# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EMC VNXe Series</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Introduction to the EMC VNXe Series</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Software suites available</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Software packs available</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>VNXe application awareness</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Advantages of the VNXe platform</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Application-based provisioning overview</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>Hyper-V Planning on VNXe</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Overview of Microsoft Hyper-V</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Connection options</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>VHD</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Passthrough disk</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>iSCSI direct within the guest OS</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>EMC VNXe benefits for Hyper-V</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>VNXe storage pools</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Default storage pools</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Custom storage pools</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Capacity planning</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Performance planning</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Hyper-V Deployment on VNXe</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Provisioning overview</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Initial setup of EMC VNXe storage</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Hyper-V server configuration</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Create iSCSI Servers for VNXe</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Add Hyper-V Servers and guest OSs as hosts in VNXe</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Create storage pools for VNXe Hyper-V</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>VNXe: Create Hyper-V data stores and grant access to hosts</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Connect Hyper-V hosts to VNXe Hyper-V storage</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Set up Hyper-V hosts to use the data store</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Create virtual machines</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Provisioning summary</td>
<td>32</td>
</tr>
<tr>
<td>4</td>
<td>High Availability Planning</td>
<td>35</td>
</tr>
</tbody>
</table>
Contents

High Availability overview ................................................................. 36
VNXe High Availability architecture ...................................................... 36
  Active-Active clustering ................................................................. 36
No single point of failure .................................................................. 36
RAID group hot spares .................................................................... 36
Chapter 5  VNXe Performance Scaling ................................................ 39
VNXe performance overview ............................................................ 40
  Use case overview ........................................................................ 40
Test methodology ............................................................................ 40
Results ........................................................................................... 40
Chapter 6  VNXe Hyper-V Protection .................................................. 43
Overview ....................................................................................... 44
Protection storage considerations ..................................................... 44
VNXe iSCSI snapshots ...................................................................... 44
  Scheduled snapshots .................................................................... 44
  On-demand snapshots .................................................................. 46
Snapshot use cases .......................................................................... 47
  Snapshot restore ......................................................................... 47
Test/dev environment ...................................................................... 47
Snapshots for backup applications .................................................. 48
Backup and recovery ....................................................................... 49
  Backup strategy .......................................................................... 49
Hyper-V host and guest-based backups .......................................... 49
Backup and recovery using DPM 2010 ............................................. 50
Backup of VNXe Hyper-V storage using DPM 2010 ......................... 50
Hyper-V data restore ...................................................................... 53
Chapter 7  Hyper-V Virtual Machine Migration to VNXe ....................... 55
Migration overview ......................................................................... 56
Quick migration ............................................................................. 56
Live migration ............................................................................... 57
Quick storage migration .................................................................. 59
Chapter 8  VNXe Replication using Replication Manager ......................... 63
Disaster recovery .......................................................................... 64
VNXe replication overview ............................................................ 64
  Create a replication source ....................................................... 64
  Establish replication connections ............................................ 64
  Create a replication destination ............................................. 66
Install Replication Manager Server and Agents .............................. 67
  Attach hosts to Replication Manager ...................................... 67
Create an application set .............................................................. 68
Create a replication job ................................................................. 70
Run a Replication Manager job .................................................... 74
Mount a Replication Manager replica .......................................... 76
Replication failover ....................................................................... 76
Appendix A  VNXe iSCSI Server Target Setup .................................. 79
  Configure VNXe for iSCSI connectivity .................................... 80
Appendix B  Host Creation in VNXe .................................................. 83
Figures

Figure 1  VNXe management dashboard ................................................................. 16
Figure 2  VNXe iSCSI connection options for Hyper-V ........................................... 18
Figure 3  VNXe Hyper-V storage provisioning flowchart ....................................... 24
Figure 4  Storage Pools link in Unisphere ............................................................. 25
Figure 5  Disk Configuration Wizard .................................................................... 26
Figure 6  Select Storage Type page ....................................................................... 27
Figure 7  Select Amount of Storage page .............................................................. 28
Figure 8  Configure Storage page ......................................................................... 29
Figure 9  Configure Protection page ..................................................................... 30
Figure 10 Configure Protection Storage Size page .................................................. 31
Figure 11 Configure Host Access page ................................................................... 32
Figure 12 Configure Spares page ........................................................................... 37
Figure 13 Use case reference architecture ............................................................. 40
Figure 14 Performance behavior .......................................................................... 41
Figure 15 Create a schedule ................................................................................. 45
Figure 16 Add Schedule Rule dialog box ............................................................... 46
Figure 17 Hyper-V snapshots ............................................................................... 46
Figure 18 Take Snapshot Now dialog box .............................................................. 47
Figure 19 VNXe snapshot promotion process ....................................................... 48
Figure 20 Flowchart for VNXe backup and restore using DPM 2010 ....................... 50
Figure 21 Add destination storage to DPM ............................................................. 51
Figure 22 Install Agent software on the hosts ....................................................... 51
Figure 23 Create protection group ......................................................................... 52
Figure 24 Select Group Members page ................................................................. 52
Figure 25 Recovery of Hyper-V data ..................................................................... 53
Figure 26 Recovery Wizard ................................................................................... 54
Figure 27 Select quick migration destination node ................................................ 56
Figure 28 Save memory ......................................................................................... 57
Figure 29 Select live migration destination node ................................................... 58
Figure 30 Live migration progress ........................................................................ 58
Figure 31 Initiate quick storage migration ............................................................. 60
Figure 32 Migrate Virtual Machine Wizard .......................................................... 60
Figure 33 VNXe Hyper-V replication flowchart .................................................... 64
Figure 34 Replication Connections page ............................................................... 65
<p>| Figure 35 | Add Replication Connection Wizard | 66 |
| Figure 36 | Generic iSCSI Storage page | 67 |
| Figure 37 | Add a host | 68 |
| Figure 38 | Create an application set | 68 |
| Figure 39 | Application Set Name and Objects page | 69 |
| Figure 40 | Completing the Application Set Wizard page | 70 |
| Figure 41 | Job Wizard | 71 |
| Figure 42 | Job Name and Settings page | 72 |
| Figure 43 | Celerra replication storage page | 73 |
| Figure 44 | Mount Options page | 73 |
| Figure 45 | Starting the Job page | 74 |
| Figure 46 | Run a job | 75 |
| Figure 47 | View Replication Manager snapshots | 75 |
| Figure 48 | Mount a replica | 76 |
| Figure 49 | Replication failover | 77 |
| Figure 50 | iSCSI Server Settings | 80 |
| Figure 51 | iSCSI Server Settings page | 81 |
| Figure 52 | iSCSI Server wizard | 82 |
| Figure 53 | Host Wizard page | 84 |
| Figure 54 | Operating System page | 85 |
| Figure 55 | iSCSI Access page | 86 |
| Figure 56 | Microsoft iSCSI service message | 88 |
| Figure 57 | iSCSI target discovery | 89 |
| Figure 58 | Discover Portal | 89 |
| Figure 59 | Discover Target Portal dialog box | 90 |
| Figure 60 | Advanced Settings dialog box | 91 |
| Figure 61 | Configure MCS | 92 |
| Figure 62 | Multiple Connected Session (MCS) dialog box | 93 |
| Figure 63 | Add a new connection | 94 |
| Figure 64 | Disk Management page | 96 |
| Figure 65 | Bring the disk online | 97 |
| Figure 66 | Passthrough disk | 98 |
| Figure 67 | Extend existing volume | 99 |
| Figure 68 | Extend storage pool | 102 |
| Figure 69 | Extend a Hyper-V data store | 103 |
| Figure 70 | Modify host access | 104 |
| Figure 71 | Delete a storage pool | 105 |
| Figure 72 | System Capacity page | 110 |
| Figure 73 | System Health page | 111 |
| Figure 74 | Health status Icons | 111 |
| Figure 75 | Storage Resource Health page | 112 |
| Figure 76 | CPU utilization | 112 |
| Figure 77 | System Alerts page | 113 |
| Figure 78 | Alert Severity icons | 114 |
| Figure 79 | Logs page | 114 |
| Figure 80 | Logging standards | 115 |
| Figure 81 | Support options | 115 |</p>
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Default storage pools</td>
<td>20</td>
</tr>
<tr>
<td>Table 2</td>
<td>Storage protection recommendations for Hyper-V data stores</td>
<td>20</td>
</tr>
<tr>
<td>Table 3</td>
<td>Ratings for various disk types for Hyper-V Storage - Database</td>
<td>27</td>
</tr>
<tr>
<td>Table 4</td>
<td>Ratings for various disk types for Hyper-V Storage - Datastore</td>
<td>28</td>
</tr>
<tr>
<td>Table 5</td>
<td>Ratings for various disk types for Hyper-V Storage - General Purpose</td>
<td>28</td>
</tr>
<tr>
<td>Table 6</td>
<td>Protection size recommendations</td>
<td>30</td>
</tr>
<tr>
<td>Table 7</td>
<td>Host access levels</td>
<td>31</td>
</tr>
<tr>
<td>Table 8</td>
<td>VNXe model components and limits</td>
<td>108</td>
</tr>
<tr>
<td>Table 9</td>
<td>Software configuration limits</td>
<td>108</td>
</tr>
</tbody>
</table>
This document provides an overview of the deployment options for Microsoft Hyper-V with EMC VNXe series storage arrays developed by the EMC Unified Storage Solutions group.

Purpose
Information in this document can be used as the basis for a solution build, white paper, best practices document, or training. Information in this document can also be used by other EMC organizations (for example, the technical services or sales organization) as the basis for producing documentation for a technical services or sales kit.

Audience
This document is intended for internal EMC personnel, EMC partners, and customers. Familiarity with Hyper-V and networking is assumed.

Scope
This guide describes the considerations to be taken into account when planning to deploy the Hyper-V technology on EMC VNXe series arrays, and provides installation and configuration details that will help deploy Hyper-V successfully. This solution is built and tested at the EMC Application Solutions Engineering lab in Research Triangle Park, N.C. Implementation instructions and sizing guidelines are provided.

The following areas are covered:
- Preparation and planning
- Storage provisioning
- Server configuration
- Data protection
- Data recovery

Related documents
The following document, located on the EMC Powerlink website, provide additional, relevant information. Access to these documents is based on your login credentials. If you do not have access to the content listed below, contact your EMC representative:
- EMC Replication Manager Product Guide

The following documents are available on the Microsoft website:
- Hyper-V Planning and Deployment Guide
About this Document

- DPM 2010 Datasheet - How to Protect Microsoft Virtualization Environments
- Planning a System Center Data Protection Manager 2010 Deployment
Chapter 1  EMC VNXe Series

This chapter presents these topics:

Introduction to the EMC VNXe Series................................................................. 14
Application-based provisioning overview......................................................... 16
Introduction to the EMC VNXe Series

The EMC® VNX™ family of products and supporting software is a new brand of unified storage for midtier and entry-level customers. The VNX family is made up of two series—VNX and VNXe™.

EMC VNXe series delivers exceptional flexibility for the small-to-medium business user, combining a unique, application-driven management environment with complete consolidation for all IP storage needs. Customers can benefit from the new VNXe features such as:

♦ Next-generation unified storage, optimized for virtualized applications.
♦ Capacity optimization features including file deduplication and compression, thin provisioning, and application-consistent snapshots and replicas (only available for VNXe for file).
♦ High availability, designed to deliver five 9s availability.
♦ Multiprotocol support for file and block.
♦ Simplified management with EMC Unisphere™ for a single management interface for all file, block, and replication needs.

