Manage SVM-scoped NDMP mode for FlexVol volumes

ONTAP 9

NetApp
November 16, 2022

Table of Contents

Manage SVM-scoped NDMP mode for FlexVol volumes

Manage SVM-scoped NDMP mode for FlexVol volumes overview

You can manage NDMP on a per SVM basis by using the NDMP options and commands. You can modify the NDMP options by using the `vserver services ndmp modify` command. In the SVM-scoped NDMP mode, user authentication is integrated with the role-based access control mechanism.

You can add NDMP in the allowed or disallowed protocols list by using the `vserver modify` command. By default, NDMP is in the allowed protocols list. If NDMP is added to the disallowed protocols list, NDMP sessions cannot be established.

You can control the LIF type on which an NDMP data connection is established by using the `-preferred -interface-role` option. During an NDMP data connection establishment, NDMP chooses an IP address that belongs to the LIF type as specified by this option. If the IP addresses do not belong to any of these LIF types, then the NDMP data connection cannot be established. For more information about the `-preferred -interface-role` option, see the man pages.

For more information about the `vserver services ndmp modify` command, see the man pages.

Related information

Commands for managing SVM-scoped NDMP mode

What Cluster Aware Backup extension does

ONTAP concepts

What SVM-scoped NDMP mode is

System administration

Commands for managing SVM-scoped NDMP mode

You can use the `vserver services ndmp` commands to manage NDMP on each storage virtual machine (SVM, formerly known as Vserver).

If you want to…	Use this command…
Enable NDMP service	`vserver services ndmp on` NDMP service must always be enabled on all nodes in a cluster. You can enable NDMP service on a node by using the `system services ndmp on` command. By default, NDMP service is always enabled on a node.
Disable NDMP service	`vserver services ndmp off`
Display NDMP configuration	`vserver services ndmp show`
Modify NDMP configuration	`vserver services ndmp modify`
Display default NDMP version	`vserver services ndmp version`
Display all NDMP sessions	`vserver services ndmp status`
Display detailed information about all NDMP sessions	`vserver services ndmp probe`
Terminate a specified NDMP session	`vserver services ndmp kill`
Terminate all NDMP sessions	`vserver services ndmp kill-all`
Generate the NDMP password	`vserver services ndmp generate-password`
Display NDMP extension status	`vserver services ndmp extensions show` This command is available at the advanced privilege level.
Modify (enable or disable) NDMP extension status	`vserver services ndmp extensions modify` This command is available at the advanced privilege level.
Start logging for the specified NDMP session	`vserver services ndmp log start` This command is available at the advanced privilege level.

If you want to…	Use this command…
Stop logging for the specified NDMP session	`vserver services ndmp log stop` This command is available at the advanced privilege level.

For more information about these commands, see the man pages for the `vserver services ndmp` commands.

What Cluster Aware Backup extension does

CAB (Cluster Aware Backup) is an NDMP v4 protocol extension. This extension enables the NDMP server to establish a data connection on a node that owns a volume. This also enables the backup application to determine if volumes and tape devices are located on the same node in a cluster.

To enable the NDMP server to identify the node that owns a volume and to establish a data connection on such a node, the backup application must support the CAB extension. CAB extension requires the backup application to inform the NDMP server about the volume to be backed up or restored prior to establishing the data connection. This allows the NDMP server to determine the node that hosts the volume and appropriately establish the data connection.

With the CAB extension supported by the backup application, the NDMP server provides affinity information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and tape device are located on the same node in a cluster.

Availability of volumes and tape devices for backup and restore on different LIF types

You can configure a backup application to establish an NDMP control connection on any of the LIF types in a cluster. In the storage virtual machine (SVM)-scoped NDMP mode, you can determine the availability of volumes and tape devices for backup and restore operations depending upon these LIF types and the status of the CAB extension.

The following tables show the availability of volumes and tape devices for NDMP control connection LIF types and the status of the CAB extension:

Availability of volumes and tape devices when CAB extension is not supported by the backup application

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Data LIF	Only volumes that belong to the SVM hosted by a node that hosts the data LIF	None
Cluster-management LIF	All volumes hosted by a node that hosts the cluster-management LIF	None
Intercluster LIF	All volumes hosted by a node that hosts the intercluster LIF	Tape devices connected to the node hosting the intercluster LIF

Availability of volumes and tape devices when CAB extension is supported by the backup application

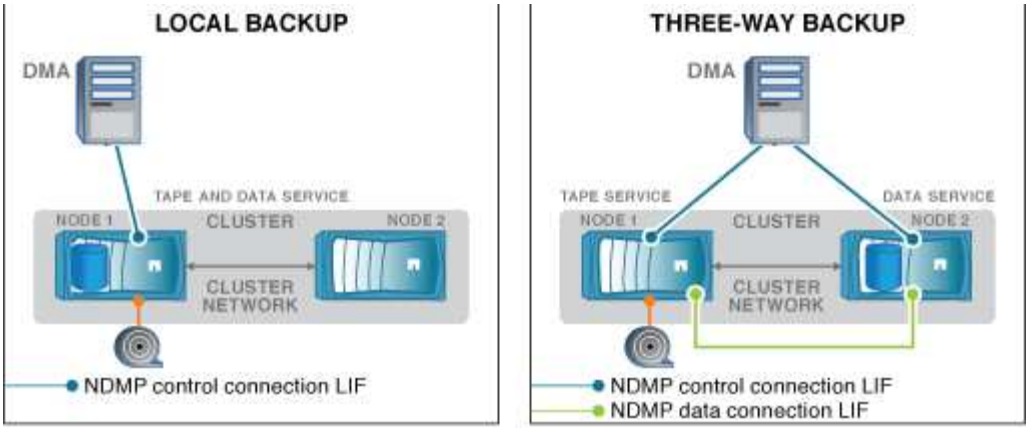
NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM that hosts the data LIF	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

What affinity information is

With the backup application being CAB aware, the NDMP server provides unique location information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and a tape device share the same affinity.

