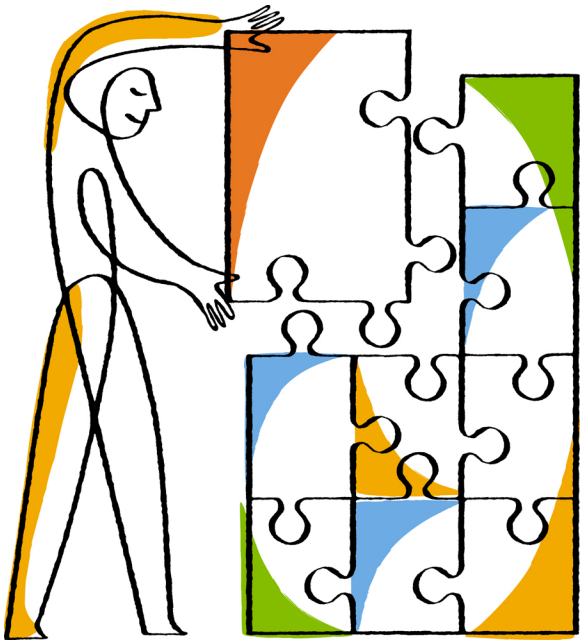
Data ONTAP® DSM 4.1 For Windows® MPIO

Installation and Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08396_A0
January 2014

Contents

DSM concepts 8
Device-specific module overview 8
Tasks required for installing and configuring the DSM 9
Windows configurations supported by the DSM 10
ALUA support and requirements 10
Mixing FC and iSCSI paths 12
Microsoft iSCSI DSM 12
I_T and I_T_L nexus overview 12
Multiple paths require MPIO software 13
Load balance policies determine failover behavior 13
Path limits 14
Windows Administrator account option 14
Timeout and tuning parameters overview 15
FC HBA and CNA parameters set by Data ONTAP DSM for Windows MPIO 15
Registry values set by Data ONTAP DSM for Windows MPIO 16
When to change the load balance policy 22
Path types and Windows clusters affect failover behavior 22
DSM prefers optimized paths 22
DSM can use disabled paths 23
Failover examples 23
Least queue depth example 23
Round robin example 24
Round robin with subset example 24
Failover-only example 25
Auto-assigned example 25
Mapping identifiers between the host and storage system 27
Dynamic disk support 27
What the Hyper-V Guest Utilities are 28
What Hyper-V is 28
Methods for using storage with Hyper-V 28
Methods for clustering Windows hosts with Hyper-V 29

Recommended LUN layout with Hyper-V 29
About SAN booting 29
Support for non-English operating system versions 30
Installing the DSM 31
Verifying your host configuration 31
Stopping host I/O and the cluster service 32
Installing Windows hotfixes 33
List of required hotfixes for Windows Server 33
Removing or upgrading SnapDrive for Windows 35
Confirming your storage system configuration 36
Configuring FC HBAs and switches 36
Checking the media type of FC ports 37
Configuring iSCSI initiators 38
iSCSI software initiator options 38
Downloading the iSCSI software initiator 39
Installing the iSCSI initiator software 40
Options for iSCSI sessions and error recovery levels 40
Options for using CHAP with iSCSI initiators 40
Using RADIUS for iSCSI authentication 41
Enabling ALUA for FC paths 42
Obtaining a DSM license key 42
Installing PowerShell 2.0 43
Installing .NET framework on Windows Server 2003 or 2008 43
DSM installation options 44
Running the DSM installation program interactively 44
Running the DSM installation program from a command line 46
Configuring Hyper-V systems 48
Adding virtual machines to a failover cluster 48
Configuring SUSE Linux and RHEL 5.5 and 5.6 guests for Hyper-V 49
Configuring RHEL 6.0 and 6.1 guests for Hyper-V 50
Hyper-V VHD requires alignment for best performance 51
Upgrading the DSM 54
Verifying your host configuration 54
Stopping host I/O and the cluster service 55
Installing Windows hotfixes 56
List of required hotfixes for Windows Server 56

Removing FC or iSCSI paths to 7-Mode LUNs 58
Enabling ALUA for FC paths 59
Installing PowerShell 2.0 59
Running the DSM upgrade program 59
Upgrading Windows cluster configurations 60
Running the DSM upgrade interactively 60
Running the DSM upgrade from a command line 62
Removing or repairing the DSM 65
Uninstalling the Data ONTAP DSM interactively 65
Uninstalling the DSM silently (unattended) 66
Repairing the Data ONTAP DSM installation 67
Managing the DSM using the GUI 68
Starting the DSM GUI 68
Discovering new disks 68
Viewing summary information for virtual disks 69
Viewing events report information for virtual disks 70
Displaying the events report 71
Changing the number of entries in the detailed events report 71
Viewing detailed information for virtual disks 72
Viewing path information for virtual disks 72
Viewing LUN information for virtual disks 73
Viewing I/O statistics for virtual disks 74
Viewing history information for virtual disk 75
Changing the load balance policy 77
Changing the default load balance policy 78
Changing the operational state of a path 79
Changing the administrative state of a path 79
Changing the path weight 80
Changing the preferred path 80
Displaying the persistent reservation key for a virtual disk 81
Setting persistent reservation parameters 81
Changing what gets logged by the DSM 82
Setting MPIO tunable parameters 83
Setting the DSM GUI auto refresh rate 84
Refreshing the display manually 84
Viewing the DSM license key 85

Managing the DSM using Windows PowerShell cmdlets 86
What you can do with the PowerShell cmdlets 86
Requirements for the PowerShell cmdlets 87
Running PowerShell cmdlets on the local host 88
Running PowerShell cmdlets from a remote host 88
Getting help with PowerShell cmdlets 89
Displaying DSM settings 89
Getting information about virtual disks 90
Changing the load balance policy using a cmdlet 91
Changing the default load balance policy using a cmdlet 92
Viewing path information using a cmdlet 93
Changing path status using a cmdlet 94
Supported path changes for load balance policies 95
Changing the path weight using a cmdlet 95
Displaying statistics about SAN connectivity 96
Clearing SAN connectivity statistics 97
Prioritizing FC paths over iSCSI paths 97
Modifying values for DSM parameters 98
Configuring for Fibre Channel and iSCSI 100
What FC and iSCSI identifiers are 100
Recording the WWPN 100
Recording the iSCSI initiator node name 102
Setting up LUNs 103
LUN overview 103
Initiator group overview 104
About FC targets 105
Adding iSCSI targets 106
Overview of initializing and partitioning the disk 108
Setting up a SAN boot LUN for Windows Server 109
Troubleshooting 111
Troubleshooting installation problems 111
Installing missing Windows hotfixes 111
Internal Error: Access is Denied during installation 111
Installing Windows Host Utilities after installing the DSM resets the persistent reservation timeout value incorrectly 113
Troubleshooting failover problems 113

Troubleshooting ALUA configuration problems 113
Troubleshooting interoperability problems 114
Areas to check for possible problems 114
Installing fcinfo for Windows Server 2003 FC configurations 115
Updating the HBA software driver 115
Enabling logging on the Emulex HBA 116
Enabling logging on the QLogic HBA 116
FCoE troubleshooting overview 117
Installing the nSANity data collection program 119
Collecting diagnostic data using nSANity 120
Windows event log entries 121
How DSM event log entries relate to MPIO driver event log entries 121
Changing what gets logged by the DSM 122
Event data section encoding 122
Event message reference 123
Copyright information 137
Trademark information 138
How to send your comments 139
Index 140

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 a NetApp 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

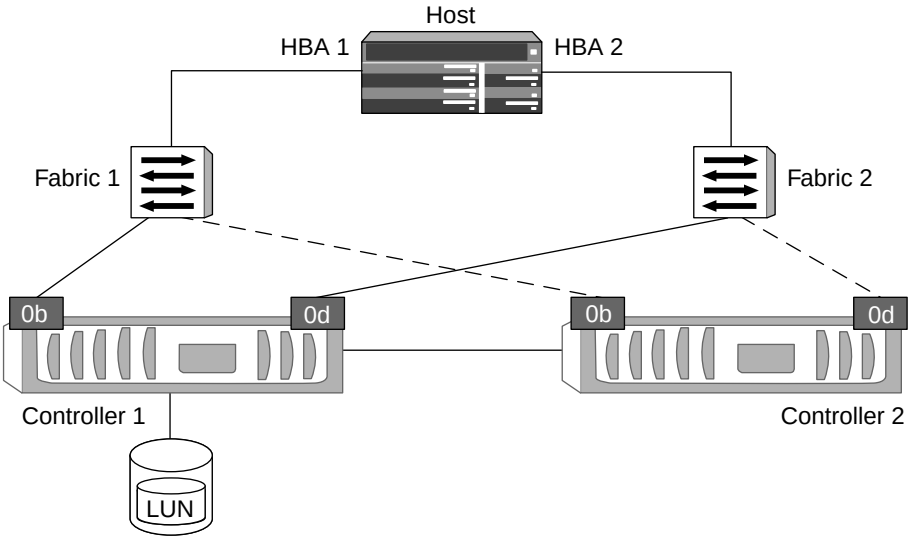
The Data ONTAP DSM for Windows MPIO is a device-specific module (DSM) that works with Microsoft Windows MPIO drivers to manage multiple paths between NetApp and Windows host computers.

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 and later, 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 NetApp storage systems. These LUNs have the vendor identifier and product identifier (VID/PID) pair "NETAPP LUN" for Data ONTAP operating in 7-Mode or "NETAPP LUN C-Mode" for clustered Data ONTAP.

You can use Microsoft-branded DSMs 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 named `msiscdsm` that you can use to manage iSCSI paths.
- Windows Server 2008 and later includes a DSM named `msdsm` that you can use to manage FC and iSCSI paths.

The native DSMs claim only devices that are not claimed by other DSMs. They can coexist with the Data ONTAP DSM, provided that the versions of each product in use on the host are compatible.

A third-party DSM that complies with the Microsoft MPIO framework can coexist with the Data ONTAP DSM, provided that the product is configured not to claim NetApp LUNs, and does not require hotfixes that may interfere with Data ONTAP DSM operations.

The Data ONTAP DSM cannot coexist with legacy MPIO solutions that do not comply with the Microsoft MPIO framework.

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.

   Note: If you install Windows Host Utilities 6.0 or later after installing DSM 4.0 or later, you must repair the DSM using the Windows repair option.

2. Record the FC and iSCSI initiator identifiers.
3. Create LUNs and make them available as virtual disks on the host computer.

Optionally, depending on your configuration, you can configure SAN booting of the host.

Related concepts

Setting up LUNs on page 103
What FC and iSCSI identifiers are on page 100

Related tasks

Setting up a SAN boot LUN for Windows Server on page 109
Installing the DSM on page 31

Windows configurations supported by the DSM

The DSM supports a number of different 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, Windows Server 2012, Windows Server 2012 R2) or Virtual Server 2005 (Windows Server 2003), both parent and guest
- SAN booting

Use the Interoperability Matrix to find a supported combination of host and storage system components and software and firmware versions.

Related information

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 version	ALUA supported and required?
Windows Server 2003	iSCSI	7-Mode	No
		Clustered Data ONTAP	Yes
	Fibre Channel	7-Mode	Yes
		Clustered Data ONTAP	Yes

Windows version	Protocol	Data ONTAP version	ALUA supported and required?
Windows Server 2008	iSCSI	7-Mode	No
		Clustered Data ONTAP	Yes
	Fibre Channel	7-Mode	Yes
		Clustered Data ONTAP	Yes
Windows Server 2012	iSCSI	7-Mode	No
		Clustered Data ONTAP	Yes
	Fibre Channel	7-Mode	Yes
		Clustered Data ONTAP	Yes
Windows Server 2012 R2	iSCSI	7-Mode	Yes
	Fibre Channel	Clustered Data ONTAP	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 clustered Data ONTAP 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 concepts

Mixing FC and iSCSI paths on page 12

Related tasks

Enabling ALUA for FC paths on page 42
Troubleshooting ALUA configuration problems on page 113

Mixing FC and iSCSI paths

The Data ONTAP DSM supports both FC and iSCSI paths to the same LUN for clustered Data ONTAP. 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

Load balance policies determine failover behavior on page 13
ALUA support and requirements on page 10

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 iSCSI initiator can manage LUNs from other vendors' storage systems.

