



Deploying Microsoft® Hyper-V™ with Dell EqualLogic™ PS Series Arrays

ABSTRACT

This technical report details information and best practices for deploying Microsoft® Hyper-V™ with Dell EqualLogic™ PS Series iSCSI storage arrays.



Copyright © 2010 Dell Inc. All Rights Reserved.

Dell EqualLogic is a trademark of Dell Inc.

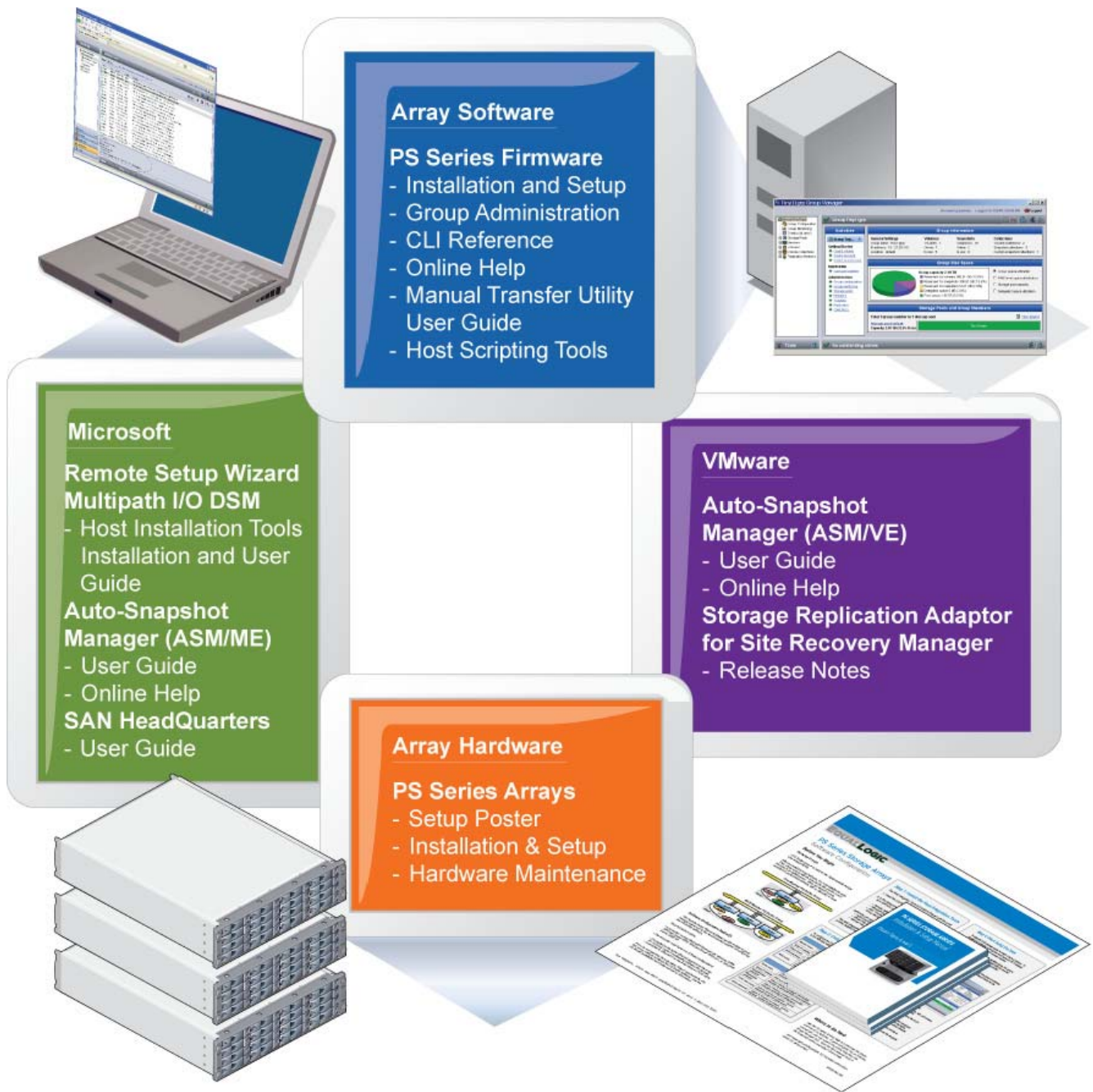
All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Possession, use, or copying of the documentation or the software described in this publication is authorized only under the license agreement specified herein.

Dell, Inc. will not be held liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change.

May 2010

WWW.DELL.COM/PSseries



PREFACE

Thank you for your interest in Dell EqualLogic™ PS Series storage products. We hope you will find the PS Series products intuitive and simple to configure and manage.

PS Series arrays optimize resources by automating volume and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates. The following value-add features and products integrate with PS Series arrays and are available at no additional cost:

- **PS Series Array Software**

- **Firmware** – Installed on each array, this software allows you to manage your storage environment and provides capabilities such as volume snapshots, clones, and replicas to ensure data hosted on the arrays can be protected in the event of an error or disaster.
 - **Group Manager GUI:** Provides a graphical user interface for managing your array
 - **Group Manager CLI:** Provides a command line interface for managing your array.
- **Manual Transfer Utility (MTU):** Runs on Windows and Linux host systems and enables secure transfer of large amounts of data to a replication partner site when configuring disaster tolerance. You use portable media to eliminate network congestion, minimize downtime, and quick-start replication.

- **Host Software for Windows**

- **Host Integration Tools**

- **Remote Setup Wizard (RSW):** Initializes new PS Series arrays, configures host connections to PS Series SANs, and configures and manages multipathing.
- **Multipath I/O Device Specific Module (MPIO DSM):** Includes a connection awareness-module that understands PS Series network load balancing and facilitates host connections to PS Series volumes.
- **VSS and VDS Provider Services:** Allows 3rd party backup software vendors to perform off-host backups.
- **Auto-Snapshot Manager/Microsoft Edition (ASM/ME):** Is a VSS Requesting application that provides point-in-time SAN protection of critical application data using PS Series snapshots, clones, and replicas of supported applications such as SQL Server, Exchange Server, Hyper-V, and NTFS file shares.
- **SAN HeadQuarters (SANHQ):** Provides centralized monitoring, historical performance trending, and event reporting for multiple PS Series groups.

- **Host Software for VMware**

- **Storage Adapter for Site Recovery Manager (SRM):** Allows SRM to understand and recognize PS Series replication for full SRM integration.
- **Auto-Snapshot Manager/VMware Edition (ASM/VE):** Integrates with VMware Virtual Center and PS Series snapshots to allow administrators to enable Smart Copy protection of Virtual Center folders, datastores, and virtual machines.

Current Customers Please Note: You may not be running the latest versions of the tools and software listed above. If you are under valid warranty or support agreements for your PS Series array, you are entitled to obtain the latest updates and new releases as they become available.

To learn more about any of these products, contact your local sales representative or visit the Dell EqualLogic™ site at <http://www.equallogic.com>. To set up a Dell EqualLogic support account to download the latest available PS Series firmware and software kits visit:

<https://www.equallogic.com/secure/login.aspx?ReturnUrl=%2fsupport%2fDefault.aspx>

TABLE OF CONTENTS

Preface	iii
Revision Information.....	v
Introduction.....	1
Planning and Deployment.....	1
Setting up the Hyper-V™ Server	1
Configuring the Hyper-V™ Networks.....	4
Setting Up the PS Series Storage	5
Performance Considerations	8
Provisioning and Deploying Stand-Alone Virtual Machines.....	9
Step 1: Creating Volumes on the PS Series Array to Host Virtual Machines ...	9
Step 2: Connect to the PS Series Volumes from Hyper-V Server.....	9
Using Hyper-V™ Manager.....	10
Using System Center Virtual Machine Manager.....	11
Provisioning and Deploying Highly Available Virtual Machines	12
Clustered Shared Volumes vs. Traditional Cluster Volumes	12
Standard Cluster Volume Deployments	13
Clustered Shared Volume Deployments	16
Protecting the Virtual Environment.....	17
Protecting Virtual Machines	17
Protecting Applications Running in Windows Guests	18
Summary	19
Technical Support and Customer Service	20

REVISION INFORMATION

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	March 2009	Initial Release
1.1	December 2009	Template change request
2.0	May 2010	Added content for Server 2008 R2 and CSV, template redesign

The following table shows the software and firmware used for the preparation of this Technical Report.

