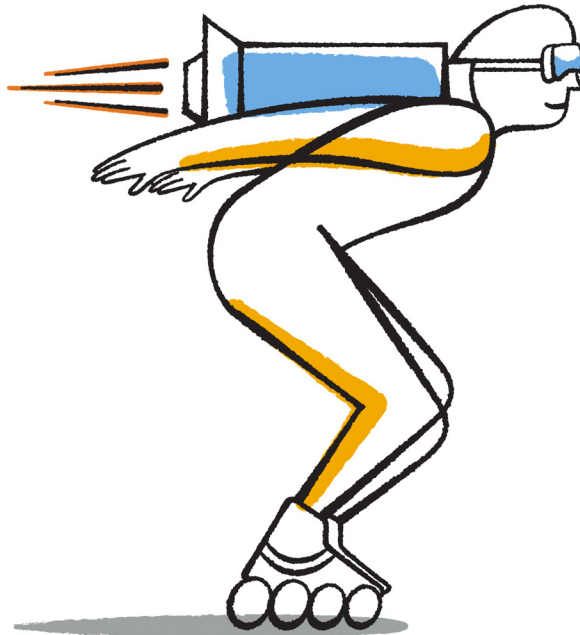




**NetApp®**

## Clustered Data ONTAP® 8.3

### NDMP Configuration Express Guide



NetApp, Inc.  
495 East Java Drive  
Sunnyvale, CA 94089  
U.S.

Telephone: +1 (408) 822-6000  
Fax: +1 (408) 822-4501  
Support telephone: +1 (888) 463-8277  
Web: [www.netapp.com](http://www.netapp.com)  
Feedback: [doccomments@netapp.com](mailto:doccomments@netapp.com)

Part number: 215-09755\_A0  
January 2015



# Contents

<b>Deciding whether to use this guide .....</b>	<b>4</b>
<b>NDMP configuration workflow .....</b>	<b>5</b>
Preparing for NDMP configuration .....	6
Verifying tape device connections .....	8
Enabling tape reservations .....	9
Configuring NDMP at the SVM level or the node level .....	9
Configuring SVM-scoped NDMP .....	10
Configuring node-scoped NDMP .....	15
Configuring the backup application .....	18
<b>Where to find additional information .....</b>	<b>20</b>
<b>Copyright information .....</b>	<b>21</b>
<b>Trademark information .....</b>	<b>22</b>
<b>How to send comments about documentation and receive update     notification .....</b>	<b>23</b>
<b>Index .....</b>	<b>24</b>

## Deciding whether to use this guide

---

This guide describes how to quickly configure a Data ONTAP 8.3 cluster to use the Network Data Management Protocol (NDMP) to back up data directly to tape using a third-party backup application.

