Technical Report

NDMP in Clustered Data ONTAP for Tape Backup Software Applications

Subhash Athri, NetApp
June 2015 | TR-4376

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 NDMP Backups

The Network Data Management Protocol (NDMP) developed by NetApp is used for controlling backup services to network-attached storage (NAS) devices. NDMP allows data to be transferred between storage devices and backup targets and reduces the load on the backup server.

NDMP specifies a common architecture for the backup of network file servers. This protocol enables the creation of a common agent that a centralized program can use to back up the data on file servers running on different platforms. By separating the data path from the control path, NDMP minimizes demands on network resources and enables localized backups and disaster recovery. With NDMP, heterogeneous network file servers can communicate directly to a network-attached tape device for backup or recovery operations. Without NDMP, administrators must remotely mount NAS volumes on their server and back up or restore the files to directly attached tape library devices.

Most backup applications (also called data management applications, or DMAs) and hardware vendors support NDMP-based backups. NetApp® FAS storage systems can be backed up through NDMP by using its native backup engines: dump and SMTape.

A dump backup writes file system data from disk to a backup target by using a predefined process. Because the dump backup uses NetApp Snapshot® copies to back up the data, the administrator does not need to take the storage system or volume offline before creating the backup. Dump backups traverse the directories to identify the files to be backed up, and the file history (catalog) is sent to the backup application that is managing the NDMP client. Dump also supports incremental backups to tape.

SMTape offers a disaster recovery solution that backs up blocks of data to tape by using Snapshot copies. Unlike dump, SMTape performs backup and recovery operations at the volume level and does not support the backup and restore of files and directories.

Note: Before the 8.0 release of the NetApp Data ONTAP® operating system, SMTape was referred to as SM2T. In releases 8.0, 8.1, and 8.2, SMTape was available only in Data ONTAP operating in 7-Mode. The 8.3 release makes SMTape available in clustered Data ONTAP.

1.1 Tape Backup Topologies in Clustered Data ONTAP

The clustered Data ONTAP operating system supports three tape backup topologies:

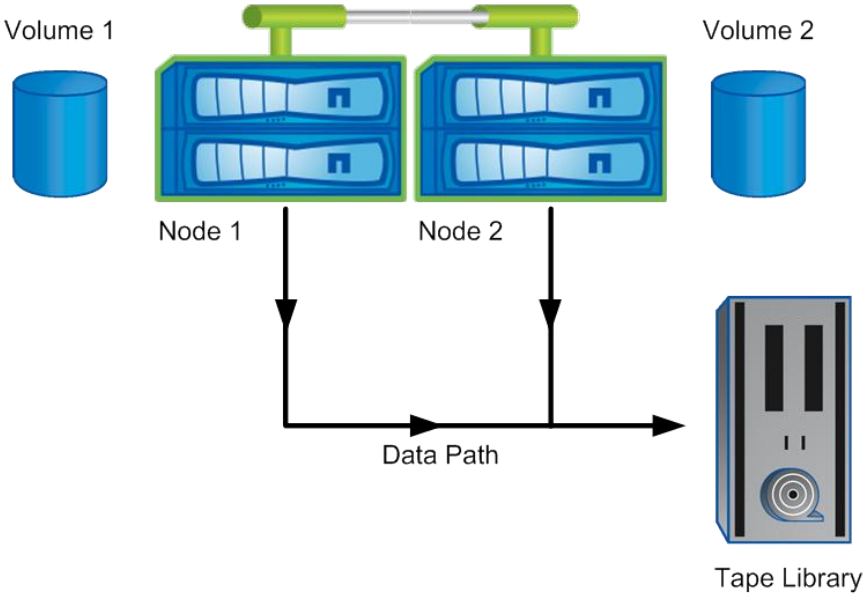
- Local tape backups
- Three-way tape backups
- Remote tape backups

Local Tape Backups

In the local tape backup topology, the volume being backed up and the tape library are colocated on the same node of a clustered Data ONTAP system that runs the cluster-aware backup (CAB) extension. As Figure 1 shows, the tape device is made visible to both nodes in the cluster through FC SAN so that a CAB data management application can drive the local backup to tape for both volume 1 and volume 2, which are hosted on node 1 and node 2, respectively.

For a local backup to tape, the data traverses directly from the controller node that hosts the volume to the tape library.

Figure 1) Local backup to tape.