Vendor	Model	Software Revision
Microsoft®	Windows Server® 2008, 2008 R2	Enterprise and Datacenter Editions
Microsoft®	System Center Virtual Machine Manager 2008, 2008 R2	Version 2.0.3 and later
Dell™	PS Series Array Firmware	Version 4.3.2 and later
Dell™	Host Integration Tools for Windows	Version 3.3.1 and later

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: support.dell.com or the EqualLogic website at: <http://www.equallogic.com/resourcecenter/documentcenter.aspx>.

*Support account required.

Vendor	Document Title
Dell™	Dell™ Solutions Guides for Microsoft® Hyper-V™ http://support.dell.com/support/edocs/software/HyperV/en/index.htm
Microsoft®	Windows Server 2008 Deployment http://technet.microsoft.com/en-us/cc339386.aspx
Microsoft®	Windows Server 2008 TechCenter http://go.microsoft.com/fwlink/?LinkId=93752
Microsoft®	Hyper-V™ Step-By-Step Guide: Failover Clustering http://technet.microsoft.com/en-us/library/cc732181.aspx
Dell™	PS Series Array Network Performance Guidelines http://www.equallogic.com/resourcecenter/documentcenter.aspx
Dell™	Configuring and Deploying the Dell EqualLogic Multipath IO Device Specific Module (DSM) in a PS Series SAN http://www.equallogic.com/resourcecenter/documentcenter.aspx
Dell™	Deploying Tiered Storage in a PS Series SAN http://www.equallogic.com/resourcecenter/documentcenter.aspx

INTRODUCTION

Server virtualization is a common practice in today's data centers for server consolidation, power reduction, rapid provisioning, high availability, and data protection. All of these reasons lead to lower data center costs and TCO. Virtual servers together with intelligent virtual storage increase the chances for successful deployments of virtual data centers.

With the introduction of Windows Server 2008™ and Hyper-V™, Microsoft® has positioned itself to be one of the leaders in virtual server technologies. iSCSI has become the premier storage technology for Hyper-V™ deployments due to its lower costs, ease of use, data protection, and performance characteristics.

In 2008 Dell became the leader in iSCSI SAN deployments with the inclusion of Dell PS Series arrays. PS Series storage arrays offer great benefits for virtual server environments including:

- Simplified management of storage resources
- Comprehensive data protection of virtual resources
- Load balancing and performance optimization of storage resources
- Host Integration Tools

This technical report will discuss Hyper-V™ concepts and best practices when deployed with Dell EqualLogic™ PS Series iSCSI storage arrays.

PLANNING AND DEPLOYMENT

Part of a successful deployment is planning and considerations for all aspects of the Hyper-V™ environment. For this document, those planning aspects will include:

- Setting up Hyper-V™ Server
- Configuring the Hyper-V™ Network
- Setting up the PS Series Storage
- Performance Considerations

For more information on planning and deploying Hyper-V™ see the Microsoft® TechCenter at: <http://go.Microsoft.com/fwlink/?LinkId=93752>

For additional planning and deployment guides visit the Dell™ Solutions Guides for Microsoft® Hyper-V™ solutions site at:

<http://support.dell.com/support/edocs/software/HyperV/en/index.htm>

Setting up the Hyper-V™ Server

Hyper-V™ is a hypervisor aware virtualization layer that shares physical resources through a VMBus. The VMBus utilizes in-system memory for all calls from VMs to hardware and manages the device drivers that the virtual machines rely on to run

normally within the operating system. The physical servers running Hyper-V™ must be hypervisor aware and enabled to run virtual server environments. It's important to consider the performance of the Hyper-V™ server and how much of each physical resource will be needed to host the virtual machines.

Physical Server Resources

Server resources refer to physical processors, memory, network interfaces, and local storage. This section will cover considerations for planning physical server resources when deploying Hyper-V™.

Today's processors come in many different flavors from multi-core processors to hardware-assisted virtualization such as Intel VT and AMD-V processors. Although there is no conclusive data supporting one type of processor over another, it is important to plan for enough processing capabilities to support the number of virtual machines deployed. Microsoft® recommends using standard operating system and application requirements when planning virtual machine and Hyper-V™ deployments. Table 1 shows a hypothetical example for deploying 4 physical servers planned for specific roles. The same is true if the servers were virtual machines hosted on a single Hyper-V™ server.

Table 1: Example of Processor Planning

	Operating System	Application	# of Processor Cores
Server 1	Windows Server 2008	SQL Server 2008	4
Server 2	Windows Server 2008	Exchange Server 2007	4
Server 3	Windows Server 2003	Domain Controller	2
Server 4	Windows Server 2003	Backup Server	2

Based on the information in Table 1, the Hyper-V™ server would need to have enough processing capabilities to handle these different application servers as well as the parent operating system. Given that most modern processors are multi-core and that VMs run at average workloads, this example might require 4 quad-core processors to handle the load requirements of the VMs and the parent OS. It is also important to know how many virtual processors are supported for the guest operating system. For more information on supported guest operating systems see the Windows Server 2008 product information at: <http://www.Microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx>.

The same principle applies to server memory. As a default Microsoft® recommends to plan for a minimum of 2GB of physical memory per processor core but ideally plan for 4GB per core. Windows Server 2008 Enterprise and Datacenter can support up to 1TB of physical memory but not all servers support memory this large. Planning should be used when choosing server hardware to support Hyper-V™ and virtual machine loads.

The Hyper-V™ server should have two or more network adapters depending on the use cases for the NICs. One dedicated NIC should be configured for remote management of the physical server and one or more NICs should be configured for virtual network traffic. Additional network adapters will be required when connecting to iSCSI SAN volumes and Failover Clusters including a dedicated NIC for VM Live Migration if using CSVs. For basic iSCSI SAN connectivity one dedicated NIC is needed but ideally two should be configured for redundant SAN storage connections.

Over time as the Hyper-V™ environment grows the need for additional resources such as physical memory, processors, or additional network interfaces may become apparent. These resources can be added to increase performance and reduce contention as long as the physical server has additional capacity to grow these resources.

Technology Considerations

For the purpose of this document, technology considerations include any additional technologies that the operating system supports such as multipath IO, clustering and high availability. These technologies and how they apply to Hyper-V™ will be discussed below.

Multipath IO – MPIO

Multipath IO or MPIO is a software layer that provides more than one path for IO to travel. In Hyper-V™ environments this is possible by utilizing the native MPIO capabilities of the Microsoft® iSCSI Initiator Service or optionally installing the EqualLogic MPIO Device Specific Module (DSM).

The EqualLogic MPIO DSM is an extension of the Microsoft® MPIO driver stack with additional components designed to understand and adapt to the load-balancing capabilities of PS Series iSCSI storage arrays. The PS Series array connection load-balancing feature monitors network port utilization so that if one array port gets overloaded, iSCSI connections get shifted to another more available port on the array. This is accomplished by a standard feature of the iSCSI protocol that allows a connection to be redirected to a more available port. All this happens in a split second with no disruption to applications or data flow.

The MPIO DSM recognizes and understands the load-balancing characteristics of the arrays through a connection awareness/management module built into the DSM. The EqualLogic Host Connection Manager Service (EHCMservice) automatically makes the appropriate connections based on the number of network ports it sees active on the host. For example, if the Hyper-V™ host has 4 NICs, two for Client/LAN traffic and 2 for iSCSI SAN traffic, administrators can designate which subnets are to be used for SAN traffic and MPIO by including the iSCSI SAN subnet for MPIO using the Remote Setup Wizard shipped with the Host Integration Tools for Windows. This will not only improve performance of the Hyper-V™ environment but also ensures best practice deployment with PS Series arrays. For more information on the MPIO DSM, see the technical report *Configuring and Deploying the Dell EqualLogic MPIO DSM in a PS Series SAN* on the EqualLogic support website:

(<http://www.equallogic.com/resourcecenter/documentcenter.aspx>).

