IBM System Storage N series

Data ONTAP DSM 3.5 for Windows MPIO Installation and Administration Guide

Contents

Preface

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in *Websites* on page 9).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:
  www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:
  www.ibm.com/storage/support/nseries/
  This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:
  www.ibm.com/systems/storage/network/interophome.html
- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:
  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains

information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in *Websites* on page 9) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in *Websites* on page 9).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in *Websites* on page 9).

> **Note:** If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by e-mail to *starpubs@us.ibm.com*.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Changes to this document: May 2012

Several changes have been made to this document since it was first published.

May 2012 update

In May 2012, this document was updated with the following information for the Data ONTAP DSM 3.5 for Windows MPIO release:

- ALUA requirements were updated to clarify the configurations in which ALUA is required.
  See *ALUA support and requirements* on page 17.
- The list of hotfixes that are required for Windows Server was added.
  See *List of required hotfixes for Windows Server* on page 41.
- Instructions for upgrading the Data ONTAP DSM in Windows cluster configurations were added.
  See *Upgrading Windows cluster configurations* on page 72.
- Instructions for setting up a SAN boot LUN were updated.
  See *Setting up a SAN boot LUN for Windows Server* on page 125.
- Supported Data ONTAP versions were removed from this document. You can find supported Data ONTAP versions in the IBM N series interoperability matrix website (accessed and navigated as described in *Websites* on page 9).

DSM Concepts

The Data ONTAP DSM for Windows MPIO enables you to have multiple Fibre Channel (FC) and iSCSI paths between a Windows host computer and an IBM N series storage system.

Note: FC support includes traditional Fibre Channel and Fibre Channel over Ethernet (FCoE). FCoE is used like traditional FC unless otherwise noted.

Device-specific module overview

The Data ONTAP DSM for Windows MPIO is a device-specific module (DSM) that works with Microsoft Windows MPIO drivers (mpdev.sys, mpio.sys, and mpspfltr.sys) to manage multiple paths between IBM N series storage systems and Windows host computers.

For Windows Server 2003, the DSM installation program installs or upgrades the Windows MPIO components to the version required by the DSM if needed. For Windows Server 2008, the DSM uses the standard MPIO components included with the operating system.

DSM includes storage-system-specific intelligence needed to identify paths and manage path failure and recovery.

You can have multiple optimized paths and multiple non-optimized paths. If all of the optimized paths fail, the DSM automatically switches to the non-optimized paths, maintaining the host's access to storage.

The following illustration shows an example of an FC multipathing topology. The DSM manages the paths from the Windows host to the LUN.
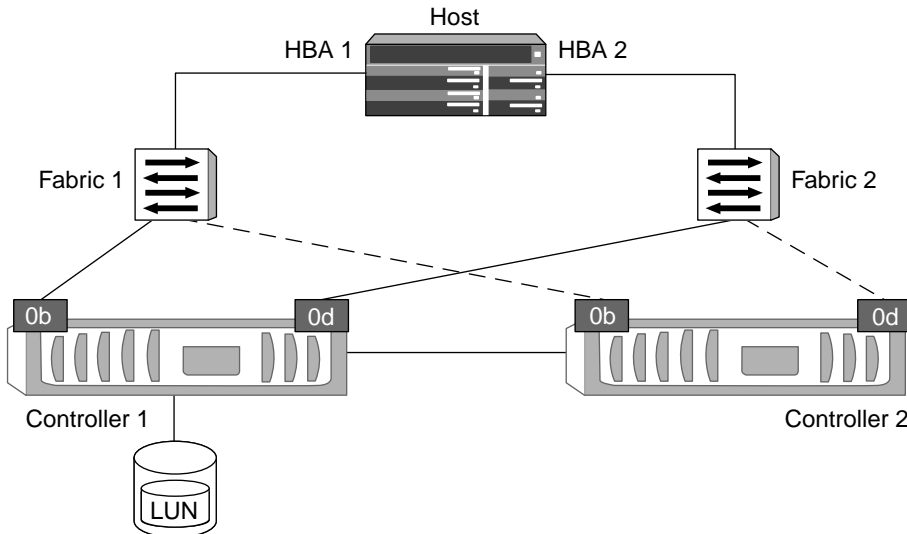
Coexistence with other DSMs

The Data ONTAP DSM claims all LUNs it discovers on IBM N series storage systems. These LUNs have the vendor identifier and product identifier (VID/PID) pair "NETAPP LUN" for Data ONTAP operating in 7-Mode and "NETAPP LUN C-Mode" for Data ONTAP operating in Cluster-Mode. Other DSMs can be used on the same Windows host to claim LUNs from other storage systems with other VID/PID values.

The Microsoft iSCSI Initiator for Windows Server 2003 includes a DSM (msiscsidsm) that can manage the iSCSI paths that use the software initiator. The Data ONTAP DSM and msiscsidsm can co-exist, as long as both versions are listed on the appropriate support matrixes.

Microsoft Windows Server 2008 includes a DSM (msdsm) that can manage FC and iSCSI paths. The msdsm claims any devices not claimed by other DSMs. The Data ONTAP DSM and the msdsm can co-exist as long as the configuration is listed on the appropriate support matrixes.

The Data ONTAP DSM is not intended to be used on the same system as the Veritas DMP DSM.

Tasks required for installing and configuring the DSM

Installing and configuring the DSM involves performing a number of tasks on the host and the storage system.

The required tasks are as follows.

1. Install the DSM.

2. Record the FC and iSCSI initiator identifiers.

3. Create LUNs and make them available as disks on the host computer.

The following tasks are optional, depending on your configuration.

- Change the Fibre Channel cfmode setting of the storage system to single_image.
- Configure SAN booting of the host.

Related concepts

Setting up LUNs on page 117
What FC and iSCSI identifiers are on page 115
Required cfmode setting on page 34

Related tasks

Setting up a SAN boot LUN for Windows Server on page 125
Installing the DSM on page 39

Related information

Changing the Cluster cfmode Setting in Fibre Channel SAN Configurations - www.ibm.com/storage/support/nseries/

Windows configurations supported by the DSM

The DSM supports a number of Windows host configurations.

Depending on your specific environment, the DSM supports the following:

- iSCSI paths to the storage system
- Fibre Channel paths to the storage system
- Multiple paths to the storage system
- Virtual machines using Hyper-V (Windows Server 2008, Windows Server 2008 R2) or Virtual Server 2005 (Windows Server 2003), both parent and guest
- SAN booting

Use the IBM N series interoperability matrix to find a supported combination of host and storage system components and software and firmware versions.

Related information

IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

ALUA support and requirements

Data ONTAP uses ALUA (asymmetric logical unit access) to identify optimized paths. ALUA is required for specific configurations.

ALUA is an industry standard protocol for identifying optimized paths between a storage system and a host. ALUA enables the initiator to query the target about path attributes, such as primary path and secondary path. It also allows the target to communicate events back to the initiator.

ALUA must be enabled for specific configurations.

Windows version	Protocol	Data ONTAP operating mode	ALUA supported and required?
Windows Server 2003	iSCSI	7-Mode	No
		Cluster-Mode	Yes
	Fibre Channel	7-Mode	Yes
		Cluster-Mode	Yes

Windows version	Protocol	Data ONTAP operating mode	ALUA supported and required?
Windows Server 2008	iSCSI	7-Mode	No
		Cluster-Mode	Yes
	Fibre Channel	7-Mode	Yes
		Cluster-Mode	Yes

ALUA support is enabled or disabled on the igroup or igroups to which a LUN is mapped. All igroups mapped to a LUN must have the same ALUA setting. Windows detects a change to the ALUA setting when rebooted.

ALUA is enabled by default on Cluster-Mode igroups. In some situations, ALUA is not automatically enabled on 7-Mode igroups.

> **Note:** Data ONTAP does not support ALUA on single-controller storage systems. Even though ALUA is not supported, the Data ONTAP DSM supports paths to single-controller storage systems. The DSM identifies paths to single-controller storage systems as active/optimized.

Related tasks

Mixing FC and iSCSI paths

The Data ONTAP DSM supports both FC and iSCSI paths to the same LUN for Data ONTAP operating in Cluster-Mode. The DSM does not support both FC and iSCSI paths to the same LUN for Data ONTAP operating in 7-Mode.

> **Note:** FC refers to traditional Fibre Channel and Fibre Channel over Ethernet (FCoE).

Because ALUA is required for FC paths, and ALUA is not supported for iSCSI paths to 7-Mode LUNs, the DSM does not support both FC and iSCSI paths to the same 7-Mode LUN. All paths must have the same ALUA setting.

You can still have FC paths to some 7-Mode LUNs and iSCSI paths to other 7-Mode LUNs.

If you are upgrading from an earlier version of the Data ONTAP DSM and have mixed FC and iSCSI paths to a 7-Mode LUN, you must remove either the FC or the iSCSI paths to the LUN before you enable ALUA and upgrade the DSM.

Related concepts

Microsoft iSCSI DSM

If you are using iSCSI to access another vendor's storage, install the Microsoft iSCSI DSM by selecting the **Microsoft MPIO Multipathing Support for iSCSI** check box when installing the iSCSI initiator for Windows Server 2003.

The Microsoft iSCSI DSM can manage LUNs from other vendors' storage systems.

When both DSMs are installed, the Data ONTAP DSM has priority in claiming iSCSI LUNs on IBM N series storage systems.

I_T and I_T_L nexus overview

An initiator-target (I_T) nexus represents the path from the host's initiator to the storage systems's target. An initiator-target-LUN (I_T_L) nexus represents one virtual disk (LUN) as seen by the DSM. The DSM groups all I_T_L nexuses to the same LUN together, and presents a single virtual disk to the Windows disk manager.

The I_T_L nexus is assigned an eight-character DSM identifier. The identifier is made up of four fields: port, bus, target, and LUN. For example, DSM ID 03000101 represents port 03, bus 00, target 01, and LUN 01.

Each path (I_T nexus) also has an eight-character identifier made up of four fields. The first three fields are the same as the DSM ID: port, bus, and target. The fourth field indicates the path type:

01   Optimized FC paths

02   Non-optimized FC paths

03   • iSCSI paths (Data ONTAP operating in 7-Mode)
       • Optimized iSCSI paths (Data ONTAP operating in Cluster-Mode)

04   Non-optimized iSCSI paths (Data ONTAP operating in Cluster-Mode)

Multiple paths require MPIO software

If you have multiple paths between a storage system and a Windows host computer, you must have some type of MPIO software so that the Windows disk manager sees all of the paths as a single virtual disk.

Multipath I/O (MPIO) solutions use multiple physical paths between the storage system and the Windows host. If one or more of the components that make up a path fails, the MPIO system switches I/O to other paths so that applications can still access their data.

Without MPIO software, the disk manager treats each path as a separate disk, which can corrupt the data on the virtual disk.

Path limits

You can have a maximum of 32 paths to a LUN. This maximum applies to any mix of FC and iSCSI paths. This is a limitation of the Windows MPIO layer.

> **Attention:** Additional paths can be created, but are not claimed by the DSM. Exceeding 32 paths leads to unpredictable behavior of the Windows MPIO layer and possible data loss.

Do not mix 10 Gb and 1 Gb iSCSI sessions to a LUN

Mixing 10 Gb and 1 Gb iSCSI sessions to the same LUN is not supported.

To avoid multipathing problems with iSCSI sessions, use either all 10 Gb sessions or all 1 Gb sessions to a given LUN.

Windows Administrator account requirement

The Windows service installed by the Data ONTAP DSM for Windows MPIO runs under the default SYSTEM account.

When you install the DSM, the default action is to run the Data ONTAP DSM Management Service under the default SYSTEM account.

You can optionally supply the user name and password of an Administrator-level account. If you later change the password of this user-specified account, you must run the **Repair** option of the DSM installation program and enter the new password. You can also update the credentials of the Data ONTAP DSM Management Service in the Windows Services applet.

Related tasks

Timeout and tuning parameters overview

The Data ONTAP DSM for Windows MPIO uses a number of parameters to optimize performance and ensure correct failover and giveback behavior.

You should not change these values unless directed to do so by your storage system support representative.

More information about what each setting does is included in the following topics.

FC HBA and CNA parameters set by Data ONTAP DSM for Windows MPIO

The DSM installer sets required parameters for Fibre Channel host bus adapters (HBA) and converged network adapters (CNA).

The names of the parameters may vary slightly depending on the program. For example, in QLogic SANsurfer, the parameter is displayed as Link Down Timeout. The fcconfig.ini file displays this same parameter as MpioLinkDownTimeOut.

Emulex HBAs and CNAs

For Emulex HBAs and CNAs, the DSM installation program sets the following parameters:

LinkTimeOut=1   The LinkTimeOut parameter specifies the interval after which a link that is down stops issuing a BUSY status for requests and starts issuing SELECTION_TIMEOUT error status. This LinkTimeOut includes port login and discovery time.

NodeTimeOut=10   The NodeTimeOut parameter specifies the interval after which a formerly logged-in node issues SELECTION_TIMEOUT error status to an I/O request. This causes the system to wait for a node that might reenter the configuration soon before reporting a failure. The timer starts after port discovery is completed and the node is no longer present.

QLogic HBAs and CNAs

For QLogic HBAs and CNAs, the DSM installation program sets the following parameters:

LinkDownTimeOut=1   The LinkDownTimeOut parameter controls the timeout when a link that is down stops issuing a BUSY status for requests and starts issuing SELECTION_TIMEOUT error status. This LinkDownTimeOut includes port login and discovery time.

PortDownRetryCount=10   The PortDownRetryCount parameter specifies the number of times the I/O request is re-sent to a port that is not responding in one second intervals.

Registry values set by Data ONTAP DSM for Windows MPIO

The Data ONTAP DSM for Windows MPIO uses a number of Windows registry values to optimize performance and ensure correct failover and giveback behavior. The settings that the DSM uses are based on the operating system version.

The following values are decimal unless otherwise noted. *HKLM* is the abbreviation for HKEY_LOCAL_MACHINE.

Registry key	Value	When set
HKLM\Cluster**ClusSvcHangTimeout**	240	Windows Server 2008 R2 cluster configurations
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**InquiryRetryCount**	6	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**InquiryTimeout**	2	Always
HKLM\SOFTWARE\IBM\MPIO**InstallDir**	`C:\Program Files\IBM \MPIO\`	Always
HKLM\SYSTEM\CurrentControlSet\Control\Class\ {*iSCSI_driver_GUID*}\ *instance_ID*\Parameters **IPSecConfigTimeout**	60	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**iSCSILeastPreferred**	Not set	Not set unless you manually set it
HKLM\SYSTEM\CurrentControlSet\Control\Class\ {*iSCSI_driver_GUID*}\ *instance_ID*\Parameters **LinkDownTime**	30	Always
HKLM\SOFTWARE\IBM\MPIO**LogDir**	`C:\temp \ibm\`	Always
HKLM\SYSTEM\CurrentControlSet\Services\ClusDisk \Parameters**ManageDisksOnSystemBuses**	1	Always
HKLM\SYSTEM\CurrentControlSet\Control\Class\ {*iSCSI_driver_GUID*}\ *instance_ID*\Parameters **MaxRequestHoldTime**	60	Always
HKLM\SYSTEM\CurrentControlSet\Control\MPDEV **MPIOSupportedDeviceList**	"NETAPP LUN", "NETAPP LUN C-Mode"	Always
HKLM\SYSTEM\CurrentControlSet\Services\mpio \Parameters**PathRecoveryInterval**	40	Windows Server 2008 or 2008 R2 only
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**PathVerifyEnabled**	0	Always

Registry key	Value	When set
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**PersistentReservationKey**	A unique generated binary value	Windows Server 2003 only
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**PDORemovePeriod**	130	Always
HKLM\SOFTWARE\IBM\MPIO**ProductVersion**	Installed version of Data ONTAP DSM for Windows MPIO	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**Protocols**	3	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**ReservationRetryInterval**	1	Windows cluster configurations
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**ReservationTimeout**	60	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**RetryCount**	6	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**RetryInterval**	2	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**SupportedDeviceList**	"NETAPP LUN", "NETAPP LUN C-Mode"	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**TestUnitReadyRetryCount**	6	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**TestUnitReadyTimeout**	2	Always
HKLM\SYSTEM\CurrentControlSet\Services\disk **TimeOutValue**	60	Always
HKLM\SYSTEM\CurrentControlSet\Services\mpio \Parameters**UseCustomPathRecoveryInterval**	1	Windows Server 2008 or 2008 R2 only

Note: If you configure a Windows cluster after installing DSM, run the Repair option of the DSM installation program to set ClusSvcHangTimeout.

ClusSvcHangTimeout setting

The ClusSvcHangTimeout setting controls the interval between heartbeats before Windows Server determines that the cluster service is not responding.

InquiryRetryCount setting

The InquiryRetryCount parameter specifies how many times the DSM retries SCSI inquiry requests to the storage system.

The DSM sends SCSI inquiry requests to the storage system controller to get information about a LUN or about storage system configuration. If a response is not received within the InquiryTimeout time, the request is retried the number of times specified by InquiryRetryCount before failing the request.

InquiryTimeout setting

The InquiryTimeout parameter specifies how long the DSM waits before retrying SCSI inquiry requests of the storage system.

The DSM sends SCSI inquiry requests to the storage system controller to get information about a LUN or about storage system configuration. If a response is not received within the InquiryTimeout time, the request is retried the number of times specified by InquiryRetryCount before failing the request.

InstallDir setting

The InstallDir parameter specifies the installation directory used by the DSM.

IPSecConfigTimeout setting

The IPSecConfigTimeout parameter specifies how long the iSCSI initiator waits for the discovery service to configure or release ipsec for an iSCSI connection.

The supported value enables the initiator service to start correctly on slow-booting systems that use CHAP.

iSCSILeastPreferred setting

The iSCSILeastPreferred parameter specifies whether the Data ONTAP DSM prioritizes FC paths over iSCSI paths to the same LUN. You might enable this setting if you want to use iSCSI paths as backups to FC paths.

By default, the DSM uses ALUA access states to prioritize paths. It does not prioritize by protocol. If you enable this setting, the DSM prioritizes by ALUA state and protocol, with FC paths receiving priority over iSCSI paths. The DSM uses iSCSI optimized paths only if there are no FC optimized paths available.

This setting applies to LUNs that have a load balance policy of either Least Queue Depth or Round Robin with Subset.

This parameter is not set by default. The allowed values for this setting are "0" (no preference) and "1" (FC preferred).

LinkDownTime setting

The LinkDownTime setting specifies the maximum time in seconds that requests are held in the device queue and retried if the connection to the target is lost.

If MPIO is installed this value is used. If MPIO is not installed, MaxRequestHoldTime is used instead.

LogDir setting

The LogDir parameter specifies the directory used by the DSM to store log files.

ManageDisksOnSystemBuses setting

The ManageDisksOnSystemBuses parameter is used by SAN-booted systems to ensure that the startup disk, pagefile disks, and cluster disks are all on the same SAN fabric.

For detailed information about the ManageDisksOnSystemBuses parameter, see Microsoft Support article 886569.

Related information

[Microsoft support site article 886569](#)

MaxRequestHoldTime setting

The MaxRequestHoldTime setting specifies the maximum time in seconds that requests are queued if connection to the target is lost and the connection is being retried.

After this hold period, requests are failed with "error no device" and the disk is removed from the system. The supported setting enables the connection to survive the maximum expected storage failover time.

MPIOSupportedDeviceList

The MPIOSupportedDeviceList setting specifies that the Windows MPIO component should claim storage devices with the specified vendor identifier and product identifier (VID/PID).

PathRecoveryInterval setting

The PathRecoveryInterval setting specifies how long in seconds the MPIO component waits before retrying a lost path.

The PathRecoveryInterval setting causes the MPIO component to try to recover a lost path that had a transient error before it decides the disk device is no longer available.

Note that this parameter affects all DSMs on the system.

PathVerifyEnabled setting

The PathVerifyEnabled parameter specifies whether the Windows MPIO driver periodically requests that the DSM check its paths.

Note that this parameter affects all DSMs on the system.

PDORemovePeriod setting

This parameter specifies the amount of time that the multipath pseudo-LUN stays in system memory after all paths to the device are lost.

PersistentReservationKey setting

The PersistentReservationKey parameter stores the persistent reservation key generated by the DSM for Windows Server 2003 systems.

The DSM uses a persistent reservation key to track which host in a Microsoft Windows cluster (MSCS) is currently allowed to write to a virtual disk (LUN).

ProductVersion setting

The ProductVersion parameter indicates the version of Data ONTAP DSM for Windows MPIO installed on the host.

Protocols setting

The Protocols parameter specifies which LUNs are claimed by the DSM. Starting with DSM 3.3.1, both FC and iSCSI LUNs are always claimed.

The parameter was used by previous versions of the DSM to specify which types of LUNs are claimed.

ReservationRetryInterval setting

The ReservationRetryInterval parameter is used by the DSM to control persistent reservation handling in a Windows cluster configuration.

ReservationTimeout setting

The ReservationTimeout parameter is equivalent to the TimeOutValue parameter, except that it is specific to persistent reservation commands within Data ONTAP DSM.

RetryCount setting

The RetryCount parameter specifies the number of times the current path to a LUN is retried before failing over to an alternate path.

The RetryCount setting enables recovery from a transient path problem. If the path is not recovered after the specified number of retries, it is probably a more serious network problem.

RetryInterval setting

The RetryInterval parameter specifies the amount of time to wait between retries of a failed path.

This setting gives the path a chance to recover from a transient problem before trying again.

SupportedDeviceList setting

The SupportedDeviceList parameter specifies the vendor identifier (VID) and product identifier (PID) of LUNs that should be claimed by the DSM.

TestUnitReadyRetryCount setting

The TestUnitReadyRetryCount parameter specifies the number of times the DSM sends a SCSI TEST UNIT READY command on a path before marking a path as failed and rebalancing paths.

The DSM sends a SCSI TEST UNIT READY command to the target to verify a path is available for use. Occasionally, the target may fail to respond to the command, so the DSM sends it again.

TestUnitReadyTimeout setting

The TestUnitReadyTimeout parameter specifies the number of seconds the DSM waits between sending SCSI TEST UNIT READY commands.

The DSM sends a SCSI TEST UNIT READY command to the target to verify a path is available for use.

TimeOutValue setting

The disk TimeOutValue parameter specifies how long an I/O request is held at the SCSI layer before timing out and passing a timeout error to the application above.

> **Attention:** Installing the cluster service on Windows 2003 changes the disk TimeOutValue. Upgrading the Emulex or QLogic HBA driver software also changes TimeOutValue. If cluster service is installed or the HBA driver is upgraded after you install this software, use the Repair option of the installation program to change the disk TimeOutValue back to the supported value.

UseCustomPathRecoveryInterval setting

The UseCustomPathRecoveryInterval setting enables or disables use of the PathRecoveryInterval setting.

Note that this parameter affects all DSMs on the system.

Load balance policies determine failover behavior

The DSM chooses one or more active I_T_L nexuses between the LUN on the storage system and the Windows host based on several factors.

The factors include:

- Load balance policy of the LUN
- Whether the path is optimized or non-optimized
- State of all possible paths
- Load on each path

There are six load balance policies that can be used for FC and iSCSI paths:

Least Queue Depth	The Least Queue Depth policy is an "active/active" policy. I/O to the virtual disk is automatically sent on the available path with the smallest current outstanding queue. The queue length is determined at the I_T nexus level and not the LUN path level. This policy enables you to maximize bandwidth utilization without the need for administrator intervention. For FC, the initial paths used are selected in order of optimized paths first, then non-optimized paths. Least Queue Depth is the default policy.
Least Weighted Paths	The Least Weighted Paths policy is an "active/passive" policy. The available path with the lowest weight value is used to access the virtual disk. If multiple paths with the same weight value are available, the DSM selects the path shared with the fewest other LUNs. The weight value can be set from 0 to 2146999999. Set the weight of a path to 0 to always use it when it is available.
Round Robin	The Round Robin policy is an "active/active" policy. All optimized paths to the storage system are used when available.