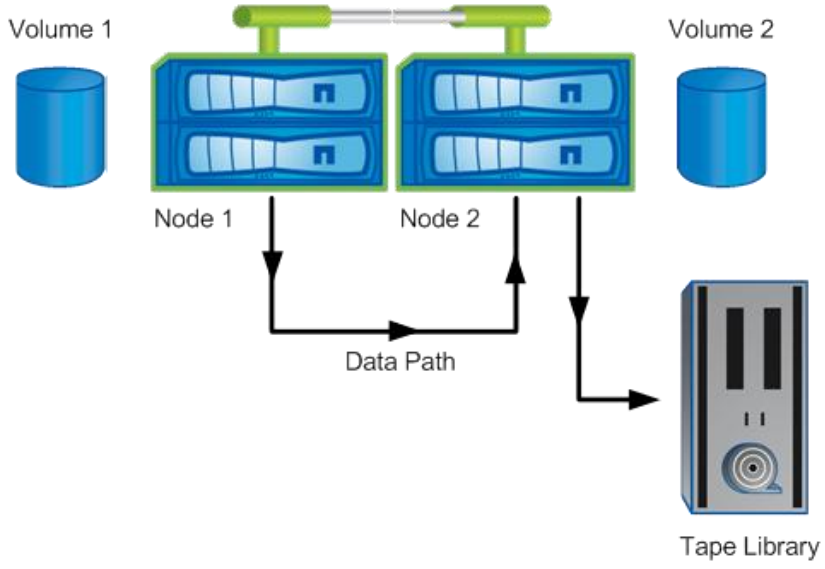
Three-Way Tape Backups

In the three-way tape backup topology, a tape subsystem that is connected to one of the nodes in the cluster is used to back up a volume that is hosted on another node in the same cluster or in a different cluster. As Figure 2 shows, the backup of volume 1 on node 1 follows a three-way path to the tape device because node 1 does not have tape visibility. The backup of volume 2 on node 2, on the other hand, is a local backup to tape because volume and tape are colocated on node 2.

Note: The path for a given backup job (either a three-way backup or a local backup) is defined by the data management application without user intervention, depending on volume and tape colocation.

For a three-way backup to tape, the data traverses from the node that hosts the volume to the node that hosts the tape device before it is written to the tape drive.

Figure 2) Three-way backup to tape.

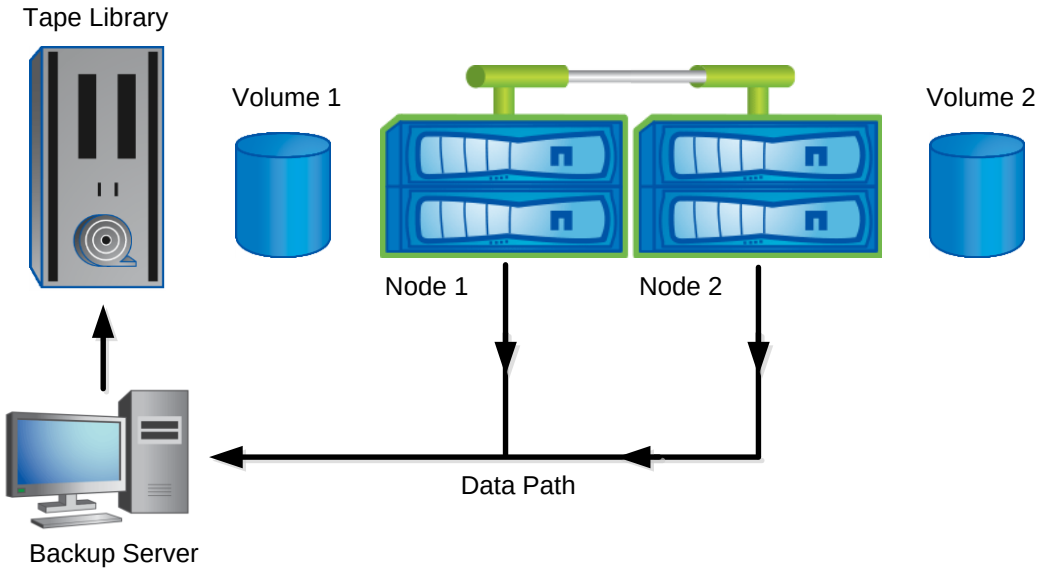


Remote Tape Backups

In the remote backup topology, the tape subsystem is hosted by a backup or media server that belongs to the DMA architecture. This configuration is also known as a storage system-to-server backup architecture.

As Figure 3 shows, the data path for a remote backup to tape is from volume 1 hosted on node 1 and volume 2 hosted on node 2 to the backup server that hosts the tape subsystem.

