Dell EMC SC Series Replay Manager 7 and Hyper-V

Abstract

This document provides Replay Manager best practices and configuration guidance for Dell EMC™ SC Series and Microsoft® Hyper-V® environments.

July 2017

Revisions

Date	Description
May 2013	Initial release
January 2017	Updated for Replay Manager 7.7
July 2017	Updated for Replay Manager 7.8 and Microsoft Windows Server® 2016

Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Author: Marty Glaser

Feedback

Dell EMC values customer feedback and strives to provide high-quality documentation. Send feedback or recommendations about this document to StorageSolutionsFeedback@dell.com.

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of contents

Executive summary

This document provides Replay Manager best practices and configuration guidance for Dell EMC™ SC Series and Microsoft® Hyper-V® environments. It builds upon the information presented in the *Replay Manager Administrator's Guide*, which is the primary information resource to deploy and configure Replay Manager. The administrator's guide provides installation and configuration guidance to configure Replay Manager to protect Microsoft Exchange, Microsoft SQL Server®, VMware®, and Windows Server® Hyper-V environments on Dell EMC SC Series storage.

1 Introduction

The ability to protect and recover important data reliably and quickly is a critical requirement of business continuity planning. Administrators have many options to choose from, and in many cases, more than one means of data protection is required in order to ensure short- and long-term recoverability from a variety of potential disaster scenarios.

Dell Replay Manager plays an important role in the overall data protection strategy for a Dell EMC SC Series storage environment because of its ability to obtain application-consistent backups (restore points) of protected workloads. In Microsoft environments, Replay Manager leverages the Microsoft Volume Shadow Copy Service (VSS) to ensure that uncommitted data is flushed to disk and writes are held before a restore point is created.

Section 2 provides a brief overview of the major components in a typical Hyper-V configuration on SC Series storage. The sections that follow include best practices recommendations and configuration tips to protect Hyper-V environments with Replay Manager.

Determining best practices is often subject to factors that vary based on the customer environment. These factors include the type of data, budgetary constraints, complexity, required depth of knowledge, service-level agreements, regulations, and personal preference. What works well for one environment may not be ideal for another. On occasion, the chosen solution might not be completely harmonious with typical best practices. For example, it might be perfectly acceptable to implement a more cost-effective solution that omits some redundancies for a test, development, or DR environment that can suffer downtime without significant impact to the business. When different configuration options are possible, determining the best design is ultimately up to the customer.

1.1 Audience

This document is for technology professionals interested in learning more about best practices to configure Replay Manager to protect Hyper-V environments with SC Series storage arrays. Readers should have working knowledge of Hyper-V and SC Series storage. See appendix A for additional resources for configuring Hyper-V with SC Series storage.

2 Overview

This document features Replay Manager 7.8, Dell EMC SC Series storage, Storage Center Operating System (SCOS) 7.1, and Microsoft Windows Server 2016 R2 Hyper-V which includes the Hyper-V VSS writer. See the *Replay Manager Administrator's Guide* for your version of Replay Manager (available on Dell.com/support) for a complete list of the supported software versions.

The following subsections provide a brief overview of each of these components.

2.1 SC Series Replay Manager

Replay Manager is a GUI-based client/server application that creates and manages application-consistent backups (restore points) that consist of Replays (snapshots) of volumes that host the protected workload on SC Series storage.

While Replay Manager is a valuable data-protection and recovery tool for administrators, it is not designed to serve as the only means for backup and recovery. For longer-term archival storage beyond a few days or weeks, other methods that are better suited for long-term storage (such as tape or cloud-based backups) should continue to be used. Because most recoveries leverage the most recent backup to minimize data loss, the availability of application-consistent Replay Manager restore points is of great benefit to administrators.

For more information on the setup, installation, and configuration of Replay Manager, see the *Replay Manager Administrator's Guide*.

2.1.1 Replay Manager integrations

Replay Manager application-consistent restore points can be obtained for the following:

- Guest VMs in Hyper-V environments (the focus of this guide)
- Guest VMs in VMware® environments
- VMware datastores
- Microsoft Exchange Server
- Microsoft SQL Server®
- Windows Server local volumes

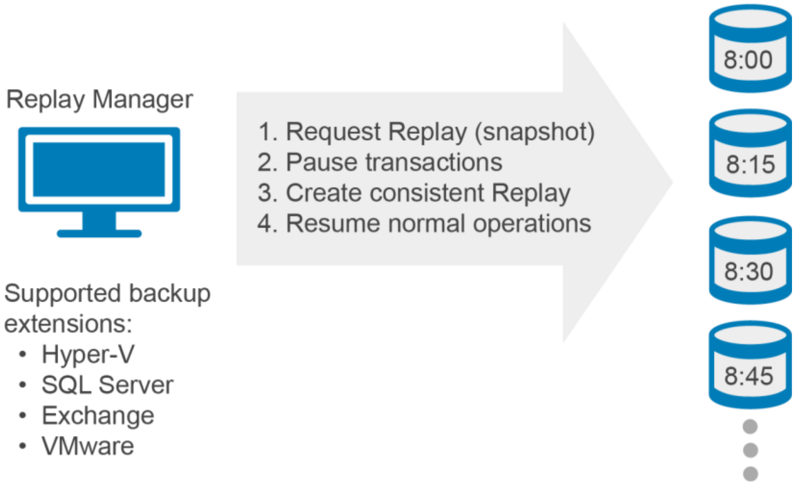

Replay Manager
1. Request Replay (snapshot)
2. Pause transactions
3. Create consistent Replay
4. Resume normal operations
Supported backup extensions:
• Hyper-V
• SQL Server
• Exchange
• VMware
8:00
8:15
8:30
8:45

Figure 1 Replay Manager backup extensions

2.1.2 Replay Manager and PowerShell

In addition to the GUI, Replay Manager supports a number of Microsoft PowerShell® cmdlets. The ability to script backup processes is a great benefit to administrators. For example, a backup process that incorporates Replay Manager can be automated with PowerShell so it will run unattended outside of normal working hours.

