Contents

Deciding whether to use this guide ............................................................. 4
NDMP configuration workflow ................................................................. 5
  Preparing for NDMP configuration .......................................................... 6
  Verifying tape device connections ......................................................... 7
  Enabling tape reservations ................................................................... 8
  Configuring NDMP at the SVM level or the node level ............................ 8
    Configuring SVM-scoped NDMP ......................................................... 9
    Configuring node-scoped NDMP ....................................................... 13
  Configuring the backup application ..................................................... 15
Where to find additional information ..................................................... 17
Copyright information ............................................................................ 18
Trademark information .......................................................................... 19
How to send comments about documentation and receive update
  notifications ............................................................................................ 20
Index ........................................................................................................ 21
Deciding whether to use the NDMP Configuration Express Guide

This guide describes how to quickly configure an ONTAP 9 cluster to use the Network Data Management Protocol (NDMP) to back up data directly to tape using a third-party backup application.

You should use this guide if you want to configure NDMP in the following context:

- The cluster is running ONTAP 9.
- You have a third-party backup application (also called a Data Management Application or DMA).
- You are a cluster administrator.
- You want to perform backup operations either at the cluster level (using the admin storage virtual machine (SVM)) or node level.
- Tape devices and an optional media server are installed.
- Tape devices are connected to the cluster through a Fibre Channel (FC) switch and not directly attached.
- At least one tape device has a logical unit number (LUN) of 0.
- You are using FlexVol volumes and not Infinite Volumes.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

If these assumptions are not correct for your situation, you should see the Data Protection Tape Backup and Recovery Guide.

Data protection using tape backup
NDMP configuration workflow

Setting up tape backup over NDMP involves preparing for NDMP configuration, verifying the tape device connections, enabling tape reservations, configuring NDMP at the SVM or node level, enabling NDMP on the cluster, configuring a backup user, configuring LIFs, and configuring the backup application.

Steps

1. **Preparing for NDMP configuration** on page 6
   Before you configure tape backup access over Network Data Management Protocol (NDMP), you must verify that the planned configuration is supported, verify that your tape drives are listed as qualified drives on each node, verify that all nodes have intercluster LIFs, and identify whether the backup application supports the Cluster Aware Backup (CAB) extension.

2. **Verifying tape device connections** on page 7
   You must ensure that all drives and media changers are visible in ONTAP as devices.

3. **Enabling tape reservations** on page 8
   You must ensure that tape drives are reserved for use by backup applications for NDMP backup operations.

4. **Configuring NDMP at the SVM level or the node level** on page 8
   If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as SVM-scoped at the cluster (admin SVM) level, which enables you to back up all volumes hosted across different nodes of the cluster. Otherwise, you can configure node-scoped NDMP, which enables you to back up all the volumes hosted on that node.
5. Configuring the backup application on page 15
   After the cluster is configured for NDMP access, you must gather information from the cluster configuration and then configure the rest of the backup process in the backup application.

Preparing for NDMP configuration

Before you configure tape backup access over Network Data Management Protocol (NDMP), you must verify that the planned configuration is supported, verify that your tape drives are listed as qualified drives on each node, verify that all nodes have intercluster LIFs, and identify whether the backup application supports the Cluster Aware Backup (CAB) extension.

Steps

1. Verify that the planned configuration is supported by using the Interoperability Matrix (IMT).
   
   **NetApp Interoperability Matrix Tool**
   
   You should verify that the following components are compatible:
   
   - The version of ONTAP 9 that is running on the cluster.
   - The backup application vendor and application version: for example, Symantec NetBackup 7.6 or CommVault Simpana 10 SP8.
   - The tape devices details, such as the manufacturer, model, and interface of the tape drives: for example, IBM Ultrium-TD4 FC or HP Ultrium-5 SAS.
   - The platforms of the nodes in the cluster: for example, FAS3260 or FAS6280.

2. Verify that your tape drives are listed as qualified drives in each node’s built-in tape configuration file:
   
   a. On the command line-interface, view the built-in tape configuration file by using the `storage tape show-supported-status` command.

   **Example**
   ```
   cluster1::> storage tape show-supported-status
   Node: cluster1-1
   Is Tape Drives Supported Support Status
   -------------------------- -------- -------------------------
   Certance Ultrium 2 true Dynamically Qualified
   Certance Ultrium 3 true Dynamically Qualified
   Digital DLT2000 true Qualified
   ....
   ```
   
   b. Compare your tape drives to the list of qualified drives in the output.
      