Figure 3) Remote backup to tape.



1.2 NDMP Modes of Operation in Clustered Data ONTAP

In clustered Data ONTAP 8.2, NDMP has two modes of operation:

- Node-scoped NDMP mode
- Storage virtual machine (SVM)-scoped NDMP mode, also called SVM-aware NDMP mode

In clustered Data ONTAP releases earlier than 8.2, NDMP had only the node-scoped mode of operation. The SVM-aware NDMP mode was introduced in clustered Data ONTAP 8.2 to enable NDMP backups of any SVM instance that is hosted by the cluster. The SVM-aware NDMP mode allows tape backup and restore operations at the SVM level, is available cluster-wide, and supports backups in the global namespace architecture of clustered Data ONTAP systems.

To enable the SVM-aware NDMP feature in clustered Data ONTAP, the CAB extension must be implemented in the NDMP data management application. If the application is not using the CAB extension, NDMP can be operated only in node-scoped mode.

Data ONTAP 8.3 introduces support for the SMTape backup engine in clustered Data ONTAP. SMTape works in SVM-aware NDMP mode only. A data management application that uses the CAB extension can take advantage of SMTape in clustered Data ONTAP environments.

Node-Scoped NDMP Mode

The node-scoped NDMP mode is used when NDMP connections to nodes in the cluster are made locally. For example, in a two-node cluster, the node-scoped NDMP mode allows NDMP sessions to be established for each node separately. Volumes that are hosted by a particular node can be backed up by the NDMP session that is hosted on that same node.

Technically, NDMP backups can be configured on any logical interface (LIF) type that is hosted on the physical interface of a node in the cluster. The only golden rule is that the LIF type hosted on the interface of a node to which the control connection is established must also own the underlying volume. This rule curtails the scope of the backup to the volumes hosted on that node. If a volume is moved to a different node in the cluster, the backup must be reconfigured accordingly.

Table 1 summarizes the tape and volume visibility rules for backup and restore operations performed in node-scoped NDMP mode.

Table 1) Visibility rules for volumes and tape devices in node-scoped NDMP mode.

NDMP Control Connection on LIF Type	Volumes Available for Backup or Restore	Tape Devices Available for Backup or Restore
Node-management LIF	All volumes hosted by the node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes hosted by the node hosting the data LIF	Tape devices connected to the node hosting the data LIF
Cluster-management LIF	All volumes hosted by the node hosting the cluster-management LIF	Tape devices connected to the node hosting the cluster-management LIF
Intercluster LIF	All volumes hosted by the node hosting the intercluster LIF	Tape devices connected to the node hosting the intercluster LIF

SVM-Aware NDMP Mode

The SVM-aware NDMP mode optimizes NDMP backup performance by choosing efficient data transfer paths and being fully compatible with the nondisruptive operations and volume mobility capabilities of clustered Data ONTAP. Backups created in the SVM-aware NDMP mode have the following prerequisites:

- The backup application must be compatible with the SVM-aware NDMP mode.
- The SVM-aware NDMP mode must be enabled in clustered Data ONTAP.

Note: Before configuring NDMP backups, consult the documentation for the backup application to learn which NDMP backup topologies are supported in SVM-aware mode and if this mode is supported at all.

A backup in SVM-aware NDMP mode can be implemented in two ways:

- By configuring a backup policy that applies to the cluster SVM (admin SVM), which can access all volumes in the cluster
- By configuring backup policies for individual SVMs (data SVMs), which can access only the volumes hosted in that respective SVM

  Note: To allow multi-tenancy, configure backup policies for individual SVMs in large enterprises or in cloud environments so that each SVM can have its own backup administrator and backup rules.

Table 2 summarizes the tape and volume visibility rules for backup and restore operations performed in SVM-aware NDMP mode.

Table 2) Visibility rules for volumes and tape devices in SVM-aware NDMP mode.

NDMP Control Connection on LIF Type	Volumes Available for Backup or Restore	Tape Devices Available for Backup or Restore
Node-management LIF	All volumes hosted by the node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM hosting the data LIF	None
Cluster-management LIF	All volumes in the cluster	All tape devices in the cluster
Intercluster LIF	All volumes in the cluster	All tape devices in the cluster

Note: The visibility rules in Table 2 represent the basis of an overall CAB implementation, but backup applications are likely to have their own algorithms for managing visibility. The information in the table corresponds to what is expected; NetApp strongly recommends that you refer to the documentation for your backup application to learn which exact visibility rules and best practices are applicable for volume and tape discovery.

