HPE Nimble Storage Deployment Considerations for Microsoft Hyper-V on Windows Server 2012 R2 and Windows Server 2016
# Contents

Introduction..................................................................................................4  
Features of a Highly Available Hyper-V Installation..................................................4  
Clustered Hyper-V Server High Availability..............................................................5  

Storage Architecture Considerations for Hyper-V.................................................6  
Separating the OS and Application Volume from the Data Volumes.............................6  
Configuring Volume Collections..............................................................................7  
Using Guest-Connected Volumes for Storing Data....................................................8  
Install the HPE Nimble Storage PowerShell Toolkit..................................................8  
Connect Through vFC.............................................................................................9  
Connect Through iSCSI.........................................................................................13  
Implementing Storage for Failover Clustering..........................................................13  
Enabling CSV.........................................................................................................17  
Using Protection Templates.....................................................................................18  
Using Zero-Copy Clones.......................................................................................20  
Provisioning VMs.................................................................................................21  

Hyper-V Backups and Disaster Recovery...............................................................23  
Better Hyper-V Backups.........................................................................................23  
Offsite Replication for Hyper-V..............................................................................23  
Hyper-V Disaster Recovery Architecture and Configuration.....................................24  

Appendix A: Import a VM in Hyper-V.................................................................25  

Appendix B: Disaster Recovery Failover...............................................................27  
Planned Failover: Hand Over Production Volumes....................................................27  
Unplanned Failover: Promote Volumes....................................................................27  
Steps Shared by the Two Failover Methods.............................................................28  
Mount the Disaster Recovery Volume......................................................................28  
Import the Hyper-V VM.........................................................................................28  
Add the Imported VM as a Clustered Resource......................................................29  

About the Author.................................................................................................31  

Version History.................................................................................................32
**Introduction**

Microsoft Hyper-V high-availability and disaster-recovery solutions can be implemented in many different ways. This guide presents considerations and best practices for a feature-rich protection solution that combines HPE Nimble Storage arrays and Hyper-V on clustered Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016. By observing these best practices, you can implement and manage an architecture that maximizes your Hyper-V system availability and offsite recovery with minimal effort.

**Features of a Highly Available Hyper-V Installation**

The solution described in the guide offers the following primary benefits:

- **Support for Hyper-V live migration.** In a block-based (iSCSI or Fibre Channel) storage environment, Hyper-V requires the Microsoft Failover Clustering feature to perform live migration between host servers. Live migration greatly reduces the amount of effort required to migrate server data during maintenance, load balancing, or hardware consolidation. The migration does not interrupt services or interfere with the server's ability to process data.

- **Support for Hyper-V live storage migration.** Hyper-V can natively relocate VHD-based storage that is attached to a virtual machine (VM) and all of the files needed to run that machine, such as the configuration file, from their existing location to a new location. Both the source and destination locations can be either block-based storage (iSCSI or Fibre Channel) or an SMB 3.x file share that supports the Continuous Availability (CA) feature. The CA feature allows a Hyper-V VM to evacuate an existing storage device and populate a new storage device. When the storage move is complete, the VM is still hosted on the same physical server. From that point on, however, the server consumes space from the destination storage location instead of the original storage location. This operation does not interrupt services or interfere with the server’s ability to process data.

- **Performance policies.** Traditional storage devices force application writes into static-sized block containers or page containers that do not optimize storage space. The patent-pending HPE Nimble Storage CASL file system uses variable-length blocks that match application write sizes precisely to maximize storage space. Variable-length blocks combined with real-time inline compression greatly reduce the footprint for data storage, snapshots, and replication, enabling you to store more data and reduce bandwidth costs, especially over wide-area networks (WANs).

- **SCSI UNMAP.** This functionality enables you to reclaim storage space on thin-provisioned volumes when data is deleted.

- **Application awareness.** Storage replication by itself can put your data at risk for applications that perform transactional write processes, such as databases. HPE Nimble Storage arrays provide application integration to ensure that applications properly flush their write buffers to a quiescent state before point-in-time operations, such as snapshot backup and replication, are triggered.

- **Zero-copy cloning.** HPE Nimble Storage arrays greatly reduce the amount of storage required for VMs by eliminating duplicate files that are common to multiple operating system images.

- **High availability.** When a system failure occurs, Failover Clustering automatically restarts VMs on surviving hosts. This capability reduces the amount of effort required to manually perform virtual server recovery. HPE Nimble Storage arrays fully support the Failover Clustering and Hyper-V technologies, providing high-speed fault-tolerant storage.