2.1.3 Replay Manager components

The main Replay Manager components include:

Replay Manager Explorer GUI: Install this GUI on the server, workstation, or guest VM of your choice to enable centralized management of the Replay Manager environment.

Replay Manager agent: Install this agent on each physical server to be protected (on Hyper-V hosts in this example). It can also be installed on a guest VM for granular protection of SQL Server or Exchange Server databases on direct-attached iSCSI or pass-through disks.

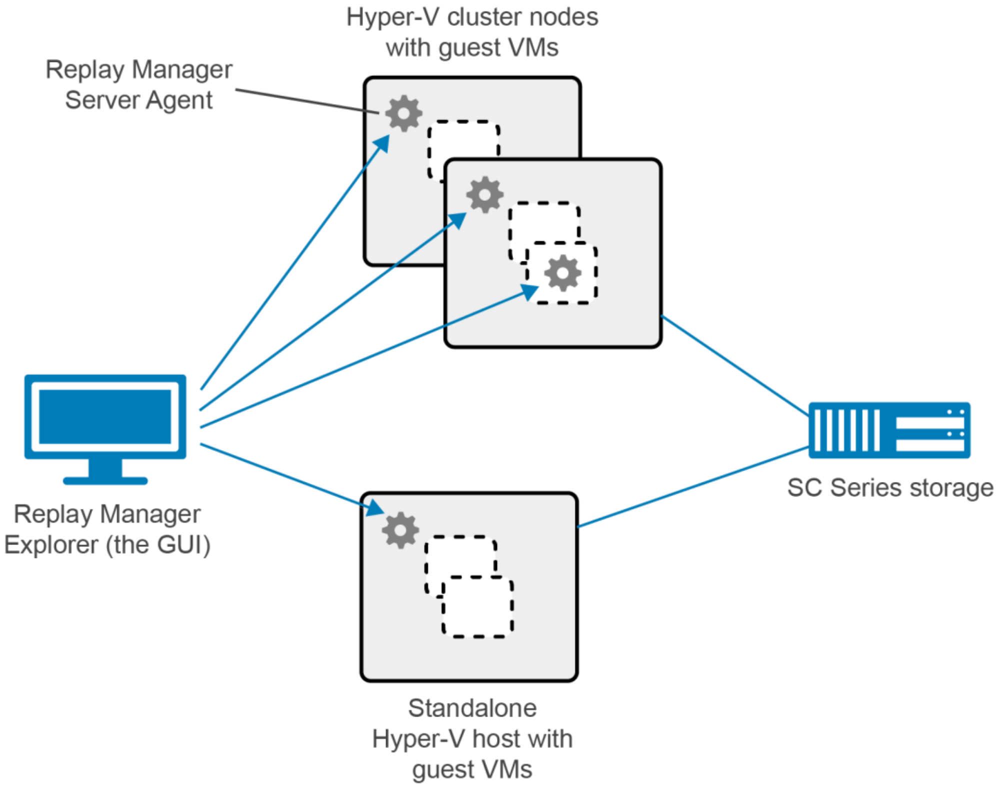

Hyper-V cluster nodes with guest VMs
Replay Manager Server Agent
Replay Manager Explorer (the GUI)
SC Series storage
Standalone Hyper-V host with guest VMs

Figure 2 Replay Manager components

2.2 SC Series storage

SC Series storage solutions provide many robust features such as true flash optimization, thin provisioning, data optimization, data reduction (deduplication and compression), automated sub-LUN tiering, sub-disk RAID levels, synchronous replication with automatic failover, and intelligent read and write data placement.

In addition to raw capacity and I/O performance, other important factors such as monitoring, reporting, trending, protection of data (backups, snapshots, and replication) and the ability to recover in case of a disaster are equally important. The SC Series array is well suited to provide solid, proven solutions to Hyper-V environments to meet all of these business needs. To learn more about specific SC Series storage arrays, visit the SC Series product family page on Dell.com.

2.3 Windows Server and Hyper-V

The Windows Server platform leverages Hyper-V for virtualization technology. Initially offered with Windows Server 2008, Hyper-V has matured with each release to include many new features and enhancements. This guide features Windows Server 2016 with the Hyper-V role installed. See the *Replay Manager Administrator's Guide* for a complete list of supported configurations for Hyper-V.

Microsoft Hyper-V has evolved to become a mature, robust, proven virtualization platform. At a basic level, it is a layer of software that presents the physical host server hardware resources in an optimized and virtualized manner to one or more guest virtual machines (VMs). Hyper-V hosts (also referred to as nodes when clustered) can greatly enhance host server hardware utilization (including processors, memory, NICs, and power supplies) by allowing many VMs to share these resources at the same time. Hyper-V Manager and related management tools (such as Failover Cluster Manager, Virtual Machine Manager, and PowerShell) offer administrators great control and flexibility for managing host and VM resources, VM mobility, SAN storage, balancing workloads, provisioning systems, and ensuring quick recovery.

To learn more about Hyper-V, including tools, videos, blogs, and the feature enhancements that have been made available with each new release of Hyper-V, visit the Microsoft TechNet Library.

In addition to this document, the SC Series Technical Documents page at Dell TechCenter contains deployment guides, demo videos, and reference architectures in support of single and heterogeneous application workloads running on Hyper-V and SC Series arrays, including Microsoft Exchange, Microsoft SQL Server, and VDI.

Both Hyper-V and SC Series storage are feature-rich solutions that together present administrators with a diverse range of configuration options to solve key business objectives.

2.4 Terminology

The following terms are used in this guide:

Snapshot: An industry-standard term for a point-in-time, crash-consistent copy of a SAN volume. Depending on the SAN vendor, a snapshot may be physical (an actual copy of the volume) or virtual (metadata). With SC Series storage, volume snapshots are very space efficient because they consist of metadata pointers to existing data blocks.