Round Robin with Subset	The Round Robin with Subset policy is an "active/active" policy. The Round Robin with Subset policy also uses multiple paths. However, you can specify the paths you want used when available.
	By default, all optimized paths are initially selected. To specify the subset, you make individual paths preferred or not preferred. Although you can specify non-optimized (proxy) paths as part of the active subset, this is not recommended.
FailOver Only	The FailOver Only policy is an "active/passive" policy. The FailOver Only policy enables you to manually select a single preferred I_T_L nexus. This I_T_L nexus will be used whenever it is available.
Auto Assigned	The Auto Assigned policy is an "active/passive" policy. For each LUN, only one path is used at a time. If the active path changes to a passive path, the policy chooses the next active path. The Auto Assigned policy does not spread the load evenly across all available local paths.

When to change the load balance policy

The Data ONTAP DSM sets the default load balance policy to Least Queue Depth. This policy provides the best method of distributing I/O to all active optimized LUN paths. Other load balance policies exist for specialized uses. Work with your application vendor to determine if another load balance policy is appropriate.

Path types and Windows clusters affect failover behavior

In addition to the load balance policy, failover behavior is affected by optimized paths, disabled paths, and Windows clusters.

DSM prefers optimized paths

The DSM differentiates between FC optimized (local or non-proxy) and non-optimized (proxy) FC paths.

Non-optimized (proxy) paths use the cluster interconnect between storage system controllers in an active/active configuration (High Availability (HA) pair or storage system cluster) and are less efficient than optimized paths.

Non-optimized paths are not used when optimized paths are available, unless you explicitly set non-optimized paths to active when using the FailOver-only or Round Robin with Subset policy, or you set non-optimized paths to a lower weight using the Least Weighted Paths policy.

Note: Do not make non-optimized paths active, except for brief maintenance work on the optimized paths. For fabric-attached MetroCluster configurations, never make non-optimized paths active manually.

DSM can use disabled paths

If you manually disable an I_T_L nexus, the DSM does not normally fail over to it.

However, if the active I_T_L nexus fails, and there are no enabled I_T_L nexuses available, the DSM will try to enable and fail over to a disabled I_T_L nexus. As soon as an enabled I_T_L nexus is available, the DSM will fail back to the enabled I_T_L nexus and return the I_T_L nexus to the disabled state.

Failover examples

Examples of the failover behavior for different load balance policies demonstrate how the DSM selects active paths.

Least queue depth example

This example demonstrates failover behavior with FC paths to a LUN.

A Windows host has four FC paths to a LUN, two optimized paths to one node (controller) in an active/active storage system configuration and two non-optimized paths to the partner node. The load balance policy is Least Queue Depth.

Although the status of the non-optimized paths is called Active/Non-optimized, these paths are not actively used for I/O as long as an optimized path is available.

Initial path selection with all components working:

- ITL_1 Optimized FC - Used for I/O
- ITL_2 Optimized FC - Used for I/O
- ITL_3 Non-optimized FC - Not used for I/O
- ITL_4 Non-optimized FC - Not used for I/O

I/O between the host and storage system is sent on ITL_1 or ITL_2, depending on which currently has the shorter queue.

After ITL_1 fails, all I/O is sent over ITL_2:

- ITL_2 Optimized FC - Used for I/O
- ITL_3 Non-optimized FC - Not used for I/O
- ITL_4 Non-optimized FC - Not used for I/O

If both ITL_1 and ITL_2 fail, I/O is sent on ITL_3 or ITL_4, depending on which currently has the shorter queue:

- ITL_3 Non-optimized FC - Used for I/O
- ITL_4 Non-optimized FC - Used for I/O

Round robin example

This example demonstrates failover behavior of iSCSI paths using the round robin load balance policy. The example applies to Data ONTAP operating in 7-Mode.

A Windows host has four iSCSI paths to a LUN on a controller in an active/active (HA pair) storage system configuration. The load balance policy is round robin.

For iSCSI, all paths connect to ports on the controller that owns the LUN. If that controller becomes unavailable, all paths fail over to partner ports on the partner controller.

All available iSCSI paths are treated as optimized paths.

Before path failover:

• ITL_1 Optimized iSCSI - Used for I/O
• ITL_2 Optimized iSCSI - Used for I/O
• ITL_3 Optimized iSCSI - Used for I/O
• ITL_4 Optimized iSCSI - Used for I/O

After one active I_T_L nexus (path) fails, the other active I_T_L nexus continues to deliver data:

• ITL_2 Optimized iSCSI - Used for I/O
• ITL_3 Optimized iSCSI - Used for I/O
• ITL_4 Optimized iSCSI - Used for I/O

If the second active I_T_L nexus fails, the two remaining paths continue to serve data:

• ITL_2 Optimized iSCSI - Used for I/O
• ITL_3 Optimized iSCSI - Used for I/O

Round robin with subset example

This example demonstrates failover behavior of FC paths when you select a preferred path using the round robin load balance policy.

A Windows host has four FC paths to a LUN, two paths to each node (controller) in an active/active (HA pair) storage system configuration. The load balance policy is round robin with subset. The administrator has set ITL_1 and ITL_4 as the preferred paths.

Before path failover:

• ITL_1 Optimized FC, Preferred - Used for I/O
• ITL_2 Non-optimized FC - Not used for I/O
• ITL_3 Non-optimized FC - Not used for I/O
• ITL_4 Optimized FC, Preferred - Used for I/O

After ITL_4 fails, the other preferred path continues to deliver data:

• ITL_1 Optimized FC, Preferred - Used for I/O
• ITL_2 Non-optimized FC - Not used for I/O

- ITL_3 Non-optimized FC - Not used for I/O

After losing the optimized, preferred paths, the two non-preferred paths are activated:

- ITL_2 Non-optimized FC - Used for I/O
- ITL_3 Non-optimized FC - Used for I/O

Finally, both optimized paths become available again, and the preferred paths are again active and the other two paths are not used to deliver data.

Failover-only example

This example demonstrates failover behavior of FC paths when you select an active path using the failover only load balance policy. Because this is an active/passive policy, only one path is active at a time.

A Windows host has four FC paths to a LUN, two paths to each node in an active/active (HA pair) storage system configuration. The load balance policy for the LUN is failover only. ITL_1 has been selected as the preferred ITL nexus by manually activating it.

Before path failover:

- ITL_1 Optimized FC - Active
- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive
- ITL_4 Optimized FC - Passive

After the active I_T_L nexus fails, the DSM selects the passive optimized I_T_L nexus:

- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive
- ITL_4 Optimized FC - Active

After losing both optimized I_T_L nexuses, the DSM selects the non-optimized I_T_L nexus with the lowest load:

- ITL_2 Non-optimized FC - Active
- ITL_3 Non-optimized FC - Passive

Whenever the preferred optimized I_T_L nexus becomes available again, the DSM activates that I_T_L nexus for I/O to the LUN.

Auto-assigned example

This example demonstrates failover behavior of FC paths using the auto assigned load balance policy. Because this is an active/passive policy, only one path is active at a time.

In this example, the Windows host has four FC paths and the load balance policy is auto assigned. The DSM activates the optimized I_T_L nexus that uses the path with the fewest active I_T_L nexuses. In this example, ITL_4 is selected. The administrator is not allowed to manually activate a path.

Before path failover:

- ITL_1 Optimized FC - Passive
- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive
- ITL_4 Optimized FC - Active

The failover behavior is the same as for the failover only load balance policy. The DSM will first select an optimized passive I_T_L nexus. If there are no optimized I_T_L nexuses, the DSM will select a proxy I_T_L nexus. The particular I_T_L nexus selected depends on which available path has the lowest current load. After the active I_T_L nexus fails, the DSM selects the passive optimized I_T_L nexus:

- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive
- ITL_4 Optimized FC - Active

After losing both optimized I_T_L nexuses, the DSM selects the non-optimized I_T_L nexus with the lowest load:

- ITL_2 Non-optimized FC - Active
- ITL_3 Non-optimized FC - Passive

The auto-assigned failback behavior is somewhat different from failover only. If a non-optimized I_T_L nexus is in use, the DSM will activate the first available optimized I_T_L nexus. If ITL_1 was the first optimized I_T_L nexus available, it would be activated:

- ITL_1 Optimized FC - Active
- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive

As additional optimized paths become available, the DSM rebalances paths so that active I_T_L nexuses are distributed evenly across paths. In this example, ITL_4 becomes available and uses a path with no active I_T_L nexus. ITL_1 uses a path that currently has two active I_T_L nexuses. The DSM activates ITL_4 so that each path has one active I_T_L nexus:

- ITL_1 Optimized FC - Passive
- ITL_2 Non-optimized FC - Passive
- ITL_3 Non-optimized FC - Passive
- ITL_4 Optimized FC - Active

If the paths are used by a clustered Windows host, the DSM waits two minutes after the path becomes available before balancing the load. This enables the I/O to stabilize and prevents the Windows cluster from failing over unnecessarily. Of course if a Windows cluster loses an active I_T_L nexus, a passive I_T_L nexus is activated immediately.

Required cfmode setting

The single_image FC cfmode setting is required starting with DSM 3.3.1. The setting applies to Data ONTAP operating in 7-Mode.

The single_image cfmode setting is now required for all storage systems with Fibre Channel (FC) connections to the Windows host.

The cfmode setting applies only to FC connections. It does not apply to iSCSI-only access.

Mapping identifiers between the host and storage system

The Data ONTAP DSM for Windows MPIO includes a number of identifiers to help you map the virtual disks (LUNs) and paths (I_T_L nexuses) between the Windows host and the storage system.

Disk serial number	The Virtual Disks page in the DSM GUI, and the output of the get-sandisk cmdlet include a serial number for each virtual disk. This serial number is assigned by Data ONTAP to a LUN on the storage system.
	The Data ONTAP lun show -v command displays the serial number. You can also view the serial number in the FilerView interface by selecting **LUN > Manage** and clicking the path name in the LUN column.
	The DSM virtual disks GUI page also shows the host name of the storage system controller, the LUN path, and the LUN identifier on the storage system for each virtual disk.
DSM Identifier (DSM ID)	Each path (I_T_L nexus) is assigned an eight-character DSM identifier. The identifier is made up of four fields: port, bus, target, and LUN. For example, DSM ID 03000101 represents port 03, bus 00, target 01, and LUN 01. The DSM ID is displayed on the DSM GUI details page for each virtual disk and is returned by the get-sanpath cmdlet.
	The DSM ID is included in most event log messages written by the Data ONTAP DSM.
Path Identifier	Each path also has an eight-character identifier made up of four fields. The first three fields are the same as the DSM ID: port, bus, and target. The fourth field indicates the path type:

01	Optimized FC paths
02	Non-optimized FC paths
03	• iSCSI paths (Data ONTAP operating in 7-Mode)
	• Optimized iSCSI paths (Data ONTAP operating in Cluster-Mode)

    04   Non-optimized iSCSI paths (Data ONTAP operating in Cluster-Mode)

The Path ID is displayed on the DSM GUI details page for each virtual disk and is returned by the `get-sanpath` cmdlet.

Dynamic disk support

Windows dynamic disks are supported with specific configuration requirements.

When using the native Windows storage stack, all LUNs composing the dynamic volume must be located on the same storage system controller.

Dynamic disks are not supported by SnapDrive for Windows.

What the Hyper-V Guest Utilities are

When you install Data ONTAP DSM, you can choose to install the Hyper-V Guest Utilities. You use the Hyper-V Guest Utilities to configure Hyper-V systems.

The Hyper-V Guest Utilities consist of the following components:

LinuxGuestConfig.iso	Sets disk timeouts for Hyper-V virtual machines that run Linux. Setting timeout parameters on a Linux guest ensures correct failover behavior.
mbralign.exe	Detects and corrects master boot record (MBR) partition alignment problems for Hyper-V virtual hard disks. Aligning the partition ensures best performance.

Related concepts

What is Hyper-V

Hyper-V is a Windows technology that enables you to create multiple virtual machines on a single physical x64 computer running Microsoft Windows Server 2008 or Windows Server 2008 R2.

Hyper-V is a "role" available in Microsoft Windows Server 2008 and Windows Server 2008 R2. Each virtual machine runs its own operating system and applications.

Methods for using storage with Hyper-V

Hyper-V enables you to provision storage using a virtual hard disk, an unformatted (raw) LUN, or an iSCSI LUN.

Virtual machines use storage on a storage system in the following ways:

- A virtual hard disk (IDE or SCSI) formatted as NTFS. The virtual hard disk is stored on a LUN mapped to the Hyper-V parent system. The guest OS must boot from an IDE virtual hard disk.
- An unformatted (raw) LUN mapped to the Hyper-V parent system and provided to the virtual machine as a physical disk mapped through either the SCSI or IDE virtual adapter.
- An iSCSI LUN accessed by an iSCSI initiator running on the guest OS.

  - For Windows Vista, use the built-in iSCSI initiator; multipathing is not supported.
  - For Windows XP, use Microsoft iSCSI initiator 2.07; multipathing is not supported.
  - For Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2, use an iSCSI initiator and multipathing solution that is supported by IBM for use on a standard host platform. The guest OS supports the same iSCSI configurations as if it was not running on a virtual machine.
  - For SUSE Linux Enterprise Server, use a supported iSCSI initiator and multipathing solution. The guest OS supports the same iSCSI configurations as if it was not running on a virtual machine.

The parent Hyper-V system can connect to storage system LUNs just like any other Windows Server 2008 or Windows Server 2008 R2 host.

Methods for clustering Windows hosts with Hyper-V

Hyper-V provides two ways to let you cluster Windows hosts.

- You can cluster the parent Hyper-V system with other parent systems using Windows failover clustering.
- You can cluster guest systems running in virtual machines with other guest systems using the clustering solution supported on the operating system You must use an iSCSI software initiator on the guest system to access the quorum and shared disks.

Recommended LUN layout with Hyper-V

You can put one or more virtual hard disks (VHDs) on a single LUN for use with Hyper-V.

The recommended LUN layout with Hyper-V is to put up to 10 VHDs on a single LUN. If you need less than ten VHDs, put each VHD on its own LUN. If you need more than ten VHDs for a Windows host, spread the VHDs evenly across about ten LUNs.

When you create virtual machines, store the virtual machine and the VHD it boots from in the same LUN.

For Windows failover clusters, the layout is different.

- For Windows Server 2008 R2 with cluster shared volumes (CSVs), you can have VHDs for multiple guests on the same LUN.
- For failover clusters without CSV, use a separate LUN for each guest's VHDs.

About SAN booting

SAN booting is the general term for booting a Windows host from a storage system LUN instead of an internal hard disk. The host might or might not have any hard drives installed.

SAN booting offers many advantages. Because the system (C:\) drive is located on the storage system, all of the reliability and backup features of the storage system are available to the system drive. You can also clone system drives to simplify deploying many Windows hosts and to reduce the total storage needed. SAN booting is especially useful for blade servers.

The downside of SAN booting is that loss of connectivity between the host and storage system can prevent the host from booting. Be sure to use a reliable connection to the storage system.

There are three options for SAN booting a Windows host:

Fibre Channel HBA	Requires one or more supported adapters. These same adapters can also be used for data LUNs. The Data ONTAP DSM for Windows MPIO installer automatically configures required HBA settings.
iSCSI HBA	Requires one or more supported adapters. These same adapters can also be used for data LUNs, or you can use an iSCSI software initiator for data. You must manually configure the HBA settings.
iSCSI software boot	Requires a supported network interface card (NIC) and a special version of the Microsoft iSCSI software initiator.

For information on iSCSI software boot, see the vendor (Intel or IBM) documentation for the iSCSI boot solution you choose. Also, see Technical Report 3644.

Note: This technical report contains information about NetApp products that IBM licenses and in some cases customizes. Technical reports might contain information about models and features that are not supported by IBM.

Related tasks

Related information

Technical Report 3644: iSCSI Software Boot for Windows with NetApp Storage

Support for non-English operating system versions

Data ONTAP DSM for Windows MPIO is supported on all Language Editions of Windows Server 2003, Server 2008, and Server 2008 R2. All product interfaces and messages are displayed in English. However, all variables accept Unicode characters as input.

Installing the DSM

Complete the following tasks in the order shown to install the DSM and related software components.

Steps

Verifying your host's configuration

Verify your configuration before you install or upgrade the DSM.

Step

1. Use the IBM N series interoperability matrix to verify that you have a supported combination of the following components:

   - Data ONTAP software
   - Windows operating system
   - SnapDrive for Windows software
   - Fibre Channel host bus adapter model, driver, and firmware
   - Fibre Channel switch model and firmware version
   - iSCSI software or hardware initiator

Related information

IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Stopping host I/O and the cluster service

The installation of hotfixes and the Data ONTAP DSM requires rebooting the Windows host. Stop all host applications that use the storage system.

Steps

1. Stop all host applications that use storage on the storage system.

2. Stop any remaining I/O between the host and the storage system.

3. For Windows Server 2003 running MSCS, optionally stop the cluster service.

   The installation might run very slowly if the cluster service is running.

Installing Windows hotfixes

Obtain and install the required Windows hotfixes for your version of Windows.

Before you begin

Some of the hotfixes require a reboot of your Windows host. You can wait to reboot the host until after you install or upgrade the DSM.

When you run the installer for the Data ONTAP DSM, it lists any missing hotfixes. You must add the required hotfixes before the installer will complete the installation process.

The DSM installation program might also display a message instructing you to install additional Windows hotfixes after installing the DSM.

Note: Some hotfixes for Windows Server 2008 are not recognized unless the affected feature is enabled. For example, an MPIO hotfix might not be recognized as installed until the MPIO feature is enabled. If you are prompted to install a hotfix that is already installed, try enabling the affected Windows feature and then restart the DSM installation program.

Steps

1. Determine which hotfixes are required for your version of Windows.

2. Download hotfixes from the Microsoft support site.

   Note: Some hotfixes must be requested from Microsoft support. They are not available for direct download.

3. Follow the instructions provided by Microsoft to install the hotfixes.

Related information

[Microsoft support site](#)

[IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html](#)

List of required hotfixes for Windows Server

Specific Windows Server hotfixes are required before you install or upgrade the Data ONTAP DSM.

The hotfixes listed in this section are the minimum requirement. The following tables specify the name and version of the file that is included in each hotfix and required for the Data ONTAP DSM. The specified file version is the minimum requirement.

The IBM N series interoperability matrix lists updates to hotfix requirements when new hotfixes supersede older hotfixes.

Note: The product installer does not check for the hotfixes that are required for Windows Failover Clustering configurations. The installer checks for all other hotfixes.

Windows Server 2003 SP2 and Windows Server 2003 R2 SP2

The following table lists the minimum required hotfixes for Windows Server 2003 SP2 and Windows Server 2003 R2 SP2.

Hotfix	When required	File name	File version
945119	Always	Storport.sys	5.2.3790.4189
982109	Always	Mpio.sys	5.2.3790.4706

Windows Server 2008 SP2

The following table lists the minimum required hotfixes for Windows Server 2008 SP2.

Hotfix	When required	File name	File version
968675	Always	Storport.sys	6.0.6002.22128
2522766	Always	Mpio.sys	6.0.6002.22637
2637162	Windows Failover Clustering configurations	Clusres.dll	6.0.6002.22717

Windows Server 2008 R2

The following table lists the minimum required hotfixes for Windows Server 2008 R2.

Hotfix	When required	File name	File version
2522766	Always	Mpio.sys	6.1.7600.20970

Hotfix	When required	File name	File version
2528357	Always	Storport.sys	6.1.7600.20959
979711	Always	Msiscsi.sys	6.1.7600.16519
2520235	Windows Failover Clustering configurations	Clusres.dll	6.1.7600.20921

Windows Server 2008 R2 SP1

The following table lists the minimum required hotfixes for Windows Server 2008 R2 SP1.

Hotfix	When required	File name	File version
2522766	Always	Mpio.sys	6.1.7601.17619
2528357	Always	Storport.sys	6.1.7601.21720
2520235	Windows Failover Clustering configurations	Clusres.dll	6.1.7601.21680
2531907	Windows Failover Clustering configurations	Failoverclusters.agent.interop.dll	6.1.7601.17514
		Failoverclusters.validation.bestpracticetests.dll	6.1.7601.21710
		Failoverclusters.validation.common.dll	6.1.7601.21710
		Failoverclusters.validation.generaltests.dll	6.1.7601.21710
		Failoverclusters.validation.storagetests.dll	6.1.7601.21710
		Failoverclusters.validation.wizard.dll	6.1.7601.21710

Related information

Microsoft support site
IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Removing or upgrading SnapDrive for Windows

The Data ONTAP DSM for Windows MPIO works with supported versions of SnapDrive for Windows. If you have an earlier version of SnapDrive on your Windows host, remove it or upgrade

before the DSM is installed. For the currently supported SnapDrive for Windows versions, see the IBM N series interoperability matrix.

Steps

1. To upgrade SnapDrive for Windows, follow the instructions in the *Installation and Administration Guide* for the new version of SnapDrive.

2. To uninstall SnapDrive for Windows, use the Windows Add or Remove Programs utility as explained in the SnapDrive for Windows *Installation and Administration Guide*.

Related information

   [IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html](www.ibm.com/systems/storage/network/interophome.html)

Confirming your storage system configuration

You must make sure your storage system is properly cabled and the FC and iSCSI services are licensed and started.

About this task

This topic describes the high-level tasks you must complete to configure your storage system for use with Fibre Channel and iSCSI hosts. See the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP for detailed instructions.

Steps

1. Add the iSCSI or FCP license and start the target service. The Fibre Channel and iSCSI protocols are licensed features of Data ONTAP software. If you need to purchase a license, contact your IBM or sales partner representative.

2. Verify your cabling. See the *FC and iSCSI Configuration Guide* for detailed cabling and configuration information.

Related information

   [FC and iSCSI Configuration Guide - www.ibm.com/storage/support/nseries/](www.ibm.com/storage/support/nseries/)

Configuring FC HBAs and switches

Install and configure one or more supported Fibre Channel host bus adapters (HBAs) for Fibre Channel connections to the storage system.

About this task

The Data ONTAP DSM for Windows MPIO installer sets the required Fibre Channel HBA settings.

> **Note:** Do not change HBA settings manually.

Steps

1. Install one or more supported Fibre Channel host bus adapters (HBAs) according to the instructions provided by the HBA vendor.

2. Obtain the supported HBA drivers and management utilities and install them according to the instructions provided by the HBA vendor.

   The supported HBA drivers and utilities are available from the following locations:

Emulex HBAs	Emulex support page for IBM.
QLogic HBAs	QLogic support page for IBM.

3. Connect the HBAs to your Fibre Channel switches or directly to the storage system.

4. Create zones on the Fibre Channel switch according to your Fibre Channel switch documentation.

   For Data ONTAP 8.1 operating in Cluster-Mode, zone the switch by WWPN. Be sure to use the WWPN of the logical interfaces (LIFs) and not of the physical ports on the storage controllers.

Related information

FC and iSCSI Configuration Guide - www.ibm.com/storage/support/nseries/
Emulex support page for IBM
QLogic support page for IBM

Checking the media type of FC ports

The media type of the storage system FC target ports must be configured for the type of connection between the host and storage system.

About this task

The default media type setting of "auto" is for fabric (switched) connections. If you are connecting the host's HBA ports directly to the storage system, you must change the media setting of the target ports to "loop".