- **Offsite disaster recovery.** When you use HPE Nimble Storage WAN-efficient replication to recover production applications to an offsite disaster recovery location, you achieve fast recovery and business continuity cost-effectively in the event of a catastrophic site outage.
Clustered Hyper-V Server High Availability

The primary drawback of server virtualization is that system outages can affect multiple machines simultaneously. To protect your environment against such impact, you can implement Hyper-V by using the Windows Server Failover Cluster role, which provides automatic recovery in the event of a server failure. This architecture offers two main benefits:

- It greatly simplifies the management effort required to recover applications after an outage.
- It enables you to use Hyper-V live migration to proactively move VMs between host servers for better application scaling.

Figure 1: Common clustering architecture for Hyper-V

A Microsoft failover cluster requires a shared SAN that all hosts of the cluster can access. HPE Nimble Storage arrays offer a high-performance, fault-tolerant storage platform that is fully compatible with Microsoft clustering. To ensure compatibility with your server platform, follow the Microsoft best practices for implementing the cluster.

**Note** Hyper-V on Windows Server enables you to perform live migration and live storage migration of running VMs without requiring shared storage. However, these technologies are best used for proactively migrating VMs, and they do not provide high availability in the event of host failure. Shared storage, such as HPE Nimble Storage CS-Series arrays, is a requirement for high availability within a Hyper-V clustered environment.
Storage Architecture Considerations for Hyper-V

A highly available Hyper-V cluster requires shared storage that is accessible by all hosts participating in the cluster. HPE Nimble Storage arrays offer a robust storage architecture that gives you redundant hardware and seamless access to volumes from all Hyper-V cluster nodes.

**Figure 2: Possible Hyper-V storage layers**

To maximize the benefits that the HPE Nimble Storage environment can provide to your Hyper-V implementation, observe the recommendations and guidelines described in the sections that follow.

**Separating the OS and Application Volume from the Data Volumes**

When you create a new virtual machine (VM), separate the volume for the operating system and the application binaries from the volumes for data. Operating systems and application binaries change infrequently enough that simple volume crash consistency is acceptable. Therefore, you can place operating system virtual disks on Cluster Shared Volumes (CSVs).
To separate the operating system and the application from the data, attach database volumes from the HPE Nimble Storage array to the guest VM that is running the database application. This design segregates the data so that it can be cloned for development and testing. Cloning gives you quick access to production datasets without wasting storage space to make copies of the data.

Data volumes tend to change constantly, and they typically have more critical protection needs than the volume that holds the operating system. Database applications usually write changes to a transaction log before writing them to the database files so that any partial write activity can be recovered in the event of a catastrophic system failure, such as a sudden power outage.

If database applications did not perform this write process (WAL algorithm), the database could be left in a nonrecoverable and thus nontrusted state that would force a complete restore from a backup. Therefore, it is important to protect the transaction logs and the database in a coordinated fashion when you perform any type of backup operation. HPE Nimble Storage arrays give you the ability to group volumes that must be mutually consistent into the same volume collection.

**Figure 3: Design for Microsoft SQL Server storage for Hyper-V**

Configuring Volume Collections

A volume collection enables you to schedule the frequency with which snapshots are created and replicated to other HPE Nimble Storage arrays and the retention time for these snapshots and replicated copies. A volume collection can coordinate protection activities between separate yet related volumes (such as the volumes for the database transaction log and for the database files) to create database snapshots that are application consistent.

Volume collections integrate with the Microsoft Volume Shadow Copy Service (VSS). VSS forces volume collections to momentarily quiesce the write activity of the file system or application to ensure the data integrity of the point-in-time backup.
Using Guest-Connected Volumes for Storing Data

To improve performance and achieve better data protection, application consistency, and offsite replication, store data on HPE Nimble Storage volumes to take full advantage of the HPE Nimble Storage array optimization features. Make sure that you install the HPE Nimble Storage Windows Integration Toolkit (NWT) on each guest VM that stores data. The NWT is available for download on the Software Downloads page on HPE InfoSight. You must also install the HPE Nimble Storage PowerShell Toolkit.

Important Hewlett Packard Enterprise (HPE) recommends that you do not store data on virtual hard disks (VHD or VHDX) if the data needs to be quiesced before you create a snapshot. This recommendation includes database and transaction logs for applications such as SQL Server and Microsoft Exchange.

Install the HPE Nimble Storage PowerShell Toolkit

To deploy the HPE Nimble Storage PowerShell Toolkit, you must first install it on a management machine in your infrastructure. After that, you must install it again on each server that acts as a file server or as a file server cluster node.