Replay: An SC Series snapshot created by Replay Manager. Replays leverage VSS (in the case of Microsoft workloads) to achieve application consistency.

Microsoft shadow copy: A VSS-generated, point-in-time snapshot of a component such as the server OS, Hyper-V guest VM, SQL Server, or Exchange.

Backup set: A backup job configured in Replay Manager.

Restore point: A backup created by Replay Manager.

View Volume: A new space-efficient SAN volume that is created using metadata pointers to an SC Series snapshot or Replay. View Volumes can be mapped to a host server or guest VM for recovery or other purposes. Replay Manager leverages View Volumes for operations such as restores and transfers.

Microsoft VSS: The means by which Replay Manager is able to achieve application consistency of a Microsoft workload when creating a backup set. Application consistency means in-flight I/O is flushed to disk and I/O is paused temporarily before creating a backup.

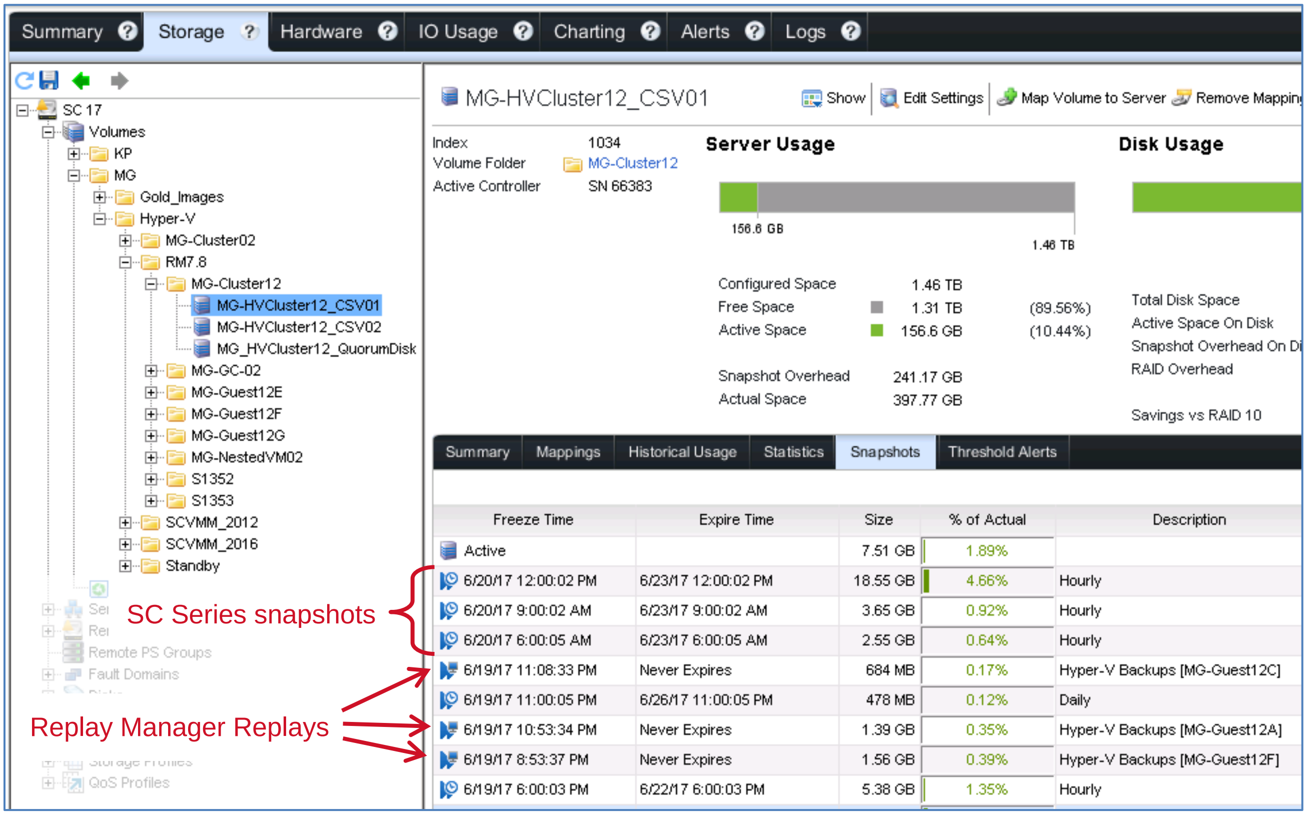
2.5 Microsoft VSS

In Microsoft Hyper-V environments, Replay Manager 7 leverages the Microsoft VSS for Hyper-V to achieve application consistency for a backup set by performing the following steps:

1. A Replay Manager backup job starts.
2. Replay Manager requests that VSS place the guest VM into an application-consistent state by flushing I/O to disk and briefly pausing I/O (including transactional data such as SQL Server and Exchange).
3. VSS creates a native Hyper-V snapshot of the guest VM to disk.
4. Replay Manager creates a restore point by doing the following:

   a. Replay Manager takes a Replay (snapshot) of the SAN volume that contains the guest VM and the native Hyper-V snapshot.

   b. The Replay is listed under the volume and assigned a unique icon to help differentiate it from regular crash-consistent snapshots as shown in Figure 3.



