This document has been archived and will no longer be maintained or updated. For more information go to the Storage Solutions Technical Documents page on Dell TechCenter or contact support.
THIS BEST PRACTICES GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2013 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge are trademarks of Dell Inc. Microsoft® and Windows® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.
# Table of Contents

1  Preface ........................................................................................................................................2

1.1 Audience...................................................................................................................................2

1.2 Purpose......................................................................................................................................2

1.3 Disclaimer.................................................................................................................................2

1.4 Customer Support ....................................................................................................................2

2  Introduction..................................................................................................................................3

2.1 Dell Compellent Storage Center Overview .............................................................................3

2.2 Dell Compellent Replay Manager 7 Overview ........................................................................3

2.2.1 Snapshot Terminology Overview ........................................................................................4

2.3 Microsoft Hyper-V Overview ..................................................................................................4

2.3.1 Hyper-V Version and Feature Comparison ........................................................................4

3  Overview of Disaster Recovery Concepts ..................................................................................6

3.1 Cost-Risk Analysis....................................................................................................................6

3.2 Disaster Recovery and Disaster Avoidance ..............................................................................8

3.3 Testing and Documenting Business Continuity Plans ..............................................................8

3.4 Virtualization and Disaster Recovery ......................................................................................9

3.5 Microsoft Hyper-V and Disaster Recovery ..............................................................................9

3.5.1 Server 2008 R2 Hyper-V ....................................................................................................9

3.5.2 Server 2012 Hyper-V .........................................................................................................10

4  Addressing DR Prerequisites ......................................................................................................11

4.1 Multiple Sites............................................................................................................................11

4.2 Alternate Sites ..........................................................................................................................11

4.3 Dell Compellent Storage Centers at Primary and Alternate Locations ...............................11

4.4 Connectivity between the Primary and Alternate Sites .........................................................12

4.5 Network Design at Alternate Sites ..........................................................................................12

4.6 Documentation .........................................................................................................................13

5  Volume Replication Options ......................................................................................................14

5.1 Volume Replication Overview ................................................................................................14

5.2 Recovery of Hyper-V Resources from Replicated Data .......................................................15

6  Disaster Recovery of a Hyper-V Guest from a Replay ...............................................................16
# Document Revisions

**Table 1: Document revisions**

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/19/2011</td>
<td>1.0</td>
<td>Marty Glaser</td>
<td>Initial release for Server 2008 R2</td>
</tr>
<tr>
<td>05/01/2013</td>
<td>2.0</td>
<td>Marty Glaser</td>
<td>Updated to include Server 2012</td>
</tr>
</tbody>
</table>
1 Preface

1.1 Audience
This document is highly technical and is intended for system administrators who are interested in learning more about how Microsoft Hyper-V integrates with the Dell Compellent Storage Center. Readers should have a good working knowledge of the following:
- Dell Compellent Storage Center
- Microsoft Hyper-V
- Business continuity, disaster recovery, and disaster avoidance planning

1.2 Purpose
This document provides disaster recovery best practices recommendations for Microsoft Hyper-V Server 2008 R2 and Server 2012 when using the Dell Compellent Storage Center. A review of some key disaster recovery concepts will be provided below.

1.3 Disclaimer
The information contained within this best practices document is intended to provide general recommendations only. Actual configurations in customer environments may need to vary due to individual circumstances, budget constraints, service level agreements (SLAs), applicable industry-specific regulations, or other factors. Configurations should be tested before implementing them in a production environment.

1.4 Customer Support
Dell Compellent provides live support at 1-866-EZSTORE (866.397.8673), 24 hours a day, 7 days a week, 365 days a year for current customers. For additional support, email Dell Compellent at support@compellent.com. Dell Compellent responds to emails during normal business hours.
2 Introduction

2.1 Dell Compellent Storage Center Overview

The Dell Compellent Storage Center is an enterprise class storage area network (SAN) that lowers costs, reduces storage management and administration time, provides continuous data availability and enables storage virtualization. Storage Center’s Fluid Data Architecture manages data dynamically at the block-level, maximizing utilization, automating tiered storage, simplifying replication and speeding data recovery.

2.2 Dell Compellent Replay Manager 7 Overview

Dell Compellent Replay Manager 7 is a GUI-based backup and recovery application that enables administrators to create application-consistent backups of:

- Guest VMs in Server 2008 R2 and Server 2012 Hyper-V environments
- Guest VMs in VMware environments
- VMware datastores
- Exchange Server data
- SQL Server data
- Local volumes

In Microsoft environments, Replay Manager 7 leverages the power of the Microsoft Volume Shadow Copy Service (VSS) to create and manage application-consistent Replays (snapshots) on the Dell Compellent Storage Center.

For more information about Replay Manager 7 best practices for Hyper-V, please refer to the list of references under Additional Resources in this document.
2.2.1 Snapshot Terminology Overview

The snapshot terms used in this document are defined as follows:

- A **Snapshot** is an industry-standard term used for a point-in-time copy of a SAN volume.
- A **Shadow Copy** is Microsoft’s terminology for a VSS-based point-in-time snapshot. VSS can be leveraged to pause IO and quiesce data in order to obtain application consistency with snapshots of the OS, Hyper-V, SQL Server, Exchange, etc.
- A **Restore Point** is a Dell Compellent point-in-time snapshot of one or more SAN volumes using Replay Manager. Because Replay Manager leverages VSS, Replay Manager snapshots of Hyper-V guest VMs, SQL Server databases, Exchange Servers, and VMware datastores are ensured application consistency.
- A **Replay** is a Dell Compellent point-in-time snapshot of a SAN volume using Storage Center Manager or Enterprise Manager.

2.3 Microsoft Hyper-V Overview

Hyper-V is virtualization software that sits between the physical server’s hardware layer and the Hyper-V guest virtual machines (VMs). Hyper-V presents virtualized hardware resources from the host server to the guest VMs. Hyper-V servers (known as hosts, nodes or virtualization servers) are capable of hosting multiple Hyper-V guest VMs, which are isolated from each other but share the same underlying hardware resources (e.g. processors, memory, networking, and other I/O devices).

More and more server roles that were previously limited to running on physical server hardware for one reason or another can now be virtualized and consolidated to a single host server or a server cluster. For example, the increased scalability offered with Server 2012 Hyper-V now provides for up to 64 CPUs per guest (instead of 4), 1 TB of RAM per guest (instead of 64 GB), and VHDX files up to 64 TB (instead of 2 TB with VDH files). Virtualization offers many advantages such as:

- Increased agility and mobility
- Better resource utilization
- Increased power efficiency
- Reduced operational and maintenance costs
- Faster recovery
- Reduced datacenter footprint and datacenter sprawl

In addition, Hyper-V guest VMs and associated management tools offer greater flexibility for managing resources, balancing load, provisioning systems, and ensuring quick recovery.

2.3.1 Hyper-V Version and Feature Comparison

As shown in in the table below, Hyper-V was first introduced with Windows Server 2008. Server 2012 incorporates the 3rd generation of Hyper-V, which includes many new
enhancements and features. Replay Manager support for Server 2012 Hyper-V was introduced with Replay Manager 6.5.

For more information about the different versions of Hyper-V, please refer to the list of references found under Additional Resources in this document.

**Table 2: Hyper-V version comparison**

<table>
<thead>
<tr>
<th>Windows Server Version</th>
<th>Hyper-V Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2008 Hyper-V</td>
<td>1</td>
</tr>
<tr>
<td>Server 2008 R2 Hyper-V</td>
<td>2</td>
</tr>
<tr>
<td>Server 2012 Hyper-V</td>
<td>3</td>
</tr>
</tbody>
</table>
3 Overview of Disaster Recovery Concepts

A good business continuity strategy will always incorporate disaster recovery and disaster avoidance planning. At a high level, a disaster recovery plan is a process whereby a company ensures they are able to recover as quickly as possible from data loss (by restoring the most recent data) or from an interruption or failure that prevents access to data. It is a very important part of overall IT strategy and in some cases is governed by regulations specific to particular industries.