Clustering and High Availability

High availability can be achieved through Failover Clusters and clustering Hyper-V™ servers. It's important to properly configure network and storage resources prior to creating the Hyper-V™ cluster. In Windows Server 2008 Microsoft® has included a Cluster Validation Wizard that will analyze the hosts and resources prior to creating the cluster.

Note: Cluster validation may fail due to an invalid network configuration stating there are two network interfaces with the same address.

Cluster validation can fail for a number of reasons including NIC teaming. If using NIC teaming see the following KB article: <http://support.microsoft.com/kb/254101/>. If NIC teaming is not used, verify that the NICs on all cluster nodes are configured with different addresses. If cluster validation continues to fail this may be caused by a hidden network adapter called **Teredo Tunneling Pseudo-Interface** that is created automatically by Windows Server 2008 explicitly for use with IPv6. This device automatically configures itself and can prevent cluster validation from passing. If IPv6 is not needed, this device can be disabled by opening **Server Manager-Diagnostics-Device Manager-Network adapters**. To show the device use the Actions pane of Server Manager and click on **More Actions-View** and check **Show hidden devices**. This device should now be listed in the Network adapters list and can be disabled. Do this on all cluster nodes and run the cluster validation test again.

The Hyper-V™ Failover Cluster should be created in the following order:

1. Configure physical NICs on both Hyper-V™ servers
2. Configure storage resources on both Hyper-V™ servers
3. Install Hyper-V™ role on each servers
4. Install Failover Cluster feature on both servers
5. Create the virtual networks used for the Virtual Machines
6. Validate the cluster configuration
7. Create the cluster

For a step-by-step guide on Hyper-V™ Failover Clustering see the Microsoft® TechNet article: <http://technet.microsoft.com/en-us/library/cc732181.aspx>.

Configuring the Hyper-V™ Networks

The networks used for Hyper-V™ should be configured to separate LAN traffic from iSCSI SAN traffic. To accomplish this, network switches can be completely isolated per network or configured using VLANs. For more information on configuring the network and switches, consult the *PS Series Array Network Performance Guidelines* Technical Report on the EqualLogic website:

<http://www.equallogic.com/resourcecenter/documentcenter.aspx>.

The Hyper-V™ server should be configured to utilize each network for its specific purpose, LAN or SAN traffic. NIC teaming can be used for high availability and load-balancing of the LAN network but not for the iSCSI network. It is recommended to configure MPIO for the SAN network interfaces to maximize performance of the iSCSI

traffic. Physical NICs should be configured prior to creating the Hyper-V™ virtual network interfaces.

The Virtual Networks can later be added using the Hyper-V™ Virtual Network Manager. To allow virtual machine connections to a physical network interface such as those configured for LAN and SAN communications, use an External virtual network. Be sure to choose the correct physical network interface in the Virtual Network Manager wizard. See Figure 1 for a Virtual Network Manager example.

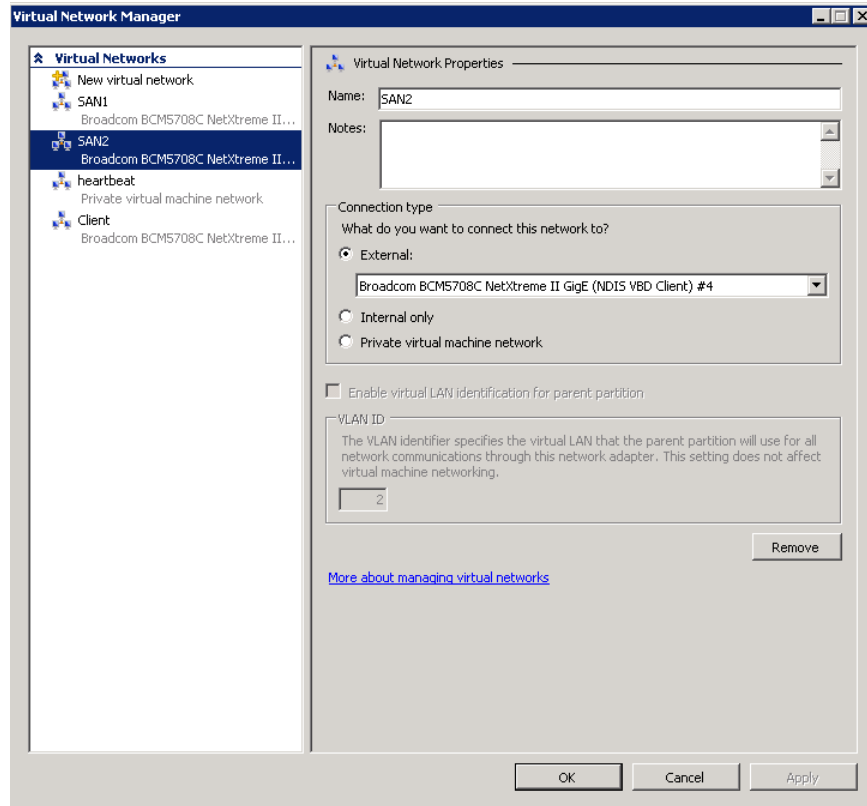


Figure 1: Hyper-V™ Virtual Network Manager – Example Network

Setting Up the PS Series Storage

PS Series arrays offer shared storage resources to the Hyper-V™ servers. These resources can be configured for many elements of the Hyper-V™ configuration. This section assumes familiarity with PS Series storage concepts and how to deploy and provision simple volumes with Windows Server systems. For more information on setting up and administrating PS Series arrays see the EqualLogic website: <http://www.equallogic.com/resourcecenter/documentcenter.aspx>.

PS Series volumes used for Hyper-V™ should be designed in accordance to Microsoft's best practices as well as the purpose of the volume. For example; some volumes will host virtual machines while others host library information or application data running inside the virtual machine.

These criteria should also be used to determine the RAID type of the volume. For example PS Series arrays designated for VHDs hosting guest operating systems can be set to RAID 50 and arrays designated for Direct Connect disks supporting high

performance application data can be set to RAID 10. PS Series arrays can be modified online to change the RAID designation within a PS Series Group.

Tiering or pooling can also be used in a PS Series storage group made up of more than one array. The benefits of creating multiple pools in a PS Series group include separating storage resources for specific purposes. For example one pool can be determined to host VHD or guest OS volumes and a second pool can be determined to host application data that the VM's are running. For more information on tiering and pools within a PS Series group see the *Deploying Tiered Storage in a PS Series SAN* Technical Report on the EqualLogic website: (<http://www.equallogic.com/resourcecenter/documentcenter.aspx>).

Hyper-V™ Disk Types

The type of disks used for Hyper-V™ can include Virtual Hard Disks (VHDs), pass-through disks, and disks directly connected through the guest OS iSCSI initiator. Table 2 compares these disk types and show advantages and disadvantages of using each.

Table 2: Hyper-V™ Disk Types

Disk Type	Advantage	Disadvantage
Virtual Hard Disks	<ul style="list-style-type: none"> • Hyper-V™ VSS supported for host-based backup of VMs • Supports VM checkpoints • Greater portability for exporting VMs to new locations 	<ul style="list-style-type: none"> • Limited to less than 2TB per VHD • Processor resources from parent server required to manage IO requests to the VHD
Pass-Through Disks	<ul style="list-style-type: none"> • Supports greater than 2TB LUNs • Offers greater performance for IO requests 	<ul style="list-style-type: none"> • Not supported by Hyper-V™ VSS or VM checkpoints • Does not offer VM portability through export operations • May get reordered after parent reboots, see more.
Direct Connect Disks	<ul style="list-style-type: none"> • Supports greater than 2TB LUNs • Accessed by the guest iSCSI initiator • Can be protected with VSS-aware backup applications 	<ul style="list-style-type: none"> • Not supported by Hyper-V™ VSS or VM checkpoints • Cannot be used as boot device for guest OS • Does not offer VM portability through export operations

Virtual Hard Disks are created and managed as files by the Hyper-V™ Parent partition. VHDs should be used to host the virtual machine guest OS files. This will allow the VM to be protected using Volume Shadow Copy Services (VSS) or Hyper-V™ Virtual Machine snapshots (checkpoints). Additionally VMs can be exported and moved to another location if they reside on VHDs. A single disk can host multiple VMs but Microsoft® currently recommends using separate disks per each VM. Using separate disks for each Virtual Machine can increase protection capabilities and high availability but also pose limitations in terms of server and storage connections. Keep in mind

each disk will use a drive letter as well as multiple connections to shared storage and it is important to understand how many connections will be used per volume including multipath IO connections. Alternatively hosting multiple VMs per disk enables easier Virtual Machine management and deployment of more VMs per physical server. Clustered Shared Volumes makes this easy in Windows Server R2.