When both DSMs are installed, the Data ONTAP DSM has priority in claiming iSCSI LUNs on NetApp and 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 system’s target. An initiator-target-LUN (I_T_L) nexus represents the DSM's view of the LUN on a particular I_T nexus. 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 is for internal use.

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.

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 active/optimized path with the smallest current outstanding queue. The policy selects paths on a per I/O basis. It checks the queues serially, rather than all at once. It is not uncommon if some paths are not used for I/O because the policy always selects the active/optimized path with the smallest queue. The queue length is determined at the I_T_L nexus level. Active/non-optimized paths are not used for I/O if an optimized path is available. This policy enables you to maximize bandwidth utilization without the need for administrator intervention. Least Queue Depth is the default policy.

> **Note:** If the mapped LUN is 2TB or greater and you are using the Least Queue Depth policy on any Windows Server operating system, I/O is serviced on only one path instead of across all available Active/Optimized paths. You should use the Round Robin with Subset policy for LUNs that are 2TB or greater

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 255. 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.

Related concepts

Mixing FC and iSCSI paths on page 12

Path limits

In clustered Data ONTAP, you can have a maximum of 32 paths to a LUN. In Data ONTAP operating in 7-Mode, you can have a maximum of 8 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 the maximum paths leads to unpredictable behavior of the Windows MPIO layer and possible data loss.

Windows Administrator account option

When installing DSM, you can opt to 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.

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 might vary slightly depending on the program. For example, in QLogic QConvergeConsole, one 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 a 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 a 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 a 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\SYSTEM\CurrentControlSet\Services\ontapdsm\Parameters**InquiryRetryCount**	6	Always
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm\Parameters**InquiryTimeout**	2	Always
HKLM\SOFTWARE\NetApp\MPIO**InstallDir**	`C:\Program Files\NetApp\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**	15	Always
HKLM\SOFTWARE\NetApp\MPIO**LogDir**	`C:\temp\netapp\`	Always
HKLM\SYSTEM\CurrentControlSet\Services\ClusDisk\Parameters**ManageDisksOnSystemBuses**	1	Always
HKLM\SYSTEM\CurrentControlSet\Control\Class\{*iSCSI_driver_GUID*}*instance_ID*\Parameters**MaxRequestHoldTime**	60	Always

Registry key	**Value**	**When set**
HKLM\SYSTEM\CurrentControlSet\Control\MPDEV**MPIOSupportedDeviceList**	"NETAPP LUN", "NETAPP LUN C-Mode"	Always
HKLM\SYSTEM\CurrentControlSet\Services\mpio\Parameters**PathRecoveryInterval**	40	Windows Server 2008, 2008 R2, 2012, or 2012 R2 only
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm\Parameters**PathVerifyEnabled**	0	Always
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\NetApp\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**	2	Always
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

Registry key	Value	When set
HKLM\SYSTEM\CurrentControlSet\Services\ontapdsm \Parameters**TestUnitReadyRetryCount**	20	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, 2008 R2, 2012, or 2012 R2 only

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. This parameter is configurable.

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.

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

LinkDownTime setting

For iSCSI only, 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 article 886569 - http://support.microsoft.com/kb/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 node 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.

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 optimized and non-optimized paths.

Non-optimized paths use the cluster interconnect between storage system controllers in an 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 of least queue depth failover 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 HA 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. When no Active/Optimized paths are available, the Active/Non-optimized paths are become Active/Optimized.

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.

Mapping identifiers between the host and storage system

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

Disk serial number

The upper pane of 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 System Manager 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 consisting of four two-character 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 consisting of four two-character fields. The first three fields are the same as the DSM ID: port, bus, and target. The fourth field is for NetApp internal use. The path identifier references an I_T nexus. The DSM ID references an I_T_L nexus. The path identifier can be repeated across LUNs and disks, but the combinations of DSMID/PathID are unique.

The Path ID is displayed on the DSM GUI details pane 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.

Use LinuxGuestConfig.iso in the Hyper-V Guest Utilities to set disk timeouts for Hyper-V virtual machines that run Linux. Setting timeout parameters on a Linux guest ensures correct failover behavior.

Related concepts

Configuring Hyper-V systems on page 48

What Hyper-V is

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

Hyper-V is a “role” available in the following versions of Microsoft Windows Server.

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 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, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, use an iSCSI initiator and multipathing solution that is supported by NetApp 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 host for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.

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 fewer 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 approximately 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 and Windows Server 2012 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 two 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 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.

Related tasks

Setting up a SAN boot LUN for Windows Server on page 109
Downloading the iSCSI software initiator on page 39

Related information

Technical Report 3644 - http://media.netapp.com/documents/tr-3644.pdf

Support for non-English operating system versions

Data ONTAP DSM for Windows MPIO is supported on all Language Editions of Windows Server. 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

1. *Verifying your host configuration* on page 31
2. *Stopping host I/O and the cluster service* on page 32
3. *Installing Windows hotfixes* on page 33
4. *Removing or upgrading SnapDrive for Windows* on page 35
5. *Confirming your storage system configuration* on page 36
6. *Configuring FC HBAs and switches* on page 36
7. *Checking the media type of FC ports* on page 37
8. *Configuring iSCSI initiators* on page 38
9. *Enabling ALUA for FC paths* on page 42
10. *Obtaining a DSM license key* on page 42
11. *Installing PowerShell 2.0* on page 43
12. *Installing .NET framework on Windows Server 2003 or 2008* on page 43
13. *DSM installation options* on page 44
14. *Configuring Hyper-V systems* on page 48

Related concepts

Tasks required for installing and configuring the DSM on page 9

Windows Administrator account option on page 14

Verifying your host configuration

Verify your configuration before you install or upgrade the DSM.

Steps

1. Use the 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

After you search for your configuration and click a configuration name, details for that configuration display in the Configuration Details dialog box. In this dialog box, be sure to review the information in the following tabs:

Notes	Lists important alerts and notes that are specific to your configuration. Review the alerts to identify the hotfixes that are required for your operating system.
Policies and Guidelines	Provides general guidelines for all SAN configurations. For example, you can view support information about Hyper-V in the Virtualization section and you can view support information about third-party HBAs and CNAs in the section titled Third-party Host Bus Adapter (HBA) and Converged Network Adapter (CNA) Model Support.

2. **For ESX Virtualized Windows Server:** You should use the Interoperability Matrix to verify your ESX Virtualized Windows Server guests if the following applies to your configuration:
   - Your parent server is running a version of ESX that is listed as a supported version on the Interoperability Matrix.
   - You are using the Microsoft iSCSI software initiator to connect directly to a SAN configuration from the Windows Server guest.

Related information

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

Stopping host I/O and the cluster service

The installation of hotfixes and the Data ONTAP DSM requires rebooting the Windows host. Before rebooting, you must first 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.

   See bug 373412 at Bugs Online for the latest information about this issue.

Related information

Bugs Online - support.netapp.com/NOW/cgi-bin/bol/

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 required 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. If you are prompted to install a hotfix that is already installed, try enabling the affected Windows feature and then restarting 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 personnel. They are not available for direct download.

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

Related information

Microsoft support site - http://support.microsoft.com
NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 required hotfix for Data ONTAP DSM. The specified file version is the minimum requirement.

The 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 2012

The following hotfix is not required for Windows Server 2012, but is recommended.

Hotfix	When recommended	File name
2796995	Always	Csvfs.sys

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
945119	Always	Storport.sys
982109	Always	Mpio.sys

Windows Server 2008 SP2

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

Hotfix	When required	File name
968675	Always	Storport.sys
2754704	Always	Mpio.sys
2684681	Always	Msiscsi.sys

Windows Server 2008 R2

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

Hotfix	When required	File name
2528357	Always	Storport.sys
979711	Always	Msiscsi.sys
2684681	Always	Iscsilog.dll
2754704	Always	Mpio.sys

The following hotfix is not required for Windows Server 2008 R2, but is recommended.

Hotfix	When recommended	File name
2520235	Always	Clusres.dll

Windows Server 2008 R2 SP1

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

Hotfix	When required	Filename
2528357	Always	Storport.sys
2754704	Always	Mpio.sys
2684681	Always	Iscsilog.dll

Windows Server 2008

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

Hotfix	When required	Filename
2754704	Always	Mpio.sys
2684681	Always	Iscsilog.dll

Related information

Microsoft support site - http://support.microsoft.com
NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 Interoperability Matrix.

Steps

1. To upgrade SnapDrive for Windows, follow the instructions in the *SnapDrive for Windows nstallation 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

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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.

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 NetApp or sales partner representative.
2. Verify your cabling. See the *SAN Configuration Guide* (formerly the *Fibre Channel and iSCSI Configuration Guide*) for your version of Data ONTAP for detailed cabling and configuration information.

Related information

Documentation on the NetApp Support Site: support.netapp.com

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 NetApp.
QLogic HBAs	QLogic support page for NetApp.

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 clustered Data ONTAP, 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

Emulex support page for NetApp - www.emulex.com/downloads/netapp.html

QLogic support page for NetApp - http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/OEM_Product_List.aspx?oemid=372

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 clustered Data ONTAP.

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

See the Interoperability Matrix for initiators supported with iSCSI configurations.

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.

Note: You configure iSCSI paths differently for clustered Data ONTAP. 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.

Related information

Interoperability Matrix: support.netapp.com/matrix

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 box is available from Administrative Tools.
Windows Server 2008 R2	The iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog box is available from Administrative Tools.
Windows Server 2012	The iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog box is available from **Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator**.
Windows Server 2012 R2	The iSCSI initiator is built into the operating system. The iSCSI Initiator Properties dialog box is available from **Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator**.
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 NetApp 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 box is available from Administrative Tools. Note that a Windows Vista iSCSI connection to NetApp storage is supported only on Hyper-V virtual machines.
Linux 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 stand-alone 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 stand-alone hardware. A supported version of Linux Host Utilities is required.

Related tasks

Configuring SUSE Linux and RHEL 5.5 and 5.6 guests for Hyper-V on page 49

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 website at *http://www.microsoft.com/*.
2. Click **Downloads**.
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

About SAN booting on page 29

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 its 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.

Options for iSCSI sessions and error recovery levels

By default, Data ONTAP enables four TCP/IP connections per iSCSI session, and an error recovery level of 0.

You can optionally enable more than four connections per session and error recovery level 1 or 2 by setting Data ONTAP option values. For more information, see the chapter about managing the iSCSI network in the *SAN Administration Guide* (formerly the *Block Access Management Guide for iSCSI and FC*) for your version of Data ONTAP.

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.
- For Windows Server 2012 or Windows Server 2012 R2, see the Configuration Properties 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 iSCSI Initiator Properties dialog box on the host.

- For Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2, click **Start** > **Administrative Tools** > **iSCSI Initiator** > **Discovery** > **Advanced** to specify inbound values for each storage system when you add a target portal. Click **General** > **Secret** in the iSCSI Initiator Properties dialog box to specify the outbound value (mutual CHAP only).
- For Windows Server 2012 or Windows Server 2012 R2, click **Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator** > **Targets** > **Discovery** > **Advanced** to specify inbound values for each storage system when you add a target portal. Click **Configuration** > **CHAP** in the iSCSI Initiator Properties dialog box 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 following versions of Windows Server, which include a RADIUS server.

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

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.

For information about configuring this RADIUS server, see the Windows online Help.

For information about configuring the storage system to use RADIUS, see the *SAN Administration Guide* (formerly the *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 clustered Data ONTAP. 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.

Related concepts

ALUA support and requirements on page 10

Obtaining a DSM license key

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

Before you begin

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

Steps

1. To obtain a license key for a new copy of the Data ONTAP DSM for Windows MPIO (MPIO-WIN key), go to the NetApp Support Protocol License page.
2. In the **Show Me All** field, select **DSM-MPIO-WIN**, and then click **Go**.
3. Record the appropriate license key.