When a major event happens, a disaster recovery plan will require the involvement of more than just the information technology (IT) department. A business continuity/disaster recovery response team should be comprised of key staff from various parts of the organization that are assigned and trained to handle the various aspects of dealing with a disaster.

In addition to the IT department’s role with recovering data or failing over services and applications to alternate sites, others may be assigned to deal with communications, media releases, security, notifying customers, accounting for employees, etc.

The disaster recovery scenarios that may be encountered (and therefore planned for) are quite diverse, but may vary by location. Disasters can be small (the loss of a single document that impacts one user) or large (an entire site becomes inaccessible). For the most part, the essential elements of disaster recovery are now commonplace, reliable, fairly inexpensive, easy to implement, and are able to address or prevent the majority of events that are most likely to occur. These protections and safeguards include tape backups with off-site storage, on-line backups, disk-to-disk backups, network and physical security measures, malware protection, redundant hardware and internet connections, SAN-based snapshots with remote replication, and battery backups or generators. Many of the more common types of protection are now ubiquitous and are probably already in place in your environment.

Business continuity becomes more complicated with size and number of locations. While virtualization technologies such as Microsoft Hyper-V can help ensure continuity in case of a disaster, they also add complexity to the underlying design. This document will help administrators running Microsoft Hyper-V on Dell Compellent to better understand their disaster recovery and avoidance options, particularly when the design involves multiple locations.

3.1 Cost-Risk Analysis

Disaster recovery planning is an ongoing process that involves cost/risk analysis. Some of the more ubiquitous protections are simple and rather inexpensive to implement. They can provide adequate safeguards for events which are most likely to occur. Other protections for more catastrophic events may be too cost prohibitive or complicated to implement especially when considering the very low odds such events may ever occur.
The graph in Figure 2 shows the relationship between the odds, cost, complexity, and business impact of a particular event that invokes a disaster recovery response. In general, the more disruptive or catastrophic events tend to have much lower odds of occurring, but they also usually require more expensive or complicated designs to ensure business continuity. Therefore, informed business decisions must be made based on these factors as to which disaster recovery measures will be implemented. Where to draw the line will be unique to each company and each location. Implementing more costly protections may be phased in as part of a multi-year plan to spread the cost out over time.

Questions that might be asked as part of a cost/risk analysis include:

- What regulations apply to my industry?
- What are the terms of any service level agreements (SLAs) for business continuity that must be honored?
- What applications and data are the most mission critical to the business or our customers?
- What is the Recovery Time Objective (RTO) for each application or service? In other words, how long can something be down before the business impact becomes too great? For example:
  - Practice Management System – 30 minutes
  - Messaging system – 4 hours
  - Research and Development Server – 2 days
- What is the Recovery Point Objective (RPO)? In other words, how much data loss is acceptable for a particular subset of data? Is backing up the mail server once a day determined to be adequate? If so, the mail server has an RPO of 24 hours. In other words, up to 24 hours of mail data may be lost in the event the mail server has to be recovered from the last backup.
- What types of events are most likely to occur, factoring in the geographic location? A coastal location may be subject to hurricanes. A location on a fault line may be subject to earthquakes. A location in a low lying area may be prone to flooding.
• Is an alternate site far enough away so that the same event does not impact both locations?
• How much will it cost (hardware, software, and staff) to design, implement and support the desired protections? Is that cost justified given the risk?

3.2 Disaster Recovery and Disaster Avoidance

Disaster recovery usually means reacting to an event that causes down time, and takes place unexpectedly with little or no warning. These events can be categorized as follows:

• Events that cause data loss such as malware infection, corruption, accidental deletion, sabotage, or hardware failure of disks or disk arrays.
• Events that interrupt the ability to access data within or between sites, such as damaged Internet lines (e.g. a backhoe operator cuts the fiber link to your main site), short or extended power outages, or network hardware failures.
• Events that cause both loss of data and loss of access to a site, typically caused by more significant and destructive events such as a fire or natural disaster.

Disaster avoidance implies having enough lead time to proactively deal with an event before it happens in a way that prevents or minimizes down time. This is the strategy commonly used when doing system maintenance. An administrator may live-migrate Hyper-V guest VMs to another node in the cluster in order to perform maintenance on the node. Once the node is back on line, the guest VMs can be live-migrated back again, without any guest VM down time.

Disaster Avoidance also comes in to play when a site has advanced notice of a disaster, such as a coastal location that has several days warning of an impending hurricane, or when a site located in a flood plain learns that a projected flood crest may overwhelm the levees. With the advance warning, administrators have limited time to proactively fail over or move applications and services to an alternate location that is safe from the impending disaster before it strikes. However, having advance notice of disaster-causing events is usually the exception and not the rule.

A good business continuity plan will include both disaster recovery and disaster avoidance strategies that leverage a combination of manual and automatic processes to address a wide range of possible scenarios.

• A manual process might be required to restore lost data from a backup or snapshot, or to bring a Hyper-V guest VM on line at an alternate site.
• An automatic process kicks in on its own, such as when a Hyper-V guest VM fails over to another node in the same cluster if the node that currently owns the guest VM experiences a hardware failure.

3.3 Testing and Documenting Business Continuity Plans

The time to find out if your business continuity plan will work is not when faced with a disaster event. Testing your plan periodically is just as important as having a plan. This will help ensure that given an actual event, RTO and RPO objectives can still be met for the most critical parts of the business.

Maintaining good documentation is also key, especially when manual processes are required as part of a disaster recovery plan. Steps and configurations may seem familiar and easy to
remember at present. But with the passage of time, familiarity with the process may diminish. Without good documentation, coupled with the sudden stress of having to deal with an unexpected event, the ability to effectively respond to a DR event may be greatly diminished. Practicing the plan to maintain readiness is therefore important, but the ability to maintain readiness is often impacted by other priorities, limited staffing or budget.

3.4 Virtualization and Disaster Recovery

Virtualization technology now allows servers to be virtualized so that the resources the VM needs (disk, CPU, RAM, etc.) are not tied to any one piece of physical hardware. Some advantages of virtualization include higher density, higher utilization, lower maintenance and support costs, and more efficient use of power. Another big advantage, which lends itself well to business continuity planning, is VM mobility – the ability for a VM to move from one host or node to another.

VM mobility, along with the lower cost of faster and more reliable Internet connections, has made it possible for companies to take advantage of disaster recovery and avoidance options involving multiple locations that were previously too complicated or cost prohibitive to implement.

While VM server mobility can be extended to remote locations over WAN connections, many complex and often expensive design considerations may still be faced, especially when the goal is to automate the fail-over and fail-back processes as much as possible.

Some reasons why automated failover is highly desirable when faced with disaster include:

- Manual failover and failback processes may take too long - RTO goals cannot be met.
- IT resources can be quickly overwhelmed with manual processes when a disaster occurs.
- Manual processes, which can often be complicated, are more prone to user error especially when administrators are under the stress of dealing with a disaster.

3.5 Microsoft Hyper-V and Disaster Recovery

3.5.1 Server 2008 R2 Hyper-V

Microsoft Hyper-V 2008 R2 has some native features that allow administrators limited disaster recovery and avoidance options, but these are limited, primarily between nodes of the same Hyper-V cluster. The DR design limitations of Hyper-V 2008 R2 become more apparent when the goal of a business continuity plan is to extend VM mobility (e.g. failover of guest VMs) to other sites or between separate Hyper-V clusters. New features included with Server 2012 Hyper-V provide some additional DR options (see the next section below).

