



Dell EqualLogic Host Integration Tools for Microsoft

Installation and User's Guide

Version 4.7

© Copyright 2004-2014 Dell Inc. All rights reserved.

Dell™ and EqualLogic® are registered trademarks of Dell Inc.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Information in this document is subject to change without notice.

Reproduction in any manner whatsoever without the written permission of Dell is strictly forbidden.

Published: April 2014

Part Number: 110-6183-EN-R2

Table of Contents

Preface	v
1 Introduction to Host Integration Tools	1
Host Integration Tools Components	1
SMP Support	2
SMP Configuration	3
SCVMM Support	3
Configure VMM	3
Supported VMM Operations	4
Supported Applications	4
Microsoft Exchange Server	4
Microsoft SQL Server	5
Microsoft Hyper-V	6
Microsoft SharePoint	6
2 Installation	7
Obtain the Installation Kit	7
Administrative Installation Using Active Directory	7
Installation Considerations	8
Install HIT	9
Update an Installation	9
Uninstall HIT or a Component	10
Install HIT on a Windows Server 2008 Core Machine	10
Install HIT on a Windows Server 2008 Core Cluster	10
Install HIT in Each VM in a Windows Server 2008 R2 CSV Configuration	11
About Remote Host Installations	11
Install HIT on Remote Hosts Using the Add Hosts Wizard	11
Install HIT on Remote Hosts Using PowerShell Scripts	14
Install HIT on a Microsoft Failover Cluster	17
Specify the ASM/ME Backup Document Directory	18
Change the Logon Account for ASM/ME Services (EQLReqService and EqlASMAgent)	18
Joining a Computer into a Windows Failover Cluster	18
Silent Installations	19
Support for Silent Installation	19
Using HIT with a SharePoint Farm	21
Specify Index File Locations When Installing SharePoint	22
Modify Index File Locations in an Existing SharePoint Farm	23
Best Practices for SharePoint	25
3 Remote Setup Wizard	27
PS Series Group Requirements for Using RSW	27
Windows System Requirements for Using RSW	27
Launch RSW on the Host	28
Launch RSW from ASM/ME	28
Initialize a PS Series Array Using RSW	28
Search for a PS Series Array Using RSW	28
Information Required for Initializing a PS Series Array	29
Initialize an Array and Create a PS Series Group	31
Initialize an Array and Add It to an Existing Group	32
Troubleshoot RSW	32
4 Remote Setup Command Line Utility	33
General Command Syntax for the RSWCLI	33
Getting Help on Commands	33
Using RSWCLI Commands	34
Discover a PS Series Array	34
Initialize a PS Series Array	35
List or Modify MPIO Settings	37

List Included and Excluded Subnets for MPIO	38
Include a Subnet or Adapter for Use by MPIO	39
Exclude a Subnet or Adapter from Use By MPIO	41
5 Using the Multipath I/O Component	43
Introduction to Multipath I/O DSM	43
Prerequisites for Configuring Multipath I/O DSM	46
Requirements for Multipath I/O	46
Configure Multipath I/O Between a Computer and a Group	47
Log In to a Volume with Multipath I/O	48
Log Off a Volume with Multipath I/O	48
View MPIO Sessions	49
Set the MPIO Load Balancing Policy	51
6 Use the VDS Provider	53
VDS Provider Requirements	53
VDS Provider Guidelines and Restrictions	53
Simple Target and LUN Naming	54
Import VSS Snapshots	54
Modify	55
About Creating a Volume Using Storage Manager for SANs	55
Start Storage Manager for SANs	56
7 Use VMM with the Dell EqualLogic SMP	57
Install the Dell EqualLogic Storage Management Provider	57
Configure the Dell EqualLogic Storage Management Provider	57
Create a Classification for Dell EqualLogic Storage Resources	58
Import the SMP through the VMM GUI	58
Configure PS Series Groups	61
Configure Group Access on Managed Hosts and Clusters	61
Configure Storage for VM Rapid Provisioning	63
Create a VM Template for the Library Share	64
Create a VM Template from a VHD	66
Migrate the Rapid-Provisioned VMs	69
Migrate Storage of a Deployed VM to Another Location	70
Troubleshoot SCVMM Issues	71
Supported SMP PowerShell Cmdlets	73
8 Use the HPC iSCSI Provider	75
About the Dell EqualLogic HPC iSCSI Provider Installation	75
Configure the PS Series Array	75
HPC iSCSI Provider Settings	75
9 Tools and Utilities	77
EqIXcp Utility	77
EqIXcp Utility Restrictions	77
Run the EqIXcp Utility	78
EqLog Utility	78
Overview of the EqLog Utility	78
Run the EqLog Utility	79
EqLog Command Line Options	79
Trace Log Daemon	80
EqRethin Utility	81
Run the EqRethin Utility	81
Index	83

Preface

Dell™ EqualLogic® Host Integration Tools give you the ability to manage and configure PS Series storage arrays from the servers that use them. From initializing new arrays to creating application-consistent snapshots, to scripting management operations, the Host Integration Tools expose a wide variety of capabilities to server administrators.

Audience

The information in this guide is intended for administrators using Host Integration Tools to manage snapshots, replicas, and clones through Smart Copies, using the ASM/ME interface.

Related Documentation

For detailed information about FS Series appliances, PS Series arrays, groups, volumes, array software, and host software, log in to the [Documentation page](#) at the customer support site.

Dell Online Services

You can learn about Dell products and services using this procedure:

1. Visit www.dell.com or the URL specified in any Dell product information.
2. Use the locale menu or click on the link that specifies your country or region.

Dell EqualLogic Storage Solutions

To learn more about Dell EqualLogic products and new releases being planned, visit [Dell EqualLogic TechCenter](#). Here you can also see articles, demos, online discussions, and more details about the benefits of our product family.

Technical Support and Customer Service

Dell support service is available to answer your questions about PS Series SAN arrays and FS Series appliances.

Contacting Dell

If you are a customer in the United States or Canada in need of technical support, call 1-800-945-3355. If you are outside of the United States or Canada, visit [Dell EqualLogic Product Support](#).

If you have an Express Service Code, have it ready. The code helps the Dell automated support telephone system direct your call more efficiently.

1 Introduction to Host Integration Tools

The Dell EqualLogic Host Integration Tools (HIT) simplify the configuration and administration of Dell EqualLogic PS Series storage arrays on Microsoft® Windows® computers.

Host Integration Tools Components

[Table 1](#) lists the Host Integration Tools application components and [Table 2](#) lists the service components.

Table 1: Host Integration Tools Application Components

Component	Description
Remote Setup Wizard	Enables you to initialize a PS Series array and set up or expand a PS Series group. See Remote Setup Wizard on page 27 .
Remote Setup Wizard Command Line Utility (RSWCLI)	Provides an alternative to using the Remote Setup Wizard, with setup commands that you can execute at the Windows command prompt instead of using the GUI. The RSWCLI is described in Remote Setup Command Line Utility on page 33 .
Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition (ASM/ME)	Enables you to create and manage Smart Copies (snapshots, clones, and replicas). An alternate command-line interface facilitates custom operations and scripting. See the <i>Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide</i> .
PowerShell® Tools	Enables you to manage one or many PS Series groups through a comprehensive set of PowerShell cmdlets.
Dell EqualLogic Storage Management Provider (SMP)	Enables you to manage Dell EqualLogic storage directly through native Windows storage interfaces such as PowerShell cmdlets, File Services UI in the Windows Server® 2012 Server Manager console, or the standard Windows Management Instrumentation API. See SMP Support on page 2 .

Table 2: Host Integration Tools Service Components

Component	Description
Dell EqualLogic VSS Provider	Supports VSS management of application-consistent Smart Copies.
Dell EqualLogic VDS Provider	Enables you to use Microsoft VDS and Microsoft Storage Manager for SANs to create and manage volumes in a PS Series group. See Use the VDS Provider on page 53 .
Dell EqualLogic Multipath I/O DSM (MPIO DSM)	Supports multipathing. This driver module works with the Microsoft MPIO driver. This feature dynamically balances your iSCSI SAN traffic load over multiple network paths between the computer and the PS Series group. You need multiple iSCSI host bus adapters to use this feature. Configure Dell EqualLogic Multipath I/O DSM using the ASM/ME GUI, as described in the <i>Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide</i>, or you can use the RSWCLI, described in Remote Setup Command Line Utility on page 33.
Dell EqualLogic HPC iSCSI Provider	Allows the Microsoft High Performance Computing (HPC) Service to provision volumes and deploy compute nodes on Dell EqualLogic SANs. This service is available only on systems running Windows HPC Server 2008 R2 or later. See http://www.microsoft.com/hpc for more information.
Microsoft iSCSI Initiator	Enables connections to iSCSI targets. Required by Remote Setup Wizard, ASM/ME, and the VDS provider. For information about using the initiator, see the Microsoft documentation. See Installation Considerations on page 8 .
iSCSI Initiator properties tab	Provides information about the status and history of the multipath connections supported by the Multipath I/O DSM.

SMP Support

HIT/Microsoft includes a Storage Management Provider (SMP) for Windows 8 or greater and Windows Server 2012 or greater operating systems. This framework is preferred for enabling support for Windows-based storage management.

The Dell EqualLogic SMP allows you to manage Dell EqualLogic storage directly through native Windows storage interfaces such as storage PowerShell cmdlets (Storage Module), the File Services UI in the Windows 2012 Server Manager console, or the standard Windows Management Instrumentation API.

The SMP infrastructure is native to Windows 8 or greater and Windows Server 2012 or greater systems.

The Dell EqualLogic SMP is an optional component installed in default configuration by the HIT/Microsoft installer. The provider is hosted by the Dell EqualLogic SMP Host Service (EqLSMPHost).

SMP Configuration

The Dell EqualLogic SMP implementation requires Dell EqualLogic PS Series group access to be configured. After installing, you must configure group access using the Dell EqualLogic PowerShell Tools (`New-EqlGroupAccess` cmdlet) or ASM. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

For a list of features not supported in the Dell EqualLogic SMP, see the *Host Integration Tools for Microsoft Release Notes*.

SCVMM Support

HIT/Microsoft includes support for the System Center Virtual Machine Management (SCVMM, or VMM) interface 2012 SP1.

You must install the Host Integration Tools to enable support for VMM with Dell EqualLogic storage. PS Series groups configured on the host are available for managing storage within VMM. All the configured PS Series groups have one provider. VMM refers to the PS Series groups as storage arrays (or storage devices), and to the pools within the PS Series groups as managed storage pools. In the VMM GUI, you can create new volumes (referred to as Logical Units in VMM).

VMM uses the Dell EqualLogic Storage Management Provider (SMP) to communicate with the PS Series groups. The Dell EqualLogic SMP allows you to manage Dell EqualLogic storage directly through native Windows storage interfaces such as storage PowerShell cmdlets (Storage Module), the File Services UI in the Windows Server 2012 or greater Server Manager console, or the standard Windows Management Instrumentation API.

Configure VMM

1. Install the Host Integration Tools.
2. Open a PowerShell window and enter the following cmdlets, using the name and IP address of the PS Series group to which you want to establish a connection. You must enter an administrator account name and password:

```
New-EqlGroupAccess -GroupName name -GroupWKAddress ip_address -UserName  
Administrator -Password "AcctPassword"
```

```
Connect-EqlGroup
```

3. Verify that the connection to the group was established successfully by entering the following two commands and checking the output:

```
Get-EqlGroupAccess
```

```
Get-EqlGroup
```

4. If the connection to the group was established successfully, restart the EqlSMPhost service.

5. Import the storage provider module using the following command:

```
Import-SCStorageProvider
```

6. Do either of the following to update VMM with the group information:

- Enter the cmdlet: `Update-StorageProviderCache`.
- In the VMM GUI, click Rescan.

If successful, the Dell EqualLogic Storage Management Provider is displayed in the list of Storage Providers.

Supported VMM Operations

After VMM is configured, you can use the VMM interface to perform the following operations:

- Create a volume (Logical Unit), with the following properties:
 - Name, size, storage pool (if the group has multiple pools), thin-provisioning enabled or not
- Delete a volume
- Clone a volume
- Increase the size of a volume
- Provision virtual machines to hosts or clusters
- Mount volumes on hosts or clusters
- Create snapshots of volumes
- Migrate VMs from hosts to clusters
- Migrate VMs from clusters to hosts

Supported Applications

Through the Auto-Snapshot Manager/Microsoft Edition component, the Host Integration Tools support backup and restore operations for the following applications.

Microsoft Exchange Server

Auto-Snapshot Manager/Microsoft Edition supports online backup and quick restore of Microsoft® Exchange Server® components by using the ASM/ME GUI.

Supported features for Microsoft Exchange Server include:

- Creating snapshot, replica, and clone Smart Copies of Microsoft Exchange Server Mailbox Databases (for Exchange 2010 and 2013) residing on PS Series volumes
- Automatic discovery of the Microsoft Exchange Server instance and its components
- Consistent, online backup and quick restore of Microsoft Exchange Mailbox Databases (for Exchange 2010 and 2013) residing on PS Series volumes

The following types of Microsoft Exchange Server application behaviors are supported for Smart Copies:

- Copy backup type (on all supported Microsoft Exchange Server versions)
- Scheduling Smart Copy creation for Microsoft Exchange Mailbox Databases for Exchange 2010 and 2013
- Recovery Mailbox Database creation for Microsoft Exchange 2010 and 2013 brick-level restores
- The Clone and Restore as New option is available for Smart Copies of all supported Microsoft Exchange Server versions. The Clone and Restore as New feature allows you to clone a Mailbox Database from a source Exchange server, and then set it up as a new Mailbox Database on a target Exchange server.
- The option to perform Checksum Verification (database and transaction log) and optional Soft Recovery immediately after Smart Copy creation. You can also use this feature by setting up a global verification task on the Exchange Server host or a remote host.

See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Microsoft SQL Server

Auto-Snapshot Manager/Microsoft Editions supports online backup and quick restore of Microsoft® SQL Server® databases using the ASM/ME GUI.

Supported features for Microsoft SQL Server include:

- Support for creating snapshots, replicas, or clones of Microsoft SQL Server databases residing on PS Series volumes
- Automatic discovery of Microsoft SQL Server instance and all SQL databases
- Consistent, online backups and quick restores of Microsoft SQL Server databases residing on PS Series volumes

Microsoft SQL Server application supports both full and copy backup type Smart Copies on Microsoft SQL Server 2008 and 2012.

The following Microsoft SQL Server database restore operations are supported:

- Restore All—Restores databases to the point-in-time represented by a Smart Copy. Optionally, you can apply transaction log backups to a database being restored.

- Restore individual databases—Selectively restores one or more databases sharing the same volume (uses an automated file copy operation after the Smart Copy is imported, if volume sharing is detected).
- Restore As New—Restores all databases as new databases with new mount points.
- Clone and Restore as New—Recovers a database from a cloned replica Smart Copy on the secondary group. Optionally, you can mount a read-only copy of the replica Smart Copy for backup to tape or for data mining (volume replication stops while replica is mounted).

See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Microsoft Hyper-V

Microsoft® Hyper-V® enables you to run a client virtual machine (also called a guest O/S) in child partitions. ASM/ME enables you create application-consistent and crash-consistent Smart Copies of virtual machines, dependent on Guest O/S type. You can also:

- Define collections of virtual machines
- Set up schedules for creating Smart Copies of virtual machines, cluster shared volumes, or collections of virtual machines or cluster shared volumes
- Restore Smart Copies of virtual machines
- Restore virtual hard drive (VHD) volumes

See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Microsoft SharePoint

Microsoft® SharePoint® enables users to create blogs, wikis, and other web pages that enable people to share information and manage documents from a single management view.

SharePoint introduces the concept of a farm, which is a collection of hosts logically connected by the SharePoint application. SharePoint has a VSS writer on one or more hosts.

ASM/ME enables you create Smart Copies of complete farms, farm components, search indices, or Search Service Applications (SSAs).

You can also restore a complete farm, a set of content databases, an individual database, or an SSA.

See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

2 Installation

There are two methods that you can use to install the Host Integration Tools for Microsoft on a host: manual installation and remote host installation. For first-time installations, you must perform a manual installation. After that, you can easily install the Host Integration Tools on any number of hosts using the remote installation process from the ASM/ME GUI.

Obtain the Installation Kit

Obtain the installation kit using either of the following methods:

- Find the Host Integration Tools distribution CD-ROM that shipped with your PS Series array. The CD-ROM uses autorun to start automatically (if your computer is configured to allow autorun).
- Download the installation kit. This requires a Dell EqualLogic customer user account, which you can set up at the following URL: <https://support.dell.com/equallogic>

When you have set up the support account, obtain the kit as follows:

1. Log in to your account and click the Customer Service Home tab.
2. Click Downloads in the navigation bar and select Host Integration Toolkit.
3. Click the latest revision of the toolkit to display the web page for that revision.
4. Under Current Software, click Host Integration Tools version.
5. Click Accept to accept the terms and conditions of the download.
6. Save the executable installation image to a temporary location on your local computer.

Before you begin any installation procedures:

- Check the Dell Technical Support Web site to make sure you have the latest Host Integration Tools version and documentation.
- Read the current revision of the *Host Integration Tools for Microsoft Release Notes* for the most recent information about:
 - Supported and required software and firmware releases
 - Supported operating system versions
 - The latest information about Host Integration Tools known issues and usage constraints

Administrative Installation Using Active Directory

Windows supports administrative installation of programs using Active Directory. Administrative installs might require the use of an .MSI file. To support administrative installations, the .MSI versions of the Host Integration Tools installation are available on the download page. Unless you are performing an

administrative install through Active Directory, you should use the .EXE versions of the installers.

Note: Using the .MSI file results in an incomplete installation; that is, not all of the required third-party products needed by HIT/Microsoft are installed when you use the .MSI file. You have to install the following required third-party products after installing the .MSI file:

- Install the Microsoft C++ Redistributable—The installers are included in Microsoft Visual Studio 2012 Update 4. The Update 4 version used by ASM is 11.0.61030.0.
 - Install the x86 version on all 32-bit systems.
 - Install the x64 version on 64-bit systems.

These products show up in Add/Remove Programs with the version listed if they are installed. You might need to reboot your system after installing the Redistributable.

- Install the Microsoft Native MPIO—You should install the version that is built into the version of the Windows operating system you are using. It can be installed through the Add/Remove Features wizard. For instructions on how to install this feature, see <http://technet.microsoft.com/en-us/library/cc725907.aspx>.
- Install Microsoft .Net 4.0 manually.
- Deploy the MSI package via Group Policy (Computer Config).

Installation Considerations

Consider the following parameters before you begin an installation:

- Computer downtime

You do not need to reboot the computer unless you choose to install the MPIO DSM component or the volume rethinning driver.

- Installation options

Review the documentation (this manual and the *Host Integration Tools for Microsoft Release Notes*) to determine:

- Whether Host Integration Tools supports the installed applications and operating system versions
- Which Host Integration Tools components are applicable to your site

- Installation location

You can install the Host Integration Tools in the default location of C:\Program Files\EqualLogic, or in a different location.

The installation process automatically performs the following tasks so that the Host Integration Tools can run properly:

- Microsoft iSCSI Initiator service

The Microsoft iSCSI Initiator is integrated into Windows Server 2008 rather than provided as an installation package. The Host Integration Tools installation process automatically starts the iSCSI Initiator service.

- Windows Firewall and Dell EqualLogic MPIO

The Host Integration Tools installation process automatically configures the Windows firewall to allow ICMP echo requests (pings). This configuration enables MPIO to function properly.

- Microsoft MPIO service

The Host Integration Tools installation process automatically configures and starts the Microsoft MPIO service to enable MPIO to function properly.

Install HIT

If you install Host Integration Tools on a cluster, the installer prompts you to configure the installation for cluster operation. To install Host Integration Tools on a failover cluster, see [Install HIT on a Microsoft Failover Cluster on page 17](#).

On a single computer, you must log in to Windows as administrator or be a member of the administrators group to install and use the Host Integration Tools.

1. Obtain the installation kit. See [Obtain the Installation Kit on page 7](#).
2. Follow the prompts on the CD-ROM installation dialog or double-click the downloaded `Setup.exe` package to start the installation wizard. `Setup.exe` is for 32-bit operating systems, and `Setup64.exe` is for 64-bit operating systems.

The installer automatically performs the following operations:

- If you chose to install Dell EqualLogic MPIO, the Installer automatically configures the Windows MPIO service.
- The installer automatically adds necessary rules to configure the Windows firewall. These rules are needed in order for the Host Integration Tools to work properly.

Update an Installation

To update an installation after you have already installed the Host Integration Tools:

1. Double-click the downloaded `Setup.exe` file to start the installation wizard.
2. Select `Modify` and click `Next`.
3. Select the components you want to install and click `Next`.

4. Click `Install` to install the selected components.

You will see the following differences in an update installation procedure:

- The installer detects the previous version and notifies you that it will attempt to update the installed version to the latest version.
- You are prompted to deselect components (which removes those components) or select additional components for installation.
- If you select the Dell EqualLogic MPIO DSM component, you are prompted to restart the computer.