The VNXe series includes four new software suites and two new software packs, making it easier and simpler to protect data.

Software suites available

♦ **VNXe Local Protection Suite**—Practices safe data protection and repurposing.
♦ **VNXe Remote Protection Suite**—Protects data against localized failures, outages, and disasters.
♦ **VNXe Application Protection Suite**—Automates application copies and proves compliance.
♦ **VNXe Security and Compliance Suite**—Keeps data safe from changes, deletions, and malicious activity.

Software packs available

♦ **VNXe Total Protection Pack**—Includes local, remote and application protection suites.
♦ **VNXe Total Value Pack**—Includes all three protection software suites and the Security and Compliance Suite (the VNXe3100™ exclusively supports this package).

VNXe application awareness

The VNXe platform features a simplified user interface that is designed for the IT generalist rather than a storage specialist. The key management concept is that storage is strongly tied to an application so that the storage view of the world can be easily translated into how it impacts the applications that drive a business. At the time of publication, application support is provided for:

♦ Microsoft Exchange
♦ VMware® data stores
  • Network file system (NFS)
  • VMware vStorage Virtual Machine File System (VMFS) and Raw Device Mapping (RDM) using iSCSI
♦ Hyper-V data stores using iSCSI
EMC VNXe Series

Microsoft Windows Server 2008 R2 Hyper-V on EMC VNXe Series Deployment Guide

♦ Shared folders
  • Common Internet File System (CIFS) for Windows
  • NFS for UNIX or Linux
♦ Generic application storage using iSCSI

When combined with simple wizard-driven installation and provisioning, flexible options for storage media, and EMC’s proven track record for reliability and high availability, the platform provides a low-cost entry point into the family of EMC storage.

Advantages of the VNXe platform

This section discusses the major advantages of VNXe.

Accessibility

The platform provides consolidated access to stored data from multiple hosts, users, and applications by using existing IP network connectivity and industry-standard protocols, including CIFS, NFS, and iSCSI.

Ease of management

A simple-to-use, web-based user interface to control VNXe system operations, including tools to manage, monitor, and configure storage and system settings.

High-performance, high-density storage

The platform has the ability to store data on high-speed SAS, high-capacity nearline (NL) SAS storage disk drives, and extremely fast random I/O performance with EFD disks, thus accommodating most organizational and application requirements.

Expandable capacity and flexible upgrades

The platform provides SAS, NL-SAS, and Flash resources to store and protect files, folders, and application data. The capacity of these resources can be expanded to accommodate a variety of application, host, or organization requirements.

Compliance with application storage best practices

The platform has built-in best practices to provision and manage application data such as Microsoft Exchange, Microsoft Windows Hyper-V, VMware, generic iSCSI, and shared folder storage.

Automatic or manual data protection

The platform has built-in tools to protect valuable data by using snapshot schedules to create point-in-time images of the data. Storage checkpoints from which data can be restored can be created manually or by using standard snapshot schedules or custom schedules.

High availability

Redundant disks and processors ensure that the failure of a single component of the platform does not cause a prolonged disruption to the environment. Failed components can be easily replaced and brought online without affecting users or applications.

Security

Secure system management is provided through HTTPS communication, manageable system accounts and authentication, and user roles. Secure access to VNXe storage resources is provided through Challenge-Handshake Authentication Protocol (CHAP) for iSCSI storage and compliance with NFS and CIFS access controls for storage resource security.
EMC VNXe Series

Antivirus support

VNXe supports VEE Common Anti-Virus Agent (CAVA). CAVA is a component of the VNX Event Enabler (VEE) 4.5.1, which is part of the Security and Compliance Suite. CAVA provides an antivirus solution to clients using a VNXe platform. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the VNXe platform.

File-level retention

The VNX File-Level Retention (FLR) feature provides a way to set file-based permissions to limit write access to the files for a specific period of time. FLR can ensure the integrity of data during that period by creating an unalterable set of files and directories. On VNXe, the FLR feature can be enabled for shared folders and VMware NFS data stores. FLR for VNXe is available as part of the Security and Compliance Suite.

Application-based provisioning overview

The key difference between VNXe and other storage platforms is its awareness of what applications are using storage and embedding the best practices for those applications into the provisioning and management process. Figure 1 shows the first page of the user interface.

Figure 1 VNXe management dashboard

The dashboard not only displays the usable capacity of the array in terms of the applications using it, but it also provides wizard-driven mechanisms to create additional application storage using best practices. This guide focuses on provisioning for Microsoft Hyper-V.

The provisioning process has three main steps:
1. Create a pool of storage to use
2. Configure host connectivity
3. Use the application-provisioning wizard to provision Hyper-V data stores

The first two steps are independent and can be performed in any order. The third step requires the first two to be complete. Chapter 3 Hyper-V Deployment on VNXe covers each step in detail.
This chapter presents these topics:

Overview of Microsoft Hyper-V ................................................................. 18
Connection options .................................................................................... 18
EMC VNXe benefits for Hyper-V .............................................................. 19
VNXe storage pools .................................................................................. 19
Capacity planning ..................................................................................... 20
Performance planning .............................................................................. 20
Overview of Microsoft Hyper-V

Microsoft Hyper-V is virtualization software that provides server consolidation by enabling several instances of similar and dissimilar operating systems to run as virtual machines on one physical machine. This cost-effective, highly scalable virtual machine platform offers advanced resource management capabilities.

Hyper-V minimizes the total cost of ownership (TCO) of computing infrastructure by:

♦ Increasing resource utilization
♦ Decreasing the number of servers and all associated costs
♦ Maximizing server manageability

The Hyper-V software’s architecture and deployment best practices are extensive and well beyond the scope of this paper. However, the storage best practices for the application are covered in the following sections.

Connection options

Microsoft Hyper-V and EMC VNXe support multiple connection options. 1 Gb and 10 Gb Ethernet options are available. Hardware and software iSCSI initiators can be used. The VNXe Hyper-V data store can be connected to the Hyper-V parent OS as Virtual Hard Disks (VHDs) and passthrough disks and to the guest OS using iSCSI direct as shown in Figure 2. Microsoft also supports Hyper-V guest clustering with iSCSI. iSCSI is the only supported method of providing shared disks over virtual NICs.

Figure 2  VNXe iSCSI connection options for Hyper-V
VHD

VHD is a disk image format implemented by Microsoft. Its specification is available to third parties so that other hypervisors such as XenServer can leverage this technology. VHDs are created as .vhd files that reside on the native host file system of the server running Hyper-V and support a wide range of storage types including iSCSI, or theoretically, any other file systems recognized and accessible by Windows Server 2008 R2.

You can create three types of VHDs with Hyper-V:

- Dynamically expanding—This is thin provisioning where the .vhd file grows as data is stored to the disk, up to the size specified. The .vhd file does not shrink automatically when data is deleted.
- Fixed size—The .vhd file is preallocated to the amount of space specified for the disk size, regardless of how much data is saved to the virtual hard disk.
- Differencing—This type of disk is associated in a parent-child relationship with another disk that must be left intact. It is possible to make changes to the data or operating system without affecting the parent disk. Therefore, it is easy to roll back the changes.

Passthrough disk

Passthrough disk is an alternative to VHD, whereby virtual machines have direct access to the physical disk. This is similar to Raw Device Mapping (RDM) with VMware. Passthrough is only applicable to block devices such as iSCSI or FC. The VNXe Hyper-V data store can be presented as a passthrough disk to the Hyper-V virtual machine.

iSCSI direct within the guest OS

One additional option is to expose disks directly to the guest OS (without exposing it to the parent partition) by using a software iSCSI initiator within the guest OS. Hyper-V’s virtual BIOS does not support booting to iSCSI directly, so at least one disk must be available to the guest as an IDE disk to boot to it. However, all other disks can be direct iSCSI LUNs. You can select the iSCSI direct model to manage the iSCSI targets of the guest applications in the same way that it is done in a physical environment.

EMC VNXe benefits for Hyper-V

EMC VNXe benefits Hyper-V environments in many ways:

- Simplifies the storage provisioning process for Hyper-V. The application-aware storage pool wizard understands Hyper-V requirements and builds storage pools optimizes for Hyper-V deployments automatically.
- Interfaces with Microsoft’s Volume Shadow Copy Service (VSS) to offload snapshot processing to the storage processors.
- Asynchronously replicates Hyper-V storage either to a separate location within the same storage array (local replication) or to a completely different storage array (remote replication) using an Internet Protocol (IP) network (extra licensing required).

VNXe storage pools

The VNXe platform does not provision storage by using a traditional model where users build a RAID group and then build logical disk units in that group. Instead, VNXe creates pools of storage. The members of this pool all have similar characteristics. Using this approach, application-based storage provisioning is possible. This is discussed in the next section.
Default storage pools

Even though the RAID group and the LUN groupings are not exposed to the user, the array is still using those mechanisms behind the scenes to ensure that the data is properly protected. Table 1 lists the storage pools that are available by default and also describes their characteristics. Four default storage pools are available on the VNXe series.

<table>
<thead>
<tr>
<th>Pool name</th>
<th>Disk type</th>
<th>RAID type</th>
<th>Available capacities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme performance</td>
<td>EFD</td>
<td>RAID 5 (4+1)</td>
<td>100 GB</td>
</tr>
<tr>
<td>High performance</td>
<td>SAS</td>
<td>RAID 10 (3+3)</td>
<td>300 GB 600 GB</td>
</tr>
<tr>
<td>Balanced performance/Capacity</td>
<td>SAS</td>
<td>RAID 5 (6+1) – VNXe3300™</td>
<td>300 GB 600 GB</td>
</tr>
<tr>
<td>Capacity pool</td>
<td>NL-SAS</td>
<td>RAID 6 (4+2)</td>
<td>1 TB 2 TB</td>
</tr>
</tbody>
</table>

Custom storage pools

The default storage pools can be augmented with custom storage pools, which are user-defined. In general, it is recommended to use custom pools for performance-sensitive applications such as Exchange because the custom pool mechanism enables precise control of how many disks are used in the pool and prevents other applications from sharing the disks without explicitly provisioning application storage from the custom pool.

Capacity planning

You must calculate the required sizes of the iSCSI LUNs for Hyper-V. Use the results to calculate the capacity needed in the storage pools. Ensure that extra space required for the protection storage for replication and snapshots is considered. The minimum amount of protection storage space for a Hyper-V data store (a Hyper-V data store is a LUN formatted as NTFS for holding VHDs) is 105 percent of each iSCSI LUN size. Table 2 shows the recommended amount of protection storage based on the snapshot schedule chosen.