Despite the limited DR functionality with Hyper-V 2008 R2, administrators can leverage the features available with the Dell Compellent Storage Center to help close some of the gaps, as will be shown later in the step-by-step examples in this document.

**Note:** Third party software may be required to bridge the gap if automating the failover/failback of Hyper-V guest VMs between sites and/or separate Hyper-V clusters is necessary in order to meet RTO goals.
3.5.2 Server 2012 Hyper-V

Server 2012 Hyper-V introduced some new features that provide administrators more options as they consider disaster recovery and disaster avoidance planning for their guest VMs. These include the following:

- **“Share-nothing” migrations of guest VMs:** In Server 2008 R2, a guest VM can only be migrated to another host if it is part of the same Hyper-V cluster. With Server 2012, guest VMs can now be migrated between different hosts and clusters. This migration process is storage agnostic, meaning that the only connectivity required to “share-nothing” migrate a guest VM to another host or cluster is adequate network connectivity between the hosts or clusters.
  - Even though the share-nothing migration process is storage agnostic, Dell Compellent Replays, Volume replications, and Enterprise Manager DR plans can still be leveraged as part of a DR plan when moving or failing over guest VM data between Storage Centers at the same or different locations.
  - Because share-nothing guest VM migrations now make it much easier to move guest VMs regardless of host or cluster boundaries, they become a useful part of disaster avoidance strategy. However, share-nothing migrations don’t provide much if any disaster recovery protection, in cases where a site becomes inaccessible unexpectedly.

- **Hyper-V Replica** provides administrators with a significant DR enhancement for their Server 2012 Hyper V environments. Replica allows administrators to replicate guest VMs to another location. In the event of a disaster, these replicated guest VMs can be brought on line at the alternate location as part of a DR plan. Hyper-V Replica is also storage agnostic. For more information about Hyper-V Replica and how to configure it for DR situations, please refer to the Microsoft TechNet Hyper-V library as listed under Additional Resources in this document.
4 Addressing DR Prerequisites

Regardless of the version of Hyper-V, in order for Hyper-V guest VMs to be brought online at an alternate location in the most time sensitive way possible, a number of prerequisite design considerations must be taken into account and be planned for in advance:

4.1 Multiple Sites

With only one location available, recovery options are extremely limited if a major event causes data loss or prevents access to that site. With two locations, they should ideally be far enough apart so that the same event does not prevent access to both sites.

4.2 Alternate Sites

Alternate sites can be referred to as hot, warm or cold.

- A “hot” site usually means that one or more applications or systems at a primary site are mirrored or clustered at a secondary site in such a way that automatic failover of at least some of these resources can occur between the two sites. For example, A Hyper-V cluster may have nodes that exist at both locations (stretch clustering), allowing for guest VM Live Migration in conjunction with Live Volume, given a disaster avoidance situation. Given a full DR event, an Enterprise Manager DR plan can be invoked, to map replicated volumes to Hyper-V hosts and nodes at the DR site.

- A “warm” site means an alternate site has all the necessary hardware and networking components in place to accommodate the primary site’s Hyper-V guest VMs if they need to be manually failed over. This would typically require having Server 2008 R2 or 2012 Hyper V hosts or clusters pre-provisioned at the alternate site that have the capacity to accommodate the primary site’s guest VMs. Recovery would include creating View Volumes from replicated Storage Center volumes at the DR site, mapping them to Hyper-V hosts or clusters, and recovering the guest VMs manually. Hyper-V VM replicas (if using Server 2012 Hyper-V) can also be brought online fairly quickly at a hot or warm DR site.

- A “cold” site means that there is rack space and power at a DR site but some (or all) of the necessary hardware infrastructure is lacking. Given a DR event, this hardware would need to be obtained, transported to the site, and then staged. For DR recovery at a “cold” site, administrators have to plan for the additional time and resources required to set up the required hardware. This additional set-up time may make it difficult or impossible to meet RTO goals.

4.3 Dell Compellent Storage Centers at Primary and Alternate Locations

The Storage Centers at any alternate locations should have adequate disk performance and capacity to accommodate the primary site’s Hyper-V guest VMs and data. To save money, a company may choose to do the following at their alternate location(s):

- Install fewer hardware redundancies (at their own risk).
- “Cascade” an older Storage Center from a primary site down to an alternate site to serve as a backup or DR Storage Center there.
• Alternate sites may feature lower performance, lower tier disks and slower back-end connectivity, as long as the design will still provide adequate I/O performance.

4.4 Connectivity between the Primary and Alternate Sites

Over long distances, this is usually accomplished by private (dedicated) circuits or public Internet connections of sufficient bandwidth to allow for remote replication of Dell Compellent volumes, Replays and Restore Points from one Storage Center (at a primary site) to another Storage Center (at an alternate site).

Within shorter distances, such as within a metro area or a campus, dedicated fiber circuits may be available as a means of connecting sites that are in closer proximity to each other. With high-speed low-latency fiber connectivity between two locations, stretch clustering (in conjunction with Dell Compellent Live Volume) becomes a viable disaster avoidance (not disaster recovery) strategy. Enterprise Manager DR plans also become a good disaster recovery option for stretched Hyper-V clusters.

4.5 Network Design at Alternate Sites

The network design at an alternate site needs to allow users and systems (on site and remote) to continue to access the Hyper-V resources once they are brought on line there. Design considerations include:

• Configuration at the ISP level, with rules to re-route traffic to an alternate site automatically if the primary site goes down (for example, redirect customer access to a web portal to an alternate site)
• Local routing rules and or gateway settings
• VLAN configurations
• Firewall rules
• DNS resolution (both internal and external)
• Domain Authentication for end users, domain service accounts, clusters, etc.

If Active Directory (AD) Domain Controllers (DCs) and Domain Name Service (DNS) servers are virtualized as Hyper-V guest VMs, there are some special design considerations to keep in mind to avoid some pitfalls. For example, it is a best practice to avoid virtualizing DCs on a Hyper-V cluster if that cluster depends on them for authentication. Doing so could result in cluster down time if there isn’t another DC outside of the cluster to authenticate cluster services.

• To recover from this situation, it may be necessary to manually recover the virtual DC to a standalone Hyper-V host in order to get the DC, and then the cluster, back on line.
• Due to the predicaments that virtualizing DC/DNS servers on clusters can cause, there are a couple different strategies that can be used to avoid the pitfalls.
  o Virtualize DC/DNS servers but place them on standalone Hyper-V hosts, making sure the host’s local administrator password is documented and accessible.
  o Keep at least one DC/DNS server running on physical hardware.

Note: The best-case recovery scenario provides for stretched Layer 2 networking functionality between the two sites so that guest VMs will function at either location without having to change their IP, DNS and gateway settings. This will greatly simplify the process of
bringing guest VMs on line, and minimize the manual changes that must be made to guest VMs before they will function. However, Layer 2 extensibility across sites can involve complex network design considerations that may not always be practical or possible.

4.6 Documentation

Documentation is a critical (and often overlooked or neglected) component of ensuring that a disaster recovery plan goes as smoothly as possible.

- Documenting key information about Hyper-V guest VMs that may need to be manually recovered at an alternate site is important because some settings may have to be manually reconfigured. Some essential specifications for a guest VM might include:
  - Number of CPU cores assigned.
  - Static or dynamic memory settings.
  - Disk configurations (e.g. which VHDs, pass-through disks, and direct-attached volumes are presented as which drive letters or mount points to the guest VM).
  - Static IP settings (IP, subnet mask, DNS, default gateway).
  - Which applications or services on a guest VM are tied to the guest's name or current IP address, or MAC address? Application-level changes may also be necessary in some cases if the server's name, IP, or MAC settings change.