Related information

NetApp Support Protocol License page - support.netapp.com/eservice/agree.do

Installing PowerShell 2.0

PowerShell 2.0 or later is required for Data ONTAP DSM operations. On Windows Server 2003 or 2008 (but not 2008 R2), PowerShell is not installed by default. You must install it before running the DSM installation or upgrade program.

Steps

1. Download PowerShell from the Microsoft support site.
2. Follow the instructions provided by Microsoft to install the software.

Related information

Microsoft support site - http://support.microsoft.com

Installing .NET framework on Windows Server 2003 or 2008

Only .NET framework 3.5 is supported for Data ONTAP DSM 4.0 and later. On Windows Server 2003 or 2008 (but not 2008 R2), .NET framework is not installed by default. You must install it before running the DSM installation or upgrade program.

Steps

1. Download .NET framework from the Microsoft support site.
2. Follow the instructions provided by Microsoft to install the application development platform software.

Related information

Microsoft support site - http://support.microsoft.com

DSM installation options

You can use either of two methods to install Data ONTAP DSM. You can run the installation program interactively by using an installation wizard, or you can run the installation program silently (unattended) 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 upgrade process instead.

You must have already completed the following tasks:

- Stopped applications, I/O, and for hosts in a cluster configuration, stopped the cluster service
- Backed up any critical data on your Windows host
- Installed Windows hotfixes
- Obtained a DSM license key
- For Windows Server 2003 and 2008 (but not 2008 R2), installed PowerShell 2.0 or later

Note: The installation will fail if the local computer does not have Internet access.

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

About this task

The installation program displays the existing and new versions of DSM and Windows MPIO components. It never installs new Windows MPIO components for Windows Server 2008, 2012, or 2012 R2.

For Windows Server 2003 and 2008 (but not 2008 R2), the installation program will not let you continue if PowerShell 2.0 or later is not installed.

Note: For Windows Server 2008 or later, if the Hyper-V role is not enabled, the installation program sets the SAN Policy on the Windows host to "Online All."

Steps

1. Change to the directory to which you downloaded the executable file.
2. Launch the installation program and follow the instructions on the screen.
3. Enter the DSM license key when prompted.

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.

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

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

6. Follow the instructions on the screen to complete the installation.

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, 2008 R2, 2012, and 2012 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

Note: PowerShell 2.0 is required for Data ONTAP DSM operations. Do not uninstall PowerShell 2.0 if you plan to continue using the DSM.

Related concepts

Windows Administrator account option on page 14
What the Hyper-V Guest Utilities are on page 28

Related tasks

Installing Windows hotfixes on page 33
Installing PowerShell 2.0 on page 43
Stopping host I/O and the cluster service on page 32
Obtaining a DSM license key on page 42
Running the DSM installation program from a command line on page 46
Upgrading the DSM on page 54

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 for new DSM installations. For upgrades, follow the upgrade process instead.

You must have already completed the following tasks:

- Stopped applications, I/O, and for hosts in a cluster configuration, stopped the cluster service
- Backed up any critical data on your Windows host.
- Installed Windows hotfixes
- Obtained a DSM license key
- For Windows Server 2003 and 2008 (but not 2008 R2), installed PowerShell 2.0 or later

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

About this task

- 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.

Note: For Windows Server 2008 or later, if the Hyper-V role is not enabled, the installation program sets the SAN Policy on the Windows host to "Online All."

Steps

1. Download or copy the appropriate installation file for the processor architecture of your Windows host.
2. 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 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\NetApp\MPIO\`.

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

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

Check to ensure the installation was a success. Then, search the installation log file for the term "hotfix" to locate messages about any missing Windows hotfixes you need to install.

For Windows Server 2008, 2008 R2, 2012, and 2012 R2, use Windows Disk Management to verify that all existing disks are online. If any disks are offline, set them online.

Note: PowerShell 2.0 is required for Data ONTAP DSM operations. Do not uninstall PowerShell 2.0 if you plan to continue using the DSM.

Related concepts

Windows Administrator account option on page 14
What the Hyper-V Guest Utilities are on page 28

Related tasks

Running the DSM installation program interactively on page 44
Installing Windows hotfixes on page 33
Installing PowerShell 2.0 on page 43
Stopping host I/O and the cluster service on page 32
Obtaining a DSM license key on page 42
Upgrading the DSM on page 54

Configuring Hyper-V systems

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

Related concepts

What the Hyper-V Guest Utilities are on page 28

Adding virtual machines to a failover cluster

Hyper-V virtual machines stored on the same LUN can be added to a cluster only if all of the virtual machine resources are in the same storage resource group.

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 storage resource group. Otherwise, adding virtual machines to the cluster fails.

Steps

1. Move the available storage resource group to the node on which you are creating and adding virtual machines. (The available storage resource group in a Windows Server 2008, 2008 R2, 2012, or 2012 R2 Windows failover cluster is hidden.)
   - For Windows Server 2008, enter the following command at a Windows command prompt on the cluster node:

     `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.
   - For Windows Server 2008 R2, 2012, or 2012 R2 enter the following command at a Windows command prompt on the cluster node:

```
c:\PS>Move-ClusterGroup "Available Storage" -Node 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. 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. For Windows Server 2012 and later, virtual machines should be created using Cluster Manager.

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 stand-alone 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 NetApp 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\NetApp\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 references

iSCSI software initiator options on page 38

Related information

Microsoft Connect - http://connect.microsoft.com

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 NetApp 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 - http://connect.microsoft.com

Hyper-V VHD requires alignment for best performance

On a Windows Server 2003, Windows 2000 Server, or Linux virtual machine, a Hyper-V virtual hard drive (VHD) partitioned with a master boot record (MBR) needs to be aligned with the underlying LUN for best performance. Use the Data ONTAP PowerShell Toolkit to check and correct MBR partition alignment 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 NetApp LUNs. Partitions created by Windows Server 2008, 2008 R2, 2012, and 2012 R2 should be aligned by default.

Use the Get-NaVirtualDiskAlignment cmdlet in the Data ONTAP PowerShell Toolkit to check whether partitions are aligned with underlying LUNs. If partitions are incorrectly aligned, use the Repair-NaVirtualDiskAlignment cmdlet to create a new VHD file with the correct alignment. The cmdlet copies all partitions to the new file. The original VHD file is not modified or deleted. The virtual machine must be shut down while the data is copied.

You can download the Data ONTAP PowerShell Toolkit at NetApp Communities. Unzip the DataONTAP.zip file into the location specified by the environment variable %PSModulePath% (or

use the Install.ps1 script to do it for you). Once you have completed the installation, use the Show-NaHelp cmdlet to get help for the cmdlets.

Note: The PowerShell Toolkit supports only fixed-size VHD files with MBR-type partitions. VHDs using Windows dynamic disks or GPT partitions are not supported.

The PowerShell Toolkit requires a minimum partition size of 4 GB. 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 PowerShell Toolkit.

Related information

NetApp Communities

Reinstalling GRUB for Linux guests after correcting MBR alignment with PowerShell Toolkit

After correcting MBR alignment with PowerShell Toolkit on 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 PowerShell Toolkit cmdlet has completed on the VHD 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 Esc 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, 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 VHD, enter the following command to identify the boot disk:

   ```
   find /boot/grub/stage1
   ```

   Then 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. A reboot of the Windows host is required to complete the upgrade.

Before you begin

Windows Server systems must be running Data ONTAP DSM 3.4 or later before they can be upgraded directly to DSM 4.1.

Note: On Windows Server 2008 R2 systems, you must uninstall earlier versions of the Data ONTAP DSM before installing DSM 4.1.

Steps

1. *Verifying your host configuration* on page 54
2. *Stopping host I/O and the cluster service* on page 55
3. *Installing Windows hotfixes* on page 56
4. *Removing FC or iSCSI paths to 7-Mode LUNs* on page 58
5. *Enabling ALUA for FC paths* on page 59
6. *Installing PowerShell 2.0* on page 59
7. *Running the DSM upgrade program* on page 59

Related concepts

Windows Administrator account option on page 14

Verifying your host configuration

Verify your configuration before you install or upgrade the DSM.

Steps

1. Use the 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

After you search for your configuration and click a configuration name, details for that configuration display in the Configuration Details dialog box. In this dialog box, be sure to review the information in the following tabs:

Notes	Lists important alerts and notes that are specific to your configuration. Review the alerts to identify the hotfixes that are required for your operating system.
Policies and Guidelines	Provides general guidelines for all SAN configurations. For example, you can view support information about Hyper-V in the Virtualization section and you can view support information about third-party HBAs and CNAs in the section titled Third-party Host Bus Adapter (HBA) and Converged Network Adapter (CNA) Model Support.

2. **For ESX Virtualized Windows Server:** You should use the Interoperability Matrix to verify your ESX Virtualized Windows Server guests if the following applies to your configuration:
   - Your parent server is running a version of ESX that is listed as a supported version on the Interoperability Matrix.
   - You are using the Microsoft iSCSI software initiator to connect directly to a SAN configuration from the Windows Server guest.

Related information

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

Stopping host I/O and the cluster service

The installation of hotfixes and the Data ONTAP DSM requires rebooting the Windows host. Before rebooting, you must first 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.

   See bug 373412 at Bugs Online for the latest information about this issue.

Related information

Bugs Online - support.netapp.com/NOW/cgi-bin/bol/

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 required 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. If you are prompted to install a hotfix that is already installed, try enabling the affected Windows feature and then restarting 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 personnel. They are not available for direct download.

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

Related information

Microsoft support site - http://support.microsoft.com
NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 required hotfix for Data ONTAP DSM. The specified file version is the minimum requirement.

The 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 2012

The following hotfix is not required for Windows Server 2012, but is recommended.

Hotfix	When recommended	File name
2796995	Always	Csvfs.sys

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
945119	Always	Storport.sys
982109	Always	Mpio.sys

Windows Server 2008 SP2

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

Hotfix	When required	File name
968675	Always	Storport.sys
2754704	Always	Mpio.sys
2684681	Always	Msiscsi.sys

Windows Server 2008 R2

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

Hotfix	When required	File name
2528357	Always	Storport.sys
979711	Always	Msiscsi.sys
2684681	Always	Iscsilog.dll
2754704	Always	Mpio.sys

The following hotfix is not required for Windows Server 2008 R2, but is recommended.

Hotfix	When recommended	File name
2520235	Always	Clusres.dll

Windows Server 2008 R2 SP1

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

Hotfix	When required	Filename
2528357	Always	Storport.sys
2754704	Always	Mpio.sys
2684681	Always	Iscsilog.dll

Windows Server 2008

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

Hotfix	When required	Filename
2754704	Always	Mpio.sys
2684681	Always	Iscsilog.dll

Related information

Microsoft support site - http://support.microsoft.com
NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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, the DSM does not support both FC and iSCSI paths to the same 7-Mode LUN.

About this task

Note: Creating iSCSI and FC paths to the same LUN is not supported in Data ONTAP operating in 7-Mode.

Step

1. Use the `lun unmap` command to unmap a LUN from an igroup. For more information, see the *SAN Administration Guide* (formerly the *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 clustered Data ONTAP. 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.

Installing PowerShell 2.0

PowerShell 2.0 or later is required for Data ONTAP DSM operations. On Windows Server 2003 or 2008 (but not 2008 R2), PowerShell is not installed by default. You must install it before running the DSM installation or upgrade program.

Steps

1. Download PowerShell from the Microsoft support site.
2. Follow the instructions provided by Microsoft to install the software.

Related information

Microsoft support site - http://support.microsoft.com

Running the DSM upgrade program

You can use either of two methods to upgrade Data ONTAP DSM. You can run the upgrade program interactively by using an installation wizard, or you can run the upgrade program silently (without

periodic user intervention in response to wizard prompts) by running a command. A reboot of the Windows host is required to complete the upgrade.

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 on all 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 the current version interactively, or use the silent (command line) upgrade option.

Before you begin

You must have already completed the following tasks:

- Stopped applications, I/O, and for hosts in a cluster configuration, stopped the cluster service
- Backed up any critical data on your Windows host
- Installed Windows hotfixes
- For Windows Server 2003 and 2008 (but not 2008 R2), installed PowerShell 2.0 or later

Note: The installation will fail if the local computer does not have Internet access.

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

About this task

The installation program displays the existing and new versions of DSM and Windows MPIO components. It never installs new Windows MPIO components for Windows Server 2008 and 2012.

For Windows Server 2003 and 2008 (but not 2008 R2), the installation program will not let you continue if PowerShell 2.0 or later is not installed.

Note: For Windows Server 2008 or later, if the Hyper-V role is not enabled, the installation program sets the SAN Policy on the Windows host to "Online All."

Steps

1. Change to the directory to which you downloaded the executable file.
2. Launch the installation program and follow the instructions on the screen.
3. Enter the DSM license key when prompted.
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.

   The DSM service requires an Administrator-level account to allow it to manage disks and paths on the Windows host.
5. Choose whether to install the Hyper-V Guest Utilities.
6. Follow the instructions on the screen to complete the installation.
7. When prompted, click **Yes** to reboot the Windows host and complete the installation.

Result

The installer maintains the existing load balance policies for virtual disks if it can. Verify that your load balance policies are configured the way you want.

Note: If you upgrade to the DSM from a release prior to 3.4, the default load balance policy is changed to Least Queue Depth. The load balance policy for virtual disks previously assigned the default load balance policy is also changed to Least Queue Depth. The installer maintains the existing load balance policies if you upgrade from DSM 3.4.

After you finish

For Windows Server 2008, 2008 R2, and 2012, 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.

Note: PowerShell 2.0 is required for Data ONTAP DSM operations. Do not uninstall PowerShell 2.0 if you plan to continue using the DSM.

Related concepts

What the Hyper-V Guest Utilities are on page 28

Related tasks

Installing Windows hotfixes on page 33

Installing PowerShell 2.0 on page 43
Stopping host I/O and the cluster service on page 32
Running the DSM upgrade from a command line on page 62

Running the DSM upgrade from a command line

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

Before you begin

You must have already completed the following tasks:

- Stopped applications, I/O, and for hosts in a cluster configuration, stopped the cluster service
- Backed up any critical data on your Windows host
- Installed Windows hotfixes
- For Windows Server 2003 and 2008 (but not 2008 R2), installed PowerShell 2.0 or later

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

About this task

- 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.

Note: For Windows Server 2008 or later, if the Hyper-V role is not enabled, the installation program sets the SAN Policy on the Windows host to "Online All."

Steps

1. Download or copy the appropriate installation file for the processor architecture of your Windows host.
2. 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 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\NetApp\MPIO\`.

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

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 load balance policies for virtual disks if it can. Verify that your load balance policies are configured the way you want.

Note: If you upgrade to the DSM from a release prior to 3.4, the default load balance policy is changed to Least Queue Depth. The load balance policy for virtual disks previously assigned the default load balance policy is also changed to Least Queue Depth. The installer maintains the existing load balance policies if you upgrade from DSM 3.4.

After you finish

For Windows Server 2008, 2008 R2, and 2012, 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.

Note: PowerShell 2.0 is required for Data ONTAP DSM operations. Do not uninstall PowerShell 2.0 if you plan to continue using the DSM.

Related concepts

What the Hyper-V Guest Utilities are on page 28

Related tasks

Running the DSM upgrade interactively on page 60
Installing Windows hotfixes on page 33
Installing PowerShell 2.0 on page 43
Stopping host I/O and the cluster service on page 32

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 Control Panel 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 needed registry entries 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 (because 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 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 version without uninstalling.

Steps

1. Quiesce host I/O and stop any applications accessing the LUNs on the storage system.
2. Select **Add or Remove Programs** (Windows Server 2003) or **Programs and Features** (Windows Server 2008, 2008 R2, 2012, or 2012 R2) in the Control Panel.
3. Select **Data ONTAP DSM for Windows MPIO**.
4. Click **Remove** (Windows Server 2003) or **Uninstall** (Windows Server 2008, 2008 R2, 2012, or 2012 R2).
5. 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 in the Control Panel.

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 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.

   `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 Control Panel.

About this task

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

Steps

1. Click **Add or Remove Programs** (Windows Server 2003) or **Programs and Features** (Windows Server 2008, 2008 R2, 2012, or 2012 R2) in the Control Panel.
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.

   Optionally, you can enter the user name and password of the account on the Windows host under which the DSM management service runs. This account must be in the Windows Administrators group.
5. Follow the instructions on the screen and reboot the Windows host when prompted.

Related concepts

Windows Administrator account option on page 14

Managing the DSM using the GUI

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

Related tasks

Managing the DSM using Windows PowerShell cmdlets on page 86

Starting the DSM GUI

The DSM GUI is a Microsoft management console (MMC) Snapin Extension under the Storage node in both the Computer Management console and the Server Manager console. You can use either utility to start the DSM. The following procedure describes how to start the DSM GUI using the Computer Management console.

About this task

Note: Prior to DSM 4.1, the Data ONTAP (R) DSM Management window displayed the DSM driver version. Beginning with DSM 4.1, the product version is displayed instead of the driver version.

Steps

1. Select **Administrative Tools > Computer Management** in the Windows Control Panel.
2. Expand the **Storage** node in the navigation tree.
3. Click **Data ONTAP (R) DSM Management**.

Result

The DSM GUI is displayed.

Discovering new disks

LUNs on your storage system appear as disks to the Windows host. Any new disks for LUNs you add to your system are not automatically discovered by the host. You must manually rescan disks to discover them.

Steps

1. Open the Windows Computer Management utility:

For...	Click...
Windows Server 2012	**Tools** > **Computer Management**
Windows Server 2008	**Start** > **Administrative Tools** > **Computer Management**

2. Expand the **Storage** node in the navigation tree.
3. Click **Disk Management**.

Viewing summary information for virtual disks

The Windows host treats LUNs on your storage system as virtual disks. The upper pane of the DSM GUI displays summary information for the virtual disks visible to the host.

The virtual disks summary displays the following information.

Disks	Virtual disk ID and drive letter or mount point. There are two special cases: • A dummy disk ID is displayed while the LUN is being taken offline on the target. • No drive letter or mount point is displayed when the virtual disk is taken offline on the host.
Storage System	For Data ONTAP operating in 7-Mode, the name of the storage system to which the LUN belongs. For clustered Data ONTAP, the name of the Storage Virtual Machine (SVM) to which the LUN belongs.
Storage System Path	Volume path to the LUN on the storage system.
Load Balance Policy	Load balance policy in effect for the virtual disk.
Reserved By This Node	Whether the LUN for the virtual disk is reserved under a persistent reservation request by a Windows cluster. Right-click in the field to display the reservation key. The key identifies the cluster node that holds the reservation for the LUN.
Total Paths	Number of available paths for the virtual disk.

Related tasks

Displaying the persistent reservation key for a virtual disk on page 81
Changing the load balance policy on page 77

Related references

Viewing detailed information for virtual disks on page 72

Viewing events report information for virtual disks

The events report displays significant GUI events such as errors encountered during automatic and manual refreshes, changes in the DSM/MPIO properties, and changes in load balance properties.

The following events are displayed in the events report.

Note: The events report could be blank if there are no errors or other GUI events to display.

Level Severity level of the event.

- **Information** Indicates the successful completion of a particular event during refresh.
- **Error** Indicates an error occurred during refresh.
- **Warning** Indicates a warning that occurred during refresh.

Date and Time Date and time of the event.

Description More information about the event.

Event ID A unique identifier for each type of event.

Error and Information Levels and Event IDs

The following table summarizes the various events displayed in this tab along with their event IDs and levels.

Level	Description	Event ID
Error	Failed to get disk information	101
Error	Failed to get path information	102
Error	Failed to get I/O stats information	103
Error	Partially displaying disk information under error conditions	104
Error	Failed to change LBP of a disk	105
Error	Failed to change any DSM parameters	106
Error	Failed to change any of the MPIO parameters	107

Level	Description	Event ID
Information	Successfully changed the LBP of disk/disks	6
Information	Successfully changed the DSM parameters	7
Information	Successfully changed the MPIO parameters	8
Information	Successfully changed the Powershell timeout period	9

Displaying the events report

The events report is hidden by default, but you can display it through the Computer Management or Server Management control windows.

Steps

1. Select **Administrative Tools** > **Computer Management** in the Windows Control Panel.
2. Expand the **Storage** node in the navigation tree.
3. Click **Data ONTAP (R) DSM Management**.
4. Right-click **Data ONTAP (R) DSM Management** and select **View Events**.
5. To hide the events report, right-click **Data ONTAP (R) DSM Management** and select **Hide Events**.

Changing the number of entries in the detailed events report

The number of entries displayed in the detailed events report is set by default to 100. However, you can increase or decrease the number of entries displayed to match your preference.

About this task

Once the maximum number of entries has been reached, the oldest entries will be removed as newer entries are added. To change the default number of entries, do the following:

Steps

1. Select **Administrative Tools** > **Computer Management** in the Windows Control Panel.
2. Expand the **Storage** node in the navigation tree.
3. Click **Data ONTAP (R) DSM Management**.
4. Right-click **Data ONTAP (R) DSM Management** and select **Settings**.

5. Update the **Max Event Entries** field to reflect the number of entries you prefer.

Viewing detailed information for virtual disks

For each LUN visible to the Windows host as a virtual disk, the DSM displays the paths to the LUN, the properties of the LUN, input/output statistics, and path history for the available paths.

The virtual disks detail pane displays the following tabs.

Paths	Information about the available paths for the selected virtual disk.
LUN Info	Properties of the LUN for the selected virtual disk.
I/O statistics	Input/output statistics for the available paths for the selected virtual disk.
History	History of significant I/O errors and changing path properties.

The bottom left corner of the virtual disks detail pane also displays the date and time of the last successful disk refresh.

Related references

Viewing summary information for virtual disks on page 69

Viewing path information for virtual disks

For each LUN visible to the Windows host as a virtual disk, the DSM displays the paths to the LUN. The **Paths** tab in the lower pane of the DSM GUI displays the available paths for the selected disk. If multiple disks are selected in the disk summary panel, no information about paths, LUN details, stats, or history will be seen in the lower panel.

Note: You can select multiple paths for each action available in the tab.

The **Paths** tab displays the following information.

Note: The load balance policy for the selected virtual disk determines the available fields. Unless otherwise indicated, a field is available under each policy.

Disk ID	Virtual disk ID. A dummy disk ID is displayed while the LUN is being taken offline on the target.
Path ID	ID of the path. An eight-character identifier consisting of four two-character fields. The first three fields identify the port, bus, and target. The fourth field is for internal use.