<table>
<thead>
<tr>
<th>Protection schedule</th>
<th>Create snapshots every</th>
<th>Keep for</th>
<th>Recommended protection size</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>N/A</td>
<td>N/A</td>
<td>105% of primary storage</td>
</tr>
<tr>
<td>Default</td>
<td>Day at 3:00</td>
<td>7 days</td>
<td>135% of primary storage</td>
</tr>
<tr>
<td>More Protection</td>
<td>Day at 3:00 and 11:00</td>
<td>14 days</td>
<td>135% of primary storage</td>
</tr>
<tr>
<td>Less Protection</td>
<td>Day at 03:00</td>
<td>3 days</td>
<td>135% of primary storage</td>
</tr>
</tbody>
</table>

Performance planning

VNXe has predefined storage pools that can be used based on the performance requirements and the drives in the platform. Enterprise Flash Drives (EFDs) provide the greatest performance followed by 15k rpm SAS drives. Do not use 7200 rpm NL-SAS drives for performance-sensitive applications. They are primarily used for capacity.
Also, place Hyper-V servers on the same VLAN (or LAN segment) and IP subnet as the VNXe iSCSI target ports. Use 1 Gb or 10 Gb Ethernet for maximum speed. Avoid switch and interconnect oversubscription where possible.
This chapter presents these topics:

- Provisioning overview .......................................................... 24
- Create virtual machines ...................................................... 32
- Provisioning summary ....................................................... 32
Provisioning overview

The VNXe platform for Hyper-V results in a highly available, protected environment with simplified management. It enables administrators to create, configure, and manage storage for Hyper-V virtual machines. Easy-to-use wizards automate the storage provisioning for Microsoft Hyper-V virtual machines by using embedded best practices engines. The Hyper-V administrator with little or no storage expertise can easily deploy and manage storage resources to meet the business requirements. Figure 3 shows the steps involved in deploying the Hyper-V environment by using VNXe storage.

Figure 3  VNXe Hyper-V storage provisioning flowchart

Initial setup of EMC VNXe storage

The VNXe system configuration refers to the hardware setup, cabling, software installation, and activation of the required licenses. It is assumed that the VNXe platform is in a healthy state with proper network connectivity and with an IP address assigned to the management port. All the initial installation steps of the VNXe platform are not discussed in this document. The GUI of the VNXe platform is accessed by using the management IP or hostname of the VNXe platform.

Hyper-V server configuration

The Windows Server 2008 R2 operating system must be installed on the host machines that will use the VNXe storage. The Hyper-V role must be installed on the server to host virtual machines. The Hyper-V Planning and Deployment Guide available on the Microsoft website provides details about the planning and configuration of Hyper-V.

Create iSCSI Servers for VNXe

An iSCSI Server is an iSCSI service that functions as a storage resource in a distributed iSCSI network and provides one iSCSI target. To use the VNXe Hyper-V storage, the VNXe platform requires at least one iSCSI Server. Each iSCSI Server is independent of the other iSCSI Server. If an iSCSI Server is not added during the VNXe installation, use Unisphere to add the iSCSI
Hyper-V Deployment on VNXe

Microsoft Windows Server 2008 R2 Hyper-V on EMC VNXe Series

25

Deployment Guide

Hyper-V Deployment on VNXe

Add Hyper-V Servers and guest OSs as hosts in VNXe

This step is implemented whenever a Hyper-V server or a guest OS is added for the first time. If the host is already configured, skip to the next step, or else follow the steps covered in Appendix B Host Creation in VNXe.

Create storage pools for VNXe Hyper-V

A storage pool is an aggregation of storage disk resources that is configured with a particular storage profile. The storage profile defines the type of disks that are used to provide storage and the type of RAID configured on the component disks. The storage pool configuration defines the number of disks and the quantity of storage associated with the pool. When multiple pools are configured, choose the pool to use when creating new storage resources. If only one storage pool is available, the available pool is automatically assigned to the new storage resources. Before VNXe storage resources are created, configure at least one storage pool and allocate storage disks to that pool. Storage pools are usually configured to optimize the available storage for a particular set of applications or conditions.

To create storage pools, complete the following steps:

1. To access storage pools in Unisphere, click the System tab, and then click Storage Pools.

![Storage Pools link in Unisphere](image)

2. To create a new storage pool, click Configure Disks.

3. The Disk Configuration Wizard appears. Select the disk configuration mode.

Storage pools can be automatically configured, which consumes all disks on the platform in a generic manner, or created as needed with different drive characteristics per pool. Pools can be specifically created for Hyper-V. By default, three types of Hyper-V application-specific profiles are available:
Hyper-V Deployment on VNXe

- Hyper-V storage for a database
- Hyper-V storage for a data store
- General purpose Hyper-V storage

Select the application type and click Next.

**Figure 5** Disk Configuration Wizard

4. The **Specify Pool Name** page appears. Type a name and a description for the storage pool.

5. The **Select Storage Type** page appears. The VNXe platform provides a list of disk type recommendations that are ranked according to the application chosen. Select the disk type that best fits the intended use.
The following section discusses the disk types and their ratings for all three Hyper-V applications.

- **Hyper-V Storage – Database**
  
  Table 3 lists the disk types and their ratings when Hyper-V Storage – Database is selected as the storage pool.

### Table 3 Ratings for various disk types for Hyper-V Storage - Database

<table>
<thead>
<tr>
<th>Rating</th>
<th>Disk Type</th>
<th>Storage profile</th>
<th>Underlying RAID configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>***</td>
<td>EFD</td>
<td>Best Performance</td>
<td>RAID 5 (4+1)</td>
</tr>
<tr>
<td>**</td>
<td>SAS</td>
<td>High Performance</td>
<td>RAID 10 (3+3)</td>
</tr>
<tr>
<td>*</td>
<td>SAS</td>
<td>Balanced Performance/Capacity</td>
<td>RAID 5 (6+1)</td>
</tr>
<tr>
<td></td>
<td>NL-SAS</td>
<td>High Capacity</td>
<td>RAID 6 (4+2)</td>
</tr>
</tbody>
</table>

A rating of three stars is the best disk type and a rating of zero stars is the worst disk type. The Disk Configuration Wizard shows how much space is available for each storage profile based on unassigned drives in the array.

- **Hyper-V Storage – Datastore**
  
  Table 4 on page 28 lists the storage types and their ratings when Hyper-V Storage – Datastore is selected as the storage pool.
Table 4  Ratings for various disk types for Hyper-V Storage - Datastore

<table>
<thead>
<tr>
<th>Rating</th>
<th>Disk type</th>
<th>Storage profile</th>
<th>Underlying RAID configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>EFD</td>
<td>Best Performance</td>
<td>RAID 5 (4+1)</td>
</tr>
<tr>
<td>**</td>
<td>SAS</td>
<td>High Performance</td>
<td>RAID 10 (3+3)</td>
</tr>
<tr>
<td>***</td>
<td>SAS</td>
<td>Balanced Performance/Capacity</td>
<td>RAID 5 (6+1)</td>
</tr>
<tr>
<td></td>
<td>NL-SAS</td>
<td>High Capacity</td>
<td>RAID 6 (4+2)</td>
</tr>
</tbody>
</table>

The VNXe term “data store” in Hyper-V is an iSCSI LUN formatted with NTFS that holds VHDs. The maximum LUN size supported by Hyper-V is 2 TB, the maximum LUN size supported by VNXe is 1.99 TB, and the maximum VHD file size supported by Hyper-V is 2,040 GB.

- Hyper-V Storage - General Purpose

Table 5 lists the storage types and their ratings when Hyper-V Storage - General Purpose is selected as the storage pool.

Table 5  Ratings for various disk types for Hyper-V Storage - General Purpose

<table>
<thead>
<tr>
<th>Rating</th>
<th>Disk type</th>
<th>Storage profile</th>
<th>Underlying RAID configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFD</td>
<td></td>
<td>Best Performance</td>
<td>RAID 5 (4+1)</td>
</tr>
<tr>
<td>*</td>
<td>SAS</td>
<td>High Performance</td>
<td>RAID 10 (3+3)</td>
</tr>
<tr>
<td>***</td>
<td>SAS</td>
<td>Balanced Performance/Capacity</td>
<td>RAID 5 (6+1)</td>
</tr>
<tr>
<td>**</td>
<td>NL-SAS</td>
<td>High Capacity</td>
<td>RAID 6 (4+2)</td>
</tr>
</tbody>
</table>

A rating of three stars is the best disk type and a rating of zero stars is the worst disk type. The Disk Configuration Wizard shows how much space is available for each storage profile based on unassigned drives in the array.

6. The Select Amount of Storage page appears. Select the number of disks to add to the storage pool. The options depend on the RAID type associated with the storage profile selected in step 5. Click Next.

You can select disks only in multiples of the number of drives present in the base RAID group.

![Select Amount of Storage page](image-url)
7. The **Summary** page appears. Review the details and click **Finish** to complete the storage pool creation.

**VNXe: Create Hyper-V data stores and grant access to hosts**

To create Hyper-V data stores and grant access to hosts, complete the following steps:

1. In Unisphere, click the **Storage** tab, and then click **Microsoft Hyper-V**.
2. The **Hyper-V Storage** page appears. Click **Create**.
3. Type a name and description for the Hyper-V data store.
4. The **Configure Storage** page appears. Complete the following steps:
   a. Based on the performance requirement, select the storage pool from the list of pools available in the table.
   b. In the **Size** field, type the required size for the Hyper-V data store.
   c. To enable thin provisioning, select **Enabled** for the **Thin** field. The initial allocation will be 10 GB.
   d. Click **Next**.

![Configure Storage page](image)

**Note**: The default size of the Hyper-V data store is 100 GB. The maximum size possible is 1.999 TB and the minimum size required is 10 GB.

5. The **Configure Protection** page appears. Configure the protection storage as required for replication and snapshots. Click **Next**.

   “VNXe iSCSI snapshots” on page 44 provides more information about snapshot protection.
Figure 9 Configure Protection page

6. The Configure Protection Storage Size page appears. In the Protection Size field, type the protection reserve size for the Hyper-V data store. Click Next.

Table 6 provides recommendations on the protection size.

<table>
<thead>
<tr>
<th>Virtual provisioning</th>
<th>Protection size - No protection</th>
<th>Protection size - Allow protection (No snapshot schedule)</th>
<th>Protection size - Allow protection (Snapshot schedule configured)</th>
<th>Maximum protection size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min/Default</td>
<td>Min Default</td>
<td>Default/Recommended Min</td>
<td>Default/Recommended Min</td>
<td>14 TB</td>
</tr>
<tr>
<td>Enabled</td>
<td>0%</td>
<td>105%</td>
<td>105%</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>0%</td>
<td>5%</td>
<td>5%</td>
<td>14 TB</td>
</tr>
</tbody>
</table>
Figure 10  Configure Protection Storage Size page

7. The Configure Host Access page appears. Select host access for the Hyper-V data store. Click Next.

VNXe provides four access levels for the Hyper-V data store. Table 7 describes the four access levels.

Table 7  Host access levels

<table>
<thead>
<tr>
<th>Access level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>The host cannot access the storage.</td>
</tr>
<tr>
<td>Hyper-V Datastore</td>
<td>The host can access the storage but not the snapshots.</td>
</tr>
<tr>
<td>Snapshot</td>
<td>The host can access only promoted snapshots but not the primary storage.</td>
</tr>
<tr>
<td>Hyper-V Datastore and Snapshot</td>
<td>The host can access both the primary storage and the promoted snapshots.</td>
</tr>
</tbody>
</table>

Note: It is recommended to avoid granting data store access to more than one host unless the hosts are part of the same cluster.
8. The Summary page appears. Review the summary of the Hyper-V resource allocation and click Finish.