This task applies to Data ONTAP operating in 7-Mode. It does not apply to Data ONTAP operating in Cluster-Mode.

Steps

1. To display the current setting of the storage system's target ports, enter the following command at a storage system command prompt:

   ```
   fcp show adapter -v
   ```

   The current media type setting is displayed.

2. To change the setting of a target port to "loop" for direct connections, enter the following commands at a storage system command prompt:

   ```
   fcp config adapter down
   ```

   ```
   fcp config adapter mediatype loop
   ```

   ```
   fcp config adapter up
   ```
   adapter is the storage system adapter directly connected to the host.

   For more information, see the fcp man page or *Data ONTAP Commands: Manual Page Reference, Volume 1* for your version of Data ONTAP.

Configuring iSCSI initiators and HBAs

For configurations using iSCSI, you must either download and install an iSCSI software initiator or install an iSCSI HBA, or both.

An iSCSI software initiator uses the Windows host CPU for most processing and Ethernet network interface cards (NICs) or TCP/IP offload engine (TOE) cards for network connectivity. An iSCSI HBA offloads most iSCSI processing to the HBA card, which also provides network connectivity.

The iSCSI software initiator typically provides excellent performance. In fact, an iSCSI software initiator provides better performance than an iSCSI HBA in most configurations. The iSCSI initiator

software for Windows is available from Microsoft at no charge. In some cases, you can even SAN boot a host with an iSCSI software initiator and a supported NIC.

iSCSI HBAs are best used for SAN booting. An iSCSI HBA implements SAN booting just like an FC HBA. When booting from an iSCSI HBA, it is recommended that you use an iSCSI software initiator to access your data LUNs.

> **Note:** You configure iSCSI paths differently for Data ONTAP 8.1 operating in Cluster-Mode. You need to create one or more iSCSI paths to each storage controller that can access a given LUN. Unlike earlier versions of Data ONTAP software, the iSCSI ports on a partner node do not assume the IP addresses of the failed partner. Instead, the MPIO software on the host is responsible for selecting the new paths. This behavior is very similar to Fibre Channel path failover.

iSCSI software initiator options

Select the appropriate iSCSI software initiator for your host configuration.

The following is a list of operating systems and their iSCSI software initiator options.

Windows Server 2003	Download and install the iSCSI software initiator.
Windows Server 2008	The iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog is available from Administrative Tools.
Windows Server 2008 R2	The iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog is available from Administrative Tools.
Windows XP guest systems on Hyper-V	For guest systems on Hyper-V virtual machines that access storage directly (not as a virtual hard disk mapped to the parent system), download and install the iSCSI software initiator. You cannot select the Microsoft MPIO Multipathing Support for iSCSI option; Microsoft does not support MPIO with Windows XP. Note that a Windows XP iSCSI connection to IBM N series storage is supported only on Hyper-V virtual machines.
Windows Vista guest systems on Hyper-V	For guest systems on Hyper-V virtual machines that access storage directly (not as a virtual hard disk mapped to the parent system), the iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog is available from Administrative Tools. Note that a Windows Vista iSCSI connection to IBM N series storage is supported only on Hyper-V virtual machines.
SUSE Linux Enterprise Server guest systems on Hyper-V	For guest systems on Hyper-V virtual machines that access storage directly (not as a virtual hard disk mapped to the parent system), use an iSCSI initiator solution on a Hyper-V guest that is supported for standalone hardware. A supported version of Linux Host Utilities is required.
Linux guest systems on Virtual Server 2005	For guest systems on Virtual Server 2005 virtual machines that access storage directly (not as a virtual hard disk mapped to the parent system), use an iSCSI initiator solution on a Virtual Server 2005 guest that is supported

for standalone hardware. A supported version of Linux Host Utilities is required.

Note: If you want to use an iSCSI HBA on Windows Server 2003 hosts to access the storage system, you must download and install the iSCSI initiator service.

Related tasks

Downloading the iSCSI software initiator

To download the iSCSI initiator, complete the following steps.

About this task

If you are using iSCSI software boot, you need a special boot-enabled version of the iSCSI software initiator.

Steps

1. Go to the Microsoft Web site at http://www.microsoft.com/.

2. Click **Downloads & Trials**.

3. Click **Download Center**.

4. Keep the default setting of All Downloads. In the Search box, type

   iSCSI Initiator
   and then click **Go**.

5. Select the supported Initiator version you want to install.

6. Click the download link for the CPU type in your Windows host. You might also choose to download the *Release Notes* and *Users Guide* for the iSCSI Initiator from this Web page.

7. Click **Save** to save the installation file to a local directory on your Windows host.

Result

The initiator installation program is saved to the Windows host.

Related concepts

Installing the iSCSI Initiator software

On the Windows host, complete the following steps to install the iSCSI Initiator.

Before you begin

You must have downloaded the appropriate iSCSI initiator installer to the Windows host.

Steps

1. Open the local directory to which you downloaded the iSCSI Initiator software.
2. Run the installation program by double-clicking the icon.
3. When prompted to select installation options, select **Initiator Service** and **Software Initiator**.
4. For all multipathing solutions except Veritas, select the **Microsoft MPIO Multipathing Support for iSCSI** check box, regardless of whether you are using MPIO or not. For the Veritas multipathing, clear this check box.

   Multipathing is not available for Windows XP and Windows Vista.
5. Follow the prompts to complete the installation.

Installing the iSCSI HBA

If your configuration uses an iSCSI HBA, you must make sure that the HBA is installed and configured correctly.

Before you begin

If you use an iSCSI HBA on Windows Server 2003 hosts, you also need to install the Microsoft iSCSI initiator service. If you are using only the iSCSI HBA, you can clear the "iSCSI Initiator" check box when installing the initiator package. The initiator service is built into Windows Server 2008 and Windows Server 2008 R2.

About this task

You can optionally boot your Windows host from a storage system LUN using a supported HBA.

Steps

1. Install one or more supported iSCSI host bus adapters according to the instructions provided by the HBA vendor.
2. Obtain the supported HBA drivers and management utilities and install them according to the instructions provided by the HBA vendor.
3. Manually set the required QLogic iSCSI HBA settings.

a. Start the SANsurfer program on the Windows host and select the iSCSI HBA. See the SANsurfer online Help for more information.

b. Specify an IP address for each HBA port.

c. Set the Connection KeepAliveTO value to 180.

d. Enable ARP Redirect.

e. Set the iSCSI node name of all iSCSI HBA ports to the same name as shown in the iSCSI initiator GUI on the Windows host.

f. Save the HBA settings and reboot the Windows host.

4. Connect the iSCSI HBA to your Ethernet switches or directly to the storage system. Avoid routing if possible.

5. Using the iSCSI initiator GUI, configure the iSCSI target addresses of your storage system. If you are using more than one path, explicitly select the initiator and target for each path when you log on.

After you finish

If you are SAN booting from an iSCSI HBA, you must also manually set the boot BIOS on the HBA.

Related tasks

Setting up a SAN boot LUN for Windows Server on page 125

Related information

QLogic support page for IBM

Options for iSCSI sessions and error recovery levels

The defaults allowed by Data ONTAP are one TCP/IP connection per iSCSI session and an error recovery level of 0.

You can optionally enable multiple connections per session and error recovery level 1 or 2 by setting Data ONTAP option values. Regardless of the settings, you can always use error recovery level 0 and single-connection sessions. For more information, see the chapter about managing the iSCSI network in the *Data ONTAP Block Access Management Guide for iSCSI and FC*.

The iSCSI initiator does not automatically create multiple sessions. You must explicitly create each session using the iSCSI Initiator GUI.

Options for using CHAP with iSCSI Initiators

You can use one-way or mutual (bidirectional) authentication with the challenge handshake authentication protocol (CHAP).

For one-way CHAP, the target only authenticates the initiator. For mutual CHAP, the initiator also authenticates the target.

The iSCSI Initiator sets strict limits on the length of both the initiator's and target's CHAP passwords. For Windows Server 2003, see the readme file on the host (C:\Windows\iSCSI \readme.txt) for more information. For Windows Server 2008 or Windows Server 2008 R2, see the Manage iSCSI Security topic in Help.

There are two types of CHAP user names and passwords. These types indicate the direction of authentication, relative to the storage system:

Inbound The storage system authenticates the iSCSI Initiator. Inbound settings are required if you are using CHAP authentication.

Outbound The iSCSI Initiator authenticates the storage system using CHAP. Outbound values are used only with mutual CHAP.

You specify the iSCSI Initiator CHAP settings using the Microsoft iSCSI Initiator GUI on the host. Click **Advanced** on the **GUI Discovery** tab to specify inbound values for each storage system when you add a target portal. Click **Secret** on the **General** tab to specify the outbound value (mutual CHAP only).

By default, the iSCSI Initiator uses its iSCSI node name as its CHAP user name.

Always use ASCII text passwords; do not use hexadecimal passwords. For mutual (bidirectional) CHAP, the inbound and outbound passwords cannot be the same.

Using RADIUS for iSCSI authentication

You can optionally use a RADIUS (Remote Authentication Dial-in User Service) server to centrally manage passwords for iSCSI authentication. Using RADIUS simplifies password management, increases security, and offloads authentication processing from storage systems.

Support for RADIUS is available starting with Data ONTAP 8.0 for the iSCSI target and Windows Server 2008 or Windows Server 2008 R2 for the iSCSI initiator.

You can configure either one-way authentication (the target authenticates the initiator), or mutual authentication (the initiator also authenticates the target).

There are three parts to enabling RADIUS authentication for iSCSI initiators:

• Set up a RADIUS server
• Configure the storage system to use RADIUS
• Configure iSCSI initiators to use RADIUS

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 include a RADIUS server. For information about configuring this RADIUS server, see the Windows online Help.

For information about configuring the storage system to use RADIUS, see the *Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

Configuring iSCSI initiators for one-way authentication using RADIUS

One-way authentication means the target verifies the identity of the initiator; the initiator does not verify the identity of the target. To use one-way RADIUS authentication, you must configure the Windows Server 2008 or Windows Server 2008 R2 iSCSI software initiator to use the RADIUS server.

Before you begin

Set up the RADIUS server and configure the storage system before configuring the iSCSI initiator to use RADIUS.

Steps

1. On the Windows Server 2008 or Windows Server 2008 R2 host, click **Start > Administrative Tools > iSCSI Initiator** to open the Windows iSCSI Initiator Properties dialog.

2. On the **Targets** tab, select an iSCSI target and click **Log on > Advanced**.

3. Select the **CHAP logon information** and **Use RADIUS to authenticate target credentials** check boxes.

Related tasks

Configuring iSCSI initiators for mutual authentication using RADIUS

Mutual authentication means the target verifies the identity of the initiator, and the initiator verifies the identity of the target. To use mutual RADIUS authentication, you must configure the Windows Server 2008 or Windows Server 2008 R2 iSCSI software initiator to use the RADIUS server.

Before you begin

Set up the RADIUS server and configure the storage system before configuring the iSCSI initiator to use RADIUS.

Steps

1. On the Windows Server 2008 or Windows Server 2008 R2 host, click **Start > Administrative Tools > iSCSI Initiator** to open the Windows iSCSI Initiator Properties dialog.

2. On the **RADIUS** tab, click **Add** and specify the IP address of the RADIUS server.

You can optionally add additional RADIUS servers.

3. Click **RADIUS** and enter the shared secret for the RADIUS server.

   The 26-character shared secret should be the same value as is used in the RADIUS client for this initiator.

4. On the **Discovery** tab, click **Add Portal**.

5. Enter the IP address of the iSCSI target port on the storage system, and then click **Advanced**.

6. Select the **CHAP logon information** check box, and then enter the CHAP user name and target secret.

   These values must match the outbound user name and password specified on the storage system.

7. Select the **Use RADIUS to generate authentication credentials** and **Perform mutual authentication** check boxes, then click **OK**.

8. On the **Targets** tab, select the iSCSI target and click **Log on**. Optionally select the **Automatically restore this connection when the computer starts** and **Enable multi-path** check boxes.

9. Click **Advanced**.

10. In the **Local adapter** field, select **Microsoft iSCSI Initiator**. Select the desired IP addresses for **Source IP** and **Target portal**.

11. Select the **CHAP logon information** check box, and then enter the CHAP user name and target secret.

   Use the same values you entered for the **Discovery** tab.

12. Select the **Use RADIUS to generate authentication credentials** and **Perform mutual authentication** check boxes, then click **OK**.

13. Click **OK** twice to close the Windows iSCSI Initiator Properties dialog.

Related tasks

Enabling ALUA for FC paths

ALUA is required for Fibre Channel paths mapped to LUNs used by the Windows host. Enable ALUA on the igroups for any LUNs with FC paths.

About this task

This task describes how to enable ALUA on igroups in Data ONTAP operating in 7-Mode. ALUA is enabled by default on igroups in Data ONTAP operating in Cluster-Mode. In some situations, ALUA is not automatically enabled on 7-Mode igroups.

Steps

1. To check whether ALUA is enabled, enter the following command on the storage controller:

   igroup show -v *igroup_name*

2. If ALUA is not enabled, enter the following command to enable it:

   igroup set *igroup_name* alua yes

   The Windows host does not detect the ALUA setting until it is rebooted.

After you finish

For Data ONTAP operating in 7-Mode, remove any iSCSI paths to LUNs that also use FC paths. All igroups mapped to a LUN must have the same ALUA setting. Because ALUA is not supported for iSCSI paths to 7-Mode LUNs, mixed FC and iSCSI paths to the same 7-Mode LUN are not supported.

Related concepts

ALUA support and requirements on page 17
Mixing FC and iSCSI paths on page 18

Related tasks

Troubleshooting ALUA configuration problems on page 130

Obtaining an MPIO license key

The Data ONTAP DSM for Windows MPIO requires a license key. You must purchase a separate license for each Windows host.

Before you begin

If you have an MPIO license key for your host from an earlier version of the DSM, you can use that key when upgrading.

Step

1. Use the key provided by your IBM representative.

Enabling the Multipath I/O feature for Windows Server 2008 and 2008R2

The Windows MPIO components are built into Windows Server 2008 and 2008R2, but are not enabled by default. Enable the Multipath I/O feature before installing the DSM.

Steps

1. Start Windows Server Manager and select **Features** in the navigation tree.
2. Click **Add Features**.
3. Select the **Multipath I/O** check box and then click **Next**.
4. Follow the instructions on your screen to complete the installation. Reboot the Windows host if prompted.

Running the DSM installation program

You can use two methods to install Data ONTAP DSM. You can run the installation program interactively by using an installation wizard and you can run the installation program silently by running a command.

Running the DSM installation program interactively

Run the installation program to install the DSM code and to set required parameters for HBAs and in the Windows registry. You can also use the silent (command line) installation option.

Before you begin

This process is for new DSM installations. For upgrades, follow the upgrading process instead.

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled IBM N series customers who have completed the registration process on the N series support website (accessed and navigated as described in *Websites* on page 9).

You must have already completed the following tasks:

• Stopped applications, I/O, and for hosts running MSCS, stopped the cluster service.
• Obtained an MPIO license key.
• Backed up any critical data on your Windows host.
• For Windows Server 2008 and 2008R2, enabled the Windows Multipath I/O feature.

A reboot of the Windows host is required to complete the installation.

The installation program displays the current and new versions of DSM and Windows MPIO components. However, the installation program never installs new Windows MPIO components for Windows Server 2008.

About this task

For Windows 2003 hosts, the installer will warn you that Windows PowerShell is not installed. You have two options when this happens:

* You can exit the Data ONTAP DSM installer, install Windows PowerShell, and then restart the DSM install.
* You can complete the Data ONTAP DSM install, install Windows PowerShell, repair the DSM, and then reboot your host.

Steps

1. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.

2. Obtain the product software by inserting the DSM CD-ROM into your host machine or by downloading the software from the N series support website (accessed and navigated as described in *Websites* on page 9).

3. Launch the installation program and follow the instructions on the screen.

4. Enter the MPIO license key when prompted.

5. Select the **Use the default system account** check box. Or optionally enter the user name and password of the account on the Windows host under which the DSM management service will be logged on. This account must be in the Windows Administrators group.

   The DSM service requires an Administrator-level account to allow it to manage disks and paths on the Windows host.

6. Choose whether to install the Hyper-V Guest Utilities.

7. When prompted, click **Yes** to reboot the Windows host and complete the installation.

After you finish

If the installer reports a problem, such as a required hotfix not found, correct the problem and run the installer again.

The installation program might also display a message instructing you to install Windows hotfixes *after* installing the DSM. If so, download the specified hotfixes from the Microsoft support site and install them.

For Windows Server 2008 and 2008 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

Related concepts

Related tasks

Running the DSM installation program from a command line

Run the installation program from a command prompt to install the DSM code and to set required parameters for HBAs and in the Windows registry without operator intervention. You can also run the installation program interactively.

Before you begin

This process is written for new DSM installations. If you are upgrading, be sure to read the upgrading process as well.

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled IBM N series customers who have completed the registration process on the N series support website (accessed and navigated as described in *Websites* on page 9).

You must have already completed the following tasks:

- Stopped applications, I/O, and for hosts running MSCS, stopped the cluster service.
- Obtained an MPIO license key.
- Backed up any critical data on your Windows host.
- For Windows Server 2008 and 2008R2, enabled the Windows Multipath I/O feature.

Note: Some of the command options are case sensitive. Be sure to enter the commands exactly as shown.

Note: The account doing the actual installation must be in the Administrators group. For example, when using rsh, programs are executed under the SYSTEM account by default. You must change the rsh options to use an administrative account.

To include the silent install command in a script, use `start /b /wait` before the `installer.exe` command. For example: `start /b /wait msiexec /package installer.msi ...` The wait option is needed to get the correct installation return value. If you just run `installer.msi`, it returns "success" if the Windows installer is successfully launched. However, the installation itself may still fail. By using the wait option as shown above, the return code describes the success or failure of the actual installation.

Steps

1. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.

2. Obtain the product software by inserting the DSM CD-ROM into your host machine or by downloading the software from the N series support website (accessed and navigated as described in *Websites* on page 9).

3. Enter the following command on your Windows host:

```
msiexec /package installer.msi /quiet /l*v log_file_name LICENSECODE=key
HYPERVUTIL={0|1} USESYSTEMACCOUNT={0|1} [SVCUSERNAME=domain\user
SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password]
[INSTALLDIR=inst_path] [TEMP_FOLDER=temp_path]
```

installer.msi is the DSM installation program for your Windows host's processor architecture.

log_file_name is the file path and name for the MSI installer log. Note the first character of the l*v option is a lower case L.

key is the MPIO license code for the DSM.

HYPERVUTIL=0 specifies that the installation program does not install the Hyper-V Guest Utilities.

HYPERVUTIL=1 specifies that the installation program does install the Hyper-V Guest Utilities.

USESYSTEMACCOUNT=1 specifies that the DSM management service runs under the default SYSTEM account. You do not specify account credentials.

USESYSTEMACCOUNT=0 specifies that the DSM management service run under a different account. You must provide the account credentials.

domain\user is the Windows domain and user name of an account in the Administrators group on the Windows host under which the DSM management service will be logged on. The DSM service requires an Administrator-level account to allow it to manage disks and paths on the Windows host.

password is the password for the account above.

inst_path is the path where the DSM files are installed. The default path is C:\Program Files \IBM\MPIO\.

temp_path is the path where log files are written (except the MSI installer log). The default path is C:\temp\ibm\.

> **Note:** To view help for the Windows installer, run the following command:
>
> ```
> msiexec /?
> ```

Because installing the DSM requires a reboot, the Windows host will automatically be rebooted at the end of the quiet installation. There is no warning or prompt before reboot.

After you finish

Search the installation log file for the term "hotfix" to locate messages about missing Windows hotfixes you need to install.

For Windows Server 2008 and 2008 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

Related concepts

Windows Administrator account requirement on page 20
What the Hyper-V Guest Utilities are on page 35

Related tasks

Stopping host I/O and the cluster service on page 40
Obtaining an MPIO license key on page 53
Running the DSM installation program interactively on page 54
Upgrading the DSM on page 67

Configuring Hyper-V systems

Hyper-V systems require special configuration steps for some virtual machines.

Adding virtual machines to a failover cluster

To add Hyper-V virtual machines to a cluster, they must be on a node to which you are creating and adding virtual machines.

About this task

When you have more than one virtual machine (configuration files and boot.vhd file) stored on the same LUN, and you are adding the virtual machines to a failover cluster, you must put all of the virtual machine resources in the same resource group. Otherwise adding virtual machines to the cluster fails.

Steps

1. Move the available storage group to the node on which you are creating and adding virtual machines. (The available storage resource group in a Windows Server 2008 or Windows Server 2008 R2 failover cluster is hidden.) On the cluster node, enter the following command at a Windows command prompt:

   `c:\cluster group "Available Storage" /move:node_name`
   node_name is the host name of the cluster node from which you are adding virtual machines.

2. Move all of the virtual machine resources to the same failover cluster resource group.

3. Run the Virtual Machine Resource Wizard to create the virtual machines and then add them to the failover cluster. Be sure that the resources for all virtual machines are configured as dependent on the disk mapped to the LUN.

Configuring SUSE Linux and RHEL 5.5 and 5.6 guests for Hyper-V

Linux guest operating systems running on Hyper-V require a timeout parameter setting to support virtual hard disks and the Linux Host Utilities to support iSCSI initiators. Data ONTAP DSM provides a script for setting the timeout. You must also install the Linux Integration Components package from Microsoft.

Before you begin

Install a supported version of the Linux operating system on a Hyper-V virtual machine.

About this task

This task applies to SUSE Linux Enterprise Server and to Red Hat Enterprise Linux (RHEL) 5.5 and 5.6.

Setting timeout parameters on a Linux guest ensures correct failover behavior.

You can use an iSCSI initiator solution on a Hyper-V guest that is supported for standalone hardware. Be sure to install a supported version of Linux Host Utilities. Use the linux type for LUNs accessed with an iSCSI initiator and for raw Hyper-V LUNs. Use the windows_2008 or hyper_v LUN type for LUNs that contain VHDs.

Steps

1. Download and install the Linux Integration Components package from Microsoft. Follow the installation instructions included with the download from Microsoft.

   The package is available from the Microsoft Connect site. Registration is required.

2. Set the timeout parameter.

   You set the timeout parameter only once. The timeout parameter will be used for all existing and new SCSI disks that use IBM N series LUNs.

   a. Using the Windows Hyper-V Manager, mount the supplied .iso file on the virtual machine's virtual DVD/CD-ROM. On the **Settings** tab for the virtual machine, select the DVD/CD-ROM drive and specify the path to the .iso file in the **Image file** field. The default path is `C:\Program Files\IBM\MPIO\LinuxGuestConfig.iso`.

   b. Log into the Linux guest as root.

   c. Create a mount directory and mount the virtual DVD/CD-ROM.

      Example

      ```
      linux_guest:/ # mkdir /mnt/cdrom
      linux_guest:/ # mnt /dev/cdrom /mnt/cdrom
      ```

    d. Run the script.

    Example

```
linux_guest:/ # /mnt/cdrom/linux_gos_timeout-install.sh
```

3. Set all virtual network adapters for the virtual machine to use static MAC addresses.

4. If you are running an iSCSI initiator on the Linux guest, install a supported version of the Linux Host Utilities.

Related information

   Microsoft Connect

Configuring RHEL 6.0 and 6.1 guests for Hyper-V

Linux guest operating systems running on Hyper-V require a timeout parameter setting to support virtual hard disks and the Linux Host Utilities to support iSCSI initiators. Data ONTAP DSM provides a script for setting the timeout. You must also install the Linux Integration Components package from Microsoft.

Before you begin

Install a supported version of the Linux operating system on a Hyper-V virtual machine.