Operational State	Operational state of the path. Available values are: **Active/ Optimized** — Under an active/active load balance policy, an optimized path currently used to access the virtual disk.

Active/Non-Optimized	Under an active/active load balance policy, a non-optimized path currently used to access the virtual disk.
Active	Under an active/passive load balance policy, a path currently used to access the virtual disk.
Passive	Under an active/passive load balance policy, a path not currently used to access the virtual disk, but available to take over for the active path if the active path fails.

Admin State Administrative state of the path. Available values are:

Enabled	A path available for use.
Disabled	A path not available for current or takeover use, unless all enabled paths are unavailable.

Path Weight	The priority of the path relative to other paths for the virtual disk. The path with the lowest value has the highest priority. Available for disks with Least Weighted Paths load balance policy only.
Preferred Path	Whether the path is preferred for use relative to other paths for a virtual disk. Available for disks with Round Robin with Subset load balance policy only.
Initiator Name	Name of the FC HBA or iSCSI initiator used for the path.
Initiator Address	Worldwide port name (WWPN) of the FC HBA or IP address of the iSCSI initiator used for the path.
Target Address	Remote endpoint address for SAN paths managed by the DSM. For FC, this is the WWPN of the target adapter port. For iSCSI, this is the IP address and port number of the iSCSI portal.
Target Group ID	ALUA target port group identifier.
Target Port ID	ALUA relative target port identifier.

Viewing LUN information for virtual disks

For each LUN visible to the Windows host as a virtual disk, the DSM displays the LUN's properties. The **LUN Info** tab in the lower pane of the DSM GUI displays the properties of the LUN for the selected disk.

The **LUN Info** tab displays the following information.

Disk ID	Virtual disk ID. A dummy disk ID is displayed while the LUN is being taken offline on the target.
LUN	LUN number of the LUN. 0 is displayed while the LUN is being taken offline on the target.

LUN Type	LUN identifier on the storage system.
Serial Number	LUN serial number on the storage system.
Size	Virtual disk unformatted size. Usable capacity will be less.
Cluster Mode	The mode in which Data ONTAP is operating on the storage system.
	C-Mode — Clusted Data ONTAP FC or iSCSI targets.
	Single Image — FC targets operating in 7-mode.
	None — Non-ALUA-enabled iSCSI targets operating in 7-mode.
ALUA Enabled	Whether ALUA is enabled for the LUN.

Viewing I/O statistics for virtual disks

For each LUN visible to the Windows host as a virtual disk, the DSM displays input/output statistics for the available paths to the LUN. The **I/O Statistics** tab in the lower pane of the DSM GUI displays the statistics for the paths to the LUN for the selected disk.

The **I/O Statistics** tab displays the following information. For virtual disks that reside on a LUN that has a LUN size of 2TB or larger, I/O statistics are displayed in MB.

Note: You can click the **Reset** button to reset the statistical fields to 0.

Average Read Size	Average size of read request serviced by the path.
Disk ID	ID of the virtual disk.
Path ID	ID of the path. An eight-character identifier consisting of four two-character fields. The first three fields identify the port, bus, and target. The fourth field is for internal use.
Operational State	Operational state of the path. Available values are:
	Active/ Optimized — Under an active/active load balance policy, an optimized path currently used to access the virtual disk.
	Active/Non-Optimized — Under an active/active load balance policy, a non-optimized path currently used to access the virtual disk.
	Active — Under an active/passive load balance policy, a path currently used to access the virtual disk.
	Passive — Under an active/passive load balance policy, a path not currently used to access the virtual disk, but available to take over for the active path if the active path fails.

Minimum read size	Minimum size of read request serviced by the path in bytes.
Maximum read size	Maximum size of read request serviced by the path in bytes.
Average read Size	Average size of read request serviced by the path in bytes.
Total Reads	Number of read requests serviced by the path in bytes.
Total Bytes Read	Cumulative read byte count.
Minimum write size	Minimum size of write request serviced by the path in bytes.
Maximum write size	Maximum size of write request serviced by the path in bytes.
Average write Size	Average size of write request serviced by the path in bytes.
Total Writes	Number of write requests serviced by the path in bytes.
Total Bytes Written	Cumulative write byte count.
Total Failovers	Number of times the path experienced a failover between arrival and removal.
Total I/O Errors	Number of times I/O requests on the path resulted in errors.
Total Outstanding Requests	Number of queued requests that have not yet been serviced.

Viewing history information for virtual disk

For each LUN visible to the Windows host as a virtual disk, the DSM displays the paths to the LUN. The **History** tab in the lower pane of the DSM GUI displays past activity on each path including significant errors that resulted in either failover or retry exhaustion.

In addition to error messages, the **History** tab also displays other events such as success or failure when changing path attributes. The **History** tab displays the following information.

Note: If there are not significant errors or other events to report, there will be no information in the history tab. It will be blank.

Disk ID	Virtual disk ID. A dummy disk ID is displayed while the LUN is being taken offline on the target
Path ID	ID of the path. An eight-character identifier consisting of four two-character fields. The first three fields identify the port, bus and target. The fourth field is for internal use.
Level	Severity level of the history event. The possible values are Information, Warning, and Error.
Date and Time	Date and time of the event
Description	A brief description of the history event.

Event ID A unique identifier for each type of history event.

The following table summarizes the various events displayed in this tab along with their Event IDs and levels.

Level	Event Type	Event ID
Error	Failed to change admin state	1101
Error	Failed to change operational state	1102
Error	Failed to change path weight	1103
Error	Failed to change preferred path	1104
Error	Error I/O Failover or Retry Exhaustion	1105
Information	Successfully changed admin state	1000
Information	Successfully change of Operational state	1001
Information	Successful change of Path Weight	1002
Information	Successful change of Preferred Path	1002

Changing the number of entries displayed in the history view

The number of entries displayed in the history view is set by default to 100. However, you can increase or decrease the number of displayed entries to match your preference.

About this task

Once the maximum number of entries has been reached, the oldest entries will be removed as newer entries are added. To change the default number of entries, do the following.

Steps

1. Select **Administrative Tools** > **Computer Management** in the Windows Control Panel.
2. Expand the **Storage** node in the navigation tree.
3. **Right-click** on your node and select **Settings**.
4. Update the **Max History Entries** field to reflect the number of entries you prefer.

Changing the load balance policy

You can change the load balance policy for virtual disks in the upper pane of the DSM GUI. The DSM sets the load balance policy for newly discovered disks by default, based on your settings in the Data ONTAP DSM Properties window.

Steps

1. In the upper pane of the DSM GUI, select the disks whose load balance policy you want to change.
2. Right-click in the **Load Balance Policy** column and choose the desired load balance policy from the pop-up menu. All policies use optimized paths before non-optimized paths.

Option	Description
Auto Assign	Active/passive. An arbitrary path is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
Failover Only	Active/passive. The path you specify is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
Round Robin	Active/active. All paths are used to access the virtual disk, in round-robin order.
Round Robin with Subset	Active/active. The paths you specify are used to access the virtual disk, in round-robin order. A non-preferred path takes over for a preferred path if the preferred path fails.
Least Weighted Paths	Active/passive. The path with the lowest weight value is used to access the virtual disk.
Least Queue Depth	Active/active. All paths are used to access the virtual disk, in order of the available path with the smallest queue.

Related concepts

Load balance policies determine failover behavior on page 13
When to change the load balance policy on page 22
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Changing the default load balance policy on page 78

Changing the default load balance policy

The default load balance policy setting determines the load balance policy assigned to new virtual disks. Changing this setting has no effect on existing virtual disks.

Steps

1. In the DSM GUI window, choose **Action** > **Properties**.

   The Data ONTAP DSM Properties window is displayed.

2. In the **Data ONTAP DSM Properties** window, click the **Data ONTAP DSM** tab.

3. In the Default Load Balance Property group, click the check box for the desired policy. Click **Reset to Default** and then click **OK** to restore the default value. For all policies, optimized paths are used before non-optimized paths.

Option	Description
Auto Assign	Active/passive. An arbitrary path is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
Failover Only	Active/passive. The path you specify is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
Round Robin	Active/active. All paths are used to access the virtual disk, in round-robin order.
Round Robin with Subset	Active/active. The paths you specify are used to access the virtual disk, in round-robin order. A non-preferred path takes over for a preferred path if the preferred path fails.
Least Weighted Paths	Active/passive. The path with the lowest weight value is used to access the virtual disk.
Least Queue Depth	Active/active. All paths are used to access the virtual disk, in order of the available path with the smallest queue.

Related concepts

Load balance policies determine failover behavior on page 13
When to change the load balance policy on page 22
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Changing the load balance policy on page 77

Changing the operational state of a path

The operational state of a path determines whether it is active or passive. For a virtual disk with a Failover Only load balance policy, you can change the operational state of a path in the lower pane of the DSM GUI.

Steps

1. In the lower pane of the DSM GUI, select the paths whose operational state you want to change. You can only select one path at a time.
2. Right-click in the **Operational State** column and choose **Set Active** to change a passive operational state to active. Operational states are as follows:

Option	Description
Set Active	The path is used to access the virtual disk.
Set Passive	The path is not used to access the virtual disk, but is available to take over for the active path if the active path fails.

Related concepts

Load balance policies determine failover behavior on page 13
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Changing the administrative state of a path

The administrative state of a path determines whether it is enabled or disabled. You can change the administrative state of a path in the lower pane of the DSM GUI.

Steps

1. In the lower pane of the DSM GUI, select the paths whose administrative state you want to change.
2. Right-click in the **Administrative State** column and choose the desired administrative state from the pop-up menu.

Option	Description
Enabled	The path is available for use.
Disabled	The path is not available for current or takeover use, unless all enabled paths are unavailable.

Changing the path weight

The weight of a path determines its priority relative to other paths for a virtual disk. The path with the lowest value has the highest priority. For a virtual disk with a Least Weighted Paths load balance policy, you can change the weight of a path in the lower pane of the DSM GUI.

About this task

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

Steps

1. In the lower pane of the DSM GUI, select the paths whose weight you want to change.
2. Right-click in the **Path Weight** column and choose **Set Path Weight** in the pop-up menu.
3. In the **Set Path Weight** dialog box, enter a value between 0 (highest priority) and 255 (lowest priority).

Related concepts

Load balance policies determine failover behavior on page 13
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Changing the preferred path

Preferred paths are preferred for use relative to other paths for a virtual disk. For a virtual disk with a Round Robin with Subset load balance policy, you can specify which paths are preferred in the lower pane of the DSM GUI.

About this task

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

Steps

1. In the lower pane of the DSM GUI, select the paths you want to prefer.
2. Right-click in the **Preferred Path** column and choose **Set Preferred** from the pop-up menu.

   Note: Skip this step if the Preferred Path value is already set to Yes.
3. Select the paths you do not want as preferred paths.
4. Right-click in the **Preferred Path** column and choose **Clear Preferred** from the pop-up menu.

Note: Skip this step if the Preferred Path value is already set to No.

Related concepts

Load balance policies determine failover behavior on page 13
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Displaying the persistent reservation key for a virtual disk

A Windows cluster may issue a *persistent reservation request* to reserve access to LUNs. The *persistent reservation key* for a virtual disk identifies the node in the Windows cluster that holds the reservation for the LUN. You can display the key in the upper pane of the DSM GUI.

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.

Note: The option to view the persistent reservation key will only be available if the `Reserved by this Node` field is set to `yes`.

Steps

1. In the upper pane of the DSM GUI, select the disk whose persistent reservation key you want to display.
2. Right-click in the Reserved field and choose **Display Persistent Reservation Key** to display the persistent reservation key.

   Note: The menu choice is not available if a persistent reservation key has not been issued for the LUN.

Related tasks

Setting persistent reservation parameters on page 81

Setting persistent reservation parameters

Persistent reservation parameters control how the DSM handles storage controller faults when servicing persistent reservation requests on behalf of a Windows cluster.

Steps

1. In the DSM GUI window, choose **Action** > **Properties**.

The Data ONTAP DSM Properties window is displayed.

2. In the **Data ONTAP DSM Properties** window, click the **Data ONTAP DSM** tab.
3. In the Persistent Reservations Parameters group, edit the parameters as needed. Click **Reset to Default** to restore the default values.

Option	Description
Timeout (sec)	The amount of time in seconds that the DSM waits to receive a response for reservation commands.
Retry Interval (sec)	The amount of time in seconds that the DSM waits before retrying a failed reservation command.
Retry Count	Read only. The number of times the DSM retries a failed reservation command.

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

Related tasks

Displaying the persistent reservation key for a virtual disk on page 81

Changing what gets logged by the DSM

The event log level determines the number of messages the DSM writes to Windows event logs. Changing the event log level affects only messages written by the DSM itself. It does not affect messages written by other Windows MPIO components.

Steps

1. In the DSM GUI window, choose **Action** > **Properties**.

   The Data ONTAP DSM Properties window is displayed.
2. In the **Data ONTAP DSM Properties** window, click the **Data ONTAP DSM** tab.
3. In the Event Log Level group, click the radio button for the desired level. Click **Reset to Default** to restore the default value.

Option	Description
None	The DSM logs no messages to Windows event logs.
Normal	The DSM logs the normal level of messages to Windows event logs.
Info	In addition to the normal level of messages, the DSM logs messages for path transitions and reservation changes to Windows event logs.
Debug	The DSM logs all messages to Windows event logs. Recommended for debugging only.

Note: The Info and Debug levels may impair system performance.

The new event log level is effective immediately. No reboot is necessary.

Related tasks

Modifying values for DSM parameters on page 98

Related references

Event message reference on page 123

Setting MPIO tunable parameters

You can set tunable parameters for the Windows MPIO driver in the **MPIO** tab of the properties window. These parameters affect the behavior of all DSMs on the host.

Steps

1. In the DSM GUI window, choose **Action** > **Properties**.

   The Data ONTAP DSM Properties window is displayed.

2. In the **Data ONTAP DSM Properties** window, click the **MPIO** tab.

3. On the **MPIO** tab, edit the parameters as needed. Click **Reset to Default** to restore the default values.

Option	Description
Enable Path Verify	Whether the Windows MPIO driver periodically requests that the DSM check its paths.
Path Verification Period (sec)	When **Enable Path Verify** is selected, determines the amount of time in seconds that the DSM waits to check its paths.
Retry Count	The number of times the DSM retries a path before the path fails over.
Retry Interval (sec)	The amount of time in seconds that the DSM waits before retrying a failed path.
PDO Removal Period (sec)	The amount of time in seconds that the DSM keeps the multipath pseudo-LUN in system memory after all paths to the device are lost.

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

Setting the DSM GUI auto refresh rate

You can set the auto refresh rate for disk, path, and path I/O information in the Data ONTAP DSM GUI Settings window. You can also edit the PowerShell timeout period.

Steps

1. In the DSM GUI window, choose **Action** > **Settings**.

   The Data ONTAP DSM GUI Settings window is displayed.

2. Select the **Enable Auto Refresh** check box to enable the auto refresh feature.
3. Edit the auto refresh rate settings as needed.

Option	Description
Disks Refresh Rate (sec)	The amount of time in seconds before the DSM auto-refreshes disk information.
Paths Refresh Rate (sec)	The amount of time in seconds before the DSM auto-refreshes path information.
I/O Stats Refresh Rate (sec)	The amount of time in seconds before the DSM auto-refreshes path I/O statistics.

4. In the **Powershell Timeout Period (sec)** field, enter the amount of time in seconds the DSM GUI waits to receive a response from the PowerShell engine.

Related tasks

Refreshing the display manually on page 84

Refreshing the display manually

The DSM automatically refreshes the display based on your settings in the Data ONTAP DSM GUI Settings window. You can refresh the display manually if you prefer.

Step

1. In the DSM GUI window, choose **Action** > **Refresh**.

Related tasks

Setting the DSM GUI auto refresh rate on page 84

Viewing the DSM license key

You can view the license key for the DSM in the **License Information** tab of the properties window.

Before you begin

You must obtain a license for each Windows host computer.

Step

1. In the **Data ONTAP DSM Properties** window, click the **License Information** tab.

   The license key is displayed.

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 were deprecated (but still available) in DSM 3.5. The dsmcli commands are not available in DSM 4.1.

Related tasks

Managing the DSM using the GUI on page 68

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 following table lists the common tasks that you can complete with the cmdlets. For users upgrading from previous releases, it also lists the corresponding deprecated dsmcli commands.

Task	PowerShell cmdlet	Deprecated dsmcli command
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 virtual disks	`get-sandisk`	`dsmcli lun list`
Display details about virtual disks	`get-sandisk`	`dsmcli lun attributes`
Display the current load balance policy for a virtual disk	`get-sandisk`	`dsmcli path list -v`
Display the load balance policies that you can use with a virtual disk	`get-ontapdsmparams`	`dsmcli lun getlbp`
Change the load balance policy for a virtual disk	`set-sandisk`	`dsmcli lun setlbp`

Task	PowerShell cmdlet	Deprecated dsmcli command
Display the persistent reservation key for a Windows 2003 host	`get-ontapdsmparams`	`dsmcli lun getprkey`
Display path information for a virtual disk	`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`
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

The Windows host must meet the following requirements before you can use the Windows PowerShell cmdlets with Data ONTAP DSM.

PowerShell version

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

Windows Server 2003

PowerShell is not installed by default. The Data ONTAP DSM installation program instructs you to install PowerShell 2.0 before continuing the installation.

Windows Server 2008

PowerShell 1.0 is installed by default. The Data ONTAP DSM installation program instructs you to install PowerShell 2.0 before continuing the installation.

Windows Server 2008 R2

PowerShell 2.0 is installed and enabled by default.

Windows Server 2012	PowerShell 2.0 is installed and enabled by default.
Windows Server 2012 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.

Running PowerShell cmdlets on the local host

You can use the Windows Start utility to launch a PowerShell session on the local host.

About this task

Using the Start utility automatically loads the PowerShell cmdlets included with the DSM. Other methods of launching a PowerShell session do not automatically load the cmdlets.

Step

1. Launch a PowerShell session on the local host.
   - For Windows Server 2012 or 2012 R2 press the Windows logo key, then click **Host Service PowerShell** in the Start screen.
   - For Windows Server 2003, 2008, or 2008 R2, click **Start** > **All Programs** > **NetApp** > **Host Service PowerShell**.

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     : 2
PersistentReservationKey     : :0:0:0:0:0:0:0:0
PathVerificationRetryCount   : 6
PathVerificationTimeout      : 2
EventLogLevel                : 1
iSCSILeastPreferred          : 0
```

