NDMP configuration

ONTAP 9

NetApp
April 24, 2024

Table of Contents

NDMP configuration

NDMP configuration overview

You can 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.

If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as *SVM-scoped* or *node-scoped*:

- SVM-scoped at the cluster (admin SVM) level enables you to back up all volumes hosted across different nodes of the cluster. SVM-scoped NDMP is recommended where possible.
- Node-scoped NDMP enables you to back up all the volumes hosted on that node.

If the backup application does not support CAB, you must use node-scoped NDMP.

SVM-scoped and node-scoped NDMP are mutually exclusive; they cannot be configured on the same cluster.

> Node-scoped NDMP is deprecated in ONTAP 9.

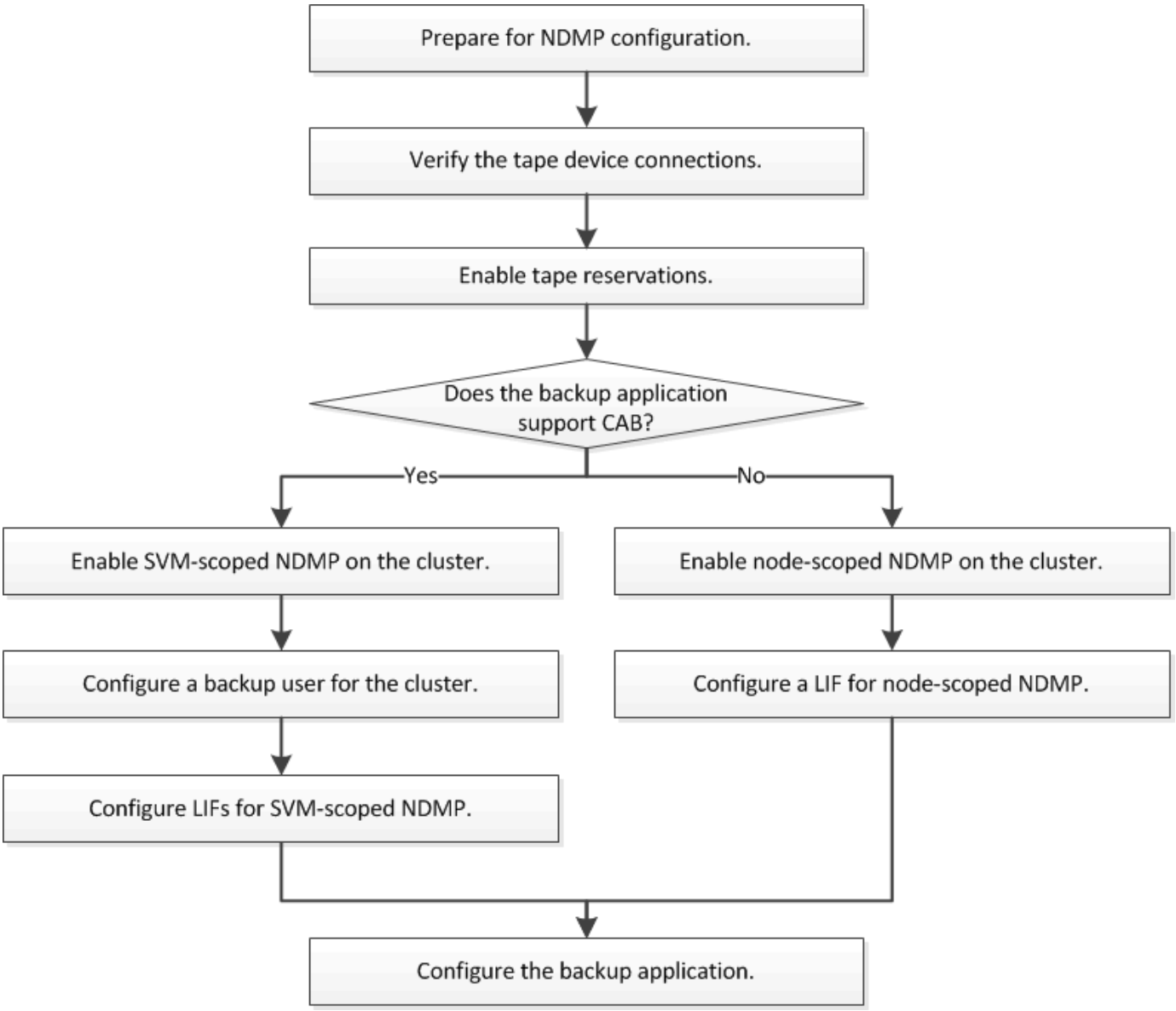
Learn more about Cluster Aware Backup (CAB).