9. Click Close to exit the wizard. After the successful creation of the Hyper-V storage, view it in the Hyper-V page.

Connect Hyper-V hosts to VNXe Hyper-V storage

The connection to the VNXe Hyper-V storage from the host may vary based on the version of the iSCSI software available at the time of deployment and the choice of software or hardware iSCSI initiator. Appendix C Host iSCSI Configuration provides instructions about using the Microsoft iSCSI Initiator.

Set up Hyper-V hosts to use the data store

The VNXe Hyper-V data store is formatted on Hyper-V servers or the guest OS as NTFS so that it is presented to the Hyper-V environment either as VHD or passthrough, respectively. Appendix D Host Configuration of iSCSI Volumes describes the steps on how to present the data store in both cases.

Create virtual machines

The Hyper-V data store is ready for deploying virtual machines. The creation of virtual machines is beyond the scope of this guide.

Provisioning summary

This section described how to provision storage to Hyper-V environments by using the VNXe platform. The process involves creating a custom storage pool, configuring host access, and running the deployment wizard. Additional operations such as expanding the existing installation
and monitoring the environment are covered in Appendix E VNXe Platform Management and Appendix G VNXe System Monitoring, respectively.
This chapter presents these topics:

High Availability overview ................................................................. 36
VNXe High Availability architecture ..................................................... 36
High Availability overview

High Availability is the idea that data should be safe in a wide variety of normally troubling conditions. It encompasses the idea that minor failures should be nondisruptive to the ongoing operation of a system and major failures should be recovered as quickly and easily as possible. This chapter provides recommendations to ensure that the Hyper-V environment deployed on the VNXe platform is able to meet these challenges.

VNXe High Availability architecture

The architecture of the VNXe series of storage arrays is such that there is no single point of failure. If a hardware or software component fails, the VNXe platform automatically takes appropriate action to return to a normal operating condition.

Active-Active clustering

The VNXe has two identical storage processor blades in the hardware chassis. During normal operations, both are active and serving data. This is called an active-active configuration. If one fails during normal operations, the surviving blade takes over the work assigned to both blades until the second one is back online. This may affect the overall performance of the system, but it continues to serve data.

Note: There is a single storage processor variant of the VNXe3100 where active-active clustering is not possible.

No single point of failure

The architecture of the internal hardware of the array is such that the failure of any one component, such as a disk drive, power supply, or an internal data transfer connection, does not cause data to become unavailable.

The external network is similarly protected. VNXe supports iSCSI multipathing and Ethernet link aggregation to protect against network link failures. It is also recommended to design the network architecture for high availability by using multiple switches. However, the design of such a network is not in the scope of this guide.

It is highly recommended to apply the network settings of one storage processor (SP) blade to the other SP blade so that in the event of a failover, the surviving SP can continue to service operations.

These architectural decisions lead to EMC’s reputation for having 99.999 percent or “five 9s” uptime.

RAID group hot spares

An important addition to the concept of RAID groups is that the array can automatically rebuild the faulted drive on to a spare drive. After the RAID group member is rebuilt, the group is once again resilient to single disk failures. On EMC arrays, the designated spare drive for rebuild operations is called a hot spare.

Hot spare recommendations

It is recommended to create a hot spare drive for every 30 active drives on the VNXe platform. So for 60 active drives, two hot spare drives are required. It is recommended to have at least one hot spare for every type of drive on the VNXe platform. For example, for 14 SAS drives and 12 NL-SAS drives, it is considered a best practice to have one SAS hot spare and one NL-SAS hot spare.
Create a hot spare drive

To create a hot spare drive, complete the following steps:

1. In Unisphere, click the System tab, and then click Storage Pool.
2. Click Configure Disks.
3. The Disk Configuration Wizard appears. Select Manually add disks to an existing pool, and then select Hot Spare Pool from the pool list.
4. The Configure Spares page appears. Select the number of hot spares to configure for each type of drive on the VNXe platform. The recommended value is indicated with a star.

**Note:** It is a best practice to adhere to the number of hot spares recommended by the system.

5. The Summary page appears. Confirm the selections and click Finish.
This chapter presents this topic:
VNXe performance overview................................................................. 40
**VNXe performance overview**

This chapter describes the use case that was developed to test the performance of the VNXe platform in the Hyper-V environment. The main intention of this use case was to showcase the performance of VNXe in the Hyper-V environment when scaling virtual machines and servers.

**Use case overview**

This use case was designed to analyze the performance of VNXe when scaling both virtual machines and servers. The Iometer tool was used to generate the load and to analyze the performance under a realtime workload.

A Hyper-V application-specific storage pool was created with 600 GB SAS drives and four 4+1 RAID 5 groups. Two Hyper-V data stores were created on this application-specific pool and shared as Cluster Shared Volumes (CSV) to two Hyper-V failover clusters using the Microsoft iSCSI connection as shown in Figure 13.

![Use case reference architecture](image)

**Figure 13** Use case reference architecture

**Test methodology**

Twenty-five Hyper-V virtual machines were created on VNXe Hyper-V data stores. Each virtual machine had an OS drive and application drives. The load had been generated on some portion of each virtual machine’s application drive using Iometer. Initially, the performance was analyzed when the virtual machines were scaled from 1 to 5 on the same Hyper-V server by running Iometer tests and then the Hyper-V servers were scaled from 1 to 5.

**Results**

Figure 14 on page 41 shows the performance behavior of VNXe when the virtual machines and the Hyper-V servers are scaled. The graph shows the average IOPS and the average I/O response times.
Figure 14  Performance behavior

The graph shows that the throughput increases linearly in both virtual machine and Hyper-V server scaling scenarios. There is a slight variation in response times when virtual machines are scaled, and response times increased when Hyper-V servers are scaled.
This chapter presents these topics:

Overview ....................................................................................................................................... 44
Protection storage considerations .................................................................................................. 44
VNXe iSCSI snapshots ................................................................................................................. 44
Snapshot use cases ........................................................................................................................ 47
Backup and recovery ..................................................................................................................... 49
Overview

Data protection for VNXe consists of three categories—snapshots, VNXe user data backup, and replication. This chapter describes the Hyper-V environment protection using VNXe snapshots and the Hyper-V environment backup using Microsoft Data Protection Manager (DPM) 2010.

Protection storage considerations

Along with deciding the storage requirements for the Hyper-V virtual environment, the administrator also has to consider the amount of storage reserved for protection. The amount of resources that a snapshot schedule consumes is primarily affected by the frequency of the scheduled snapshot operations and the length of time that the snapshots are retained. When creating a VNXe storage resource, it is safe to use the recommended protection storage amount or an amount greater than that. The depleted protection resources can lead to data loss in the storage resource primary or protection data. To use the snapshot data for testing or debugging purposes, it is recommended to create manual snapshots. Because VNXe snapshots work at the LUN level, it is important to keep all the virtual machine files (.vhd, .vsv, .xml, and so on) on the same VNXe data store for a successful recovery.

VNXe iSCSI snapshots

A snapshot of a Hyper-V storage resource creates a point-in-time, read-only virtual copy of the Hyper-V storage resource, its virtual disk, and the files and data on the virtual disk. Each production LUN resides within its own file system. All the snapshots for the LUN reside within the same file system. The file system is enabled with auto-extend, regardless of the virtually provisioned status for the LUN, and grows as more snapshot space is needed. Deleted snapshots free up space within the file system and this free space can then be reused.

Snapshots can be in one of the following states:

♦ Unmountable—The snapshot has not been promoted and does not currently have a LUN ID associated with it.
♦ Mountable—The snapshot has been promoted, has a LUN ID, and may be mounted read/write by a host. The host may write to the snapshot, but the changes are lost when the snapshot is unmounted and moved back to the not mountable state.
♦ Restoring—The snapshot is used to restore a production LUN to a point in time.

Snapshots can be created in many ways—scheduled, manual, and snapshots initiated by backup applications. The following section explains each method in detail.

Scheduled snapshots

Because data can change rapidly, snapshots can become out of date quickly. The VNXe platform provides tools to choose and customize snapshot schedules that specify regular times to perform snapshot operations (such as automatic snapshot creation and deletion). With these tools, the intervals, times, days, and dates at which the snapshot operations occur can be selected. A collection of rules within the schedule specify the interval, frequency, and time that the snapshots are taken.

During provisioning of the Hyper-V data store, the Disk Configuration Wizard provides an option of automatically scheduling snapshots with a default snapshot schedule. The administrator may modify the snapshot schedule. Scheduling may be done on a combination of hourly, daily, weekly, and monthly schedules. Each schedule entry specifies the length of time to retain the snapshots. Scheduled snapshots may also be deleted by a manual delete.

There are three system-defined snapshot protection schedules:
Less Protection—Takes a snapshot of the data store every day at 13:30 and saves the snapshot for 3 days.

Default Protection—Takes a snapshot of the data store every day at 13:30 and saves the snapshot for 7 days.

More Protection—Takes snapshots twice everyday at 13:30 and 21:30 and saves them for 14 days.

These default protection schedules can be modified or a new protection schedule can be created to match the requirements.

To create or modify a protection schedule, complete the following steps:

1. In the Configure Protection page of the Hyper-V Storage Wizard (Figure 9 on page 30), click the Customize Schedule button.

2. A dialog box appears where you need to click No to modify the VNXe predefined schedule, and click Yes to create a new schedule.

3. If Yes is clicked, type a name for the new schedule as shown in Figure 15. By default, it displays two rules that can be modified or removed by using Modify and Remove respectively. Click Add a New Rule to define a new rule.

4. The Add Schedule Rule dialog box appears. Select the rule from the Type of Rule list box. The type of rule can be specified as a combination of hours, days, and months. Based on the type of rule selected, the Rule Details displayed in the dialog box will change. When finished, click Add Rule.
VNXe Hyper-V Protection

Figure 16 Add Schedule Rule dialog box

5. The **Configure Protection** page appears (Figure 15 on page 45). To pause the schedule initially and later resume it, select the **Create Storage with Schedule Initially Paused** checkbox.

6. After creating or modifying the protection schedule, click **Revert to Previously Defined Schedule** to discard the changes and return to the previous schedule.

On-demand snapshots

VNXe provides a way for administrators to manually initiate a snapshot of the Hyper-V data store.

To initiate a manual snapshot, complete the following steps:

1. In **Unisphere**, click the **Storage** tab, and then click **Microsoft Hyper-V**.
2. Select the Hyper-V data store and click **Details**.
3. Click the **Snapshots** tab, and then click **Take Snapshot Now**.

Figure 17 Hyper-V snapshots

4. The **Take Snapshot** dialog box appears. Complete the following steps:
a. In the **Name** field, type a name for the snapshot.
b. In the **Keep For** box, type or select the number of days to store the snapshot in the protection storage. After the snapshot completes the specified time, it is deleted automatically.
c. Click **OK**.

![Take Snapshot Now dialog box](image)

**Figure 18** Take Snapshot Now dialog box

5. The snapshot is taken immediately and can be viewed in the snapshots list.

Manual snapshots can be distinguished from scheduled snapshots by checking the **Taken by** column entry. Manual snapshots are displayed with the taken by entry as **admin** and scheduled snapshots are entered with the schedule name.

