Dell NX3000 with Windows Storage Server 2008 R2 for Compellent Storage Center

Best Practices

This document has been archived and will no longer be maintained or updated. For more information go to the Storage Solutions Technical Documents page on Dell TechCenter or contact support.
## Contents

Document revision................................................................. 3

Contents.................................................................................. 4

General syntax ........................................................................ 5

Conventions.............................................................................. 5

Preface .................................................................................... 6

Audience ................................................................................ 6

Purpose6

Customer support .................................................................... 6

Introduction ............................................................................. 7

Connecting the NX3000 to a Storage Center ................................ 8

Connection Examples .............................................................. 8

Networking.............................................................................. 11

Networking Considerations .................................................... 11

NIC Teaming ........................................................................... 11

Teaming Example .................................................................... 12

Failover Clustering ................................................................... 17

Microsoft Multipath I/O (MPIO).............................................. 18

MPIO Load Balancing Policies ................................................ 18

Verifying MPIO Policy ............................................................ 19

Share and Storage Management ............................................. 20

Shadow Copies of Shared Folders .......................................... 21

Enable and configure Shadow Copies of Shared Folders .......... 21

Recovering data from Shadow Copies ................................... 24

Distributed File System (DFS) ................................................ 24

Network File System (NFS) Integration .................................... 24

Single Instance Storage (SIS).................................................. 25

Introduction to Single Instance Storage (SIS) .......................... 25

Enable or Disable SIS on a Volume ......................................... 26

Uninstall SIS .......................................................................... 27

Manage SIS by using sisadmin.exe ....................................... 28

Examples - sisadmin.exe ...................................................... 29

SIS - known issues .............................................................. 29

Performance Tuning............................................................... 30
General syntax

Table 1. Document syntax

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu items, dialog box titles, field names, keys</td>
<td>Bold</td>
</tr>
<tr>
<td>Mouse click required</td>
<td>Click:</td>
</tr>
<tr>
<td>User Input</td>
<td>Monospace Font</td>
</tr>
<tr>
<td>User typing required</td>
<td>Type:</td>
</tr>
<tr>
<td>Website addresses</td>
<td><a href="http://www.compellent.com">http://www.compellent.com</a></td>
</tr>
<tr>
<td>Email addresses</td>
<td><a href="mailto:info@compellent.com">info@compellent.com</a></td>
</tr>
</tbody>
</table>

Conventions

Notes are used to convey special information or instructions.

Timesavers are tips specifically designed to save time or reduce the number of steps.

Caution indicates the potential for risk including system or data damage.

Warning indicates that failure to follow directions could result in bodily harm.
Preface

Audience
The audience for this document is experienced System Administrators with a basic knowledge of SMB/CIFS and/or NFS as well as basic network knowledge. Readers should have a working knowledge of Windows Server 2008 R2 and the Dell Compellent Storage Center.

Purpose
This document recommends and describes the best practices for administering the Dell NX3000 for Compellent product. The recommendations in this document are provided as starting points that cover the most common uses. Following these guidelines will help efficiently administer the NX3000 and potentially increase performance. For installation procedures, download the Dell NX3000 for Compellent Setup Guide from http://knowledgecenter.compellent.com

Customer support
Dell Compellent provides live support 1-866-EZSTORE (866.397.8673), 24 hours a day, 7 days a week, 365 days a year. For additional support, email Dell Compellent at support@compellent.com. Dell Compellent responds to emails during normal business hours.
Introduction

Based on Microsoft Windows Storage Server 2008 R2, Dell NX3000 for Compellent is a unified SAN/NAS solution that is ideal for Microsoft Windows environments. While the Dell Compellent Storage Center uses block-level storage (SAN), the NAS servers use file-level storage. The Dell NX3000 for Compellent provides conversion of NAS data to SAN data, thus integrating the NAS-based server into the Dell Compellent SAN-based Storage Center. The product operates as second-tier storage alongside existing storage and supports the following:

- Common Internet File System (CIFS), Network File System (NFS), Distributed File System (DFS), and Internet (HTTP and HTTPS) protocols for heterogeneous file sharing
- Virtual Disk Service (VDS) Manager for Compellent Storage Center volume provisioning from the NAS interface
- Indexing service available for easy file search
- Single Instance Storage (SIS) for automatic de-duplication at the file level to save disk space and reduce storage costs
- User self-service file restore and previous version recovery via Volume Shadow Copy Services (VSS) for Shared Folders
- Windows File Server consolidation
- Windows Failover Clustering providing highly available file and print services
- Web-based access to files using WebDAV
Connecting the NX3000 to a Storage Center

The NX3000 connects to a Storage Center by either an 8Gb Fibre channel connection, or by a 10Gb iSCSI connection. To provide maximum redundancy, multi-pathing and dual fabrics are recommended. Each NX3000 server should have at least two paths to both Storage Center controllers through two separate switches.

As always with multi-pathing, it is highly recommended to test failure scenarios before going into production. This includes cable, switch and controller failures.

Connection Examples

Note: The following examples do not account for port level redundancy on either Storage Center, but do provide for multi-pathing.

Example showing a 2 Node NX3000 Cluster connected to dual Storage Centers via 8GB Fibre Channel
Example showing a 4 Node NX3000 Cluster connected to dual Storage Centers via 8Gb Fibre Channel

Example showing a 2 Node NX3000 Cluster connected to dual Storage Centers via 10Gb iSCSI
Example showing a 4 Node NX3000 Cluster connected to dual Storage Centers via 10Gb iSCSI
Networking

Networking Considerations

The NX3000 comes with four 1Gb connections on the motherboard, and either four 1Gb ports or two 10Gb ports via expansion card for front-end connectivity. How these network ports are configured and utilized depends heavily on the deployment scenario for the NX3000.

- The four onboard connections are recommended for heartbeat link, and for remote management.
- The expansion card ports are recommended for all front-end connectivity. These ports are designed for off-load functionality providing higher throughput and lower CPU utilization.
- Aggregate interfaces (synonymous with “teams” or “trunks”) can be configured to provide increased network throughput.
- Best performance will come from having an interface in the same subnet as the load.
- It is generally not recommended to have multiple interfaces configured in the same subnet that are not in a trunked to aggregated NIC team. This can cause routing issues and lead to performance problems.

NIC Teaming

NIC teaming takes two or more ports and joins them together to look like a single port to clients. This is typically done to increase performance or availability. Usually this takes place on the server side and not the client side. The switch equipment must understand the type of teaming taking place and “know” that the single server is represented by multiple ports, all of which are receiving the same end-point address.

With the NX3000 server, the ports on the expansion card can be configured as one network interface to serve files out to clients. This is done through the Intel NIC driver that is already installed into the OS.

The example below illustrates one possible network configuration. The most likely scenario would be to combine all four ports into a team for performance. Since the network switch must also support the configuration, one possible example is shown. Network administrators need to verify and confirm what steps are necessary to allow teaming to work in their environment.

The exact switch configuration needed varies from vendor to vendor and even between model and firmware levels. Administrators should install and test all configurations in a development environment before implementing into the end-user production environment.
Teaming Example

The following example shows one case of teaming setup using the quad-port expansion card. All site configurations are different and while the exact steps and adapter names shown here may differ for your site, the overall process and concepts are similar.

Note: To team the ports on the 10Gb expansion card, follow the instructions below using the adapters labeled “Intel(R) Ethernet Server Adapter X520-2”.

1. Go to the Network Connection Properties window on the NX3000.

2. Right click on one of the Local Area Connection icons to see the pop-up menu from which you can set properties.

3. Click Properties for one of the ports labeled “Intel(R) Gigabit ET Quad Port Server Adapter”. In this example, Local Area Connection 5 was selected. The Local Area Connections 5 Properties window is displayed.
4. Click the Configure button. The Network Connections Properties window is displayed.
5. Choose the Teaming tab to display the following window.

6. Check the “Team this adapter with other adapters” box and click the “New Team” button. This opens the New Team Wizard.

