchback

During a switchover process from cluster 1 to cluster 2, if an SMTape backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback process from cluster 2 to cluster 1, if an SMTape backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

Monitoring tape backup and restore operations for FlexVol volumes

You can view the event log files to monitor the tape backup and restore operations. ONTAP automatically logs significant backup and restore events and the time 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:

- Checking whether a nightly backup was successful
- Gathering statistics on backup operations
- For using the information in past event log files to help diagnose problems with backup 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 in 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.

About this task

With additional configurations, such as an access-control role with access to the **`spi`** web service or a user account set up with the **`http`** access method, you can also use a web browser to access these log files.

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`

Related information

System administration
ONTAP concepts

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
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.

Maximum number of allowed dumps or restores (maximum session limit) in progress

Message

`Maximum number of allowed dumps or restores (`*`maximum session limit`*`) in progress`

Cause

The maximum number of backup or restore jobs is 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 connection prepare precondition error

Message

```
DATA LISTEN: CAB data connection prepare precondition error
```

Cause

NDMP data listen fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP_CAB_DATA_CONN_PREPARE and the NDMP_DATA_LISTEN messages.

Corrective action

Contact your backup application vendor.

DATA CONNECT: CAB data connection prepare precondition error

Message

```
DATA CONNECT: CAB data connection prepare precondition error
```

Cause

NDMP data connect fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP_CAB_DATA_CONN_PREPARE and the NDMP_DATA_CONNECT messages.

Corrective action

Contact 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

NDMP dump backup is attempted on a SnapMirror destination volume that is part of either a `snapmirror break` or a `snapmirror resync` operation.

Corrective action

Wait for the `snapmirror break` or `snapmirror resync` operation to finish and then perform the dump operation.

Note: Whenever the state of a SnapMirror destination volume changes from read/write to read-only or from read-only to read/write, you must perform a baseline backup.

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.

SMTape error messages

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

Chunks out of order

Message

```
Chunks out of order
```

Cause

The backup tapes are not being restored in the correct sequence.

Corrective action

Retry the restore operation and load the tapes in the correct sequence.

Chunk format not supported

Message

```
Chunk format not supported
```

Cause

The backup image is not of SMTape.

Corrective action

If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

Failed to allocate memory

Message

```
Failed to allocate memory
```

Cause

The system has run out of memory.

Corrective action

Retry the job later when the system is not too busy.

Failed to get data buffer

Message

```
Failed to get data buffer
```

Cause

The storage system ran out of buffers.

Corrective action

Wait for some storage system operations to finish and then retry the job.

Failed to find snapshot

Message

```
Failed to find snapshot
```

Cause

The Snapshot copy specified for the backup is unavailable.

Corrective action

Check if the specified Snapshot copy is available. If not, retry with the correct Snapshot copy.

Failed to create snapshot

Message

```
Failed to create snapshot
```

Cause

The volume already contains the maximum number of Snapshot copies.

Corrective action

Delete some Snapshot copies and then retry the backup operation.

Failed to lock snapshot

Message

```
Failed to lock snapshot
```

Cause

The Snapshot copy is either in use or has been deleted.

Corrective action

If the Snapshot copy is in use by another operation, wait for that operation to finish and then retry the backup. If the Snapshot copy has been deleted, you cannot perform the backup.

Failed to delete snapshot

Message

```
Failed to delete snapshot
```

Cause

The auto Snapshot copy could not be deleted because it is in use by other operations.

Corrective action

Use the `snap` command to determine the status of the Snapshot copy. If the Snapshot copy is not required, delete it manually.

Failed to get latest snapshot

Message

```
Failed to get latest snapshot
```

Cause

The latest Snapshot copy might not exist because the volume is being initialized by SnapMirror.

Corrective action

Retry after initialization is complete.

Failed to load new tape

Message

```
Failed to load new tape
```

Cause

Error in tape drive or media.

Corrective action

Replace the tape and retry the operation.

Failed to initialize tape

Message

```
Failed to initialize tape
```

Cause

You might get this error message for one of the following reasons:

- The backup image is not of SMTape.
- The tape blocking factor specified is incorrect.
- The tape is corrupt or damaged.
- The wrong tape is loaded for restore.

Corrective action

- If the backup image is not of SMTape, retry the operation with a tape that has SMTape backup.
- If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
- If the tape is corrupt, you cannot perform the restore operation.
- If the wrong tape is loaded, retry the operation with the correct tape.

Failed to initialize restore stream

Message

```
Failed to initialize restore stream
```

Cause

You might get this error message for one of the following reasons:

- The backup image is not of SMTape.
- The tape blocking factor specified is incorrect.
- The tape is corrupt or damaged.
- The wrong tape is loaded for restore.