SC Series snapshots

Replay Manager Replays

Index 1034
Volume Folder MG-Cluster12
Active Controller SN 66383

Configured Space	1.46 TB	
Free Space	1.31 TB	(89.56%)
Active Space	156.6 GB	(10.44%)
Snapshot Overhead	241.17 GB	
Actual Space	397.77 GB	

Total Disk Space
Active Space On Disk
Snapshot Overhead On Di
RAID Overhead
Savings vs RAID 10

Freeze Time	Expire Time	Size	% of Actual	Description
Active		7.51 GB	1.89%	
6/20/17 12:00:02 PM	6/23/17 12:00:02 PM	18.55 GB	4.66%	Hourly
6/20/17 9:00:02 AM	6/23/17 9:00:02 AM	3.65 GB	0.92%	Hourly
6/20/17 6:00:05 AM	6/23/17 6:00:05 AM	2.55 GB	0.64%	Hourly
6/19/17 11:08:33 PM	Never Expires	684 MB	0.17%	Hyper-V Backups [MG-Guest12C]
6/19/17 11:00:05 PM	6/26/17 11:00:05 PM	478 MB	0.12%	Daily
6/19/17 10:53:34 PM	Never Expires	1.39 GB	0.35%	Hyper-V Backups [MG-Guest12A]
6/19/17 8:53:37 PM	Never Expires	1.56 GB	0.39%	Hyper-V Backups [MG-Guest12F]
6/19/17 6:00:03 PM	6/22/17 6:00:03 PM	5.38 GB	1.35%	Hourly

Figure 3 Location of Replay Manager Replays

   c. After the Replay (restore point) is created, the native Hyper-V snapshot is deleted by VSS to free up disk space on the SAN.

5. Guest VM I/O resumes.

VSS for Hyper-V allows the protected workload to stay online while the restore point is created. The I/O is paused just long enough for Replays to be obtained so there is no service interruption. The exception is guest VMs with Windows Server NT4 or Windows Server 2000, which must be placed in a saved state to achieve consistency before a restore point is created. This causes a brief service interruption for these older OS versions.

3 Protect Hyper-V resources with snapshots and Replays

For Hyper-V environments on SC Series storage, crash-consistent SAN-based snapshots (see column 2 in Table 1) provide great short- and long-term protection, especially when volumes and their associated snapshot histories are replicated to other SC Series arrays.

Table 1 Snapshot and Replay options for Hyper-V resources

		Replay Manager Replays (application consistent)		
Protected data	**SC Series snapshot (crash consistent)**	**Hyper-V guests extension**	**Local volume backup (agent installed on the host)**	**Local volume backup (agent installed on the guest VM)**
Physical Hyper-V server boot disk (OS) (boot-from-SAN)	✓		✓[1]	
Quorum disk for a Hyper-V cluster	✓		✓[2]	
CSV (hosting one or more guest VMs)	✓	✓	✓	
CSV (hosting one or more shared virtual hard disks)	✓		✓	
Pass-through disk attached to a guest VM	✓			✓[3]
Direct-attached disk mapped to a guest VM (iSCSI)	✓			✓
Direct-attached disk mapped to a guest VM (virtual Fibre Channel)	✓			✓[4]
Nested Hyper-V hosts, clusters and VMs (Server 2016 Hyper-V & newer)	✓	✓[5]	✓[5]	✓[5]

[1] VSS may fail to fully pause I/O on a very active boot volume, resulting in a backup failure.

[2] The Hyper-V node that owns the quorum disk can change, resulting in a backup failure.

[3] Use of pass-through disks, while supported, is discouraged with newer versions of Hyper-V. Use direct-attached iSCSI disks instead. Replay Manager supports protecting pass-through disks attached to a guest VM using a virtual SCSI controller. Protecting a pass-through disk attached to a guest VM using a virtual IDE controller is not supported with Replay Manager.

[4] Although Replay Manager can be configured to protect virtual Fibre Channel (vFC) disks mapped to a guest VM, this configuration is not officially supported with Replay Manager 7.8 and is therefore not recommended in a production environment.

[5] Requires the use of direct-attached iSCSI disks for any data protected with Replay Manager. All nested Hyper-V hosts, clusters, and guest VMs (when the Replay Manager server agent is installed locally) require iSCSI server mappings on the SC Series array in order for Replay Manager restore operations to complete successfully.

As a best practice, every SAN volume should have at least one SC Series snapshot profile applied, with a retention policy that ensures at least one unexpired snapshot exists when daily Data Progression and data reduction (compression and deduplication) operations run. These processes (when enabled) require the presence of at least one unexpired snapshot for a SAN volume to be eligible.

If Replay Manager is used to protect a volume, then Replay Manager Replays (snapshots created by Replay Manager) will satisfy this requirement also. However, it is still a good idea to apply a basic SC Series snapshot profile to each SAN volume regardless of Replay Manager. The SAN supports both types of snapshots concurrently, including the ability to replicate both types of snapshots to other SC Series arrays, extending DR recovery options.

Note: Replay Manager is not supported on volumes that are configured as Live Volumes. They are mutually exclusive features for any given volume.

In addition, regular SC Series snapshots provide an alternate method of recovery (to a crash-consistent state) in case recovery with Replay Manager is not possible or fails.

Without means to flush and pause I/O, SAN-based snapshots are usually not considered to be application consistent. For some workloads, lack of application consistency may not be an issue. However, for transactional workloads such as a database that may span two or more volumes, lack of application consistency can result in a recovery failure due to corrupt data.

Replay Manager solves the challenge of obtaining application consistency by leveraging the Microsoft VSS to flush in-flight I/O to disk and pause new I/O before creating restore points.