- Document the fail-over process itself and refine it as part of testing. Understand which Hyper-V guest VMs take priority based on RTO goals for specific services or subsets of data.

- Accessibility – loss of access to a primary site should not interfere with being able to access key documentation. Make sure that current documentation exists at one or more alternate locations and that it can be accessed remotely and securely by the necessary staff.
5 Volume Replication Options

5.1 Volume Replication Overview

Dell Compellent provides several different kinds of replication options for replicating Hyper-V data to alternate locations for disaster recovery and disaster avoidance purposes. Whether using automated or manual Hyper-V DR recovery methods at a remote location, DR cannot happen at a remote location if the necessary data isn’t there. Storage Center volume replication provides a simple, easy-to-manage means for ensuring that the data needed for DR is available on a DR Storage Center at a remote site.

1) **Remote Volume Replication**: Replication is a configuration option that can be enabled between two or more Storage Centers to replicate volumes (on a volume by volume basis) and all their associated Replays (snapshots). There are two types of volume replication:
   - **Asynchronous replication**: the primary Storage Center will replicate a volume and its associated Replays to a remote Storage Center asynchronously.
   - **Synchronous Replication**: which has two modes with Storage Center 6.3 and newer:
     - **High consistency mode**: this ensures that a volume (and its Replays) stays completely synchronized between a primary and secondary Storage Center. This means that maintaining consistency of the volume between the two Storage Centers takes precedence over availability.
     - **High availability mode**: this option is very similar to high consistency mode, except that availability (e.g. continuing read/write access to the volume) is favored over consistency. As along as synchronization can keep up, high availability mode acts just like high consistency mode. But if the link between the Storage Centers goes down, or latency gets too high, high availability mode will allow the secondary instance of the volume to fall out of sync in favor of keeping the primary instance of the volume online to prevent a service outage. When the connectivity, link or latency issue affecting the secondary instance of the volume is resolved, volume synchronization catches up and is reestablished.

   **Note**: For more detailed information about asynchronous and synchronous volume replication options, please refer to the Enterprise Manager Administrator’s Guide as listed under Additional Resources in this document.

2) **Live Volume**: this option is useful for disaster avoidance (not disaster recovery) situations, such as for maintenance. Live Volume can be used to move the primary ownership of a replicated volume to another Storage Center without causing a service interruption to servers and applications using that volume. In order for Live Volume to work correctly, both Storage Centers must remain online with connectivity to each other. Live Volume is therefore not a viable option for DR situations where a site might go off line unexpectedly, or the link between Storage Centers is lost unexpectedly.
   - **Live Volume use case #1**: A customer with a single Storage Center has experienced growth, and has decided to install a 2nd Storage Center in their data center. To balance utilization between the two Storage Centers, an
administrator uses Live Volume to move some volumes to the new Storage Center.

- **Live Volume use case #2**: A Storage Center has to be taken completely off line for a short time to move it to a new location, or to perform maintenance. Live Volume can be used to move volumes to other Storage Centers without causing a service outage, and once the affected Storage Center is back on line, the volumes can be moved back again.

- **Live Volume use case #3**: A company with two locations learns that spring flooding may affect their main site. Because they have several days advance notice, they are able to use Live Volume to move their mission critical volumes to a Storage Center at another location that will be unaffected by the flooding. Once the risk at the primary location has past, Live Volume can again be used to move the volumes back to the main location again.

**Note**: It is very important to understood that Live Volume is *not* a valid consideration for disaster recovery planning (only for disaster avoidance planning). This is because if the primary instance of a Live Volume goes off line during an unexpected disaster event, the secondary instance of the Live Volume at the alternate location is not accessible. While Copilot support can help with fracturing (clearing) the Live Volume attributes by using the Storage Center command line, this is risky because there is no way to guarantee the integrity of the data on the fractured volume. Live Volume is intended to be used for disaster avoidance situations only, such as in the three use cases listed above.

### 5.2 Recovery of Hyper-V Resources from Replicated Data

Once data is replicated to another Storage Center, the replicated data can be used in a number of different ways to aid in the recovery Hyper-V hosts and guest VMs.

- Manual recovery, using replicated volumes and associated Replays (see Disaster Recovery of a Hyper-V Guest from a Replay below).
- Create an Enterprise Manager DR plan, which helps to automate the process of recovering Hyper-V resources at a remote location (see Enterprise Manager DR Plans and Hyper-V below).

In Server 2008 R2 Hyper-V environments, where guest failover and live migration is limited to within the same cluster, native Hyper-V DR and disaster avoidance options are very limited. With Server 2012, which offers share-nothing guest VM migrations and Hyper-V Replica, more DR and disaster avoidance options are provided natively within Hyper-V. For more information on share-nothing migrations and Hyper-V Replica, please see Server 2012 Hyper-V above and also the Microsoft TechNet Hyper-V library (see Additional Resources).

While the examples shown in the remainder of this document can be used for either Server 2008 R2 or Server 2012 Hyper-V environments, they are most applicable to Server 2008 R2 environments where native DR and disaster avoidance functionality is limited.
6 Disaster Recovery of a Hyper-V Guest from a Replay

In this example, a Server 2008 R2 Hyper-V guest VM on a Server 2008 R2 cluster will be recovered at a secondary site using either a Storage Center Replay or Replay Manager Replay. This example assumes that:

- An unexpected disaster at the primary site has resulted in a loss of data and access.
- A secondary site is available and located far enough away from the primary site so it is unaffected by the event.
- The secondary site is at least a “warm” site (hot, warm and cold site definitions are reviewed above in Section 4.2).
- The secondary site has all of the design considerations met to allow for manual recovery of Hyper-V guest VMs, as reviewed in the Section 4 of this document.

For more information on how to set up and use Storage Center Data Instant Replays, Replay Manager Backups, and Volume Replication to a remote Storage Center, please refer to the Dell Compellent documentation listed under Additional Resources in this document.

6.1 Verifying the Environment

Figure 3: Hyper-V Guest configuration at the primary site
1) As shown in Figure 3, the configuration at the primary location shows (as set up before the disaster) that the Hyper-V guest VM “Guest01” is configured to use a cluster shared volume (CSV) on TS-HV-Cluster01.

2) The Hyper-V cluster nodes, along with the CSV containing Guest01’s VHD files, are configured on Storage Center 12 at the primary location. Hourly, daily, and weekly Storage Center Data Instant Replays are being taken of the CSV volume.

![Figure 4: Replay Manager Restore Points](image)

3) For purposes of this example, Replay Manager with the Hyper-V extension for VSS (application consistent) backups is also configured for Guest01, as shown in Figure 4.

![Figure 5: Remote Replication to a remote Storage Center](image)

4) As shown in Figure 5, from the perspective of Storage Center 12 at the primary location, the CSV has been replicated from Storage Center 12 to Storage Center 13 at the remote site. Note that the volume icon helps to visually identify quickly which volumes are being replicated.
5) From the perspective of Storage Center 13 at the alternate location, the CSV and all of its Replays have been replicated to Storage Center 13 (as shown under the Replays tab). This includes Storage Center Replays and Replay Manager Replays as shown in Figure 6.

Note: The presence of "Repl_" indicates that the volume is a replication volume. This makes them easy to identify on a remote Storage Center.