2 NDMP Configuration in Clustered Data ONTAP

2.1 Enable Node-Scoped NDMP Mode

To enable the node-scoped NDMP mode for backups, complete the following steps:

1. Enable NDMP on each node in the cluster.

```
::> system services ndmp on
```

2. Enable the node-scoped NDMP mode.

```
::> system services ndmp node-scoped mode on
```

Note: By default, the node-scoped mode is disabled in clustered Data ONTAP 8.2.

3. Set an NDMP password for the root user on each node.

```
::> system services ndmp password -node node_name
```

4. Get the list of IP addresses that are physically hosted on each node. A node can be a data LIF, an intercluster LIF, or a node-management LIF.
5. Using any of these physical IP addresses, configure the NDMP server through your NDMP-compliant backup application to detect the tape devices and volumes that are attached to the respective nodes.

Note: To define backup selections, always use `/vserver_name/vol_name`. In the clustered Data ONTAP CLI, Vserver is the term used to refer to an SVM.

6. Using an NDMP-compliant backup application, configure backups in node-scoped NDMP mode.

Note: NetApp recommends using a data LIF or the intercluster LIF that is hosted on the node to establish NDMP data connections. The `e0M` port, which hosts the node-management LIF, is allocated less bandwidth; therefore, if you use the node-management LIF for data connections, NDMP backups may suffer performance issues. If, on the other hand, the node-management LIF is hosted on a regular Ethernet port, data connections through the node-management LIF should not lead to performance problems. You can use the NDMP preferred interface role to set the connection.

2.2 Enable SVM-Aware NDMP Mode

To enable the SVM-aware NDMP mode for backups, complete the following steps:

1. Enable the SVM-aware NDMP mode.

```
::> system services ndmp node-scoped mode off
```

2. Ensure that NDMP is in the allowed protocols list on each SVM.

```
::> vserver modify -vserver vserver_name -allowed-protocols ndmp
```

Note: Always append NDMP to the existing allowed protocols list. Do not run the command directly on your production system. If you do so, the command will delete the existing list and just update NDMP.

3. Enable NDMP on an SVM.

```
::> vserver services ndmp on
```

4. Generate a password for the SVM. The password will be used by the backup application to authenticate the NDMP connection.

```
::> vserver services ndmp generate password -vserver vserver_name -user vsadmin
```

Note: For a cluster-wide configuration, use the cluster-management LIF. The default user to authenticate NDMP is `admin`. For an SVM-wide configuration, use a data LIF. The default user for authentication is `vsadmin`. For more information, refer to the "NDMP Authentication Methods" section.

5. Configure the NDMP tape libraries through the backup application.

Note: For information about tape discovery rules, refer to the documentation for the backup application.

3 NDMP Behavior and Features in Clustered Data ONTAP

3.1 NDMP Backups and Volume Move

In the node-scoped NDMP mode, a backup operation after a volume move to an aggregate in another node within the cluster fails because the volume is no longer accessible by the node on which NDMP is configured. The backup can be reconfigured in one of two ways:

- Configure a new NDMP backup policy for the node to which the volume was moved. If you are running an incremental or differential backup sequence, you must create a full backup after the volume move and the backup policy reconfiguration. After you run the full backup, you can start an incremental or differential backup.
- Create a LIF specific to NDMP traffic with the role `data` on each node. Use this LIF to configure NDMP backups. Migrate this LIF to the node to which the volume was moved. By performing these tasks, you can continue to create incremental or differential backups from the last backup. A full backup is not necessary.

  Note: To automate the LIF-specific workflow, you must first associate a LIF with the volume being backed up by NDMP. After the volume is moved, you can then initiate an automated script to migrate the LIF as well. Multiple IP addresses dedicated to NDMP are required for this solution.

Backups in node-scoped NDMP mode and volume move operations interact in the following ways:

- If a volume move request comes in while a backup is in progress, the backup is given precedence over the volume move operation.

- If a backup request comes in during a volume move but before the volume move reaches the cutover phase, the backup and the volume move run in parallel. When the volume move reaches the cutover phase, it is put on hold to wait for the backup to complete. After the backup is complete, the cutover phase is initiated.
- A backup starting after the cutover phase fails if the volume is moved to an aggregate in another node within the cluster. If the volume is moved to a different aggregate in the same node, then the next backup goes through.

In the SVM-aware NDMP mode, the volume move operation is completely transparent to the backup application.