3.1 Snapshot and Replay best practices for Hyper-V

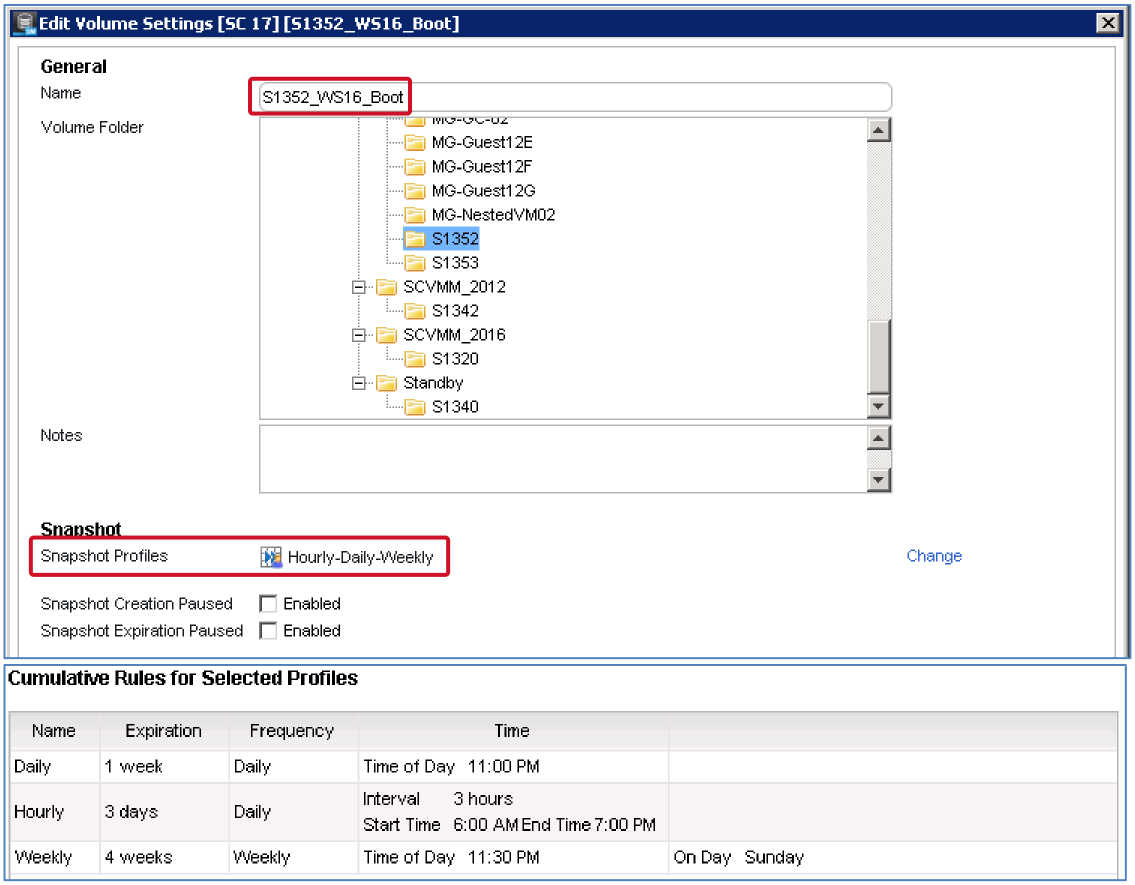
Referring to Table 1, consider the following best practices for configuring snapshot and Replay protection for components in a Hyper-V environment.

3.1.1 Boot disks for physical Hyper-V hosts that leverage boot-from-SAN

Option 1: Protect with SC Series snapshots (recommended).

- Make sure that only the OS resides on the boot disk (install transactional workloads on other disks).
- Risk of complication with recovery of a Windows or Hyper-V host boot-from-SAN disk to a crash-consistent state is minimal. Recovery of a boot disk with a crash-consistent snapshot is similar to powering on the server after a power loss at that point in time.

In Figure 4, the Hyper-V host server S1352 has a boot-from-SAN disk that is protected with a custom profile — hourly (every 3 hours), daily (at 11 p.m.), and weekly (on Sunday evening) — that retains the hourly snapshots for 3 days, the daily snapshots for 1 week, and the weekly snapshots for 4 weeks.



Edit Volume Settings [SC 17] [S1352_WS16_Boot]

General

Name: S1352_WS16_Boot

Volume Folder: S1352

Notes:

Snapshot

Snapshot Profiles: Hourly-Daily-Weekly

Snapshot Creation Paused □ Enabled

Snapshot Expiration Paused □ Enabled

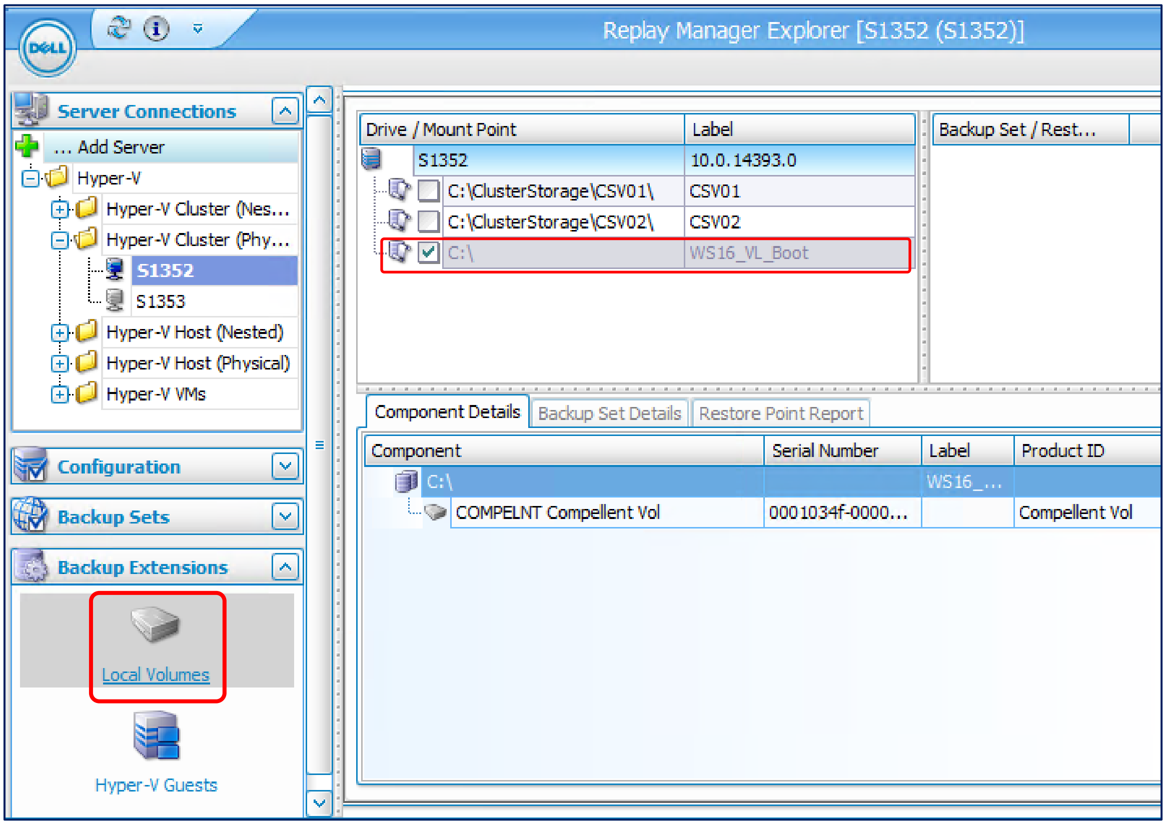
Cumulative Rules for Selected Profiles

Name	Expiration	Frequency	Time	
Daily	1 week	Daily	Time of Day 11:00 PM	
Hourly	3 days	Daily	Interval 3 hours Start Time 6:00 AM End Time 7:00 PM	
Weekly	4 weeks	Weekly	Time of Day 11:30 PM	On Day Sunday

Figure 4 Snapshot profile applied to a Windows Hyper-V host server boot-from-SAN disk

Option 2: Protect with a Replay Manager Local Volumes backup set.

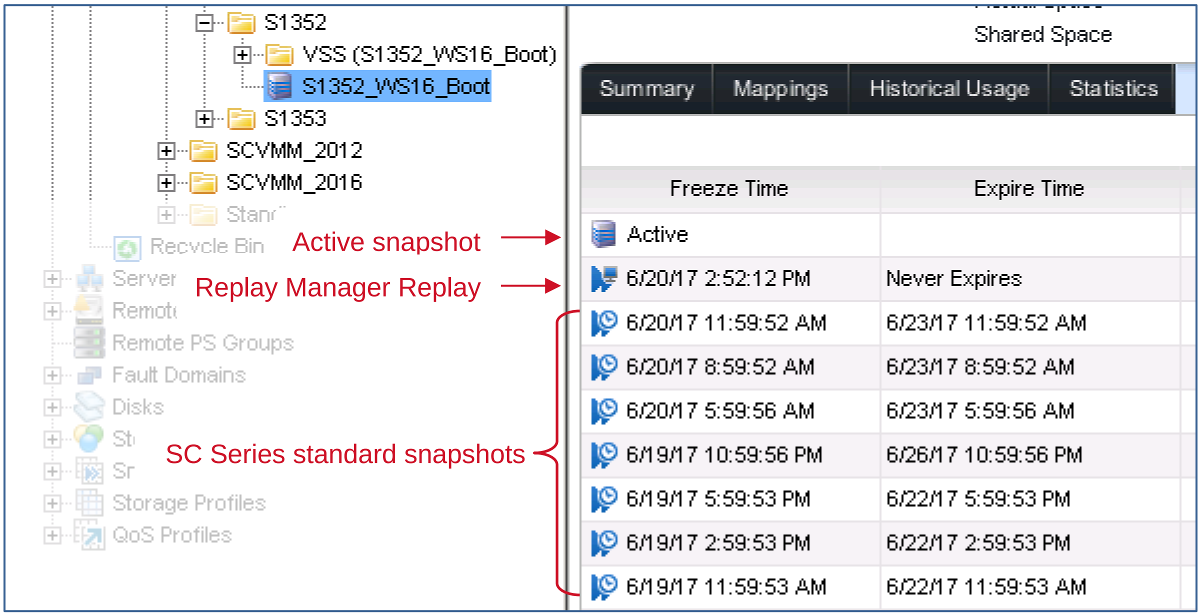
- VSS may have difficulty pausing the I/O on an extremely active boot drive so these backups may fail. This is to be expected for Hyper-V hosts or nodes under heavy I/O load.
- Apply at least one SC Series snapshot profile (see option 1) to provide a means of crash-consistent recovery should the Replay Manager local volumes backup fail due to high I/O.



Drive / Mount Point	Label
S1352	10.0.14393.0
□ C:\ClusterStorage\CSV01\	CSV01
□ C:\ClusterStorage\CSV02\	CSV02
☑ C:\	WS16_VL_Boot

Component	Serial Number	Label	Product ID
C:\		WS16_...	
COMPELNT Compellent Vol	0001034f-0000...		Compellent Vol

Figure 5 Local Volumes backup for a boot-from-SAN disk



Active snapshot

Replay Manager Replay

SC Series standard snapshots

Freeze Time	Expire Time
Active	
6/20/17 2:52:12 PM	Never Expires
6/20/17 11:59:52 AM	6/23/17 11:59:52 AM
6/20/17 8:59:52 AM	6/23/17 8:59:52 AM
6/20/17 5:59:56 AM	6/23/17 5:59:56 AM
6/19/17 10:59:56 PM	6/26/17 10:59:56 PM
6/19/17 5:59:53 PM	6/22/17 5:59:53 PM
6/19/17 2:59:53 PM	6/22/17 2:59:53 PM
6/19/17 11:59:53 AM	6/22/17 11:59:53 AM

Figure 6 SC Series supports snapshots and Replays of the same volume concurrently

3.1.2 Quorum disk

Option 1: Protect with SC Series snapshots (recommended).

Option 2: Protect with a Replay Manager Local Volumes backup. Option 2 is not recommended because the Hyper-V node that owns the quorum disk can change (this is per Microsoft design). If quorum disk node ownership changes, the Replay Manager backup job will fail.