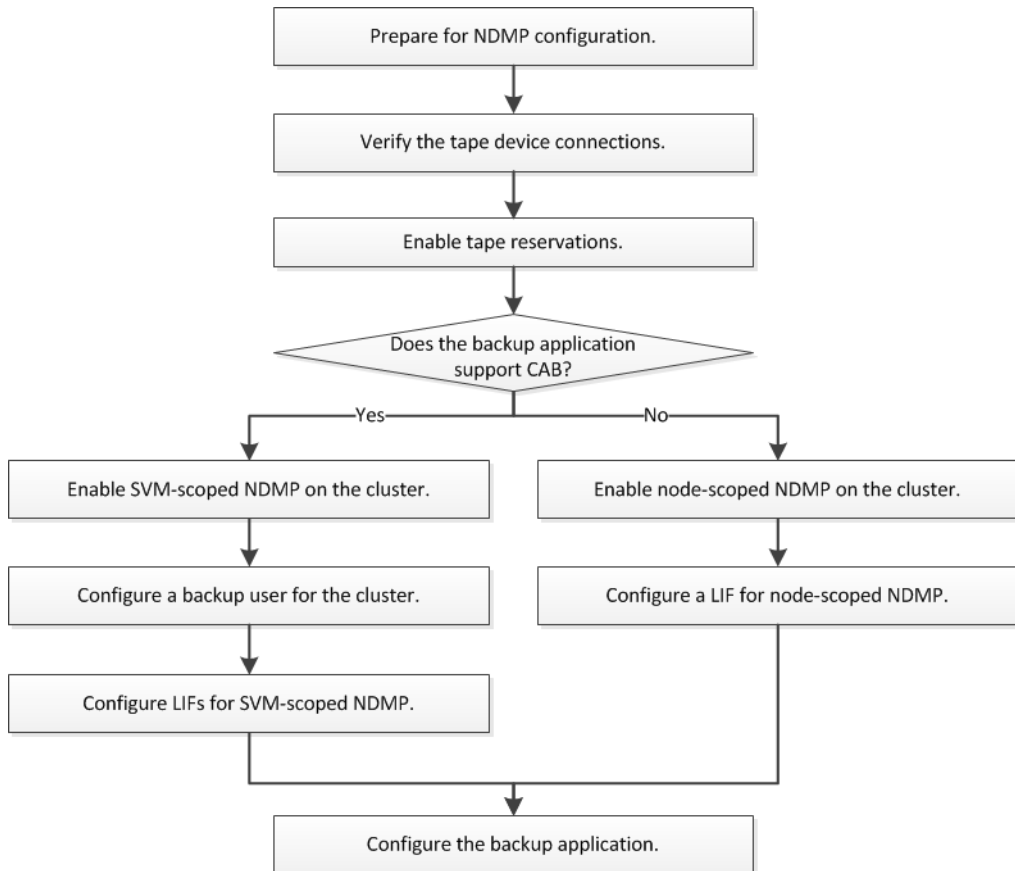
You should use this guide if you want to configure NDMP in the following context:

- The cluster is running Data ONTAP 8.3.
- 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—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 [Clustered Data ONTAP 8.3 Data Protection Tape Backup and Recovery Guide](#).

# 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 NDMP, you must verify that the planned configuration is supported, ensure that your tape drives are listed as qualified drives on each node, ensure 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 8  
You must ensure that all drives and media changers are visible in Data ONTAP as devices.
3. [Enabling tape reservations](#) on page 9  
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 9  
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 18  
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 NDMP, you must verify that the planned configuration is supported, ensure that your tape drives are listed as qualified drives on each node, ensure 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 Data ONTAP 8.3 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. Ensure 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

Tape Drives                                Is
-----                                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. Ensure 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

Vserver      Logical  Status  Network      Current      Current  Is
Interface    Admin/Oper Address/Mask Node          Port        Home
-----
cluster1     IC1     up/up   192.0.2.65/24 cluster1-1   e0a       true
```

- 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

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

### *Clustered Data ONTAP 8.3 Network Management Guide*

- 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 what type of backup you can perform.

## Verifying tape device connections

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

### Steps

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

### Example

```
cluster1::> storage tape show

Node: cluster1-01
Device ID           Device Type      Description      Status
-----
sw4:10.11           tape drive      HP LTO-3         normal
0b.125L1           media changer   HP MSL G3 Series normal
0d.4               tape drive      IBM LTO 5 ULT3580 normal
0d.4L1            media changer   IBM 3573-TL      normal
...
```

- If a tape drive is not displayed, troubleshoot the problem.
- 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
  WNNN: 2:00a:000e11:10b919
  WWPB: 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.

### Choices

- [Configuring SVM-scoped NDMP](#) on page 10
- [Configuring node-scoped NDMP](#) on page 15

## 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 10
2. [Configuring a backup user for the cluster](#) on page 11
3. [Configuring LIFs](#) on page 12

## 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: qG5CqQHYxw7tE57g
```

**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:

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is 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

The following command displays the cluster-management LIF:

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
cluster1	cluster_mgmt	up/up	192.0.2.60/24	cluster1-2	e0M	true

The following command displays the node-management LIFs:

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
cluster1	cluster1-1_mgmt1	up/up	192.0.2.69/24	cluster1-1	e0M	true
	cluster1-2_mgmt1	up/up	192.0.2.70/24	cluster1-2	e0M	true