7. Assign a team name or accept the default name. In this example, a new team name of Team#0 was entered.

8. Press Next to continue.
9. Select the adapters to include in the team. The team can consist of two, three, or all ports on the expansion card. In this example, all ports will be used in the team.

10. Click Next to continue.

Note: At this point, the administrator must decide what type of team is required. Each team is slightly different and operates in a unique way. Contact your network administrator to determine which type of teaming is appropriate for your infrastructure. **Dynamic Link Aggregation** is recommended for maximum throughput to the NX3000.

11. Choose an appropriate team type for your requirements and click “Next” to continue. For this example, the **IEEE 802.3ad Dynamic Link Aggregation** option was chosen.
12. Click Finish to finalize your selections.

13. The expected result is a window that displays the new interface with the name given to the new team. In this example, the Team Properties window shows the new Team#0.

14. Click OK to close the window.
When you return to the Network Connections window, it now shows a new “Local Area Connection 9” icon that represents the members of the newly created team.

15. To assign an IP address and configure other settings for the team, open the properties of the newly created team adapter. Settings applied to this adapter will apply to all adapters included in the team.

Failover Clustering

The Dell NX3000 for Compellent is purchased as a clustered solution. Dell Compellent supports up to four (4) nodes in a single Failover Cluster instance, with a minimum of two (2) nodes required for a Failover Cluster. Failover Clustering provides the capability to tie multiple servers together to offer high availability for business-critical applications and services. It can also improve performance if multiple volumes are used and resources are balanced across the cluster nodes.

For guidance in setting up a Windows Failover Cluster, please refer to the document titled “How To Setup a Microsoft Windows Server 2008 Failover Cluster” located on Dell Compellent Knowledge Center.

More detailed information about Failover Clustering can be found at Microsoft’s official cluster website.
Microsoft Multipath I/O (MPIO)

Microsoft Multipath I/O (MPIO) is a framework that allows administrators to configure load balancing and failover processes for Fibre Channel and iSCSI connected storage devices.

Although Dell Compellent Storage Centers provide redundancy and failover with multiple controllers and RAID, servers still need a way to spread the I/O load and handle internal failover form one path to the next. This is where MPIO plays an important role. Without MPIO, servers see multiple instances of the same disk device in Disk Management.

MPIO Load Balancing Policies

Microsoft offers five different load balancing policies to choose from:

- **Fail Over Only**
  - Policy that does not perform load balancing. This policy uses a single active path, and the rest of the paths are standby paths. The active path is used for sending all I/O. If the active path fails, then one of the standby paths is used. When the path that failed is reactivated or reconnected, the standby path that was activated returns to standby.

- **Round Robin**
  - Load balancing policy that allows the Device Specific Module (DSM) to use all available paths for MPIO in a balanced way. This is the default policy that is chosen when the storage controller follows the active-active model and the management application does not specifically choose a load-balancing policy.

- **Round Robin With Subset**
  - Load balancing policy that allows the application to specify a set of paths to be used in a round robin fashion, along with a set of standby paths. The DSM uses paths from a primary pool of paths for processing requests as long as at least one of the paths is available. The DSM uses a standby path only when all the primary paths fail. For example, given 4 paths: A, B, C, and D, paths A, B, and C are listed as primary paths and D is the standby path. The DSM chooses a path from A, B, and C in round robin fashion as long as at least one of them is available. If all three paths fail, the DSM uses D, the standby path. If paths A, B, or C become available, the DSM stops using path D and switches to the available paths among A, B, and C.

- **Least Queue Depth**
  - Load balancing policy that sends I/O down the path with the fewest currently outstanding I/O requests. For example, consider that there is one I/O that is sent to LUN 1 on Path 1, and the other I/O is sent to LUN 2 on Path 1. The cumulative outstanding I/O on Path 1 is 2, and on Path 2, it is 0. Therefore, the next I/O for either LUN will process on Path 2.

- **Weighted Paths**
  - Load balancing policy that assigns a weight to each path. The weight indicates the relative priority of a given path. The larger the number, the lower ranked the priority. The DSM chooses the least-weighted path from among the available paths.

