■ NetApp

Configure SVM-scoped NDMP

ONTAP 9

NetApp September 13, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/ndmp/configure-svm-scoped-ndmp-task.html on September 13, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Configure SVM-scoped NDMP	
Configure SVM-scoped NDMP overview	
Enable SVM-scoped NDMP on the cluster	
Configure a backup user for the cluster	
Configure LIFs	

Configure SVM-scoped NDMP

Configure SVM-scoped NDMP overview

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.

What you'll need

The CAB extension must be supported by the DMA.

Enable 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.

```
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.

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

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



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

Configure 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.

What you'll need

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 <code>-user-or-group-name</code> parameter.

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.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

Vserver: cluster1
   User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configure 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.

Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies.

For more information, see LIFs and service policies in ONTAP 9.6 and later.

Steps

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

The following command displays the intercluster LIFs:

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

The following command displays the cluster-management LIF:

cluster1::>	network interface	show -role	cluster-mgmt	
	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port Home	Э			
cluster1	cluster_mgmt	up/up	192.0.2.60/24	cluster1-2
e0M true	е			

The following command displays the node-management LIFs:

cluster1	.::>	network interface	show -role	node-mgmt	
		Logical	Status	Network	Current
Current	Is				
Vserver		Interface	Admin/Oper	Address/Mask	Node
Port	Home	Э			
cluster1	-	cluster1-1_mgmt1	up/up	192.0.2.69/24	cluster1-1
e0M	true	Э			
		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.

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	http https ** ndmp ndmps ntp rsh snmp ssh	0.0.0.0/0** 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0	
10 entries	were display	ed.		

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
                           0.0.0.0/0, ::/0**
                   **ndmp
                   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
                   **ndmp
                           0.0.0.0/0, ::/0**
                           0.0.0.0/0, ::/0
                   ndmps
                           0.0.0.0/0, ::/0
                   ntp
                   rsh
                           0.0.0.0/0, ::/0
                   snmp
                           0.0.0.0/0, ::/0
                   ssh
                   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.

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.

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

	Tanàna 1	II	D- : 1
Failover	Logical	Home	Failover
Vserver Group	Interface		Policy
cluster	cluster1_clus1	cluster1-1:e0a	local-only
Targets:			Failover
<u>5</u>			
**cluster1 wide Defau	—	cluster1-1:e0m	broadcast-domain-
Targets:			Failover
<u> </u>			• • • • • •
Default**	**IC1	cluster1-1:e0a	local-only
Targets:			Failover
Default**	**IC2	cluster1-1:e0b	local-only
Targets:			Failover
-	-1 cluster1-1_mgmt1	cluster1-1:e0m	local-only
Targets:			Failover
cluster1 Default	-2 cluster1-2_mgmt1	cluster1-2:e0m	local-only
Targets:			Failover
rargees.			

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.

```
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.

```
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.

Copyright Information

Copyright © 2022 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, 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.