3.2 NDMP Preferred Interface Role

In the SVM-aware NDMP mode, the NDMP `preferred-interface-role` option sets the preferred interface for the NDMP data connection. You can control the LIF types on which the NDMP data connection is established by using this option. The format of the `preferred-interface-role` option is a comma-separated list of LIF types.

The `preferred-interface-role` option is set up in the following way:

- **If the backup client is a cluster LIF**, run the following command:

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

  The admin SVM can have either `intercluster`, `cluster-mgmt`, or `node-mgmt` as its preferred interface role.

  Note: If `intercluster` is the preferred interface role, ensure that the intercluster LIF type is hosted on all nodes of the cluster that hosts the volume being backed up.

- **If the backup client is an SVM (a data LIF)**, run the following command:

```
 ::> vserver services ndmp modify -vserver data-vserver -preferred-interface-role
intercluster,data
```

  A data SVM can have only `intercluster` or `data` as its preferred interface role. If you choose `data` as the preferred interface role, ensure that the data LIF type belonging to the SVM is hosted on each node of the cluster that hosts volumes for that particular SVM-aware NDMP backup.

To establish a data connection, NDMP chooses an IP address that belongs to a LIF type specified by the `preferred-interface-role` option. Preference is given to the first LIF type listed by the option. If that interface is not available, the data connection switches to the next available preferred interface. If the IP addresses do not belong to any of the LIF types, the NDMP data connection cannot be established.

The NDMP data connection preferably should be directed to either the intercluster LIF or a data LIF. The cluster-management LIF hosts the control connection, and the node-management LIF is allocated less bandwidth when it is hosted on the `e0M` port.

Note: In node-scoped NDMP mode, you do not need to set an NDMP preferred interface because the interface that is used to establish the control connection is also used for the data connection.

3.3 NDMP Authentication Methods

Data ONTAP 8.2 supports two methods for authenticating NDMP access to a storage system: plaintext and challenge.

Authentication in Node-Scoped NDMP Mode

In the node-scoped NDMP mode, the challenge and plaintext authentication methods are enabled by default, but the challenge method cannot be disabled. You can enable and disable the plaintext method. In the plaintext method, the login password is transmitted as cleartext.

You must use NDMP-specific credentials to access a storage system in order to perform tape backup and restore operations in node-scoped NDMP mode. The default user ID is `root`. Before using NDMP on a node, ensure that you change the default NDMP password associated with the NDMP user. You can also change the default NDMP user ID.

Authentication in SVM-Aware NDMP Mode

In the SVM-aware NDMP mode, the authentication method is challenge by default. You can enable and disable both the plaintext method and the challenge method.

In this mode, the NDMP user authentication is integrated with role-based access control. In an SVM context, the NDMP user must have either the `vsadmin` or the `vsadmin-backup` role. In a cluster context, the NDMP user must have either the `admin` or the `backup` role. You must generate an NDMP password for a given user account.

Cluster users in the `admin` or `backup` role can access a node-management LIF, a cluster-management LIF, or an intercluster LIF. Users in the `vsadmin-backup` or `vsadmin` role can access only the data LIF. Therefore, depending on the role of a user, the availability of volumes and tape devices for backup and restore operations will vary.

Note: For specific information about visibility rules for the SVM-aware NDMP mode, refer to Table 2.

The SVM-aware NDMP mode also supports user authentication for NIS users and LDAP users, so these users can access multiple SVMs with a common user ID and password. However, NDMP authentication does not support Active Directory users. In this mode, a user account must be associated with the SSH application and the user password authentication method.

In clustered Data ONTAP 8.3, plaintext_sso is a new authentication method that is available along with the plaintext and challenge authentication methods for NDMP access in SVM-aware mode. With this new option, you can have a common password and user across all SVMs with LDAP or NIS integration.

References

The following references and resources were used in this technical report:

- Interoperability Matrix Tool (IMT): http://support.netapp.com/matrix/mtx/login.do
- Presentation: NDMP-Tape Backup Data ONTAP 8.2: https://fieldportal.netapp.com/DirectLink.aspx?documentID=105365&contentID=163626
- TR-3815: Implementing an NDMP Backup Solution Using NetBackup 6.5 and 7.0 on NetApp Storage: https://fieldportal.netapp.com/?oparams=64442
- TR-4200i: SMTape and NDMP Performance Report: Data ONTAP 8.2: https://fieldportal.netapp.com/?oparams=142585

Version History

Version	Date	Document Version History
Version 1.1	June 2015	Unrestricted release
Version 1.0	January 2015	Initial release on Field Portal

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.