- **Least Blocks**
  - Load balancing policy that sends I/O down the path with the least number of data blocks currently being processed. For example, consider that there are two I/Os: one is 10 bytes and the other is 20 bytes. Both are in process on Path 1, and there are no outstanding I/Os on Path 2. The cumulative outstanding amount of I/O on Path 1 is 30 bytes. On Path 2, it is 0. Therefore, the next I/O will process on Path 2.
**Note:** Dell Compellent recommends using **Round Robin** as the MPIO policy for all Storage Center volumes attached to the NX3000. Round Robin is designed to load balance across all available I/O paths, thus increasing throughput to the Storage Center volumes. When connected properly, path failover will only suffer a loss of maximum throughput, with no loss of connectivity.

**Verifying MPIO Policy**

MPIO policies are set on a per-volume basis. To verify the MPIO policy set on a specific Storage Center volume, perform the following tasks:

1. Open Device Manager by clicking **Start ➔ Control Panel ➔ then click on “Device Manager”**
2. Expand “Disk Drives”

   ![Device Manager](image)

3. Right-Click on one of the Compellent Volumes, and choose **Properties**

   ![Properties](image)
4. Click the “MPIO” tab
5. Verify “Round Robin” is set as the MPIO Policy

Please refer to the document titled “Dell Compellent Storage Center Microsoft Multipath (MPIO) Best Practices” located on Dell Compellent Knowledge Center for more information regarding setup and configuration of Microsoft MPIO.

Share and Storage Management
With the Share and Storage Management snap-in provided with Windows Storage Server 2008 R2, you can more easily set up and manage shared folders and storage. Share and Storage Management provides the following:

- MMC-based management of shared folders and storage.
- Provision Storage Wizard for creating and configuring storage for file sharing and block sharing, including creating LUNs on storage subsystems, as well as creating and formatting volumes on LUNs or server disks.
- Provision a Shared Folder Wizard for creating and configuring shared folders that can be accessed by using either the server message block (SMB) or NFS protocol.
- Single Instance Storage (SIS) can be enabled or disabled for each volume that is displayed in Share and Storage Management. SIS recovers disk space by reducing the amount of redundant data stored on a volume. It identifies identical files, storing only a single copy of the file in the SIS Common Store and replacing the files with pointers to the file in the SIS Common Store.

The Share and Storage Management snap-in makes it possible to complete most of the administrative tasks that are required to create and manage shared folders and volumes without having to use the Shared Folder Management, Storage Manager for SANs, or Disk Management snap-ins. These tasks include configuring quotas to restrict the quantity of data, configuring file screening to prevent certain file types or only allowing certain file types defined by the administrator, and enabling indexing.

Share and Storage Management includes the following tabs for managing shared folders and volumes:

- **Volumes**
  This tab displays all volumes that are available to the server and information about each volume. From here you can track and manage volumes.

- **Shares**
  This tab displays all shared folders created by using Share and Storage Management and information about each shared folder. From here you can track and manage shared folders.
Note: In order to use the Share and Storage Management snap-in, you must first install the Compellent Virtual Disk Service (VDS) Manager 5. Detailed installation and configuration instructions for the Compellent VDS can be found in the document titled “Storage Center Virtual Disk Service (VDS) Manager 5 for Microsoft Servers User Guide” located on Dell Compellent Knowledge Center.

Shadow Copies of Shared Folders

Utilizing the Microsoft Volume Shadow Copy Service (VSS), Shadow Copies of Shared Folders provides point-in-time copies of files that are located on shared resources, such as a file server. With Shadow Copies of Shared Folders, users can view files and folders as they existed at points of time in the past.

Note: Shadow Copies of Shared Folders can only be set on a per-volume basis. You cannot select specific shared folders and files on a volume to be copied or not copied.