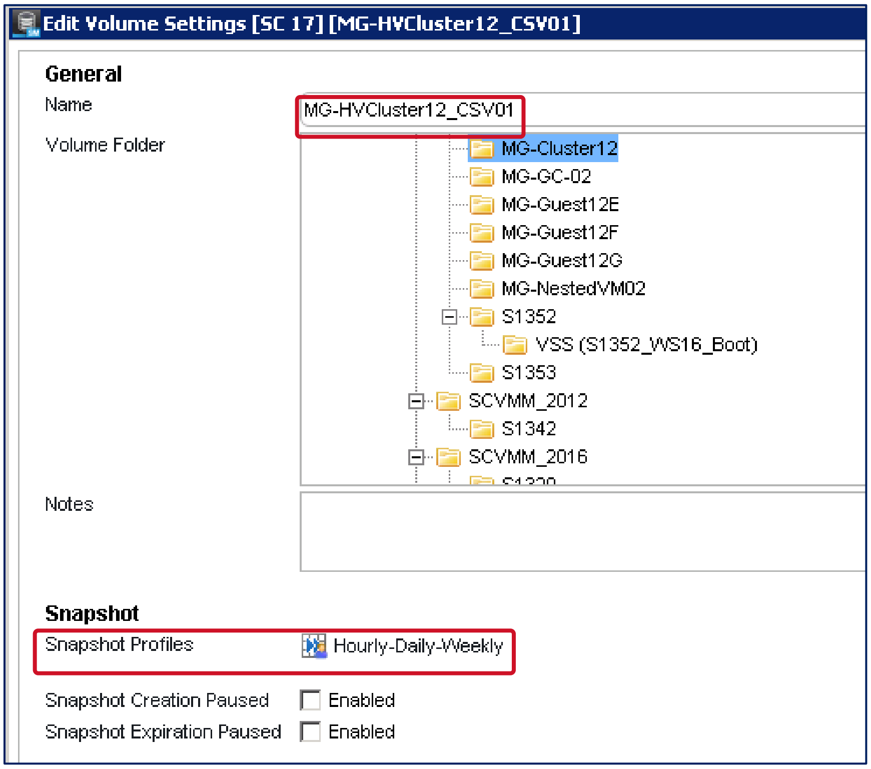
3.1.3 Cluster shared volumes and guest VMs

As shown in Table 1, there are three ways to protect a CSV hosting one or more guest VMs that are configured to use virtual hard disks.

Option 1: As noted previously, it is a best practice with any SAN volume to apply at least one SC Series snapshot profile to provide a secondary (crash-consistent) method of recovery in addition to Replay Manager. This ensures that at least one unexpired snapshot is associated with a SAN volume so that data migration and data reduction policies (compression and deduplication, if enabled) will apply to that volume.

In Figure 7, a custom hourly-daily-weekly snapshot profile is applied to each CSV.

Note: Leverage consistency groups if any guest VMs span more than one CSV.



Edit Volume Settings [SC 17] [MG-HVCluster12_CSV01]

General

Name: MG-HVCluster12_CSV01

Volume Folder: MG-Cluster12

Notes

Snapshot

Snapshot Profiles: Hourly-Daily-Weekly

Snapshot Creation Paused □ Enabled

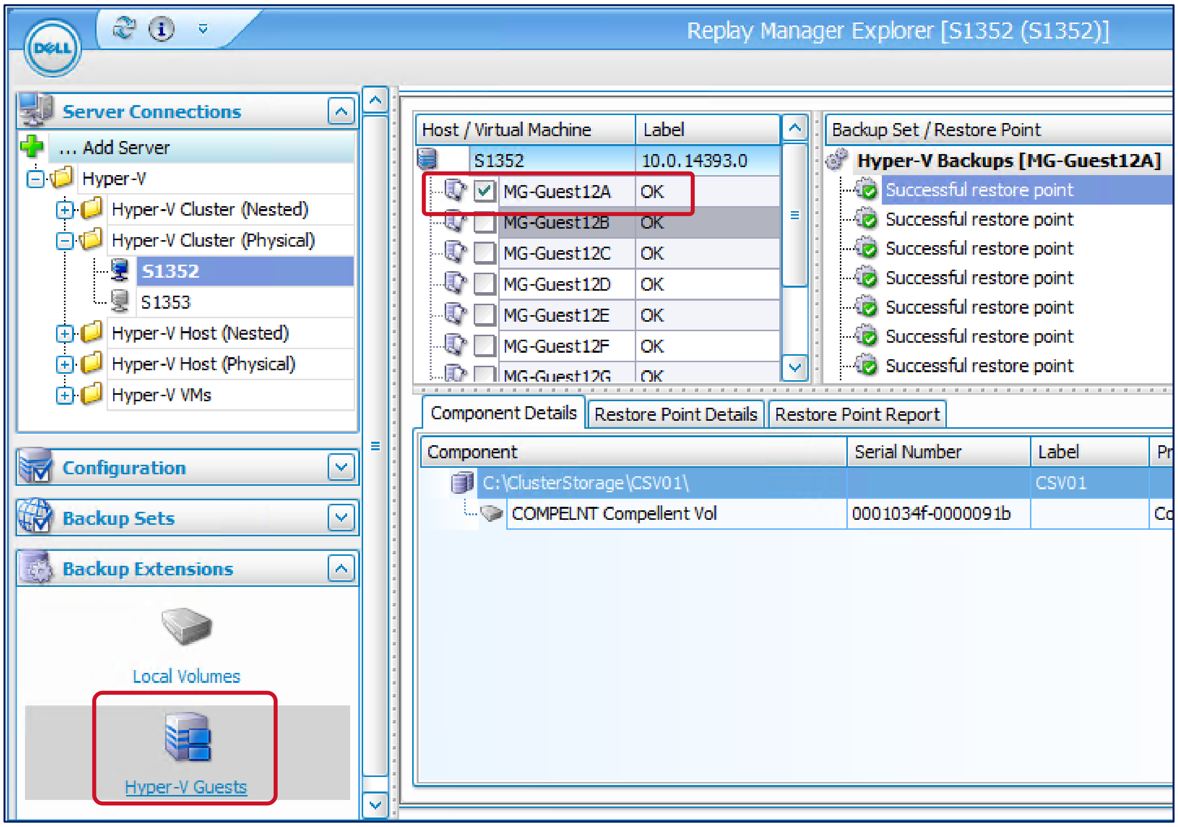
Snapshot Expiration Paused □ Enabled

Figure 7 Dell EMC SC Series snapshot profile applied to a CSV

Option 2: Use the **Hyper-V Guests** backup extension (recommended) to create Replay Manager backup sets to protect a specific guest VM or a group of VMs that are configured to use virtual hard disks. This method allows for recovery of individual guest VMs to an application-consistent state in cases where a CSV may host more than one guest VM. VSS ensures that in-flight I/O is flushed to disk and that I/O is paused before restore points are created. Each restore point will consist of Replay Manager Replays (snapshots) of the underlying CSVs used by the protected guest VM or VMs.