Uninstall HIT or a Component

To uninstall the Host Integration Tools, or to remove components after you have already installed the Host Integration Tools:

1. Open the Control Panel and select `Programs and Features`.
2. Select the Dell EqualLogic Host Integration Tools and click `Uninstall`.

Install HIT on a Windows Server 2008 Core Machine

If you are installing Host Integration Tools on a computer running Windows Server 2008 Core, review the requirements and support statements included in the *Host Integration Tools for Microsoft Release Notes*. Because Windows Server 2008 Core does not provide a GUI, you must begin the installation as follows:

1. Copy the installation package (such as `Setup64.exe`) to a location on the computer. Note the path to the file.
2. Connect to the computer running Windows Server 2008 Core and open the Windows command line terminal.
3. Type the following command and press enter:
`run<pathname>Setup64.exe`
4. The Host Installation Tools graphical installer launches. Follow the procedure described in [Install HIT on page 9](#). Only supported components are installed.

To uninstall Host Integration Tools from a computer running Windows Server 2008 Core, run the installation package a second time and select the option to remove the current installation.

Install HIT on a Windows Server 2008 Core Cluster

Because Windows Server 2008 Core does not provide a user interface, you can use a non-clustered Windows host with a regular GUI to help you easily and efficiently push parallel installations out to every cluster node.

1. Using the manual installation procedure described in [Install HIT on page 9](#), install the Host Integration Tools on a non-clustered Windows host with a regular user interface. This installation will allow you to use ASM/ME to perform parallel installations on all of the cluster nodes.
2. Open ASM/ME on the non-clustered host.
3. Use the remote installation procedure described in [Install HIT on Remote Hosts Using the Add Hosts Wizard on page 11](#) to push an installation out to each cluster node.

Install HIT in Each VM in a Windows Server 2008 R2 CSV Configuration

For Smart Copies of Virtual Machines to work correctly in a Windows Server 2008 R2 configuration using Cluster Shared Volumes (CSVs), the Host Integration Tools must be installed in each VM. This requirement applies to all such configurations, including Enterprise, Datacenter, Core, or any other Microsoft Server release configuration, but only for Windows Server 2008 R2. The requirement does not apply to CSVs with Windows Server 2012 or greater.

This requirement applies whether you start the Smart Copy operation or create a schedule from the VM or the Volume node in the ASM/ME GUI.

If the Host Integration Tools are not installed on each VM, you can create a Smart Copy but an error is displayed stating that ASM/ME could not open a connection to the VM. The Smart Copy will not be file system consistent, but will be crash consistent with respect to the file system in the VM. You might have to run the `ckdisk` utility the next time the VM restarts.

About Remote Host Installations

If you are managing a large number of hosts, you can easily install the Host Integration Tools on each host by using a PowerShell script or by using the Add Hosts wizard in ASM/ME. You no longer have to log in to each host separately, run the installer on each host, and continuously monitor and respond to prompts typical of an installation wizard.

This streamlined process improves performance and saves the amount of time typically required for large scale installations. Upgrading the version of Host Integration Tools on each host is also easily accomplished through these methods.

Install HIT on Remote Hosts Using the Add Hosts Wizard

After ASM/ME is installed on a host, you can perform new installations or upgrades on other hosts through that instance of ASM/ME. If multiple hosts are specified, the installations will be performed in parallel. After the installation on another host is complete, the host is added to the ASM/ME console as a new member of the HIT Group, and it can be viewed or managed from there. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information about HIT Groups.

If you have already created a HIT Group, ASM/ME will display a message if any of the hosts are not running a version of Host Integration Tools greater than or equal to the version running on the local host. You can then use the Add Hosts wizard to remotely upgrade the Host Integration Tools on the other hosts.

After the installation, if a remote system reboot is required, it can be initiated through the Add Hosts wizard. If any users are logged into the host that you are rebooting, a message will pop up on the remote host, notifying them of the impending reboot.

The prerequisites for remote host installation are as follows:

- In order for new installations to run successfully on remote hosts, ensure that you allow incoming ping requests through the remote host's firewall to the remote host. Use Windows Server Manager to create new inbound rules for your firewall. Select ICMPv4 or ICMPv6 protocol types for IPv4 and IPv6 pings, respectively. If both the local and remote hosts are in the same domain, allow the connections over the domain profile type.

If you prefer not to edit firewall rules, you can perform a manual installation on the host you are adding, and then use the Add Hosts wizard on the local host to add the host to the HIT Group.

- You will be prompted for username and password credentials in order to install Host Integration Tools on remote hosts added to the HIT Group. These credentials are never stored; they are only used for the installation. The following requirements must be met:
 - If you are installing on a cluster, you must provide the appropriate credentials (domain user with local administrator rights) across all cluster nodes.
 - If adding or installing on multiple hosts:

Single Domain—For multiple machines that belong to a single domain, you must provide the appropriate user credentials (domain users with local admin rights) so that ASM/ME can successfully access the machines to perform the required installations.

Single Workgroup—For multiple machines that belong to a single workgroup, each machine must have the same local admin account credentials.

Multiple Domains—For machines across multiple domains, add or install on all the machines from one domain at a time.

- The Remote Procedure Call (RPC) service must be running. This service should be started by default on Windows systems, but if it is not running or if the firewall is blocking it, the installation will not work.
- If you using the Browse Network option to add hosts to the HIT Group, ensure that browsing the network is working in Windows. If you cannot add hosts by browsing the network, add them manually by using the Manual Entry option in the Add Hosts wizard.
- Copy the `Setup.exe` and `Setup64.exe` installation files into a directory of your choice. Since you must specify this directory multiple times if you are adding several hosts for management or pushing out multiple installations, you can simplify the process by copying the installation files onto a network shared directory. (The default installation directory is `C:\Program Files\EqualLogic\bin`, so you can also place it there). ASM/ME will use these files to initiate the installation procedure on

remote hosts. These installation files are available on CD-ROM that shipped with your PS Series array, or from the installation kit available at <https://support.dell.com/equallogic>.

Install HIT on Remote Hosts with the Add Hosts Wizard

1. Click the `Add Hosts` button.
2. You can specify the list of hosts to add to your HIT Group in several ways. Select one or more of the following methods and click `Next`. To view online help for any of the wizard pages, press `F1` from that specific page.
 - **Discover through PS Series group**—When this option is selected, ASM/ME queries any PS Series groups that are connected to any current HIT Group members (including the local host), and displays all the hosts connected to those groups.
 - **Browse Network**—Select a host by browsing a network. You can only browse networks for which you have permissions.
 - **Manual Entry**—Enter an IP address or host name for each host you want to add to the HIT Group. You can also import a file that lists all the hosts that you want to add to the HIT Group. The file will be parsed and each host will be run through the manual entry process. This file can be generated automatically from the ASM/ME console by clicking `File`, then `Export Host List`. You can also create your own file for importing by saving a text file that contains a comma-separated list of host IP addresses, host names (fully qualified or not), or both. When you are back on this wizard page, click `Import` and then browse to the file.
 - **Cluster Nodes**—This option is visible only if ASM/ME detects that you are running a multiple node cluster in which one or more of the nodes have not yet been added to the HIT Group. All cluster nodes should be added to the HIT Group. If only a subset of nodes are added, cluster operations will fail.
3. Select one or more of the above options to identify which hosts to add. After you have selected which hosts to add, click `Next`. The HIT Installation and Host Verification page is displayed.
4. Enter the following information:

Enter the credentials (domain, username, and password) for the host you are adding. See the prerequisites for more information about these requirements.

- a. If you want to install MPIO or the PowerShell Tools on the host, select those options.
- b. Specify the directory that contains the installation (`Setup.exe` and `Setup64.exe`) files.
- c. Click `Add Hosts` to begin the installation on the specified host. Progress and status information is displayed. (An error message will be displayed if the installation or upgrade cannot complete.) When the process is complete, click `Close`. The Summary of Hosts dialog box is displayed.

5. This page displays the hosts that have been added to the HIT Group, and what actions—such as installations or upgrades—have been performed on each host. This page also shows you whether or not a reboot is required on the remote hosts. If a reboot is required, click `Reboot All`. Otherwise, click `Finish`.

After the installation is complete on the remote host, you can launch the Remote Setup Wizard from the remote host in order to initialize a PS Series array, configure the remote host to access a PS Series group, or to configure MPIO settings for the remote host.

After the host has been added to the HIT Group, it will appear in the tree in the left panel of the ASM/ME console and you can start managing it from there. To stop managing a host, right click the host in the left panel and select `Stop Managing`.

Install HIT on Remote Hosts Using PowerShell Scripts

The PowerShell script is called `HitRemoteInstall.ps1` and is located in the directory that was specified when the Host Integration Tools were installed on the local host. (The default installation directory is `C:\Program Files\EqualLogic\bin`).

This PowerShell script allows you to perform unattended installations on remote hosts. You can specify multiple hosts when you run the script and the Host Integration Tools will be automatically installed on every host you specify.

The PowerShell script will only perform installations on remote hosts; it will not add the host to a HIT group upon completion. If you use the PowerShell script for installing the Host Integration Tools and decide to add that host to a HIT group, you can do so with the Add Hosts wizard in the ASM/ME GUI.

You can select the same installation options that the regular Windows installer allows. You can install MPIO alone since it does not require ASM/ME. If you install ASM/ME, then RSW, VSS, and the ASMCLI will automatically be installed as well. If you do not specify these components, you will be prompted accordingly.

To use a PowerShell script to install the Host Integration Tools, the following prerequisites must be met:

- PowerShell version 2.0 or later is required. You need PowerShell only on the machine from which you are running the install script.
- In order for new installations to run successfully on remote hosts, ensure that you allow incoming ping requests through the remote host's firewall to the remote host. Use Windows Server Manager to create new inbound rules for your firewall. Select ICMPv4 or ICMPv6 protocol types for IPv4 and IPv6 pings, respectively. If both the local and remote hosts are in the same domain, allow the connections over the domain profile type.
- You will be prompted for username and password credentials in order to install Host Integration Tools on remote hosts added to the HIT Group. These credentials are never stored; they are only used for the installation. The following requirements must be met:
 - If you are installing on a cluster, you must provide the appropriate credentials (domain user with local administrator rights) across all cluster nodes.
 - If adding or installing on multiple hosts:

Single Domain—For multiple machines that belong to a single domain, you must provide the

appropriate user credentials (domain users with local admin rights) so that ASM/ME can successfully access the machines to perform the required installations.

Single Workgroup—For multiple machines that belong to a single workgroup, each machine must have the same local admin account credentials.

Multiple Domains—For machines across multiple domains, add or install on all the machines from one domain at a time.

- The Remote Procedure Call (RPC) service must be running. This service should be started by default on Windows systems but if it is not running, or if the firewall is blocking it, the installation will not work.
- Copy the `Setup.exe` and `Setup64.exe` installation files into a directory of your choice. Because you must specify this directory multiple times if you are pushing out several installations, you can simplify the process by copying the installation files onto a network shared directory. (The default installation directory is `C:\Program Files\EqualLogic\bin`, so you can also place it there). ASM/ME will use these files to initiate the installation procedure on remote hosts. These installation files are available on the CD-ROM that shipped with your PS Series array, or from the customer support site: <https://support.dell.com/equallogic>.

Syntax for PowerShell Remote Host Installation

```
HitRemoteInstall.ps1 [-ComputerNames "<computer 1> <computer 2> ..."]
[-InstallerLocation "<path>"]
[-BackupDocumentLocation "<path>"]
[-InstallOptions "<Install Option 1> <Install Option 2> ..."]
[-UserName "<Domain>\<Username>"] [-Password "<Password>"]
```

The `BackupDocumentLocation` parameter allows you to specify the backup document directory. This directory is especially important for cluster installations, for which a network share must be specified. For information about backup document directories and cluster configurations, see the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide*.

When specifying host names, you can specify the host's IP address, host name, fully qualified domain name, or IPv6 address. If you are specifying an IPV6 address, enter the address as follows:

1. Change all the “.” characters to “-” characters.
2. If there is a “%” character, change it to “s”.
3. Add “.ipv6-literal.net” to the end.

For example, an address of `fe80::2c02:db79%8` must be entered as `fe80-2c02-db79s8.ipv6-literal.net`.

Table 3 lists the install options you can specify when running the PowerShell script.

Table 3: Install Options

Option	Description
ALL	Installs all options listed here.
RSW	Remote Setup Wizard
VSS	Volume Shadow Copy Service Provider
ASMCLI	ASM/ME Command Line Interface
ASM	Auto-Snapshot Manager
VDS	Virtual Disk Service Provider
MPIO	Multipath I/O DSM (might require system reboot)
PS	PowerShell Tools
HPC	HPC iSCSI Provider (valid only on 64-bit servers)
TRIM	Volume rethinning driver (system reboot required)
SMP	Storage Management Provider for Windows 8 or greater

If you are running the script for the first time, you must allow remote signed scripts to run, as follows:

1. Open a PowerShell window.
2. Navigate to the directory that was specified when the Host Integration Tools were installed on the local host. (The default installation directory is `C:\Program Files\EqualLogic\bin`).
3. Type `set-executionpolicy remotesigned` and enter `Y` to confirm the change.

Install HIT on Remote Hosts with PowerShell

1. Open a PowerShell window.
2. Navigate to `Program Files\EqualLogic\bin` or the directory that was specified when the Host Integration Tools were installed on the local host.
3. At the command prompt, type the following command to install ASM/ME on the remote host. Replace *ipaddress*, *myUsername*, and *myPassword* with the remote host's IP address, and your own credentials.

```
.\HitRemoteInstall.ps1 -ComputerNames ipaddress -InstallerLocation
"C:\Program Files\EqualLogic\bin" -BackupDocumentLocation
```

```
"\\server\share\subdirectory1" -InstallOptions ASM -Username  
myUsername  
-Password myPassword
```

You can specify any of the install options listed in [Table 3](#). You can also specify multiple hosts. Instead of listing the IP address to specify the remote host, you can also specify the host name, domain name, or IPv6 address.

Install HIT on a Microsoft Failover Cluster

If you install Host Integration Tools on a running cluster, you are prompted to configure the installation for cluster operation and it is not necessary to complete the tasks described in the previous sections.

Before you begin, make sure the following prerequisites are met:

- You must use an account that is a Microsoft domain user account with local administrative access. Consider creating a named account such as `ASMAadmin` to use for ASM/ME operations on the cluster. You can use this account to log on to required services. If any cluster node is running Microsoft Exchange and Microsoft SQL Server, (using PS Series iSCSI volumes) you must also make sure that your user account has the appropriate security group access for those applications.
- If you are using multipathing with the Dell EqualLogic MPIO DSM, you must use an identical configuration on each node.

To install the Host Integration Tools on a failover cluster:

1. Set up a shared network folder for the backup documents and collection definitions on a volume that is accessible to all cluster nodes. If you create the shared folder on a clustered iSCSI volume on your PS Series group, ASM/ME identifies the volume as a supported volume on the cluster node that owns the share. However, it prevents you from restoring data from any Smart Copies of the shared volume.
2. Install the same version of Host Integration Tools on every cluster node. Select the same set of components to install on each node. After you perform a first-time manual installation on a cluster node, click `Add Hosts` in the ASM/ME GUI to push parallel installations to the rest of the cluster nodes. See [Install HIT on Remote Hosts Using the Add Hosts Wizard on page 11](#) for how to perform this operation.
3. Configure PS Series group access for each node, specifying identical responses each time. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for information about configuring group access.
4. Use ASM/ME to specify the backup document directory and ASM services logon account on each cluster node. Because ASM/ME uses the specified logon account credentials to access the shared network folder, specify both the document directory and logon account at the same time. To specify the network folder, see [Specify the ASM/ME Backup Document Directory on page 18](#). To specify the logon account, see [Change the Logon Account for ASM/ME Services \(EQLReqService and EqlASMAgent\) on page 18](#).

Specify the ASM/ME Backup Document Directory

To set or modify the ASM/ME Backup Document directory:

1. In ASM/ME, click `Settings` in the navigation area.
2. Click on the `General Settings` tab.
3. Specify a directory for backup documents. Specify the UNC path for the shared volume instead of the default location. You specify the network share name by using UNC format such as `\\server-name\shared-resource-pathname` or `\\ClustersystemFS\H$\VSS Requestor\`.
4. Click `Save`.

Change the Logon Account for ASM/ME Services (EQLReqService and EqlASMAgent)

1. In ASM/ME, click `Settings` in the navigation area.
2. Click on the `General Settings` tab. If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts.
3. Select the option to run the ASM/ME services from the local system user account, or another specified user account. If you want to specify another user, you must provide the domain, username, and password credentials. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Joining a Computer into a Windows Failover Cluster

The prerequisites for joining a computer running Host Integration Tools into a Microsoft Failover Cluster are as follows:

- Use an account that is a Microsoft domain user account with local administrative access. Consider creating a named account such as `ASMadmin` to use for ASM/ME operations on the cluster. You can use this account to log on to required services. If any cluster node is running Microsoft Exchange and Microsoft SQL Server, (using PS Series iSCSI volumes) you must also make sure that your user account has the appropriate security group access for those applications.
- Change the logon account for the `EQLReqService` and `EqlASMAgent` services. If you are using Cluster Continuous Replication (CCR) or a Database Availability Group (DAG) under Microsoft Exchange or SQL Server 2012, you do not need to change the logon account. See [Change the Logon Account for ASM/ME Services \(EQLReqService and EqlASMAgent\) on page 18](#) for how to change the logon account.
- If the host being added is not running the same (or any) version of the Host Integration Tools as the other cluster nodes, then after you add the host, run ASM/ME and select the Add Hosts wizard to install ASM/ME and add the new node to the HIT group. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Silent Installations

A silent installation does not require you to monitor and respond to typical installation prompts. You create a template of your installation selections as you perform a silent installation. You can then clone this installation template to other computers, if the other computers have:

- Very similar or identical hardware configurations.
- The same operating system and service pack level.
- The same system configuration for all optionally installed features that are affected by the installation, including (but not limited to) firewall, iSCSI initiator version and configuration, Microsoft MPIO.

Cloning an installation works best when you are setting up a large number of identically configured and newly-installed computers. The following considerations apply when performing a silent installation:

- During the installation process, installation messages from third-party products might appear, indicating what software is being installed. However, these messages do not interfere with the installation and can be ignored.
- The drive letter you specify in the installation script is used on every computer on which you run the script. For example, if you specified `F:\Eq1` in the script, all the other computers on which you run the script will attempt to install the kit on the `F:\` drive.
- The installation applies the selections you make when you create the original recording of an installation. However, only those Host Installation Tools components that are supported by the target computer are installed.
- When installing on a failover clusters, you must perform the installation from an account that is a member of the domain administrator group.

Support for Silent Installation

Host Integration Tools installations are built using Install Shield, which is based on the Microsoft Windows Installer. This product contains built-in support for silent installations.

Syntax

```
Setup.exe /s /v/qn /V"/q /norestart
[ADDLOCAL = HPC,RemoteSetupWiz,PowerShell,ASMME,COREVSSPROVIDER,VDS,MPIO|
ALL>]
[INSTALLDIR=<drive>:\<install_path>]
[IS_NET_API_LOGON_USERNAME=<Domain\Username>]
[IS_NET_API_LOGON_PASSWORD=<password>] /l*v <log_path>"
```

- `Setup.exe` or `Setup64.exe` is the single executable installer for the Host Integration Tools.

- `ADDLOCAL`, if used, specifies which features are to be installed. If the operating system does not meet the requirements to install the feature, the feature will not be installed even if it is specified.
- `INSTALLDIR`, if used, specifies the drive and path of the installation. If not specified, the installation will go into the default location, which is `C:\Program Files\EqualLogic`.
- `IS_NET_API_LOGON_USERNAME` and `IS_NET_API_LOGON_PASSWORD`, if used, specify the domain and username credentials to assign to the required Host Integration Tools services. Service as log on rights will be granted to this user during installation. If not specified, the local system account will be used.

Table 4 lists the case-sensitive feature names that you can specify when performing a silent installation.

Table 4: Case-Sensitive Feature Name

Case-Sensitive Feature Name	Description
HPC	HPC iSCSI Provider (only valid on 64-bit servers)
RemoteSetupWiz	Remote Setup Wizard
PowerShell	PowerShell Tools
ASMME	ASM/ME Command Line Interface, Auto-Snapshot Manager, Volume Shadow Copy Service Provider
COREVSSPROVIDER	Volume Shadow Copy Service Provider (Core Operating Systems only)
VDS	Virtual Disk Service Provider
MPIO	Multipath I/O DSM (May require system reboot)
TRIM	Volume rethinning driver (system reboot required)
SMP	Storage Management Provider for Windows 8 or greater
ALL	All features

Perform a Silent Installation

To perform a silent install on a 32-bit Windows system, enter the following command:

```
Setup.exe /s /v/qn /V"/q ADDLOCAL=RemoteSetupWiz INSTALLDIR=C:\HitKit\Eql"
```

To install all supported features to the default installation directory and specify a custom username and password for the HIT services, enter the following command:

```
Setup.exe /s /v/qn /V"/q ADDLOCAL=ALL IS_NET_API_LOGON_
USERNAME=Domain\Administrator IS_NET_API_LOGON_PASSWORD=password"
```

To install all supported features to the default installation directory on a 64-bit Windows system, enter the following command (if MPIO is being installed, the host might be rebooted):

```
Setup64.exe /s /v/qn /V"/q ADDLOCAL=ALL"
```

Perform a Silent Uninstallation

To perform a silent uninstallation, enter the following command:

- For 32-bit systems: `Setup.exe /s /v/qn /x`
- For 64-bit systems: `Setup64.exe /s /v/qn /x`

To uninstall completely on a 32 bit system, enter the following command:

```
Setup.exe /s /v/qn /x
```

To uninstall completely on a 64 bit system, enter the following command:

```
Setup64.exe /s /v/qn /x
```

Create a Log File During Silent Mode

If you want to create a log file describing the installation, add `"/L C:\<path>setup.log"` to the command (including the quotation marks). For example, entering the following command will cause the log to be written to the setup.log file:

```
Setup64.exe /s /v/qn /V"/q ADDLOCAL=ALL /L C:\<path>setup.log"
```

Use `/L*v` for a verbose log.