About this task

This task applies to Red Hat Enterprise Linux (RHEL) 6.0 and 6.1.

Setting timeout parameters on a Linux guest ensures correct failover behavior.

You can use an iSCSI initiator solution on a Hyper-V guest that is supported for standalone hardware. Be sure to install a supported version of Linux Host Utilities. Use the linux type for LUNs accessed with an iSCSI initiator and for raw Hyper-V LUNs. Use the windows_2008 or hyper_v LUN type for LUNs that contain VHDs.

Steps

1. Download and install the Linux Integration Components package from Microsoft. Follow the installation instructions included with the download from Microsoft.

The package is available from the Microsoft Connect site. Registration is required.

2. Set the timeout parameter.

You set the timeout parameter only once. The timeout parameter will be used for all existing and new SCSI disks that use IBM N series LUNs.

    a. Create the following file:

```
/etc/udev/rules.d/20-timeout.rules
```

    b. Add the following entry to the file:

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
        RUN+="/bin/sh -c 'echo 180 > /sys$$DEVPATH/timeout'"
```

    c. Save and close the file.

    d. Reboot the host.

3. Set all virtual network adapters for the virtual machine to use static MAC addresses.

4. If you are running an iSCSI initiator on the Linux guest, install a supported version of the Linux Host Utilities.

Related information

   Microsoft Connect

Hyper-V VHD requires alignment for best performance

A Hyper-V virtual hard drive (VHD) partitioned with a master boot record (MBR) that is used by a Window Server 2003, Windows 2000 Server, or Linux virtual machine needs to be aligned with the underlying LUN for best performance. Data ONTAP DSM for Windows MPIO includes the mbralign program for aligning partitions on VHDs.

If the data block boundaries of a disk partition do not align with the block boundaries of the underlying LUN, the storage system often has to complete two block reads or writes for every operating system block read or write. The additional block reads and writes caused by the misalignment can cause serious performance problems.

The misalignment is caused by the location of the starting sector for each partition defined by the master boot record. Partitions created by Windows Server 2003, Windows 2000 Server, and Linux are usually not aligned with underlying IBM N series LUNs. Partitions created by Windows Server 2008 and Windows Server 2008 R2 should be aligned by default.

Data ONTAP DSM for Windows MPIO includes the mbralign.exe program that tests and corrects MBR partition alignment on VHDs. If the partition is found to not be correctly aligned with underlying storage, the mbralign.exe program creates a new VHD file with the correct alignment and copies all partitions to it. The original VHD file is not modified or deleted. The virtual machine must be shut down while the data is copied.

The mbralign.exe program supports only fixed size VHD files with MBR type partitions. VHDs using Windows dynamic disks or GPT partitions are not supported.

The mbralign.exe program requires a minimum partition size of 4GB. Smaller partitions cannot be correctly aligned.

For Linux virtual machines using the GRUB boot loader on a VHD, you must update the boot configuration after running the mbralign program.

Checking and fixing VHD partition alignment with mbralign

Use the mbralign.exe program included in Data ONTAP DSM for Windows MPIO to check and fix partition alignment for Hyper-V virtual hard disks. Aligning the partition ensures best performance.

About this task

Partitions created on VHDs by Windows Server 2003, Windows 2000 Server, and Linux usually need their alignment fixed. Partitions created by Windows Server 2008 and Windows Server 2008 R2 should be aligned by default.

Steps

1. Shut down the virtual machine.

   If you want to preserve the existing disk letter mappings for a Windows virtual machine, use the `-vm` option in the next step and do not shut down the virtual machine until prompted.

2. Enter the following command at the Hyper-V parent Windows command prompt:

   `mbralign [-bs=size] [-preview] [-vm hostname [-vm_user username -vm_pass password]] SourceFile [DestinationFile]`

   size is the optional block size for the file in KB. Value can be 8, 16, 32, 64, 128, or 1024. The default is 64.

   `-preview` checks alignment but does not change anything.

   -vm *hostname* specifies the DNS name or IP address of the Windows virtual machine using the VHD being aligned. Specify this option to preserve the drive letter mappings on the virtual machine after alignment. You are prompted to shut down the virtual machine after the current drive letter information is collected by the mbralign program.

   -vm_user *username* specifies a user account on the virtual machine. Used only with the `-vm` option. The default is to use the credentials you used to log into the Hyper-V parent.

   -vm_pass *password* specifies the password for the user account specified with the `-vm_user` option.

   SourceFile is the complete path, including file name, to the VHD on the Hyper-V parent. *SourceFile* is optional when using the `-vm` option, assuming the VM's host name, DNS name, and Hyper-V VM name all match; mbralign presents a list of VHDs found for that VM.

   DestinationFile is the optional complete path, including file name, to the aligned VHD. The default path is the source file with "-aligned" appended before the .vhd extension.

   For additional command options, enter

   `mbralign -help`

   ```
   C:\>mbralign -vm vmdc-01
   Connecting to HyperV server WSHEDC001 and gathering data for vmdc-01
   ```

```
Connecting to virtual machine vmdc-01 to determine drive mappings.
Successfully gathered drive letter information from the specified
virtual
machine. Please shutdown the Virtual Machine.
Press Enter to continue...
0: G:\ClusterStorage\Volume1\VMDC-01\VMDC-01_DE.vhd
1: G:\ClusterStorage\Volume1\VMDC-01\VMDC-01_SysVol.vhd
2: Manual Input
Select a VHD by entering its number
:0
              PARTITION TABLE SUMMARY
 Part  Type Mount    Start LBA  New Start LBA    New End LBA    Length
in KB
 ----  ---- -----    ---------  -------------    -----------
------------
   P1   07               63           64           2104516
1052226
Please review the summary above. This application is unable to
reliably detect
that the VHD file is not currently in use. It is important to verify
that there
are no virtual machines, or any other software accessing this file.
Enter "yes" to continue or "no" to exit...
:yes
The current VHD file is G:\ClusterStorage
\Volume1\VMDC-01\VMDC-01_DE.vhd.
Please specify a destination file name, or press enter to have a file
name
generated for you.
:
Creating a new VHD file with 5368891903 bytes...
Done
Copying partition P1, from LBA: 63 to LBA: 64. 100.0% of 1077479424
bytes copied.
Done
Completed copying 1077479424 bytes of partition P1
Would you like to align additional VHD files?
:n
Ready to update the Virtual Machine drive letters. Please boot the
Virtual
Machine using the newly aligned VHD file(s). Make sure it is
responding on the
network
```

After you finish

For Linux virtual machines using the GRUB boot loader, reinstall GRUB to ensure the guest operating system boots correctly.

Reinstalling GRUB for Linux guests after running mbralign

After running `mbralign` on disks for Linux guest operating systems using the GRUB boot loader, you must reinstall GRUB to ensure that the guest operating system boots correctly.

Before you begin

The `mbralign` program has completed on the on the file for the virtual machine.

About this task

This topic applies only to Linux guest operating systems using the GRUB boot loader and SystemRescueCd.

Steps

1. Mount the ISO image of Disk 1 of the installation CDs for the correct version of Linux for the virtual machine.

2. If the VM is running and hung at the GRUB screen, click in the display area to make sure it is active, then to reboot the VM. If the VM is not running, start it, and then immediately click in the display area to make sure it is active.

3. As soon as you see the VMware BIOS splash screen, press the Escape key once.

   The boot menu is displayed.

4. At the boot menu, select CD-ROM.

5. At the Linux boot screen, enter

   :linux rescue

6. Take the defaults for Anaconda (the blue/red configuration screens). Networking is optional.

7. Launch GRUB by entering:

   grub

8. If there is only one virtual disk in this VM, or if there are multiple disks, but the first is the boot disk, then run the following GRUB commands:

   root (hd0,0)

   setup (hd0)

   quit

   If you have multiple virtual disks in the VM, and the boot disk is not the first disk, or you are fixing GRUB by booting from the misaligned backup, enter the following command to identify the boot disk:

   find /boot/grub/stage1

   Run the following commands:

```
root (boot_disk,0)

setup (boot_disk)