6.2 Recover a Hyper-V Guest VM from a Replay

In this example, Guest01, a Server 2008 R2 guest VM on a Server 2008 R2 Hyper-V cluster, will be recovered from a Replay (snapshot) on the remote Storage Center at the secondary location.
6.2.1 Verify Documentation

Table 3: Guest VM details needed for manual guest VM recovery (differences at the recovery site in bold text)

<table>
<thead>
<tr>
<th>Guest Details</th>
<th>Primary Location</th>
<th>Recovery Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Name</td>
<td>Guest01</td>
<td>Guest01</td>
</tr>
<tr>
<td>Hyper-V Cluster</td>
<td>Cluster01</td>
<td>Cluster04</td>
</tr>
<tr>
<td>Guest Static IP Address</td>
<td>172.16.23.220</td>
<td>172.16.23.220</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.16.23.1</td>
<td>172.16.23.1</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>172.16.23.10, 11</td>
<td>172.16.23.10, 11</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB (static)</td>
<td>4 GB (static)</td>
</tr>
<tr>
<td>Number of CPU’s</td>
<td>4 cores</td>
<td>4 cores</td>
</tr>
<tr>
<td>AD Domain name</td>
<td>techsol.local</td>
<td>techsol.local</td>
</tr>
<tr>
<td>Backup Methods</td>
<td>Storage Center Replays</td>
<td>Storage Center Replays</td>
</tr>
<tr>
<td></td>
<td>Replay Manager Hyper-V Backups</td>
<td>Replay Manager Hyper-V Backups</td>
</tr>
<tr>
<td>Virtual DVD drive</td>
<td>Z:\</td>
<td>Z:\</td>
</tr>
<tr>
<td>Boot Vol.</td>
<td>Drive Letter</td>
<td>C:\</td>
</tr>
<tr>
<td></td>
<td>VHD Name</td>
<td>TSHVC01_Guest01_Boot</td>
</tr>
<tr>
<td></td>
<td>Volume Name</td>
<td>...CSV01_Guests</td>
</tr>
<tr>
<td></td>
<td>Storage Center</td>
<td>Storage Center 12</td>
</tr>
<tr>
<td>Data Vol.</td>
<td>Drive Letter</td>
<td>D:\</td>
</tr>
<tr>
<td></td>
<td>VHD Name</td>
<td>TSHVC01_Guest01_Data01</td>
</tr>
<tr>
<td></td>
<td>Volume Name</td>
<td>...CSV01_Guests</td>
</tr>
<tr>
<td></td>
<td>Storage Center</td>
<td>Storage Center 12</td>
</tr>
</tbody>
</table>

Review the available documentation for Guest01. Table 3 above shows an example of data that an administrator might need when manually recovering a Hyper-V guest VM at an alternate site. With no access to the primary site, it might be difficult to recreate guest VMs with exactly the same configuration without some minimal documentation available.

6.2.2 Terminate Volume Replication

Decide what do with the volume replication between the primary and alternate site:

1) If the Storage Center hardware was lost at the primary location, then volume replication settings should be removed. Use Enterprise Manager at the remote location to remove the volume replication (see Step 3 below).

2) If the primary site will come back on line with its Storage Center and data intact, then an administrator may choose to leave the volume replication settings it place. Once both sites come back on line, volume replication will resume.

3) To remove remote volume replication, from the Enterprise Manager GUI, click on Replications and Live Volumes, select the Source and Destination Storage Centers, click on the desired volume replication to highlight it, and then click on Delete. Leave the Recycle Dest Volume box unchecked to preserve the replicated volume on the destination storage center.

6.2.3 Create a View Volume

1) The next step in the recovery process is to create a View Volume from a Replay (usually the most recent Replay) that is associated with the replicated volume. As
shown in Figure 6 above, there are two types of Replays to choose from in this example: Storage Center Replays or Replay Manager Replays.

- Storage Center Replay. These can be either crash-consistent (e.g. if the server was running with active IO at the time of the snapshot) or application-consistent (e.g. the server was powered off at the time the snapshot was taken).

- A Replay that was initiated by Replay Manager or other external application. Replay Manager Replays leverage VSS for application-consistency.

2) A View Volume for recovery purposes can be created from either type of Replay, but if choosing to recover from a Replay Manager Replay, a few extra steps are required, as detailed below, to clear some volume attributes.

Figure 7: Create a View Volume from a Replay

3) To create a View Volume, identify the desired Storage Center Replay or Replay Manager Replay. Choose the most recent Replay to minimize data loss. Replays are listed under the Replays tab for a volume.

4) Right click on the Replay, and select Create Volume from Replay, as shown in Figure 7. In this example, a Replay Manager Replay was chosen to create the View Volume; therefore, a few volume attributes will need to be cleared, as detailed below.

Figure 8: Create a View Volume from a Replay

5) Complete the View Volume creation wizard.
   - Provide a name for the new View Volume. By Default, the suggested name will be the Volume’s original name with View1 appended as shown in Figure 8.
• Indicate the volume folder to save the new View Volume to (under TS-HV-Cluster04 in this example).

6.2.4 Clear Volume Attributes

If the View Volume was created from a Replay Manager Restore Point (as in this example), it will contain some volume attributes (e.g. read-only) that need to be cleared. It is also not possible to present it to a Hyper-V Cluster using Failover Cluster Manager until the VSS structure is removed from the volume. Steps to clear these attributes and the VSS structure are provided below.

1) Determine if manually clearing volume attributes is necessary. If the Replay chosen is a regular Storage Center Replay, then volume attributes do not need to be cleared and it can be mapped to a Hyper-V host or a cluster. Please skip to Section 6.2.5 below to continue.

2) If the Replay chosen was a Replay Manager Replay, some volume attributes need to be cleared. In addition, if the View Volume will be presented to Hyper-V cluster, the VSS structure also needs to be cleared.

3) The first step to clear volume attributes from a View Volume is to map the View Volume to a standalone server host.

4) Use Disk Management to bring the View Volume on line on the Windows Server host and note its volume information.

5) Then open a command prompt window.
At the command prompt, type:

```
Diskpart <enter>
```

Using Figure 9 as an example, select the correct volume (volume 3 in this example). Verify, and then clear the attributes by entering the commands as shown in Figure 9 above. Verify that the attributes are cleared (set to "No") and then exit DiskPart.

If the disk does not have a drive letter assigned to it, then use Disk Management to assign a drive letter of your choice. In this example, the letter D is assigned to the disk.
Figure 10: Run CHKDSK after modifying attributes

10) As shown in Figure 10, check-disk has to be run after clearing the attributes, as follows:

   CHKDSK <DRIVELETTER:> /F <enter>

11) Verify that the CHKDSK command completes without any errors. If errors are indicated (e.g. "an unspecified error has occurred") then repeat the CHKDSK command. It should complete without any errors before continuing.

12) If the View Volume is already mapped to the desired standalone Hyper-V Server, then leave the disk on line and proceed to manually recover any guest VMs or data. If the View Volume is to be attached to a Hyper-V cluster as a new CSV (as in this example), then clearing the VSS structure as shown starting with Step 13 below, is necessary.
13) A View Volume of a Replay Manager Restore Point has a disk IO structure (assigned to it by VSS) that needs to be reset (removed) before Failover Cluster Manager will recognize the View Volume as available disk space for clustering. If attempting to add a volume to a cluster that has not had the VSS structure removed, Failover Cluster Manager will not recognize the disk space as valid for clustering. As shown in Figure 11, the presence of this IO structure on a disk can be verified by:

- Validating the cluster (run all tests)
- After the test finishes, view the report
- Under Results by Category, click on Storage, then on List all Disks.
- Examine the detail under the Disk Characteristics column. In this example, Physical Drive 1 contains the IO structure that needs to be cleared, as indicated by the presence of the “Disk is a snapshot disk” characteristic.

14) To remove this disk IO structure, first ensure that the disk is mapped to a standalone 2008 or 2012 Server (not a cluster). Assign a drive letter to the disk, and make sure the disk is online.

15) On this same server, install the latest Dell Compellent PowerShell Command Set (if not already installed). The installer can be downloaded for free from the Dell Compellent Knowledge Center.