To verify if a silent installation succeeded, scroll to the end of the log file.

Using HIT with a SharePoint Farm

For the best results when using the Host Integration Tools on a SharePoint farm:

- Create or verify the domain accounts in the domain. At a minimum, create one account for SQL administration and optionally, a separate account for SharePoint administration: for example, `domain\sp_sqladmin` and `domain\sp_admin`. These accounts must be in the local administrators group of every host in the farm (directly or through group membership). For more information, see the following URL: <http://technet.microsoft.com/en-us/library/ee662513.aspx>
- On the PS Series group, create separate volumes for the SharePoint Search Service Application or Foundation Search. The search components must reside on PS Series storage so that ASM/ME includes them in Smart Copies.

- Do not place search components on the same volumes as the farm databases.
- Place all SharePoint search indexes on PS Series volumes, or else ASM/ME will display the components as gray, and will not include them in Smart Copies.

Specify Index File Locations When Installing SharePoint

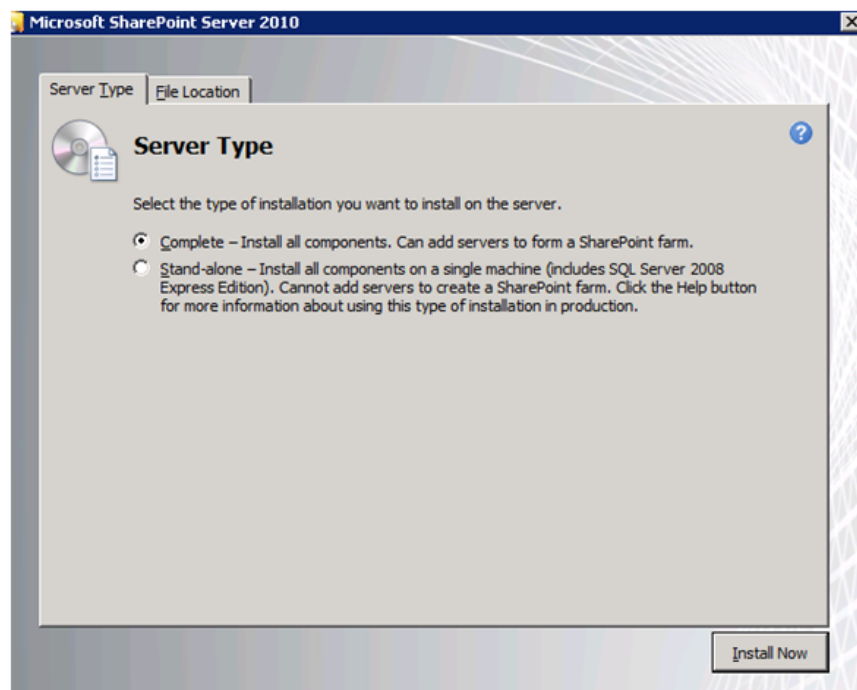
For best results using the Host Integration Tools with SharePoint, make sure to specify PS Series volumes as the location for all the search index files at the time you install SharePoint.

If you have already installed your SharePoint farm, see [Modify Index File Locations in an Existing SharePoint Farm on page 23](#) for information on how to change the search index file locations.

To specify PS Series volumes for the index file locations during SharePoint installation:

1. Enter the license key.
2. On the next screen, select Server Farm.
3. On the next screen, click the Server Type tab, and choose the option for a complete installation ([Figure 1](#)).

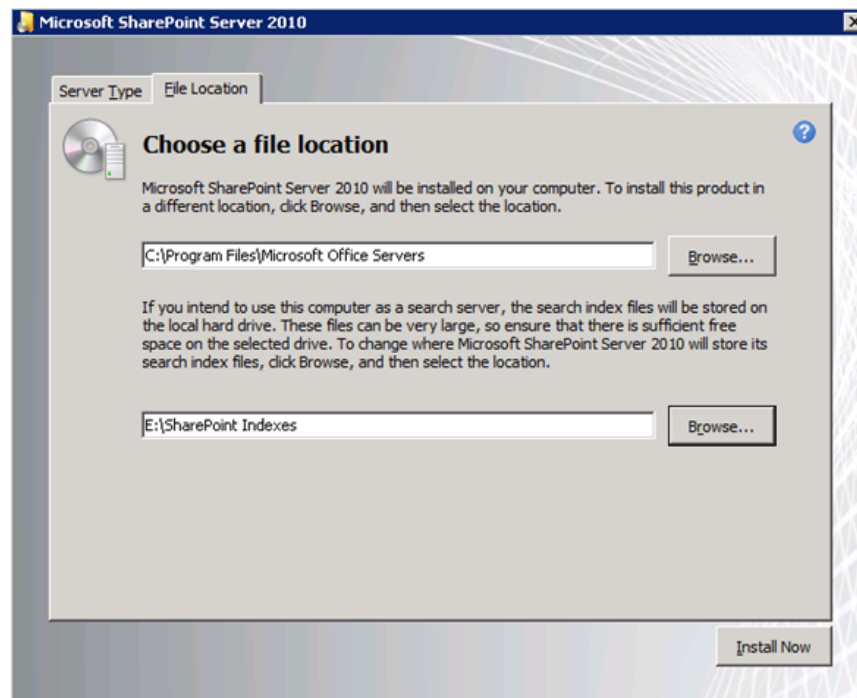
Figure 1: SharePoint Installation—Server Type Tab



4. Click the File Location tab.

5. In the bottom field, for the location of the search index files, enter the path to the PS Series volume that contains the search indexes; for example, `E:\SharePoint Indexes` (Figure 2). In this example, the `E:\` drive is a PS Series volume that was created in advance and logged on the search host. The `SharePoint Indexes` directory was created to store the search indexes.

Figure 2: SharePoint Installation—File Location Tab



Modify Index File Locations in an Existing SharePoint Farm

If you already have a SharePoint farm deployment and can modify its topology, you can change the query and crawl component index locations using the Central Administration interface after installation.

In an existing farm, by default all three types of search components are on the `C:` drive. You must move these onto PS Series volumes. However, if you create a new SSA or change the topology of your existing SSA, the components will be placed on the `C:` drive, again by default, and ASM will ignore those components.

To resolve this problem, you can:

- Specify the file location during a new SharePoint installation (see [Specify Index File Locations When Installing SharePoint on page 22](#)).
- Uninstall and then reinstall SharePoint with the new default file location. If you do this, you must make sure your farm can handle the temporary loss of a host, such as by setting up a redundant service application.
- Change the location of the different search files. See the following sections:
 - [Change the Default Index Location Using PowerShell cmdlets on page 24](#)

- [Change Index Locations Using Central Administration on page 24](#)
- [Change Administration Component Index File Location on page 24](#)
- [Change the SPSearch Index File Location on page 25](#)

Change the Default Index Location Using PowerShell cmdlets

On every application host that has search provisioned:

1. Open Office Search.
2. Open the SharePoint PowerShell shortcut.
3. Enter the following cmdlet to see the current index location:

```
Get-SPEnterpriseSearchServiceInstance
```

4. Enter the following cmdlet to change the default search index location (in this example, to E:\SharePoint Indexes):

```
Get-SPEnterpriseSearchServiceInstance | Set-SPEnterpriseSearchServiceInstance -  
DefaultIndexLocation "E:\SharePoint Indexes"
```

Repeat this procedure whenever a new host is provisioned for search, if you did not change the default during installation.

Change Index Locations Using Central Administration

1. In Central Administration, select Application Management, then Manage Service Applications, then Search Service Application, then Search Application Topology.
2. Select Modify from the drop-down menu.
3. Under Index Partition, click Query Component.
4. Select Edit Properties from the drop-down menu.
5. Change the search index file location for each query component.
6. In Crawl Component, select Edit Properties from the drop-down menu.
7. Change the index location for each crawl component.
8. Click OK to apply the topology changes.

Change Administration Component Index File Location

No direct method is available in Central Administration to change the administration component index file location. Instead, follow this procedure to temporarily change the Administration Component server to a different server, then immediately change it back to the original server. This process forces the administration component index file location to change.

Before you begin, complete the steps in [Change the Default Index Location Using PowerShell cmdlets on page 24](#).

1. In Central Administration, click Administration Component, then click Edit Properties.
2. In the Edit Properties dialog box, change the Administration Component server to a different server, then click OK.

This is a temporary step.

3. In Central Administration, click Administration Component, then click Edit Properties.
4. In the Edit Properties dialog box, change the Administration Component server to the previous (original) server, then click OK.
5. Click Apply Topology Changes.

Change the SPSearch Index File Location

If SPSearch is enabled on a host, change the default index location to a PS Series volume using the `stsadm.exe` utility.

- For SharePoint 2010, the default index location is:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server  
Extensions\14\BIN\
```

- To see the current index location, enter:

```
stsadm.exe -o spsearch -action list
```

- To change the index location, enter:

```
stsadm.exe -o spsearch -indexlocation "E:\SharePoint Indexes"
```

Best Practices for SharePoint

- Dell recommends that you reinstall SharePoint on the application server and define the default index location as described in [Specify Index File Locations When Installing SharePoint on page 22](#).
- Create more volumes on the SQL host to separate content DBs for restores.
- Place database and log files on separate volumes so the Smart Copy operations always create pairs of volumes.
- Create directories and specify the default database location in SQL (Select Server, then Properties/Database Settings). This makes sure the initial SharePoint databases are created on PS Series volumes and minimizes the manual work of moving them off of the C: drive.
- Consider using Virtual Machines on PS Series volumes for Web front-end servers. Smart Copy Snapshots of the Virtual Machines will allow recovery of IIS if the WFE fails or needs rebuilding.

3 Remote Setup Wizard

Remote Setup Wizard (RSW) allows you to initialize a PS Series array, either creating a new PS Series group with the array as the first member, or having the array join an existing group. The wizard includes links to the ASM/ME GUI that enable you to:

- Configure PS Series group access to the computer
- Configure MPIO settings

To install RSW, see [Installation on page 7](#). See the *Host Integration Tools for Microsoft Release Notes* for the latest information about the wizard.

The Host Integration Tools also include the Remote Setup Command Line Interface (RSWCLI). Use the RSWCLI utility to configure PS Series groups and MPIO settings from a command line or in scripts. For details, see [Remote Setup Command Line Utility on page 33](#).

PS Series Group Requirements for Using RSW

If you are using RSW to initialize an array, make sure the following requirements are met:

- The uninitialized PS Series array must be running the minimum supported firmware revision. The array hardware must be installed and a network cable must be attached to Ethernet port 0. Follow the hardware installation procedure described in the setup documentation for your array model. You do not require a serial cable if you are using RSW, although you should keep the serial cable for later use in case there is no network access to the array or group.
- Two options are available for connecting the array and computer to each other:
 - Connect the computer to the same Ethernet segment as the array, and make sure that Layer 2 multicasting is not blocked between the array and the computer. This connection method required if you want to configure computer access to a group or configure multipath I/O between the computer and a group.
 - Use an Ethernet cable to connect the computer to Ethernet port 0 on the uninitialized PS Series array.

Windows System Requirements for Using RSW

To use RSW, your computer must have the following:

- A supported operating system and a supported version of the Microsoft iSCSI Software Initiator. See the *Host Integration Tools for Microsoft Release Notes* for information about RSW operating system support.
- Two or more supported network interface cards (NICs) or host bus adapters (HBAs) that are at least 1Gbps. Multipath I/O does not utilize NICs with speeds of less than 1Gbps.

Launch RSW on the Host

1. Click **Start**, then **All Programs**, then **EqualLogic**, and then **Remote Setup Wizard**.
2. The **Thank You for choosing Dell EqualLogic** screen appears, which provides a link to the customer support site. Click this link to log in to your support account, or to create one. You can optionally check the box to prevent display of this screen the next time you run RSW.
3. Click **OK**.
4. Decide which task you want to perform:
 - Initialize an array. (This option also allows you to create a PS Series group with the array as its first member, or to have the array join an existing PS Series group).
 - Configure the computer to access a PS Series group (launches the Auto-Snapshot Manager GUI)
 - Configure multipathing (MPIO) settings for the computer (launches the Auto-Snapshot Manager GUI)

Launch RSW from ASM/ME

1. In the ASM/ME Menu bar, click **Launch**.
2. Select **Remote Setup Wizard**.

Initialize a PS Series Array Using RSW

This section contains information on how to use RSW to initialize a PS Series array. If you are initializing a PS Series array, you will have the option of creating a new PS Series group and adding the array as its first member, or adding it to an existing PS Series group.

Search for a PS Series Array Using RSW

RSW discovers all accessible, uninitialized arrays in your SAN and displays them in a formatted list. You can then search and sort this list to identify a specific PS Series array that you want to initialize and set up as a member of a group. You can enter an alphanumeric string, such as part of the array's serial number, and the first matching array is returned.

You can enter an alphanumeric string or substring for any of the following attributes:

- **Serial Number**—The array's serial number. Typical PS Series serial numbers are SHU946170103CB8 or B035687.

- **Product Family**—The model number of the array. For example, the string `60` matches arrays with model numbers PS6000 and PS6010. (The string `60` also finds matches in the serial number fields.)
- **Firmware**—The revision number of the PS Series firmware that is running on the array, such as: `5.2.0`.
- **Disk Info**—The number or capacity of drives in the array. For example, the string `14` matches all arrays that contain 14 drives. (That string also finds matches in the serial number fields.) Similarly, `8.00GB` matches all arrays that contain 8 GB drives.

If the search feature matches an array in the list, you can mouse over any line item to display other information about the array, including its:

- MAC address for Ethernet port 0 (`eth0`)
- Host adapter MAC address to which the array is connected
- Supported RAID levels

To sort the list of arrays, click on a column heading. For example, click on the Firmware heading to sort firmware revisions in ascending order. Click a second time to sort in descending order. A triangle to the right of the column header indicates the current sort column, if any, and the sort direction.

Information Required for Initializing a PS Series Array

When you initialize the PS Series array, RSW will prompt you for the information described in [Table 5](#) and [Table 6](#).

Table 5: Array Configuration

Prompt	Description
Member name	Unique name used to identify the array in the group. The name string must be fewer than 64 alphanumeric characters or hyphens. No other characters are permitted. The first character must be a letter or number.
IP address (IPv4)	Network address for the Ethernet 0 network interface, which must be an IPv4 address. Each member must have at least one network interface on the same subnet as the group IP address, described in Table 6 .
Netmask	Combines with the IP address to identify the subnet on which the Ethernet 0 network interface resides.
Default gateway	Network address for the device used to connect subnets and forward network traffic beyond the local network. A default gateway is used to allow the Ethernet 0 network interface to communicate outside the local network (for example, to allow access to volumes from computers outside the local network). The default gateway must be on the same subnet as the Ethernet 0 network interface.

Prompt	Description
RAID policy	RAID policy configured on the first member of the group: - RAID 6—Of the total number of disks installed in the array, two disks are used for parity and one disk is a spare. The rest are data disks. - RAID 6-Accelerated—Has the same disk configuration as RAID 6, but is used on PS Series arrays that have a mix of HDD (hard disk drives) and SDD (solid state disk drives). - RAID 10—Striping on top of multiple RAID 1 (mirrored) sets, with one or two spare disks. RAID 10 provides good performance for random writes, in addition to the highest availability. - RAID 50 [Not Recommended]—Striping on top of multiple RAID 5 (distributed-parity) sets, with one or two spare disks. RAID 50 provides a good balance of performance (especially for sequential writes), availability, and capacity. Note: To use RAID 5, you must configure the RAID policy using the Group Manager CLI. If you are adding an array to an existing group, use the Group Manager GUI or CLI to set the RAID policy for the new member.

Note: For a complete discussion of RAID policies on PS Series systems, see the Dell Technical Report *PS Series Storage Arrays: Choosing a Member RAID Policy*, which is available from the following location: <http://en.community.dell.com/techcenter/storage/w/wiki/equallogic-tech-reports.aspx>

Table 6: Group Configuration

Prompt	Description
Group name	Unique name used to identify the group. The name string must be fewer than 64 alphanumeric characters or hyphens. No other characters are permitted. The first character must be a letter or number.
Group IP address	Network address for the group. The group IP address is used for group administration and computer access to data stored in the group. You cannot specify IPv6 addresses when initializing a group. However, you can add host access to a group that is already configured to use IPv6 addresses.
Password for managing group membership	Password required when adding members to the group. The password must have 3 to 16 alphanumeric characters and is case-sensitive.
Password for the default group administration account	Password that will override the factory-set password (grpadmin) for the default grpadmin account. The password must have 3 to 16 alphanumeric characters and is case-sensitive.
Microsoft service user name and password	CHAP user name and password used to enable Microsoft service (VSS or VDS) access to the group. The user name must have between 3 and 54

Prompt	Description
	alphanumeric characters. The password must have 12 to 16 alphanumeric characters, and is case-sensitive. Microsoft services running on a computer must be allowed access to the group in order to create VSS snapshots in the group or use VDS.

Initialize an Array and Create a PS Series Group

1. Gather the information described in [Information Required for Initializing a PS Series Array on page 29](#).
2. Click **Start**, then **All Programs**, then **EqualLogic**, and then **Remote Setup Wizard**.
3. Select **Initialize a PS Series array** and click **Next**. RSW discovers and lists all uninitialized arrays accessible to the computer. If no arrays appear, click the **Rediscover** button.
4. Select a PS Series array from the list and click **Next**. You can also search for a specific array or sort the list of arrays. For information on how to search for a specific array, see [Search for a PS Series Array Using RSW on page 28](#).
5. Enter the member information (Member Name, IP Address, Subnet Mask, and Default Gateway). Select the **Create a new group** option and click **Next**.
6. Enter the group information in the required fields and click **Next**.
7. Click **OK**. The next screen displays a message stating that the array has been successfully initialized and the PS Series group has been created.
8. Click **Finish** to exit the wizard, click **View Log** to view a summary of the array configuration, or click **Next** to configure additional arrays.

If a problem occurs during the RSW setup, see [Troubleshoot RSW on page 32](#).

When you exit RSW, it performs the following tasks:

- Configures the group IP address as an iSCSI target discovery address. This configuration enables the computer to discover volumes and snapshots (iSCSI targets) in the group.
- Stores the CHAP user name and password that allow Microsoft services (VDS or VSS) access to the group.
- Creates a corresponding VSS/VDS access control record and local CHAP account in the group. To view the VSS/VDS access control record in the Group Manager GUI, click **Group Configuration**, then click on the **VDS/VSS** tab. To display the local CHAP account in the Group Manager GUI, click **Group Configuration**, then click on the **iSCSI** tab.

After you create a group, you can use the Group Manager GUI or CLI to create and manage volumes.

Initialize an Array and Add It to an Existing Group

1. Gather the information described in [Information Required for Initializing a PS Series Array on page 29](#).
2. Click `Start`, then `All Programs`, then `EqualLogic`, and then `Remote Setup Wizard`.
3. Select `Initialize a PS Series array` and click `Next`. RSW discovers and lists all uninitialized arrays accessible to the computer. If no arrays appear, click the `Rediscover` button.
4. Select a PS Series array from the list and click `Next`. You can also search for a specific array or sort the list of arrays. For information on how to search for a specific array, see [Search for a PS Series Array Using RSW on page 28](#).
5. Enter the member information (Member Name, IP Address, Subnet Mask, and Default Gateway). Select the `Join an existing group` option and click `Next`.
6. Enter the group name, IP address, membership password, and click `Next`. When the array joins the group, a message appears stating that the new member was successfully added to the group.
7. Click `Yes` to open the Group Manager GUI immediately to configure a RAID policy for the new member, or click `No` if you will configure RAID later. If you configure RAID later, you must use the Group Manager GUI or CLI to set the RAID policy for the new group member. For more information, see the *Dell EqualLogic Group Manager Administrator's Guide* or *Dell EqualLogic Group Manager CLI Reference Manual*.
8. Click `Finish` to exit the wizard, click `View Log` to view a summary of the array configuration, or click `Next` to initialize additional arrays.

If a problem occurs during the RSW setup, see [Troubleshoot RSW on page 32](#).

When you exit RSW, it configures the group IP address as an iSCSI target discovery address. This configuration enables the computer to discover volumes and snapshots (iSCSI targets) in the group.

Troubleshoot RSW

If the Remote Setup Wizard is interrupted while initializing an array and the operation fails, you must reset the array before running the wizard again. To reset an array:

1. Connect the serial cable that was shipped with the array, between the active control module and a console terminal, or a computer running a terminal emulator.
2. Enter the `reset` command and wait for the reset operation to complete.
3. Disconnect the serial cable, and launch the Remote Setup Wizard from the computer where it is installed.

4 Remote Setup Command Line Utility

The Remote Setup Command Line Utility (also referred to as the Remote Setup CLI or RSWCLI) provides an alternative to using the Remote Setup Wizard. You can perform the same set of operations provided by the Remote Setup Wizard, except that the setup and configuration tasks are performed through commands executed at a Windows command prompt instead of the wizard. When you install the Remote Setup Wizard, the Remote Setup CLI is also installed.

General Command Syntax for the RSWCLI

The general command syntax is as follows:

```
rswcli [-]sub_command required_parameter="argument" [-optional_parameter...]
```

The following constraints apply to the syntax:

- [-]sub_command—Prefix subcommands with a dash (-).
- "argument"—An argument requires quotation marks only when the argument variable contains an embedded space.
- Several parameters are mutually exclusive, and if more than one of these parameters are specified, it is treated as an error and causes the command to fail. The command parser automatically ignores any redundant parameters.

Getting Help on Commands

To see all the available RSWCLI commands and their options, enter:

```
rswcli -?
```

For help on a specific command, enter:

```
rswcli -sub_command -?
```

For example:

```
rswcli -Discover -?
```

```
Remote Setup Command Line Utility
Dell EqualLogic Remote Setup Wizard CLI Version 4.0.2000.6246
Copyright 2004-2013 Dell Inc. All rights reserved.
Discover uninitialized storage arrays
rswcli -Discover
[-Detail]
```

Using RSWCLI Commands

The RSWCLI executable is located under the default installation folder, or the folder that you specified for HIT during installation. The default folder is: `C:\Program Files\EqualLogic\bin`

You execute a command by starting the Windows Server command prompt:

1. Click **Start**, then **Run**. Then type `cmd`.
2. In the command window, you can change directory to `C:\Program Files\EqualLogic\bin` or add the RSWCLI commands folder to your path by editing your Windows `PATH` environment variable.

Discover a PS Series Array

Use the `rswcli -Discover` command to discover uninitialized PS Series arrays. The command displays a list of uninitialized PS Series array serial numbers and service tag numbers (if known).

The command syntax is as follows:

```
rswcli -Discover [-Detail]
```

The `[-Detail]` option specifies whether RSWCLI should display the array MAC address, Host Adapter MAC address, firmware version, and supported RAID levels for each array.

Initialize a PS Series Array

Use the `rswcli -Initialize` command to initialize an array. This command also allows you to create a new PS Series group with the array as its first member, or to have the array join an existing group.

The command syntax is as follows:

```
rswcli -Initialize
    -ServiceTag=<service tag> | -SerialNumber=<serial number>
    -MemberName=<name>
    -MemberIPeth0=<IP address>
    -MemberSubnet=<Subnet Mask>
    -MemberGateway=<IP address>
    -CreateGroup | -JoinGroup -GroupName=<name>
    -GroupIP=<IP address>
    -Membership=<password>
    -RAID=<10|50|6|6-accelerated>
    -Admin=<password>
    -ChapUser=<username>
    -ChapSecret=<password>
    -DCBVlanID=<DCBVlanID>
```

Table 7 describes the command parameters.

Table 7: Initialize Array Command Options

Parameter	Argument	Description
Initialize		Initializes a PS Series array. The following parameters are required: • <code>-SerialNumber</code> <code>ServiceTag</code> • <code>-MemberName</code> • <code>-MemberIPeth0</code> • <code>-MemberSubnet</code> • <code>-MemberGateway</code> You must specify either the <code>-CreateGroup</code> or the <code>-JoinGroup</code> parameter. With the <code>-CreateGroup</code> parameter, you must also enter the <code>-GroupName</code> and <code>-GroupIP</code> command parameters.
<code>SerialNumber=</code>	serial number	Designates the serial number of the PS Series array to be initialized. Use either this option or the <code>ServiceTag</code> option, but not both.

Parameter	Argument	Description
ServiceTag=	service tag number	Designates the service tag number of the PS Series array to be initialized. Use either this option or the <code>SerialNumber</code> option, but not both.
MemberName=	member name	Required—Designates the member name of the PS Series array to be initialized.
MemberIPeth0=	IP address	Required—Designates the IP address for the Ethernet 0 network interface that controls access to the PS Series array to be initialized.
MemberSubnet=	subnet mask	Required—Designates the IP address for the subnet controlling access to the PS Series array to be initialized.
MemberGateway=	IP address	Required—Designates the IP address of the gateway to use for access to the PS Series array to be initialized.
CreateGroup		Specifies that a new group should be created using the specified group name and group IP address. Make sure the name and IP address you enter are not used by any other group.
GroupName=	group name	Required with <code>CreateGroup</code> —Designates the name of a specific PS Series group for which configuration information is requested.
JoinGroup		Specifies that the member array should join the group with the specified group name and group IP address.
GroupIP=	IP address	Designates the IP address to be used for accessing the group.
Admin=	password	Required with <code>CreateGroup</code> —Specifies the password to be used for default group administration user access to the specified group.
Membership=	password	Specifies the password to be used for authenticating membership access to the specified group.
RAID=	{10 50 6 6-accelerated}	Required with <code>CreateGroup</code> —Specifies the RAID policy for the member.
ChapUser=	CHAP user name	Required with <code>CreateGroup</code> —Specifies the CHAP username to be used for authenticating access to arrays in the specified group.

Parameter	Argument	Description
ChapSecret=	CHAP password	Required with <code>CreateGroup</code> —Specifies the password to be used for authenticating access to arrays in the specified group.
DCBVlanID=	DCB VLAN ID	Designates the VLAN ID if you are using Data Center Bridging (DCB).

Note: For a complete discussion of RAID policies on PS Series systems, see the Dell Technical Report *PS Series Storage Arrays: Choosing a Member RAID Policy*, which is available from the following location: <http://en.community.dell.com/techcenter/storage/w/wiki/equallogic-tech-reports.aspx>

List or Modify MPIO Settings

Use the `rswcli -MPIOParameters` command to list or modify MPIO settings.

All parameters are optional. If no parameters are entered for this command, the current values for all parameters are listed.

The command syntax is as follows:

```
rswcli -MPIOParameters
    -MaxSessionsPerVolumeSlice=<1-4>
    -MaxSessionsPerEntireVolume=<1-12>
    -DefaultLoadBalancing=<LQD|RR|FO>
    -UseMPIOForSnapshots=<yes|no>
    -UseIPv4 | -UseIPv6
    -ClearDeviceLBPolicy
    -MinAdapterSpeed=<100|1000|10000> (as Mbps)
```

Table 8 describes the command parameters.

Table 8: Listing or Modifying MPIO Settings Command Options

Parameter	Argument	Description
MaxSessionsPerVolumeSlice=	1-4	Designates the maximum number of connections that MPIO should use per volume per member.
MaxSessionsPerEntireVolume=	1-12	Designates the maximum number of connections that MPIO should use in per volume for all members.
DefaultLoadBalancing=	LQD RR FO	Specifies the default load balancing policy for MPIO as Least Queue Depth (LQD), Round robin

Parameter	Argument	Description
		(RR), or Failover Only (FO). This change does not affect existing device load balancing policy, unless the <code>-ClearDeviceLBPolicy</code> parameter is also specified.
MinAdapterSpeed=	100 1000 10000	Specifies that MPIO will only use NICs that meet the minimum speed specified in Mbps, if at least two meet the speed.
UseMPIOForSnapshot=	yes or no	Specifies whether MPIO should be used for snapshots.
UseIPv4		Specifies that MPIO will use IPv4 IP addresses only. This parameter is mutually exclusive with the <code>-UseIPv6</code> parameter.
UseIPv6		Specifies that MPIO used use IPv6 IP addresses only. This parameter is mutually exclusive with the <code>-UseIPv4</code> parameter.
ClearDeviceLBPolicy		Specifies that if the default load balancing policy is changed, then the load balancing policies for individual devices should be cleared if they are not set to use the default.

List Included and Excluded Subnets for MPIO

Use the `rswwcli -ListMPIO` command to list subnets that are included or excluded for MPIO.

The default output for this command lists the adapters available. The state of each adapter is shown following the adapter name, either included or excluded. Optionally, the rules used to generate the include and exclude lists can also be displayed.

The command syntax is as follows:

```
rswwcli -ListMPIO [-IncludeOnly | -ExcludeOnly] [-Detail]
```

[Table 9](#) describes the command parameters. Note these parameters apply to the adapter list, not the rules list.

Table 9: List Subnets Command Options

Parameter	Description
IncludeOnly	Displays only the included subnets. Cannot be used with the <code>-ExcludeOnly</code> parameter.
ExcludeOnly	Displays only the excluded subnets. Cannot be used with the <code>-IncludeOnly</code> parameter.
Detail	Displays the rules used to generate the subnet list as well.

Include a Subnet or Adapter for Use by MPIO

By default, all subnets, adapters, and IP addresses accessible to the group start out in the included list.

Use the `rswcli -MPIOInclude` command to include a subnet, adapter, or IP address for use by MPIO, or to move a subnet, adapter, or IP address from the excluded list to the included list.

If the subnet, adapter MAC address, or IP address defined by these arguments is already in the included subnet, adapter, or IP address list, the command will fail.

The command syntax is as follows:

```
rswcli -MPIOInclude -Network=<IP_address> -Mask=<IP_address> [-Force]
```

```
rswcli -MPIOInclude -MAC=<MAC_Address> [-Force]
```

```
rswcli -MPIOInclude -IpAddress=<IP_address> [-Force]
```

```
rswcli -MPIOInclude -Default=<Include|Exclude> [-Force]
```

[Table 10](#) describes the command parameters.

Table 10: Include Subnet or Adapter Command Options

Parameter	Argument	Description
Network=	IP_address	Required for a subnet—Designates a new IP address for a network that, in combination with the <code>-Mask</code> parameter, matches exactly a subnet that is in the excluded subnet list and moves it to the included subnet list.
Mask=	IP_address	Required for a subnet—Designates a subnet mask to be used in conjunction with the network IP address to define a subnet to be added to the included list.
MAC=	MAC_address	Required for an adapter—Designates a new MAC address (also called

Parameter	Argument	Description
		physical address) for a single adapter that matches exactly a MAC address for the adapter that is in the excluded adapter list and moves it to the included adapter list. The MAC address can be specified as any of the following, where AA, BB, CC, DD, EE, FF, represent the high-order to low-order portions of a 6-byte hexadecimal (48-bit) MAC address that uniquely identifies a Host Network Adapter: • AABCCDDEEFF • AA-BB-CC-DD-EE-FF • AA:BB:CC:DD:EE:FF • AA.BB.CC.DD.EE.FF
IpAddress=	IP_address	Required for an IP address—Designates a new IP address for a single adapter that matches exactly an IP address for the adapter that is in the excluded IP address list, and moves it to the included IP address list.
Default=	Include Exclude	Controls whether any new adapters or subnets are included or excluded by default from MPIO usage. You cannot combine the <code>-Default</code> parameter with any other parameter except <code>-Force</code>.
Force		Use this parameter if the included list already contains a combination of subnet, adapter, or IP address. This will result in the included list containing only one type (either subnet, or adapter, or IP address), as specified by the command used with the relevant parameter. If the existing included list entries are of the same type (subnet, adapter or IP address) and are not already in the included list, then the new subnet, adapter or IP address is added to the include list. All other include list entries that are not of same type are removed; for example, <code>-MAC</code> with <code>-Force</code> saves only the existing adapter settings in the included list, but removes all other subnets and IP addresses from the include list. To preserve mixed types of subnets, adapters, and IP addresses, use the ASM CLI.

Exclude a Subnet or Adapter from Use By MPIO

By default, all subnets, adapters, and IP addresses accessible to the group start out in the included list.

Use the `rswcli -MPIOExclude` command to to exclude a subnet, adapter, or IP address from use by MPIO, or to move a subnet, IP address, or adapter from the included list to the excluded list.

If the subnet, adapter MAC address, or IP address defined by these arguments is already in the excluded subnet, adapter MAC address, or IP address list, the command will fail.

The command syntax is as follows:

```
rswcli -MPIOExclude -Network=<IP_address> -Mask=<IP_address> [-Force]
```

```
rswcli -MPIOExclude -MAC=<MAC_address> [-Force]
```

```
rswcli -MPIOExclude -IpAddress=<IP_address> [-Force]
```

```
rswcli -MPIOExclude -Default=<Include|Exclude> [-Force]
```

[Table 11](#) describes the command parameters.

Table 11: Exclude Subnet or Adapter Command Options

Parameter	Argument	Description
Network=	IP_address	Required for a subnet—Designates a new IP address for a network that, in combination with the <code>-Mask</code> parameter, matches exactly a subnet that is in the included subnet list and moves it to the excluded subnet list.
Mask=	IP_address	Required for a subnet—Designates a subnet mask to be used in conjunction with the network IP address to define a subnet to be added to the excluded list.
MAC=	MAC_address	Required for an adapter—Designates a new MAC address (also called physical address) for a single adapter that matches exactly a MAC address for the adapter that is in the included adapter list and moves it to the excluded adapter list. The MAC address can be specified as any of the following, where AA, BB, CC, DD, EE, FF, represent the high-order to low-order portions of a 6-byte hexadecimal (48-bit) MAC address that uniquely identifies a Host Network Adapter: • AABBCCDDEEFF • AA-BB-CC-DD-EE-FF • AA:BB:CC:DD:EE:FF • AA.BB.CC.DD.EE.FF

Parameter	Argument	Description
IpAddress=	IP_address	Required for an IP address—Designates a new IP address for a single adapter that matches exactly an IP address for the adapter that is in the included IP address list, and moves it to the excluded IP address list.
Default=	Include Exclude	Controls whether any new adapters or subnets are included or excluded by default from MPIO usage. You cannot combine the <code>-Default</code> parameter with any other parameter except <code>-Force</code> .
Force		Use this parameter if the excluded list already contains a combination of subnet, adapter, or IP address. This will result in the excluded list containing only one type (either subnet, or adapter, or IP address), as specified by the command used with the relevant parameter. If the existing excluded list entries are of the same type (subnet, adapter or IP address) and are not already in the excluded list, then the new subnet, adapter or IP address is added to the excluded list. All other excluded list entries that are not of same type are removed; for example, <code>-MAC</code> with <code>-Force</code> saves only the existing adapter settings in the excluded list, but removes all other subnets and IP addresses from the excluded list. To preserve mixed types of subnets, adapters, and IP addresses, use the ASM CLI.

5 Using the Multipath I/O Component

The Dell EqualLogic Multipath I/O (MPIO) DSM (Device Specific Module) enables you to configure redundant network paths from a Windows computer to PS Series volumes for high availability and high-performance SAN data traffic.

Introduction to Multipath I/O DSM

The Dell EqualLogic MPIO DSM coordinates activity between the MPIO drivers and PS Series group storage, maximizing the capabilities of both the operating system and the iSCSI SAN.

The EqualLogic MPIO component works with the Microsoft iSCSI initiator and MPIO driver to improve both reliability and performance. The component consists of a kernel driver (`eqldsm.sys`) and a user mode service (`EHCMservice.exe`).

When you install the MPIO DSM on a Windows operating system, it establishes and manages multiple I/O data paths to the same iSCSI target (a PS Series volume). If a fatal path failure occurs, the failure is quickly detected and I/O transparently fails over to a functioning path. The MPIO DSM recognizes and responds to a variety of network errors, device errors, and timeout conditions.

The Dell EqualLogic MPIO DSM provides the following features:

- Automatic connection management
- Increased bandwidth
- Reduced network latency
- Automatic path failure detection and failover to a functioning path
- Automatic load balancing across paths
- Support for multiple connections to a single iSCSI target (volume)
- Support for a variety of iSCSI initiators
- Per-pool connection throttling

[Figure 3](#) shows a typical multipath I/O configuration.

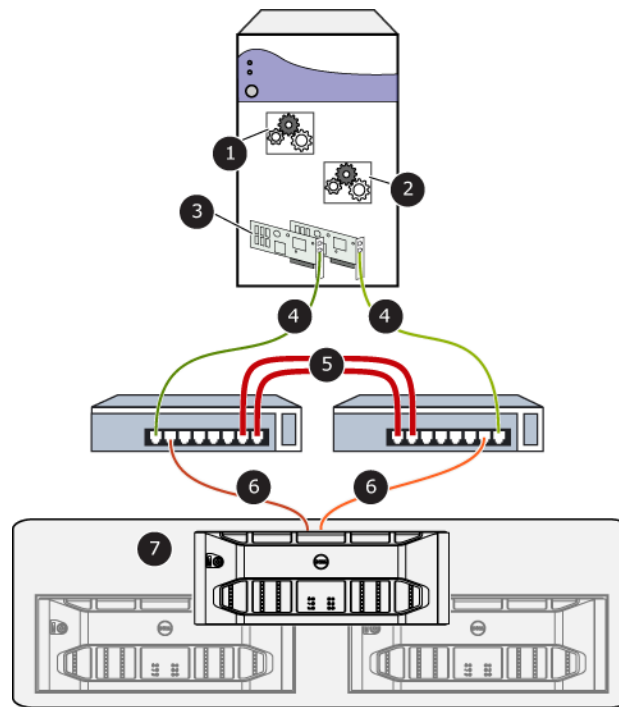
Figure 3: Multipath I/O Configuration

Table 12 describes the callouts in Figure 3.

Table 12: Callouts in Figure 3

Number	Callout Description
1	<code>eqldsm.sys</code> kernel mode driver (performs I/O path selection and error handling)
2	<code>EHCMService.exe</code> user mode service (manages iSCSI sessions)
3	Two or more gigabit Ethernet (1 Gb/sec) NICs or HBAs
4	Two or more (redundant) physical paths to dual redundant network switches
5	Two or more (redundant) physical paths provide a network switch interlink
6	Two or more (redundant) physical paths from the network switches (connected to the separate redundant controllers in each member in the PS Series group)
7	PS Series group

The number of paths created by the MPIO DSM depends on the topology of your SAN and the MPIO settings on the host computer. Every volume is distributed across one or more members in the PS Series

volume slice. The `EHCMservice` creates one or more iSCSI sessions to each volume slice. The actual number of sessions is determined through the following steps:

1. Calculate the optimal number of sessions to maximize the bandwidth between the host and the member. This calculation takes into account the speed of available host adapters and network interface cards (NICs) on each member hosting part of the volume. The algorithm will not create unnecessary sessions when there is no performance benefit. Therefore, in configurations that have limited numbers of computer and member Ethernet ports, the actual number of sessions created might be fewer than the user limits specified in the next step.

Example A—You have two 1Gb host NICs, and are connecting to a volume on members with four 1Gb Ethernet ports. The optimal number of sessions is two per member, because that number will saturate the host NICs.

Example B—You have one 10Gb host NIC, and are connecting to a volume on members with four 1Gb Ethernet ports. The optimal number of sessions is four per member, because that number will saturate the member Ethernet ports.

Example C—You have two 10Gb host NICs, and are connecting to a volume on members with one 10Gb Ethernet port. The optional number of sessions is one per member, because that number will saturate the member Ethernet ports.

2. Apply any user-configured session limits. The default behavior is to limit to two sessions per volume slice or six sessions per volume, whichever is reached first. However, you can modify these limits, as described in [Configure Multipath I/O Between a Computer and a Group on page 47](#).
3. Apply a per-pool throttle to ensure the group remains below 90 percent of the maximum number of allowed connections per pool. This throttling logic ensures the connections are equitably shared among all the pool members and all the hosts using HIT multipathing to connect to volumes on the group. See the *Dell EqualLogic PS Series Storage Arrays Release Notes* for the current configuration limits.

iSCSI sessions are distributed across all available adapters and PS Series group Ethernet ports. The `EHCMService` monitors the topology of the SAN. If you change the configuration, such as modify the number of Ethernet interfaces, or move a PS Series volume, it automatically reconfigures the MPIO DSM sessions.

The MPIO DSM and PS Series group firmware create secure CHAP credentials that enable only the `EHCMService` to add iSCSI sessions to a volume. These CHAP credentials are for internal use only and are not displayed by the Group Manager GUI or CLI.

The MPIO DSM also provides load balancing capabilities that enable you to maximize I/O throughput. The MPIO DSM has knowledge of the distributed nature of volumes on the PS Series group and uses this knowledge to route each I/O packet by using the optimal path to the volume.

See the *Host Integration Tools for Microsoft Release Notes* for specific statements concerning supported Host Bus Adapter (HBA) hardware and firmware.

Prerequisites for Configuring Multipath I/O DSM

Your computer must meet the following requirements to use MPIO:

- A supported version of Windows, as specified in the *Host Integration Tools for Microsoft Release Notes*.
- The Dell EqualLogic MPIO DSM is a subordinate module running within the Microsoft MPIO framework. All supported versions of Windows include the MPIO as a service; the installer will configure and start the service.
- Two or more supported Gigabit Ethernet (or faster) network interface cards (NICs) or host bus adapters (HBAs). See the *Host Integration Tools for Microsoft Release Notes* for more information.
- For greatest redundancy, each host adapter must be connected to a different network switch.

The PS Series group must meet the following requirements to use MPIO:

- All group members (arrays) must be running the correct firmware revision, as specified in the *Host Integration Tools for Microsoft Release Notes*.
- Each PS Series group member must have at least two, and preferably three, connected and configured network interfaces.
- For greatest redundancy, connect the PS Series network interfaces to different network switches.

Consider also your local network configuration. A typical iSCSI SAN configuration provides two groups of communication interfaces. One group is dedicated to storage data traffic and a second group is dedicated to general LAN traffic, computer intercommunication, and other purposes. Normally, these networks are discrete and maintained on separate subnets.

To maximize bandwidth, the MPIO DSM automatically uses any available network interfaces. When you configure MPIO DSM, consider restricting its access to subnets dedicated to iSCSI data traffic.

Requirements for Multipath I/O

Collect the information specified in [Table 13](#).

Table 13: Configuring Multipath I/O

Prompt	Description
Subnets included	The IP address range for subnets (in IPv4 or IPv6 format) that you intend to use for multipathing.
Subnets excluded	The IP address range for subnets (in IPv4 or IPv6 format) that you intend to

Prompt	Description
	exclude from multipathing.
Load balancing policy	By default, the MPIO DSM applies a policy of <i>least queue depth</i> . You can optionally select <i>fail over only</i> or <i>round robin</i> . See Set the MPIO Load Balancing Policy on page 51 for a complete description of these options.
Max sessions per volume slice	For volumes that span multiple group members, you can specify the maximum sessions permitted for a volume per group member. Select a value <i>n</i> in the range 1-4.
Max sessions per entire volume	For volumes that span multiple group members, you can specify the maximum session permitted for the volume. Select a value <i>n</i> in the range 1-12, where <i>n</i> is greater than or equal to the value of the max sessions per volume slice. A value that is three times the max sessions per volume slice is typical because volumes typically span up to three members. Reduce this value if you want to reduce the total number of session established to a volume.
Use MPIO for snapshots	You can specify whether to use MPIO when connecting to snapshots.
Use IPv6 or IPv4	You can specify whether to use IPv4 (the default) or IPv6, if configured.
Minimum adapter speed	You can specify the slowest acceptable speed that a NIC can have when used for MPIO. The choices are based on the speeds of the NICs available on the host machine. If only one speed is available, this field is read-only.

Configure Multipath I/O Between a Computer and a Group

Before you begin, see [Prerequisites for Configuring Multipath I/O DSM on page 46](#)

- Open the MPIO settings screen either from the ASM/ME GUI or from within the iSCSI initiator dialog box.
 - From the desktop:
 - Start the ASM/ME GUI.
 - Click MultiPath in the tree panel.
 - Click MPIO settings in the dashboard.
 - From the Microsoft iSCSI Initiator:
 - Open the iSCSI Initiator.
 - Click the Dell EqualLogic MPIO tab, then click MPIO Settings.

The `MPIO Settings` screen is displayed. See *Setting MPIO Properties* in the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Changes to the list of included or excluded subnets are effective immediately for new connections, while changes to existing connections might take several minutes.

To verify that you correctly configured Multipath I/O, use the procedures described in [View MPIO Sessions on page 49](#).

Log In to a Volume with Multipath I/O

1. Start the iSCSI Initiator Properties control panel.
2. Click the `Targets` tab after discovery of the group targets is complete.
3. Select the target, and click `Log On`. The `Log On to Target` dialog appears.
4. Select options as follows:

If you need to enter CHAP credentials, click `Advanced`, enter the information, and click `OK`.

You do not need to select the `Enable multi-path` option unless an iSCSI session to the volume already exists.

6. Click `OK`.

After you log on to a target, the Multipath I/O DSM automatically creates additional connections to that target. The DSM might wait several minutes before adding these additional sessions.

The Multipath I/O DSM does not manage persistent connections to iSCSI targets. For maximum redundancy on a computer with multiple adapters, Dell recommends that you create persistent logins to each target for each adapter.

Log Off a Volume with Multipath I/O

To log off a volume with multiple connections under Windows Server 2008 R2:

1. Click the `Targets` tab and select the target.
2. Click `Disconnect`.

To log off a volume with multiple connections when using other Windows variants, you must select and log out of each connection session as follows:

1. Click the `Targets` tab, select the target, and click `Details`. The `Target Properties` dialog box is displayed.
2. Click the `Sessions` tab.
3. Select all sessions and click `LogOff`.

If you see a message warning you that a device is in use, wait a few seconds, click the `Refresh` button, and then repeat step 3.

View MPIO Sessions

The status of the MPIO DSM is logged for display in the Dell EqualLogic MPIO tab of the iSCSI Initiator properties page. The properties page appears when you double-click the Initiator icon, or when you launch the Initiator interface from the Windows control panel.

The status tab provides:

- Details of the NIC or HBA adapters present in the system, identifying which adapters support MPIO.
- The status of MPIO sessions and paths.

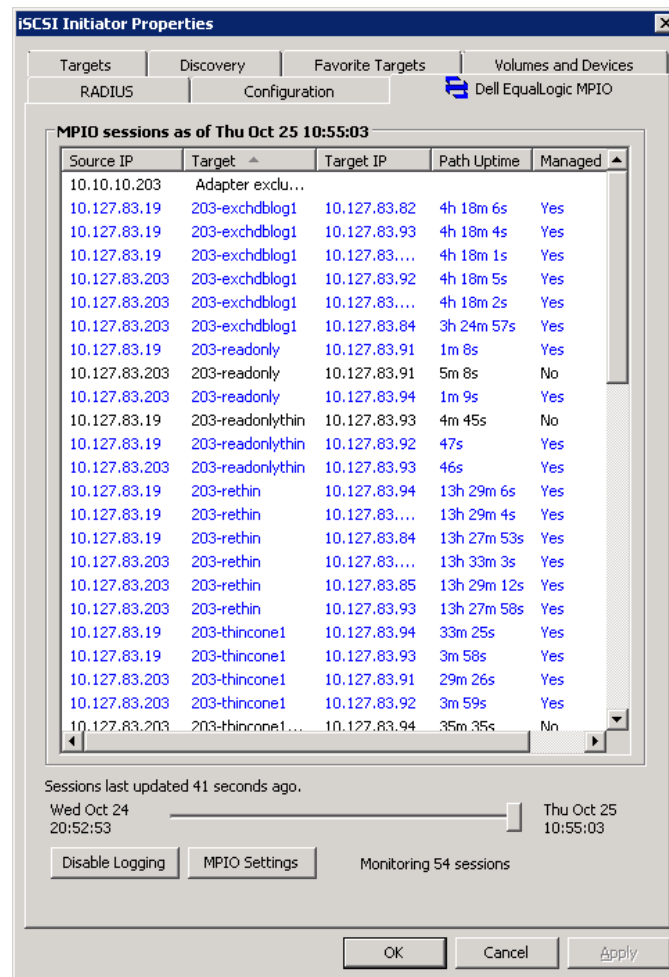
Data is stored in a cumulative log file at: `<installation_path>\EqualLogic\Logs\ehcm.log`. When the current log file is full, the logger renames it to `ehcm0.log` and deletes the previous log. Only one previous log file is retained.

To adjust the length of history stored, you can change the size of the log file by modifying the Windows registry entry under: `HKEY_LOCAL_MACHINE\SOFTWARE\Equallogic\EHCM`.

The following limits (in MB) apply to the XMLLogsize registry key:

- Default—10
- Minimum—1
- Maximum—50

The `ehcm.log` file provides data for a custom MPIO properties tab in the iSCSI initiator properties pages ([Figure 4](#)). When you launch the initiator properties, it might take up to a minute to load data from the log.

Figure 4: MPIO Properties Tab in the iSCSI Initiator

The MPIO properties tab provides the information shown in [Table 14](#).

Table 14: MPIO Log Data

Column Title	Data Description
Source IP	TCP/IP address of the link source device. This is the NIC or HBA installed in the computer that accesses an iSCSI volume.
Target	Name of the iSCSI volume that is the target of the link. When MPIO is configured, you will see multiple links.
Target IP	TCP/IP address of the PS Series array's Ethernet port. (One of the ports on the active controller).
Path Uptime	Elapsed time during which this path is connected. Significant differences in uptime indicate potential path failovers.

Column Title	Data Description
Managed	Indicates whether the sessions are actively managed. This is also indicated by the color of the text. Sessions colored blue are managed, sessions colored black are not.

The MPIO properties tab also provides the following options:

- Using the scroll bar control beneath the information pane, you can scroll back through the log file to examine MPIO status at a specific point in the current log.
- You can temporarily disable logging.
- You can change the MPIO settings. Click the button to open the ASM/ME GUI directly to the MPIO Settings screen. For detailed information on what you can change, see *Setting MPIO Properties* in the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Set the MPIO Load Balancing Policy

When you have configured multiple data pathways, it is appropriate to configure MPIO DSM to balance data traffic loads across the pathways. Choose from:

- **Least Queue Depth**—(Recommended) MPIO DSM sends SAN data traffic packets out to each available connection, with preference given to the connection that is least busy at the time it requests the I/O. This option is appropriate for most installations.
- **Round Robin**—MPIO DSM sends SAN data traffic packets over each available connection in a rotating sequence, fully utilizing all available paths.
- **Fail Over Only**—MPIO DSM uses one connection for all SAN data traffic until it times out or otherwise fails. At that time, traffic fails over to any other available path. Selecting this load balance policy causes the EHCMService to no longer add and remove additional sessions to the target.

For both Round Robin and Least Queue Depth policies, sessions to the group member containing the data are given preference over other sessions.

On Windows Server 2008 R2

1. Double-click the Microsoft iSCSI Initiator to display its properties.
2. Click the **Targets** tab and click a target (volume) that has a status of Connected to highlight and select that target.
3. Click **Devices** to display devices.
4. Click **MPIO**.
5. Use the pull-down menu underneath Load balance Policy to configure the policy for this device.

If you view the sessions tab, be aware that the MPIO DSM does not use multiple connections per session. Therefore the Load Balance Policy setting accessible through the Properties button has no effect. If the MPIO tab does not appear in the initiator control panel, you might not have selected MPIO support when installing the initiator, or you might need to reboot the computer to complete the installation.

On Other Operating Systems

1. Double-click the Microsoft iSCSI Initiator to display its properties.
2. Click the `Targets` tab, and click a target (volume) that has a status of `Connected` to highlight and select that target.
3. Click `Details` to display the `Target Properties` for the selected volume and then click the `Devices` tab to display devices.
4. Verify that the entry in the `MPIOCapable` column is `Multi-Path Support`. If the entry is anything other than that (such as `Disk Drive`), it means that either the Microsoft MPIO DSM is not properly installed, or there is a problem recognizing an HBA as MPIO-compliant.
5. Click `Advanced` to display the `Device Details`, then click `MPIO`.
6. Use the pull-down menu underneath `LoadBalancePolicy` to configure the policy for this device.

If you view the sessions tab, be aware that the MPIO DSM does not use multiple connections per session, therefore the Load Balance Policy setting accessible through the `Connections` button has no effect.

If the MPIO tab does not appear in the initiator control panel, you might not have selected MPIO support when installing the initiator, or you might need to reboot the computer to complete the installation.

6 Use the VDS Provider

The Dell EqualLogic Virtual Disk Service (VDS) provider enables you to use Microsoft VDS version 1.1 and Microsoft Storage Manager for SANs to create and manage volumes in a PS Series group.

VDS Provider Requirements

To use VDS, you need:

- A PS Series group running the minimum supported revision
- A supported version of Microsoft Windows Server (see the *Host Integration Tools for Microsoft Release Notes*)
- On the computer, a supported version of the Microsoft iSCSI Software Initiator (see the *Host Integration Tools for Microsoft Release Notes*)
- On the computer, you must install the VDS provider, as described in [Install HIT on page 9](#)
- Access to the PS Series group by Microsoft services (VDS and VSS) running on the computer. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

VDS Provider Guidelines and Restrictions

Use the VDS provider in conjunction with Microsoft VDS version 1.1 and Storage Manager for SANs to create and manage volumes in a PS Series group. Guidelines and useful information about these configurations are listed below:

- **Storage Pools**—The Dell EqualLogic VDS provider provides support for storage pools on Windows Server 2008 R2 and later platforms. This enables you to use a VDS management application such as `DiskRAID` to enumerate and create LUNs in storage pools other than the default pool.
- **Provisioning Volumes**—Dell recommends that you select a method by which to provision volumes and use that method consistently to create and manage volumes, with the exception of activities that explicitly require a particular method. For example, if you create a volume using Storage Manager for SANs, use that method to manage the volumes, except when you must use Group Manager to modify snapshot settings and configure replication.
- **Access Controls**—If you are using Microsoft Storage Manager for SANs to create a volume in a PS Series group, it automatically creates access controls for the volume. If CHAP is used, the user name is always the iSCSI initiator name (as required by Microsoft VDS rules). You can also specify a password. Storage Manager for SANs then automatically creates a corresponding access control record and local CHAP account, if CHAP is used, in the group. Always use Storage Manager for SANs to manage these access controls.

However, for a volume created with Storage Manager for SANs, you can use the Group Manager GUI or CLI to create additional access controls in the group. Always use Group Manager to manage these access controls.

- **Snapshot Settings**—A volume created with Storage Manager for SANs inherits the group-wide snapshot settings (snapshot reserve, warning percentage, and space recovery policy).
- **VDS Volumes in Group Manager**—Volumes created by using Storage Manager for SANs appear in the Group Manager Volume Access window with `yes` in the VDS column.

Simple Target and LUN Naming

The Dell EqualLogic VDS provider implements the simple target configuration. When you use Microsoft Storage Manager for SANs to create a LUN, the Dell EqualLogic VDS provider automatically creates an iSCSI target and associates that target with the LUN. When you delete a LUN, VDS deletes the associated iSCSI target. You cannot independently manage LUNs and targets.

A target's iSCSI name and friendly name is based on the LUN name for ease of use. Because the LUN name is not specified at LUN creation time, the Dell EqualLogic VDS provider delays setting these target names to allow the creator to first set a more descriptive LUN name. Dell recommends that VDS clients set the friendly name before querying the target properties so that the desired friendly name can be used in the target name. When a VDS client has queried the properties of the associated target, the iSCSI name cannot be changed even if the LUN name is updated. The target's friendly name will continue to be updated on LUN name changes so the two values match.

When using Storage Manager for SANs or diskraid to create a LUN, the LUN friendly name is correctly set before the target is created. If you use Storage Manager for SANs to create multiple LUNs, wait until each LUN is created and displayed before creating any additional LUNs. This avoids a situation in which two LUNs are created and renamed simultaneously, which can result in the target name on the second LUN being created before the LUN name is set.

Import VSS Snapshots

To import VSS snapshots of a volume that you created by using Storage Manager for SANs, the computer must present access credentials. The credentials must match an access control record that you configured in the PS Series group for all snapshots related to the volume:

1. Configure an access control record in the PS Series group that applies to the target volume's snapshots.
2. (Optional) Configure a local CHAP account in the PS Series group only if you protected access to snapshots by using CHAP. Either:
 - Specify the same CHAP user name and password that you specified when you created the volume.
 - Specify different credentials.

3. Specify the CHAP username and password when prompted, or use ASM/ME to specify the user name and password in the Properties Password dialog box.

This user name and password now applies to all VSS snapshots created in the group and accessed from the computer.

Modify

If you change access controls related to Microsoft service access to the PS Series group or computer access to VSS snapshots, make sure you make the necessary changes on both the computer and the group as follows:

- For volumes created by using Storage Manager for SANs, use the same method to change the access controls on both the computer and the group.
- For VSS snapshots of volumes created with Storage Manager for SANs:
 - Use the Group Manager GUI or CLI to modify the snapshot access control records and CHAP accounts, if CHAP is used.
 - On the computer, use the ASM/ME Properties Password dialog box to specify the CHAP user name and password.
- For Microsoft service access to the group:
 - Use the Remote Setup Wizard to modify the computer configuration.
 - In the group, use the Group Manager GUI or CLI to modify VSS/VDS access control records and CHAP accounts, if CHAP is used.

About Creating a Volume Using Storage Manager for SANs

To use Microsoft Storage Manager for SANs to create a volume in a PS Series group, configure the group and install the VDS provider.

Volumes created with Storage Manager for SANs use the default group-wide volume snapshot settings for snapshot space, warning level, and action to take when snapshot space is exceeded. You can use the Group Manager GUI or CLI to change the snapshot settings.

When Storage Manager for SANs creates a volume in a group, it automatically creates access controls for the volume. If CHAP is used, the user name is always the iSCSI initiator name. You can optionally specify a secret (password).

Storage Manager for SANs automatically creates an access control record in the group with matching access controls, in addition to a local CHAP account, if you use CHAP.

The volume access controls that Storage Manager for SANs creates in the group also apply to snapshots of the volume. Once these credentials are assigned, you cannot change them using the Group Manager

GUI or CLI. Instead, you must use Storage Manager for SANs to change the CHAP credentials. You can set up additional access controls for a volume created with Storage Manager for SANs by using normal Group Manager access control records.

Start Storage Manager for SANs

To start Storage Manager for SANs, click **Start**, then **Administrative Tools**, then **Storage Manager for SANs**.

Because of the way it gathers storage information, the Microsoft Storage Manager for SANs application incorrectly reports the total capacity and used space of a PS Series group. Use the Group Manager GUI to obtain accurate free space information. You can also use the Provision Storage Wizard (found within Storage Manager for SANs), which reports the size of actual storage space available on the group as maximum volume size.

See the Microsoft Storage Manager for SANs documentation for more information about using this utility.

7 Use VMM with the Dell EqualLogic SMP

This release of the Host Integration Tools supports the System Center Virtual Machine Manager (SCVMM, or VMM) 2012 SP1 and 2012 R2. The scope of this chapter is limited to essential storage management tasks in VMM with the Dell EqualLogic Storage Management Provider (SMP) for PS Series storage.