quit
```

boot_disk is the disk identifier of the boot disk.

9. Press Ctrl-D to log out.

Linux rescue shuts down and then reboots.

Upgrading the DSM

Complete the following tasks in the order shown to upgrade the DSM.

Before you begin

Windows Server 2003 or Server 2008 systems must be running Data ONTAP DSM 3.2R1 or later to upgrade directly to DSM 3.5. For earlier DSM versions, you must first upgrade to DSM 3.2R1 and reboot before you can upgrade to DSM 3.5.

Windows Server 2008 R2 systems must be running Data ONTAP DSM 3.3.1 to upgrade directly to DSM 3.5. You must uninstall earlier versions of the Data ONTAP DSM before installing DSM 3.5. You must also remove the Windows MPIO feature after uninstalling the DSM and before installing DSM 3.5.

Steps

1. *Verifying your host's configuration* on page 67
2. *Stopping host I/O and the cluster service* on page 68
3. *Installing Windows hotfixes* on page 68
4. *Removing FC or iSCSI paths to 7-Mode LUNs* on page 70
5. *Enabling ALUA for FC paths* on page 71
6. *Running the DSM upgrade program* on page 72

Verifying your host's configuration

Verify your configuration before you install or upgrade the DSM.

Step

1. Use the IBM N series interoperability matrix to verify that you have a supported combination of the following components:

   • Data ONTAP software
   • Windows operating system
   • SnapDrive for Windows software
   • Fibre Channel host bus adapter model, driver, and firmware
   • Fibre Channel switch model and firmware version
   • iSCSI software or hardware initiator

Related information

   IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Stopping host I/O and the cluster service

The installation of hotfixes and the Data ONTAP DSM requires rebooting the Windows host. Stop all host applications that use the storage system.

Steps

1. Stop all host applications that use storage on the storage system.

2. Stop any remaining I/O between the host and the storage system.

3. For Windows Server 2003 running MSCS, optionally stop the cluster service.

   The installation might run very slowly if the cluster service is running.

Installing Windows hotfixes

Obtain and install the required Windows hotfixes for your version of Windows.

Before you begin

Some of the hotfixes require a reboot of your Windows host. You can wait to reboot the host until after you install or upgrade the DSM.

When you run the installer for the Data ONTAP DSM, it lists any missing hotfixes. You must add the required hotfixes before the installer will complete the installation process.

The DSM installation program might also display a message instructing you to install additional Windows hotfixes after installing the DSM.

   Note: Some hotfixes for Windows Server 2008 are not recognized unless the affected feature is enabled. For example, an MPIO hotfix might not be recognized as installed until the MPIO feature is enabled. If you are prompted to install a hotfix that is already installed, try enabling the affected Windows feature and then restart the DSM installation program.

Steps

1. Determine which hotfixes are required for your version of Windows.

2. Download hotfixes from the Microsoft support site.

   Note: Some hotfixes must be requested from Microsoft support. They are not available for direct download.

3. Follow the instructions provided by Microsoft to install the hotfixes.

Related information

> *Microsoft support site*
> *IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html*

List of required hotfixes for Windows Server

Specific Windows Server hotfixes are required before you install or upgrade the Data ONTAP DSM.

The hotfixes listed in this section are the minimum requirement. The following tables specify the name and version of the file that is included in each hotfix and required for the Data ONTAP DSM. The specified file version is the minimum requirement.

The IBM N series interoperability matrix lists updates to hotfix requirements when new hotfixes supersede older hotfixes.

Note: The product installer does not check for the hotfixes that are required for Windows Failover Clustering configurations. The installer checks for all other hotfixes.

Windows Server 2003 SP2 and Windows Server 2003 R2 SP2

The following table lists the minimum required hotfixes for Windows Server 2003 SP2 and Windows Server 2003 R2 SP2.

Hotfix	When required	File name	File version
945119	Always	Storport.sys	5.2.3790.4189
982109	Always	Mpio.sys	5.2.3790.4706

Windows Server 2008 SP2

The following table lists the minimum required hotfixes for Windows Server 2008 SP2.

Hotfix	When required	File name	File version
968675	Always	Storport.sys	6.0.6002.22128
2522766	Always	Mpio.sys	6.0.6002.22637
2637162	Windows Failover Clustering configurations	Clusres.dll	6.0.6002.22717

Windows Server 2008 R2

The following table lists the minimum required hotfixes for Windows Server 2008 R2.

Hotfix	When required	File name	File version
2522766	Always	Mpio.sys	6.1.7600.20970

Hotfix	When required	File name	File version
2528357	Always	Storport.sys	6.1.7600.20959
979711	Always	Msiscsi.sys	6.1.7600.16519
2520235	Windows Failover Clustering configurations	Clusres.dll	6.1.7600.20921

Windows Server 2008 R2 SP1

The following table lists the minimum required hotfixes for Windows Server 2008 R2 SP1.

Hotfix	When required	File name	File version
2522766	Always	Mpio.sys	6.1.7601.17619
2528357	Always	Storport.sys	6.1.7601.21720
2520235	Windows Failover Clustering configurations	Clusres.dll	6.1.7601.21680
2531907	Windows Failover Clustering configurations	Failoverclusters.agent.interop.dll	6.1.7601.17514
		Failoverclusters.validation.bestpracticetests.dll	6.1.7601.21710
		Failoverclusters.validation.common.dll	6.1.7601.21710
		Failoverclusters.validation.generaltests.dll	6.1.7601.21710
		Failoverclusters.validation.storagetests.dll	6.1.7601.21710
		Failoverclusters.validation.wizard.dll	6.1.7601.21710

Related information

Microsoft support site
IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Removing FC or iSCSI paths to 7-Mode LUNs

If you use both iSCSI and FC paths to the same LUN on Data ONTAP operating in 7-Mode, you need to remove either the iSCSI path or the FC path. Because ALUA is required for FC paths, and

ALUA is not currently supported for iSCSI paths to 7-Mode LUNs, DSM 3.5 does not support both FC and iSCSI paths to the same 7-Mode LUN.

Step

1. Use the `lun unmap` command to unmap a LUN from an igroup. For more information, see the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

Enabling ALUA for FC paths

ALUA is required for Fibre Channel paths mapped to LUNs used by the Windows host. Enable ALUA on the igroups for any LUNs with FC paths.

About this task

This task describes how to enable ALUA on igroups in Data ONTAP operating in 7-Mode. ALUA is enabled by default on igroups in Data ONTAP operating in Cluster-Mode. In some situations, ALUA is not automatically enabled on 7-Mode igroups.

Steps

1. To check whether ALUA is enabled, enter the following command on the storage controller:

   `igroup show -v igroup_name`

2. If ALUA is not enabled, enter the following command to enable it:

   `igroup set igroup_name alua yes`

   The Windows host does not detect the ALUA setting until it is rebooted.

After you finish

For Data ONTAP operating in 7-Mode, remove any iSCSI paths to LUNs that also use FC paths. All igroups mapped to a LUN must have the same ALUA setting. Because ALUA is not supported for iSCSI paths to 7-Mode LUNs, mixed FC and iSCSI paths to the same 7-Mode LUN are not supported.

Related concepts

Related tasks

Running the DSM upgrade program

You can use two methods to upgrade Data ONTAP DSM. You can run the upgrade program interactively by using an installation wizard, and you can run the upgrade program silently by running a command.

Before you begin

Special upgrade procedures apply to Windows Server 2003 MSCS (cluster) and Windows Server 2008 Windows Failover Cluster configurations.

Upgrading Windows cluster configurations

Special steps are required to successfully upgrade the DSM on clustered Windows systems.

About this task

This procedure is recommended for DSM upgrades to Windows Server 2003 MSCS (cluster) and Windows Server 2008 Windows Failover Cluster configurations. If downtime is acceptable, you can instead upgrade all nodes at the same time.

Steps

1. Upgrade the DSM on the passive cluster node and reboot Windows.

2. Fail over all cluster resources to the upgraded node that is now running the current DSM version.

3. Upgrade the DSM on the second cluster node and reboot Windows.

Running the DSM upgrade interactively

If you have an earlier version of Data ONTAP DSM for Windows MPIO, you can upgrade to this version. You can also use the silent (command line) upgrade option.

Before you begin

You can upgrade the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled IBM N series customers who have completed the registration process on the N series support website (accessed and navigated as described in *Websites* on page 9).

About this task

For Windows 2003 hosts, the installer will warn you that Windows PowerShell is not installed. You have two options when this happens:

- You can exit the Data ONTAP DSM installer, install Windows PowerShell, and then restart the DSM upgrade.
- You can complete the Data ONTAP DSM upgrade, install Windows PowerShell, repair the DSM, and then reboot your host.

Steps

1. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.

2. Obtain the product software by inserting the DSM CD-ROM into your host machine or by downloading the software from the N series support website (accessed and navigated as described in *Websites* on page 9).

3. Launch the installer program and follow the instructions on the screen.

4. Verify the MPIO license key when prompted. The installer automatically gets the current key value.

5. Select the **Use the default system account** check box. Or optionally enter the user name and password of the account on the Windows host under which the DSM management service will be logged on. This account must be in the Windows Administrators group.

6. Choose whether to install the Hyper-V Guest Utilities.

7. When prompted, click **Yes** to reboot the Windows host and complete the installation.

Result

The installer maintains the existing failover policies for existing LUNs if it can. Verify that your new failover policies are configured the way you want.

> **Note:** If you upgrade to DSM 3.5 from a release prior to 3.4, the default load balance policy and the load balance policy assigned to each existing LUN is changed to Least Queue Depth. Least Queue Depth is the default load balance policy. The installer maintains the existing failover policies if you upgrade from DSM 3.4 to DSM 3.5.

After you finish

For Windows Server 2008 and 2008 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

If the installation program displays a message instructing you to install a Windows hotfix after installing the DSM, download the hotfix from the Microsoft support site and install it.

Related concepts

What the Hyper-V Guest Utilities are on page 35

Running the DSM upgrade from a command line

Run the DSM upgrade from a command prompt to upgrade DSM without operator intervention. You can also upgrade the DSM interactively.

Before you begin

You can upgrade the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled IBM N series customers who have completed the registration process on the N series support website (accessed and navigated as described in *Websites* on page 9).

About this task

Note the following:

- Some of the command options are case sensitive. Be sure to enter the commands exactly as shown.
- The account doing the actual installation must be in the Administrators group. For example, when using rsh, programs are executed under the SYSTEM account by default. You must change the rsh options to use an administrative account.
- To include the silent install command in a script, use `start /b /wait` before the `installer.exe` command. For example: `start /b /wait msiexec /package installer.msi ...` The wait option is needed to get the correct installation return value. If you just run `installer.msi`, it returns "success" if the Windows installer is successfully launched. However, the installation itself may still fail. By using the wait option as shown above, the return code describes the success or failure of the actual installation.

Steps

1. Check the publication matrix page for important alerts, news, interoperability details, and other information about the product before beginning the installation.

2. Obtain the product software by inserting the DSM CD-ROM into your host machine or by downloading the software from the N series support website (accessed and navigated as described in *Websites* on page 9).

3. Enter the following command on your Windows host:

   ```
   msiexec /package installer.msi /quiet /l*v log_file_name LICENSECODE=key
   HYPERVUTIL={0|1} USESYSTEMACCOUNT={0|1} [SVCUSERNAME=domain\user
   SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password]
   [INSTALLDIR=inst_path] [TEMP_FOLDER=temp_path]
   ```

   installer.msi is the DSM installation program for your Windows host's processor architecture.

   log_file_name is the file path and name for the MSI installer log. Note the first character of the l*v option is a lower case L.

`key` is the MPIO license code for the DSM.

HYPERVUTIL=0 specifies that the installation program does not install the Hyper-V Guest Utilities.

HYPERVUTIL=1 specifies that the installation program installs the Hyper-V Guest Utilities.

USESYSTEMACCOUNT=1 specifies that the DSM management service runs under the default SYSTEM account. You do not specify account credentials.

USESYSTEMACCOUNT=0 specifies that the DSM management service run under a different account. You must provide the account credentials.

`domain\user` is the Windows domain and user name of an account in the Administrators group on the Windows host under which the DSM management service will be logged on. The DSM service requires an Administrator-level account to allow it to manage disks and paths on the Windows host.

`password` is the password for the account above.

`inst_path` is the path where the DSM files are installed. The default path is C:\Program Files \IBM\MPIO\.

`temp_path` is the path where log files are written (except the MSI installer log). The default path is C:\temp\ibm\.

> **Note:** To view help for the Windows installer, run the following command:
>
> **msiexec /?**

Because installing the DSM requires a reboot, the Windows host will automatically be rebooted at the end of the quiet installation. There is no warning or prompt before reboot.

Result

The installer maintains the existing failover policies for existing LUNs if it can. Verify that your new failover policies are configured the way you want.

> **Note:** If you upgrade to DSM 3.5 from a release prior to 3.4, the default load balance policy and the load balance policy assigned to each existing LUN is changed to Least Queue Depth. Least Queue Depth is the default load balance policy. The installer maintains the existing failover policies if you upgrade from DSM 3.4 to DSM 3.5.

After you finish

For Windows Server 2008 and 2008 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

If the installation program displays a message instructing you to install a Windows hotfix after installing the DSM, download the hotfix from the Microsoft support site and install it.

Related concepts

Removing or repairing the DSM

You can remove the Data ONTAP DSM for Windows MPIO from your Windows host. The Repair option updates HBA and registry settings and replaces any damaged or missing components.

Uninstalling the Data ONTAP DSM interactively

In most cases you can use the Windows Add or Remove Programs applet to uninstall the Data ONTAP DSM for Windows MPIO interactively.

Before you begin

You will have to reboot your Windows host computer after removing the DSM.

Data ONTAP DSM sets some of the same registry entries as Windows Host Utilities. If you remove the DSM and you have an installed version of the Windows Host Utilities that you still want to use, you must restore the registry entries needed by repairing the Host Utilities.

To prevent accidentally removing the Windows Server 2003 MPIO components needed by another multipathing solution when removing the Data ONTAP DSM (the installer cannot reliably detect a DSM that is not currently active), the installer does not remove all Windows MPIO components. The Data ONTAP DSM 3.5 for Windows MPIO uses MPIO version 1.23 for Windows Server 2003. If you plan to install a program that needs an earlier version of the Windows MPIO code, contact technical support for assistance.

> **Note:** You should not uninstall the DSM for a SAN-booted Windows Server 2003 host. Because the boot LUN uses the DSM and MPIO software, you might lose access to the boot LUN. If you must remove the DSM software, contact technical support for assistance. You can safely upgrade SAN-booted Server 2003 hosts to a later DSM without uninstalling.

Steps

1. Open the Windows **Add or Remove Programs** applet.
2. Select **Data ONTAP DSM for Windows MPIO**.
3. Click **Remove**.
4. Reboot the Windows host when prompted.

After you finish

If the Windows Host Utilities are installed and you still want to use them, run the **Repair** option for Windows Host Utilities from **Add or Remove Programs**.

Uninstalling the DSM silently (unattended)

You can uninstall the Data ONTAP DSM without operator intervention. A reboot of your Windows host is required to complete the procedure.

Before you begin

Data ONTAP DSM sets some of the same registry entries as Windows Host Utilities. If you remove the DSM and you have an installed version of the Windows Host Utilities that you still want to use, you must restore the registry entries needed by repairing the Host Utilities.

To prevent accidentally removing the Windows Server 2003 MPIO components needed by another multipathing solution when removing the Data ONTAP DSM (the installer cannot reliably detect a DSM that is not currently active), the installer does not remove all Windows MPIO components. The Data ONTAP DSM 3.5 for Windows MPIO uses MPIO version 1.23 for Windows Server 2003. If you plan to install a program that needs an earlier version of the Windows MPIO code, contact technical support for assistance.

Note: You should not uninstall the DSM for a SAN-booted Windows Server 2003 host. Because the boot LUN uses the DSM and MPIO software, you might lose access to the boot LUN. If you must remove the DSM software, contact technical support for assistance. You can safely upgrade SAN-booted Server 2003 hosts to a later DSM without uninstalling.

Steps

1. Quiesce host I/O and stop any applications accessing LUNs on the storage system.

2. Open a Windows command line and change to the directory or CD where the Data ONTAP DSM setup program is located.

3. Enter the following command:

   msiexec /uninstall *installer.msi* /quiet /l*v *log_file_name*
   installer.msi is the DSM installation program for your Windows host's processor architecture.

   installer.msi is the DSM installation program for your Windows host's processor architecture.

   log_file_name is the file path and name for the MSI installer log. Note the first character of the l*v option is a lower case L.

After you finish

If the Windows Host Utilities are installed and you still want to use them, run the **Repair** option for Windows Host Utilities from **Add or Remove Programs**.

Repairing the Data ONTAP DSM installation

The installer for the Data ONTAP DSM for Windows MPIO includes a repair option that updates the HBA and Windows registry settings and puts new copies of the DSM and MPIO driver files into the Windows driver folder.

Before you begin

The repair option is available from the Windows **Add or Remove Programs** applet.

You must reboot your Windows host to complete the repair procedure.

Steps

1. Open the Windows Add or Remove Programs applet.

2. Select **Data ONTAP DSM for Windows MPIO**, and click **Change**.

3. Select the **Repair** option.

4. Select the **Use the default system account** check box. Or optionally enter the user name and password of the account on the Windows host under which the DSM management service will be logged on. This account must be in the Windows Administrators group.

5. Following the instructions on the screen and reboot the Windows host when prompted.

Managing the DSM using the GUI

You can manage the Data ONTAP DSM for Windows MPIO using a graphical user interface (GUI), Windows PowerShell cmdlets, or a deprecated command line interface (CLI). The following topics describe how to complete typical management tasks using the GUI.

Related tasks

Starting the DSM GUI

To start the Data ONTAP DSM for Windows MPIO graphical user interface (GUI), open Windows Computer Management. The DSM GUI is a Microsoft management console (MMC) Snapin Extension under the Storage node in both the Server Manager console and the Computer Management console.

Steps

1. Open the Windows Computer Management utility. Select **Start > Administrative Tools > Computer Management**.

2. Expand the **Storage** option in the tree view of Computer Management.

3. Select **Data Ontap DSM Management**.

Result

The DSM GUI is displayed.

After you finish

By default, the DSM GUI manages the local Windows host. To manage the DSM on another Windows host on your network, select **Action > Connect to another computer**.

DSM GUI icon descriptions

The Data ONTAP DSM for Windows MPIO graphical user interface (GUI) uses icons to identify objects displayed in the interface.

Icon	Description
	LUN (virtual disk)
	SAN boot LUN - note that some systems display the LUN icon above for both data LUNs and SAN boot LUNs
	Active path
	Passive path
	Disabled path
	Failed path
	Pending transition path

Discovering new virtual disks (LUNs)

When you add new LUNs to your storage system, the new virtual disks are not automatically discovered by the Windows host. You must manually rescan disks to discover them for the host.

Steps

1. Click **Start > Administrative Tools > Computer Management**.

2. Click **Storage > Disk Management** in the navigation pane.

   The **Initialize and Convert Disk** wizard starts.

3. If the wizard does not start, click **Action > Rescan Disks**.

4. Follow the prompts to initialize the disks, but do not convert them to dynamic disks. Partition and format the disks if desired.

   The new virtual disks appear in the DSM GUI (you may have to refresh the display).

Viewing LUNs (virtual disks)

You can view a list of virtual disks (LUNs) mapped to the Windows host using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI).

Steps

1. In the DSM GUI navigation pane, expand **Data ONTAP DSM Management**.

2. Select **Virtual Disks** in the navigation pane.

   Each LUN is displayed as a virtual disk in the task pane.

After you finish

If you add a new LUN on a storage system and it does not appear in the list, run **Action > Rescan Disks** in Windows **Disk Management** and then refresh the Virtual Disks view.

Virtual Disks view

The Virtual Disks view in Data ONTAP DSM Management displays information about each virtual disk (LUN) mapped to the Windows host from an IBM N series storage system.

The Virtual Disks view is displayed when you select **Virtual Disks** in the navigation tree of Data ONTAP DSM Management.

Field Descriptions

The Virtual Disks view displays the following fields.

Physical Device ID (Mount Points)	Virtual disk name and drive letter or mount point.
Storage System	For Data ONTAP operating in 7-Mode, the name of the storage system to which the LUN belongs. For Data ONTAP operating in Cluster-Mode, the name of the Vserver to which the LUN belongs.
Storage System Path	Volume path to the LUN on the storage system.

LUN	LUN identifier on the storage system.
Serial Number	LUN serial number on the storage system.
Disk Size	Virtual disk unformatted size (usable capacity will be less).
Load Balance Policy	Policy in effect for the virtual disk.
Cluster Mode	Identifies the mode in which Data ONTAP is operating (7-Mode or Cluster-Mode) for the specified LUN.

> **Note:** For Data ONTAP operating in 7-Mode, the storage system's cfmode setting is displayed (for example, Single System Image).

Viewing paths

You can view a list of paths between the storage system and Windows host using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI).

Steps

1. In the DSM GUI navigation pane, expand **Data ONTAP DSM Management**.

2. Select **Virtual Disks** in the navigation pane.

   Each LUN is displayed as a virtual disk in the task pane.

3. Double click the desired virtual disk.

   Each path to the virtual disk is displayed in the task pane.

Paths view

The Paths view in Data ONTAP DSM Management displays information about each path to a virtual disk (LUN).

The Paths view is displayed when you select a virtual disk in the navigation tree of Data ONTAP DSM Management.

Field Descriptions
The Paths view displays the following fields.

Operational State	Available values are as follows:	
	Active	This path is currently used to access the virtual disk. Used for iSCSI paths to LUNs on Data ONTAP operating in 7-Mode.

Active/ Optimized	This path is currently used to access the virtual disk. Optimized paths do not use the storage system interconnect between partner controllers. Used for FC paths to LUNs for Data ONTAP operating in 7-Mode or Cluster-Mode and for iSCSI paths to LUNs for Data ONTAP operating in Cluster-Mode. The DSM also identifies paths to single-controller storage systems as Active/Optimized. This state is applicable to active/active load balance policies only.
Active/Non-optimized	This path is available to take over if no Active/Optimized paths are available. Non-optimized (also called *proxy*) paths use the storage system interconnect between partner controllers and typically have lower performance than Optimized paths. Used for FC paths to LUNs for Data ONTAP operating in 7-Mode or Cluster-Mode and for iSCSI paths to LUNs for Data ONTAP operating in Cluster-Mode. This state is applicable to active/active load balance policies only.
Failed	The system detected an error on this path. It is not used to access the virtual disk.
Passive	This path is available to take over for the active path if the active path fails.
Pending Active	This path is transitioning to an active state.
Pending Passive	This path is transitioning to the passive state.
Pending Remove	This path is in the process of being removed.
Unavailable	The path normally uses the storage system interconnect between partner controllers, but the interconnect is not currently connected.

Administrative State	Available values are as follows:	
	Enabled	The path is enabled for use.
	Disabled	This path is not available to take over for the active path because an administrator set it to disabled.
DSM ID	A unique eight-character identifier on the host for the path. The identifier is made up of four two-digit fields: port, bus, target, and LUN.	

Path ID	An eight-character identifier made up of four two-digit fields. The first three fields are the same as the DSM ID: port, bus, and target. The fourth field indicates the path type: 01 for optimized (non-proxy) and 02 for proxy.
Initiator HBA Name	Name of the FC HBA or iSCSI initiator used for the path.
Initiator HBA Address	World wide port name (WWPN) of the HBA or IP address of the iSCSI initiator used for the path.
Target Adapter/ Portal IP	For FC paths to LUNs for Data ONTAP operating in 7-Mode, the WWPN and port number of the FC adapter on the storage system. For FC paths to LUNs for Data ONTAP operating in Cluster-Mode, the WWPN and the logical interface (LIF), which represents a network access point to a node. For iSCSI paths, the IP address of the storage system and the iSCSI port used for the path.
Preferred Path	Paths that are selected by the administrator to be used when available. Applies only to the Round Robin with Subset and FailOver Only load balance policies.
Path Weight	The priority value assigned to the path by the administrator. The lowest value is the highest priority. Applies only to the Least Weighted Paths load balance policy.

Changing the default load balance policy

The default load balance policy applies to newly-created virtual disks. You can change the default policy using the Data ONTAP DSM for Windows MPIO GUI. The default policy does not affect existing virtual disks.

Steps

1. In the DSM GUI navigation pane, select **Data ONTAP DSM Management**.

2. Click **Action > Set default Load Balance Policy**.

3. Select the desired policy.

Related concepts

Related tasks

Changing the load balance policy for existing LUNs

You can change the load balance policy for an existing LUN (virtual disk) using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI).

About this task

If a virtual disk is not eligible for a given policy, that policy is not available to be selected.

Steps

1. In the DSM GUI navigation pane, expand **Data ONTAP DSM Management**.

2. Select **Virtual Disks** in the navigation pane and then select the desired disk.

3. Select **Action > Set Load Balance Policy**, and then select the desired policy.

After you finish

Select the preferred path or path weights if appropriate.

Related concepts

Load balance policies determine failover behavior on page 28
When to change the load balance policy on page 29

Related tasks

Changing the default load balance policy on page 86

Method for making a path active varies by load balance policy

The method you use to manually make a path active varies, depending on the load balance policy used for the LUN.

When the load balance policy is FailOver Only, you can make the path active directly with the **Action > Set Active** command.

With policy Least Weighted Paths, you can adjust the path weight to specify which path is active.

Related tasks

Disabling a path on page 89
Setting path weight on page 89

Making a path Active

You can make a Passive path Active directly using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI). This action applies only when the load balance policy is FailOver Only.

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. In the task pane, select a Passive path and then click **Action > Set Active**.

Specifying Preferred paths

You can specify the Preferred path that is used whenever it is available using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI). This action applies only when the load balance policy is FailOver Only or Round Robin with Subset.

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. In the task pane, select the desired path and then do the following:

If the policy is...	Then...
FailOver Only	Click **Action > Set Active**.
Round Robin with Subset	Do one of the following: • To make the path preferred, click **Action > Set Preferred**. • To clear the preferred setting, click **Action > Clear Preferred**.

Note: You should avoid making non-optimized (proxy) paths Preferred.

Setting path weight

You can set the weight of a path using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI). This action applies only when the load balance policy is Least Weighted Paths. The available path with the lowest weight is used to access the virtual disk.

About this task

If multiple paths with the same weight value are available, the DSM selects the path shared with the fewest other LUNs.

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. In the task pane, select the desired path and then click **Action > Set Path Weight**.

4. Enter a value between 0 (highest priority) and 2146999999 (lowest priority).

Enabling a path

You can enable a disabled path using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI).

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. In the task pane, select the Disabled path and then click **Action > Enable**.

Disabling a path

You can disable a Passive path using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI). You cannot disable an Active path, except for paths using the Least Queue Depth policy. You must first make another path Active so that the path you want to disable becomes a Passive path.

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. In the task pane, select a Passive path, or an active path using the Least Queue Depth policy, and then click **Action > Disable**.

   If there are multiple passive paths that use the same initiator or HBA port, you can disable all of them at once by selecting **Disable all paths for this initiator**.

Managing the DSM license key

You can view or change the license key for the Data ONTAP DSM for Windows MPIO using the graphical user interface (GUI).

Before you begin

You must purchase a license for each Windows host computer.

Steps

1. In the DSM GUI, select **Data ONTAP DSM Management** in the navigation pane.

2. Click **Action > Modify License Information**.

   The current license key value is displayed.

3. If desired, enter a new key value and then click **OK**.

Displaying the persistent reservation key

You can display the persistent reservation key using the Data ONTAP DSM for Windows MPIO graphical user interface (GUI). This key is used for clustered Windows systems to identify the current owner of a virtual disk (LUN).

About this task

For Windows Server 2003, all LUNs are assigned the same key value on the host. For Windows Server 2008, each LUN has a unique key value.

Steps

1. In the DSM GUI, expand **Data ONTAP DSM Management** in the navigation pane.

2. Expand **Virtual Disks** in the navigation pane, and then select the desired disk.

3. Click **Action > Display Persistent Reservation Key**.

Managing the DSM using Windows PowerShell cmdlets

You can manage the Data ONTAP DSM for Windows MPIO using Windows PowerShell cmdlets. The cmdlets replace the dsmcli commands, which are deprecated starting in DSM 3.5. The dsmcli commands will be removed in a future release.

Related tasks

What you can do with the PowerShell cmdlets

Data ONTAP DSM for Windows MPIO includes Windows PowerShell cmdlets that you can use to manage the DSM. The cmdlets enable you to perform tasks that are available through the legacy dsmcli commands.

The following table lists the common tasks that you can complete with the cmdlets and the dsmcli commands.

Task	PowerShell cmdlet	dsmcli command
Get a list of DSMs on the system	No cmdlet available	`dsmcli dsm list`
Get DSM versions	No cmdlet available	`dsmcli dsm version`
Display the default load balance policy	`get-ontapdsmparams`	`dsmcli dsm getdefaultlbp`
Set a new default load balance policy	`set-ontapdsmparams`	`dsmcli dsm setdefaultlbp`
Display a list of LUNs	`get-sandisk`	`dsmcli lun list`
Display details about LUNs	`get-sandisk`	`dsmcli lun attributes`
Display the current load balance policy for a LUN	`get-sandisk`	`dsmcli path list -v`
Display the load balance policies that you can use with a LUN	`get-ontapdsmparams`	`dsmcli lun getlbp`

Task	PowerShell cmdlet	dsmcli command
Change the load balance policy for a LUN	`set-sandisk`	`dsmcli lun setlbp`
Display the persistent reservation key for a Windows 2003 host	`get-ontapdsmparams`	`dsmcli lun getprkey`
Display path information for a LUN	`get-sanpath`	`dsmcli path list`
Change the status of a path	`set-sanpath`	`dsmcli path`
Change the weight assigned to a path	`set-sanpath`	`dsmcli path weight`
Display SAN connectivity statistics	`get-sanstats`	No command available
Clear SAN connectivity statistics	`clear-sanstats`	No command available
Change values for DSM parameters	`set-ontapdsmparams`	No command available
Change the number of messages that the DSM logs	`set-ontapdsmparams`	No command available

Requirements for the PowerShell cmdlets

You need to follow certain requirements to use the Windows PowerShell cmdlets with Data ONTAP DSM.

Note the following requirements:

PowerShell version PowerShell version 1.0 or 2.0 is required. Note the following about your operating system version:

Windows Server 2003 PowerShell is not installed by default. The Data ONTAP DSM installer instructs you to install PowerShell if you want to use the PowerShell cmdlets with Data ONTAP DSM.

Windows Server 2008 PowerShell 1.0 is installed by default, but not enabled. The DSM installer enables it.

Windows Server 2008 R2 PowerShell 2.0 is installed and enabled by default.

User account for remote execution	A user account with administrator-level credentials is required to run the cmdlets from a remote host. You must enter a user account for the host where Data ONTAP DSM is installed.

Loading the PowerShell cmdlets

You need to load the PowerShell cmdlets before you can use them.

About this task

You can load the cmdlets automatically by launching a PowerShell session from a shortcut in the Start menu or you can manually load them in a PowerShell session.

Note: The shortcut in the Start menu is available for PowerShell 2.0 only. It is not available for PowerShell 1.0. If you have PowerShell 1.0, you need to manually load the cmdlets.

Step

1. Do one of the following:

Option	Description
Launch the PowerShell session from a shortcut in the Start menu	On the host where the Data ONTAP DSM is installed, click **Start > Programs > IBM > Data ONTAP DSM PowerShell**.
Load the cmdlets manually	Enter the following cmdlets at a Windows PowerShell prompt: `set-executionpolicy remotesigned` `add-pssnapin ntapmp` You need to set the execution policy only once on the host. You need to add the snap-in once per PowerShell session.

Running PowerShell cmdlets from a remote host

You do not have to run the PowerShell cmdlets directly from the host on which you want to run the commands. You can run the cmdlets from a remote host.

About this task

The cmdlets use Windows Management Instrumentation (WMI) to gather data remotely and locally. When you run a cmdlet from a remote host and use the `-Credential` parameter to specify a user account, the DSM secures the credentials.

Step

1. When you enter a cmdlet, use the `-ComputerName` parameter and the `-Credential` parameter.

   Where:

   `-ComputerName` specifies the fully qualified domain name or IP address of the host where Data ONTAP DSM is installed. When the remote host is in a different domain from the local host, you must use a fully qualified domain name.

   `-Credential` specifies the user name for a user account that has administrator-level credentials on the host where Data ONTAP DSM is installed. If you do not use this parameter, the cmdlet runs under the user account with which you are currently logged in. Type a user name, such as User01, Domain01\User01, or User@example.com. You can also enter a PSCredential object, such as an object that is returned by the `get-credential` cmdlet. After you enter the command, you will be prompted for a password.

   Example

   ```
   PS C:\>set-sanpath -disk disk4 -path 03000302 -state enable -
   ComputerName host1.example.com -Credential admin
   ```

Getting help with PowerShell cmdlets

Each cmdlet has a help file that you can view to get more information about the cmdlet.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   `get-help cmdlet_name [-detailed]`

   Example

   ```
   PS C:\>get-help set-sanpath -detailed
   ```

Displaying DSM settings

You can use the `get-ontapdsmparams` cmdlet to get information about Data ONTAP DSM. The cmdlet displays the current values for the default load balance policy, for the event log level, and for the parameters that affect how the DSM works.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   `get-ontapdsmparams`

Example

```
PS C:\>get-ontapdsmparams

PathVerifyEnabled          : 0
PathVerificationPeriod     : 30
RetryCount                 : 6
RetryInterval              : 2
PDORemovePeriod            : 130
DefaultLoadBalancePolicy   : DLQD
SupportedLoadBalancePolicies : FO, RR, RRwS, DLQD, WP, Auto
InquiryRetryCount          : 6
InquiryTimeout             : 2
ReservationTimeout         : 60
ReservationRetryCount      : 20
ReservationRetryInterval   : 1
PersistentReservationKey   : :0:0:0:0:0:0:0:0
PathVerificationRetryCount : 6
PathVerificationTimeout    : 2
EventLogLevel              : 1
iSCSILeastPreferred        : 0
```

Setting the default load balance policy

You can use the `set-ontapdsmparams` cmdlet to set the default load balance policy for new virtual disks (LUNs). Load balance policies determine failover behavior.

About this task

The default load balance policy applies to newly created virtual disks. To change the policy for an existing virtual disk, use the `set-sandisk` cmdlet.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   `set-ontapdsmparams -DefaultLoadBalancePolicy lbpolicy`

   Where *lbpolicy* is one of the following:

FO	FailOver Only
RR	Round Robin
RRwS	Round Robin with Subset
DLQD	Least Queue Depth
WP	Least Weighted Paths
Auto	Auto Assigned

Example

```
PS C:\>set-ontapdsmparams -DefaultLoadBalancePolicy RRwS
```

Related concepts

Load balance policies determine failover behavior on page 28
When to change the load balance policy on page 29

Related tasks

Changing the load balance policy for a virtual disk on page 97

Getting information about virtual disks

You can use the get-sandisk cmdlet to view information about the virtual disks (LUNs) that are mapped to the Windows host. For example, you can view the load balance policies assigned to virtual disks and the number of paths to virtual disks.

About this task

If you add a virtual disk on a storage system and it is not listed, rescan disks using the Windows disk manager and then run the get-sandisk cmdlet again.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   get-sandisk [-Disk *DiskID*]

   Example

```
PS C:\>get-sandisk

DiskId LUN MPIODisk    State SerialNumber Size   DsmName          LBPolicy Pat...
------ --- --------    ----- ------------ ----   -------          -------- ---...
Disk7  1   MPIO Disk6  OK    2FiMZ]-7MVhF 10 G   Data ONTAP DSM   RRwS     1  ...
Disk6  0   MPIO Disk5  OK    2FiMg]2SMrCv 50 G   Data ONTAP DSM   FO       2  ...
Disk4  0   MPIO Disk3  OK    2FiMg]2SMrCy 75 G   Data ONTAP DSM   FO       2  ...
Disk5  1   MPIO Disk4  OK    2FiMg]2SMrCz 80 G   Data ONTAP DSM   DLQD     2  ...
Disk1  0   MPIO Disk0  OK    C4e6SJOzpuRC 5122 M Data ONTAP DSM   DLQD     4  ...
Disk3  2   MPIO Disk2  OK    C4e6SJVboRyS 10 G   Data ONTAP DSM   WP       4  ...
Disk8  0   MPIO Disk7  OK    C4e6SJYoOFUc 5122 M Data ONTAP DSM   RRwS     4  ...
Disk2  1   MPIO Disk1  OK    C4e6hJOzqAJ8 40 G   Data ONTAP DSM   DLQD     4  ...
```

Changing the load balance policy for a virtual disk

You can use the set-sandisk cmdlet to change the load balance policy for a virtual disk (LUN). Changing the load balance policy affects how the DSM selects active paths.

About this task

You specify a virtual disk by entering the disk ID. The get-sandisk cmdlet displays disk IDs.

To display the current load balance policy for each virtual disk, use the get-sandisk cmdlet.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   set-sandisk -disk *DiskID* -lbpolicy *lbpolicy*

   Where *lbpolicy* is one of the following:

FO	FailOver Only
RR	Round Robin
RRwS	Round Robin with Subset
DLQD	Least Queue Depth
WP	Least Weighted Paths
Auto	Auto Assigned

   Example

   ```
   PS C:\>set-sandisk -disk disk8 -lbpolicy RR
   ```

Related concepts

Load balance policies determine failover behavior on page 28
When to change the load balance policy on page 29

Related tasks

Getting information about virtual disks on page 96

Displaying path information

You can use the `get-sanpath` cmdlet to view information about all of the paths for one or all virtual disks (LUNs) that are mapped to the Windows host. For example, you can view the path IDs and path states for virtual disks.

About this task

You can display path information for a single virtual disk by specifying the disk ID. The `get-sandisk` cmdlet displays disk IDs.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   `get-sanpath [-Disk DiskID]`

   Example

```
PS C:\>get-sanpath

DiskId DSMId     PathId   OperationalState       AdminState Protocol Preferred W...
------ -----     ------   ----------------       ---------- -------- --------- -...
Disk1  04000100 04000101 Active/Optimized       Enabled    FC       True      0...
Disk1  03000100 03000101 Active/Optimized       Enabled    FC       True      0...
Disk1  03000000 03000002 Active/Non-Optimized   Enabled    FC       False     0...
Disk1  04000000 04000002 Active/Non-Optimized   Enabled    FC       False     0...