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
```

Vserver	Policy	Service	Allowed
cluster	cluster	dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		<b>ndmp</b>	<b>0.0.0.0/0</b>
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		rsh	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
		telnet	0.0.0.0/0

10 entries were displayed.

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	-
		http	-
		https	-
		<b>ndmp</b>	<b>0.0.0.0/0, ::/0</b>
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

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

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

Vserver	Policy	Service	Allowed
cluster1-1	mgmt	dns	0.0.0.0/0, ::/0
		http	0.0.0.0/0, ::/0
		https	0.0.0.0/0, ::/0
		<b>ndmp</b>	<b>0.0.0.0/0, ::/0</b>
		ndmps	0.0.0.0/0, ::/0
		ntp	0.0.0.0/0, ::/0
		rsh	-
		snmp	0.0.0.0/0, ::/0
		ssh	0.0.0.0/0, ::/0
		telnet	-

10 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.

**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
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster	cluster1_clus1	cluster1-1:e0a	local-only	cluster
			Failover Targets:	
			.....	
cluster1	cluster_mgmt	cluster1-1:e0m	broadcast-domain-wide	Default
			Failover Targets:	
			.....	
	IC1	cluster1-1:e0a	local-only	Default
			Failover Targets:	
			.....	
	IC2	cluster1-1:e0b	local-only	Default
			Failover Targets:	
			.....	
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	Default
			Failover Targets:	
			.....	
cluster1-2	cluster1-2_mgmt1	cluster1-2:e0m	local-only	Default
			Failover Targets:	
			.....	

- 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.

**Example**

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred-interface-role
intercluster,cluster-mgmt,node-mgmt
```

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 15
2. [Configuring a LIF](#) on page 16

**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.

## 16 | NDMP Configuration Express Guide

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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is 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	-
		http	-
		https	-
		<b>ndmp</b>	<b>0.0.0.0/0, ::/0</b>
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		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.

**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 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.

**Example**

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

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster1	<b>IC1</b>	<b>cluster1-1:e0a</b>	<b>local-only</b>	<b>Default</b>

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.

**Example**

```

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 Data 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 Data ONTAP, display the aliases that Data ONTAP assigned to each device by using the `storage tape alias show` command.

The aliases are often useful in configuring the backup application.

**Example**

```

cluster1::> storage tape show -alias

Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                Alias      Mapping
-----
stsw-3220-4a-4b-02  st2       SN[HU19497WVR]
...
    