Before configuring NDMP, verify the following:

- You have a third-party backup application (also called a Data Management Application or DMA).
- You are a cluster administrator.
- 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.

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.



Prepare 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. Refer to your backup application provider's compatibility matrix for ONTAP support (NetApp does not qualify third-party backup applications with ONTAP or NDMP).

   You should verify that the following NetApp components are compatible:

   - The version of ONTAP 9 that is running on the cluster.
   - The backup application vendor and version: for example, Veritas NetBackup 8.2 or CommVault.

- The tape devices details, such as the manufacturer, model, and interface of the tape drives: for example, IBM Ultrium 8 or HPe StoreEver Ultrium 30750 LTO-8.
- The platforms of the nodes in the cluster: for example, FAS8700 or A400.

> You can find legacy ONTAP compatibility support matrices for backup applications in the NetApp Interoperability Matrix Tool.

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.

```
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.

> 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.

```
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
```

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

```
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
```

Network 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.

Verify 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.

```
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
...
```

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.

```
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
...
```

Enable 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.

   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.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                 persistent

   cluster1-2
       tape.reservations                 persistent
   2 entries were displayed.
   ```

Configure SVM-scoped NDMP

Enable SVM-scoped NDMP on the cluster

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, enabling NDMP service on the cluster (admin SVM), and configuring LIFs for data and control connection.

What you'll need

The CAB extension must be supported by the DMA.

About this task

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

Steps

1. Enable SVM-scoped NDMP mode:

```
cluster1::> system services ndmp node-scope-mode off
```

   SVM-scoped NDMP mode is enabled.

2. Enable NDMP service on the admin SVM:

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

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

   For secure communication, you should keep plaintext authentication disabled.

3. Verify that NDMP service is enabled:

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

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Enable a backup user for NDMP authentication

To authenticate SVM-scoped NDMP from the backup application, there must be an administrative user with sufficient privileges and an NDMP password.

About this task

You must generate an NDMP password for backup admin users. You can enable backup admin users at the cluster or SVM level, and if necessary, you can create a new user. By default, the users with the following roles can authenticate for NDMP backup:

- Cluster-wide: `admin` or `backup`
- Individual SVMs: `vsadmin` or `vsadmin-backup`

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

Steps

1. Display the current admin users and permissions:

```
security login show
```

2. If needed, create a new NDMP backup user with the `security login create` command and the appropriate role for cluster-wide or individual SVM privileges.

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

   The following command creates the backup user `backup_admin1` with the `backup` role for the entire cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   The following command creates the backup user `vsbackup_admin1` with the `vsadmin-backup` role for an individual SVM:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Enter a password for the new user and confirm.

3. 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

            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
```

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
----------- ----------        ---------- ------------------
------------- ------- ----
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

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

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

   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:

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

          Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
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.

```
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.

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

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
             Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

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:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode is enabled.

2. Enable NDMP service on all nodes in the cluster:

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:

   Using the wildcard "*" disables the `-clear-text` option on all nodes at the same time.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Verify that NDMP service is enabled and the `-clear-text` option is disabled:

```
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

            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.

      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
            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
```

Configure 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

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.