Procedure

1. Extract the file by using one of the following methods:
   - To install for the current user only, extract the ZIP file containing the toolkit to the following location:
     
     ```
     $env:HOMEDRIVE\users\<user>\Documents\WindowsPowerShell\Modules
     ```
   - To install for all users, extract the ZIP file containing the toolkit to the following location:
     
     ```
     C:\Windows\system32\WindowsPowerShell\v1.0\Modules
     ```
2 Use the following commands to verify the script execution policy and to set it to Unrestricted or Bypass:

```
Get-ExecutionPolicy
Set-ExecutionPolicy -ExecutionPolicy Unrestricted
Get-ExecutionPolicy
Import-Module NimblePowerShellToolkit
```

3 Establish a connection to an HPE Nimble Storage array or group by authenticating with the HPE Nimble Storage group leader, using the following command to prompt for credentials:

```
Connect-NsGroup -Group 10.18.125.32
```

**Note** The session established with the `Connect-NsGroup` command expires after 30 minutes of idle time.

**Connect Through vFC**

If your HPE Nimble Storage target device uses a Fibre Channel connection, you can enable the virtual Fibre Channel (vFC) feature on the Windows failover cluster that is hosting Hyper-V.

The important concept to note is that when you create a vFC adapter, a pair of worldwide port names (WWPNs) is assigned to that single vFC. The second WWPN is used for live migration so that the new vFC with the new WWPN can be brought up and made operational before you release the old WWPN. These WWPNs are referred to as set A and set B.

The most common scenario is to deploy two HBAs to a physical node and to create two virtual SANs. A VM hosted on this physical node uses the WWPNs in set A on each of its virtual SANs. If you use the live migration feature to move the VM to physical node 2, the WWPNs in set B are activated on physical node 2 and the VM is relocated to the new adapters. After the VM is relocated to node 2, it turns off and deallocates set A. However, the WWPNs in set A are still reserved for this VM and will be reactivated if the VM is live-migrated to another physical node; for instance, if the VM is migrated to physical node 3.

Before you create vFC adapters, ensure that the physical HBAs in the server support the N_Port ID Virtualization (NPIV) feature. If the HBA vendor requires NPIV to be enabled separately, ensure that it is enabled.

**Procedure**

1 In Hyper-V Manager, click **Virtual SAN Manager** in the **Actions** pane.
2 Click **Create** to create a virtual SAN that is based on an HBA installed in the server.

3 Assign a name to the fabric and identify which HBA (by WWPN) will be connected to that fabric.
4 Repeat these steps to create additional SAN fabric/HBA combinations in the machine.

In the scenario in this procedure, which is the most common scenario, the server has a set of two HBAs, with the first HBA connected to fabric A and the second HBA connected to fabric B.

5 Verify that the VMs on which you will create the vFC adapters are shut down. If they are not, shut them down before proceeding to the next step.

6 To create individual vFC adapters, navigate to the VM's Settings page, click Add Hardware, and choose Fibre Channel Adapter.

7 After you create a new vFC adapter, the GUI gives you the set of WWPNs that will be required for any zoning commands on the switch and that must be added to the initiator group as unique initiators.
8 Run the following PowerShell command to obtain all WWPNs for the specified VM:

```
(Get-VM VMName | Get-VMFibreChannelHBA).WorldWidePortNameSetA
(Get-VM VMName | Get-VMFibreChannelHBA).WorldWidePortNameSetB
```

9 To create an initiator group for this VM, run the following commands from the HPE Nimble Storage PowerShell Toolkit:

```
New-NSInitiatorGroup -name "VMName" -access_protocol "FC" -description "Initiator Group for VMName"

$MyGroupID = ( Get-NSInitiatorGroup -name "VMName" ).id

New-NSInitiator -initiator_group_id $MyGroupID -access_protocol "fc" -alias "VMName_SetA_FC0" -wwpn "51:13:14:15:16:17:18:24"

New-NSInitiator -initiator_group_id $MyGroupID -access_protocol "fc" -alias
```
Connect Through iSCSI

If your HPE Nimble Storage target device uses an iSCSI connection, you can enable the iSCSI initiator inside each VM. HPE strongly recommends that you create virtual Ethernet switches dedicated to the iSCSI traffic and that you separate this traffic from the VM’s production network.

Deploying iSCSI to a VM is no different from deploying iSCSI to a physical node. To create the initiator group for the VM, you must first install the HPE Nimble Storage PowerShell Toolkit in the guest operating system and connect to the array.