16) Verify the serial number of the disk (volume) on the Storage Center, as found under the General tab for the disk. In this example, the disk serial number is 000002bb-0000b0eb.

17) On the server where the PowerShell Command set is installed, go to Start→All Programs→Compellent Technologies→Storage Center PowerShell Snapin→Compellent Storage Center Command Set Shell.

18) Connect to the desired Storage Center and make the changes by using the PowerShell Cmdlet “Set-DiskDevice” with the “-ResetSnapshotInfo” parameter. This Cmdlet is available with the Dell Compellent Command Set 6.1 (or newer) for PowerShell release.

For example:

Get-SCConnection <enter>.
scl3 <enter> (to connect to Storage Center 13)
$username <enter> (must be a valid user on the Storage Center)
$password <enter>
Get-Help Set-DiskDevice <enter> (for syntax if desired)
Set-DiskDevice -ResetSnapshotInfo -SerialNumber 000002bb-0000b0eb <enter>
The Set-DiskDevice command should return a result such as the following:

<table>
<thead>
<tr>
<th>DeviceName</th>
<th>Size</th>
<th>Status</th>
<th>Health</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>\PhysicalDrive1</td>
<td>550.00GB</td>
<td>Online</td>
<td>Healthy</td>
<td>000002bb-0000b0e9</td>
</tr>
</tbody>
</table>

**Note:** For more information on using PowerShell cmdlets to clear the VSS disk structure, please refer to the PowerShell command set release notes and also the administrator’s guide as listed in the Additional Resources section of this document.

19) Close out of the PowerShell window. Use DiskPart to ensure that the read only, hidden, and shadow copy attributes have been removed from the volume (see Figure 9). Then take the disk off line.

**6.2.5 Map the View Volume to a Hyper-V Cluster**

1) Using Storage Center Manager or Enterprise Manager, map the disk to the desired servers or (preferred) the desired cluster servers object.

2) Using Disk Manager, make sure that the disk is off line, and that it is visible to all nodes in the cluster. If necessary, rescan the disks on each node.

3) Launch Failover Cluster Manager and add the new disk space to the cluster. Then add the disk space as a new CSV.

**Note:** If Failover Cluster Manager fails to see the new disk space, make sure that the disk is offline on all nodes in the cluster, and that the volume attributes and VSS structure have been removed. It may be necessary to run the Cluster Validation Wizard to verify that “this is a Snapshot Disk” is no longer listed as a disk characteristic (see Figure 11).

![Figure 12 Add the View Volume to the cluster as a new CSV](image)

4) After adding the CSV to the cluster, make note of the data path (where the VHDs are located), in this case, C:\ClusterStorage\Volume2 on cluster TS-HV-Cluster04 as shown in Figure 12.

5) Recover any resources from the CSV. In this case, a guest VM is manually recovered (recreated) using the guest VM configuration information from Table 3 above. In this
example, Guest01 has two VHDs on the CSV: one for the OS (as the C:\ drive), and one for data (as the D:\ drive).

6) Boot the guest VM and verify functionality.
7) Repeat the steps above to recover additional Hyper-V guest VM resources at the alternate site (for example, if there are multiple guest VMs on the CSV, recover each guest VM).
8) Configure Storage Center Replays as desired for this View Volume.
9) If another Storage Center is available at this or another alternate location, Volume replication for this View Volume can be set up to another Storage Center.
10) If Replay Manager Backups of the recovered guest VMs are desired, then configure new Replay Manager Backup Sets from an instance of Replay Manager Explorer at the alternate location.

6.3 Considerations before Bringing the Primary Site Back on Line

If a disaster resulted in loss of hardware, data and infrastructure at the primary location, it is not possible for guest VMs to come back on line there. When and if the site does come back on line, it will be as though it were a new site with new hardware.

But what if the disaster resulted in loss of access only (no loss of data or infrastructure)? Once the event has passed or has been resolved, the primary site will come back on line with Hyper-V guest VMs and data that were current as of the start of the outage.

If it is possible (or anticipated) that the primary site will come back on line with infrastructure, servers, and old data intact, the administrator must take some precautions. For example, the original Hyper-V guest VMs at the primary location should not be allowed to come back on line at the same time as the recovered guest VMs at the alternate location. Allowing this to happen might result in a number of undesirable consequences such as data loss or corruption. Strategies to avoid this might include:

- Suspending connectivity between the primary location and alternate location.
- Preventing the guest VMs from coming on line at the primary site.
- Isolating the guest VMs at the primary site so they cannot be accessed by users or other systems, at least not initially.

6.4 Fail-back Options

Fail-back options might include:

- No fail-back will happen (the secondary site will become the primary site for the recovered guest VMs and data).
- Set up Volume Replication from the Dell Compellent Storage Center at the alternate site back to the Storage Center at the primary site. Once replication has finished, then schedule a maintenance window, and from a Storage Center Replay or a Replay Manager Restore Point, create a View Volume and manually recover guest VMs to their original location at the primary location.
- Live Volume could also be used as a means of moving data volumes assuming there is adequate bandwidth between the sites. For more information see Disaster Avoidance and Live Volumes below.
• Restore only the changed data from the manually recovered guest VMs at the secondary site back to the original guest VMs at the primary site. This might require a short maintenance window.

6.5 Disaster Avoidance and Live Volume

As has been stated previously under Disaster Recovery and Disaster Avoidance above, the use of Dell Compellent Live Volume is not considered to be a valid disaster recovery strategy.

If the primary site’s Storage Center contains the primary copy of a Live Volume, and an alternate site’s Storage Center contains the secondary copy of a Live Volume, if the primary site goes down (the connectivity between the two Storage Centers is lost), access the secondary Live Volume at the alternate site is also lost.

While it is possible to have Copilot forcibly remove (fracture) Live Volume attributes from the secondary volume in the event of a disaster, there is no way to guarantee the integrity of the data on the fractured secondary volume. For more information, please refer to the Live Volume Best Practices Guide as listed in the Additional Resources section of this document.

The main purpose of Live Volume is to be able to gracefully move volumes between separate Storage Centers on either a temporarily or permanent basis, while both Storage Centers are one line and are linked to other.

With disaster avoidance, many prerequisites come into play, as reviewed above in this document. Three key components include:

• Stretch Clustering. This means that a Hyper-V cluster has one or more nodes at two separate locations on separate Storage Centers. One Hyper-V cluster is in essence “stretched” across two sites.

• Layer 2 networking functionality is also “stretched” between the two sites, so that Hyper-V guest VMs can be live migrated to either site without having to reconfigure any network settings. While stretched Layer 2 networking is not a requirement for Live Volume to function, it is required for seamless migration of Hyper-V guest VMs between sites.

• The primary and alternate sites must be “well connected” to ensure that adequate bandwidth is available along with low latency. Connectivity would ideally be a high bandwidth fiber connection. This “well connected” requirement limits the maximum distance between the two sites to shorter distances - making disaster avoidance a challenge given that sites located too close together may be affected by the same disaster.

Given a disaster avoidance situation affecting the primary location, an administrator has time to proactively:

• Live-migrate Hyper-V guest VMs to a Storage Center at an alternate site.

• Shift primary ownership of the Live Volumes to the remote Storage Center.

• Once the event has passed or been resolved, the guest VMs and Live Volumes can be moved back to the primary site.

For more details on how to set up and use Live Volume in conjunction with Microsoft Hyper-V and stretch clustering, please refer to the Live Volume Best Practices Guide as listed in the Additional Resources section of this document.
7 Enterprise Manager DR Plans and Hyper-V

7.1 Introduction

Enterprise Manager allows administrators to predefine a DR plan for one or more replicated volumes. A predefined DR plan specifies which hosts or clusters to map the replicated volumes to at the DR site when activating disaster recovery.