If the NDMP control connection is established on a node management LIF, cluster management LIF, or an intercluster LIF, the backup application can use the affinity information to determine if a volume and tape device are located on the same node and then perform either a local or a three-way backup or restore operation. If the NDMP control connection is established on a data LIF, then the backup application always performs a three-way backup.

Local NDMP backup and Three-way NDMP backup



Using the affinity information about volumes and tape devices, the DMA (backup application) performs a local NDMP backup on the volume and tape device located on Node 1 in the cluster. If the volume moves from Node 1 to Node 2, affinity information about the volume and tape device changes. Hence, for a subsequent backup the DMA performs a three-way NDMP backup operation. This ensures continuity of the backup policy for the volume irrespective of the node to which the volume is moved to.

Related information

What Cluster Aware Backup extension does

NDMP server supports secure control connections in SVM-scoped mode

A secure control connection can be established between the Data Management Application (DMA) and NDMP server by using secure sockets (SSL/TLS) as the communication mechanism. This SSL communication is based on the server certificates. The NDMP server listens on port 30000 (assigned by IANA for “ndmps” service).

After establishing the connection from the client on this port, the standard SSL handshake ensues where the server presents the certificate to the client. When the client accepts the certificate, the SSL handshake is complete. After this process is complete, all of the communication between the client and the server is encrypted. The NDMP protocol workflow remains exactly as before. The secure NDMP connection requires server- side certificate authentication only. A DMA can choose to establish a connection either by connecting to the secure NDMP service or the standard NDMP service.

By default, secure NDMP service is disabled for a storage virtual machine (SVM). You can enable or disable the secure NDMP service on a given SVM by using the `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` command.

NDMP data connection types

In the storage virtual machine (SVM)-scoped NDMP mode, the supported NDMP data connection types depend on the NDMP control connection LIF type and the status of the CAB extension. This NDMP data connection type indicates whether you can perform a local or a three-way NDMP backup or restore operation.

You can perform a three-way NDMP backup or restore operation over a TCP or TCP/IPv6 network. The following tables show the NDMP data connection types based on the NDMP control connection LIF type and

the status of the CAB extension.

NDMP data connection type when CAB extension is supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	LOCAL, TCP, TCP/IPv6
Intercluster LIF	LOCAL, TCP, TCP/IPv6

NDMP data connection type when CAB extension is not supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	TCP, TCP/IPv6
Intercluster LIF	LOCAL, TCP, TCP/IPv6

Related information

What Cluster Aware Backup extension does

Network management

User authentication in the SVM-scoped NDMP mode

In the storage virtual machine (SVM)-scoped NDMP mode, NDMP user authentication is integrated with role-based access control. In the SVM context, the NDMP user must have either the “vsadmin” or “vsadmin-backup” role. In a cluster context, the NDMP user must have either the “admin” or “backup” role.

Apart from these pre-defined roles, a user account associated with a custom role can also be used for NDMP authentication provided that the custom role has the “vserver services ndmp” folder in its command directory and the access level of the folder is not “none”. In this mode, you must generate an NDMP password for a given user account, which is created through role-based access control. Cluster users in an admin or backup role can access a node-management LIF, a cluster-management LIF, or an intercluster LIF. Users in a vsadmin-backup or vsadmin role can access only the data LIF for that SVM. Therefore, depending on the role of a user, the availability of volumes and tape devices for backup and restore operations vary.

This mode also supports user authentication for NIS and LDAP users. Therefore, NIS and LDAP 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.

Related information

Commands for managing SVM-scoped NDMP mode

System administration

ONTAP concepts

Generate an NDMP-specific password for NDMP users

In the storage virtual machine (SVM)-scoped NDMP mode, you must generate a password for a specific user ID. The generated password is based on the actual login password for the NDMP user. If the actual login password changes, you must generate the NDMP-specific password again.

Steps

1. Use the `vserver services ndmp generate-password` command to generate an NDMP-specific password.

   You can use this password in any current or future NDMP operation that requires password input.

   > From the storage virtual machine (SVM, formerly known as Vserver) context, you can generate NDMP passwords for users belonging only to that SVM.

   The following example shows how to generate an NDMP-specific password for a user ID user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. If you change the password to your regular storage system account, repeat this procedure to obtain your new NDMP-specific password.

How tape backup and restore operations are affected during disaster recovery in MetroCluster configuration

You can perform tape backup and restore operations simultaneously during disaster recovery in a MetroCluster configuration. You must understand how these operations are affected during disaster recovery.

If tape backup and restore operations are performed on a volume of anSVM in a disaster recovery relationship, then you can continue performing incremental tape backup and restore operations after a switchover and switchback.

Copyright information

Trademark information