Procedure

1. Gather the iSCSI qualified name (IQN) of the VM.

   ```powershell
   Get-InitiatorPort | where {$_._connectiontype -like "iSCSI"} | format-list nodeaddress
   nodeaddress
   ```

2. Automatically insert the IQN into the creation process of the HPE Nimble Storage initiator groups. Set the command to run from each server in your Windows failover cluster.

   ```powershell
   $MyIQN=(Get-InitiatorPort | where {$_._ConnectionType -like "iSCSI"})
   $MyHost=hostname
   New-NSInitiatorGroup -name $MyHost -access_protocol "iSCSI" -description "Initiator Group for $MyHost"
   $MyGroupID = (Get-NSInitiatorGroup -name $MyHost).id
   New-NSInitiator -initiator_group_id $MyGroupID -access_protocol "ISCSI" -alias $MyHost -iqn $MyIQN
   ```

Implementing Storage for Failover Clustering

To configure shared cluster storage for Hyper-V, you must provision a volume on the HPE Nimble Storage array. Provisioning the volume is a prerequisite for using a SAN with a Windows cluster.

To create a volume for Hyper-V, use a performance policy that preconfigures new volumes with optimized settings for different scenarios. For example, the Hyper-V CSV performance policy is tuned to use 4 KB volume blocks to provide the best performance for Windows storage LUNs. This policy also includes inline compression and high-performance caching. Therefore, use the Hyper-V CSV performance policy for CSVs.
Provisioning Storage for Data

When provisioning storage for your data, use a performance policy that is specific to your application. HPE Nimble Storage arrays have performance policies for commonly used applications, such as SQL Server and Exchange, or you can create your own policies. For example, you might have large files that are already highly compressed (such as a video or an image server) that perform better with larger block sizes and no compression. Use the HPE Nimble Storage array monitoring tools to view your volume performance under simulated production loads to better understand your unique application best practices.

Using Access Control

Isolate your storage by using access control lists (ACLs) that include an initiator group for the cluster, and add each node's IQN to that initiator group. ACLs reduce management effort and improve security by isolating volumes only to the machines that should have access to that data.

Configuring Initiator Groups

For initiator groups, use the server's IQN instead of using IP addresses because the IQN is tied to the server and not to a particular NIC. A server with multiple NIC ports and IP addresses has a single IQN. In addition, the IQN changes only if the host name changes; if the IP addresses change, the IQN stays the same.
When provisioning the HPE Nimble Storage volume, select the option **Allow multiple initiator access**. This option allows all nodes in the cluster to see the same volumes and enables high-availability failover if a node fails.

Connect the HPE Nimble Storage volume to each cluster host by using Microsoft iSCSI Initiator. If you have multiple NIC ports from each host to the HPE Nimble Storage array, you can enable MPIO to take advantage of the additional bandwidth and to make your storage connectivity more resilient to a single-path failure.

After the volume is connected to each node, you can use Disk Management on Windows Server or choose **File > Storage Services** from any node in the cluster to see the new disk (the HPE Nimble Storage volume). To bring the disk online, right-click the disk and choose **Online**.
If the disk is not displayed in Disk Management, run the following PowerShell command to force a disk rescan operation:

```
"rescan" | diskpart
```

**Note** If a disk that you have attached by using Microsoft iSCSI Initiator is not displayed immediately after you connect the disk, refresh the **Server Manager Disks** view. Click the **Refresh** button in the upper right side of the Server Manager GUI to reinventory the server. The process is complete when the scrolling status indicator in the title bar and the top of the **Disks** pane stops moving. You may need to scroll down the disk list to find the new disk.

**Determining Windows Disk Numbers and Adding Disks**

If you have many volumes attached to the system and you are not certain which disk is the volume that you are looking for, you can use commands to verify the disk number. When possible, try to name your volumes and clustered disks with the same name as the underlying HPE Nimble Storage volume. This best practice proves useful when you manage systems with many different disks and when you work with clustered disks and CSVs.

**Note** Windows disk numbers are not permanently assigned and may change between server reboots. In addition, the disk number might not match on each cluster node that mounts the same volume. This behavior is determined by Windows and does not affect the cluster functionality.

After you determine the disk number, format the disk as an NTFS volume. You do not need to specify a drive letter or folder to mount the disk at this time. Use the default cluster block size or force the size to 4 KB for the CSV; this volume will hold operating system virtual disks and not data. After the HPE Nimble Storage volume is attached as a disk to each cluster node and it is formatted, put it under control as a cluster resource to enable monitoring and failover between nodes.

**Note** Use GPT-partitioned Windows disks. When initializing a new disk, initialize the partition table as GPT, which is easier to work with than MBR volumes in many circumstances.