Enable and configure Shadow Copies of Shared Folders

1. Click Start → Administrative Tools → Computer Management
2. In the console tree, right-click Shared Folders → All Tasks → Configure Shadow Copies

3. In Select a volume, click the volume that you want to enable Shadow Copies of Shared Folders for, and then click Enable.

4. Click Yes to continue
5. To make changes to the default schedule and storage area, click Settings

![Settings Window]

6. Click Schedule to change the default backup schedule for shadow copies

![Schedule Window]

**Note:** By default, backups occur at 7:00 AM and 12:00 PM daily. Adjust this schedule to best accommodate your system and user requirements.

For further information about configuring Shadow Copies of Shared Folders, please refer to [Best Practices for Shadow Copies of Shared Folders](#)
Recovering data from Shadow Copies

Users can recover and restore files and folders from Shadow Copies on their local PC using the Shadow Copies for Shared Folders client. This client is built into the OS beginning with Windows XP SP2. Users running earlier operating systems can download the client from Microsoft.

To restore a file or folder from a previous version right-click on the file or folder, select Properties, click on the Previous Versions tab, and then select a restore point from which you’d like to restore the file or folder.

Distributed File System (DFS)

DFS allows users to view files distributed across multiple servers or volumes that appear as if they reside in one directory structure. The decision to implement a DFS namespace in your environment largely depends on your network topology, and the amount of data that you need to share to your users.

DFS can be implemented in one of two ways, either as a stand-alone root distributed file system, or as a domain distributed file system.

**Note:** Although DFS design and implementation is beyond the scope of this document, Dell Compellent recommends implementing a domain distributed file system to aid in server consolidation and management. Windows Storage Server 2008 R2 automatically publishes the DFS mapping to Active Directory. This ensures that the DFS namespace is always visible to users on all servers in the domain.

DFS Replication keeps folders synchronized between servers across limited bandwidth network connections. DFS Replication in Windows Storage Server 2008 R2 includes the ability to add a failover cluster as a member of a replication group. For more information about adding a failover cluster to a replication group, see Add a Failover Cluster to a Replication Group.

For more information about DFS, please refer to the DFS management page on Microsoft TechNet.

Network File System (NFS) Integration

In Windows Storage Server 2008 R2, NFS is implemented to allow UNIX users access to folders and files located on Windows Servers. Windows and UNIX operating systems use different account and security systems. Windows operating systems represent users and groups with a unique security identifier (SID), while UNIX operating systems represent users with user identifiers (UIDs), and group identifiers (GIDs). Account mapping is the process of correlating the UNIX UIDs and GIDs to corresponding Windows user and group SIDs.

There are a number of account mapping methods available in Windows Storage Server 2008 R2. These methods can be divided into the following categories:

- **Mapped user access**
  - This method is typically used when files and folders are shared using both the NFS and SMB protocols.
  - The 3 Mapped user access methods are as follows:
• Account mapping using Active Directory Domain Services
• Account mapping using Active Directory Lightweight Directory Services
• Account mapping using User Name Mapping service

• **Unmapped access**
  • This method is typically used when the files and folders are shared using only the NFS protocol.
  • The 2 Unmapped user access methods are as follows:
    • Anonymous access
    • Unmapped UNIX User Access

*Note:* Depending on your NFS solution, you may need to use a combination of the account mapping methods listed above. Consult your UNIX administrator to develop an account mapping strategy that works for your specific network configuration.

For more information regarding NFS account mapping and deployment, please refer to the [NFS Account Mapping Whitepaper](#).

---

**Single Instance Storage (SIS)**

**Introduction to Single Instance Storage (SIS)**
The Single Instance Storage (SIS) feature included with Windows Storage Server 2008 R2 reduces the amount of space that is used to store data on a volume. SIS does this by replacing duplicate files with a 4K reparse point which points to a single copy of the file in the SIS Common Store. The Common Store is a hidden folder located in the root directory of the volume.

SIS consists of two primary components that together maintain a database of file signatures. These components include:

- **Groveler Service**
  The Groveler service scans the hard-disk volumes on a server for duplicate copies of files. If the service locates duplicate copies of files, the information about the duplicates is sent to the Single Instance Storage Filter. The Groveler service runs as a user-level service.