VMs can also use VHDs as normal disks for additional file storage or application data. Using a VHD for application files allows Hyper-V™ VSS operations to protect the Virtual Machine and the application running inside the VM if the applications support VSS.

Hyper-V™ supports three types of VHDs, Fixed Size, Dynamically Expanding, and Differencing.

- Fixed Size VHDs allocate the full size specified at creation of the VHD. Fixed size disks offer the best performance and should be used for most production environments.
- Dynamically Expanding VHDs allocate only a portion of the total size at creation and then grow as data is added to the VHD. As a result, Dynamically Expanding disks require overhead for additional writes during expansion operations.
- Differencing VHDs use a parent-child relationship where the parent disk remains intact and changes are made to the child disk. Any changes can then be reverted back easily.

Note: Differencing VHDs can have performance impacts due to write overhead operations on the differencing disk. Read performance can also be impacted based on the size of the differencing chain. The larger the differencing chain the larger the impact.

Pass-Through disks are disks presented to the Hyper-V™ server that VMs can connect to and use as normal hard disks. Since pass-through disks are first presented to the parent partition they require some additional performance resources of the parent partition due to IO requests from the VM passing through the parent to the disk. Pass-Through disks offer advantages like increased disk size and greater performance than VHDs but lack some of the advanced integration capabilities. Pass-through disks are not supported for Hyper-V™ VSS or Live Migration operations and VMs hosted on pass-through disks cannot be exported.

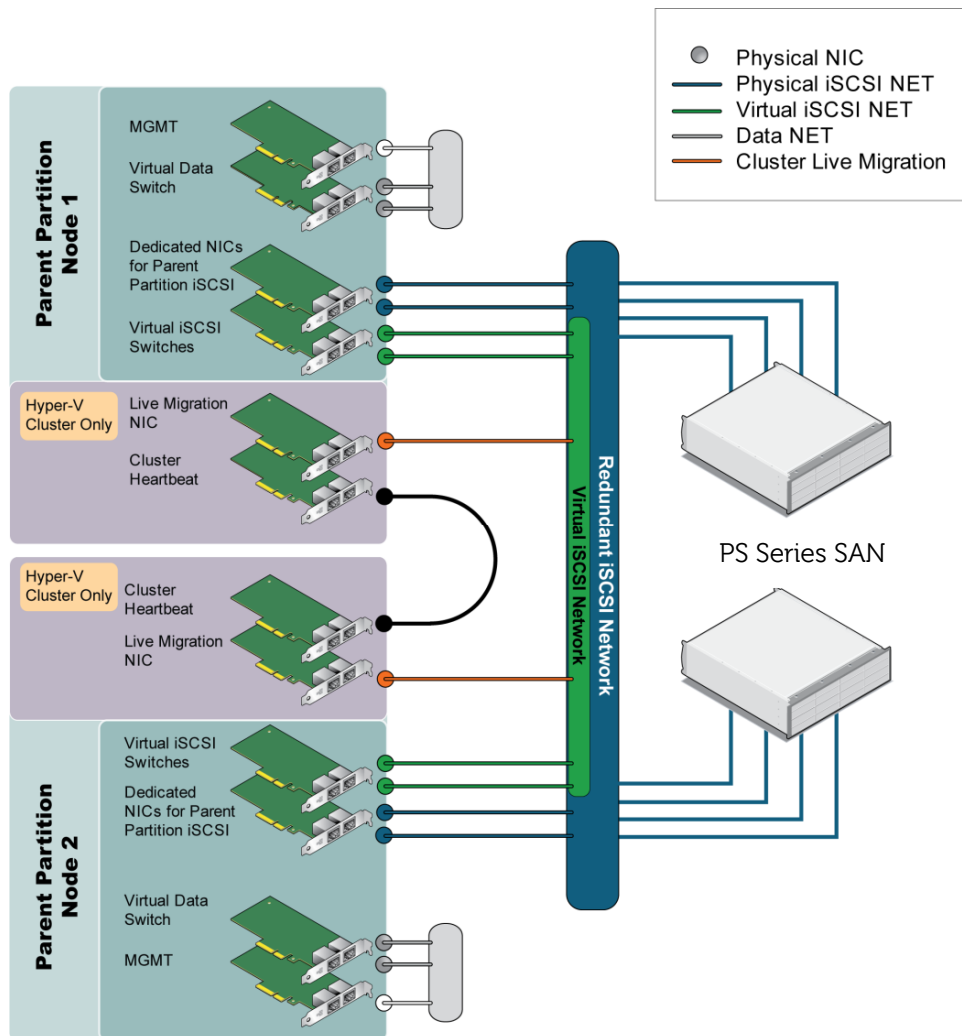
Direct Connect disks are disks that the VM directly connects to using an iSCSI initiator installed in the guest OS. Like pass-through disks, Direct connect disks are not supported by Hyper-V™ VSS and cannot be exported but Direct Connect disks do support Live Migration operations. Protecting Direct connect disks is similar to protecting shared disks connected to a physical server. VSS-aware application data sets residing on Direct Connect PS Series volumes can be protected by applications such as Dell's Auto-Snapshot Manager/Microsoft Edition. ASM/ME can be installed within the guest OS to protect applications that are VSS-aware. For more information ASM/ME see the section on [Protecting the Virtual Environment](#).

Performance Considerations

Although there are some general best practices for optimizing performance of Hyper-V™ systems the important thing to consider is adequate monitoring of the Hyper-V™ server. When the Hyper-V™ role is installed, additional Hyper-V™ performance counters are enabled for Windows® Performance Monitor. The Hyper-V™ counter set is a good start to determine how the Hyper-V™ server and VMs are performing. [Appendix A](#) of this document lists some of the Hyper-V™ counters.

The first step in optimizing performance of VMs is making sure the latest version of Hyper-V™'s Integration Services is installed on the guest OS. Hyper-V™ Integration Services install the latest device drivers for supported OSs. These drivers improve performance of calls between the guest OS and the server hardware. The virtual machine operating system can support the same server technologies as physical systems. When configured correctly VMs with dedicated NICs for iSCSI can utilize MPIO and improve performance of applications running inside the guest OS. Figure 2 shows an example of physical port allocation for stand-alone or cluster Hyper-V server configuration.

Figure 2: Hyper-V Server – Physical Network Port Allocation



For additional performance recommendations for Hyper-V and guest VMs refer to the following: http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv-R2.mspx.

PROVISIONING AND DEPLOYING STAND-ALONE VIRTUAL MACHINES

Deploying Hyper-V™ virtual machines with PS Series storage is similar to provisioning volumes for any application server. The volume must be created and given access to the host so the host can initialize and partition the disk. Once a partition is created on the volume, a VHD can be added and used to host virtual machine files. This section will show how to accomplish the following steps using Hyper-V™ Manager and System Center Virtual Machine Manager.

1. Create the volume on the PS Series Group with access to the Hyper-V™ server or servers if it is a failover cluster configuration.
2. Connect to the volume with an iSCSI initiator on the Hyper-V™ server.
3. Use Disk Management to format the disk and give it a drive letter or mount point.
4. **Important** - Once the disk has been formatted bind the disk in the iSCSI initiator using the Volumes and Devices tab.
5. Use Hyper-V™ Manager or SCVMM to create a new VHD on the volume and install the new VM.