The following code example identifies the number of a disk, initializes the partition table as GPT, brings the disk online, and formats the disk:

```
$MySerial=Get-NSVolume -name “MyVolumeName”
```
Enabling CSV

The Cluster Shared Volumes (CSV) feature of Failover Clustering introduced in Windows Server 2008 R2 provides an abstraction layer between the clustered application and the storage. With CSV, all Hyper-V nodes of the cluster can see the storage simultaneously. The feature reduces the time that is required for application failover and allows more than one VM to be stored per iSCSI volume even if the VMs are running on different nodes.

To enable cluster shared storage on your cluster, select the cluster in Failover Cluster Manager and click the Enable Cluster Shared Volumes link in the Configure pane.
After you enable CSV, you should see a new container in Failover Cluster Manager called **Cluster Shared Volumes**. CSV is implemented by mounting storage to each cluster node as junction points beneath the C:\ClusteredStorage directory. CSV creates a subdirectory called \Volume#, where # is a number that is incremented for each successive volume that you attach as a CSV disk.

If you have multiple CSVs, confirm that you are using the correct mount point and thus the correct CSV before you attach it to the nodes. If you are unsure about the exact mount point for a particular CSV, you can verify it in Failover Cluster Manager:

- In Windows Server 2008 R2, expand the CSV entry tree; the branch indicates the mount point.
- In Windows Server 2012 and later versions, select the CSV disk and verify the mount point in the **Details** pane.

### Using Protection Templates

HPE Nimble Storage arrays provide protection templates that contain preconfigured schedules for snapshots, replication, and retention policies.
Protection Schedules for Volumes

When you create a new volume collection, you can select a protection template that inserts a default schedule that is based on existing business rules. For example, you can create protection templates based on the criticality of the application data:

- Less critical applications can use longer snapshot schedule intervals (4 hours) and shorter retention schedules (10 days).
- More critical applications whose data frequently changes, such as databases, usually require shorter snapshot schedule intervals (15 minutes or less) and longer retention schedules (90 days).

Protection templates reduce the amount of work required to create storage volumes and increase consistency for managing similar applications.

Figure 11: Protection template for Hyper-V

Hardware Snapshots versus Software Snapshots

Snapshots are the basis for creating point-in-time versions of storage volumes and backups that can be mounted and accessed just like any other iSCSI volume. You can create snapshots at different layers of the virtualization architecture, including within the guest software, the host software, and the storage hardware. Connecting data volumes directly to the guest allows HPE Nimble Storage Protection Manager (NPM) to trigger snapshots that use the HPE Nimble Storage hardware provider rather than inefficient software-based snapshots.

HPE Nimble Storage arrays provide highly efficient hardware snapshot functionality that is optimized by HPE Nimble Storage inline compression and block-level incremental efficiencies. Snapshots created through native operating system software, such as Microsoft VSS, are not efficiently stored within HPE Nimble Storage volumes. Software snapshots do not take advantage of the optimized snapshot backup functionality of HPE Nimble Storage arrays.

The following diagram summarizes the differences between software snapshots and HPE Nimble Storage snapshots and shows the locations in which they are stored. HPE recommends that you use hardware-based snapshots that take advantage of the performance, inline compression, and cloning capabilities of the HPE Nimble Storage array rather than creating software snapshots that have far less flexibility.
Using Zero-Copy Clones

The HPE Nimble Storage zero-copy cloning feature gives you the ability to quickly clone a volume without duplicating all of the blocks in that volume. Zero-copy clones are valuable for creating test copies of production data without doubling the amount of space required to copy the data. When you clone production data volumes and mount them to test machines to perform QA and development, you get the benefit of working with production data while avoiding the chance of data corruption.

Reporting servers are another great use case because the zero-copy cloning feature enables you to shift the ad-hoc reporting load off of production database servers without increasing the amount of storage space needed to hold that load.

Figure 13: Hyper-V zero-copy clones
Provisioning VMs

You can provision VMs by using one of three primary methods:

- The native Hyper-V Manager
- Failover Cluster Manager
- System Center Virtual Machine Manager (SCVMM)

Hyper-V Manager can be started directly or used indirectly through Failover Cluster Manager. Avoid using Hyper-V Manager directly because this method does not create VMs on an individual server or as highly available clustered resources.

Creating VMs Through Hyper-V Manager and Failover Cluster Manager

To use Hyper-V Manager and Failover Cluster Manager to create a VM, you must know where the CSV disks are mounted to the file system.