Getting information about virtual disks

You can use the `get-sandisk` cmdlet to view information about virtual disks. 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 SerialNumber Size   LBPolicy PathCount LUN LunType
------ ------------ ----   -------- --------- --- -------
Disk7  2FiMZ]-7MVhF 10 G   RRwS     1         1   windows_2008...
Disk6  2FiMg]2SMrCv 50 G   FO       2         0   windows_2008...
Disk4  2FiMg]2SMrCy 75 G   FO       2         0   windows_2008...
Disk5  2FiMg]2SMrCz 80 G   DLQD     2         1   windows_2008...
Disk1  C4e6SJOzpuRC 5122 M DLQD     4         0   windows_2008...
Disk3  C4e6SJVboRyS 10 G   WP       4         2   windows_2008...
Disk8  C4e6SJYoOFUc 5122 M RRwS     4         0   windows_2008...
Disk2  C4e6hJOzqAJ8 40 G   DLQD     4         1   windows_2008...
```

Changing the load balance policy using a cmdlet

You can use the `set-sandisk` cmdlet to change the load balance policy for existing virtual disks. The DSM sets the load balance policy for newly discovered virtual disks based on your settings in the `set-ontapdsmparams` cmdlet.

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. All policies use optimized paths before non-optimized paths.

Option	Description
Auto	Auto Assign. Active/passive. An arbitrary path is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
FO	Failover Only. Active/passive. The path you specify is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
RR	Round Robin. Active/active. All paths are used to access the virtual disk, in round-robin order.
RRwS	Round Robin with Subset. Active/active. The paths you specify are used to access the virtual disk, in round-robin order. A non-preferred path takes over for a preferred path if the preferred path fails.
WP	Least Weighted Paths. Active/passive. The path with the lowest weight value is used to access the virtual disk.
DLQD	Least Queue Depth. Active/active. All paths are used to access the virtual disk, in order of the available path with the smallest queue.

Example

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

Related concepts

Load balance policies determine failover behavior on page 13
When to change the load balance policy on page 22

Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Changing the default load balance policy using a cmdlet on page 92
Getting information about virtual disks on page 90

Changing the default load balance policy using a cmdlet

You can use the `set-ontapdsmparams` cmdlet to change the default load balance policy for new virtual disks.

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. For all policies, optimized paths are used before non-optimized paths.

Option	Description
Auto	Auto Assign. Active/passive. An arbitrary path is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
FO	Failover Only. Active/passive. The path you specify is used to access the virtual disk. A passive path takes over for the active path if the active path fails.
RR	Round Robin. Active/active. All paths are used to access the virtual disk, in round-robin order.
RRwS	Round Robin with Subset. Active/active. The paths you specify are used to access the virtual disk, in round-robin order. A non-preferred path takes over for a preferred path if the preferred path fails.
WP	Least Weighted Paths. Active/passive. The path with the lowest weight value is used to access the virtual disk.
DLQD	Least Queue Depth. Active/active. All paths are used to access the virtual disk, in order of the available path with the smallest queue.

Example

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

Related concepts

Load balance policies determine failover behavior on page 13
When to change the load balance policy on page 22
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Changing the load balance policy using a cmdlet on page 91
Modifying values for DSM parameters on page 98

Viewing path information using a cmdlet

You can use the `get-sanpath` cmdlet to view information about the paths for virtual disks. 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 or disk serial number. The `get-sandisk` cmdlet displays disk IDs and serial numbers.

Step

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

   `get-sanpath [-Disk DiskID] [-SerialNumber SerialNumber]`

   #### Example

```
PS C:\>get-sanpath

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

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

Changing path status using a cmdlet

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 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

Load balance policies determine failover behavior on page 13

Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Viewing path information using a cmdlet on page 93
Changing the path weight using a cmdlet on page 95

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 using a cmdlet

You can use the `set-sanpath` cmdlet to set the weight assigned to each path for virtual disks with a Least Weighted Path load balance policy. DSM uses the available path with the lowest weight to access the disk.

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 255 (lowest priority).

   #### Example

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

Related concepts

Load balance policies determine failover behavior on page 13
Path types and Windows clusters affect failover behavior on page 22
Failover examples on page 23

Related tasks

Changing path status using a cmdlet on page 94
Viewing path information using a cmdlet on page 93
Getting information about virtual disks on page 90

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 (I/O) for a path to a virtual disk. 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 or disk serial number. The `get-sandisk` cmdlet displays disk IDs and serial numbers.

Step

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

   `get-sanstats [-Disk DiskID] [-SerialNumber SerialNumber]`

   #### Example

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

   DiskId PathId   NumberOfReads NumberOfWrites NumberOfBytesRead Numb...
   ------ ------   ------------- -------------- ----------------- ----...
   ```

```
Disk5  03000302 757          21            3280384          8601...
Disk5  04000202 2            1             1024             4096...
```

Related tasks

Clearing SAN connectivity statistics on page 97

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

Displaying statistics about SAN connectivity on page 96

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.

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
```

Related tasks

Modifying values for DSM parameters on page 98

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

Changing the default load balance policy using a cmdlet on page 92
Prioritizing FC paths over iSCSI paths on page 97

Changing what gets logged by the DSM on page 82

Related references

Registry values set by Data ONTAP DSM for Windows MPIO on page 16

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.

Related concepts

Tasks required for installing and configuring the DSM on page 9

Recording the WWPN

Record the worldwide port names (sometimes styled "World Wide 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, you record four values.

The WWPN looks like this:

```
WWPN: 10:00:00:00:c9:73:5b:90
```

Steps

1. Display the WWPNs.

For	Use
Windows Server 2012 or Windows Server 2012 R2	The HBA manufacturer's management software, such as OneCommand Manager for Emulex HBAs or QConvergeConsole for QLogic HBAs.
Windows Server 2008 or Windows Server 2008 R2	The Storage Explorer application or the HBA manufacturer's management software, such as OneCommand Manager for Emulex HBAs or QConvergeConsole for QLogic HBAs.
Windows Server 2003	The Microsoft `fcinfo.exe` program or the HBA manufacturer's management software, such as OneCommand Manager for Emulex HBAs or QConvergeConsole for QLogic HBAs.

OneCommand Manager is the successor to HBAnyware. QConvergeConsole is the successor to SANsurfer

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 Storage Explorer

For hosts running Windows Server 2008 or Windows Server 2008 R2, you can obtain the Fibre Channel Worldwide Port Name (WWPN) using the 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

If your host OS supports fcinfo.exe, then you can obtain the Fibre Channel Worldwide Port Name (WWPN) using the Microsoft fcinfo.exe.

Steps

1. If it is 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. Open a command prompt and enter the following command: `fcinfo /ports /details`

   For more options, run the `fcinfo /??` command.
3. Record the value of the **Port WWN** field for each HBA port.