### Snapshot use cases

VNXe snapshots can be used to restore lost data. When a VNXe Hyper-V snapshot is promoted, the snapshot image becomes read/write enabled. Therefore, it is known as a temporary writeable snapshot (TWS). Because you can provision TWS rapidly and present it to the same or a different host, consider the following use cases for VNXe Hyper-V snapshot features:

- **Snapshot restore**
- **Test/dev environment**
- **Snapshots for backup applications**

#### Snapshot restore

Many times, data loss occurs due to the accidental deletion of files or due to the corruption of data or files. To retrieve the data, snapshots can be restored to previous point-in-time copies. It is recommended to power off virtual machines during the snapshot restoration process.

To restore a snapshot, select the snapshot that is taken at a specific time before the data loss occurred and click **Restore**, as shown in **Figure 17** on page 46.

**Note:** After the snapshot restore is completed successfully, the data store is moved to its previous point-in-time copy. Hence, all the snapshots that were created after this time are deleted.

#### Test/dev environment

VNXe snapshots can be promoted as TWS where a writeable point-in-time copy of the Hyper-V data store is mounted on the hosts that have snapshot access. For temporary usage of virtual machines, rather than creating new virtual machines, mount the snapshot and use the virtual machines. It saves a lot of time and effort in creating a similar environment as the promoting snapshot will be spontaneous.
Figure 19 on page 48 shows an example of an end-to-end path from the mapped network drive on a Windows host to the Hyper-V storage resource and to the snapshots of the Hyper-V storage resource. On Host A, drive D: maps to the virtual disk LUN 0. In accordance with the snapshot schedule, the VNXe platform makes a copy of the Hyper-V storage resource every weekday at 1:00 A.M. A user promoted the snapshot created on Friday. During promotion, the virtual disk in the snapshot received a LUN ID (128), which makes it accessible to any host with snapshot access. The user on Host B maps the virtual disk on the host, assigning the virtual disk LUN 128 to drive F:. The user can explore and recover files from the virtual disk in the snapshot.

**Figure 19 VNXe snapshot promotion process**

To promote a snapshot of the Hyper-V data store, complete the following steps:

1. Select Storage > Hyper-V and select the data store.
2. Click Details and select Snapshots.
3. Select the snapshot to promote and click Promote as shown in Figure 17 on page 46.
4. A dialog box appears prompting for confirmation. Click Yes.

After the snapshot is promoted successfully, the status of the snapshot in the Promoted column changes to Yes.

**Snapshots for backup applications**

Using a snapshot of the LUN provides two benefits:

- The snapshot is a consistent point-in-time version of the LUN. The contents of the LUN do not change during the backup process.
♦ The snapshot may be mounted directly on the backup server during the backup. Therefore, it is not necessary for the production host to participate in the backup.

The backup application can use any of the following snapshots for its backup:

♦ A snapshot that was generated by the automated schedule.
♦ A snapshot that was generated manually.
♦ If the backup application supports Microsoft VSS, it may use the VNXe platform’s VSS hardware provider to generate the snapshot. VSS enables the backup application to quiesce an application using the LUNs and then take an array-based snapshot of the LUNs. The snapshots of the LUNs are in an application-consistent state and are used in the backup.

Regardless of how the snapshot was generated, the backup application cannot use the snapshot until it moves the snapshot to the Mountable state, making it mountable by the backup host. The backup application can either use VSS or the CLI to make it mountable. The administrator can also do it manually through the user interface.

Backup and recovery

When a backup and recovery strategy for a Hyper-V virtualized server environment is planned, there are several factors to consider such as the different types of backups that are possible, the state of the virtual machine, and the type of storage provisioning (VHD or Passthrough disk) for virtual machines.

Backup strategy

The backup strategy can be logical or physical. A logical backup does not provide a physical, independent copy of the production data. It offers a view of the Hyper-V data store at a certain point in time. A logical backup can occur very rapidly, and requires very little space to store the backup. Therefore, a logical backup can be taken very frequently. Restoring from a logical backup can be quick as well, depending on the amount of data changes. This dramatically reduces the mean time to recovery. However, a logical backup cannot replace a physical backup. The logical backup protects against logical corruption of the Hyper-V data stores, accidental deletion of files in the virtual machines, and other human errors, but it does not protect from hardware failures. The logical backup can be provided by the VNXe snapshot. If multiple virtual machines share the same Hyper-V data store, it is possible to back up and recover them together in one operation. But the loss of the production Hyper-V data store LUN renders the snapshots unusable.

A physical backup takes a full and complete copy of the Hyper-V data store to a different physical media. Although the backup and recovery time may be longer, a physical backup protects against any hardware failure. Third-party backup applications can use VNXe snapshots to back up individual Hyper-V data stores. These snapshots may be mounted directly on the backup server during the backup. Therefore, the production host is not required to participate in the backup. However, the administrator has to note that performance impacts may occur due to spindle contention when reading from the snapshots.

Hyper-V host and guest-based backups

A backup application that is compatible with Hyper-V and the Hyper-V VSS writer can perform a full server backup, which helps protect all the data required to fully restore the server. The data included in such a backup includes the configuration of virtual machines, snapshots associated with the virtual machines, and virtual hard disks used by the virtual machines. Therefore, using this method makes it easy to recover the server if required because no re-creation of virtual machines or reinstallation of Hyper-V is required. Guest-based backups offer the ability to exclude certain file types from backups. This exclusion mechanism is not available for the image level. One approach is to protect the Hyper-V virtual environment by using both file and image levels. An example of this is infrequent full-server backups followed by a daily guest-level
backup to frequently protect selective files. Administrators can restore the relevant full-level backup followed by the recovery of any individual files.

Backup and recovery using DPM 2010

DPM can be considered as one of the backup solutions to protect the Hyper-V virtualized environment that is hosted on the VNXe platform. DPM can provide application-consistent backups of all virtual machines residing on a Hyper-V server. It can restore virtual machines to an alternate Hyper-V server. DPM can even restore individual files from an image-level backup. The following section explains how to back up Hyper-V virtual machines hosted on a VNXe platform using DPM 2010.

Backup of VNXe Hyper-V storage using DPM 2010

DPM 2010 is preferred as the backup technology because it takes Hyper-V application-aware snapshots. It supports the Hyper-V Live Migration feature, including CSV protection.

DPM 2010 supports the backup of the Hyper-V environment at various levels:

- Entire Hyper-V data store on which virtual machines are created
- Hypervisor level – Virtual machines along with the initial Store configuration file
- Online backup of supported guest virtual machines that are hosted on clustered or stand-alone systems

Figure 20 is a flowchart that shows the steps to protect the VNXe Hyper-V environment using DPM 2010.

DPM 2010 installation

Microsoft DPM 2010 must be installed on Windows Server 2008 or Windows Server 2008 R2, which acts as the DPM server. The installation process is out of scope of this document.

Backup destination provisioning in VNXe

The DPM backup destination can be provisioned by using the VNXe Hyper-V storage. Chapter 3 Hyper-V Deployment on VNXe provides details about creating the Hyper-V data store. The destination data store size is recommended to be at least 2.5 to 3 times the source data store size. The host access for this destination storage must be given to the DPM server.
Add destination disks to the DPM storage pool

To add a destination disk to the DPM storage pool, complete the following steps:

1. Connect the destination storage by using the iSCSI initiator from the DPM server. Appendix C Host iSCSI Configuration and Appendix D Host Configuration of iSCSI Volumes provide further details about how to connect to the destination storage.

2. Bring the disk online in Disk Management.

3. Start the DPM 2010 Administrative Console.

4. Select Management, and then click the Disks tab. Click Add from the Actions pane.

5. Select one or more destination disks and click Add. Click OK.

Install DPM Agents

The DPM Agent software must be installed on the hosts that access the VNXe Hyper-V storage to communicate with the DPM server.

To install DPM Agents, complete the following steps:

1. From the DPM 2010 Administrator Console, click the Management tab, and then click the Agents tab.

2. Click Install from the Actions pane.

3. The Protection Agent Installation Wizard appears. Select the hosts on which the agent must be installed or attach the hosts if the agent is already installed on the hosts.

4. Complete the wizard by providing login credential information and specify whether to reboot the hosts after the agent installation.
Create a protection group

To create a protection group, complete the following steps:

1. From the **DPM 2010 Administrator Console**, click the **Protection** tab.

2. Click **Create protection group** from the **Actions** pane to start the process.

3. The **Create New Protection Group** wizard appears. Click **Next**.

4. The **Select Protection Group Type** page appears. Select **Servers** and click **Next**.

   When a protection group is created, you can choose to protect servers or clients. To protect servers, it is necessary to predeploy the agent on the server to select the protection information based on the role of the server.

5. The **Select Group Members** page appears. Select **HyperV**, click “+” to expand it, and select the appropriate options. Click **Next**.

   Other protection options available are Shares, Volumes, and System Protection. By selecting Hyper-V, all virtual machines registered on the Hyper-V server and the Hyper-V data store are automatically protected.

6. The **Select Data Protection Method** page appears. Type a name for the protection group, select **I want short-term protection using Disk**, and click **Next**.
7. The **Specify Short Term Goals** page appears. Type or select the retention range (the amount of time to retain the protection) and click **Next**.

The default application recovery point setting of performing an express full backup once a day is maintained.

8. The **Review Disk Allocation** page appears. Accept the default selections and click **Next**.

9. The **Choose Replica Creation Method** page appears. Maintain the default setting of using the network to transfer the replica data, ensure that **Now** is selected so that the replica is captured immediately, and click **Next**.

10. The **Consistency Check Options** page appears. Select **Run a consistency check if the replica becomes inconsistent** and click **Next**.

11. The **Summary** page appears. Verify the options selected and click **Create Group**.

### Hyper-V data restore

The following types of restore options are possible on the VNXe platform hosting the Hyper-V environment:

- Recovery of the virtual machine to the original Hyper-V server
- Recovery of the virtual machine to an alternate Hyper-V server
- Recovery of virtual machine files to a network folder
- Item-level recovery of virtual machines backed up at the host level

To recover Hyper-V data, complete the following steps:

1. From the **DPM 2010 Administrator Console**, click the **Recovery** tab.
2. Click “+” to expand **Recoverable data** in the left pane.
3. Select the required replica to restore.
4. Right-click the replica and select **Recover**.

![Figure 25 Recovery of Hyper-V data](image)

---

**Microsoft Windows Server 2008 R2 Hyper-V on EMC VNXe Series**

**Deployment Guide**
5. The **Recovery Wizard** appears. Select the recovery type and click **Next**.

![Recovery Wizard](image)

**Figure 26 Recovery Wizard**

6. The **Specify Recovery Options** page appears. Enter the recovery options and click **Next**.

7. The **Summary** page appears. Review the summary and click **Next**.

After the recovery is complete, the status is displayed.
This chapter presents these topics:

Migration overview ....................................................................................................................... 56
Quick migration............................................................................................................................. 56
Live migration ............................................................................................................................. 57
Quick storage migration ............................................................................................................. 59
Migration overview

In today’s IT environment, the need for round-the-clock resource availability is increasing at a very high rate. Taking advantage of the clustering capabilities of Windows Server 2008 R2, Hyper-V provides support for disaster recovery in IT environments and across data centers by using geographically dispersed clustering capabilities. This chapter deals with possible Hyper-V virtual machine migration techniques.