      **Note:** The names of the tape devices in the output might vary slightly from the names on the device label or in the Interoperability Matrix. For example, Digital DLT2000 can also be known as DLT2k. You can ignore these minor naming differences.

   c. If a device is not listed as qualified in the output even though the device is qualified according to the Interoperability Matrix, download and install an updated configuration file for the device using the instructions on the NetApp Support Site.
      
      **NetApp Downloads: Tape Device Configuration Files**
      
      A qualified device might not be listed in the built-in tape configuration file if the tape device was qualified after the node was shipped.

3. Verify that every node in the cluster has an intercluster LIF:
a. View the intercluster LIFs on the nodes by using the `network interface show -role intercluster` command.

**Example**

```
cluster1::> network interface show -role intercluster
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1</td>
<td>IC1</td>
<td>up/up</td>
<td>192.0.2.65/24</td>
<td>cluster1-1</td>
<td>e0a</td>
<td>true</td>
</tr>
</tbody>
</table>

b. If an intercluster LIF does not exist on any node, create an intercluster LIF by using the `network interface create` command.

**Example**

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role intercluster -home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask 255.255.255.0 -status-admin up -failover-policy local-only -firewall-policy intercluster
```

```
cluster1::> network interface show -role intercluster
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1</td>
<td>IC1</td>
<td>up/up</td>
<td>192.0.2.65/24</td>
<td>cluster1-1</td>
<td>e0a</td>
<td>true</td>
</tr>
<tr>
<td>cluster1</td>
<td>IC2</td>
<td>up/up</td>
<td>192.0.2.68/24</td>
<td>cluster1-2</td>
<td>e0b</td>
<td>true</td>
</tr>
</tbody>
</table>

**Network and LIF management**

4. Identify whether the backup application supports Cluster Aware Backup (CAB) by using the documentation provided with the backup application.

CAB support is a key factor in determining the type of backup you can perform.

**Verifying tape device connections**

You must ensure that all drives and media changers are visible in ONTAP as devices.

**Steps**

1. View information about all drives and media changers by using the `storage tape show` command.

**Example**

```
cluster1::> storage tape show
```

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Device Type</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>sw4:10.11</td>
<td>tape drive</td>
<td>HP LTO-3</td>
<td>normal</td>
</tr>
<tr>
<td>0d.125L1</td>
<td>media changer</td>
<td>HP MSL G3 Series</td>
<td>normal</td>
</tr>
<tr>
<td>0d.4</td>
<td>tape drive</td>
<td>IBM LTO 5 ULT3580</td>
<td>normal</td>
</tr>
<tr>
<td>0d.4L1</td>
<td>media changer</td>
<td>IBM 3573-TL</td>
<td>normal</td>
</tr>
</tbody>
</table>

2. If a tape drive is not displayed, troubleshoot the problem.

3. If a media changer is not displayed, view information about media changers by using the `storage tape show-media-changer` command, and then troubleshoot the problem.
Example