Disk2  04000001 04000001 Active/Optimized       Enabled    FC       True      0...
Disk2  03000001 03000001 Active/Optimized       Enabled    FC       True      0...
Disk2  03000101 03000102 Active/Non-Optimized   Enabled    FC       False     0...
Disk2  04000101 04000102 Active/Non-Optimized   Disabled   FC       False     0...
```

Related tasks

Changing path status

You can use the `set-sanpath` cmdlet to change the status of a path. For example, you can enable and disable paths. The state that you can assign to a path depends on the load balance policy of the virtual disk (LUN) and the status of the other paths.

Before you begin

You specify the path that you want to change by entering the disk ID and path ID. The `get-sanpath` cmdlet displays disk IDs and path IDs.

Note:

- You cannot make a path Active or Passive directly for the Least Weighted Paths policy. Instead, change the weight of the paths to determine which is active using the `set-sanpath` cmdlet with the `-weight` parameter.
- You cannot disable a path if no other path is available to take over; there must always be an active path.
- Although you can make a non-optimized (proxy) path active, you should avoid doing so if any optimized paths are available.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

   `set-sanpath -disk DiskID -path PathID -state State`

   Where `State` is one of the following:

enable	Enables a disabled path.
disable	Disables a passive path. You must first make another path active so that the path you want to disable becomes a passive path.
active	Makes a passive path active.
prefer	Changes the path to a preferred path.
noprefer	Changes the path so it is no longer a preferred path.

   ### Example

   ```
   PS C:\>set-sanpath -disk disk4 -path 03000302 -state enable
   ```

Related concepts

Related tasks

Supported path changes for load balance policies

The allowed path changes using the `set-sanpath` cmdlet depends on the load balance policy for the path.

The following table lists the path changes that are allowed for each load balance policy. Note that a command might not be allowed because it tries to remove the only active path.

Load balance policy	enable	disable	active	prefer	noprefer
Auto Assigned	Yes	Yes	No	No	No
FailOver Only	Yes	Yes	Yes	No	No
Least Queue Depth	Yes	Yes	No	No	No
Least Weighted Paths	Yes	Yes	No	No	No
Round Robin	Yes	Yes	No	No	No
Round Robin with Subset	Yes	Yes	No	Yes	Yes

Note: You cannot disable an active path. First make another path active, then disable the passive path.

Changing the path weight

You can use the `set-sanpath` cmdlet to set the weight that is assigned to each path for virtual disks (LUNs) that are assigned the Least Weighted Path load balance policy. DSM uses the available path with the lowest weight to access a LUN.

Before you begin

You specify the path that you want to change by entering the disk ID and path ID. The `get-sanpath` cmdlet displays disk IDs and path IDs.

If multiple paths with the same weight value are available, the DSM selects the path that is shared with the fewest other virtual disks. Initially, all paths are set to 255. The active path is then set to 5.

You can use the `get-sandisk` cmdlet to identify the load balance policy that is assigned to a virtual disk.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

    set-sanpath -disk *DiskID* -path *PathID* -weight *pathweight*

    Where *pathweight* is a number from 0 (highest priority) to 2146999999 (lowest priority).

    Example

    ```
    PS C:\>set-sanpath -disk disk3 -path 04000101 -weight 0
    ```

Related concepts

Related tasks

Displaying statistics about SAN connectivity

You can use the `get-sanstats` cmdlet to display statistics about SAN connectivity. You can use the statistics to analyze and monitor the input/output (IO) for a path to a virtual disk (LUN). For example, you can see the number of reads and writes for a path.

About this task

You can display statistics for all virtual disks or for a single virtual disk by specifying the disk ID. The `get-sandisk` cmdlet displays disk IDs.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

`get-sanstats [-Disk DiskID]`

Example

```
PS C:\>get-sanstats -Disk Disk5

DiskId PathId    NumberOfReads NumberOfWrites NumberOfBytesRead NumberOfBytesWr...
------ ------    ------------- -------------- ----------------- ---------------...
Disk5  03000302 757           21             3280384           86016          ...
Disk5  04000202 2             1              1024              4096           ...
```

Clearing SAN connectivity statistics

The `get-sanstats` cmdlet provides statistics about SAN connectivity. You can use the `clear-sanstats` cmdlet to reset the statistics values to 0.

About this task

You can clear statistics for all virtual disks or for a single virtual disk by specifying the disk ID. The `get-sandisk` cmdlet displays disk IDs.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

```
clear-sanstats [-Disk DiskID]
```

Related tasks

Prioritizing FC paths over iSCSI paths

You can use the iSCSILeastPreferred parameter to specify that the Data ONTAP DSM uses iSCSI optimized paths only if there are no FC optimized paths available. You might enable this setting if you want to use iSCSI paths as backups to FC paths.

About this task

By default, the DSM uses ALUA access states to prioritize paths. It does not prioritize by protocol. If you enable this setting, the DSM prioritizes by ALUA state and protocol, with FC paths receiving priority over iSCSI paths that go to the same virtual disk.

This setting applies to all virtual disks that have a load balance policy of either Least Queue Depth or Round Robin with Subset.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

```
set-ontapdsmparams -iSCSILeastPreferred value
```

Where the allowed values are "0" (no preference) and "1" (FC preferred).

Example

```
PS C:\>set-ontapdsmparams -iSCSILeastPreferred 1
```

Modifying values for DSM parameters

You can use the set-ontapdsmparams cmdlet to modify values for the DSM parameters that affect how the DSM works. You should not change the values unless directed to do so by your storage system support representative.

About this task

This task describes how to use the set-ontapdsmparams cmdlet to modify values for the parameters that the Data ONTAP DSM uses to optimize performance and ensure correct failover and giveback behavior.

You can also use the set-ontapdsmparams cmdlet to change the default load balance policy, to prioritize FC paths over iSCSI paths, and to change what gets logged by the DSM. You can perform those tasks without guidance from your storage system support representative.

Step

1. Enter the following cmdlet at a Windows PowerShell prompt:

```
set-ontapdsmparams [-{pathverificationperiod, PVP} value] [-
{pathverifyenabled, PVE} value] [-{pdoremoveperiod, PDORP} value] [-
{retrycount, RC} value] [-{retryinterval, RI} value] [-
{inquiryretrycount, IRC} value] [-{inquirytimeout, IT} value] [-
{reservationtimeout, RT} value] [-{reservationretrycount, RRC} value] [-
{reservationretryinterval, RRI} value] [-{pathverificationretrycount,
PVRC} value] [-{pathverificationtimeout, PVT} value]
```

Example

```
PS C:\>set-ontapdsmparams -pathverificationperiod 60 -PVE 1
```

Related tasks

Related references

Managing the DSM using the legacy dsmcli

You can manage the Data ONTAP DSM for Windows MPIO using a command line interface (CLI); however, the dsmcli commands are deprecated starting in DSM 3.5. The commands will be removed in a future release. Windows PowerShell cmdlets replace the dsmcli commands.

Related tasks

Managing the DSM using the GUI on page 81
Managing the DSM using Windows PowerShell cmdlets on page 91

CLI overview

The DSM command line interface (CLI) uses the dsmcli command. It has three main options.

You can enter dsmcli commands from any Windows command prompt. The main dsmcli command options are:

dsmcli dsm Displays information about installed device-specific modules and displays or sets the default load balance policy.

dsmcli lun Displays information about LUNs managed by the DSM and sets the load balance policy for individual LUNs.

dsmcli path Lists the failover status of each LUN, enables and disables paths, and sets a passive path to active.

To prevent text from wrapping, it is recommend that you set the command window width to 160 characters when using the CLI.

Getting DSM information (legacy dsmcli)

The dsmcli dsm list and dsmcli dsm version commands list information about the DSM.

Steps

1. Enter the following command at a Windows command prompt:

   dsmcli dsm list

   The DSMs on the system are displayed.

2. Enter

   dsmcli dsm version

The Data ONTAP DSM and Windows MPIO components versions are displayed.

```
C:\>dsmcli dsm list
Number of DSM registered with MPIO is 1
List of DSMs registered with MPIO:
        "Data ONTAP DSM"

C:\>dsmcli dsm version
DSM MGMT Dll version 3.4.35385.2230 built on 09/21/2010 22:36:44
ONTAPDSM Driver   version 3.4.35385.2230 built on 09/21/2010 22:34:38
MSFT MPIO Driver version 6.0.6002.22355 built on 03/05/2010 12:31:03
MSDSM Driver version 6.0.6002.18005 built on 04/11/2009 00:15:30
```

Setting the default load balance policy (legacy dsmcli)

The dsmcli dsm setdefaultlbp command sets the default load balance policy for new virtual disks. The dsmcli dsm getdefaultlbp displays the current default policy.

About this task

The default load balance policy applies only to newly created virtual disks. To change the policy for an existing virtual disk, use the dsmcli lun setlbp command.

Steps

1. Enter the following command at a Windows command prompt to display the current policy:

   dsmcli dsm getdefaultlbp

2. Enter the following command to set a new policy:

   dsmcli dsm setdefaultlbp -l*policy*

   policy values are: AA (Auto Assigned), FO (FailOver Only), LQD (Least Queue Depth), RR (Round Robin), RS (Round Robin with Subset), or WP (Least Weighted Paths).

```
C:\>dsmcli dsm getdefaultlbp
dsmcli: The default load balance policy for the dsm is   LEAST QUEUE
DEPTH

C:\>dsmcli dsm setdefaultlbp -l WP
```

```
dsmcli: The default load balance policy for the dsm is set to
WEIGHTED PATH.
```

Related concepts

Getting LUN information (legacy dsmcli)

The dsmcli lun list and dsmcli lun attributes commands display information about the LUNs (virtual disks) mapped to the Windows host.

About this task

If you add a LUN on a storage system and it is not listed, rescan disks using the Windows disk manager and then run the dsmcli command again.

Steps

1. Enter the following command at a Windows command prompt to display a list of LUNs:

   dsmcli lun list

2. Enter the following command to display details about the LUNs:

   dsmcli lun attributes

```
C:\>dsmcli lun list
Luns managed by Data ONTAP(R) DSM
C4e6SJ-o-rl1
C4e6SJ-oA5R9
C4e6hJBOr61c
C4e6hJBOr8rk

C:\>dsmcli lun attributes
Luns managed by Data ONTAP(R) DSM
SerialNumber   Storage System   Storage System Path      MountPath
************   **************   ******************       *********
C4e6SJ-o-rl1   SS1              /vol/vol1/winserv_0       E:\
C4e6SJ-oA5R9   SS1              /vol/vol1/winserv_1       F:\
```

```
C4e6hJBOr61c  SS2                 /vol/vol1/winserv_2        G:\
C4e6hJBOr8rk  SS2                 /vol/vol1/winserv_3        H:\
```

Changing the load balance policy for a LUN (legacy dsmcli)

The dsmcli lun setlbp command sets the load balance policy for a single LUN (virtual disk).

Before you begin

You can specify the LUN by serial number or by Windows disk letter. You can get the serial number of a LUN using the dsmcli lun attribute command.

The available load balance policies for a LUN depend on your configuration. The dsmcli lun getlbp command displays the valid policies for a specified LUN.

The dsmcli path list -v command displays the current load balance policy for each LUN.

Step

1. Enter the following command at a Windows command prompt:

   dsmcli lun setlbp -l *policy* { -s *serial_number* | - d *drive_letter* }

   policy values are: AA (Auto Assigned), FO (FailOver Only), LQD (Least Queue Depth), RR (Round Robin), RS (Round Robin with Subset), or WP (Least Weighted Paths).

   ```
   C:\>dsmcli lun setlbp -l RR -s  C4e6hJBOr8rk
   dsmcli: The load balance policy for the lun is set to  ROUND ROBIN

   C:\>dsmcli lun setlbp -l AA -d H
   dsmcli: The load balance policy for the lun is set to  AUTO ASSIGNED
   ```

Related concepts

Load balance policies determine failover behavior on page 28
When to change the load balance policy on page 29

Related tasks

Getting LUN information (legacy dsmcli) on page 107
Getting the load balance policy for a LUN (legacy dsmcli) on page 109
Listing available load balance policies for a LUN (legacy dsmcli) on page 109

Getting the load balance policy for a LUN (legacy dsmcli)

The `dsmcli path list -v` command displays the current load balance policy for each LUN.

Before you begin

The available load balance policies for a LUN depend on your configuration. The `dsmcli lun getlbp` command displays the valid policies for a specified LUN.

Step

1. Enter the following command at a Windows command prompt:

   dsmcli path list -v

```
C:\>dsmcli path list -v

Path Info for C4e6hJIOegMp:
Load Balance Policy:  LEAST QUEUE DEPTH
Number of Paths: 6
...
```

Listing available load balance policies for a LUN (legacy dsmcli)

The `dsmcli lun getlbp` command displays the load balance policies that can be used with the specified virtual disk (LUN).

Before you begin

You can specify the LUN by serial number or by Windows disk letter. You can get the serial number of a LUN using the `dsmcli lun attribute` command.

Step

1. Enter the following command at a Windows command prompt: dsmcli lun getlbp { -s *serial_number* | - d *drive_letter* }

```
C:\>dsmcli lun getlbp -d E
dsmcli: The supported Load Balance policies for this LUN are
 FAILOVER
 WEIGHTED PATHS
 AUTO ASSIGNED
```

```
 ROUND ROBIN
 ROUND ROBIN WITH SUBSET
 LEAST QUEUE DEPTH

C:\>dsmcli lun getlbp -s C4e6hJIOeUJM
dsmcli: The supported Load Balance policies for this LUN are
 FAILOVER
 WEIGHTED PATHS
 AUTO ASSIGNED
 ROUND ROBIN
 ROUND ROBIN WITH SUBSET
 LEAST QUEUE DEPTH
```

Related concepts

Load balance policies determine failover behavior on page 28

Related tasks

Getting the load balance policy for a LUN (legacy dsmcli) on page 109
Getting LUN information (legacy dsmcli) on page 107

Viewing the persistent reservation key (legacy dsmcli)

The Data ONTAP DSM for Windows MPIO uses a persistent reservation key to track which host in a
Microsoft Windows 2003 cluster (MSCS) or Windows 2008 Failover Cluster is currently allowed to
write to a virtual disk (LUN). The dsmcli lun getprkey command displays the key for each
virtual disk.

Before you begin

You can specify the LUN by serial number or by Windows disk letter. You can get the serial number
of a LUN using the dsmcli lun attribute command.

In Windows Server 2003, all virtual disks on the host have the same value. In Windows Server 2008,
each virtual disk has a unique value.

For LUNs that do not belong to a cluster on Windows Server 2008 , the key is set to zeros (0 0 0 0 0
0 0 0).

Step

1. Enter the following command at a Windows command prompt:

   dsmcli lun getprkey {-s *serial_number* | -d *drive_letter*}

   ```
   C:\>dsmcli lun getprkey -d N
   ```

```
The Persistent Reservation Key for lun C4e6hJHJGdSi is: 99 54 48 99
54 2 2 5
```

Related tasks

Displaying path information (legacy dsmcli)

The dsmcli path list command displays all of the paths for one or all virtual disks (LUNs) mapped to the Windows host.

Before you begin

To display the paths for a single virtual disk, specify the serial number or drive letter. Use the verbose (-v) option to get additional details on each path.

Step

1. Enter the following command at a Windows command prompt:

dsmcli path list [-s *serial_number* | -d *drive_letter*] [-v]

Set your display to 160 columns or more to best display the verbose output.

```
C:\>dsmcli path list -v

Path Info for C4e6hJOzqAJ8:
Load Balance Policy:   LEAST QUEUE DEPTH
Number of Paths: 4
OperationalState      AdminState   DSM ID   Path ID   Initiator Na...
================      ==========   ======   =======   ============...
ACTIVE/OPTIMIZED      ENABLED      04000001 04000001 com.emulex-4...
ACTIVE/OPTIMIZED      ENABLED      03000001 03000001 com.emulex-4...
```

```
ACTIVE/NON-OPTIMIZED   ENABLED        03000101 03000102 com.emulex-4...
ACTIVE/NON-OPTIMIZED   ENABLED        04000101 04000102 com.emulex-4...
```

Changing path status (legacy dsmcli)

The `dsmcli path enable`, `dsmcli path disable`, `dsmcli path active`, and `dsmcli path passive` commands change the status of the specified path. The actions you can take depend on the load balance policy of the virtual disk and the status of the other paths.

Before you begin

You specify the path you want to change using the DSM ID. You can get the DSM ID using the `dsmcli path list` command.

Note:

- You cannot make a path Active or Passive directly for the Least Weighted Paths policy. Instead, change the weight of the paths to determine which is active using the `dsmcli path weight` command.
- You cannot disable a path if no other path is available to take over; there must always be an active path.
- Although you can make a non-optimized (proxy) path active, you should avoid doing so if any optimized paths are available.

Step

1. Enter the following command at a Windows command prompt:

dsmcli path { enable | disable | active | passive } -p *DSM_ID*

```
C:\>dsmcli path disable -p 03000001
dsmcli:Path 0x03000001 is DISABLED

C:\>dsmcli path enable -p 03000001
dsmcli:Path 0x03000001 is ENABLED

C:\>dsmcli path active -p 03000102
dsmcli:Path 0x03000102 is set to ACTIVE state

C:\>dsmcli path passive -p 03000102
dsmcli:Path 0x03000102 is set to PASSIVE state
```

Related tasks

Supported path changes for load balance policies (legacy dsmcli)

The allowed path changes using the `dsmcli path { enable | disable | active | passive }` commands depend on the load balance policy for the path.

The following table lists which commands are allowed for each load balance policy. Note that a command might not be allowed because it tries to remove the only active path.

Table 1: Path changes allowed for each load balance policy

Load balance policy	enable	disable	active	passive
Auto Assigned	Yes	Yes	No	No
FailOver Only	Yes	Yes	Yes	No
Least Queue Depth	Yes	Yes	No	No
Least Weighted Paths	Yes	Yes	No	No
Round Robin	Yes	Yes	No	No
Round Robin with Subset	Yes	Yes	No	Yes

Note: You cannot disable an active path. First make another path active, then disable the passive path.

Changing the path weight (legacy dsmcli)

The dsmcli path weight command sets the weight assigned to each path for virtual disks with the Least Weighted Path load balance policy. The available path with the lowest weight is used to access the virtual disk.

Before you begin

If multiple paths with the same weight value are available, the DSM selects the path shared with the fewest other LUNs. Initially, all paths are set to 255. The active path is then set to 5.

Step

1. Enter the following command at a Windows command prompt:

   dsmcli path weight -p *DSM_ID* -w *weight*

DSM_ID is available from the dsmcli path list command

weight can be set from 0 (highest priority) to 2146999999 (lowest priority).

```
C:\>dsmcli path weight -p 04000100 -w 0
dsmcli:Path 0x04000100 weight is set to  0
```

Related tasks

Configuring for Fibre Channel and iSCSI

You must configure both the host and the storage system to enable storage access using Fibre Channel or iSCSI connections.

Configuring for FC and iSCSI includes the following tasks.

1. Recording FC and iSCSI initiator identifiers.

2. Creating LUNs and making them available as disks on the host computer.

What FC and iSCSI identifiers are

The storage system identifies hosts that are allowed to access LUNs based on the FC worldwide port names (WWPNs) or iSCSI initiator node name on the host.

Each Fibre Channel port has its own WWPN. A host has a single iSCSI node name for all iSCSI ports. You need these identifiers when manually creating initiator groups (igroups) on the storage system.

Recording the WWPN

Record the worldwide port names of all FC ports that connect to the storage system.

About this task

Each HBA port has its own WWPN. For a dual-port HBA, you need to record two values; for a quad-port HBA, record four values.

The WWPN looks like this:

```
WWPN: 10:00:00:00:c9:73:5b:90
```

Steps

1. For Windows Server 2008 or Windows Server 2008 R2, use the Windows Storage Explorer application to display the WWPNs. For Windows Server 2003, use the Microsoft `fcinfo.exe` program.

   You can instead use the HBA manufacturer's management software, such as HBAnyware for Emulex HBAs or SANsurfer for QLogic HBAs, if it is installed on the Windows host.

2. If the system is SAN booted and not yet running an operating system, or the HBA management software is not available, obtain the WWPNs using the boot BIOS.

Obtaining the WWPN using Windows Storage Explorer

For hosts running Windows Server 2008 or Windows Server 2008 R2, you can obtain the Fibre Channel World Wide Port Name (WWPN) using the Windows Storage Explorer application.

Steps

1. In Windows Server 2008 or Windows Server 2008 R2, select **Start > Administrative Tools > Storage Explorer.**

2. Expand the **Servers** node of the Storage Explorer console tree and locate the HBAs.

3. Record the value of the **Port WWN** field for each HBA port.

Obtaining the WWPN using Microsoft fcinfo.exe

For hosts running Windows Server 2003, you can obtain the Fibre Channel World Wide Port Name (WWPN) using the Microsoft fcinfo.exe.

Steps

1. If not already installed, download and install the fcinfo.exe program from the Microsoft Download Center. Search the Download Center for "Fibre Channel Information Tool (fcinfo)".

   A reboot is not required.

2. In Windows Server 2003, open a command prompt and enter the following command: fcinfo / ports /details

   For more options, run the `fcinfo /??` command.

3. Record the port WWN value for each HBA port.

Related information

   Microsoft Download Center

Obtaining the WWPN using Emulex BootBIOS

For SAN-booted systems with Emulex HBAs that do not yet have an operating system, you can get the WWPNs from the boot BIOS.

Steps

1. Restart the host.

2. During startup, press **Alt-E** to access BootBIOS.

3. Select the menu entry for the Emulex HBA.

   BootBIOS displays the configuration information for the HBA, including the WWPN.

4. Record the WWPN for each HBA port.

Obtaining the WWPN using QLogic BootBIOS

For SAN-booted systems with QLogic HBAs that do not yet have an operating system, you can get the WWPNs from the boot BIOS.

Steps

1. Restart the host.

2. During startup, press **Ctrl-Q** to access BootBIOS.

3. Select the appropriate HBA and press **Enter**.

The Fast!UTIL options are displayed.

4. Select **Configuration Settings** and press **Enter**.

5. Select **Adapter Settings** and press **Enter**.

6. Record the WWPN for each HBA port from the **Adapter Port Name** field.

Recording the iSCSI initiator node name

Record the iSCSI initiator node name from the iSCSI Initiator program on the Windows host.

Steps

1. For Windows Server 2008, Windows Server 2008 R2, and Windows Vista, click **Start > Administrative Tools > iSCSI Initiator**. For Windows Server 2003 and Windows XP, click **Start > All Programs > Microsoft iSCSI Initiator > Microsoft iSCSI Initiator**.

The iSCSI Initiator Properties dialog box is displayed.

2. Copy the **Initiator Name** or **Initiator Node Name** value to a text file or write it down.

The exact label in the dialog box differs depending on the Windows version. The iSCSI node name looks like this:

```
iqn.1991-05.com.microsoft:server3
```

Setting up LUNs

LUNs are the basic unit of storage in a SAN configuration. The host system uses LUNs as virtual disks.

LUN overview

You can use a LUN the same way you use local disks on the host.

After you create the LUN, you must make it visible to the host. The LUN then appears on the Windows host as a disk. You can:

- Format the disk with NTFS. To do this, you must initialize the disk and create a new partition. Only basic disks are supported with the native OS stack.
- Use the disk as a raw device. To do this, you must leave the disk offline. Do not initialize or format the disk.
- Configure automatic start services or applications that access the LUNs. You must configure these start services so that they are dependent on the Microsoft iSCSI Initiator service.

LUN types to use for hosts and guest operating systems

The LUN type determines the on-disk layout of the LUN.

It is important to specify the correct LUN type to ensure good performance. The LUN type you specify depends on the Windows version and disk type and the Data ONTAP version.

Note: Not all LUN types are available when you create LUNs using the FilerView interface for some versions of Data ONTAP software. To use the hyper_v, windows_2008, windows_gpt, and windows_lhs LUN types, you might have to create the LUN using the Data ONTAP command line interface.

Use the following table to select the correct LUN type.

LUN type	Data ONTAP	Windows disk type and version
windows	All	Master boot record (MBR) on - Windows Server 2003 - Windows XP - Windows Vista
hyper_v	7.3.1 and later	Windows Server 2008 and Windows Server 2008 R2 Hyper-V LUNs containing virtual hard disks (VHDs). **Note:** For raw LUNs, use the type of child operating system as the LUN type.

LUN type	Data ONTAP	Windows disk type and version
windows_2008	7.2.5 and later 7.3.0 RC2 and later	All other disks on Windows Server 2008 and Windows Server 2008 R2
windows_gpt	7.2.1 and later	GUID Partition Type (GPT) disks on Windows Server 2003
windows_lhs	7.3.0 RC1	All disks on Windows Server 2008
linux	7.2.4 and earlier	All disks on Windows Server 2008

Overview of creating LUNs

You can create LUNs manually, or by running SnapDrive or System Manager software.

You can access the LUN using either the FC or the iSCSI protocol. The procedure for creating LUNs is the same regardless of which protocol you use. You must create an initiator group (igroup), create the LUN, and then map the LUN to the igroup.

> **Note:** If you are using the optional SnapDrive software, use SnapDrive to create LUNs and igroups. Refer to the documentation for your version of SnapDrive for specific steps. If you are using the optional System Manager software, refer to the Online Help for specific steps.

The igroup must be the correct type for the protocol. You cannot use an iSCSI igroup when you are using the FC protocol to access the LUN. If you want to access a LUN with both FC and iSCSI protocols, you must create two igroups, one FC and one iSCSI. For Data ONTAP 8.1 operating in Cluster-Mode, you can create an igroup with the mixed protocol type.

To step through the process of creating an igroup and LUN on the storage system, you can use the `lun setup` command for Data ONTAP operating in 7-Mode and the `vserver setup` command for Data ONTAP operating in Cluster-Mode. You can also create igroups and LUNs by executing a series of individual commands (such as `igroup create`, `lun create`, and `lun map`). Detailed steps for creating LUNs are in the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP software.

Initiator group overview

Initiator groups specify which hosts can access specified LUNs on the storage system. You can create igroups manually, or use the optional SnapDrive for Windows software, which automatically creates igroups.

Initiator groups (igroups) are protocol-specific.

For FC connections, create an FC igroup using all WWPNs for the host.

For iSCSI connections, create an iSCSI igroup using the iSCSI node name of the host.

For systems using both FC and iSCSI connections to the same LUN, create two igroups: one for FC and one for iSCSI. Then map the LUN to both igroups. You cannot create a combined FC/iSCSI igroup for Data ONTAP 7.3 or Data ONTAP 8.x operating in 7-Mode. Data ONTAP 8.1 operating in Cluster-Mode supports mixed protocol igroups.

There are many ways to create and manage initiator groups and LUNs on your storage system. These processes vary, depending on your configuration. These topics are covered in detail in the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP software.

If you use the optional SnapDrive for Windows software, it creates igroups as needed. Starting with SnapDrive 6.4 for Windows, the SnapDrive software enables ALUA when it detects Data ONTAP DSM 3.5 for Windows MPIO. Starting with SnapDrive 6.2 for Windows, the SnapDrive software enables ALUA when it detects the msdsm. For earlier versions of SnapDrive, you need to manually enable ALUA.

Mapping LUNs to igroups

When you map a LUN to an igroup, you assign the LUN identifier.

You must assign the LUN ID of 0 to any LUN that will be used as a boot device. LUNs with IDs other than 0 are not supported as boot devices.

If you map a LUN to both an FC igroup and an iSCSI igroup, the LUN has two different LUN identifiers.

> **Note:** The Windows operating system only recognizes LUNs with identifiers 0 through 254, regardless of the number of LUNs mapped. Be sure to map your LUNs to numbers in this range.

About mapping LUNs for Windows clusters

When you use clustered Windows systems, all members of the cluster must be able to access LUNs for shared disks.

Map shared LUNs to an igroup for each node in the cluster.

> **Attention:** If more than one host is mapped to a LUN, you must run clustering software on the hosts to prevent data corruption.

About FC targets

The host automatically discovers FC targets that are accessible to its HBAs. However, you do need to verify that the host selects only primary (optimized) paths to FC targets.

About non-optimized paths in FC configurations

Non-optimized paths are intended for use when certain storage system resources are not available.

A configuration has both optimized and non-optimized FC paths. Non-optimized paths have higher overhead and possibly lower performance. To prevent performance problems, make sure the FC paths are configured so that non-optimized paths are only used when there is a failure.

If your FC paths are not configured correctly, routine traffic can flow over a non-optimized path. The storage system measures FC traffic over optimized and non-optimized paths. If it detects significant traffic on a non-optimized path, the storage system issues a log message and triggers an AutoSupport message.

Verifying FC paths to LUNs

When you configure your host for FC, verify that the active paths are optimized paths.

About this task

You can verify the paths by mapping a LUN to the host on each storage system node, generating I/O to the LUN, and then checking the FC statistics on each node.

For Data ONTAP operating in Cluster-Mode, run the `sysstat` command through the nodeshell. You can access the nodeshell by using the `system node run` command. For information about how to use the `system node run` command, see the man page.

Steps

1. Map a LUN to the host on each node.

2. On the consoles of each node, start collecting statistics using the following command:

   `sysstat -b`

3. Generate I/O to the LUNs.

4. Check the FC statistics on each storage system node to verify that the non-optimized paths have essentially no traffic. The `sysstat` command periodically writes a line of statistics to the console. Check the Partner columns; the values should remain close to zero, while the FCP columns should show data.

   Note: Some initiators send occasional traffic over passive paths to ensure they are still available, so you typically see some traffic on non-optimized paths even when the system is correctly configured.

5. Enter **Ctrl-C** to exit the `sysstat` command on each console.

Result

If the Partner values remain close to zero, traffic is flowing over the correct paths. If the Partner values are high, as in the example below, the paths are not configured correctly.

Example of high partner values

In this example, all FC traffic is flowing over the non-optimized paths. Some columns from the `sysstat` command are removed from the example to make it easier to read.

```
CPU FCP iSCSI Partner Total FCP kB/s Partner kB/s
                            in   out    in   out
```