Quick migration

Quick migration enables Hyper-V virtual machines to move from one host to another host where the hosts are part of failover clusters with some downtime. VNXe storage supports the Hyper-V virtual machines that are stored on VNXe Hyper-V data stores. During quick migration, the memory state of the running virtual machine is saved to disk or shared storage, the storage connectivity is moved from one physical server to another, and then the virtual machine is restored on the second server. The memory state is moved from shared storage to this new server. The speed of the migration depends on how much memory must be written to disk and on the speed of the connectivity to storage.

To initiate quick migration, complete the following steps:

1. Select Start > Administrative Tools > Server Manager to open Server Manager.
2. From the left pane, select Features > Failover Cluster Manager > Cluster > Services and applications and select the virtual machine.
3. Right-click the virtual machine and select Quick migrate virtual machine(s) to another node. Alternatively, this option is accessible from the Actions pane.
4. Select the destination node as shown in Figure 27.
5. The memory state is saved to the shared storage of the failover cluster. The progress appears in the center pane as shown in Figure 28 on page 57. After the virtual machine’s memory is successfully saved, it is restored on the destination node and the restore progress is displayed.

Figure 27  Select quick migration destination node

Microsoft Windows Server 2008 R2 Hyper-V on EMC VNXe Series Deployment Guide
Note: The virtual machine experiences downtime during the saving and restoring processes.

Figure 28  Save memory

The Current Owner of the virtual machine changes from the source to the destination node.

Live migration

Though quick migration addresses business continuity needs, some applications cannot afford even this minimal downtime. Live migration makes it possible to keep virtual machines online, even during migration, and further increases the productivity.

In Windows Server 2008 R2 Hyper-V failover cluster, CSV enhances the live migration feature. CSV has many benefits such as easy storage management, ability to store many virtual machines in a single volume, and multiple host access to the volume concurrently.

The tasks involve in live migration are:

1. The virtual machine memory pages are transferred from the source to the destination host. Any modifications to the virtual machine memory pages are tracked during this process.
2. Pages modified during step 1 are transferred to the destination host.
3. Hyper-V moves the storage handle for the virtual machine VHD files to the destination physical computer.
4. The destination virtual machine is brought online on the destination Hyper-V server.

Users will not experience any downtime from step 3 to step 4.

To start live migration, complete the following steps:

1. Select Start > Administrative Tools > Server Manager to open Server Manager.
2. From the left pane, select Features > Failover Cluster Manager > Cluster > Services and applications and select the virtual machine to migrate.
3. Right-click the virtual machine or select Live migrate virtual machine to another node. Alternatively, this option is accessible from the Actions pane.
4. Select the destination node as shown in Figure 29 on page 58.
Hyper-V Virtual Machine Migration to VNXe

Figure 29  Select live migration destination node

5. The process detects the state of the virtual machines immediately. The live migration process starts. The progress appears in the center pane as shown in Figure 30. Unlike quick migration, the virtual machine continues to run during the migration process.

Figure 30  Live migration progress

After migration is completed, the virtual machine continues in the running state with the Current Owner changed to the destination node.
Quick storage migration

Using live migration and quick migration features, the virtual machines can be moved between the clustered nodes. In some scenarios, a virtual machine is migrated from a stand-alone Hyper-V host to a clustered host and likewise, from a clustered host to a stand-alone host. Another scenario is where the virtual machine has to migrate from a direct-attached storage to SAN or NAS with less downtime. Microsoft’s System Center Virtual Machine Manager (SCVMM) 2008 R2 has a feature called Quick Storage Migration (QSM) that addresses these concerns. The VNXe platform supports QSM to move virtual machines from one Hyper-V data store to another.

VNXe supports virtual machine storage migration by using the Quick Storage Migration (QSM) feature of SCVMM 2008 R2. Virtual machines can be migrated from one storage to another in the following scenarios:

♦ Within the same cluster from one CSV to another CSV
♦ From CSV to storage on the stand-alone host
♦ From storage on the stand-alone host to the Hyper-V CSV
♦ From one stand-alone host to another stand-alone host

All these configurations are supported when both virtual machines are in power-on and power-off states.

The prerequisites to perform QSM are the following:

1. Install SCVMM 2008 R2 on a physical system with Windows Server 2008 R2 installed on it.
2. Add all the required hosts in the SCVMM administrator console.

To perform QSM of a virtual machine, complete the following steps:

1. In the SCVMM administrator console, right-click the virtual machine and select one of the following:
   ♦ **Migrate**—To migrate the virtual machine to the host and to new storage. If this option is selected, enter the destination host, destination storage path, and network details.
   ♦ **Migrate storage**—To migrate the virtual machine to new storage within the same host. If this option is selected, enter only the destination storage path.
2. The **Migrate Virtual Machine Wizard** appears. Select the destination host. All the hosts connected to SCVMM are listed with a rating based on the virtual machine’s requirements. A high rating specifies that the respective host is the best choice. Click **Customize Ratings** to configure the settings that calculate the rating and click **Next**.

3. The **Select Path** page appears. Select the path to store the virtual machine files on the destination host. Click **Browse** to select the folder. Select the destination and click **OK**. The free space available for all the volumes on the destination host is displayed. This helps the administrator to choose a particular volume.
4. The **Select Networks** page appears. Select the network to migrate the virtual machine and click **Next**.
   If more than one network exists, dedicating a particular network for migration does not affect the performance of the virtual machine.

5. The **Summary** page appears. Review the details and click **Move**.
   Track the progress of QSM in the **Jobs** page.
Chapter 8  VNXe Replication using Replication Manager

This chapter presents these topics:

Disaster recovery ........................................................................................................................... 64
VNXe replication overview ........................................................................................................... 64
Disaster recovery

Replication is a key data protection strategy for enterprises of all sizes. Replication is used for critical enterprise information, copying data locally or remotely for higher levels of protection and availability, ensuring business continuity, and data repurposing for development quality assurance and business intelligence. The VNXe platform and EMC Replication Manager address the various challenges involved in the successful disaster recovery process.

EMC Replication Manager simplifies the management of EMC point-in-time replication technologies. It integrates with critical business applications, creates, mounts, and restores point-in-time replicas of databases or file systems residing on supported storage arrays, and performs automatic discovery of changes to the storage or application environment. The *EMC Replication Manager Product Guide* available on Powerlink provides more information about Replication Manager.

VNXe replication overview

EMC Replication Manager and VNXe offer advanced data replication technologies to help protect the Hyper-V virtual environment. In case of any disaster, the administrator can fail over to the destination side with minimum intervention. It provides a single management console along with wizards to simplify replication tasks. The data can be replicated within the same VNXe platform or to a remote storage array. Currently, the replication of Hyper-V data stores is possible only through Replication Manager. Figure 33 shows the disaster recovery procedure steps.

**Figure 33** VNXe Hyper-V replication flowchart

Create a replication source

Create the Hyper-V data store that acts as the replication source by using the Hyper-V configuration wizard as described in “VNXe: Create Hyper-V data stores and grant access to hosts” on page 29. The hosts that access the data store must run the Replication Manager Agent.

**Note:** Replication Manager does not support the replication of Hyper-V CSVs.

Establish replication connections

The replication destination can be a local VNXe, a remote VNXe, a remote VNX, or a remote Celerra®. A replication connection is not required to replicate to the local VNXe platform. Before
remote replication of the Hyper-V data store, establish a replication connection between the two storage platforms.

To establish a connection between two storage platforms, complete the following steps:

1. In Unisphere, click the Hosts tab and click Replication Connections.
2. The Replication Connections page appears. Click Add Replication Connection.

3. The Add Replication Connection Wizard appears. Complete the following steps:
   a. Select VNXe or Celerra or VNX from the System Type list box.
   b. Select Network Name or IP address.
   c. In the System Name field, type a name for the remote system. This name appears in replication connections.
   d. In the Passphrase field, type a common passphrase that local and remote systems will use to communicate with each other. Type the same passphrase on the remote Celerra or VNX platform to complete the configuration of the replication connection.
   e. Click Next.
4. The **Summary** page appears. Review the details and click **Finish** to complete the replication connection.

The results of the operation are displayed. If the operation fails in any of the steps due to any reason, failure details such as error code and error details are displayed.

Create a replication destination

The replication destination can reside on the local or remote storage platform based on the replication type. Destination creation steps are the same for both types and it is assumed that the remote storage system is also VNXe. Replication to other EMC storage systems such as VNX and Celerra is not in the scope of this document.

Create replication destination storage from the Generic iSCSI Storage wizard. To start the wizard, complete the following steps:

1. In **Unisphere**, click the **Storage** tab, and then click **Generic iSCSI Storage**.
2. Click **Create a Replication Destination**.
VNXe Replication using Replication Manager

Microsoft Windows Server 2008 R2 Hyper-V on EMC VNXe Series

Deployment Guide

Figure 36 Generic iSCSI Storage page

The storage creation is similar to that of the Hyper-V data store described in “VNXe: Create Hyper-V data stores and grant access to hosts” on page 29. The destination storage is created as read only, and the replication role is set as Destination. Ensure that the hosts are connected to the destination storage on the same VNXe or the remote VNXe/Celerra/VNX.

Install Replication Manager Server and Agents

You must install Replication Manager Server on a separate host that manages all the replication jobs and install the Replication Manager Agents on all the hosts that are accessing the storage resources.

Attach hosts to Replication Manager

After preparing the storage resources for replication from VNXe, configure the following steps from Replication Manager to complete the replication configuration:

1. Start the Replication Manager Console from the host on which Replication Manager Server is installed.
2. Add all the hosts running the Replication Manager Agents for Replication Manager to identify the applications running on the hosts.
3. In EMC Replication Manager, right-click Hosts, and then select New Host.
Figure 37  Add a host

4. The Register New Host dialog box appears. Complete the following steps:
   a. In the Host Name field, type the name of the host.
   b. In the Port field, type the port number.
   c. Click OK.

Create an application set

After registering the hosts successfully, create an application set.
To create an application set, complete the following details:
1. In EMC Replication Manager, right-click Application Sets, and then select New Application Set.

Figure 38  Create an application set

2. The Application Set Wizard page appears. Click Next.
3. The Application Set Name and Objects page appears. Complete the following steps:
   a. In the Name field, type a unique name for the application set.
   b. Select all the objects that have to be replicated.
c. Click **Next**.

![Application Set Name and Objects page](image)

**Figure 39 Application Set Name and Objects page**

4. The **Completing the Application Set Wizard** page appears. Complete the following steps:
   a. Click **Run Validation** to validate the application set.
   b. Click **Close**.
   c. Select the **Create a job for this application set** checkbox, which opens the **Job wizard** automatically on closing the Application Set Wizard.
   d. Click **Finish** to complete the creation of application set.
Create a replication job

To create a replication job, complete the following steps:

1. The Job Wizard automatically opens after the Application Set Wizard closes. Alternatively, right-click Jobs from the left pane in Replication Manager, and then select New Job.

