



# **Configure node-scoped NDMP**

## **ONTAP 9**

NetApp  
April 27, 2023

# Table of Contents

- Configure node-scoped NDMP ..... 1
  - Enable node-scoped NDMP on the cluster ..... 1
  - Configure a LIF..... 2

# Configure node-scoped NDMP

## Enable node-scoped NDMP on the cluster

You can back up volumes hosted on a single node by enabling node-scoped NDMP, enabling the NDMP service, and configuring a LIF for data and control connection. This can be done for all nodes of the cluster.



Node-scoped NDMP is deprecated in ONTAP 9.

### About this task

When using NDMP in node-scope mode, authentication must be configured on a per-node basis. For more information, see [the Knowledge Base article "How to configure NDMP authentication in the 'node-scope' mode"](#).

### Steps

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

```
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.

```
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.

```
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.

```
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.

## Configure 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.



Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see [Configure firewall policies for LIFs](#).

### Steps

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

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

Current Is	Logical	Status	Network	Current	
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.

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	-
		**ndmp	0.0.0.0/0, ::/0**
		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.

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
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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
```

## Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.