An example of how to predefine and activate disaster recovery for the cluster volumes associated with a stretched hyper-V cluster will be shown below; including the process for failing back after the primary site is back on line.

For more general information about configuring Enterprise Manager and DR plans, please see the Enterprise Manager Administrator’s Guide as listed under Additional Resources.

7.2 Enterprise Manager DR Plans with Stretch Clustering

With Server 2012 Hyper-V, administrators have the option of using Hyper-V Replica as the preferred means of recovering guest VMs at an alternate site.

For Server 2008 R2 Hyper-V (for which no Replica option exists), Enterprise Manager DR plans provide a means of DR with failover and failback for a stretch cluster configuration (also known as a metro or geo cluster).

In the example below, a DR plan will be configured for a Server 2012 Hyper-V stretch cluster (works equally well with a Server 2008 R2 Hyper-V stretch cluster) and then activated to show the process of bringing the cluster volumes and associated resources on line at the remote site. And finally, the cluster volumes and associated resources will be failed back to the primary location.

7.3 Stretch Cluster Environment Design

In this example, the environment has been set up as follows:

- The primary and secondary locations are “well connected” with adequate data bandwidth and low latency between them to allow for data replication. These sites should ideally be far enough apart to minimize the risk of one DR event affecting both locations.
- Both locations are remotely accessible to administrators. This is important to ensure a timely response to a DR event.
A Dell Compellent Storage Center is configured at each location, each with sufficient IO and volume (space) capacity to support the Hyper-V stretch cluster's resources. In this example, Storage Center SC 12 is the source Storage Center at Site A, and Storage Center SC 13 is at the DR location, Site B, as shown in figure 13.

A Hyper-V stretch cluster is in place (Server 2012 Hyper-V is used in this example; also applies to Server 2008 R2). All four nodes are configured boot-from-SAN to their respective local Storage Center, and the cluster has a quorum disk and two CSVs located on the Storage Center at Site A. All four nodes in the cluster are configured to access the volumes on the Storage Center at Site A as shown above. Fiber Channel is used as the transport in this example, but iSCSI is also supported. Options for replicating the data to the Storage Center at site B, as well as pre-defining a DR plan will be provided below.
Sufficient host capacity is in place at each location to accommodate the cluster resources (e.g. guest VMs) given a DR event. In this example, each site has two Hyper-V nodes, for a total of 4 nodes in the stretch cluster.

![Diagram of a stretch cluster with stretched fabric](image)

**Figure 15:** Stretch cluster with stretched fabric

- The four Hyper-V nodes are configured with dual-port fiber channel HBAs with MPIO enabled (configured to use round-robin). The fiber fabric, as well as Layer-2 networking (for LAN and iSCSI) is also stretched between the two sites.
- An Enterprise Manager Data Collector Server is installed and configured at the main location, Site A, and also at the recovery location, Site B. In this example, they are installed on virtual servers that are not part of the stretch cluster.
- A remote (DR) instance of the Data Collector at Site A is installed and configured at the remote location, Site B. In this example, the remote Data Collector is installed and configured on a virtual server at the remote location that is not part of the stretch cluster. The remote Data Collector server’s role is to maintain a copy of the volume recovery point information from the primary Data Collector server at Site A. This information on the remote Data Collector server must be accessible at the recovery site in order to activate disaster recovery.
- At least two instances of the Enterprise Manager Client are installed.
  - One instance is installed at the primary location on a virtual server that is not part of the stretch cluster.
  - A second instance is installed at the remote location on a virtual server that is not part of the stretch cluster.
    - Installing an instance of the Enterprise Manager client on the same VM as the Data Collector is supported and recommended.
  - The Enterprise Manager Client can also be installed on workstations or laptops with supported operating systems as an additional means of accessing the primary and remote Data Collector servers.
- Administrators should also ensure that adequate up-to-date documentation about the environment exists and is remotely accessible. This is an important but sometimes neglected part of a formal business continuity plan.

**Note:** The above list covers common design considerations for a stretch cluster environment but is not meant to be all-inclusive.
7.3.1 Enable Replication of Cluster Volumes

In this example, the quorum disk and the two CSVs are configured to replicate to Storage Center 13 at Site B.

![Diagram showing replication of volumes between Site A and Site B](image)

Figure 16: Replication of the Quorum and CSV volumes to a remote Storage Center

1) To enable replication on a volume, navigate to the volume under **Storage** in Enterprise Manager, right click on the volume, choose **Replicate Volume**.

![Replication Attributes window](image)

Figure 17: Choose replication options

2) Complete the wizard by selecting the destination Storage Center, and the desired replication type (Asynchronous or Synchronous). For more information on these options see **Volume Replication Options** above in this document.

**Note:** The two modes of synchronous replication (a choice between High Availability or High Consistency) were introduced with Enterprise Manager 6.3.
3) In this example, the volumes are replicated in **Synchronous High Availability** mode as shown above in Figure 18. To view the status of replicated volumes, click on **Replications and Live Volumes**, select the **Source** and **DR Storage Centers**, and under the **Replications** tab, highlight the replicated volume, and view the **Replication Information** area for the volume.

4) For more information on how to set up volume replication using Enterprise Manager, please see Dell Compellent documentation listed under **Additional Resources**.

5) To view the replication volumes, use Enterprise Manager to view them on the destination Storage Center. In this example, the three volumes on the destination...
storage center had “Repl of...” prepended automatically to help identify their purpose as replication volumes.

6) Under the Mappings tab, the volumes show as mapped to the source Storage Center, not to a server host or cluster.

7) After activating a DR plan (as will be shown below), the DR plan will automatically rename the volume names from “Repl of...” to “DR of...” as shown in Figure 20 to help differentiate them. The Mappings tab for the volumes will show that the mapping is changed from the source Storage Center to a server host or cluster object.

7.4 Create an Enterprise Manager DR plan

Once volume replication has been configured, disaster recovery can be predefined for one or more volumes using the volume Restore Points under the Restore Points tab.

Figure 20: Identifying activated DR volumes on the recovery Storage Center

Figure 21: Predefine Disaster Recovery with Enterprise Manager
1) Scroll to the desired volume Restore Point in the list.
2) Right-click on the volume and select **Predefine Disaster Recovery**, or click on the button by the same name on the toolbar as shown in Figure 21.

![Figure 22: Define server mapping for predefined Disaster Recovery](image)

3) Set the desired **Predefine Disaster Recovery** wizard options. In this example, the **Server** is set to **MG-HV-Cluster05**, which is a cluster object on the Storage Center for the four Hyper-V nodes TSSRV226 – TSSSV232 as shown in Figure 22.

4) Repeat the **Predefine Disaster Recovery** wizard for each volume. In this example, the above steps are repeated for the other CSV and the quorum disk.

### 7.5 Activate Enterprise Manager Disaster Recovery

When a disaster event occurs, a decision has to be made about when and if to activate the disaster recovery plan. Such variables as the time of day, nature and expected duration of the outage, individual service level agreements (SLAs), the type of data, and RTO objectives will affect the decision.

For example, if the disaster event is expected to be very brief in duration and it happens to occur after hours, it may be acceptable to endure a short outage at the main location, rather than failing over to the DR site.

In this example, since an extended outage is anticipated, the remote (DR) data collector will be used to activate disaster recovery at the DR site.

1) To activate disaster recovery, launch the Enterprise Manager client (located at the DR site or from your laptop or workstation) and log in to the DR instance of the Enterprise Manager Data Collector server at Site B.
2) Click on the **Restore Points** tab, and then on **Activate Disaster Recovery** from the toolbar.

3) Select the **Source** and **Destination** Storage Center pair and click on **Next**. In this example, the source Storage Center is SC 12, and the destination Storage Center is SC 13 as shown in Figure 24 above.