Using ASM/ME, you can create Smart Copies and collections of rapid-provisioned VMs created by VMM. You can also restore from them (however, selective restore is not supported). For more information, see the chapter *Using ASM/ME with Hyper-V* in the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide*.

Refer to the complete VMM documentation for all other tasks, such as cloud and tenant configuration, creating service templates and deployment configurations, and other topics.

For more information on VMM, see the following URL: <http://www.microsoft.com/systemcenter/>

Install the Dell EqualLogic Storage Management Provider

The Dell EqualLogic Storage Management Provider (SMP) is installed as part of the Host Integration Tools. It is an optional component selected by default when installing on Windows Server 2012 or greater or Windows 8 or greater systems.

To use SMP, you must configure access from the host to one or more PS Series groups. You can use either ASM/ME or the PowerShell Tools, which are always installed with the Host Integration Tools kit. See *Install HIT on page 9*.

Configure the Dell EqualLogic Storage Management Provider

1. Configure access to the Dell EqualLogic PS Series groups you intend to use for provisioning on the VMM management host.

You can configure group access in the following ways:

- Using the Dell EqualLogic PowerShell Tools group access management cmdlets such as `New-EqlGroupAccess`. See *Configure VMM on page 3* and the *Dell EqualLogic PowerShell Tools Reference Guide* for more information.
- Use the ASM/ME GUI to configure PS Series group access. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

Note: If you are configuring Single Sign-On (SSO) access for a particular PS Series group, the logon account for the VMM service (`vmm.service.exe`) must be enabled for management on that group. Alternatively, you can enable an AD user group on the group if the VMM service account is part of that AD user group. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

VMM does not allow configuring a separate Run As account to manage SMP. Refer to the Microsoft VMM documentation regarding correct setup of the service logon account.

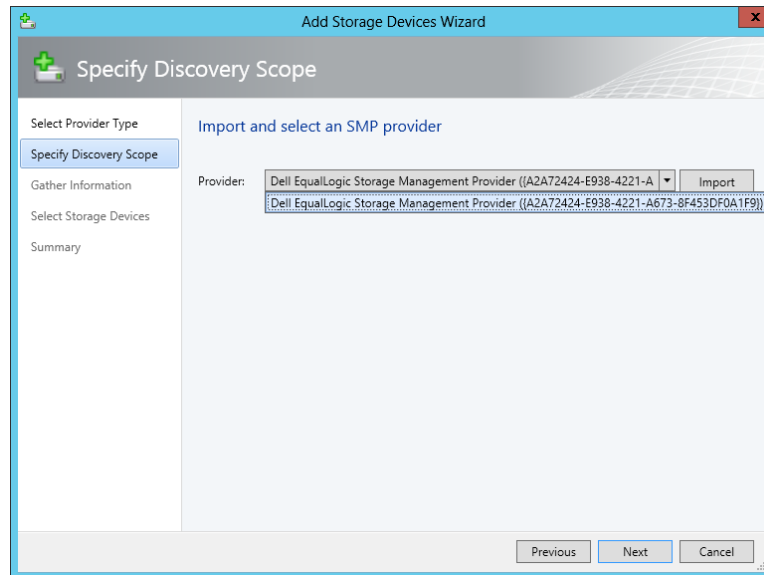
2. In the VMM server GUI, configure “PowerShell/SMP access (PS Authentication).”
3. Use the VMM Command Shell (VMM PowerShell environment) and run the `Import-SCStorageProvider` command. Alternatively, import SMP using the VMM Console GUI. See [Import the SMP through the VMM GUI on page 58](#).

Create a Classification for Dell EqualLogic Storage Resources

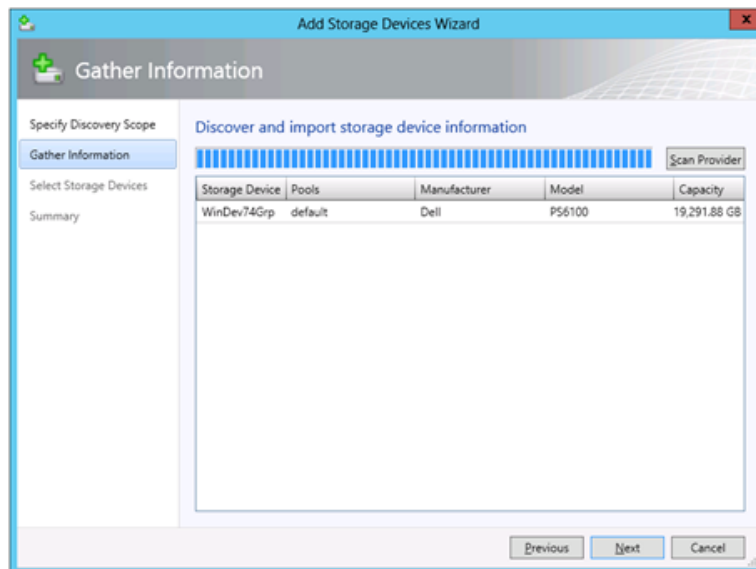
1. In the VMM Console GUI, click `Storage`, then `Classification and Pools`, then right-click and select `Create Classification`.
2. Enter a unique classification name (for example, `EqualLogic`) and optionally enter a description, then click `Add`.
3. Confirm that the new classification is displayed in the `Classification` view.
4. Continue with [Configure PS Series Groups on page 61](#).

Import the SMP through the VMM GUI

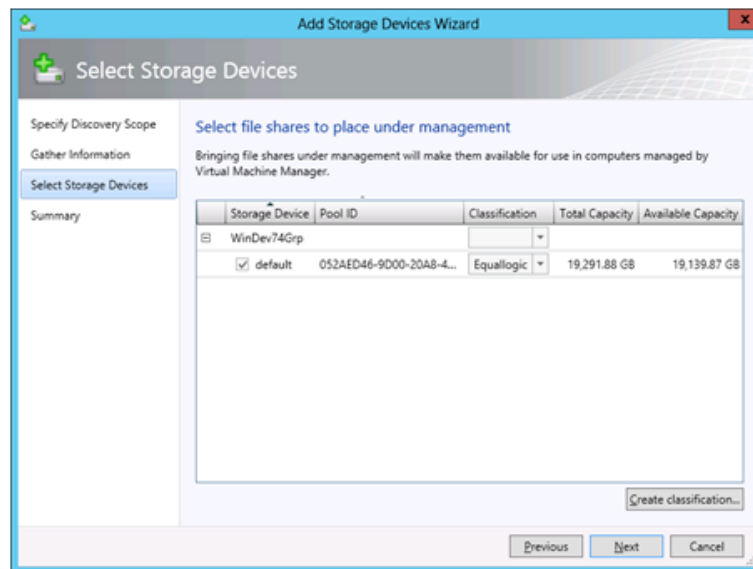
1. Open the VMM Console GUI and switch to the `Fabric` workspace view in the left bottom workspace selection pane.
2. Select `Providers` under the `Storage` sub-tree and right-click to select `Add Storage Devices`.
3. On the `Select Provider Type` screen, select the option “Add a storage device that is managed by an SMP provider,” then click `Next`.
4. On the `Specify Discovery Scope` screen ([Figure 5](#)), select “Dell EqualLogic Storage Management Provider” from the `Provider` drop-down list, click `Import`, then click `Next`.

Figure 5: Specify Discovery Scope Screen

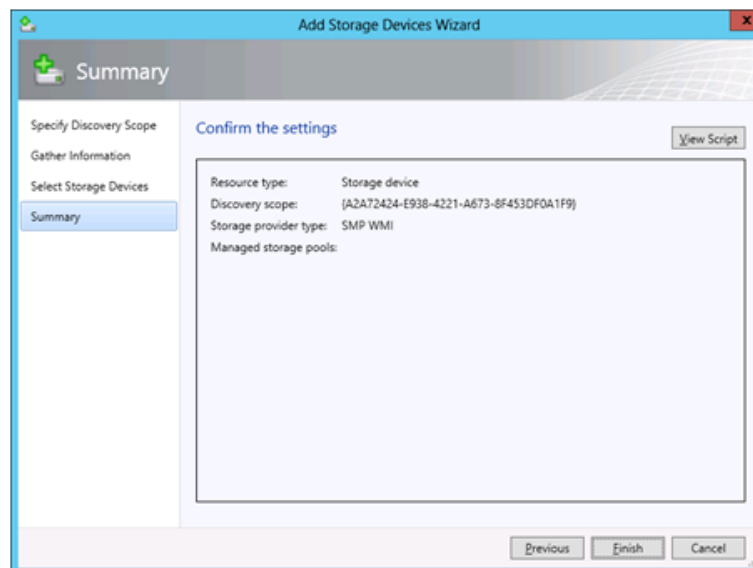
5. Verify that the configured PS Series groups (in this example, WinDev74Grp) are discovered ([Figure 6](#)), then click **Next**.

Figure 6: Gather Information Screen

6. Select one or more pools ([Figure 7](#)) on the configured groups that you intend to use for provisioning storage in VMM, then click **Next**.

Figure 7: Select Storage Devices Screen

7. Confirm the configuration on the Summary screen (Figure 8), then click **Finish**.

Figure 8: Summary Screen

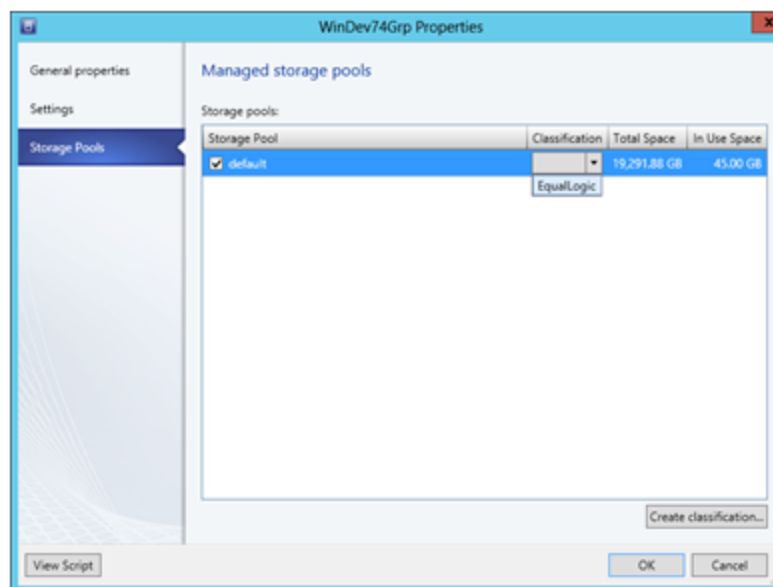
When the Dell EqualLogic SMP is successfully added the PS Series groups will appear in the Arrays view (click **Fabric**, then **Storage**, then **Arrays** in the bottom-left pane).

Continue with *Configure Group Access on Managed Hosts and Clusters on page 61*.

Configure PS Series Groups

1. In the VMM Console GUI, right-click a PS Series group in the Arrays view (click **Fabric**, then **Storage**, then **Arrays**) and open the Properties dialog box.
2. In the Properties dialog box ([Figure 9](#)):
 - a. Click the Storage Pools tab.
 - b. Select the pools you intend to use for storage provisioning.
 - c. Select the classification you created from the Classification drop-down list.
 - d. Click **OK**.

Figure 9: Storage Pools Properties Screen



3. Confirm that the EqualLogic classification is displayed in the Classification view (click **Fabric**, then **Storage**, then **Classification** and **Pools**).
4. Continue with [Configure Group Access on Managed Hosts and Clusters on page 61](#).

Configure Group Access on Managed Hosts and Clusters

VMM does not automatically configure or maintain iSCSI discovery target portals settings on managed hosts based on the provider and PS Series group configuration in the Dell EqualLogic SMP.

You must configure iSCSI target portals for every node or host you are planning to use in storage provisioning tasks using Dell EqualLogic SMP so that volumes created in provisioning tasks can be connected on the managed hosts.

If the hosts are part of a HIT group, you can use any of the following to configure group access for all the hosts at once:

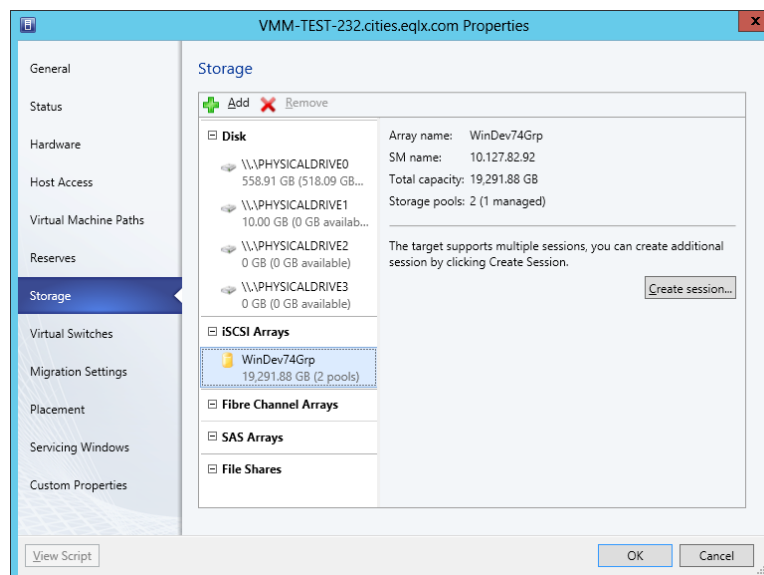
- VMM Console GUI
- ASM/ME GUI
- PowerShell Tools `New-EqlGroupAccess` cmdlet

See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* or the *Dell EqualLogic PowerShell Tools Reference Guide* for more information.

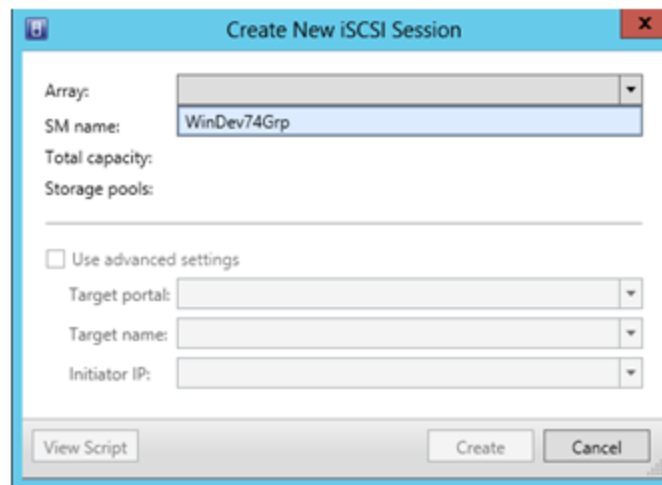
To configure iSCSI target portals using the VMM Console:

1. In the Fabric workspace view, right-click a host or a cluster node and select Properties.
2. In the Properties dialog box, click the Storage tab, then expand the iSCSI Arrays node (Figure 10). Select the PS Series group and click `Create Session`.

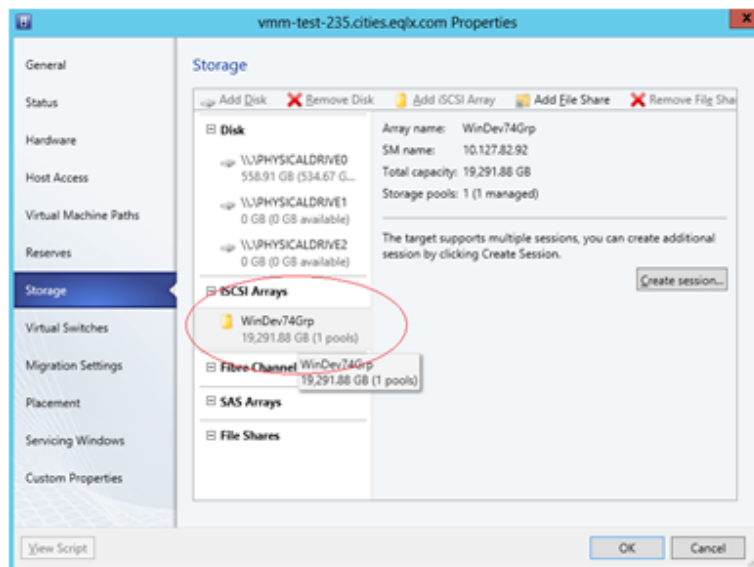
Figure 10: Storage iSCSI Arrays Screen



The Create New iSCSI Session dialog box opens (Figure 11).

Figure 11: Create New iSCSI Session Screen

3. Confirm that the PS Series group was added (Figure 12), then click OK.

Figure 12: Confirm Array

4. Continue with [Configure Storage for VM Rapid Provisioning on page 63](#).

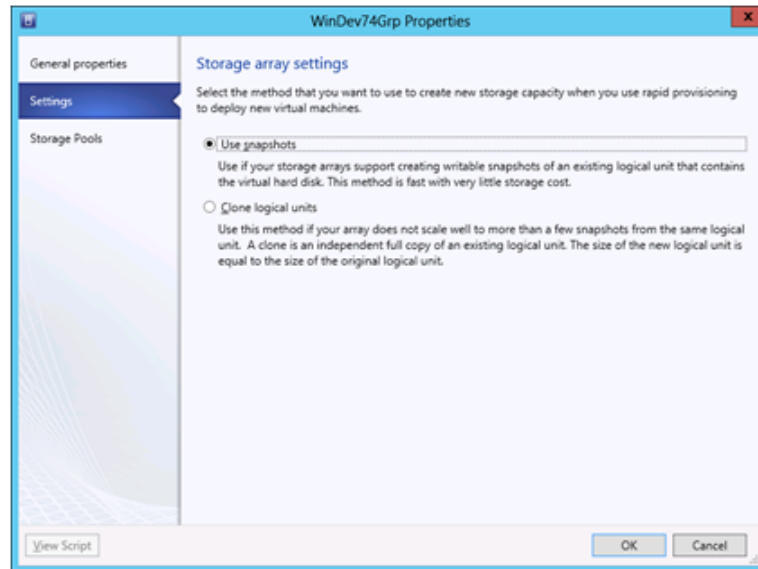
Configure Storage for VM Rapid Provisioning

Dell EqualLogic SMP supports rapid VM provisioning through the use of thin clones of template volumes.

Before performing rapid provisioning operations:

1. Expand the Storage node and select Arrays.
2. Right-click the PS Series group and select Properties.
3. In the Settings tab, make sure that the provisioning method is set to “Use snapshots” for the group intended for rapid provisioning. This setting enables use of thin clones for these tasks if the volume is a template volume (Figure 13).

Figure 13: Storage Array Settings



The other setting—Clone logical units—will result in creating regular (fully provisioned) clones of the template volume, and is not recommended for rapid provisioning using Dell EqualLogic SMP in VMM since it will not scale.

The Storage Array Settings apply to individual PS Series groups and are not a global configuration for Dell EqualLogic SMP.

4. Click **OK** to close the Properties panel.

Create a VM Template for the Library Share

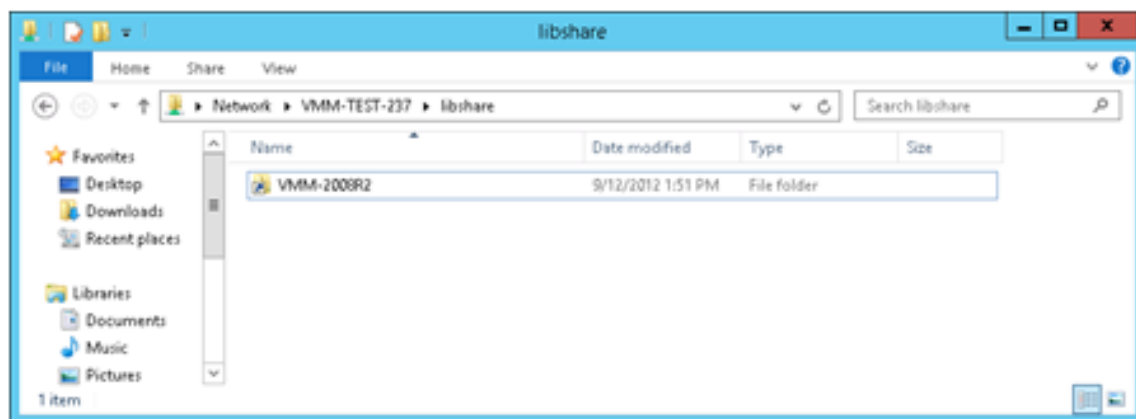
1. On the PS Series group, create a regular volume allocating enough space to store the VHD for the VM. The template volume must have a VHD to provision VMs.
2. Copy the VHD file to the volume.
3. Using the Group Manager GUI or CLI, or the PowerShell cmdlet `ConvertTo-EqlTemplateVolume`, convert the volume to a template.

When a regular volume is converted to a template it is set to read-only and the data on it cannot be changed unless the template is converted back to a regular volume. See the Dell EqualLogic Group Manager Online Help or the *Dell EqualLogic PowerShell Tools Reference Guide* for more information.

4. Set the volume online, then log into the volume from the library host.
5. Mount the template volume to a library share configured on one of the VMM library hosts.

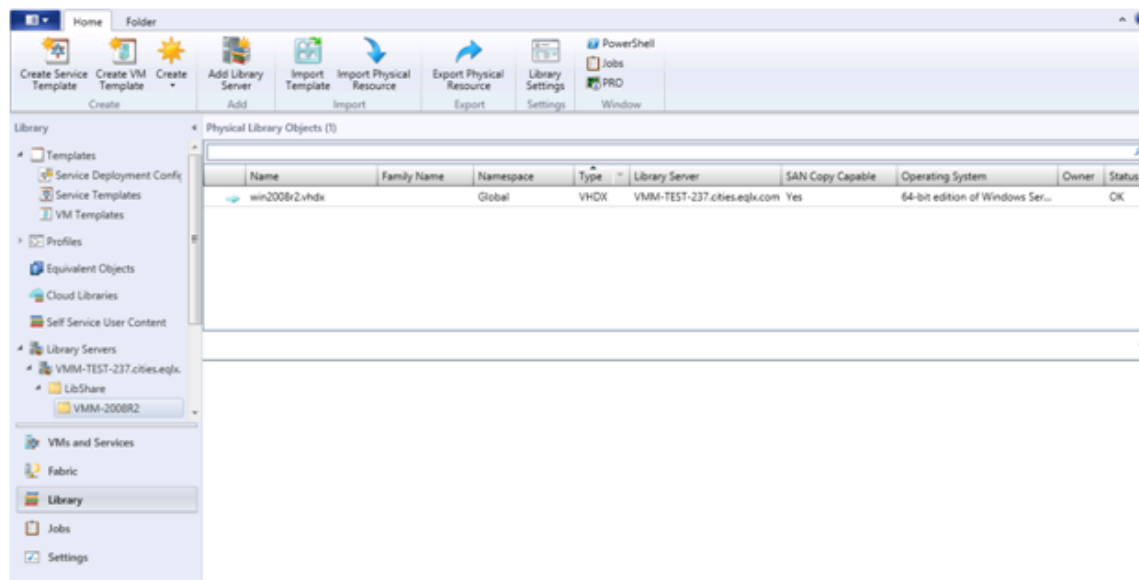
For example, in [Figure 14](#), the library share is visible on one of the library hosts, where the LibShare folder is a configured share on the library server VMM-TEST-237, which has a template volume mounted under VMM-2008R2. This template volume stores the VHD for Windows 2008 R2.

Figure 14: Library Share on Library Host



Your library host might be configured to be separate from your VMM management host, depending on your particular VMM deployment. If your library server is different from the VMM management host, the library server must be configured to access the template volumes used for provisioning. Configuring the VMM library server is outside the scope of this document.

6. Use the VHD on the volume to create a VM template. You can explore the discovered VHDs in the Library Servers (click Library workspace, then Library Servers, then Server or Share). See [Figure 15](#)

Figure 15: Library Servers in VMM

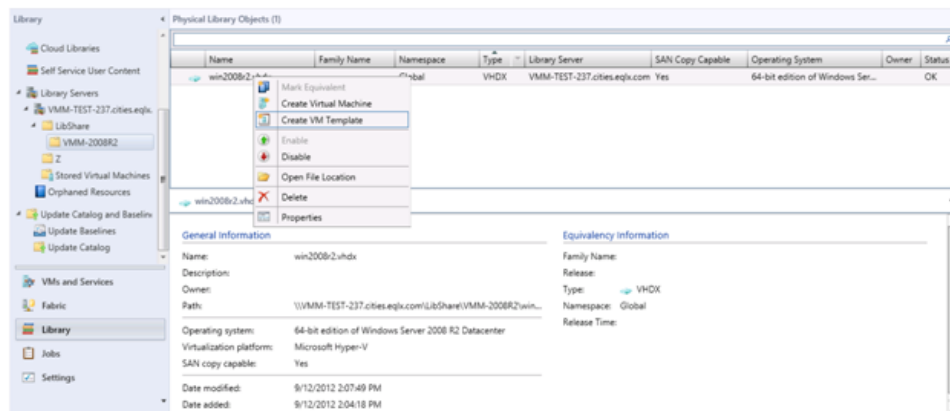
If configured correctly, when you open the library host, the discovered VHD is displayed, and shows a “Yes” in the property field labeled `SAN Copy Capable`. This setting ensures that thin clones of the underlying template volume are used instead of copying data across the network during VM provisioning.

7. Because the template volume was created outside of VMM, update the Dell EqualLogic SMP in VMM before you refresh your library resources:
 - a. Navigate to the Providers view in the Fabric workspace (click Fabric, then Providers).
 - b. Right-click the Dell EqualLogic Storage Management Provider and run the Rescan command from the menu. (The Refresh option retrieves the current state of the provider cache, but the Rescan option forces a rescan of the cache before refreshing the storage resources.)
8. Continue with [Create a VM Template from a VHD on page 66](#).

Create a VM Template from a VHD

You can create a VM using the VMM GUI, as described below, or using the VMM Command Shell and running the `New-SCVirtualMachine` cmdlet.

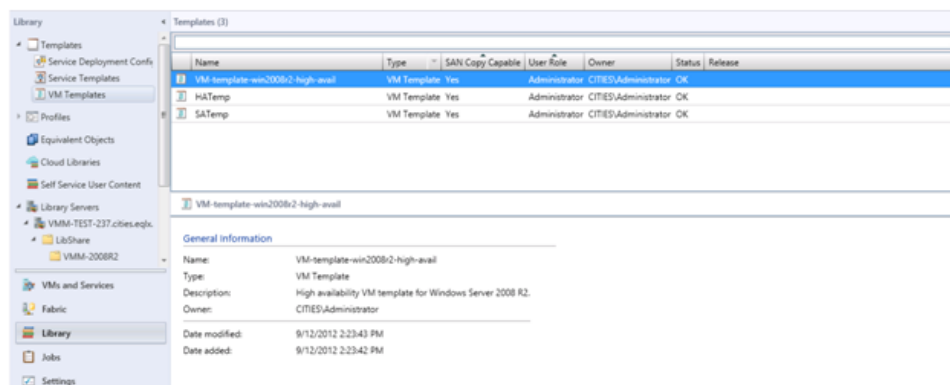
1. Click Library, then Servers to open the library resources view.
2. Right-click a VHD and select Create VM Template ([Figure 16](#)).

Figure 16: Create VM Template Screen

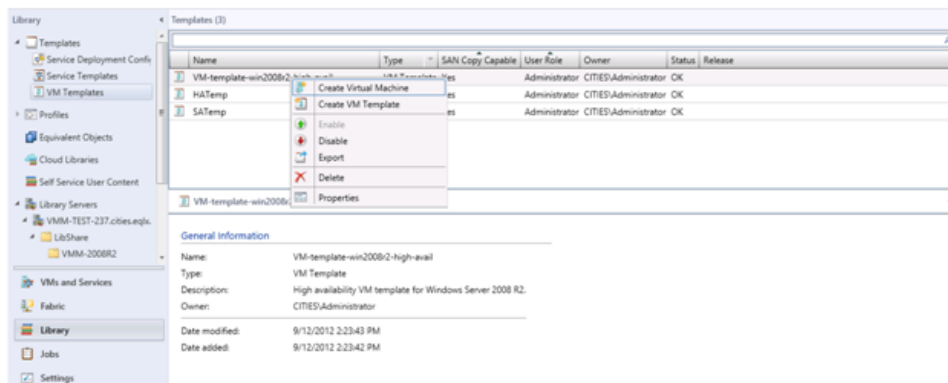
3. In the Create VM Template wizard, enter the template name and an optional description, then click Next.

For further information about configuring VM template, see the Microsoft VMM documentation.

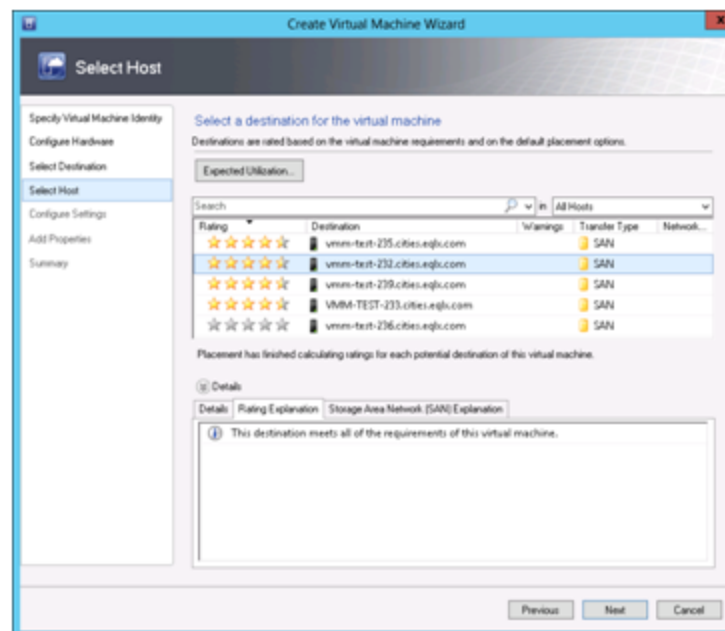
4. Make sure the new template is displayed under the VM Templates view in the Library workspace (click Library, then Templates, then VM Templates). Also confirm that the VM Template says Yes in the SAN Copy Capable property field. This setting ensures that thin clones of the underlying template volume are used instead of copying data across the network during VM provisioning (Figure 17).

Figure 17: VM Templates View

5. To create a VM from the new template, right-click the template, then select Create Virtual Machine (Figure 18).

Figure 18: Create Virtual Machine Menu Option

6. In the Specify Virtual Machine Identity screen of the Create Virtual Machine wizard, enter a VM name and optional description, then click **Next**.
7. In the Select Host screen, select the host to use as the target for VM deployment, then click **Next**. The Transfer Type column specifies the method used for VM deployment. For rapid provisioning, make sure the Transfer Type method says SAN (Figure 19).

Figure 19: Select Host Screen

8. Verify that the new VM is available in the VMs and Services view under a particular host, cluster, or private cloud.

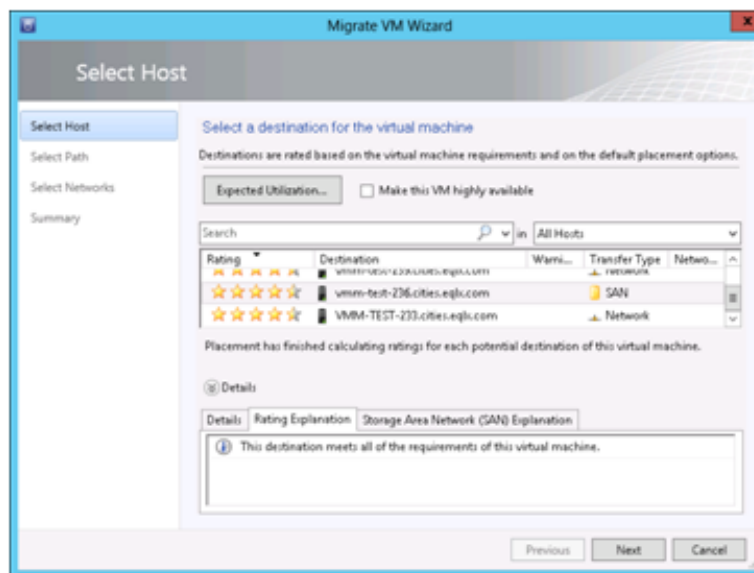
For more information about VM deployment, see the Microsoft VMM documentation.

9. Continue with *Migrate the Rapid-Provisioned VMs on page 69*.

Migrate the Rapid-Provisioned VMs

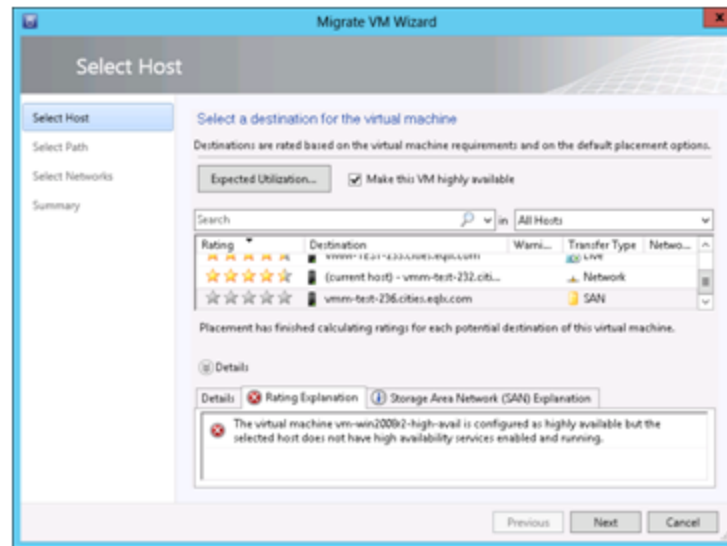
1. In the VMs and Services workspace view, right-click the VM and select Migrate Virtual Machine.
2. In the Migrate VM wizard, select the host or cluster node to use as the target for migration, then click **Next** (Figure 20).

Figure 20: Migrate VM Wizard—Select Host Screen



In a cluster on which VM is already running, VMM will use Live migration. SAN migration will be used across different clusters or standalone hosts, and will be enabled if the access to the PS Series group for the template volume is correctly configured on the target host. Unlike Live migration, the VM is saved on the source host and restored on the target host.

The ability to migrate a particular VM depends on the availability setting (high or standard) and the properties of the target host (standalone or cluster node). For more information about these limitations, click the Rating Explanation tab (Figure 21).

Figure 21: Rating Explanation Tab

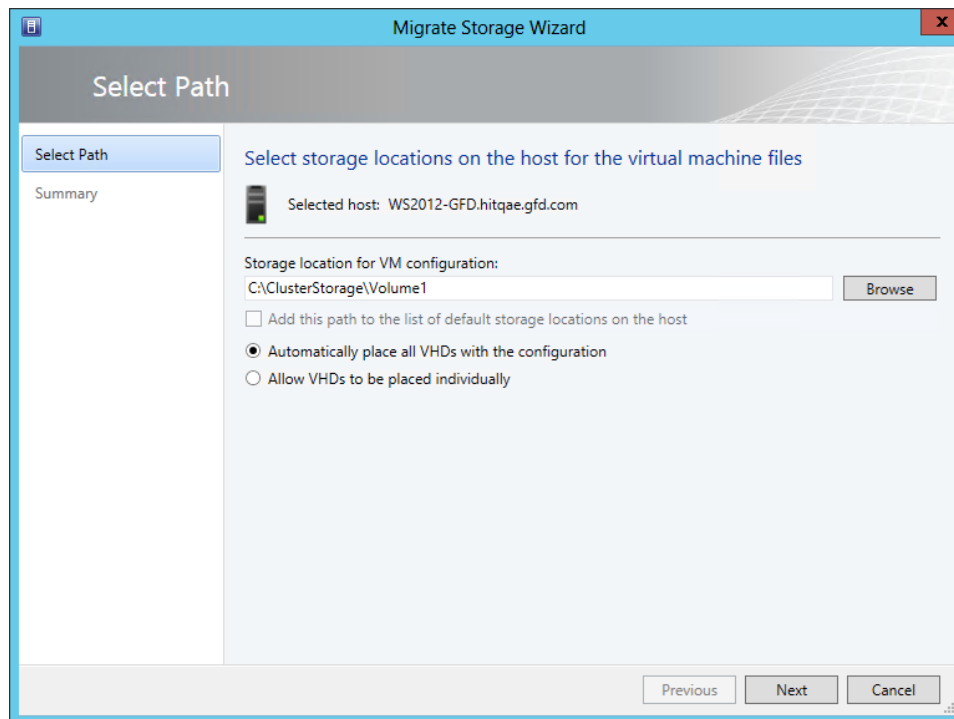
3. Continue with the remaining screens in the wizard. If the migration is successful, the VM is displayed under the target host in the VMs and Services workspace view.

For more information about VM migration, see the Microsoft VMM documentation.

Migrate Storage of a Deployed VM to Another Location

As needed, you can migrate the storage of a deployed VM from a CSV volume to a different CSV volume, or from a non-CSV volume to a CSV volume.

1. In the VMs and Services workspace view, right-click the VM and select Migrate Storage.
2. In the Migrate Storage wizard, browse to the CSV or available storage to use as the target for migration, then click **Next** (see [Figure 22](#)).

Figure 22: Migrate Storage Wizard

3. Review the chosen settings and click **Move** to complete the operation.

Troubleshoot SCVMM Issues

VMM relies on storage providers such as Dell EqualLogic SMP when performing storage provisioning tasks. When using Dell EqualLogic SMP loss of connectivity to the managed PS groups may adversely affect these operations. Note that connectivity has to be ensured on the VMM management host as well as all managed hosts or clusters involved in provisioning tasks using SMP.

The two most common causes of loss of connectivity to PS Series groups are:

- Incorrect or invalid credentials to the group. For example, user credentials have changed on the group and have not been updated on the VMM management host. If you enabled SSO (single sign-on) when you configured the group, authentication failures might also be caused by the status of the account in Active Directory (for example, expiration of account credentials and possibly other policies). See your Active Directory documentation for further steps in troubleshooting these situations.
- Actual loss of network connectivity to the group for a number of different reasons, including but not limited to the group being temporarily offline (for example, for maintenance).

Troubleshooting PS Series group connectivity issues is outside the scope of this document; however, after connectivity has been restored, do the following to verify correct configuration of storage resources on the VMM management host:

1. Refresh or rescan the Dell EqualLogic SMP in VMM.

Rescanning can be more time consuming than refreshing as it invalidates the provider cache across all of the configured storage groups. Rescanning retrieves objects from the PS Series groups and updates the local cache in the provider. Refreshing updates the state of VMM by reading the objects from the provider cache without invalidating the cache.

2. After starting a refresh or rescan operation, view the status of the job in the Jobs workspace.
3. When the job completes, return to the Providers view in the Fabric workspace (click Fabric, then Providers) to confirm that the status of the Dell EqualLogic SMP is Responding.
4. If the SMP status is Not Responding, make sure the PS Series group is accessible to the VMM Host by doing one of the following:

- Use the PowerShell Tools cmdlet `Get-EqlGroupAccess` to verify the group is configured. If the group does not appear, then use the `New-EqlGroupAccess` to configure the group. See the *Dell EqualLogic PowerShell Tools Reference Guide* for more information.
- Use the ASM GUI and configure access to the group in the PS Group Access settings screen. Click Add PS Group to add your group. See the *Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition User's Guide* for more information.

To test availability of storage resources from a particular group run the PowerShell Tools cmdlet `Get-StorageSubSystem` and make sure the group is listed in the output.

After confirming that the group is accessible, repeat step 2.

5. Make sure that storage resources on the library shares are accessible doing the following:

Open an iSCSI session from “Server Manager” of VMM.

- a. Make sure the iSCSI targets for the template volumes are shown as connected; if not, reconnect them.
 - b. Open Disk Management (click Administrative Tools, then Computer Management, then Disk Management) and make sure the disk corresponding to the active iSCSI target is currently online. Set the disk online if needed.
 - c. Make sure that the volumes still have the correct access paths (mount points) under the library shared folder.
 - d. Refresh the library shares in VMM Library workspace view (click Library, then Library Servers).
6. In the Library workspace view, right-click VM Templates and select Refresh from the menu.
 7. Confirm that both the VHD and VM template resources are enabled for SAN operations in the SAN Copy Capable property field. If correctly configured, this property says Yes. This ensures that rapid provisioning is enabled for these resources.

To troubleshoot connectivity on the managed hosts, make sure that PS Series group access is correctly configured (for example, by running the PowerShell Tools cmdlet `Get-EqlGroupAccess`) and make sure the iSCSI targets for volumes deployed to these hosts are correctly connected.

Supported SMP PowerShell Cmdlets

The PowerShell cmdlets in [Table 15](#) invoke Dell EqualLogic SMP functionality. Refer to your Microsoft PowerShell documentation for full details.

Table 15: Supported PowerShell cmdlets for EqualLogic SMP

Cmdlet	Description
Get-StorageProvider	Retrieves provider information
Get-StorageSubSystem	Retrieves storage subsystem information. Reports group information as well as features supported in EqualLogic provider implementation
Get-StoragePool	Retrieves storage pool information
Get-VirtualDisk	Retrieves particular volumes or snapshots
Get-MaskingSet	Retrieves particular masking sets
Get-InitiatorId	Retrieves particular initiator Id objects
Get-TargetPort	Retrieves target port information for volumes
Get-TargetPortal	Retrieves target portal information for a subsystem (EqualLogic group)
Get-PhysicalDisk	Retrieves physical disk information from the group – list physical disks in individual members
Get-ResiliencySetting	Retrieves resiliency setting for a storage pool (mapped to RAID setting on a member)
Get-VirtualDiskSupportedSize	Retrieves information regarding supported volume sizes in a particular storage pool
New-VirtualDisk	Creates a volume
New-VirtualDiskSnapshot	Creates a snapshot for a volume, or creates thin clone for a template volume
New-VirtualDiskClone	Clones a volume
New-StorageSubsystemVirtualDisk	Creates a volume on a particular storage subsystem (group)

Cmdlet	Description
New-MaskingSet	Creates a new masking set for a volume – creates a new ACL table for the volume
Remove-VirtualDisk	Sets the volume offline and deletes it. This cmdlet is also valid for snapshots since they are represented by VirtualDisk objects.
Show-VirtualDisk	Adds ACL entries to a MaskingSet associated with a volume
Hide-VirtualDisk	Removes ACL entries from a masking set associated with a volume
Remove-MaskingSet	Removes a masking set; deletes all ACL entries from a volume
Remove-InitiatorIdFromMaskingSet	Removes an initiator from a masking set; removes an ACL entry with this initiator name
Remove-VirtualDiskFromMaskingSet	Removes a virtual disk from a masking set; removes the virtual disk from a masking set which results in deleting the masking set itself
Remove-TargetPortFromMaskingSet	Removes a target port from a masking set; removes the target port from a masking set which results in deleting the masking set itself
Update-StorageProviderCache	Invalidates the provider cache, entirely or specific to a particular object and discovery level
Enable-PhysicalDiskIndication	Enables LED blinking on the member that owns this physical disk. The cmdlet operates on the member rather than an individual physical disk in that member
Disable-PhysicalDiskIndication	Stops LED blinking on the member that owns this physical disk

8 Use the HPC iSCSI Provider

Microsoft supports iSCSI storage in its High-Performance Compute Cluster software, HPC Server. This support appeared in the Windows Server 2008 R2 version. iSCSI support allows HPC nodes to boot from iSCSI volumes, and allows the HPC server to provision those volumes. To enable all this, a vendor-specific HPC iSCSI Provider is required. This version of Host Integration Tools includes this provider.

About the Dell EqualLogic HPC iSCSI Provider Installation

The Dell EqualLogic HPC iSCSI Provider is installed automatically with the rest of the Host Integration Tools. If you are building an HPC Server, you should install the Microsoft HPC Server package first, followed by the Host Integration Tools. During installation, the Host Integration Tools register the iSCSI Provider with the HPC Server, enabling the HPC Server's iSCSI provisioning.

If you uninstall and then reinstall the HPC Server, you will need to reinstall the Host Integration Tools so it can re-register with the HPC Server.

Configure the PS Series Array

The HPC iSCSI Provider requires an array running at least version 5.0 of the PS Series array firmware. Previous firmware versions do not support template volumes, which are required by the iSCSI Provider.

In order to use the Dell EqualLogic HPC iSCSI Provider, you will need to enable access to the VDS/VSS Control Volume on your PS Series array. The easiest way configure access to the VDS/VSS Control Volume is using Remote Setup Wizard. See [Remote Setup Wizard on page 27](#) for instructions.

If access to the VDS/VSS Control Volume is not configured, the HPC iSCSI Provider will report errors like “failed to create tunnel to group” when attempting to set up volumes for HPC nodes.

HPC iSCSI Provider Settings

The HPC iSCSI Provider has settings that can be changed using a graphical tool, `EqlHPCSettings.exe`. This tool is available from the Start menu. To launch it, click **Start**, then **Programs**, then **EqualLogic**, then **HPC iSCSI Provider Settings**. If you installed Host Integration Tools in a different directory, specify that installation directory when you launch the tool.

The settings for the HPC iSCSI Provider are described in [Table 16](#).

Table 16: HPC iSCSI Provider Settings

Setting	Default Value	Description
New Volume Size	80,000 MB	The size of all volumes created by the iSCSI HPC Provider. All HPC volumes are created thin-provisioned, so they will not occupy this much space on the group. Changing this value will not affect existing volumes already created by HPC.
Pool Name for HPC Volumes	default	The pool in which to create the volumes. This pool must exist on the PS Series group in use.
Base Volume Provisioning	10%, 80%, 100%	When thin-provisioned volumes are created, they are assigned a minimum, maximum and warning level value. The minimum value is the amount of storage to assign to the volume immediately. As data is written to the volume, additional storage will be assigned to it as needed. If the assigned storage reaches the warning level, the PS Series group will issue an alert. Once the assigned storage reaches the maximum value, no further storage can be assigned to the volume. For base volumes, the minimum volume reserve cannot be less than 10%.
Difference Volume Provisioning	0%, 80%, 100%	These parameters have the same effect as the base volume provisioning parameters, but apply to differencing volumes.
Create new volumes with open ACLs	no	Normally the HPC server maps a volume to a given node, which causes an ACL to be set on the volume. In some cases this may cause problems, particularly if the HBA is not using the IQN string the HPC Server has assigned to it during boot. Selecting this option will cause all volumes created by the iSCSI Provider to be assigned an unrestricted ACL, meaning that any initiator will be able to connect. You should only enable this option if you are experiencing authorization failures when nodes attempt to log into their assigned volumes.

9 Tools and Utilities

The Host Integration Toolkit includes the following utilities:

- [EqIXcp Utility](#)—Accelerates file copy operations by using SCSI Extended Copy commands.
- [EqLog Utility](#)—Gathers logging information into a zip file in the My Documents folder. You can then send this file to customer support for debugging.
- [EqRethin Utility](#)—Performs a volume rethinning operation on a thin-provisioned volume.

Note: Only administrators can run these utilities.

EqIXcp Utility

EqIXcp is a command-line Windows utility that uses SAN Data Copy Offload; an API that accelerates file copy operations by using SCSI Extended Copy commands. In a standard file copy operation, data is read from the source volume to the host computer, and then written to the destination volume. With SCSI Extended Copy commands, the source volume can transmit the data directly to the destination volume. The host computer is therefore eliminated from the I/O path, and network utilization is drastically reduced.

EqIXcp cannot be used to copy files between volumes when one of the volumes is using an access group ACL and the other is not. For EqIXcp to work, ensure that either both volumes are using traditional ACLs or both volumes are using access group ACLs.

Windows Server 2012 or greater has built-in support for offload data copy operations. Calling any of the standard file copy utilities or APIs on Windows Server 2012 or greater will result in an accelerated copy when possible, so you do not need to use EqIXcp on Windows Server 2012 or greater.

EqIXcp Utility Restrictions

If any of the following rules are not met, the EqIXcp utility will exit with an error message. No data will be lost.

- To use this utility, you must have the SE_MANAGE_VOLUME_NAME privilege. Administrators have this privilege by default.
- You can only copy between volumes on a single group.
- The source and destination volumes must reside on a PS Series group.
- The group members must be running PS Series firmware version 5.0 or higher.
- You cannot use this utility on compressed or sparse files. (Sparse files are files that are thin-provisioned on the NTFS file system.)

- EqlXcp is not supported on volumes that are cluster resources.

Run the EqlXcp Utility

The EqlXcp utility is located under the default installation folder, or the folder that you specified for HIT during installation. The default folder is: `C:\Program Files\EqualLogic\bin.`

Note: You must be logged in to the host as an administrator to run this utility.

1. From the Start menu, right-click Command Prompt and select Run as administrator.
2. In the command window, you can change the directory to:
`C:\Program Files\EqualLogic\bin`
3. Entering `eqlxcp` alone displays the syntax for the utility. The utility supports multiple source files on the command line, and accepts wildcards:
`eqlxcp [-hocv] source-file [source-file-n] destination-file`

Wildcards can be used to specify the source files. If multiple source files are specified, the destination must be an existing directory.

Options:

```
-h      Display this message
-o      Overwrite existing destination files
-c      Compare source and destination files after copy
-v      Verbose output
```

4. To copy `file1.zip` to a new file called `file2.zip`, enter the following command:
`eqlxcp e:\file1.zip e:\file2.zip`

EqlLog Utility

The Host Integration Tools kit includes a debug trace logging utility, EqlLog, that collects HIT trace logs, VSS logs, VDS logs, cluster logs, install logs, event logs, Setup API logs, backup documents, and MSInfo output.

Overview of the EqlLog Utility

If you ever have an issue with the Host Integration Tools kit that requires customer support, you will be asked to run the this utility, which gathers all of the logging information into a zip file in the My Documents folder. You can then send this file to customer support for debugging.

If you are managing multiple hosts from an instance of ASM/ME (also known as a HIT Group), this log collector can gather logs from those other hosts as well. To do this, specify the `-o` or `--hosts` option when you run the utility.

The EqlLog utility can also be run from ASM/ME. To do this, click the `Collect Logs` button at the top right of the ASM/ME console.

Run the EqlLog Utility

The EqlLog utility is located under the default installation folder, or the folder that you specified for HIT during installation. The default folder is: `C:\Program Files\EqualLogic\bin`.

Note: You must be logged in to the host as an administrator to run this utility.

1. From the Start menu, right-click Command Prompt and select Run as administrator.
2. In the command window, change the directory to:
`C:\Program Files\EqualLogic\bin`
3. Enter `eqllog`. The utility will gather trace logs and system information, and place them in a time-stamped zip file, located in the My Documents folder.

EqlLog Command Line Options

The EqlLog utility has several command line options, listed in [Table 17](#), which you can use to change its behavior.

Table 17: EqlLog CLI Options

Option	Description
-h, --help	Display usage information
-s, --short	Capture only the last 2 hours of HIT and event logs. This can greatly reduce the size of the data collected when you know the error occurred very recently.
-D, --destdir= <i>dir</i>	Changes the output directory where the .zip file is placed
-f, --output-file= <i>filename</i>	Changes the name of the output .zip file
-t, --only-tracelogs	Only collect the HIT trace logs.
-g, --hitgroup	Capture all the logs for all members of a HIT group.
-o, --hosts= <i>hostname</i>	Capture the logs from the specified HIT group hosts.
--no-hitlogs	Do not collect miscellaneous HIT logs.
--no-backupdocs	Do not collect VSS backup documents.
--no-msinfo	Do not collect system information from MSInfo32.
--no-setupapi	Do not collect Setup API logs.

Option	Description
--no-vss	Do not collect VSS logs.
--no-vds	Do not collect VDS logs.
--no-cluster	Do not collect cluster logs.
--no-install	Do not collect HIT installer logs.
--no-event	Do not collect Windows event logs.
--no-registry	Do not collect registry settings.
--no-ehcm	Do not collect EHCM diagnostic report.
--no-explorer	Do not launch Windows Explorer when log collection is complete.

Trace Log Daemon

The Trace Log Daemon collects trace log output from HIT components and outputs it to a single file, called `eqltrace.log`. This file is one of several other components that the EqlLog utility gathers into a single zip file for bug reports.

EqlLog will automatically locate this file. `eqltrace.log` takes up 50 MB of space by default.

In some versions of Windows, it will be in `<boot drive>:\ProgramData\EqualLogic\log`.

There is usually no need to change trace log settings for the daemon. However, default values can still be overridden in the registry if necessary. For example, trace logging can be run at levels 0 (no tracing) to 3 (verbose tracing). The normal logging level is 2. You should not need to change this, but it can be controlled with the `DebugLevel` registry entry.

In previous versions, debug trace settings were controlled separately for each HIT component, using registry values. These old values are obsolete and no longer used; setting them will have no effect. Tracing for all HIT components is now controlled by a single registry value and is on by default.

The registry values in [Table 18](#) are located in `HKLM/Software/EqualLogic/LogD`. If a value is not present in the registry, the default value from the table will be used.

Table 18: User-Changeable Settings for the Trace Log Daemon

Parameter	Default Value	Type	Definition
MaxLogSizeMB	50	DWORD	Maximum size of the trace log file, in MB. When the file exceeds this limit, the daemon will rename the existing log

Parameter	Default Value	Type	Definition
			to eqltrace.0.log and create a new eqltrace.log to continue logging.
DebugLevel	2	DWORD	Controls the level of debug tracing. Other options are 0 (no tracing) to 3 (verbose tracing). 2 is full tracing.

You do not need to restart the machine to change debug settings; the changes will automatically take effect within a few minutes.

EqlRethin Utility

EqlRethin is a command-line Windows utility that performs volume defragmentation and rethinning operations on one or more volumes.

The *Dell EqualLogic PS Series Storage Arrays Release Notes* discusses an issue with replicated volumes and volume rethinning, and recommends that you disable the SCSI unmap support in Windows 8 or greater and Windows Server 2012 or greater if you are using replicated volumes (including SyncRep). The release notes also recommend disabling automatic file system defragmentation in Windows Server 2012 or greater, and provides the steps on how to disable both the unmap and the defrag features. However, if you disable the unmap support, the Host Integration Tools rethinning tools will not work; in that case, to rethin a volume, you must use the Disk Optimization tool built into Windows.

Run the EqlRethin Utility

The EqlRethin utility is located under the default installation folder, or the folder that you specified for HIT during installation. The default folder is: C:\Program Files\EqualLogic\bin.

Note: You must be logged in to the host as an administrator to run this utility.

1. From the Start menu, right-click **Command Prompt** and select **Run as administrator**.
2. In the command window, you can change the directory to:
C:\Program Files\EqualLogic\bin
3. Entering `eqlrethin` alone displays the syntax for the utility.