Note: This section assumes familiarity with administration of PS Series groups. For more information on administrating PS Series arrays see the EqualLogic website: <http://www.equallogic.com/resourcecenter/documentcenter.aspx>.

Step 1: Creating Volumes on the PS Series Array to Host Virtual Machines

By now there should be a plan in place for the availability and responsibility of each VM deployment. This will serve as the starting point for volume creation on the PS Series group. Highly available VMs will be deployed on Hyper-V failover clustering and non-clustered VMs on stand-alone Hyper-V servers.

Volume size is determined by how many VMs will be stored on the volume. For stand-alone Hyper-V servers it is recommended to deploy a single VM per volume. For clustered Hyper-V servers, multiple VMs can be deployed on a single volume when using Cluster Shared Volumes. For clustered deployments see [Deploying Highly Available Virtual Machines](#).

PS Series volumes planned for a stand-alone Hyper-V server deployment is fairly straight forward. Create a volume for each VM on the PS Series group to host the VM and OS configuration files. The volumes hosting VMs can be created from a storage pool configured as RAID50. For IO intensive data volumes it is recommended to use RAID 10.

Step 2: Connect to the PS Series Volumes from Hyper-V Server

In each case regardless of volume purpose, access to the iSCSI initiator on the Hyper-V server is needed. Access can be granted by adding the Hyper-V server's iSCSI initiator IQN name or the IP address of the NIC on the iSCSI network, Figure 3.

Note: If the volume is going to be used in a cluster, the access type will need to be checked to “Allow simultaneous connections from initiators with different IQN names”.

Connect to the volume on the Hyper-V server checking the “Add this connection to the list of Favorite Targets” box and “Enable multi-path”.

Use Server Manager – Storage – Disk Management set the volume online and initialize the new disk. **Note:** Use the GPT partition style if the volume is greater or plans to grow greater than 2TB.

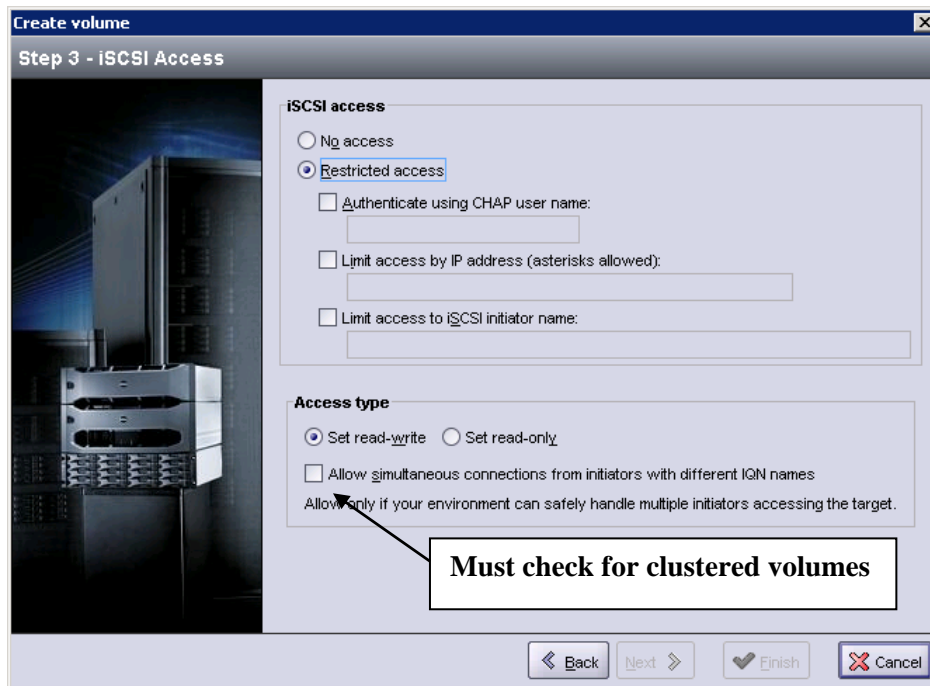


Figure 3: Volume Access Options

Now that the disk has a partition it is important to bind the volume in the iSCSI initiator. To do this open the iSCSI initiator and tab over to the **Volumes and Devices** tab and click the **Auto Configure** button to bind the volumes. Binding the volumes to the initiator will assure that the volume and disk numbering will stay intact if a server power outage occurs. This is especially important if you plan to use pass-through disks.

Using Hyper-V™ Manager

Hyper-V™ Manager is a tool provided to configure and manage the Windows Server 2008 Hyper-V™ environment. Once the Hyper-V™ role has been installed, Hyper-V™ Manager can be started through **Start-All Programs-Administrative Tools** menu on the Windows Server 2008 host. This section will show how to provision a virtual machine using a new PS Series volume that has been added to the server via the Microsoft iSCSI Initiator Service.

Using **Server Manager-Disk Management** set the disk online, initialize, and format a partition. Once the disk has a partition and drive letter it can be used to create a new VHD or virtual machine using the **Hyper-V™ Manager – Actions** menu. The New Virtual Machine wizard will create the VHD file as part of the new virtual machine

creation process. Follow the steps in the New Virtual Machine wizard to complete the setup of the VM.

1. Give the new VM a name and choose where to store the virtual machine files. This will be the location of the new VHD.
2. Determine the memory requirements for the new VM and optionally assign a virtual network.
3. Create a virtual hard disk for the VM files and point to the location of the newly added disk.
4. Choose the preferred option for installing the operating system and finish the New Virtual Machine wizard.

The new VM will be created based on the options chosen during the New Virtual Machine wizard. Virtual Machine settings can be modified at any time using the VM Settings option in Hyper-V™ Manager, however some setting changes require that the virtual machine be powered off.

Using System Center Virtual Machine Manager

System Center Virtual Machine Manager (SCVMM) is a tool Microsoft® provides for remote management of virtual server environments. SCVMM can manage multiple virtual environments including VMware ESX environments. In order for SCVMM to communicate correctly with virtual environments, these objects must all be in the same domain with a common administrative account. Always follow best practice recommendations for installing and configuring SCVMM. This section assumes System Center Virtual Machine Manager is setup and working correctly prior to creating virtual machines.

To create a VM using SCVMM select **new virtual machine** from the Actions pane on the right side of SCVMM. This will start the New Virtual Machine wizard in SCVMM. Follow the steps in the New Virtual Machine wizard to create the VM.

Note: The disk hosting the new VM files must be added and formatted on the Hyper-V™ server prior to creating the VM using SCVMM.

SCVMM Rapid Deployment with PS Series Arrays

System Center Virtual Machine Manager has added features for deploying virtual machines such as creating VM templates and clones used for quick deployment operations. These functions in conjunction with PS Series storage offer additional ease of use and automation for rapid deployment of Hyper-V™ virtual server environments. This section will cover deploying VMs using VM templates and clones with PS Series arrays.

Using templates is a quick and easy way to deploy multiple VMs of the same configuration and OS. A template can be created from any running VM but **note** the source VM will be destroyed once the template is created. Templates are stored in a library share either on the SCVMM server or another server configured with a library

share. Once the template is created, SCVMM can use the template to deploy multiple VMs based on the template's configuration and pointing the VHD files to the location of a new PS Series volume added to the Hyper-V™ server.

Cloning a VM is similar to using templates but will create a copy of a virtual machine with a new name. The benefit of using VM clones is the source VM will not be destroyed after the new VM clone is created. Like using a template the VM clone files can be pointed to the location of a newly added PS Series volume on the Hyper-V™ server.

Note: VM clones will require a computer name and IP change if hosted on the same network subnet as the source VM.

PROVISIONING AND DEPLOYING HIGHLY AVAILABLE VIRTUAL MACHINES

Deploying highly available virtual machines with failover clustering requires planning and understanding of the virtual machine responsibilities and workloads. Planning the VM layout is important to determine the storage resources needed for the VMs. Choosing to make the volumes Clustered Shared Volumes or normal cluster volumes can help determine volume size and configuration.