2. Select the application set to replicate from the list box and click Next.
3. The **Job Name and Settings** page appears. Complete the following steps:
   a. In the **Job Name** field, type a unique name for the job.
   b. Select **Primary Storage** from the **Replication Source** list box.
   c. Based on the replication type, select the replication technology from the **Replication Technology** list box:
      - Select **Celerra SnapSure™** for local replication.
      - Select **Celerra Replicator™** for remote replication.
   d. Specify the replica lifetime by number or by duration:
      - Select **Limit replica count to: <number>** to modify a replica rotation to delete replicas based on the maximum number of replicas.
      - Select **Keep replica for** option to specify the retention period on replicas.
   e. Click **Next**.
The Celerra replication storage page appears. Complete the following steps:

a. Select the destination storage system name from the Celerra Name list box.

b. Select the IP address of the destination system that is used for replicating the data from the Data mover IP address list box.

c. Select the IQN of the destination storage created on the remote system from the Celerra IQN (Optional) list box. To view the IQN of the destination generic iSCSI storage, click the Storage tab and click Generic iSCSI Storage. Select the destination iSCSI storage and click Details.

d. Click Next.
5. The **Mount Options** page appears. Select the replica’s mount host, path, and other mount options. Click **Next**.

**Figure 44 Mount Options page**

6. The **Starting the Job** page appears. A Replication Manager job can be invoked in three ways:
   
a. Start the job manually or with a third-party scheduler.
b. Create a schedule on which the job will run. If Schedule the job is selected, the Add Schedule dialog box appears. Enter the required details to define the schedule as shown in Figure 45.

c. Start the job after another job completes. The job selected can be associated with the same application set or with another application set.

Select the appropriate option according to business requirements. Click Next.

Figure 45  Starting the Job page

7. The Users to be Notified page appears. It provides the option to specify the email addresses of users to whom a notification mail is sent on completion of the job. Click Next.

8. The Completing the Job Wizard page appears. Review the details and click Finish to complete the job creation.

Run a Replication Manager job

To run a job, complete the following steps:

1. Before running the job, simulate the job to verify that the configuration settings are correct. If the simulation fails, check for the reason in the details of the simulation operation. To simulate the job, right-click the job and select Simulate.

2. If the simulation passes, run the actual job. Right-click the particular job and select Run.
3. As part of the replication process, Replication Manager creates snapshots of the source and destination data stores. To view the snapshot, click the Snapshots tab of the source/destination storage details. The snapshot’s Taken By column shows Replication Manager.

![Figure 46 Run a job](image)

![Figure 47 View Replication Manager snapshots](image)
Mount a Replication Manager replica

Replicas created by Replication Manager can be mounted to any host and used for backup/test environments.

To mount a replica, complete the following steps:

1. In EMC Replication Manager, select the application set from the left pane. The replicas associated for the application set are visible in the middle pane.
2. Right-click the replica, and then select Mount.

3. The Mount Wizard page appears. Select the destination host and path to mount the replica. The contents of the source Hyper-V data store can be viewed in the specified host and mount path.
4. To unmount the mounted replica, right-click the replica in Replication Manager, and select Unmount.

Replication failover

If the source Hyper-V data store becomes unavailable due to natural or human-related disasters, access is failed over to the destination storage. The destination data store becomes read/write and all the production hosts start using it.

To initiate the failover manually, right-click the replica and select Failover, as shown in Figure 49 on page 77.
Figure 49  Replication failover
Appendix A  VNXe iSCSI Server Target Setup

This appendix presents this topic:

Configure VNXe for iSCSI connectivity.............................................................................. 80
Configure VNXe for iSCSI connectivity

VNXe iSCSI Server is the software component that performs the storage management and monitoring operations associated with iSCSI-based storage. To use VNXe iSCSI storage, the system requires at least one iSCSI Server. If an iSCSI Server has not been added when installing the VNXe platform, use Unisphere to add at least one iSCSI Server. Both VNXe3100 and VNXe3300 platforms can have up to 12 iSCSI Servers on each SP. If multiple iSCSI Servers are created, the VNXe platform suggests an SP on which to create the server based on the number of iSCSI Servers per SP.

To add one or more iSCSI Servers, complete the following steps:

1. In Unisphere, click the Settings tab, and then click iSCSI Server Settings.

![Unisphere Settings](image)

**Figure 50 iSCSI Server Settings**

2. The iSCSI Server Settings page appears. Click Add iSCSI Server.
3. The iSCSI Server wizard appears. Complete the following steps:
   a. In the **Server Name** field, type a name for the iSCSI Server. The name is case-sensitive and must be unique on the VNXe platform.
   b. In the **IP Address** field, type the IP address of the iSCSI Server.
   c. In the **Subnet Mask** field, type the subnet mask that identifies the subnet where the iSCSI Server resides.
   d. Select the storage processor on which to create the iSCSI Server from the **Storage Processor** list box.
   e. Select the port number for the VLAN with which the iSCSI Server is associated from the **Ethernet Port** list box.
   f. In the **VLAN ID** box, type or select a VLAN ID in the range 0 to 4095.
   g. Click **Next**.
4. The **Summary** page appears. Confirm the selections and click **Finish**.
This appendix presents this topic:
Configure VNxe hosts.................................................................................................................. 84
Configure VNXe hosts

The users of VNXe storage resources can be servers, virtual machines, applications, and so on and are referred to as hosts. These hosts’ details must be provided so that the administrator can grant the required level of storage access to the respective hosts.

1. In Unisphere, click the Hosts tab, and then click Create Host.
2. The Host Wizard page appears. In the Name and Description fields, type the name and description of the new host. Click Next.

![Host Wizard page](image)

3. The Operating System page appears. Select the host operating system from the Operating System list box. Click Next.
4. The **Network Address** page appears. Select **Network Name** or **IP Address** to enter the network address of the host.

5. The **iSCSI Access** page appears. Complete the following steps:
   
   a. In the **IQN** field, type the IQN of the Hyper-V host.
      
      The IQN of the host initiator is available on the **General** tab of the Microsoft iSCSI initiator.
   
   b. In the **CHAP Secret** field, type a password that is 12 to 16 characters long. It must be specified when configuring the iSCSI connection from the Hyper-V iSCSI Initiator.
      
      VNXe provides CHAP authentication for additional security. This feature is optional. The CHAP secret is used to authenticate the initiator when establishing the connection and also for periodic verification of the initiator identity.
   
   c. Click **Next**.

---

**Figure 54** Operating System page
6. The **Summary** page appears. Review the host details and click **Finish**.
This appendix presents this topic:

Set up Hyper-V hosts to use VNXe iSCSI storage ................................................................. 88
Set up Hyper-V hosts to use VNXe iSCSI storage

This appendix describes how to use the Microsoft iSCSI initiator, which is running on Windows Server 2008 R2, to connect to an external iSCSI-based storage array through an Ethernet network adapter.

Discover the target portal

Windows Server 2008 R2 includes a native iSCSI Software Initiator.

To start the iSCSI initiator, complete the following steps:

1. Log in to the server and execute the command `iscsicpl.exe` at the command prompt. Alternatively, from the Start menu, select Control Panel and click iSCSI Initiator. If this command is running for the first time, the following message appears as shown in Figure 56.

![Microsoft iSCSI service message](image)

2. Click Yes to start the iSCSI service and set it to start automatically each time the server restarts.

In Windows Server 2008 R2, the iSCSI targets that do not require any advanced settings can be connected as follows:

1. In the iSCSI Initiator Properties dialog box, click the Targets tab.
2. In the Target field, type the IP address of the VNXe iSCSI target.
3. Click Quick Connect.
To connect iSCSI targets and configure advanced settings, complete the following steps:

1. In the **iSCSI Initiator Properties** dialog box, click the **Discovery** tab.
2. Click **Discover Portal**.
3. The **Discover Target Portal** dialog box appears. Complete the following steps:
a. In the **IP address or DNS name** field, type the VNXe iSCSI Server IP created earlier. This is described in Appendix A VNXe iSCSI Server Target Setup.

b. Click **Advanced**.

![Discover Target Portal dialog box](image)

**Figure 59** Discover Target Portal dialog box

4. The **Advanced Settings** dialog box appears. Complete the following steps:
   a. Select **Microsoft iSCSI Initiator** from the **Local adapter** list box.
   b. Select the IP address of the NIC connected to the iSCSI server from the **Initiator IP** list box.
   c. Select the IP address of the iSCSI Server of the VNXe platform from the **Target portal IP** list box.
   d. Clear the **Data digest** and **Header digest** checkboxes.
   e. Select **Enable CHAP log on** if CHAP authentication is enabled at the time of Hyper-V data store creation in the VNXe platform.
   f. In the **Name** and **Target secret** fields, type the same name and CHAP secret that were given during data store creation so that the host can be identified and a secure connection established.
   g. Click **OK**.

**Note:** The iSCSI protocol offers an additional safeguard called digests. Digests use a 32-bit cyclic redundancy checksum (CRC). The iSCSI protocol provides error detection by using the data and header digests.
5. In the iSCSI Initiator Properties dialog box, verify the Target portals details displayed on the Discovery tab.

6. Select the Targets tab, and then select the VNXe target name. Click Connect.

7. The Connect To Target dialog box appears. Complete the following steps:
   a. Select Add this connection to the list of Favorite Targets or Automatically restore this connection when the system boots.
b. Clear **Enable multi-path** even if multiple paths are present.

**Note:** iSCSI multi-path software should be installed on the server before enabling a multi-path connection. It is used for Multipath I/O (MPIO) connections. In the Targets tab of the iSCSI Initiator Properties dialog box, verify that the status of the target shows **Connected**.

**Configure Multiple Connections per Session**

To configure Multiple Connections per Session (MCS), complete the following steps:

1. Select the target logged in to and click **Properties**.
2. The **Properties** dialog box appears. Click **MCS**.

![Figure 61 Configure MCS](image)

3. The **Multiple Connected Session** (MCS) dialog box appears. To add another connection to this session, click **Add**.
4. The **Add Connection** dialog box appears. Complete the following steps:
   a. Click **Advanced**.
   b. The **Advanced Settings** dialog box appears. Select a different initiator IP such as the source IP for a different NIC.
   c. Click **OK**.

5. The **Multiple Connected Session (MCS)** dialog box appears. Complete the following steps:
   a. Select **Round Robin** from the **MCS policy** list box.
   b. Verify that both connections are listed as shown in **Figure 63** on page 94.
   c. Click **OK**.
Figure 63   Add a new connection
This appendix presents this topic:

iSCSI volume configuration.......................................................................................................... 96
iSCSI volume configuration

After an iSCSI connection is initiated and established with the target, the storage from the target appears as a new uninitialized disk under Disk Management. This section guides administrators to create and configure a volume over the newly added disk. It also provides instructions on managing the volume that is created.

Create and configure the Hyper-V VHD

To create and configure the VHD, complete the following steps:

1. On the Windows host, open Server Manager.
2. Click Storage.
3. Click Disk Management and select the disk to format.

4. To verify the source of the disk, complete the following steps:
   a. Select Start > Administrative tools > iSCSI initiator to open iSCSI Initiator.
   b. Click the Targets tab and click Devices.
      
      The Devices dialog box appears and the disk number can be verified.

5. Right-click the disk and click Initialize.
6. Select the disks to initialize and select MBR partition style.
7. Click OK.
8. Right-click the disk again and select Online.
9. Right-click the online raw disk and select **New Simple Volume**.

10. The **New Simple Volume Wizard** appears. Click **Next**.

11. The **Specify Volume Size** page appears. Type the required disk size and click **Next**.

12. The **Assign Drive Letter or Path** appears. In the **Drive letter** field, assign a **drive letter** and click **Next**.