**Note** If you are unsure about the mount points, review the information in *Enabling CSV* on page 17 for guidance on how to verify them.

VMs that you create on the CSV by using Failover Cluster Manager are cluster-aware and can fail over between cluster nodes.

**Figure 14: Hyper-V new VM**

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend you identify this virtual machine, such as the name of the guest.

**Name:** MyNewVM

You can create a folder or use an existing folder to store the virtual machine. The virtual machine is stored in the default folder or in the selected folder.

- **Store the virtual machine in a different location**

  **Location:** C:\ClusterStorage\Volume1

Creating VMs Through SCVMM

To use SCVMM to provision VMs on the Hyper-V cluster with an HPE Nimble Storage array, you must enable high availability. Otherwise, the VMs will not fail over within the cluster properly.

To enable high availability, navigate to the **Configure Hardware** page of the **Create Virtual Machine** wizard. Scroll down, expand the **Advanced** section, and select the checkbox **Make this virtual machine highly available**.

When you select this checkbox, the option to place VMs on HPE Nimble Storage shared storage is enabled in the **Configure Settings** page of the **Create Virtual Machine** wizard. If you do not select the high availability option, only local nonshared storage is enabled for provisioning VMs.
Figure 15: Hyper-V VM deployment through SCVMM
Better Hyper-V Backups

When the protection schedule of an HPE Nimble Storage volume collection is triggered, HPE Nimble Storage Protection Manager (NPM) connects directly to the VM's storage interface and asks it to place the application data into a quiescent state. Applications begin to quiesce by flushing any pending I/O write activity from memory to disk, and then they notify NPM when they are ready for a safe snapshot backup. When NPM receives the quiesce notification, it tells the volume collection to create a snapshot of all its associated volumes. After the snapshot is created, data write activity is allowed to proceed.

The HPE Nimble Storage backup method is dramatically faster, and it can be performed at regular short intervals. Other solutions have long backup windows that take hours to complete before another backup can take place. As backup windows continue to grow, many administrators find that they can no longer complete a daily backup, even with a 12-to-14-hour backup window. In addition, scheduled incremental backups leave gaps in protection and do not provide replication for offsite disaster recovery.

In contrast, HPE Nimble Storage arrays perform snapshot backups instantly. Therefore, snapshots can be scheduled for many more point-in-time backups per day than with tape, disk, or Hyper-V host-based backup solutions.

Offsite Replication for Hyper-V

HPE Nimble Storage arrays are built to replicate application-aware snapshots to other arrays by using a WAN-efficient methodology, even if the arrays are off site. Replication settings are configured on individual VMs to allow you to choose which VMs to protect, depending on their unique service-level requirements. This approach works well with the HPE Nimble Storage best practices for the Hyper-V framework, which recommend using one VHD per volume to take advantage of the HPE Nimble Storage zero-copy cloning feature.

You should consider two failover scenarios when performing disaster recovery:

- **Planned failover.** This scenario occurs when an outage is planned (such as for site maintenance) or predictable (such as before a hurricane). A planned failover is typically graceful, allowing you to shut down applications and perform a final push of data from the production site to the disaster recovery site before you start the applications off site.

- **Unplanned failover.** This scenario occurs without prior notice (as in the case of a fire or another catastrophic event), and it usually involves a site outage rather than a server failure. Unplanned failovers do not give you time to perform a graceful shutdown, so they might involve the use of older versions of volumes and cause you to lose data, depending on your replication schedule. For this reason, plan shorter
replication intervals for more critical applications such as databases to reduce the potential for data loss during an unplanned failover.

Hyper-V Disaster Recovery Architecture and Configuration

The disaster recovery architecture for Hyper-V should follow the same best practices as the production environment, especially as those practices apply to failover clustering. However, depending on your service level agreement, the number of hosts in the disaster recovery environment does not have to precisely match the number of production hosts.

Review the following considerations to ensure that your disaster recovery environment is able to properly perform failover by using the implementation framework described in this guide. For disaster recovery steps, see Appendix B: Disaster Recovery Failover on page 27.

VM Import Operations

Hyper-V R2 does not enable you to import VMs that were not previously exported by Hyper-V. You can import Hyper-V VMs by using a script to create the appropriate associations within the disaster recovery Hyper-V server. You must run the script for each VM that you want to bring online in the disaster recovery site.

For instructions on how to create the Import-VM script that you will use for disaster recovery failover and failback, see Appendix A: Import a VM in Hyper-V on page 25.