```
6%    0       0     124      124    0     0      5987    26
9%    0       0     186      186    0     0      9777    15
7%    0       0     147      147    0     0      6675    26
6%    0       0      87       87    0     0      3934    14
1%    0       0       6        6    0     0       257     0
```

Adding iSCSI targets

To access LUNs when you are using iSCSI, you must add an entry for the storage system using the Microsoft iSCSI Initiator GUI.

About this task

For Data ONTAP 7.3 and Data ONTAP operating in 7-Mode, you only need one entry for each storage system in the configuration, regardless of the number of interfaces that are enabled for iSCSI traffic. An active/active or HA pair storage system configuration must have two entries, one for each storage system node in the configuration.

For Data ONTAP 8.1 operating in Cluster-Mode, create an entry for each iSCSI logical interface on each node that can access the LUN. MPIO software on the host is needed to select the correct path or paths.

The iSCSI Initiator GUI manages connections for both the software initiator and the optional iSCSI HBAs.

You can also add entries for the targets using the `iscsicli` interface. Enter `iscsicli help` on the Windows command line for more information on `iscsicli`.

If you are using SnapDrive for Windows software, use the SnapDrive interface to add iSCSI targets.

To add a target, complete the following steps.

Steps

1. Run the Microsoft iSCSI Initiator GUI.

2. On the **Discovery** tab, create an entry for the storage system.

3. On the **Targets** tab, log on to the storage system.

4. If you want the LUNs to be persistent across host reboots, select the **Automatically restore this connection when the system boots** check box when logging on to the target.

5. If you are using MPIO or multiple connections per session, create additional connections to the target as needed.

   Enabling the optional MPIO support or multiple-connections-per-session support does not automatically create multiple connections between the host and storage system. You must explicitly create the additional connections.

   For Windows Server 2003, see the section "Multipathing I/O" in the Microsoft *iSCSI Software Initiator 2.x Users Guide* for specific instructions on configuring multiple paths to iSCSI LUNs.

For Windows Server 2008 or Windows Server 2008 R2, see the iSCSI topics in Help.

About dependent services on the Native Stack and iSCSI

When you use disks based on iSCSI LUNs on a Host Utilities Native stack, you must reconfigure any dependent service or application to start after the iSCSI service.

The Windows disks that are based on iSCSI LUNs become available later in the startup sequence than the local disks do. This can create a problem if you have not reconfigured the dependent services or applications.

Overview of initializing and partitioning the disk

You can create one or more basic partitions on the LUN.

After you rescan the disks, the LUN appears in Disk Management as an Unallocated disk.

If you format the disk as NTFS, be sure to select the **Perform a quick format** option.

The procedures for initializing disks vary depending on which version of Windows you are running on the host. See the Windows Disk Management online Help for more information.

Setting up a SAN boot LUN for Windows Server

You can boot a host from a storage system LUN instead of an internal hard disk. SAN booting can help to improve system availability, enable centralized administration, and eliminate the costs associated with maintaining and servicing hard drives.

Before you begin

- Your system must support SAN boot LUNs. Check the IBM N series interoperability matrix for the latest SAN booting requirements for your operating system version.
- For Windows 2003 configurations, store the `pagefile.sys` file on the local disk if you suspect pagefile latency issues. See the Microsoft article *Support for booting from a Storage Area Network (SAN)* for more information about pagefiles.
- For Fibre Channel HBAs, specific queue depths provide best results. It is best to tune the queue depths on the server-side HBA for Windows hosts to 254 for Emulex HBAs or 256 for QLogic HBAs.

  Note: To avoid host queuing, the host queue depths should not exceed the target queue depths on a per-target basis. For more information about target queue depths, see the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

About this task

Fibre Channel SAN booting does not require support for special SCSI operations; it is not different from any other SCSI disk operation. The HBA uses code in the BIOS that enables the host to boot from a LUN on the storage system.

iSCSI SAN booting also uses code in the BIOS that enables the host to boot from a LUN on the storage system. However, you need to set specific parameters in the BIOS to enable SAN booting.

Steps

1. Enable BootBIOS on the HBA.

   BootBIOS firmware is installed on your HBA, but it is disabled by default. For information about how to enable BootBIOS on the HBA, see your HBA vendor-specific documentation.

2. Add the HBA initiator to an igroup.

   You use this igroup to specify the host that can access the boot LUN. To add the initiator to the igroup, you can enter the WWPN for Fibre Channel HBAs or the iSCSI node name for iSCSI HBAs. For information about creating and managing igroups, see the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

3. Restrict the HBA to a single path to the boot LUN. You can add additional paths after Windows is installed and you have a multipathing solution in place.

To limit a single path to the boot LUN, you can use a Data ONTAP feature called port sets. You create a port set, add the port (or LIF) to the port set, and then bind the port set to an igroup. Port sets are supported for Fibre Channel (Data ONTAP operating in 7-Mode and Cluster-Mode) and for iSCSI (Cluster-Mode only). For more information about port sets, see the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

4. Create the LUN that you want to use as a boot device and map it to the igroup as LUN ID 0.

   For information about creating LUNs, see the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.

5. For iSCSI HBAs, configure the following boot BIOS settings:

   - Initiator IP
   - iSCSI node name
   - Adapter boot mode

   For more information about configuring the boot BIOS, refer to your HBA vendor-specific documentation.

6. Use your HBA vendor's BootBIOS utility to configure the LUN as a boot device.

   Refer to your HBA vendor-specific documentation for instructions.

7. Reboot the host and enter the host BIOS utility.

8. Configure the host BIOS to make the boot LUN the first disk device in the boot order.

   Refer to your host documentation for instructions.

9. Obtain the HBA device drivers for your version of Windows.

10. Install the Windows Server operating system and the HBA device driver on the boot LUN.

    Refer to your HBA vendor-specific documentation for instructions.

11. Install the Data ONTAP DSM for Windows MPIO.

Related information

Microsoft support site article: Support for booting from a Storage Area Network (SAN)
IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html
FC and iSCSI Configuration Guide - www.ibm.com/storage/support/nseries/
Emulex download page
QLogic driver download page

Troubleshooting

Use the information in the following topics to help you resolve typical problems with installation and operation of the Data ONTAP DSM for Windows MPIO.

Troubleshooting installation problems

Most installation problems are easily resolved. The following are typical problems when installing the Data ONTAP DSM for Windows MPIO.

Installing missing Windows hotfixes

The DSM installation program checks for required Windows hotfixes and displays an error listing any missing hotfixes. The installation will not continue until all required hotfixes are installed.

Steps

1. Record the list of missing Windows hotfixes reported by the DSM installer.

2. Obtain the Windows hotfixes from Microsoft and install them according to the instructions provided by Microsoft.

3. Run the DSM installation program again.

Related tasks

Resolving the SnapDrive 4.1 installation error

The DSM installation program checks for SnapDrive 4.1 for Windows or earlier and reports an error if found.

About this task

Your Windows system must run a version of SnapDrive for Windows that is supported with the DSM version.

Steps

1. Remove the old SnapDrive version.

2. Run the DSM installation program again.

Related tasks

Internal Error: Access is Denied during installation

On Windows Server 2008, you might receive an `Internal Error: Access is Denied` message if User Access Control is enabled and installation is attempted from a user account other than Administrator.

There are two workarounds for this problem: installing from an elevated command prompt or disabling User Access Control.

For more information about User Access Control, see the Microsoft Technet article *User Account Control Step-by-Step Guide*.

Related information

Microsoft Technet Library: User Account Control Step-by-Step Guide

Installing from an elevated command prompt

Run the installation from an elevated command prompt to avoid the `Internal Error: Access is Denied` error.

Before you begin

An elevated command prompt is required to install the DSM when User Access Control (UAC) is enabled. The elevated command prompt overrides the UAC restrictions.

Steps

1. Click **Start**.

2. Right-click **Command Prompt** and then click **Run as Administrator**.

3. Run the installation program by navigating to the directory containing the installation package and entering the package name at the command prompt.

Related information

Microsoft Technet Library: User Account Control Step-by-Step Guide

Disabling User Access Control

Disable User Access Control to avoid the `Internal Error: Access is Denied` error.

Steps

1. Log in as an administrator.

2. Select **Control Panel > User Accounts > Turn User Account Control on or off**.

3. Clear the **Use User Access Control (UAC) to help protect your computer** check box and then click **OK**.

4. Run the installation program again.

Related information

[Microsoft Technet Library: User Account Control Step-by-Step Guide](#)

Troubleshooting GUI and CLI problems

You can resolve typical graphical user interface (GUI) and command line interface (CLI) problems using the following topics.

Unable to disable path

The DSM graphical user interface (GUI) does not allow you to disable the active DSM ID (I_T_L nexus), except for paths using the Least Queue Depth policy.

You must first activate another DSM ID (path) and then disable the passive DSM ID.

In general, the GUI does not allow you to disrupt the host's access to a virtual disk.

Unable to change paths

If your DSM license expires, the DSM does not allow you to make any changes, such as changing paths.

A license that you purchase does not expire, but free demo licenses do expire. If your demo license expires, contact your sales representative to purchase a DSM license.

Changes not displayed in GUI

The DSM graphical user interface (GUI) does not automatically refresh for all events.

To manually refresh the display, first select Disks or Data ONTAP DSM Management in the navigation pane. Then select **Refresh** from the **Action** menu. If refresh does not work, try closing the GUI and opening it again.

Windows event log lists errors

The DSM writes events to the Windows event log. Check the system log for messages from Source "ontapdsm" or the application log for messages from source "Data ONTAP(R) DSM Management Service ".

Many events contain a DSM ID value. This value can be used to identify the virtual disk displayed in the GUI.

The DSM identifier is made up of four fields: port, bus, target, and LUN. For example, DSM ID 03000101 represents port 03, bus 00, target 01, and LUN 01. In the GUI, this value is displayed in the DSM ID column when you select a virtual disk.

Note that the VirtualDisk ID displayed in the GUI changes, depending on which underlying I_T_L nexus is active.

Related concepts

Mapping identifiers between the host and storage system on page 34

Troubleshooting failover problems

If a LUN is lost when an active/active storage system configuration fails over, check the storage system configuration.

Steps

1. Verify that the Windows host has a path to the LUN on each storage system node.

2. For FC, verify that the igroup for the LUN includes the world wide port name (WWPN) of each initiator (HBA on Windows host) that you want to access the LUN with.

3. For iSCSI, verify that each iSCSI port on one storage node has a partner port configured on the partner node.

4. Verify the storage system is running a supported version of Data ONTAP and a supported cfmode.

Troubleshooting ALUA configuration problems

ALUA is required for certain configurations. An event message is logged when a path is detected with ALUA disabled.

Steps

1. Using Windows Event Viewer, check the Windows logs for event 61212.

2. Record the disk serial number from the event.

3. Locate the serial number in the DSM Virtual Disks display to identify which LUN and storage controller it belongs to.

4. On the storage controller that owns the LUN, enable ALUA on the igroup mapped to the LUN.

After you finish

Reboot the Windows host to detect the ALUA configuration change.

Related concepts

ALUA support and requirements on page 17

Related tasks

Enabling ALUA for FC paths on page 52

Troubleshooting interoperability problems

Use the information in the following topics to help you resolve problems with your system's configuration.

Areas to check for possible problems

To avoid potential problems, confirm that the Data ONTAP DSM for Windows MPIO supports your combination of host operating system software, host hardware, Data ONTAP software, and storage system hardware.

- Check the IBM N series interoperability matrix.
- Verify that you have a correct iSCSI configuration. If iSCSI LUNs are not available after a reboot, verify that the target is listed as persistent on the Persistent Targets tab of the Microsoft iSCSI Initiator GUI.
  If applications using the LUNs display errors on startup, verify that the applications are configured to depend on the iSCSI service.
- For Fibre Channel paths to storage controllers running Data ONTAP 8.1 operating in Cluster-Mode, be sure the FC switches are zoned using the WWPNs of the target logical interfaces (LIFs), not the WWPNs of the physical ports on the node.
- Check for known problems. Review the *Release Notes* for Data ONTAP DSM for Windows MPIO. The *Release Notes* include a list of known problems and limitations.
- Review the troubleshooting information in the *Data ONTAP Block Access Management Guide for iSCSI and FC* for your version of Data ONTAP.
- Search the IBM N series support website for recently discovered problems.
- Collect information about your system. Record any error messages displayed on the host or storage system console. Collect the host and storage system log files. Record the symptoms of the problem and any changes made to the host or storage system just before the problem appeared.

- Contact technical support. If you are unable to resolve the problem, contact IBM N series support at 1-800-IBMSERV for assistance.

Related information

> IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html
> IBM N series support website - www.ibm.com/storage/support/nseries/

Installing fcinfo for Windows Server 2003 FC configurations

Installing the Microsoft Fibre Channel Information Tool (fcinfo) for Windows Server 2003 enables you to collect Fibre Channel HBA troubleshooting information in a standardized format.

About this task

It is recommended that you install fcinfo before you have a problem so that it is already available if needed. Customer support will tell you what commands to run if they need the information this tool collects.

Steps

1. Download the fcinfo package for your server's processor architecture from the Microsoft Download Center.

2. Run the installation program and follow the prompts.

Related information

> Microsoft Dowload Center: Fibre Channel Information Tool (fcinfo)

Updating the HBA software driver

Check the version of the HBA software driver and determine whether it needs to be upgraded.

Before you begin

Current driver requirements are in the IBM N series interoperability matrix.

About this task

To see if you have the latest driver, complete the following steps.

Steps

1. Right-click **My Computer** and select **Manage**.

   The Computer Management window is displayed.

2. Double-click **Device Manager**.

A list of installed devices displays. Previously installed drivers are listed under SCSI and RAID controller. One installed driver appears for each port on the HBA.

> **Note:** If you uninstalled a device driver, a FC controller (HBA) appears under Other devices.

3. Expand **SCSI and RAID controllers** and double-click the appropriate HBA.

   The **General** dialog box is displayed.

4. Click **Driver**.

   - If the driver version is correct, then you do not need to do anything else and can stop now.
   - If the version is not correct, proceed to the next step.

5. Obtain the latest supported version from the Emulex or QLogic Web site.

Related information

[IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html](www.ibm.com/systems/storage/network/interophome.html)
[Emulex support page for IBM]
[QLogic support page for IBM]

Enabling logging on the Emulex HBA

In some unusual circumstances, your technical support engineer might request that you enable error logging on the Emulex HBA miniport driver.

Steps

1. Open HBAnyware.

2. Select the appropriate HBA from the list and click the **Driver Parameters** tab.

3. Select the **LogErrors** parameter and change the value to the desired severity level.

4. Click **Apply**.

Enabling logging on the QLogic HBA

In some unusual circumstances, your technical support engineer might request that you enable error logging on the QLogic HBA miniport driver.

Steps

1. Open SANsurfer.

2. Open the **Settings** menu and select **Options**.

3. Ensure **Log Informational Events**, **Warning Events**, and **Enable Warning display** are selected.

4. Click **OK**.

FCoE troubleshooting overview

Fibre Channel over Ethernet (FCoE) troubleshooting is similar to traditional Fibre Channel (FC) troubleshooting, with a few specific changes for this new protocol.

FCoE encapsulates FC frames within Ethernet packets. Unlike iSCSI, FCoE does not use TCP/IP.

Troubleshooting FCoE problems should be divided into several distinct areas:

- Initiator to FCoE switch connection
- FCoE switch
- Switch to target connection

In the SAN context, the initiator is always in the host, and the target is always a component of the IBM N series storage system.

Troubleshooting the FCoE initiator to switch connection

To troubleshoot the FCoE initiator to FCoE switch connection, check the link lights, cabling, firmware versions, and switch port configuration.

Before you begin

You should have the manufacturer's documentation for your FCoE initiator (converged network adapter or CNA) and for your FCoE switch.

Steps

1. Verify that your CNA model is listed in the IBM N series interoperability matrix as supported for your configuration. Note the required FCoE firmware and host operating system versions.

2. Check the link lights on the card.

   See the manufacturer's documentation for the location and meaning of each light.

   a. If the lights indicate that there is no Ethernet link, check the cables and optical module and that the card is correctly installed.

      For copper cables, be sure to use copper cables supplied by the FCoE switch manufacturer. For optical cables, be sure to use an optical modules supplied by the CNA manufacturer in the CNA and an optical module supplied by the switch manufacturer in the switch. These items are *NOT* interchangeable between different switch and CNA brands. An FCoE component disables its port if it does not recognize the cable or optical module.

   b. Verify the CNA is cabled directly to a port on a supported FCoE switch.

   c. Verify the firmware version for the NIC function of the CNA.

      The NIC firmware version can be found in Windows **Device Manager** under **Network adapter** in the properties for the CNA. Note that a CNA has two firmware versions, one for

its FCoE function and one for its NIC function. Check the CNA manufacturer's support site to see if updated NIC firmware is available; if so, download and install it.

d. If the lights indicate that there is an Ethernet link but no FCoE connection, verify the firmware version of the CNA installed on the host computer.

The FCoE firmware version can be found in Windows **Device Manager** under **Storage controllers** in the properties for the CNA. Note that a CNA has two firmware versions, one for its FCoE function and one for its NIC function. If needed, download and install a supported FCoE firmware version.

Related information

IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Troubleshooting the FCoE switch

You should use the manufacturer's documentation for FCoE switch troubleshooting. However, a few high-level troubleshooting steps are listed here for your convenience.

Steps

1. Verify that the switch model and its firmware version are listed on the IBM N series interoperability matrix.

Note that an FCoE switch, with an integrated FC name server is required. A standard data center bridging (DCB) Ethernet switch is not sufficient.

2. Verify the switch zoning. Each initiator should be in a separate zone with one or more target ports.

3. If you are also using the CNA port as a NIC for other Ethernet traffic (iSCSI, NFS, CIFS), be sure the switch port is configured for trunking.

FCoE and other Ethernet traffic should be separated onto different VLANs.

Related information

IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html

Troubleshooting the FCoE switch to target connection

To troubleshoot the FCoE switch to target connection, check the link lights, Data ONTAP software version, and storage system configuration.

Steps

1. Check the Interoperability Matrix to verify that you have a supported version of Data ONTAP software and a supported FC or FCoE target adapter.

2. Verify that the Fibre Channel protocol is licensed on the storage system.

3. On the console of a storage controller operating in 7-Mode, run the following command:

   `fcp show adapter -v`

   On the console of a storage controller operating in Cluster-Mode, run the following command:

   `network fcp adapter show -instance`

   The target adapter should be listed and online.

4. On the console of a storage controller running in 7-Mode, run the following command:

   `fcp show initiator -v`

   On the console of a storage controller running in Cluster-Mode, running the following command:

   `vserver fcp initiator show`

   The FCoE initiator should be listed.

5. If the FCoE initiator is not listed, check the initiator group (igroup) on the storage controller and verify the initiator's world wide port name (WWPN) is configured correctly.

Related information

   [IBM N series interoperability matrix - www.ibm.com/systems/storage/network/interophome.html](http://www.ibm.com/systems/storage/network/interophome.html)

Troubleshooting FCoE failover problems

FCoE connections in a high availability configuration should fail over to paths during an outage. Verify CNA and host timeout settings if failover is not working correctly.

Steps

1. Verify you have a supported version of Data ONTAP DSM for Windows MPIO installed. If you installed the CNA after installing the DSM, run the DSM **Repair** option from Windows **Programs and Features**.

2. Verify you have supported multipathing software installed and that two or more paths are shown from the host to each LUN.

Installing the nSANity data collection program

Obtain and install the `nSANity Diagnostic and Configuration Data Collector` program when instructed to do so by your technical support representative.

Before you begin

The nSANity program replaces the diagnostic programs included in previous versions of the Host Utilities. The nSANity program runs on a Windows or Linux system with network connectivity to the component from which you want to collect data.

About this task

Contact your technical support representative to obtain the `nSANity Diagnostic and Configuration Data Collector` program.

Steps

1. Obtain the Windows zip or Linux tgz version of the nSANity program from your technical support representative and copy it to the workstation or server that you want to run it on.

2. Change to the directory to which you downloaded the zip or tgz file.

3. Extract all of the files and follow the instructions in the README.txt file. Also be sure to review the RELEASE_NOTES.txt file for any warnings and notices.

After you finish

Run the specific nSANity commands specified by your technical support representative.

Related information

   IBM N series support website - www.ibm.com/storage/support/nseries

Collecting diagnostic data using nSANity

Run the nSANity Diagnostic and Configuration Data Collector program when instructed by technical support to collect diagnostic data about your host, storage system, and Fibre Channel switches.

Before you begin

Obtain and install the latest version of nSANity on a Windows or Linux host. Be sure you have the user IDs and passwords of the components for which you need to collect data. In general, you need Administrator or root credentials to collect diagnostic data.

Steps

1. Open the Windows or Linux command prompt and change to the directory where you installed the nSANity program.

2. Enter the following command to display the nSANity command options:

   nsanity --help

3. Enter the commands specified by your technical support representative.

After you finish

Send the file or files generated by the nSANity program to your technical support representative.

Related tasks

Windows event log entries

The Data ONTAP DSM for Windows MPIO writes event log entries to the standard Windows event logs.

Because of the limitations on the data that can be written to the event log, the details of some events are written in a raw format.

Most event messages are in text format and do not require special interpretation.

Event messages that apply to a particular virtual disk (LUN) or I_T_L nexus (path) include the DSM identifier. This identifier is included on the DSM GUI page for each virtual disk, and is returned by the `get-sanpath` cmdlet.

Changing what gets logged by the DSM

You can change the number of messages that get written to the Windows event log by the Data ONTAP DSM.

About this task

Changing the event log level affects only messages written by the DSM itself. It does not affect messages written by the other Windows MPIO components.

You do not need to reboot the host after you change the log level.

Changing the event log level to a value higher than 1 might affect system performance.

Steps

1. In the DSM GUI navigation pane, select **Data ONTAP DSM Management**.

2. Click **Action > Set Data ONTAP DSM Parameters**.

3. Change the value for EventLogLevel to one of the following:

    0   No logging.

    1   Normal logging of events. 1 is the default level.

    2   Log additional events for path transitions and reservation changes.

    3   Log all events. Recommended only for debugging.

Related references

Event data section encoding

Some event log entries include raw data in their data sections. This enables these events to include more information than would be possible using text data.

The following table lists the data fields for raw event data and their offsets within the data.

Byte Offset (Hex)	Data
0x28 - 0x2B	DsmID
0x2C - 0x2F	PathID
0x30 – 0x33	NT Status Code
0x34 – 0x37	SrbFlags
0x38 – 0x39	Function
0x3A	SRB Status
0x3B	SCSI Status
0x3C	SenseKey
0x3D	ASC
0x3E	ASCQ
0x3F	Reserved
0x40-0x4F	CDB

Event message reference

The following messages can be written to the Windows system event log. The source of these messages is "ontapdsm". The severity (Sev) values are listed as **I** for informational, **W** for warning, or **E** for error.

The Level column lists the log level settings at which this message gets logged. The default level is 1.

ID	Sev	Level	Explanation
61002	I	1, 2, 3	The DSM successfully initialized. Issued once each time the driver starts.
61003	E	1, 2, 3	Reported when MPIO components cannot be located. Reinstall the DSM.
61004	W	1, 2, 3	The query did not return a serial number for a LUN. The DSM cannot manage the LUN.

ID	Sev	Level	Explanation
61005	E	1, 2, 3	The DSM could not obtain required information about the specified LUN, such as the storage system name and LUN path. The DSM cannot manage the LUN.
61006	I	1, 2, 3	The specified LUN uses an unsupported protocol. The DSM cannot manage the LUN.
61007	I	1, 2, 3	Issued once each time the DSM is unloaded.
61008	W	1, 2, 3	Invalid parameters passed to DSM Inquiry. The DSM will not claim the path.
61018	I	1, 2, 3	The specified DSM ID (I_T_L nexus) is now active.
61019	I	1, 2, 3	The administrative request to make specified DSM ID (I_T_L nexus) active failed.
61023	I	1, 2, 3	The default load balance policy for new virtual disks changed to the specified value.
61026	E	1, 2, 3	The storage system is running a version of Data ONTAP software that is not compatible with the DSM version.
61034	W	1, 2, 3	The specified LUN on the specified storage system disconnected. All paths to the LUN have been removed.
61035	I	2, 3	The DSM discovered the first path to a new LUN. The LUN, storage system, and DSM ID (I_T_L nexus) are listed. Because the storage system meets the requirements, all load balance policies are supported.
61039	E	1, 2, 3	Unable to determine the installed version of MPIO.
61040	E	1, 2, 3	An earlier revision of the Windows MPIO drivers than is required by the DSM was found on the Windows system. Reinstall the DSM.
61041	I	2, 3	The specified logical unit on the specified storage system connected using FC on the specified DSM ID (I_T_L nexus). The target WWPN is contained in the data section of this message at byte offset 0x28.

ID	Sev	Level	Explanation
61042	I	2, 3	The specified logical unit on the specified storage system connected using FC on the specified DSM ID (I_T_L nexus). The target IP address and the Nexus ID is contained in the data section of this message.
61045	I	1, 2, 3	This information is used for diagnosing problems with host bus adapters.
61048	I	2, 3	The specified DSM ID (I_T_L nexus) has been associated with the specified initiator-target nexus (path).
61049	W	1, 2, 3	There are no paths available to the specified LUN. The DSM requests path verification from the MPIO driver.
61051	W	3	The path with the specified DSM ID is in a degraded state. A SCSI command has failed.
61052	I	1, 2, 3	The specified DSM ID (I_T_L nexus) to the target is now working.
61053	E	1, 2, 3	The specified path failed. This was the last remaining path to a target. The DSM requests path verification from the MPIO driver. This event is reported during failover processing.
61054	W	1, 2, 3	The specified path failed. The DSM will use a different path.
61055	I	2, 3	The administrative request to enable the specified path for the specified LUN was successful.
61056	I	2, 3	The administrative request to disable the specified path for the specified LUN was successful.
61057	E	1, 2, 3	The administrative request to enable the specified path for the specified LUN failed.
61058	E	1, 2, 3	The administrative request to disable the specified path for the specified LUN failed.
61059	I	1, 2, 3	The DSM requested that the MPIO driver stop using this DSM ID (I_T_L nexus) and drain its queue. This is similar to disabling the DSM ID, but not persistent across host reboot.
61060	I	1, 2, 3	The MPIO driver did not allow throttling of I/O on the specified DSM ID (I_T_L nexus).

ID	Sev	Level	Explanation
61061	I	1, 2, 3	The throttling of I/O on the specified DSM ID (I_T_L nexus) was removed. I/O resumes on the DSM ID.
61062	I	1, 2, 3	Unable to remove the throttle on the specified DSM ID (I_T_L nexus).
61063	I	1, 2, 3	The specified protocol was enabled for the DSM.
61064	I	1, 2, 3	The specified protocol was disabled for the DSM.
61068	E	1, 2, 3	The attempt to change the load balance policy for the specified LUNs failed.
61070	I	2, 3	The path to a target has been removed for the specified path ID (I_T nexus). There are no other DSM IDs (I_T_L nexuses) to the target port of the nexus, so the nexus is removed.
61071	I	2, 3	The specified DSM ID (I_T_L nexus) has been activated and will be used for I/O.
61072	I	2, 3	The specified DSM ID (I_T_L nexus) is no longer active. It remains a passive I_T_L nexus that can be used if the active I_T_L nexus fails.
61073	I	1, 2, 3	The specified DSM ID (I_T_L nexus) failed to transition to the active state as requested by the administrator.
61074	I	1, 2, 3	The specified DSM ID (I_T_L nexus) failed to transition to the passive state. To make the active DSM ID passive, activate a passive DSM ID.
61075	W	1, 2, 3	The specified active DSM ID (I_T_L nexus) was replaced by the new active DSM ID.
61076	W	1, 2, 3	The specified path ID (I_T nexus) reported an I/O error. The I/O will be retried. This message contains raw data that must be decoded.
61077	W	1, 2, 3	The specified path ID (I_T nexus) failed. The DSM requests path verification from the MPIO driver. The DSM activates a new I_T_L nexus.
61078	I	1, 2, 3	The specified LUN has failed over to the new path ID (I_T nexus) specified.

ID	Sev	Level	Explanation
61079	W	1, 2, 3	The specified I_T nexus was reported as failed, but it recovered before failover processing could complete. The original nexus will continue to be used.
61080	W	1, 2, 3	The storage system reported a queue full error for the specified LUN and path ID (I_T nexus). The target port has reached its limit for outstanding requests. The I/O will be retried. This message contains raw data that must be decoded.
61081	W	1, 2, 3	The storage system reported a write error for I/O on the specified LUN and path ID (I_T nexus). The I/O will be retried. This message contains raw data that must be decoded.
61082	E	1, 2, 3	The storage system reported an invalid command for an I/O operation on the specified LUN and path ID (I_T nexus). The I/O is not retried. This message contains raw data that must be decoded.
61083	E	1, 2, 3	The storage system reported the logical block address for an I/O operation on the specified LUN and path ID (I_T nexus) is out of range. This message contains raw data that must be decoded. Contact technical support to report this error.
61084	E	1, 2, 3	The storage system reported an invalid field error for an I/O operation on the specified LUN and path ID (I_T nexus). The I/O is not retried. This message contains raw data that must be decoded.
61085	E	1, 2, 3	The storage system reported that the requested LUN does not exist. The LUN may have been deleted on the storage system by the administrator. This error can also occur during storage system giveback. Check the event data section for additional information.
61086	E	1, 2, 3	The storage system reported an invalid parameter list error for an I/O operation on the specified LUN and path ID (I_T nexus). The I/O is not retried. This message contains raw data that must be decoded.

ID	Sev	Level	Explanation
61087	E	1, 2, 3	The DSM attempted to release a persistent reservation on the specified LUN and path ID (I_T nexus) for a LUN that it does not own. The I/O is not retried.
61088	E	1, 2, 3	The storage system reported an invalid parameter list length error for an I/O operation on the specified LUN and path ID (I_T nexus). The I/O is not retried. This message contains raw data that must be decoded.
61089	E	1, 2, 3	The storage system reported an invalid task attribute error for an I/O operation on the specified LUN and path ID (I_T nexus). This message contains raw data that must be decoded.
61090	W	1, 2, 3	The storage system reported a configuration problem with the LUN on the specified path ID (I_T nexus). The I/O is not retried. This message contains raw data that must be decoded.
61091	W	1, 2, 3	The LUN on the specified path ID (I_T nexus) could not be reached because of problems with the storage system interconnect. The I/O is retried on another path ID. This message contains raw data that must be decoded.
61092	E	1, 2, 3	The storage system reported that the LUN on the specified path ID (I_T nexus) was not ready. The I/O will be retried. Check the event data section for additional information.
61093	W	1, 2, 3	The LUN on the specified path ID (I_T nexus) is not currently available because it is being formatted. The I/O will be retried. This message contains raw data that must be decoded.
61094	E	1, 2, 3	The storage system reported that the LUN on the specified path ID (I_T nexus) is not available. The I/O will be retried on another path. Check the event data section for additional information.
61095	W	1, 2, 3	The LUN on the specified path ID (I_T nexus) is not ready, but is becoming ready. The I/O will be retried. This message contains raw data that must be decoded.

ID	Sev	Level	Explanation
61096	W	1, 2, 3	The storage system reported that the LUN on the specified path ID (I_T nexus) is offline. The I/O will be retried. This message contains raw data that must be decoded. Check the LUN status on the storage system and bring online.
61097	I	3	The storage system reported that the LUN on the specified path ID (I_T nexus) was reset. The I/O will be retried immediately. This message contains raw data that must be decoded.
61098	I	2, 3	The DSM lost its SCSI reservation to the LUN on the specified path ID (I_T nexus). This message contains raw data that must be decoded.
61099	I	2, 3	The storage system reported that the SCSI reservations to the LUN on the specified path ID (I_T nexus) were released. This message contains raw data that must be decoded.
61100	I	2, 3	The storage system reported that the registration of the specified path ID (I_T nexus) was cleared. The I/O request will be retried. This message contains raw data that must be decoded.
61101	I	2,3	The storage system reported the asymmetric access to the LUN in the specified path ID (I_T nexus) changed. The I/O request will be retried. This message contains raw data that must be decoded.
61102	I	2, 3	The storage system reported that a volume was created on the LUN in the specified path ID (I_T nexus). The I/O request will not be retried. This message contains raw data that must be decoded.
61103	I	2, 3	The storage system reported a change in the availability of the LUN in the specified path ID (I_T nexus). The I/O request will not be retried. This message contains raw data that must be decoded.
61104	E	1, 2, 3	The storage system reported an attempt to write to the read-only LUN in the specified path ID (I_T nexus). The I/O request will be retried. This message contains raw data that must be decoded.

ID	Sev	Level	Explanation
61105	E	1, 2, 3	The storage system reported a write error on the LUN in the specified path ID (I_T nexus). The I/O will be retried. This message contains raw data that must be decoded. Check the storage system log for disk errors.
61106	E	1, 2, 3	The storage system reported a write error on the LUN in the specified path ID (I_T nexus) and was unable to reallocate the bad blocks. The I/O will be retried. This message contains raw data that must be decoded. Check the storage system log for disk errors.
61107	E	1, 2, 3	The storage system reported that one of the disks used for the LUN in the specified path ID (I_T nexus) was not supported. The I/O is not retried. This message contains raw data that must be decoded. Check the storage system log for disk errors.
61108	E	1, 2, 3	The storage system reported a high error rate for the LUN in the specified path ID (I_T nexus). The I/O will be retried. This message contains raw data that must be decoded. Check the storage system log for disk errors.
61109	W	1, 2, 3	The storage system aborted a SCSI command on the specified LUN and path ID (I_T nexus). The I/O will be retried. This message contains raw data that must be decoded. This is a common event during storage system giveback.
61110	E	1, 2, 3	The DSM was unable to communicate with the LUN on the specified path ID (I_T nexus). The DSM will try another path to the LUN. The data section of the event contains the NTSTATUS code.
61111	I	1, 2, 3	The DSM detected a buffer error for the LUN on the specified path ID (I_T nexus). The I/O is not retried. The data section of the event contains the NTSTATUS code.
61112	W	1, 2, 3	The DSM detected that the specified LUN and path ID (I_T nexus) is pending deletion while processing an I/O operation. The DSM will try another path to the LUN.

ID	Sev	Level	Explanation
61113	W	3	The DSM detected an invalid device request on the specified LUN and path ID (I_T nexus). The I/O is not retried. Check the event data section for additional information.
61114	I	3	The DSM found the queue for the specified LUN and path ID (I_T nexus) frozen. The queue is now unfrozen and the I/O will be retried.
61115	E	3	The DSM found the queue for the specified LUN and path ID (I_T nexus) frozen. The DSM is unable to unfreeze the queue. The I/O will be retried.
61116	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) did not finish processing an I/O request. The I/O request will not be retried.
61117	I	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) cancelled an I/O operation successfully. The I/O request will be retried.
61118	W	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) was unable to cancel an I/O operation because the I/O operation could not be located. The I/O request will be retried.
61119	W	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that it was too busy to accept an I/O request. The I/O request will be retried.
61120	W	2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that an I/O operation request was not supported. The I/O request will not be retried.
61121	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the bus is no longer valid. The I/O request will be retried on an alternate path.
61122	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the LUN is no longer present. The I/O request will be retried on an alternate path.

ID	Sev	Level	Explanation
61123	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that an I/O operation timed out. This event is usually triggered when the target is extremely busy and does not respond within the timeout period allowed. The DSM retries these operations automatically. If LUN statistics from AutoSupport or Perfstat show the LUN is not very busy at the time of the event, the event might be caused by a degraded SFP or other hardware component in the path.
61124	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the LUN did not respond to selection. The I/O request will be retried on an alternate path.
61125	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that an I/O command timed out. The I/O request will be retried.
61126	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the storage system rejected a message. The I/O request will not be retried. This response is normally returned only for SRB_FUNCTION_TERMINATE_IO requests.
61127	W	2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported a bus reset while processing an I/O request. The request will be retried.
61128	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported a parity error. The request will be retried.
61129	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) failed a request-sense command. The request will be retried.
61130	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) did not respond to an I/O request. The I/O request will be retried on an alternate path.
61131	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) disconnected unexpectedly. The I/O request will be retried on an alternate path.

ID	Sev	Level	Explanation
61132	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported an illegal phase sequence failure. The I/O request will be retried on an alternate path.
61133	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported an improper SRB request. The I/O request will not be retried.
61134	I	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that a request for status was stopped. The I/O request will not be retried.
61135	W	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the LUN is invalid. The I/O request will be retried on an alternate path.
61136	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the storage system is no longer available. The I/O request will not be retried.
61137	W	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported a bad function request in an I/O request. The I/O request will not be retried.
61138	W	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that an I/O request completed with an error and that the SCSI INITIATE RECOVERY message was received. The I/O request will be retried.
61139	E	1, 2, 3	The port servicing the specified LUN and path ID (I_T nexus) reported that the storage system is not powered. The I/O request will not be retried.
61140	W	1, 2, 3	The storage system reported that the LUN on the specified path ID (I_T nexus) is busy. The request will be retried.
61141	W	1, 2, 3	The storage system reported that the queue for the LUN on the specified path ID (I_T nexus) is full. The request will be retried.
61142	E	1, 2, 3	The specified nexus (path) failed.
61143	I	1, 2, 3	The specified nexus (path) is working normally.

ID	Sev	Level	Explanation
61144	W	1, 2, 3	The specified DSM ID (I_T_L nexus) was used for an I/O operation, because there we no paths without I/O errors.
61145	W	1, 2, 3	The specified nexus (path) is degraded. One or more DSM IDs (I_T_L nexuses) have lost connectivity with the storage system.
61146	I	2, 3	The specified DSM ID (I_T_L nexus) is reserved by host clustering software.
61147	I	2, 3	The reservation for the specified DSM ID (I_T_L nexus) was released.
61148	W	2, 3	The DSM has chosen the specified DSM ID (I_T_L nexus) even though it is on a degraded I_T nexus. All other I_T nexuses are degraded or processing I/O failures.
61149	W	1, 2, 3	The DSM has chosen the specified DSM ID (I_T_L nexus) even though it is disabled. The DSM will switch from the disabled path as soon as an enabled DSM ID is available.
61150	W	1, 2, 3	The DSM has determined that no alternate paths exist for the specified LUN on the specified storage system. The LUN is in a severely degraded state and I/O may fail. This event indicates that a LUN has lost all of its paths and if this state remains, then I/O may fail. If this event occurs, use the DSM GUI or CLI to verify that all paths are in a normal state and operational. You can safely ignore this message if it occurs at reboot time and all paths are normal after the reboot completes.
61151	W	1, 2, 3	The DSM is moving the reservation for the specified LUN to the specified path.
61152	I	1, 2, 3	The specified DSM ID (I_T_L nexus) is recovering from an I/O error. This event is reported during the first phase of error recovery, when path verification is requested after a failover.

ID	Sev	Level	Explanation
61153	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has completed error recovery from an I/O error. This event is reported as part of the second phase of error recovery after an I/O error. This event indicates that the I_T_L nexus is now operational.
61154	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has reestablished communication for its I_T nexus (path). The specified path is now normal. An I_T_L on a nexus which previously had experienced a path verification failure has detected that the nexus is now working. All of the I_T_Ls on this nexus are now available for path selection.
61155	W	1, 2, 3	The specified DSM ID (I_T_L nexus) failed to release a LUN.
61156	W	1, 2, 3	The specified DSM ID (I_T_L nexus) failed to reserve a LUN.
61157	W	1, 2, 3	The DSM is using the specified DSM ID (I_T_L nexus) to force the release of any reservations on the specified LUN.
61158	E	1, 2, 3	The reservation for the specified LUN was lost.
61201	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the active state.
61202	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the passive state.
61203	E	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the failed state.
61204	W	1, 2, 3	The specified DSM ID (I_T_L nexus) is in the process of being removed.
61205	W	1, 2, 3	The specified DSM ID (I_T_L nexus) was removed.
61206	W	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the disabled state.
61207	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the pending active state.
61208	I	1, 2, 3	The specified DSM ID (I_T_L nexus) has transitioned to the pending passive state.

ID	Sev	Level	Explanation
61209	W	1, 2, 3	The specified virtual disk does not support the active/ active load balance policies (Round Robin, Round Robin with Subset, or Least Queue Depth). The reported version of Data ONTAP software is earlier than 7.3.3 or the reported cfmode setting is not single_image or standby.
61212	E	1, 2, 3	The DSM ID for the virtual disk with the specified serial number does not have ALUA enabled. This event is logged whenever the specified path changes state or the LUN is first discovered. ALUA is required for FC paths to LUNs for Data ONTAP operating in 7-Mode or Cluster-Mode and for iSCSI paths to LUNs for Data ONTAP operating in Cluster-Mode. Enable ALUA and reboot the Windows host.
61213	I	2, 3	There was an I/O error. The ALUA state changed for the specified path to the specified LUN. The I/O will be retried.
61214	W	2, 3	The ALUA state transition failed on the specified LUN. The I/O will be retried.
61215	I	2, 3	The ALUA state was updated for the specified path to the specified LUN.
61217	E	1, 2, 3	Inquiry for ALUA failed for the DSM ID (I_T_L nexus) on the specified LUN.

Related tasks

Changing what gets logged by the DSM on page 138

Related references

Event data section encoding on page 139

Copyright and trademark information

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service

Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

Index

IBM.

NA 210-05585_A0, Printed in USA