```
EqualLogic Volume Re-Thinning Utility
Usage:
EqlRethin [OPTION] volume0 [volumeN]...
EqlReThin options:
-h [--help]                Display this text
-a [--analyze]             Show the possible results of rethinning a volume but
                           do not rethin
-d [--defragment]          Defragment volumes before rethinning
-n [--nounmap]             Skip sending SCSI unmap commands to the volume
```

```
-p [--percentage] arg <=90> Percentage of free space to rethin
```

Defragmenting a volume before rethinning can improve rethinning results, but can also take quite a while to execute.

4. To rethin a volume called tvol01 and defragment it first, enter the following command:

```
eqlrethin -d e:\
```

Note: Because defragmenting a volume can take a very long time (up to several hours), Dell recommends using the defragment option only on volumes that are known to be fragmented, or where performing the volume rethinning operation alone does not return as much space as expected.

Index

A

- access control** 53
 - modifying 55
 - VSS 55
- account for ASM/ME services** 18
- actively managed session** 51
- adapter, multipath** 43
- Add Hosts Wizard** 11
 - install HIT on remote host 13
- administrator**
 - EqlLog utility 79
 - EqlRethin utility 81
 - EqlXcp utility 78
 - group account 30
 - tools and utilities 77
- array**
 - add to group with RSW 32
 - failed initialization 32
 - initializing with RSW 32
 - network address 29
- ASM Services**
 - changing logon account 18
- Auto-Snapshot Manager**
 - See ASM/ME 1

B

- backup documents directory** 18
- bandwidth** 43
 - maximizing 46

C

- CD-ROM** 7
- changing service logon accounts** 18
- CHAP**
 - local account 31
 - MPIO DSM 45
 - password 30-31
 - user name 30-31
- cluster** 9
 - installation 9
 - See also Microsoft Failover Cluster 17
- command, resetting an array** 32
- components** 1-2
 - host integration tools 1-2

configuring

- groups with SCVMM 61
- LAN 46
- MPIO 47
- multipath I/O 46-47
- network 46
- SMP with SCVMM 57

connection management

- console terminal** 32

credentials

- CHAP 45
- MPIO 45

D

- dedicated subnet** 46
- default index file location, changing** 24
- default load balancing** 37
 - gateway 29
 - load balancing 51
- defragmenting volumes** 81
- device IP address** 50
- device specific module**
 - See MPIO DSM 43
- disabling SCSI unmap support** 81
- distributed session** 45
- DSM**
 - See MPIO DSM 43

E

- ehcm.log** 49
- EHCMSERVICE.exe** 43
- EqlASMAgent service logon account** 18
- eqldsm.sys** 43
- EqlLog utility** 78
 - administrator 79
 - command line options 79
 - running 79
- EQLReqService logon account** 18
- EqlRethin utility** 81
 - administrator 81
- EqlSMPHost** 3
- EqlXcp utility** 77, 81
 - restrictions 77
 - using 78
- EqualLogic Host Integration Tools**
 - components** 1
 - Multipath I/O DSM 2
 - VDS Provider 2

VSS Provider [2](#)
Ethernet port 0 [27](#)
Exchange Server
 See Microsoft Exchange Server [5](#)
Exchange Server 2010 [5](#)
excluded subnet [46](#)

F

fail over only [51](#)
 policy [47](#)
Failover Cluster
 See Microsoft Failover Cluster [17](#)
finding arrays [28](#)
friendly name [54](#)

G

gateway [29](#)
group
 administration account [30](#)
 configuration prompts in RSW [30](#)
 IP address [30](#)
 multipath requirements [46](#)
 name [30](#)
 password [30](#)

H

HBA [27](#)
 finding information [49](#)
 support considerations [45](#)
HIT [1](#)
 installing [7](#)
 uninstalling [10](#)
HIT utilities [77](#)
 Eqllog [78-79](#)
 EqlRethin [81](#)
 EqlXcp [77-78](#)
 run as administrator [77](#)
 trace log daemon [80](#)
host bus adapter
 see HBA [27](#)
Host Integration Tools [1-2](#)
 see HIT [1](#)
HPC iSCSI Provider [75](#)
 array requirements [75](#)
 installation [75](#)
 settings [75](#)
Hyper-V [6](#)

I

importing
 SMP through SCVMM GUI [58](#)
 VSS snapshots [54](#)
included subnet [46](#)
index files, specify location during installation [22](#)
initialization
 failed [32](#)
 using Remote Setup CLI [35](#)
initiator name
 See iSCSI initiator [43](#)
installing
 Add Hosts Wizard [11](#)
 and CSVs [11](#)
 change index locations [24](#)
 considerations [8](#)
 HIT on remote hosts with the Add Hosts Wizard [13](#)
 HIT with PowerShell [16](#)
 in VMs [11](#)
 on cluster [9](#)
 on remote host [14](#)
 preparation [7](#)
 remote [7](#)
 updating [9](#)
 using Active Directory [8](#)
 using PowerShell script [14](#)
 using the .MSI file [8](#)
 Windows Server 2008 Core Cluster [10](#)
 Windows Server 2008Core [10](#)
 Windows SharePoint [21](#)
IP address of the source device [49](#)
IP target [46, 50](#)
IPv4, specifying for MPIO [46](#)
IPv6, specifying for MPIO [46](#)
iSCSI
 initiator [2](#)
 managing connections [43](#)
 MPIO DSM properties [49](#)
 multiple connections [43](#)
 volume
 session per slice [47](#)
 sessions per [47](#)

K

kernel mode driver [43](#)

L

LAN configuration 46

latency 43

layer 2 multicasting 27

least queue depth 51

policy 47

load balancing 43, 48, 51

default 51

fail over only 47

least queue depth 47

policy 47, 51

round robin 47

logon accounts, changing 18

LUN 54

simple target 54

target 54

M

max sessions 47

maximizing bandwidth 46

member

network address 29

spanning 47

Microsoft

Exchange checksum verification 5

Exchange Mailbox Database 5

Exchange soft recovery 5

Exchange transaction log 5

Failover Cluster 18

Hyper-V 6

iSCSI Initiator 2

services, VSS/VDS 30

SharePoint 6

SQL Server. See SQL Server 5

Storage manager for SANS 2

VDS 2

minimum adapter speed, specifying for

MPIO 46

MPIO 43

optimal number of sessions 45

MPIO DSM

CHAP credentials 45

configuring 46-47

ehcm.log log file 49

introduction 43

IPv4 47

IPv6 47

LAN 46

log off volume 48

log on volume 48

logging 49

minimum adapter speed 47

multicasting 27

on Failover Cluster 17

path status 50

properties tab 49

properties tab (initiator) 50

requirements 46

snapshot connection 47

status 49

using 43

MSI file 8

multicasting 27

multipath 43

adapter 45

configure 47

configuring 46

displaying sessions 48

I/O

configure 47

initiator installation 52

load balancing 48

logging in to volume 48

logging off a volume 48

requirements

computer 46

group 46

typical configuration 43

N

naming targets and LUNs 54

netmask (member) 29

network

array IP address 29

configuration 46

gateway 29

group IP address 30

latency 43

NIC

See HBA 49

O

operating system

guest 6

supported 7

P

password 30

path

failover 43

uptime value 50

policy, load balancing 46, 51

port 0 27

PowerShell 1

change default index file location 24

for SMP 73

installing HIT 16

preparing for installation 7

properties tab for MPIO DSM 49

PS Series

configurign PS Series groups with

SCVMM 61

finding arrays 28

R

RAID policy

RAID 10 30

RAID 50 30

RAID 6 30

RAID 6-Accelerated 30

remote host

installing HIT 13

installing HIT with PowerShell 16

remote installations 11

Remote Setup

CLI

See RSWCLI 33

Wizard

See RSW 1

removing an installation 10

requirements

MPIO DSM 46

multipath I/O 46

reset command 32

resetting an array 32

restore

all (SQL) 5

all databases as new (SQL) 6

clone and restore as new (SQL) 6

named databases (SQL) 6

rethinning volumes 81

retrying array initialization 32

round robin 51

policy 47

RSW 27

adding array to group 32

failed initialization 32

group configuration prompts 30

initializing arrays 28, 32

launching 28

launching from ASM GUI 28

search feature 28

system requirements 27

RSWCLI 33

bin folder 34

command syntax 33

discover unitialized arrays 34

entering commands 34

exclude a subnet that MPIO uses 41

getting help 33

include a subnet for use by MPIO 39

initialize an array 35

list included and excluded subnets for
MPIO 38

list MPIO settings 37

modify MPIO settings 37

syntax 33

S

SAN 53

Storage Manager for 2

topology 44

SCSI unmap, effect if disabled 81

SCVMM 57

configuring 3

configuring group access on clusters 61

configuring group access on hosts 61

configuring PS Series groups 61

creating storage classification 58

creating VM template 66

migrate storage 70

migrating VMs 69

support for 3

supported operations 4

troubleshooting 71

VM rapid provisioning 63

searching for arrays 28

serial cable 32

session

actively managed 51

distribution 45

maximum per slice 47

per volume 47

per volume slice 47

SharePoint 6

- administration component index file
 - change location 24
- best practices 25
- index locations
 - change location 24
- installation
 - index file location 22
 - modify index file location 23
 - SPSearch index file
 - change location 25

silent installations 19**simple target 54****slice, volume sessions per 46****SMP 2**

- configuring 3
- configuring with SCVMM 57
- for Windows 8 16, 20
- for Windows Server 2012 57
- host service 3
- importing through SCVMM GUI 58
- infrastructure 2
- PowerShell cmdlets 73

snapshot, importing VSS 54**software required for installation 7****source IP 50****SQL Server 5**

- 2008 5
- 2012 5
- clone and restore 6
- restore all 5
- restore all as new 6
- restore named databases 6

status

- MPIO DSM 49

Storage Management Provider

- See SMP 2

Storage Manager for SANs 2

- starting 56

subnet

- dedicated 46
- excluded 46
- included 46

supported applications 4**supported software and firmware 7****syntax**

- command line (RSWCLI) 33
- MPIOExclude subcommand 41
- verify subcommand 34-35, 37-39

**System Center Virtual Machine Manager
(see SCVMM) 57****T****target**

- friendly name 54
- IP address 50
- iSCSI volume 50
- simple 54

terminal emulator 32**topology**

- changing SAN 45
- SAN 44

trace log daemon 80**transaction log 5****troubleshooting SCVMM issues 71****U****unattended installations 19****uninstalling HIT 10****updating an installation 9****user**

- CHAP 30

V**VDS 30**

- creating a volume 55
- guidelines 53
- Microsoft 2
- Provider 2
- requirements 53
- restrictions 53

VHD

- creating VM template 66
- enabling for SAN operations 72
- restoring 6

Virtual Disk Service

- See VDS 53

virtual machine

- See VM 6

VM

- enabling template for SAN operations 72
- rapid provisioning
 - with SCVMM 63

volume

- defragmenting 81
- log off with MPIO 48
- log on with MPIO 48
- MPIO target 50

- rethinning [81](#)
 - disabled [81](#)
 - driver [20](#)
 - Windows 8 [57](#)
 - Windows Server 2012 [57](#)
- sessions per slice [47](#)
- slice [44](#)
- VSS** [30](#)
 - importing snapshots [54](#)
 - modifying access control [55](#)
 - provider [2](#)

W

- Windows 8**
 - SMP provider [2](#), [16](#), [20](#)
 - volume rethinning [57](#)
- Windows Server 2008 Core**
 - installing HIT [10](#), [21](#)
- Windows Server 2008 COre cluster**
 - installing HIT [10](#)
- Windows Server 2012**
 - SMP provider [2](#), [57](#)
 - volume rethinning [57](#)

X

- XMLLogValue registry value** [49](#)