Figure 4 shows an example of a VM deployment using CSVs and a VM deployment using standard cluster volumes. Without CSV a 1 to 1 – VM to volume mapping is recommended and with CSV a many to 1 – VMs to volume mapping is recommended. Both deployments have pros and cons. Table 3 discusses the pros and cons of each choice.

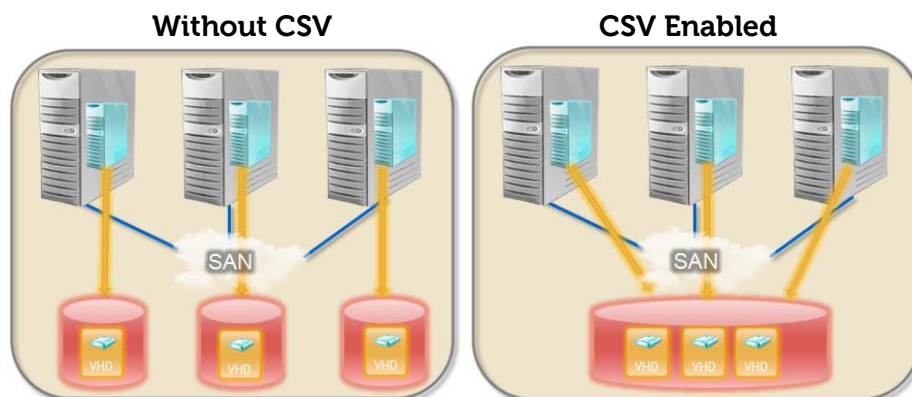


Figure 4: Virtual Machine Deployments With and Without CSV

Clustered Shared Volumes vs. Traditional Cluster Volumes

Clustered Shared Volumes offer the ability to host multiple VMs on a single volume and seamlessly "Live Migrate" VMs from one cluster node to another. Windows Server 2008 R2 offers live migration of virtual machines hosted on standard cluster volumes also.

Table 3: Pros and Cons of CSVs and Non-CSVs

	PROS	CONS
Clustered Shared Volumes	<ul style="list-style-type: none"> • Offer Live Migration of individual VMs • Can reduce the overall connections to a PS Series group • Reduces storage and server administrator burden associated with managing a large number of disks 	<ul style="list-style-type: none"> • Require more physical resources for cluster nodes • Best practice recommendation requires additional adapters on each server in the cluster for CSV related traffic
Traditional Cluster Volumes	<ul style="list-style-type: none"> • Offer better native protection and disaster recovery options • Offer Live Migration if 1:1 VM per volume is maintained 	<ul style="list-style-type: none"> • Do not offer Live Migration of individual VMs if more than one VM is placed on a volume • Recommended 1:1 VM per volume thus increasing connections to PS Series groups

Here volume size is an important characteristic and can be determined by the quantity and type of VMs being deployed. For example two scenarios will be discussed, 1) non-CSV deployments and 2) CSV deployments.

Standard Cluster Volume Deployments

Scenario 1: Non-CSV deployments are similar to stand-alone deployments where a single volume will host the VM. For these types of deployments simply follow these steps to provision a standard cluster volume:

1. Create a volume on the PS Series group and present it to the first cluster node.
Important: When creating volumes for clusters, be sure to check the box to "Allow simultaneous connections from initiators with different IQN names" in the volume access page. See **Figure 2** above.
2. Once the disk has been formatted with a partition, connect it to the other cluster nodes and assign the same drive letter as the first node.
Note: Be sure to add the second node's initiator IQN name or NIC IPs to the volume access control list before trying to connect to the volume.
3. Add the disk to the cluster by right clicking the **Storage** object and select **Add a disk** option, Figure 5.
4. Choose the newly prepared disk to add to the cluster.

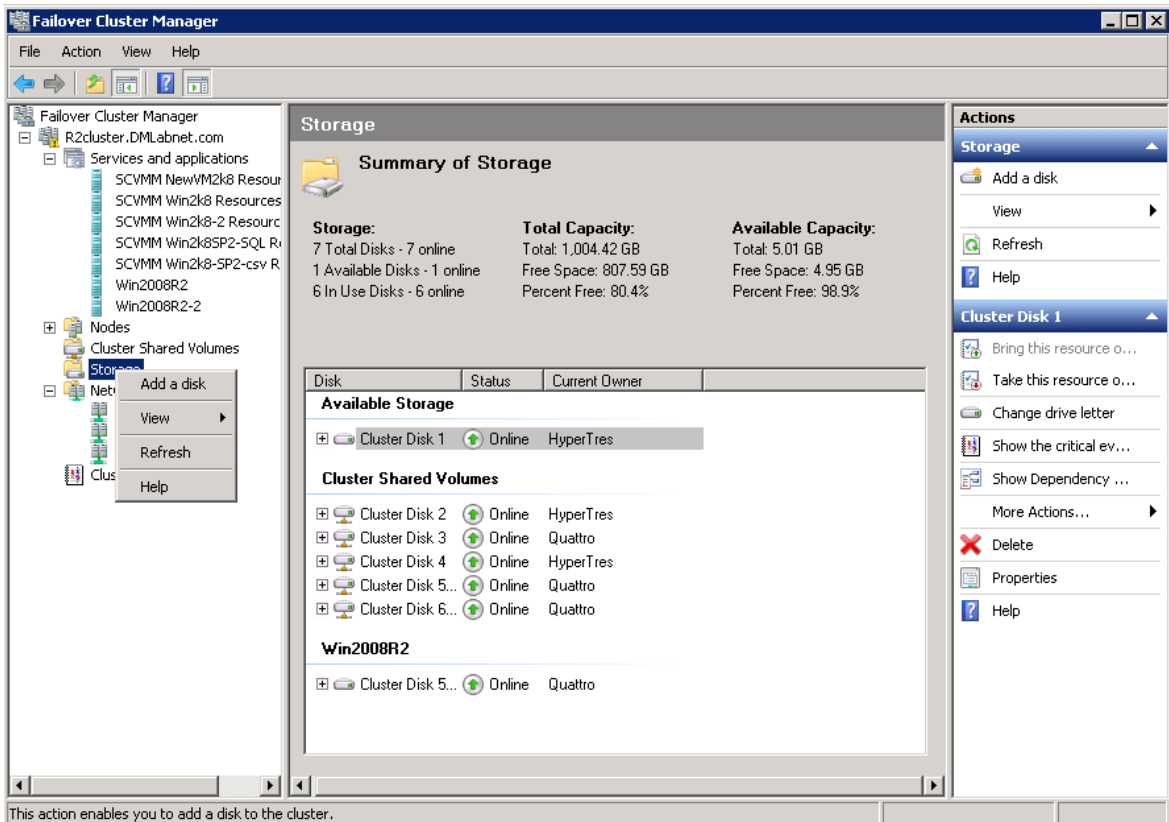


Figure 5: Adding a Stand-Alone Disk to a Failover Cluster

Now that the volume is a clustered disk, choose a method to deploy virtual machines. Three methods can be used to deploy virtual machines in a failover cluster: Hyper-V Manager, System Center Virtual Machine Manager or Failover Cluster Manager.

The recommended method of deployment is to use System Center Virtual Machine Manager described in [Provisioning and Deploying Stand-Alone Virtual Machines](#).

If SCVMM is not available then use Failover Cluster Manager to deploy the VM.

1. Right click **Services and applications** and choose **Virtual Machines... - New Virtual Machine...**, Figure 6.
2. Choose a clustered node and the new clustered disk to deploy the new virtual machine and step through the deployment wizard to finish.