```
cluster1::> storage tape show-media-changer
Media Changer: sw4:10.11L1
  Description: PX70-TL
  WWNN: 2:00a:000e11:10b919
  WWPN: 2:00b:000e11:10b919
  Serial Number: 00FRU7800000_LL1
  Errors: -
  Paths:
    Node      Initiator     Alias     Device State    Status
    -----------  ---------     -------     ---------------  --------
    cluster1-01  2b         mc0      in-use           normal
```

Enabling tape reservations

You must ensure that tape drives are reserved for use by backup applications for NDMP backup operations.

About this task

The reservation settings vary in different backup applications, and these settings must match the backup application and the nodes or servers using the same drives. See the vendor documentation of the backup application for the correct reservation settings.

Steps

1. Enable reservations by using the `options -option-name tape.reservations -option-value persistent` command.

   Example

   The following command enables reservations with the `persistent` value:

   ```
   cluster1::> options -option-name tape.reservations -option-value persistent
   2 entries were modified.
   ```

2. Verify that reservations are enabled on all nodes by using the `options tape.reservations` command, and then review the output.

   Example

   ```
   cluster1::> options tape.reservations
   cluster1-1
   tape.reservations        persistent
   cluster1-2
   tape.reservations        persistent
   2 entries were displayed.
   ```

Configuring NDMP at the SVM level or the node level

If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as SVM-scoped at the cluster (admin SVM) level, which enables you to back up all volumes hosted across different nodes of the cluster. Otherwise, you can configure node-scoped NDMP, which enables you to back up all the volumes hosted on that node.
Configuring SVM-scoped NDMP

If the DMA supports the Cluster Aware Backup (CAB) extension, you can back up all the volumes hosted across different nodes in a cluster by enabling SVM-scoped NDMP, configuring a backup user account, and configuring LIFs for data and control connection.

Before you begin

The CAB extension must be supported by the DMA.

Steps

1. Enabling SVM-scoped NDMP on the cluster on page 9
2. Configuring a backup user for the cluster on page 10
3. Configuring LIFs on page 10

Enabling SVM-scoped NDMP on the cluster

You can configure SVM-scoped NDMP on the cluster by enabling SVM-scoped NDMP mode and NDMP service on the cluster (admin SVM).

About this task

Turning off node-scoped NDMP mode enables SVM-scoped NDMP mode on the cluster.

Steps

1. Enable SVM-scoped NDMP mode by using the system services ndmp command with the node-scope-mode parameter.

   Example

   
   ```
   cluster1::> system services ndmp node-scope-mode off
   NDMP node-scope-mode is disabled.
   ```

2. Enable NDMP service on the admin SVM by using the vserver services ndmp on command.

   Example

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   The authentication type is set to **challenge** by default and plaintext authentication is disabled.

   **Note:** For secure communication, you should keep plaintext authentication disabled.

3. Verify that NDMP service is enabled by using the vserver services ndmp show command.

   Example

   ```
   cluster1::> vserver services ndmp show
   Vserver | Enabled | Authentication type
   --------|---------|-----------------------
   cluster1 | true    | challenge
   vs1     | false   | challenge
   ```
Configuring a backup user for the cluster

To authenticate NDMP from the backup application, you must create a local backup user, or an NIS or LDAP user for the cluster with the admin or backup role, and generate an NDMP password for the backup user.

Before you begin

If you are using an NIS or LDAP user, the user must be created on the respective server. You cannot use an Active Directory user.

Steps

1. Create a backup user with the admin or backup role by using the security login create command.

   You can specify a local backup user name or an NIS or LDAP user name for the -user-or-group-name parameter.

   Example

   The following command creates the backup user backup_admin1 with the backup role:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1 -application ssh -authmethod password -role backup
   Please enter a password for user 'backup_admin1':
   Please enter it again:
   ```

2. Generate a password for the admin SVM by using the vserver services ndmp generate password command.

   The generated password must be used to authenticate the NDMP connection by the backup application.

   Example

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1 -user backup_admin1
   Vserver: cluster1
   User: backup_admin1
   Password: qG5CqQHyxw7tE577g
   ```

Configuring LIFs

You must identify the LIFs that will be used for establishing a data connection between the data and tape resources, and for control connection between the admin SVM and the backup application. After identifying the LIFs, you must verify that firewall and failover policies are set for the LIFs, and specify the preferred interface role.

Steps

1. Identify the intercluster, cluster-management, and node-management LIFs by using the network interface show command with the -role parameter.

   Example

   The following command displays the intercluster LIFs:
The following command displays the cluster-management LIF:

```
cluster1::> network interface show -role cluster-mgmt
```

The following command displays the node-management LIFs:

```
cluster1::> network interface show -role node-mgmt
```

2. Ensure that the firewall policy is enabled for NDMP on the intercluster, cluster-management (cluster-mgmt), and node-management (node-mgmt) LIFs:

   a. Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

   **Example**

   The following command displays the firewall policy for the cluster-management LIF:

   ```
   cluster1::> system services firewall policy show -policy cluster
   ```

   The following command displays the firewall policy for the intercluster LIF:

   ```
   cluster1::> system services firewall policy show -policy intercluster
   ```

   The following command displays the firewall policy for the node-management LIF:

   ```
   cluster1::> system services firewall policy show -policy mgmt
   ```
b. If the firewall policy is not enabled, enable the firewall policy by using the system services firewall policy modify command with the -service parameter.

Example
The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for all the LIFs:

   a. Verify that the failover policy for the cluster-management LIF is set to broadcast-domain-wide, and the policy for the intercluster and node-management LIFs is set to local-only by using the network interface show -failover command.

Example
The following command displays the failover policy for the cluster-management, intercluster, and node-management LIFs:

```
cluster1::> network interface show -failover
```

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Home Node:Port</th>
<th>Failover Policy</th>
<th>Failover Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster cluster1_mgmt</td>
<td>cluster1-1:e0m</td>
<td>broadcast-domain-wide</td>
<td>Default</td>
</tr>
<tr>
<td>IC1</td>
<td>cluster1-1:e0a</td>
<td>local-only</td>
<td>Default</td>
</tr>
<tr>
<td>IC2</td>
<td>cluster1-1:e0b</td>
<td>local-only</td>
<td>Default</td>
</tr>
<tr>
<td>cluster1-1 cluster1-1_mgmt1</td>
<td>cluster1-1:e0m</td>
<td>local-only</td>
<td>Default</td>
</tr>
<tr>
<td>cluster1-2 cluster1-2_mgmt1</td>
<td>cluster1-2:e0m</td>
<td>local-only</td>
<td>Default</td>
</tr>
</tbody>
</table>

   b. If the failover policies are not set appropriately, modify the failover policy by using the network interface modify command with the -failover-policy parameter.

Example
```
cluster1::> network interface modify -vserver cluster1 -lif IC1 -failover-policy local-only
```

4. Specify the LIFs that are required for data connection by using the vserver services ndmp modify command with the preferred-interface-role parameter.
5. Verify that the preferred interface role is set for the cluster by using the `vserver services ndmp show` command.

Example

```
cluster1::> vserver services ndmp show -vserver cluster1
```

```
Vserver: cluster1
NDMP Version: 4

Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

### Configuring node-scoped NDMP

You can back up volumes hosted on a node by enabling node-scoped NDMP, setting up the password for the root user, and configuring a LIF for data and control connection.

**Steps**

1. [Enabling node-scoped NDMP on the cluster](#) on page 13
2. [Configuring a LIF](#) on page 14

#### Enabling node-scoped NDMP on the cluster

You can configure node-scoped NDMP by enabling node-scoped NDMP on the cluster and NDMP service on all nodes of the cluster. You must also configure the `root` user for NDMP when enabling the NDMP service.

**Steps**

1. Enable node-scoped NDMP mode by using the `system services ndmp` command with the `node-scope-mode` parameter.

   Example

   ```
   cluster1::> system services ndmp node-scope-mode on
   NDMP node-scope-mode is enabled.
   ```

2. Enable NDMP service on all nodes in the cluster by using the `system services ndmp on` command.

   Using the wildcard “*” enables NDMP service on all nodes at the same time.

   You must specify a password for authentication of the NDMP connection by the backup application.

   Example

   ```
   cluster1::> system services ndmp on -node *
   Please enter password:
   Confirm password:
   2 entries were modified.
   ```

3. Disable the `-clear-text` option for secure communication of the NDMP password by using the `system services ndmp modify` command.
Using the wildcard “*” disables the -clear-text option on all nodes at the same time.

**Example**

```
cluster1::> system services ndmp modify -node * -clear-text false
2 entries were modified.
```

4. Verify that NDMP service is enabled and the -clear-text option is disabled by using the `system services ndmp show` command.

**Example**

```
cluster1::> system services ndmp show
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

**Configuring a LIF**

You must identify a LIF that will be used for establishing a data connection and control connection between the node and the backup application. After identifying the LIF, you must verify that firewall and failover policies are set for the LIF.

**Steps**

1. Identify the intercluster LIF hosted on the nodes by using the `network interface show` command with the `-role` parameter.

**Example**

```
cluster1::> network interface show -role intercluster
Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b     true
```

2. Ensure that the firewall policy is enabled for NDMP on the intercluster LIFs:
   
   a. Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

**Example**

```
The following command displays the firewall policy for the intercluster LIF:

cluster1::> system services firewall policy show -policy intercluster
Vserver      Policy       Service    Allowed
-------      ------------ ---------- -------------------
cluster1    intercluster dns        -
cluster1    intercluster http       -
cluster1    intercluster https      -
cluster1    intercluster ndmp       0.0.0.0/0, ::/0
cluster1    intercluster ndmps      -
cluster1    intercluster ntp        -
cluster1    intercluster rsh        -
cluster1    intercluster ssh        -
cluster1    intercluster telnet     -
9 entries were displayed.
```

b. If the firewall policy is not enabled, enable the firewall policy by using the `system services firewall policy modify` command with the `-service` parameter.
The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for the intercluster LIFs:
   a. Verify that the failover policy for the intercluster LIFs is set to `local-only` by using the `network interface show -failover` command.

```
cluster1::> network interface show -failover

Logical          Home              Failover     Failover
Vserver     Interface        Node:Port         Policy       Group
--------    ---------------  ----------------- ------------ --------
cluster1     IC1               cluster1-1:e0a    local-only   Default
Failover Targets:

IC2               cluster1-2:e0b    local-only   Default
Failover Targets:

cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only    Default
Failover Targets:
```

b. If the failover policy is not set appropriately, modify the failover policy by using the `network interface modify` command with the `--failover-policy` parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1 --failover-policy local-only
```

### Configuring the backup application

After the cluster is configured for NDMP access, you must gather information from the cluster configuration and then configure the rest of the backup process in the backup application.