- **Single Instance Storage Filter**
  The Single Instance Storage Filter is a file system filter service that manages duplicate copies of files on hard-disk volumes. When notified by the Groveler service of duplicated copies of files, this component copies one instance of a duplicate file into a central folder. The duplicate is then replaced by a link (a reparse point) to the central copy. The link file contains information about the original file, such as its current location, size, and attributes. The Single Instance Storage Filter runs in kernel mode.

The Single Instance Storage Filter service cannot be stopped. If this service is disabled, the linked files are not accessible. If the central folder is deleted, the linked files can become permanently inaccessible. If you stop the Groveler service, the files cannot be automatically linked, but the existing linked files can still be accessible.
You can enable SIS on a maximum of 128 volumes per computer. SIS cannot act upon any files that are referenced through junction points, and it cannot be used with any file system except the NTFS file system. SIS will not process files that are 32 kilobytes or less in size.

If you need to access data that is stored on a SIS volume, which might be required for backup and recovery operations, you must either run or have installed Single Instance Storage Filter on your computer.

Backup and recovery via SIS has the following requirements:

- The backup software used must support SIS-enabled volumes.
- The SIS volume, SIS Common Store folder, and reparse points (links) to the files must be restored to a Windows 2000 NTFS version 5.0 (or later) file system or partition that supports reparse points or junction points.
- The Single Instance Storage Filter must be installed or enabled to access the data in the SIS volume.
- The backup program must be capable and configured to backup and restore the reparse points or junction points (links) to the files, and the SIS volume and the SIS Common Store folder must be selected.

For more information about SIS, please refer to Single Instance Store and SIS Backup

Enable or Disable SIS on a Volume

Single Instance Storage (SIS) is enabled or disabled on individual volumes on your storage appliance. When you disable SIS on a volume that has been using SIS, the Groveler service is stopped. SIS can be paused or disabled temporarily by pausing the Groveler service or changing its priority by using the Sisadmin.exe utility.

Once the Groveler service has been paused for a volume, SIS can be removed from that volume using the Sisadmin.exe utility. When SIS is removed from a volume, the files are unlinked from the SIS Common Store and restored to their original locations.

Note: Disabling SIS on a volume will fail if there is not sufficient disk space on the volume to account for each duplicate file and the SIS Common Store.

Membership in the local Administrators group is required to complete this procedure.

To enable SIS on a volume:

1. In Share and Storage Management, on the Volumes tab, click the volume for which you want to enable SIS.
2. In the Actions pane, click Properties.
3. On the Advanced tab, select the Enable SIS on this volume check box, and then click OK.

To disable SIS on a volume:
1. In Share and Storage Management, on the Volumes tab, click the volume for which you want to enable SIS.
2. In the Actions pane, click Properties.
3. On the Advanced tab, select the Enable SIS on this volume check box, and then click OK.

**Note:** Every time you enable or disable SIS on a volume, the Groveler service is restarted. To avoid performance issues when enabling or disabling SIS on a large number of volumes, specify them all in a single command. Grouping the volumes into a single command requires only a single restart of the Groveler service.

**To install SIS on a volume by using sisadmin.exe:**
1. Open an elevated command prompt. Click Start, Accessories, right click Command Prompt, and then click Run as administrator.
2. Type the command `sisadmin.exe /I <volumename>`, where `<volumename>` is the letter name of the volume where SIS is to be enabled.

**To uninstall SIS on a volume by using sisadmin.exe:**
1. Open an elevated command prompt. Click Start, Accessories, right click Command Prompt, and then click Run as administrator.
2. Type the command `sisadmin.exe /u <volumename>`, where `<volumename>` is the letter name of the volume where SIS is to be removed.

**To enable SIS on a volume by using sisadmin.exe:**
1. Open an elevated command prompt. Click Start, Accessories, right click Command Prompt, and then click Run as administrator.
2. Type the command `sisadmin.exe /e <volumename>`, where `<volumename>` is the letter name of the volume where SIS is to be enabled. The Groveler service will be enabled and started for the volume.