4) Check the box for **Allow Planned Activate Disaster Recoveries** and click on **Next**.
5) Under **Available Restore Points**, check the box in front the desired volumes. In this example, the quorum disk and the two CSV cluster disks for the stretch cluster are selected. Then click on **Next**.

![Activate Disaster Recovery](image1)

**Figure 27:** Edit the settings for each volume

6) The selected volumes will be listed as shown above. If desired, click on the **Edit Settings** button to verify the disaster recovery actions for each volume, such as which host or cluster to map the recovery volume to. In this example, those settings have already been made. Click on **Finish**.

![Message](image2)

**Figure 28:** Message prompt

7) When presented with the **Message** dialog box, click on **OK** to close it, and then monitor the progress from the **Recovery Progress** tab.

![Monitor the Recovery Progress](image3)

**Figure 29:** Monitor the Recovery Progress

8) To view the state of the recovery progress, monitor the **Restore State** and **Message** columns. DR recovery is complete for each action when **Restore State** shows as **Finished** and the **Message** column shows as **DR volume has been activated**.
9) The mappings from the cluster nodes at site B will now be mapped to the recovery volumes on the DR Storage Center, as shown in the example above in Figure 30.

7.6 Verify the Health of the Hyper-V Cluster

1) Connect to a node of the cluster at the DR site and start Failover Cluster Manager.

2) Verify that the quorum and cluster disks are on line. It may be necessary to manually bring these disks online. If the disks will not come online, it may be necessary to access Disk Management and rescan the disks on each node to make sure they are visible on each node. In this example, two of the three cluster disks are offline and need to be brought on line manually using Failover Cluster Manager.
3) Once all the cluster disks are online, then verify the health of the cluster resources. In this example, there are two guest VMs to verify. If necessary, manually start the guest VMs and then verify that they are functioning correctly.

7.7 Fail Back to the Primary Site

Once the DR event has been resolved, and the Storage Center and Hyper-V cluster nodes are back on line at the primary site, then fail-back can be accomplished by using the Restore/Restart DR Volumes option in Enterprise Manager.

Before failing back, identify a time to do so. This would typically be done during a scheduled maintenance window after hours. As part of the fail-back maintenance window, factor in enough time to allow any new data generated on the volumes at the DR site to replicate back to the primary Storage Center since the failover was initiated.

Before initiating the fail-back, if possible, suspend any cluster resources to put them into a consistent state. In this example, the two guest VMs on the cluster are powered off temporarily to put them (and their data) into a consistent state.

To fail back, complete the following steps.
Figure 33: Restore/Restart DR Volumes

1) Access Enterprise Manager at the primary site using the Enterprise Manager Client.
2) Under Replications and Live Volumes, filter the list of volumes by selecting just the desired Source and Destination Storage Centers. In this example, SC12 is the source Storage Center, and SC13 is the destination Storage Center.
3) Click on the Restore Points tab.
4) Under the State column, scroll down to locate the volumes with a status of DR Activated. Note that in this example, the quorum disk and the two CSVs for the stretch cluster show with a state of DR Activated.

**Note:** The Degraded status for these three DR Activated volumes simply reflects the fact that the volumes are currently running from the DR Storage Center instead of the source Storage Center. It is not meant to imply that there are additional problems with the drives themselves such as performance or connectivity issues that need to be resolved. When the volumes are failed back to the source Storage Center, the status will revert to Up.

5) When ready to start fail-back, click on Restore/Restart DR Volumes.

Figure 34: Select the source and destination Storage Centers

6) Select the desired Source and Destination Storage Centers. In this example, the source is still SC 12, and the destination (the DR site) is still SC 13. Then click on Next.
7) Review the warning messages. For more information about each of the options, click on the Help button. In this example, since the desire is to allow the wizard to automatically deactivate the destination (the DR) volumes as part of fail-back, the **Automatically Deactivate Destination** box is checked as shown in Figure 35. When ready to continue, click on **Next**.

8) Under **Available Restore Points**, select the desired volumes to recover. In this example, the quorum disk and the two CSVs for the stretch cluster are selected. Then click on **Next**.

Figure 35: Review the Restore/Restart DR Volumes warning messages

Figure 36: Select the desired Restore Points.

Figure 37: Edit/verify the settings for each Restore/Restart DR volume
9) Highlight each volume and click on the **Edit Setting** button to verify the mappings and other settings. When satisfied with the settings for each volume, click on **Finish**.

![Message prompt](image)

**Figure 38: Message prompt**

10) When presented with the **Message** dialog box, click on **OK** to close it, and view the progress from the **Recovery Progress** tab.

![Monitor the recovery process](image)

**Figure 39: Monitor the recovery process**

11) Monitor the state of the recovery process for each volume, noting the state of the **Restore State**, **Replication Complete**, and **Message** columns.

12) Once the **Restore State** shows as **Finished** for all the volumes being failed back, access one of the Hyper-V cluster nodes at the primary location, and start **Failover Cluster Manager**.

![Use Failover Cluster Manager to manage cluster disks](image)

**Figure 40: Use Failover Cluster Manager to manage cluster disks**

13) Verify that the cluster nodes, CSVs, and the quorum disk are all online. In this example, there are four cluster nodes, a quorum disk, and two CSVs. It may be necessary to rescan the disks on each node of the cluster before being able to bring all the cluster disks back on line.
14) Start any cluster resources and verify functionality. In this example, two guest VMs were powered off to put them into a consistent state before initiating the fail back, so it is necessary to start the guest VMs again once the fail back has completed.

15) From the Enterprise Manager Client, select the Source and Destination Storage Centers, and verify the volume replication status. In this example, the three volumes are replicating from Storage Center 12 to Storage Center 13 again in Synchronous High Availability mode, the same as before the DR plan was activated.

16) Complete any other necessary checks to ensure health of the environment.

17) Verify that the desired Replay schedules are still in place on the replicated volumes.

18) Fail-back is now complete.

7.8 Debriefing

After experiencing a disaster recovery or disaster avoidance event (even if it is a drill), it can be very beneficial to evaluate the results during a debriefing.

- Did we meet RPO/PTO goals?
- Did we satisfy SLA’s?
- What parts of the plan worked well?
- What improvements can be made so responding to future events goes smoother? (and then update procedures and documentation accordingly)
8 Conclusion

Hopefully this document has proven helpful and has accomplished its purpose by providing useful answers for many commonly asked questions about disaster recovery planning with Microsoft Hyper-V and the Dell Compellent storage Center.
9 Additional Resources

Below are some links to additional resources:

Dell Compellent Documentation:
- Dell Compellent Enterprise Manager 6.3 Administrator’s Guide
- Dell Compellent Storage Center 6.3 System Manager Administrator’s Guide
- Dell Compellent Replay Manager 7 Administrator’s Guide
- Dell Compellent Replay Manager 7 for Hyper-V Best Practices Guide and Demo Video
- Dell Compellent Microsoft System Center VMM 2012 SP1 Best Practices Guide and Demo Video
- Dell Compellent Command Set 7.0 for Windows PowerShell Administrator’s Guide
- Dell Compellent Live Volume Best Practices Guide
- Dell Compellent MPIO Best Practices Guide

http://kc.compellent.com

Microsoft System Center Technical Documentation Library

Microsoft Hyper-V (Server 2008) Planning and Deployment Guide:

Microsoft TechNet Hyper-V (Server 2008) document collection:

Microsoft TechNet Hyper-V (Server 2012) document collection:

Feature Comparison – Windows Server 2008 R2 Hyper-V and Server 2012 Hyper-V
http://download.microsoft.com/download/2/C/A/2CA38362-37ED-4112-86A8-FDF14D5D4C9B/WS%202012%20Feature%20Comparison_Hyper-V.pdf


Offloaded Data Transfers (ODX)