```

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

- [\*Clustered Data ONTAP 8.3 Data Protection Tape Backup and Recovery Guide\*](#)  
Describes how to back up and recover data using tape backup and recovery features in clusters, using NDMP, SMTape, and dump technologies.

### Documentation on other types of data protection

- [\*NetApp Documentation: Clustered Data ONTAP Express Guides\*](#)  
Specific express guides describe how to configure data protection technologies, such as SnapVault and SnapMirror.
- [\*Clustered Data ONTAP 8.3 Data Protection Guide\*](#)  
Describes how to plan and manage disaster recovery and disk-to-disk backup of clustered systems.

## Copyright information

---

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

## Trademark information

---

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

## How to send comments about documentation and receive update notification

---

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 to [doccomments@netapp.com](mailto: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., 495 East Java Drive, 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 [11](#)
    - configuring LIFs for NDMP [12](#)
    - enabling NDMP service [10](#)
  - aliases
    - gathering for configuring the backup application [18](#)
- B**
- backup
    - where to get information about configuring [20](#)
  - backup applications
    - configuring [18](#)
    - verifying support for [6](#)
  - backup users
    - configuring for the cluster or admin SVM [11](#)
    - configuring for the node [15](#)
- C**
- CAB
    - identifying support for [6](#)
  - choosing
    - where to configure NDMP [9](#)
  - Cluster Aware Backup
    - See* CAB
  - clusters
    - configuring a backup user for [11](#)
  - comments
    - how to send feedback about documentation [23](#)
  - configuring
    - backup user for the cluster or admin SVM [11](#)
    - backup user for the node [15](#)
    - LIFs for node-scoped NDMP [16](#)
    - LIFs for SVM-scoped NDMP [12](#)
    - NDMP, workflow [5](#)
    - node-scoped NDMP [15](#)
    - SVM-scoped NDMP [10](#)
- D**
- data management applications
    - See* backup applications
  - Data ONTAP
    - viewing tape devices and media changers in [8](#)
    - data protection
      - where to get information about configuring [20](#)
  - DMAs
    - See* backup applications
  - documentation
    - additional information about tape backup and restore [20](#)
    - how to receive automatic notification of changes to [23](#)
    - how to send feedback about [23](#)
- E**
- enabling
    - node-scoped NDMP and NDMP service [15](#)
    - reservations for NDMP [9](#)
    - SVM-scoped NDMP and NDMP service [10](#)
  - express guides
    - additional documentation on data protection [20](#)
    - NDMP configuration workflow [5](#)
    - requirements for using NDMP Configuration Express Guide [4](#)
  - extension
    - See* CAB
- F**
- feedback
    - how to send comments about documentation [23](#)
  - flowcharts
    - NDMP configuration workflow [5](#)
- G**
- gathering information
    - required by the backup application [18](#)
- I**
- IMT
    - verifying planned configuration for NDMP tape access [6](#)
  - information



how to send feedback about improving documentation [23](#)

## L

### LDAP

configuring a user for NDMP backup [11](#)

### LIFs

configuring for node-scoped NDMP [16](#)  
 configuring for SVM-scoped NDMP [12](#)  
 verifying prerequisites for NDMP configuration [6](#)

## M

### media changers

viewing information about [8](#)

## N

### NDMP

configuring a backup user for the cluster [11](#)  
 configuring for a node [15](#)  
 configuring LIFs for node-scoped [16](#)  
 configuring LIFs for SVM-scoped [12](#)  
 configuring SVM-scoped [10](#)  
 configuring the backup user for nodes [15](#)  
 enabling node-scoped [15](#)  
 enabling SVM-scoped [10](#)  
 enabling tape reservations [9](#)  
 requirements for using Express Guide to configure [4](#)  
 verifying planned configuration for tape access [6](#)  
 where to get information about configuring [20](#)  
 workflow for configuring [5](#)

### NDMP service

enabling on the admin SVM [10](#)  
 enabling on the node [15](#)

### Network Data Management Protocol

*See* NDMP

### NIS

configuring a user for NDMP backup [11](#)

### node-scoped NDMP

configuring [15](#)  
 configuring LIFs [16](#)  
 configuring the backup user [15](#)  
 enabling [15](#)

### nodes

configuring a backup user for [15](#)  
 configuring a LIF for node-scoped NDMP [16](#)  
 enabling NDMP service [15](#)

## P

### planned configuration

verifying [6](#)

## R

### requirements

for using NDMP Configuration Express Guide [4](#)

### reservations

tape, enabling for NDMP operations [9](#)

### restoring backups

where to get information [20](#)

### root users

configuring a root user for each node [15](#)

## S

### suggestions

how to send feedback about documentation [23](#)

### support

for planned configuration, verifying [6](#)

### SVM-scoped NDMP

configuring [10](#)  
 configuring a backup user for [11](#)  
 configuring LIFs [12](#)  
 enabling [10](#)

## T

### tape backup

requirements for using Express Guide to configure [4](#)

### tape backup and restore

where to get information [20](#)

### tape configuration files

displaying and updating [6](#)

### tape devices

viewing in Data ONTAP [8](#)

### tape drives

verifying support for [6](#)

### tape reservations

enabling for NDMP [9](#)

### twitter

how to receive automatic notification of documentation changes [23](#)

## V

verifying

## 26 | NDMP Configuration Express Guide

supported drives [6](#)  
viewing  
tape devices and media changers in Data ONTAP [8](#)

NDMP configuration [5](#)

## W

workflows