**To disable SIS on a volume by using sisadmin.exe:**
1. Open an elevated command prompt. Click Start, Accessories, right click Command Prompt, and then click Run as administrator.
2. Type the command `sisadmin.exe /d <volumename>`, where `<volumename>` is the letter name of the volume where SIS is to be disabled. The Groveler service will be stopped and disabled for the volume.

**Uninstall SIS**
By default, Single Instance Storage (SIS) is installed in Windows Storage Server 2008, but it is not enabled on any volumes. If left in this state it has no impact on system performance and can be left installed. If you decide to proceed with uninstalling SIS from your storage appliance, you must first disable SIS on each volume where it has been applied. Failing to do so may result in lost data.

**Note:** If you have already enabled SIS on one or more volumes on the NX3000 and then decide that you want to uninstall SIS from the Windows Storage Server 2008 R2 operating
system, you must use the SysAdmin.exe command-line tool to “unSIS” the files (i.e., remove all reparse points and restore all copies of the affected files) on all SIS-enabled volumes **before** you can uninstall SIS.

1. On one of the nodes running Windows Storage Server 2008 R2, open Server Manager.
2. In the console tree, expand Roles, click File Services, and then click Remove Role Services.
3. On the Select Role Services page, clear the checkbox Single Instance Storage, click Next, and then click Remove.
4. When prompted to restart the server, click Yes.
5. When the server restarts, confirm that the message on the Removal Results page indicates that Single Instance Storage role service was removed, and then click Close. After you remove SIS from the operating system, the checkbox to enable SIS no longer appears on the properties page for that volume.

**Manage SIS by using sisadmin.exe**

You can enable or disable Single Instance Storage (SIS) on a volume through the Share and Storage Management console, but the primary administration tool is sisadmin.exe. The syntax for sisadmin.exe is:

```
sisadmin.exe [/m <server>] [command]
```

Valid command options for sisadmin.exe include:

- `/m <server>` - This option shifts the focus of the command line to a remote server. If the /m option is not specified, the command line will be applied to the local server. `<server>` can be expressed as a host name, fully qualified domain name (FQDN), or as an IP address.

- `/?` or `/h` - These options displays a list of the valid command options for Sisadmin.exe.

- `/I <volumes>` - Installs SIS for the designated volumes. If SIS is already enabled on the designated volumes this command preserves the current enabled/disabled status.

- `/f <volumes>` - This option sets the Groveler service to run in foreground priority for the designated volumes.

- `/b <volumes>` - This option sets the Groveler service to run in background priority for the designated volumes, which is the default setting for the service.

- `/r <volumes>` - This option initiates a full scan of the designated volumes.

- `/e <volumes>` - This command option enables and starts the Groveler service on the designated volumes.

- `/d <volumes>` - This option stops and then disables the Groveler service on the designated volumes.

- `/v <volumes>` - This option displays statistics for the specified SIS-enabled volumes.
- `/l <volumes>` - This command option displays a list of SIS-controlled files on the designated volumes.

- `/s <files>` - This option displays information about designated SIS-controlled files. `<files>` is expressed as a space delimited list of file names, including path.

- `/u <volumes>` - This option is used to "unSIS" a volume (stop the Groveler service on the volume, restore all file copies, and remove reparse points). This option should always be used on each SIS-enabled volume prior to removing SIS from the server.

  **Note:** For each command option that uses `<volumes>` as a parameter, `<volumes>` represents a space delimited list of volume names (for example: d: e: f: g:).

**Examples - sisadmin.exe**

- To temporarily increase performance levels of the Groveler service on the E: and F: volumes of a server, you might use the following command:
  
  ```
  sisadmin.exe /f E: F:
  ```

- To disable the Groveler service on the E: volume of a server without removing SIS from the volume, you might use the following command:
  
  ```
  sisadmin.exe /d E:
  ```

- To "unSIS" or remove SIS entirely from the F: volume of a remote server using the IP address of the server, you might use the following command:
  
  ```
  sisadmin.exe /m 192.168.1.50 /u F:
  ```

  **Note:** Windows PowerShell includes Cmdlets for administering SIS. For more information about using PowerShell to administer SIS, please see [Single Instance Storage Cmdlets in Windows PowerShell](http://support.microsoft.com/kb/969199).