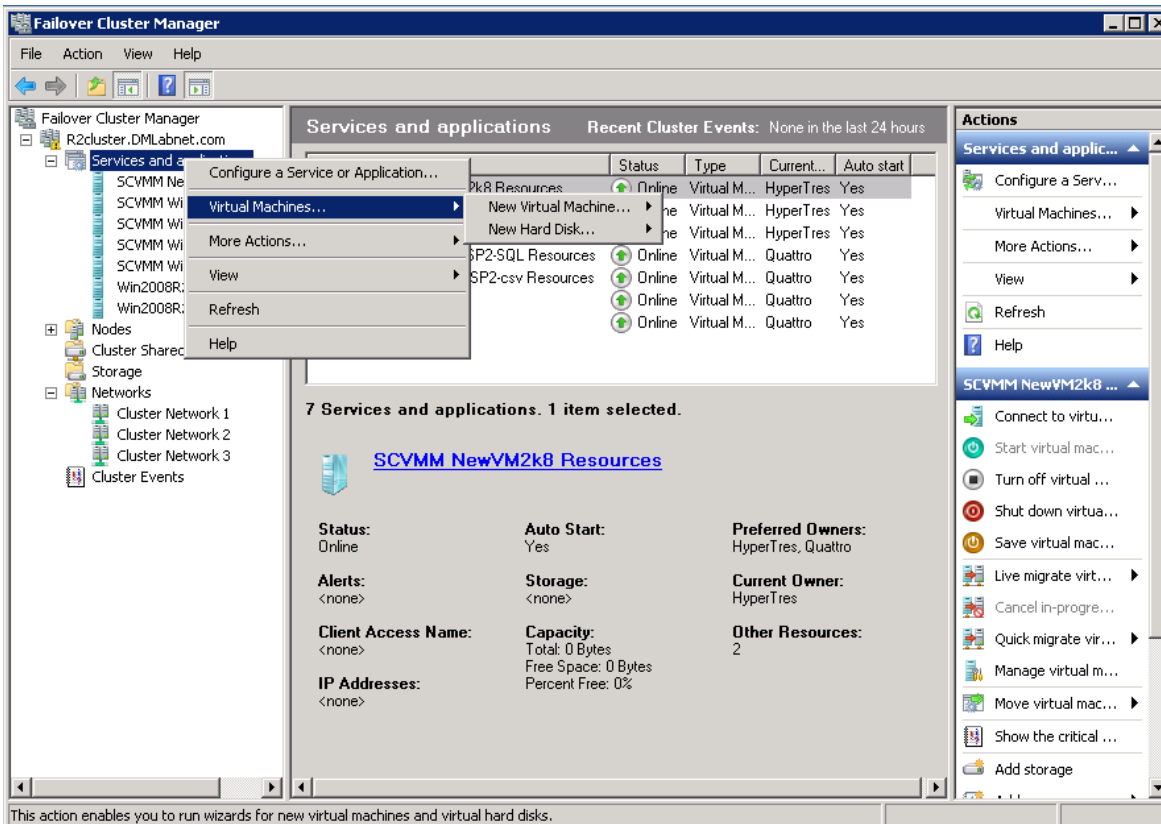


Figure 6: Using Failover Cluster Manager for VM Deployment

Lastly if Hyper-V Manager is used, the VM must still be made highly available. To make a VM highly available follow these steps:

1. From Failover Cluster Manager right click **Services and applications** and choose **Configure a service or application....**
2. Select **Virtual Machine** from the Service or Application list and follow instructions to choose and set the virtual machine to highly available, Figure 7.

Note: The virtual machine must be powered off before making it highly available and the virtual machine must be deployed on the node that owns the cluster disk at the time of deployment if Hyper-V manager is used.

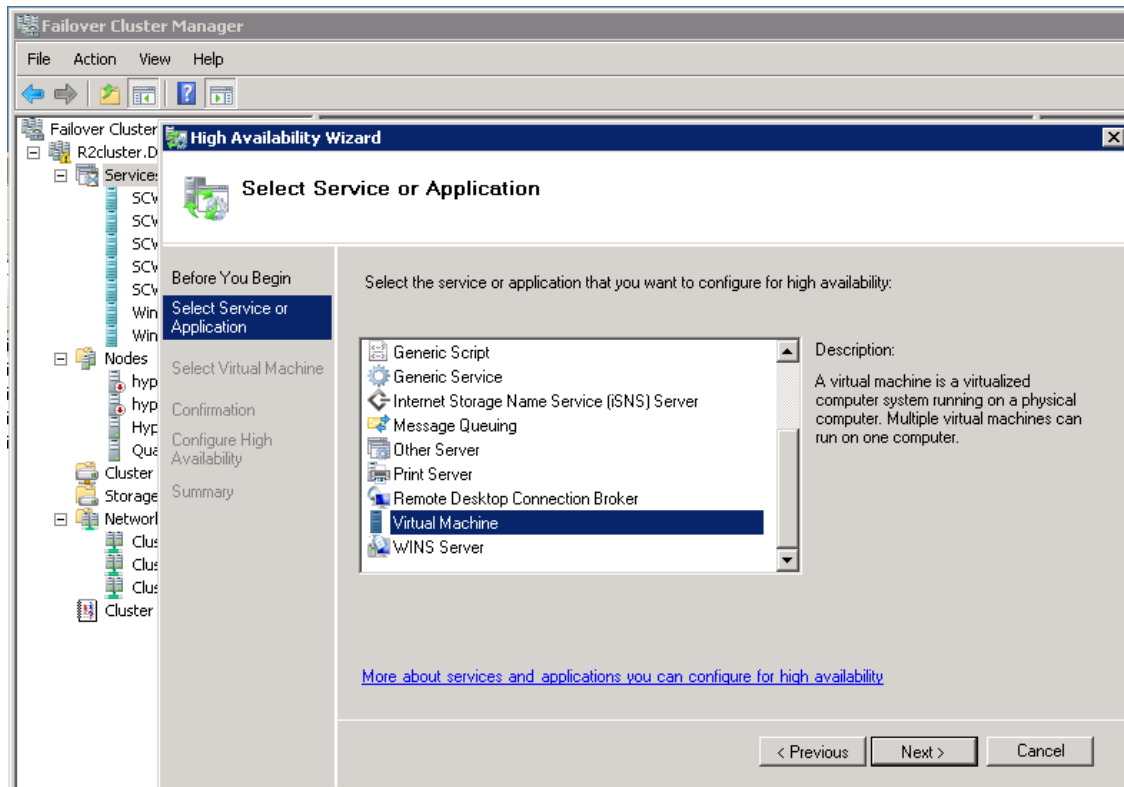


Figure 7: Make a Virtual Machine Highly Available

Clustered Shared Volume Deployments

Scenario 2: Deploying CSVs to host virtual machines is similar to deploying stand-alone cluster volumes with a few extra steps. To deploy virtual machines on Clustered Shared Volumes follow these steps:

1. First make sure Clustered Shared Volumes are enabled in Failover Cluster Manager. This will add the Clustered Shared Volumes object in the left pane of the Failover Cluster Manager.
2. After the PS Series volume has been added to cluster **Storage**, right click on **Clustered Shared Volumes – Add storage** and choose the newly added disk as the new CSV, Figure 8.
3. Once the new CSV is provisioned, deploy virtual machines using one of the methods described above in [Standard Cluster Volume Deployments](#) and point the VHD to the newly provisioned CSV.

When a new CSV is created, a new directory `C:\ClusterStorage` will be created on each node. This will be the home directory for virtual machines hosted on that CSV. This allows each node to have simultaneous read/write access to the shared volume.

The main difference between deploying virtual machines on standard clustered volumes vs. clustered shared volumes is that each node in the cluster will have read/write access to the volume. This allows virtual machines to be hosted by any of the nodes while the CSV is owned persistently by only one of the nodes at a time.