Related information

Microsoft Download Center - www.microsoft.com/downloads/en/default.aspx

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

You must record the iSCSI initiator node name from the iSCSI initiator program on the Windows host.

Steps

1. Open the **iSCSI Initiator Properties** dialog box:

For	Click
Windows Server 2012 and Windows Server 2012 R2	**Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator** > **Configuration**
Windows Server 2008, Windows Server 2008 R2, and Windows Vista	**Start** > **Administrative Tools** > **iSCSI Initiator**
Windows Server 2003 and Windows XP	**Start** > **All Programs** > **Microsoft iSCSI Initiator** > **Microsoft iSCSI Initiator**

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 initiator 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 Windows host sees LUNs on your storage system as virtual disks.

Related concepts

Tasks required for installing and configuring the DSM on page 9

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. 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 depend on the Microsoft iSCSI initiator service.

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 clustered Data ONTAP, 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 clustered Data ONTAP. 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 *SAN Administration Guide* (formerly the *Block Access Management Guide for iSCSI and FC*) for your version of Data ONTAP.

Initiator group overview

Initiator groups (igroups) 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 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. Clustered Data ONTAP supports mixed protocol igroups when used with Data ONTAP DSM 3.5 and later.

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 *SAN Administration Guide* (formerly the *Block Access Management Guide for iSCSI and FC*) for your version of Data ONTAP.

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 the Data ONTAP DSM 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 clustered Data ONTAP, 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, use the following command to start collecting statistics:

   `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 that 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 iSCSI Initiator Properties dialog box on the host.

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 clustered Data ONTAP, 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.

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.

Steps

1. Open the iSCSI Initiator Properties dialog box.

For	Click
Windows Server 2012 or Windows Server 2012 R2	**Server Manager > Dashboard > Tools > iSCSI Initiator**
Windows Server 2008 or Windows Server 2008 R2	**Start > Administrative Tools > iSCSI Initiator**

2. Discover the iSCSI target port on the storage system. On the **Discovery** tab:

For	Click
Windows Server 2012 or Windows Server 2012 R2	**Discover Portal**, then enter the IP address of the iSCSI target port
Windows Server 2008 or Windows Server 2008 R2	**Add Portal**, then enter the IP address of the iSCSI target port

3. Connect to the storage system.

For	Click
Windows Server 2012 or Windows Server 2012 R2	**Targets**, then select an iSCSI target and click **Connect**.
Windows Server 2008 or Windows Server 2008 R2	**Targets**, then select an iSCSI target and click **Log on**.

4. If you want the LUNs to be persistent across host reboots, in the Connect To Target dialog box:

For	Click
Windows Server 2012 or Windows Server 2012 R2	**Add this connection to the list of Favorite Targets**
Windows Server 2008 or Windows Server 2008 R2	**Automatically restore this connection when the computer starts**

5. If you are using MPIO or multiple connections per session, click **Enable multi-path** in the Connect To Target dialog box and 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, 2008 R2, 2012, or 2012 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 the Disk Management folder 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. For more information, see the Windows Disk Management online Help.

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 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 Knowledge Base 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 *SAN Configuration Guide* (formerly the *FC and iSCSI Configuration Guide*) 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 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 information about creating and managing igroups, see the *SAN Administration Guide* (formerly the *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 clustered Data ONTAP) and for iSCSI (clustered Data ONTAP only). For more information about port sets, see the *SAN Administration Guide* (formerly the *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 *SAN Administration Guide* (formerly the *Block Access Management Guide for iSCSI and FC*) for your version of Data ONTAP.

5. For iSCSI boot solutions, refer to your 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 concepts

Tasks required for installing and configuring the DSM on page 9
About SAN booting on page 29

Related information

Support for booting from a Storage Area Network (SAN) - http://support.microsoft.com/kb/305547/en-us
NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/
Documentation on the NetApp Support Site: support.netapp.com
Emulex downloads for Windows - www.emulex.com/downloads.html
QLogic downloads for Windows - driverdownloads.qlogic.com/QLogicDriverDownloads_UI/default.aspx

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

Installing Windows hotfixes on page 33

Internal Error: Access is Denied during installation

On Windows Server 2008 or later, 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 the latest information, see bug 312358 at Bugs Online.

For more information about User Access Control, see the Microsoft Technet article *User Account Control Step-by-Step Guide*.

Related information

Bugs Online - support.netapp.com/NOW/cgi-bin/bol/

Microsoft Technet User Account Control Step-by-Step Guide - technet.microsoft.com/en-us/library/cc709691.aspx

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 User Account Control Step-by-Step Guide - technet.microsoft.com/en-us/library/cc709691.aspx

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 User Account Control Step-by-Step Guide - technet.microsoft.com/en-us/library/cc709691.aspx

Installing Windows Host Utilities after installing the DSM resets the persistent reservation timeout value incorrectly

The persistent reservation timeout value is reset incorrectly to 30 seconds when you install Windows Host Utilities 6.0 or later after installing DSM 4.1. You need to reset this value to 60 seconds.

You can reset the persistent reservation timeout value by repairing the DSM installation using the Windows repair option, or by editing the persistent reservation timeout parameter on the **Data ONTAP DSM** tab of the **Data ONTAP DSM Properties** window.

Note: You should not change the timeout value from 60 seconds unless directed to do so by your storage system support representative.

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 worldwide 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.

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 10

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 Interoperability Matrix.
- Verify that you have the 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 clustered Data ONTAP, 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 *SAN Administration Guide* (formerly the *Block Access Management Guide for iSCSI and FC*) for your version of Data ONTAP.
- Search Bugs Online for recently discovered problems. In the Bug Types field under Advanced Search, select ISCSI - Windows, and then click Go! Repeat the search for Bug Type FCP - Windows.
- 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 NetApp technical support.

Related information

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/
Documentation on the NetApp Support Site: support.netapp.com

Bugs Online - http://support.netapp.com/NOW/cgi-bin/bol
Contacting NetApp Global Services - http://www.netapp.com/us/support/ngs-contacts.html

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

You should install fcinfo before you have a problem so that it is already available if needed. Technical support will tell you what commands to run if support personnel need the information that 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

Fibre Channel Information Tool (fcinfo) - www.microsoft.com/downloads/en/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

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 Interoperability Matrix.

About this task

To see if you have the latest driver, complete the following steps.

Steps

1. Open the Computer Management window.

For	Click
Windows Server 2012 and Windows Server 2012 R2	**Server Manager** > **Dashboard** > **Tools** > **Computer Management**
Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Vista	**My Computer** on your desktop, then right-click and select **Manage**

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 **Storage controllers** and double-click the appropriate HBA.

   The **Properties** dialog box for the HBA 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 website.

Related information

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

Emulex support page for NetApp - www.emulex.com/downloads/netapp.html

QLogic support page for NetApp - http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/OEM_Product_List.aspx?oemid=372

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 OneCommand Manager.

   OneCommand Manager is the successor to HBAnyware.

2. In OneCommand Manager, select the appropriate HBA from the list and click the **Driver Parameters** tab.

3. Select the **LogErrors** parameter and change its 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 QConvergeConsole.

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 NetApp 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 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

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 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

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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 running Data ONTAP operating in 7-Mode, execute the following command:

   `fcp show adapter -v`

   On the console of a storage controller running clustered Data ONTAP, execute 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 Data ONTAP operating in 7-Mode, execute the following command:

   `fcp show initiator -v`

   On the console of a storage controller running clustered Data ONTAP, execute 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

NetApp Interoperability Matrix - http://support.netapp.com/NOW/products/interoperability/

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

Download and install the `nSANity Diagnostic and Configuration Data Collector` program when instructed to do so by your technical support representative.

About this task

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.

Steps

1. Log in to the NetApp Support Site and search for "nSANity".
2. Follow the instructions to download the Windows zip or Linux tgz version of the nSANity program, depending on the workstation or server you want to run it on.
3. Change to the directory to which you downloaded the zip or tgz file.
4. 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 tasks

Collecting diagnostic data using nSANity on page 120

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

Download 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

Installing the nSANity data collection program on page 119

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.

How DSM event log entries relate to MPIO driver event log entries

The Microsoft MPIO driver and the DSM typically write concurrent entries in the Windows event log. For key events like takeover and giveback, it's helpful to know how these entries correspond. A significant lag by either the DSM or the MPIO driver in writing a corresponding entry, or the failure to write a corresponding entry, usually indicates some kind of problem.

Consider the event log entries you will see during takeover.

Event	DSM event log entry ID	MPIO event log entry ID
Takeover	• 61110 • 61142 • 61077 • 61078 • 61054	• 16 • 17

Each of these entries signifies path failure, of exactly the kind you would expect in a failover scenario.

Note: The DSM writes these entries only if the path in question was processing I/O.

Now consider the event log entries you will see during giveback.

Event	DSM event log entry ID	MPIO event log entry ID
Giveback	• 61143	• 2

Here the event log entries indicate successful path processing. As long as the MPIO driver writes a 2 for each path, you can be confident that giveback was successful.

Related references

Event message reference on page 123

Changing what gets logged by the DSM

The event log level determines the number of messages the DSM writes to Windows event logs. Changing the event log level affects only messages written by the DSM itself. It does not affect messages written by other Windows MPIO components.

Steps

1. In the DSM GUI window, choose **Action** > **Properties**.

   The Data ONTAP DSM Properties window is displayed.

2. In the **Data ONTAP DSM Properties** window, click the **Data ONTAP DSM** tab.

3. In the Event Log Level group, click the radio button for the desired level. Click **Reset to Default** to restore the default value.

Option	Description
None	The DSM logs no messages to Windows event logs.
Normal	The DSM logs the normal level of messages to Windows event logs.
Info	In addition to the normal level of messages, the DSM logs messages for path transitions and reservation changes to Windows event logs.
Debug	The DSM logs all messages to Windows event logs. Recommended for debugging only.

   Note: The Info and Debug levels may impair system performance.

   The new event log level is effective immediately. No reboot is necessary.

Related tasks

Modifying values for DSM parameters on page 98

Related references

Event message reference on page 123

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

Related references

Event message reference on page 123

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 was 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 (HBAs).
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 succeeded.
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 the LUN 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 were 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 clustered Data ONTAP or Data ONTAP operating in 7-Mode and for iSCSI paths to LUNs for clustered Data ONTAP. 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 concepts

How DSM event log entries relate to MPIO driver event log entries on page 121

Related tasks

Changing what gets logged by the DSM on page 82

Related references

Event data section encoding on page 122

Copyright information

Copyright © 1994–2014 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (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. 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

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, 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, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, 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.