Corrective action

- If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.
- If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
- If the tape is corrupt, you cannot perform the restore operation.
- If the wrong tape is loaded, retry the operation with the correct tape.

Failed to read backup image

Message

```
Failed to read backup image
```

Cause

The tape is corrupt.

Corrective action

If the tape is corrupt, you cannot perform the restore operation.

Image header missing or corrupted

Message

```
Image header missing or corrupted
```

Cause

The tape does not contain a valid SMTape backup.

Corrective action

Retry with a tape containing a valid backup.

Internal assertion

Message

```
Internal assertion
```

Cause

There is an internal SMTape error.

Corrective action

Report the error and send the `etc/log/backup` file to technical support.

Invalid backup image magic number

Message

```
Invalid backup image magic number
```

Cause

The backup image is not of SMTape.

Corrective action

If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

Invalid backup image checksum

Message

```
Invalid backup image checksum
```

Cause

The tape is corrupt.

Corrective action

If the tape is corrupt, you cannot perform the restore operation.

Invalid input tape

Message

`Invalid input tape`

Cause

The signature of the backup image is not valid in the tape header. The tape has corrupted data or does not contain a valid backup image.

Corrective action

Retry the restore job with a valid backup image.

Invalid volume path

Message

`Invalid volume path`

Cause

The specified volume for the backup or restore operation is not found.

Corrective action

Retry the job with a valid volume path and volume name.

Mismatch in backup set ID

Message

`Mismatch in backup set ID`

Cause

The tape loaded during a tape change is not a part of the backup set.

Corrective action

Load the correct tape and retry the job.

Mismatch in backup time stamp

Message

`Mismatch in backup time stamp`

Cause

The tape loaded during a tape change is not a part of the backup set.

Corrective action

Use the `smtape restore -h` command to verify the header information of a tape.

Job aborted due to shutdown

Message

`Job aborted due to shutdown`

Cause

The storage system is being rebooted.

Corrective action

Retry the job after the storage system reboots.

Job aborted due to Snapshot autodelete

Message

`Job aborted due to Snapshot autodelete`

Cause

The volume does not have enough space and has triggered the automatic deletion of Snapshot copies.

Corrective action

Free up space in the volume and retry the job.

Tape is currently in use by other operations

Message

`Tape is currently in use by other operations`

Cause

The tape drive is in use by another job.

Corrective action

Retry the backup after the currently active job is finished.

Tapes out of order

Message

`Tapes out of order`

Cause

The first tape of the tape sequence for the restore operation does not have the image header.

Corrective action

Load the tape with the image header and retry the job.

Transfer failed (Aborted due to MetroCluster operation)

Message

`Transfer failed (Aborted due to MetroCluster operation)`

Cause

The SMTape operation is aborted because of a switchover or switchback operation.

Corrective action

Perform the SMTape operation after the switchover or switchback operation finishes.

Transfer failed (ARL initiated abort)

Message

`Transfer failed (ARL initiated abort)`

Cause

While an SMTape operation is in progress if an aggregate relocation is initiated, then the SMTape operation is aborted.

Corrective action

Perform the SMTape operation after the aggregate relocation operation finishes.

Transfer failed (CFO initiated abort)

Message

`Transfer failed (CFO initiated abort)`

Cause

The SMTape operation is aborted because of a storage failover (takeover and giveback) operation of a CFO aggregate.

Corrective action

Perform the SMTape operation after the storage failover of the CFO aggregate finishes.

Transfer failed (SFO initiated abort)

Message

`Transfer failed (SFO initiated abort)`

Cause

The SMTape operation is aborted because of a storage failover (takeover and giveback) operation.

Corrective action

Perform the SMTape operation after the storage failover (takeover and giveback) operation finishes.

Underlying aggregate under migration

Message

`Underlying aggregate under migration`

Cause

If an SMTape operation is initiated on an aggregate that is under migration (storage failover or aggregate relocation), then the SMTape operation fails.

Corrective action

Perform the SMTape operation after the aggregate migration finishes.

Volume is currently under migration

Message

`Volume is currently under migration`

Cause

Volume migration and SMTape backup cannot run simultaneously.

Corrective action

Retry the backup job after the volume migration is complete.

Volume offline

Message

`Volume offline`

Cause

The volume being backed up is offline.

Corrective action

Bring the volume online and retry the backup.

Volume not restricted

Message

`Volume not restricted`

Cause

The destination volume to which data is being restored is not restricted.

Corrective action

Restrict the volume and retry the restore operation.

Copyright

Trademark

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

E

F

I

L

M

N

O

P

Q

R

S

T

U

V

W