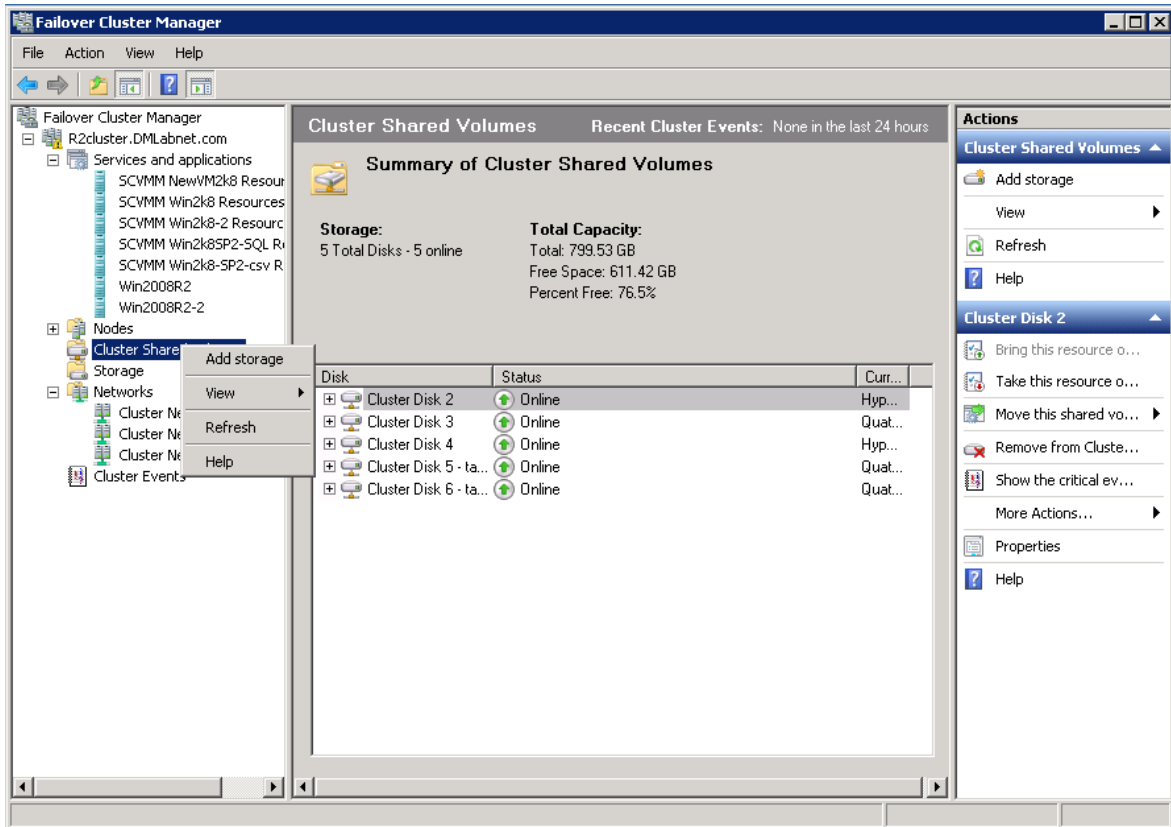


Figure 8: Adding a New Cluster Shared Volume

PROTECTING THE VIRTUAL ENVIRONMENT

Protecting the Hyper-V™ environment is an important part of the planning stage and should be a top concern for administrators. Failover clusters offer high availability by allowing resources and VMs to migrate from one Hyper-V™ host to another in the event of a physical server failure. Virtual machine protection can also be accomplished using Hyper-V™ VSS snapshots and virtual machine snapshots. It's important to distinguish between the two as they are distinctly different.

This section will discuss protecting virtual machines as well as applications running inside the virtual machine guest operating systems. Coordinating protection tasks at each level of the virtual environment can help ensure a robust protection plan.

Protecting Virtual Machines

As mentioned above virtual machine protection can be accomplished using failover clustering, virtual machine snapshots, and Hyper-V™ VSS snapshots.

Failover clustering is a common practice for creating highly available server environments and is supported by Windows Server 2008 to protect virtual machines running on Hyper-V™ hosts. For information on clustering Hyper-V™ host see the [Clustering and High Availability](#) section of this document. Additionally virtual machines

running critical applications can be clustered within the Hyper-V™ environment for additional protection against a virtual machine failure.

Virtual machine snapshots can be created using Hyper-V™ Manager and selecting the **Snapshot** option listed under the virtual machine name in the **Hyper-V™ Manager Actions** pane. System Center Virtual Machine Manager can also create VM snapshots using the **New checkpoint** option. Virtual machine snapshots are like point-in-time copies of the VM state and can be used to revert the VM back to that point-in-time state. These snapshots are stored on the same physical disk(s) as the VHD files reside and therefore must be managed accordingly. Virtual Machine snapshots are a great way to protect test or development environments where subtle changes can occur and corrupt VM's.

Hyper-V™ VSS snapshots are accomplished by installing the Hyper-V™ backup integration service inside the guest OS (installed by Hyper-V™ Integration Services). Microsoft® recommends using Hyper-V™ VSS snapshots for full protection of a Hyper-V™ virtual environment. The Hyper-V™ backup integration service includes a VSS requestor that is used to quiesce any VSS-aware writers running in the guest. The guest VSS requestor then returns control to the Hyper-V™ VSS writer running on the parent server to create a volume snapshot now. The Hyper-V™ VSS writer quiesces the VM itself and creates a snapshot of the volume on which the VM VHD files reside. This ensures consistency of the virtual machine state by backing up the configuration of the VM, the VM snapshots associated with the VM, and the VHDs used by the VM. Hyper-V™ VSS snapshots require a third party backup application that supports Hyper-V™ and VSS.

Dell provides a VSS requesting application called Auto-Snapshot Manager/Microsoft Edition (ASM/ME) that can be installed and run in the Parent partition that supports Hyper-V™ VSS snapshots. ASM/ME is a VSS-aware application that protects application data residing on PS Series volumes including Hyper-V™ Virtual Machines. ASM/ME is installed as part of the PS Series Host Integration Tools for Windows and includes a VSS provider service for PS Series arrays. When configured the Hyper-V™ VSS snapshots are stored on the PS Series array as a PS Series volume snapshots. ASM/ME with Hyper-V™ support is available in Host Integration Tools v3.2 and later and can be downloaded from the EqualLogic.com support site at no extra charge.

Note: PS Series volumes directly connected to a VM guest OS through an iSCSI initiator running inside the guest OS are not supported by the Hyper-V™ VSS writer. These volumes can be protected in the guest OS by a VSS application running inside the guest operating system. See the next section for more information on protecting applications running in the guest.

Protecting Applications Running in Windows Guests

Applications and data inside the virtual machine can be protected by Hyper-V™ VSS snapshots or by 3rd party VSS-aware applications. In order to protect data inside the guest with the Hyper-V™ VSS writer, the data must reside on a VHD. This way the Hyper-V™ VSS writer can include the application data during the snapshot process. This excludes disks that are directly connected to the guest OS using an iSCSI initiator running in the guest.

Disks connected using an iSCSI initiator running in the guest can be protected using 3rd party applications that support VSS and the application VSS writers that are running in the guest. Auto-Snapshot Manager/Microsoft Edition (ASM/ME) can be installed in the guest operating system to protect disks that are not supported by Hyper-V™ VSS. For example: application data residing on PS Series volumes directly connected by iSCSI initiators running inside a VM.

SUMMARY

Virtual server infrastructures offer great benefits for server consolidation and datacenter management. Hyper-V™ improves the Windows Virtual Server technology by incorporating a new hypervisor for improved performance and integrating with industry standard Microsoft® management software. When deployed with PS Series arrays Hyper-V™ virtual machine deployment and management is simplified by the ease of use of iSCSI and intelligent management of PS Series storage.

TECHNICAL SUPPORT AND CUSTOMER SERVICE

Dell's support service is available to answer your questions about PS Series SAN arrays. If you have an Express Service Code, have it ready when you call. The code helps Dell's automated-support telephone system direct your call more efficiently.

Contacting Dell

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services might not be available in your area.

For customers in the United States, call 800-945-3355.

Note: If you do not have access to an Internet connection, contact information is printed on your invoice, packing slip, bill, or Dell product catalog.

Use the following procedure to contact Dell for sales, technical support, or customer service issues:

1. Visit support.dell.com or the Dell support URL specified in information provided with the Dell product.
2. Select your locale. Use the locale menu or click on the link that specifies your country or region.
3. Select the required service. Click the "Contact Us" link, or select the Dell support service from the list of services provided.
4. Choose your preferred method of contacting Dell support, such as e-mail or telephone.

Online Services

You can learn about Dell products and services using the following 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