**SIS - known issues**

**SIS should not be used on sensitive data.**
For information on this issue, see the Microsoft Knowledge Base article at:

[http://support.microsoft.com/kb/969199](http://support.microsoft.com/kb/969199)

**SIS and FSRM may display incorrect disk space.**
If SIS is enabled on a volume, File Server Resource Manager (FSRM) may incorrectly report the amount of disk space usage on that volume for a user. This disparity is because files might be migrating to the SIS Common Store.

**Cannot install SIS on a volume without a mount point.**
If you install SIS on a volume without a mount point (such as a drive letter of folder mount point) the operation will fail while incorrectly displaying a message similar to the following:
SIS has been initialized on volume 'd:\Volume{f2eb8acf-0ad7-49b3-bd92-b93ce5680c85}'. Restarting the Groveler service ...

To resolve this situation, assign a valid mount point to the volume before enable SIS for the volume.

Groveler service may not recognize a volume after the drive letter changes.

SIS requires that all volumes that are using SIS be assigned either a drive letter or a folder mount point. If you use Disk Management to change the mount point or drive letter of a SIS volume, the Groveler service may fail to immediately recognize the new configuration. The Groveler service should adapt to the change within an hour and restore full functionality. To correct the issue, use the sisadmin.exe /I command.

Performance Tuning

Operating System Tuning
For guidance on tuning the performance of the NX3000 operating system, please refer to the following guide: Performance Tuning Guidelines for Windows Server 2008 R2

Server Message Block (SMB) Tuning Parameters
The following set of Windows Registry tuning parameters have been shown to improve SMB performance on the Dell NX3000:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdditionalCriticalWorkerThreads</td>
<td>64</td>
</tr>
<tr>
<td>MaxThreadsPerQueue</td>
<td>64</td>
</tr>
<tr>
<td>NtfsDisable8dot3NameCreation</td>
<td>1</td>
</tr>
</tbody>
</table>

- **AdditionalCriticalWorkerThreads**
  HKLM\System\CurrentControlSet\Control\Session Manager\Executive\(REG_DWORD)

  The default value is 0, which means that no additional critical kernel worker threads are added to the default number. This value affects the number of threads that the file system cache uses for read-ahead and write-behind requests. Raising this value can allow for more queued I/O in the storage subsystem and can improve I/O performance, particularly on systems with many processors and powerful storage hardware.

- **MaxThreadsPerQueue**
  HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\(REG_DWORD)
The default value is 10 (Windows Server 2008) and 20 (Windows Server 2008 R2). Increasing this value raises the number of threads that the file server can use to service concurrent requests. When a large number of active connections need to be serviced and hardware resources (such as storage bandwidth) are sufficient, increasing the value can improve server scalability, performance, and response times.

Note: You will need to create the `MaxThreadsPerQueue` REG_DWORD entry and assign its corresponding value.

- **NtfsDisable8dot3NameCreation**
  HKLM\System\CurrentControlSet\Control\FileSystem\(REG_DWORD)

  The default value is 0. This parameter determines whether NTFS generates a short name in the 8.3 (MS-DOS®) naming convention for long file names and for file names that contain characters from the extended character set. If the value of this entry is 0, files can have two names: the name that the user specifies and the short name that NTFS generates. Changing this value does not change the contents of a file, but it avoids the short-name attribute creation for the file, which also changes how NTFS displays and manages the file. For most SMB file servers, the recommended setting is 1.

**Network Adapter Tuning**

High-performance network adapter features improve in terms of throughput, latency, and scalability of the file server. To benefit from the network adapter’s capability, enable the offloading features by typing in the following command at an elevated command prompt:

- `netsh int tcp set global chimney=enabled rss=enabled autotuninglevel=normal`