Virtual Network Naming

To facilitate management, name your disaster recovery virtual networks with the same names that are used in the production site. Hyper-V refers to virtual networks and attaches them to NICs by using a unique ID that is different in the disaster recovery site. Therefore, keeping consistent naming makes it easier for you to reconnect virtual networks to the appropriate NIC. For example, if the public-facing NICs of the production VMs are attached to a virtual network named Public vLAN, then name the corresponding disaster-recovery virtual network also as Public vLAN.

Restores and Planned Failback

After you have successfully failed over to your disaster recovery site and resumed business operations, new data will be created and modified over time. Restoring the new data back to your production site follows the same process as a planned failover disaster recovery, but in reverse. The restore synchronizes data back to the production array so that you can resume business processes in the production facility.

If you were forced to perform an unplanned failover, you must begin the resynchronization manually. To do that, log in to your production array, select the volume collections that you failed over, and click the Demote button. After that, while the volumes remain live, reenable replication for each of the volume collections that you failed over on the disaster recovery array.
Appendix A: Import a VM in Hyper-V

To recover a VM in a Windows Server 2008 Hyper-V environment, you must first run the Import-VM script. The script is used to perform Hyper-V failover because Hyper-V does not have a native import feature that works unless you first export the VM. This limitation presents a management challenge to most Hyper-V environments, but you can overcome the challenge by registering the recovered VM volumes and configuration into Hyper-V.

You must determine the GUID for the Hyper-V VM that you want to import before you run the Import-VM script. The GUID is the name of the XML configuration file that is located in the Virtual Machines directory of the VM volume hierarchy. For example, C:\ClusteredStorage\Volume1\<VM name>\Virtual Machines\ 58AE37DA-53A1-412F-996E-9E26C602696D.xml.

Procedure

1. Copy the following code to a batch file called Import-VM.bat, which you store in both the production environment and the disaster recovery environment.

   ```
   @echo off
   mklink "%systemdrive%\programdata\Microsoft\Windows\Hyper-V\Virtual Machines\%1.xml" "%2\Virtual Machines\%1.xml"
   icacls "%systemdrive%\programdata\Microsoft\Windows\Hyper-V\Virtual Machines\%1.xml" /grant "NT Virtual Machine\%1":(F) /L
   icacls %2 /T /grant "NT Virtual Machine\%1":(F)
   rem done
   ```

2. Run the script as follows:

   ```
   Import-VM GUID "path to configuration"
   ```

   Where:

   - **GUID** is the GUID of the VM.
   - **path to configuration** is the path to the configuration file. The path must be enclosed in quotation marks.

   Example:

   ```
   Import-VM 58AE37DA-53A1-412F-996E-9E26C602696D "C:\ClusteredStorage\Volume1\NS-HV-Server-A"
   ```

   The script output should look similar to this output example:
Where:

- The first line creates a symbolic link for the VM GUID.
- Next, permissions are changed for the directories so that the VM GUID can be connected to the VM configuration files.
- The last line reports that no files failed processing.

If the script fails, verify the input parameters and run it again. If the script continues to fail and you want to run it from a clean point, you can begin fresh by deleting the symbolic link for the VM GUID in the \C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines\ directory, which is normally hidden.
Appendix B: Disaster Recovery Failover

Use the following steps to perform a planned or unplanned disaster recovery failover with HPE Nimble Storage replicated volumes. Some steps are specific to the type of failover. For example, for a planned failover, you must hand over your production volumes to the replication partner; for an unplanned failover, you must promote the volumes to change their ownership to the disaster recovery array.

The steps for mounting the disaster recovery volume, importing the Hyper-V VM, and adding the imported VM as a clustered resource are the same for a planned or an unplanned failover.

Planned Failover: Hand Over Production Volumes

Procedure

1. Gracefully shut down the applications and virtual servers that you want to fail over.
2. Log in to the production HPE Nimble Storage array.
3. Choose Manage > Protection to view the volume collections.
4. Select the volume collection that you want to fail over.
5. Click the Handover button.

The handover process takes a snapshot of the volumes and begins copying the most recent data changes to the disaster recovery array. This operation may take some time depending on how much data has changed.

The handover is complete when the Volume Collection icon of the disaster recovery array changes to the green status.

Volume Collection Icon and Status During Normal Replication

![Volume Collection Icon]

<table>
<thead>
<tr>
<th>Volume Collection</th>
<th>Status</th>
<th>Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS-HV-Server-A--572198068</td>
<td>None</td>
<td>SE Demo N01</td>
</tr>
</tbody>
</table>

Volume Collection after Handover

![Volume Collection Icon]

<table>
<thead>
<tr>
<th>Volume Collection</th>
<th>Status</th>
<th>Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS-HV-Server-A--572198068</td>
<td>None</td>
<td>SE Demo N01</td>
</tr>
</tbody>
</table>

You might need to refresh the Volume Collection view by navigating to the home page and choosing Manage > Protection in the HPE Nimble Storage user interface.