**Steps**

1. Gather the following information that you configured earlier in ONTAP:
   - The user name and password that the backup application requires to create the NDMP connection
   - The IP addresses of the intercluster LIFs that the backup application requires to connect to the cluster

2. In ONTAP, display the aliases that ONTAP assigned to each device by using the `storage tape alias show` command.
   
The aliases are often useful in configuring the backup application.

```
cluster1::> storage tape show -alias

Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5
```
3. In the backup application, configure the rest of the backup process by using the backup application's documentation.

**After you finish**

If a data mobility event occurs, such as a volume move or LIF migration, you must be prepared to reinitialize any interrupted backup operations.
Where to find additional information

Additional documentation is available to further configure tape backup, restore from tape, and configure other types of data protection.

Documentation about tape backup and restore

- Data protection using tape backup
  Describes how to back up and recover data using tape backup and recovery features in clusters, using NDMP, SM Tape, and dump technologies.

Documentation on other types of data protection

- ONTAP 9 Documentation Center
  Specific express guides describe how to configure data protection technologies, such as SnapVault and SnapMirror.

- Data protection
  Describes how to plan and manage disaster recovery and disk-to-disk backup of clustered systems.
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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

A

admin SVMs
 configuring a backup user for 10
 configuring LIFs for NDMP 10
 enabling NDMP service 9

aliases
 gathering for configuring the backup application 15

B

backup
 where to get information about configuring 17
 backup applications
 configuring 15
 verifying CAB support for 6
 backup users
 configuring for the cluster or admin SVM 10
 configuring for the node 13

C

choosing
 where to configure NDMP 8

Cluster Aware Backup
 identifying support for 6

clusters
 configuring a backup user for 10
 comments
 how to send feedback about documentation 20
 configuring
 backup user for the cluster or admin SVM 10
 backup user for the node 13
 LIFs for node-scoped NDMP 14
 LIFs for SVM-scoped NDMP 10
 NDMP, workflow 5
 node-scoped NDMP 13
 SVM-scoped NDMP 9

D

data management applications
 See backup applications
 data protection
 where to get information about configuring 17
 DMAs
 See backup applications
 documentation
 additional information about tape backup and restore 17
 how to receive automatic notification of changes to 20
 how to send feedback about 20

E

enabling
 node-scoped NDMP and NDMP service 13
 reservations for NDMP 8
 SVM-scoped NDMP and NDMP service 9

express guides
 additional documentation on data protection 17
 NDMP configuration workflow 5
 requirements for using NDMP Configuration Express Guide 4

F

feedback
 how to send comments about documentation 20

flowcharts
 NDMP configuration workflow 5

G

gathering information
 required by the backup application 15

I

information
 how to send feedback about improving documentation 20

L

LDAP
 configuring a user for NDMP backup 10
 LIFs
 configuring for node-scoped NDMP 14
 configuring for SVM-scoped NDMP 10
 verifying prerequisites for NDMP configuration 6

M

media changers
 viewing information about 7

N

NDMP
 configuring a backup user for the cluster 10
 configuring for a node 13
 configuring LIFs for node-scoped 14
 configuring LIFs for SVM-scoped 10
 configuring SVM-scoped 9
 configuring the backup user for nodes 13
 deciding whether to use the NDMP Configuration Express Guide 4
 enabling node-scoped 13
 enabling SVM-scoped 9
 enabling tape reservations 8
 verifying planned configuration for tape access 6
 where to get information about configuring 17
 workflow for configuring 5
NDMP service
   enabling on the admin SVM 9
   enabling on the node 13

NIS
   configuring a user for NDMP backup 10

node-scoped NDMP
   configuring 13
   configuring LIFs 14
   configuring the backup user 13
   enabling 13

nodes
   configuring a backup user for 13
   configuring a LIF for node-scoped NDMP 14
   enabling NDMP service 13

ONTAP
   viewing tape devices and media changers in 7

reservations
   tape, enabling for NDMP operations 8

root users
   configuring a root user for each node 13

S
   suggestions
      how to send feedback about documentation 20

SVM-scoped NDMP
   configuring 9
   configuring a backup user for 10
   configuring LIFs 10
   enabling 9

Tape backup and restore
   where to get information 17

tape backups
   deciding whether to use the NDMP Configuration Express Guide 4

tape devices
   viewing in ONTAP 7

tape drives
   verifying as qualified before NDMP configuration 6

tape reservations
   enabling for NDMP 8

Twitter
   how to receive automatic notification of documentation changes 20

V
   viewing
      tape devices and media changers in ONTAP 7

workflows
   NDMP configuration 5