   **Note**: NTFS mount can also be used. Mount a local drive at an empty folder on an NTFS volume using a drive path instead of a drive letter.

13. The **Format Partition** page appears. Select **Format this volume with the following settings** and enter the following details:
   
   a. Select **NTFS** from the **File System** list box.
   
   b. Select the required allocation unit size from the **Allocation unit size** list.
   
   c. In the **Volume label** field, type a name for the volume.
   
   d. Select **Perform a quick format**.
   
   e. Click **Next**.

14. The **Completing the New Simple Volume Wizard** page appears. Verify the details and click **Finish**. After formatting, a new healthy partition is created.

**Passthrough disk**

A passthrough disk bypasses the parent partition and is directly presented to the virtual machine as a raw physical disk. Unlike VHD, a passthrough disk is exclusively used by a virtual machine. To present a VNXe Hyper-V data store as passthrough, go to Hyper-V Manager, right-click the virtual machine, and select **Settings**. As shown in Figure 66 on page 98, add a hard drive as **Physical hard disk**.
If the size of the iSCSI LUN on the VNXe is extended to meet the growing demand for Hyper-V storage, it results in the addition of unallocated space on the same virtual disk that has been mapped to the host.

After refreshing **Disk Management** on the host, an unallocated space appears because of the iSCSI LUN extension.
To adjust the partition boundary and to expand the file system:

1. In Disk Management, right-click the existing volume and select Extend Volume.

   ![Extend existing volume](image)

   **Figure 67** Extend existing volume

   The Extend Volume Wizard appears. It shows the existing device properties and the additional capacity of the iSCSI LUN that can be extended.

2. The Select Disks page appears. Type or select the amount of space to extend the volume by. Click Next.

3. The Summary page appears. Review the details and click Finish.

   After the wizard completes, verify the volume extension in Disk Management.
Host Configuration of iSCSI Volumes
This appendix presents this topic:

Management of VNXe Hyper-V environments ................................................................. 102
Management of VNXe Hyper-V environments

The initial deployment cannot address the ever-growing business storage requirements. To meet the increasing storage needs of the business, the storage platform must be flexible enough to grow in the future. This chapter explains how to manage the VNXe platform to address a wide variety of deployment requirements.

Storage pool expansion

To expand a pool, complete the following steps:

1. In Unisphere, click the System tab and click Storage Pools.
2. Click Configure Disks.
3. The Disk Configuration Wizard appears. Select Manually add disks to an existing pool and select the pool to add drives from the list box.

VNXe can add groups of drives in multiples of the base RAID group size. If the initial group is 5 drives, then 5, 10, or 15 drives can be added to the pool.

Extend Hyper-V data store

Sometimes, the storage requirement goes beyond the initial provisioned space. To fulfill the storage space requirements of a Hyper-V server, extend the size of an existing LUN.

To extend a Hyper-V data store, complete the following steps:

1. In Unisphere, click the Storage tab and click Hyper-V.
2. Select the specific LUN to extend and click Details.
3. Click the **Datastore Capacity** tab.

4. In the **Size** field, type the required space.

5. Click **Apply Changes**.

![Extend Hyper-V data store](image)

**Figure 69** Extend a Hyper-V data store

**Extend Hyper-V data store protection size**

Based on the application requirements, careful planning is required to configure the protection storage. The amount of storage required for protection cannot be reduced at a later time. Improper planning may leave the storage resources unprotected. Based on the application demand, VNXe provides a way to increase the protection size.

To increase the protection size, complete the following steps:

1. In **Unisphere**, click the **Storage** tab and click **Hyper-V**.
2. Select the Hyper-V data store and click **Details**.
3. Click the **Protection Size** tab.
4. The maximum size that is possible is displayed. In the **Size** field, type the required amount of storage. It must be less than the maximum size.
5. Click **Apply Changes**.

**Modify host access**

You can modify host access for any Hyper-V data store whenever required.

To modify host access, complete the following steps:

1. In **Unisphere**, click the **Storage** tab and click **Hyper-V**.
2. Select the Hyper-V data store to change host access.
3. Click the **Host Access** tab.

4. Select the host access levels for the required hosts from the list boxes.

   **Note:** To give access to a new host that does not exist in the system, click **Create Host** to add the new host.

5. Click **Apply Changes**.

---

**Figure 70** Modify host access

### Delete a Hyper-V data store

Hyper-V data stores can be deleted if no longer needed so that the storage space can be added to the free pool. Therefore, more space can be added to applications that have more storage needs.

To delete a Hyper-V data store, complete the following steps:

1. In Unisphere, click the **Storage** tab and click **Hyper-V**.

2. Select the Hyper-V data store and click **Delete**.

3. A dialog box appears prompting for confirmation. This helps to avoid accidental deletion of the data store. Click **Yes** to proceed and **No** to return to the previous page.

### Delete a Hyper-V storage pool

A storage pool can be deleted if the storage resources residing on a pool are no longer needed. After the pool deletion, the drives are added to unconfigured disks. This enables the administrator to use the drives for other applications.

To delete a storage pool, complete the following steps:

1. In Unisphere, click the **System** tab and click **Storage Pools**.
2. Click **Recycle Disks**.

   **Note:** The **Recycle Disks** button is activated only when a pool is empty. Therefore, before pool deletion, delete all storage resources.

---

**Figure 71** Delete a storage pool

3. The **Recycle Disks** dialog box appears. It shows the drives to recycle. Click **Recycle** to confirm the operation.

4. Click **Close**.
This appendix presents these topics:

Model components and limits ................................................................. 108
Software configuration limits ................................................................. 108
Model components and limits

The two models in the VNXe family share the core software. However, the hardware is very different. Table 8 compares the hardware of the two VNXe models.

Table 8 VNXe model components and limits

<table>
<thead>
<tr>
<th>Component</th>
<th>VNXe3100</th>
<th>VNXe3300</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Jasper dual-core 1.73 GHz with Hyper-Threading</td>
<td>Intel Westmere quad-core 2.13 GHz</td>
</tr>
<tr>
<td>System memory (per SP)</td>
<td>4 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>Number of memory channels</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Memory speed</td>
<td>1066 MHz</td>
<td>1066 MHz</td>
</tr>
<tr>
<td>Connectivity options</td>
<td>12 x 1 GbE</td>
<td>• 16 x 1 GbE</td>
</tr>
<tr>
<td></td>
<td>• 8 x 1 GbE and 4x 10 GbE</td>
<td>• 8 x 1 GbE and 4x 10 GbE</td>
</tr>
<tr>
<td>Maximum number of disks</td>
<td>96 (Dual SP) 48 (Single SP)</td>
<td>120</td>
</tr>
<tr>
<td>Allowed drive types</td>
<td>• 300 GB 15k SAS</td>
<td>• 100 GB EFD</td>
</tr>
<tr>
<td></td>
<td>• 600 GB 15k SAS</td>
<td>• 300 GB 15k SAS</td>
</tr>
<tr>
<td></td>
<td>• 2 TB NL-SAS</td>
<td>• 600 GB 15k SAS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 TB NL-SAS</td>
</tr>
</tbody>
</table>

Software configuration limits

Table 9 shows the VNXe operating system limits.

Table 9 Software configuration limits

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts connected</td>
<td>500</td>
</tr>
<tr>
<td>Snapshots per virtual disk</td>
<td>2,000</td>
</tr>
<tr>
<td>Virtual disks</td>
<td>256</td>
</tr>
<tr>
<td>Snapshots per shared folder</td>
<td>96</td>
</tr>
<tr>
<td>Shared folders</td>
<td>500</td>
</tr>
<tr>
<td>Maximum virtual disk size</td>
<td>1.999 TB</td>
</tr>
<tr>
<td>Maximum shared folder size</td>
<td>15.533 TB</td>
</tr>
<tr>
<td>Open files</td>
<td>200,000</td>
</tr>
<tr>
<td>Concurrent connections</td>
<td>20,000</td>
</tr>
</tbody>
</table>
This appendix presents this topic:

VNXe system monitoring and alerting ................................................................. 110
VNXe system monitoring and alerting

The VNXe family of storage arrays provides a simple dashboard interface to examine the health of the system. This section describes some of the features of VNXe that help in monitoring and debugging the platform.

System utilization

The System Capacity view provides pie charts that depict the capacity utilization in detail by specifying the amount of storage used by various applications and the free space available. To view the System Capacity page in Unisphere, click the System tab and click System Capacity.

![System Capacity page](image)

As shown in Figure 72, click the Utilization History View tab to view the history of the platform utilization.

These graphs help administrators to understand the capacity needs well in advance, and thus provide them with sufficient time to plan for the future.

Monitoring system health

The System Health page monitors the state of the array through an interactive graphical representation of the hardware components. To view the System Health page in Unisphere, click the System tab and click System Health. The graphical part of the System Health page provides a graphical carousel where it is possible to click on the different components to bring them to the front. The carousel contains:

- Front and rear view of the disk processor enclosure (DPE)
- Front and rear view of the disk-array enclosure (DAE)

If more than one DAE exists, all of them are displayed.

To display information about a particular system component, click one of the following:

- An element of the hardware graphic
- An element in the expandable component list
If the component is faulted or has any issue, a pop-up window appears stating the issue as shown in Figure 73.

![System Health page](image)

**Figure 73 System Health page**

As shown in Figure 73, a detailed description of the selected component is provided in the **Component Description** pane. The following table provides the icons for the various health status levels.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Health Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Non-recoverable</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Critical</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Major</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Minor</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Degraded</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Unknown</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>OK</td>
</tr>
</tbody>
</table>

**Figure 74 Health status Icons**

The Storage Resource Health page provides the status of the storage resources created on the platform. To view the Storage Resource Health page in Unisphere, click the **System** tab and click Storage Resource Health.
Performance

The performance of both storage processors can be viewed in Unisphere. To view the Processor Performance page in Unisphere, click the System tab and click Processor Performance. As shown in Figure 76, select either one or both SPs at any time and set the timeframe slider to view the CPU usage in the last one hour (Recent), the last 24 hours, or the last 48 hours (Older).
Alerts

To view the alerts generated by the platform in Unisphere, click the System tab and click System Alerts.

![System Alerts page](image)

**Figure 77  System Alerts page**

When a particular alert is selected, alert information is displayed stating the problem along with the severity level. The icons for the various severity levels are listed in Figure 78 on page 114.
System logs

System logs are preserved and can be viewed as shown in Figure 79. To view the Logs page in Unisphere, click the System tab and click Logs. Log entries that are promoted to alerts also get displayed.
Logging standards for various icons are displayed in Figure 80.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Logging Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>Emergency</td>
</tr>
<tr>
<td>🚨</td>
<td>Alert</td>
</tr>
<tr>
<td>🚨</td>
<td>Error</td>
</tr>
<tr>
<td>🚨</td>
<td>Warning</td>
</tr>
<tr>
<td>🚨</td>
<td>Information</td>
</tr>
<tr>
<td>🚨</td>
<td>Notice</td>
</tr>
<tr>
<td>🚨</td>
<td>Debug</td>
</tr>
<tr>
<td>✔</td>
<td>OK</td>
</tr>
</tbody>
</table>

**Figure 80** Logging standards

**Support**

The VNXe interface also has integrated support features. For any issues with the array, help-related content is available directly from the user interface.

**Figure 81** Support options