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 *www.ibm.com/legal/copytrade.shtml*.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

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.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

administrator account option *14*
alignment
    VHD partition *51*
ALUA
    enabling for FC paths *42*, *59*
    requirements *10*
    support overview *10*
    troubleshooting configurations *113*
application
    configuring to start after iSCSI *108*
asymmetric logical unit access (ALUA)
    See ALUA
auto assigned failover example *25*
Auto Assigned load balance policy *13*

B

block alignment
    VHD partition *51*
boot loader
    reinstalling for Linux after running mbralign *52*
BootBIOS
    displaying FC WWPN *102*

C

CHAP
    security options for iSCSI *40*
clear-sanstats cmdlet *97*
CLI *86*
    See also PowerShell cmdlets
cluster
    mapping LUNs *105*
cluster service, stopping before installing *32*, *55*
clustering
    with Hyper-V *29*
cmdlets *86*
command line installation *46*
configurations
    supported *10*

D

Data ONTAP
    licenses required *36*
    supported versions *31*, *54*
default load balance policy
    changing using DSM GUI *78*
    changing using PowerShell cmdlet *92*
    viewing in PowerShell *89*
disabled paths *23*
discovering
    new LUNs *68*
disk
    initializing and partitioning *108*
disk serial number *27*
disks
    discovering new *68*
driver
    verifying HBA version *115*
DSM
    concepts *8*
    installing interactively *44*
    installing silently *44*, *46*
    Microsoft iSCSI *12*
    settings summary *16*
    starting management GUI *68*
    supported Windows configurations *10*
    uninstalling interactively *65*
    uninstalling silently *66*
    upgrading interactively *60*
    upgrading silently *62*
    See also GUI
DSM ID *27*
DSM license key *42*, *85*
dynamic disk support *27*

E

Emulex BootBIOS
    displaying FC WWPN *102*
Emulex HBA
    configuring *36*
    enabling logging *116*
    verifying driver version *115*
error recovery level
    for iSCSI *40*

event log *121–123*
event logging, changing *82*, *122*

F

failover behavior *22*, *23*, *25*
failover cluster
    adding Hyper-V VM *48*
    special DSM installation steps *60*
failover concepts *13*
failover example *23–25*
failover only failover example *25*
FailOver Only load balance policy *13*
failover problems *113*, *119*
FC zoning
    troubleshooting *114*
fcinfo
    troubleshooting tool for Windows Server 2003 *115*
fcinfo.exe
    using to obtain WWPN *101*
Fibre Channel
    configuring HBAs *36*
    configuring switch *36*
    enabling ALUA *42*, *59*
    mixing FC and iSCSI paths *12*
    prioritizing over iSCSI *97*
    recording WWPN *100*
    SAN booting *109*
    storage system port media type *37*
    targets *105*
    troubleshooting tool for Windows Server 2003 *115*
Fibre Channel Information Tool (fcinfo) *115*
Fibre Channel over Ethernet *119*

G

get-ontapdsmparams cmdlet *89*
get-sandisk cmdlet *90*
get-sanpath cmdlet *93*
get-sanstats cmdlet *96*
GRUB
    reinstalling for Linux after running mbralign *52*
GUI
    changing the default load balance policy *78*
    changing the load balance policy *77*
    detailed events report entries *71*
    displaying detailed events report *71*
    displaying persistent reservation key *81*
    editing GUI settings *84*
    editing properties *81*, *83*
    enabling a path *79*
    history view entries *76*
    making a path Active *79*
    refreshing the display *84*
    setting path weight *80*
    specifying a path Preferred *80*
    starting *68*
    viewing detailed events report *70*
    viewing LUNs (virtual disks) *69*
    viewing paths *72–75*
    viewing virtual disk information *72*

H

HBA
    configuring *36*
    configuring for SAN booting *109*
    configuring iSCSI *38*
    enabling logging on Emulex *116*
    enabling logging on QLogic *116*
    parameters *15*
    recording FC WWPN *100*
    verifying driver version *115*
HBAnyware
    enabling logging on Emulex HBA *116*
hotfixes
    installing *33*, *56*
    list of *33*, *56*
Hyper-V
    adding VM to failover cluster *48*
    align partitions for best performance *51*
    clustering *29*
    configuring Linux guest OS *49*, *50*
    configuring virtual machines *48*
    Guest Utilities *28*
    LUN layout *29*
    overview *28*
    storage options *28*

I

I_T nexus *27*
I_T_L nexus *27*
I/O, stopping before installing *32*, *55*
igroup
    mapping LUN *104*
    overview *104*
initializing a disk *108*
initiator
    downloading iSCSI *39*

installing iSCSI *40*
iSCSI configuring *38*
iSCSI options *38*
initiator group
mapping LUN *104*
overview *104*
initiator node names
recording iSCSI *102*
initiator-target (I_T) nexus *12*
initiator-target-LUN (I_T_L) nexus *12*
initiators
recording the node name, iSCSI *102*
InquiryRetryCount registry setting *18*
InquiryTimeout registry setting *18*
installation
overview *9*
repair options *67*
requirements *31*, *54*
special steps for Windows clusters *60*
troubleshooting *111*
InstallDir registry setting *18*
installing
DSM interactively *44*
DSM silently (unattended) *46*
iSCSI software initiator *40*
interactive upgrade *60*
IPSecConfigTimeout setting *18*
IQN
recording iSCSI *102*
iSCSI
adding target *106*
authentication using RADIUS *41*
CHAP security options *40*
configuring HBA *38*
configuring initiator *38*
dependent services *108*
downloading initiator *39*
error recovery level *40*
installing software initiator *40*
iscsicli command *106*
mixing iSCSI and FC paths *12*
multiple connections per session *40*
node name overview *100*
recording the initiator node name *102*
SAN booting *109*
iSCSI initiator
options *38*
iSCSILeastPreferred *97*

L

language versions of Windows supported *30*
least queue depth failover example *23*
Least Queue Depth load balance policy *13*
Least Weighted Paths load balance policy *13*
license key
obtaining *42*
viewing *85*
licenses, required for Data ONTAP *36*
LinkDownTime setting *19*
LinkDownTimeOut HBA parameter *15*
LinkTimeOut HBA parameter *15*
Linux
configuring Hyper-V guest OS *49*, *50*
reinstalling GRUB after running mbralign *52*
Linux Integration Components *49*, *50*
linux_gos_timeout-install.sh *49*, *50*
LinuxGuestConfig.iso *49*, *50*
load balance policy
changing for a LUN using DSM GUI *77*
changing for a single LUN using PowerShell *91*
changing the default using DSM GUI *78*
changing the default using PowerShell *92*
log messages *121*–*123*
LogDir registry setting *19*
logging, changing *82*, *122*
LUN
changing load balance policy using DSM GUI *77*
changing load balance policy using PowerShell *91*
creating *103*
creating SAN boot LUN *109*
layout with Hyper-V *29*
mapping for Windows cluster *105*
mapping to igroup *104*
overview *103*
removing FC or iSCSI paths *58*
viewing in DSM GUI *69*
viewing in PowerShell *90*
LUNs
discovering new *68*
mixing FC and ISCSI paths *12*

M

ManageDisksOnSystemBuses setting *19*
MaxRequestHoldTime setting *19*
MCS
enabling for iSCSI *40*
media type

storage system FC port *37*
Microsoft DSM (msdsm) *8*
Microsoft fcinfo.exe
using to obtain WWPN *101*
Microsoft iSCSI DSM *12*
Microsoft iSCSI DSM (msiscdsm) *8*
Microsoft iSCSI initiator
downloading *39*
misalignment
VHD partition *51*
MPIO components
installed by DSM installer *8*
MPIO concepts *13*
MPIO tunable parameters *83*
MPIOSupportedDeviceList setting *20*
MSCS
special DSM installation steps *60*
MSCS, stopping cluster service *32*, *55*
msiexec command *46*
multiple connections per session
enabling for iSCSI *40*

N

NodeTimeOut HBA parameter *15*
non-English versions of Windows supported *30*
non-optimized path
overview *105*
verifying not used *105*
nSANity
installing *119*
running *120*
NTFS disk format *108*

O

obtaining *42*
optimized path *22*

P

parameters, MPIO tunable *83*
partitioning a disk *108*
pass-through disk *28*
path
changing status using PowerShell *94*
changing weight in PowerShell *95*
enabling with DSM GUI *79*
making Active with DSM GUI *79*
removing FC or iSCSI to 7-Mode *58*
setting weight with DSM GUI *80*
specifying Preferred with DSM GUI *80*
supported path changes using PowerShell *95*
verifying correct FC path used *105*
viewing in DSM GUI *72*–*75*
viewing in PowerShell *93*
path identifier *27*
path limits *14*
path states
changing administrative state *79*
changing operational state *79*
path status
changing *94*
path types *72*
PathVerifyEnabled setting *20*
PDORemovePeriod setting *20*
performance
align VHD partitions *51*
persistent reservation key *69*, *81*
persistent reservation parameters *81*
PersistentReservationKey registry setting *20*
PID (product identifier) *8*
PortDownRetryCount HBA parameter *15*
PowerShell cmdlets
clear-sanstats cmdlet *97*
get-ontapdsmparams cmdlet *89*
get-sandisk cmdlet *90*
get-sanpath cmdlet *93*
get-sanstats cmdlet *96*
getting help *89*
loading *88*
overview *86*
requirements *87*
running remotely *88*
set-ontapdsmparams cmdlet *92*, *98*
set-sandisk cmdlet *91*
set-sanpath cmdlet *94*, *95*
PowerShell installation *43*, *59*
ProductVersion registry setting *20*
Protocols registry setting *20*
proxy path *22*

Q

QConvergeConsole
enabling logging on QLogic HBA *116*
QLogic BootBIOS
displaying FC WWPN *102*
QLogic HBA
configuring *36*

enabling logging *116*
verifying driver version *115*
quiet installation option *46*

R

RADIUS
for iSCSI authentication *41*
raw disk *28*
refreshing the display *84*
registry
values summary *16*
registry settings *15*
registry settings, repairing *67*
repairing the DSM installation *67*
requirements *31*, *54*
ReservationRetryInterval registry setting *21*
ReservationTimeout registry setting *21*
RetryCount setting *21*
RetryInterval setting *21*
round robin failover example *24*
Round Robin load balance policy *13*
round robin with subset failover example *24*
Round Robin with Subset load balance policy *13*

S

SAN booting
configuring *109*
overview *29*
scripted installation *46*
security
CHAP for iSCSI *40*
RADIUS for iSCSI *41*
set-ontapdsmparams cmdlet *92*, *97*, *98*
set-sandisk cmdlet *91*
set-sanpath cmdlet
changing path status *94*
changing path weight *95*
supported path changes *95*
settings
IPSecConfigTimeout *18*
LinkDownTime *19*
ManageDisksOnSystemBuses *19*
MaxRequestHoldTime *19*
MPIOSupportedDeviceList *20*
PathVerifyEnabled *20*
PDORemovePeriod *20*
RetryCount *21*
RetryInterval *21*
TimeOutValue *22*
UseCustomPathRecoveryInterval *20*, *22*
silent installation *46*
silent upgrade *62*
SnapDrive for Windows
creating LUNs *103*
software boot
iSCSI initiator requirement *39*
statistics
clearing *97*
displaying *96*
Storage Explorer
using to obtain WWPN *101*
storage system
protocol licenses *36*
supported configurations *31*, *54*
SupportedDeviceList registry setting *21*
SUSE Linux
reinstalling GRUB after running mbralign *52*
switch
configuring Fibre Channel *36*
sysstat command
verifying paths *105*

T

target
adding iSCSI *106*
Fibre Channel *105*
TestUnitReadyRetryCount registry setting *21*
TestUnitReadyTimeout registry setting *21*
timeout and tuning parameters *15*
TimeOutValue setting *22*
troubleshooting
ALUA configurations *113*
enabling logging on Emulex HBA *116*
enabling logging on QLogic HBA *116*
failover problems *113*
fcinfo tool *115*
FCoE failover problems *119*
HBA driver version *115*
installation *111*
items to check *114*
missing hotfixes *111*

U

unattended installation *46*
uninstalling the DSM interactively *65*
uninstalling the DSM silently *66*

upgrading the DSM
interactively *60*
overview *59*
silently *62*
UseCustomPathRecoveryInterval *20*, *22*

V

Veritas Storage Foundation
dynamic disk support *27*
logging on to iSCSI targets *106*
VID (vendor identifier) *8*
viewing *85*
virtual disk information
viewing in DSM GUI *72*
virtual disks
discovering new *68*
viewing in DSM GUI *69*
virtual hard disk (VHD)
align partitions for best performance *51*
for Hyper-V *28*

W

Windows
dynamic disk support *27*
installing on SAN boot LUN *109*
support for non-English language versions *30*
supported configurations *10*
Windows cluster
mapping LUNs *105*
Windows clusters
upgrading DSM for *60*
Windows event log *121*–*123*
Windows failover cluster
adding Hyper-V VM *48*
Windows hotfixes
installing *33*, *56*
list of *33*, *56*
Windows MPIO components
installed by DSM installer *8*
Windows registry
values summary *16*
Windows registry settings *15*
Windows registry, repairing *67*
Windows Storage Explorer
using to obtain WWPN *101*
WWPN
displaying using Emulex BootBIOS *102*
displaying using QLogic BootBIOS *102*
obtaining using Microsoft fcinfo.exe *101*
obtaining using Windows Storage Explorer *101*
overview *100*
recording from host *100*

Z

zoning
troubleshooting *114*