Unplanned Failover: Promote Volumes

Procedure

1. Log in to the disaster recovery HPE Nimble Storage array.
2. Choose Manage > Protection to view the volume collections.
3. Select the volume collection that you want to fail over.
4. Click Promote.

The promote process is used for failover only when the production array is no longer available, such as in the case of an unplanned failover. The process changes the ownership of the volume collection to the disaster recovery array.
The promotion is complete when the Volume Collection icon changes to the green status.

Steps Shared by the Two Failover Methods

In a planned or unplanned failover, you perform the same steps to mount the disaster recovery volume, import the VM to Hyper-V, and add the imported VM as a clustered resource.

Mount the Disaster Recovery Volume

**Procedure**

1. Use Microsoft iSCSI Initiator to mount the volume to a Hyper-V host in the disaster recovery site.
2. Use Disk Management to bring the volume online.
3. Use Failover Cluster Manager to add the volume to the storage container:
   a. Right-click the storage container and choose Add.
   b. Select the volume in the dialog box.
4. Add the disk to the CSV container:
   a. Right-click the storage container and choose Add.
   b. Select the volume in the dialog box.

This step mounts the volume to a junction point in the C:\ClusteredStorage directory.

Import the Hyper-V VM

**Procedure for Hyper-V on Windows Server 2012 and Later Versions**

1. In Hyper-V Manager, right-click the server and choose Import Virtual Machine.

2. Select the folder containing the VM in the CSV that you connected in the previous procedure.
3. Complete all pages of the Import wizard to finish importing the VM.

Procedure for Hyper-V on Windows Server 2008 R2

1. Open Windows Explorer and navigate to the Virtual Machines directory located in the
   \C:\ClusteredStorage\<imported volume>\<virtual machine>\ subdirectory for the HPE
   Nimble Storage volume that you added to the failover cluster.

   You should look for the Hyper-V configuration file whose name represents the GUID of the VM. A new
   configuration file and associated subdirectory are created every time that you create a VM. Therefore, if
   you see multiple configuration files and you are following the HPE Nimble Storage best practice of using
   one VM VHD per volume, select the most recent configuration and delete the older configurations. If you
   are hosting multiple VMs in the same volume, you must run the Import-VM script for each VM.

2. Copy the GUID for the VM to import.
   The easiest method is to select the VM configuration file, click the file to rename it, right-click the selected
   text, and choose Copy.

3. Open a command line on the Hyper-V host to run the Import-VM script.
   For instructions on how to create this script, see Appendix A: Import a VM in Hyper-V on page 25.

4. Run the script, using the VM GUID and the full path to the configuration file.
   Example:
   ```
   Import-VM 58AE37DA-53A1-412F-996E-9E26C602696D
   “C:\ClusteredStorage\Volume1\NS-HV-Server-A”
   ```

5. After the VM is imported successfully, you may need to restart the Hyper-V service for the VM to be
   displayed in Hyper-V Manager.

Add the Imported VM as a Clustered Resource

Procedure

1. Using Failover Cluster Manager, right-click Services and Applications and choose Configure a Service
   or Application.

   **Note** Do not try to add the imported VM by using the Virtual Machines menu because those links allow
   only the creation of a new VM.

2. Select Virtual Machine as the resource type.
3 The next page in the wizard displays the VM that you have imported. Select the checkbox for that VM and click **Next**.

4 Right-click the VM in Failover Cluster Manager and choose **Start virtual machines**.
About the Author

Chris Lionetti

Senior Technical Marketing Engineer
Hewlett Packard Enterprise

Chris Lionetti is a veteran of the storage industry who has been building complex systems and SANs for over 25 years. Chris has long been actively involved with the Storage Network Industry Association, SNIA. He is currently a reference architect on the HPE Nimble Storage team. Earlier in his career, he worked as an engineer for HP, Dell, Microsoft, and NetApp. Chris holds 10 patents on topics related to data centers, networking, and storage.
## Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.0     | April 2017   | • Updated guidance for the implementation of CSVs for Hyper-V  
|         |              | • Included vFC adapter information  
|         |              | • Added GUI importing instructions for Hyper-V to go along with CLI instructions  
|         |              | • Updated CLI commands to be PowerShell friendly or replaced them with the PowerShell equivalent  
| 1.0     | June 2013    | Initial release |