Note: The Hyper-V Guests backup extension protects data that resides on virtual hard disks only. Data on shared virtual hard disks, direct-attached disks, or pass-through disks is not included in the backup. For more information on protecting data on shared virtual hard disks with Replay Manager, see option 3 in this section. For more information on protecting data on direct-attached or pass-through disks, see section 3.1.4.

In Figure 8, **MG-Guest12A** is protected with a backup set that uses the **Hyper-V Guests** backup extension. The job is configured to run daily, with a retention policy that keeps the three most recent restore points.



Host / Virtual Machine	Label
S1352	10.0.14393.0
☑ MG-Guest12A	OK
□ MG-Guest12B	OK
□ MG-Guest12C	OK
□ MG-Guest12D	OK
□ MG-Guest12E	OK
□ MG-Guest12F	OK
□ MG-Guest12G	OK

Backup Set / Restore Point
Hyper-V Backups [MG-Guest12A]
Successful restore point
Successful restore point
Successful restore point
Successful restore point
Successful restore point
Successful restore point
Successful restore point

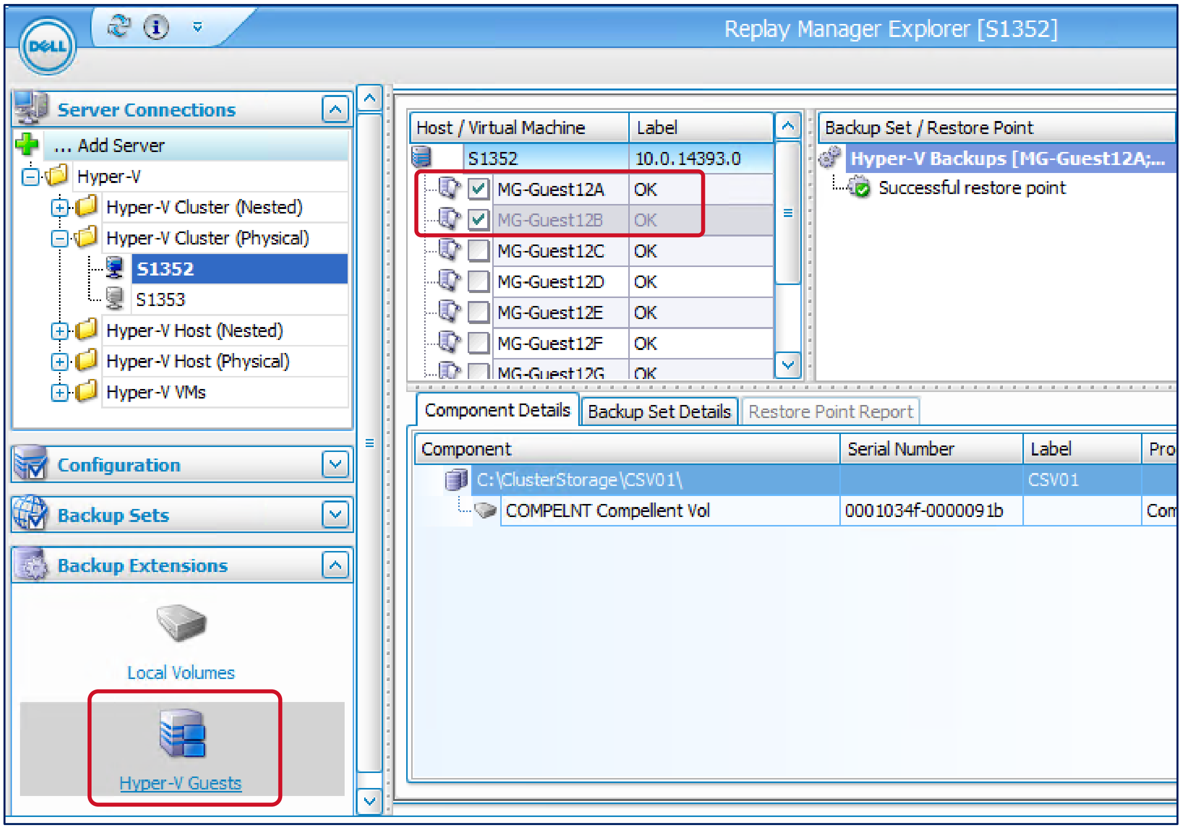
Component	Serial Number	Label	Pr
C:\ClusterStorage\CSV01\		CSV01	
COMPELNT Compellent Vol	0001034f-0000091b		Co

Figure 8 Use the Hyper-V Guests backup extension to protect individual guest VMs

If desired, multiple VMs shown in this example could be included in the same backup set. If more than one guest VM is included in a backup set, they can be restored individually, or as a group.

If a guest VM spans more than one CSV, then Replays are taken of each CSV as part of creating the restore point. For example, if the boot virtual hard disk and configuration files for a guest VM reside on CSV1, and a data virtual hard disk for the same guest VM resides on CSV2, then when a backup runs in Replay Manager for this guest VM, Replays for both CSV1 and CSV2 will be included in the restore point.

If more than one guest VM is included in a backup set, the VMs must be owned by a common node in the cluster. If one guest VM moves to another node, move the other guest VMs also so they stay grouped together on a common node. If the guest VMs get separated to dissimilar nodes, Replay Manager backup jobs will fail to complete successfully.



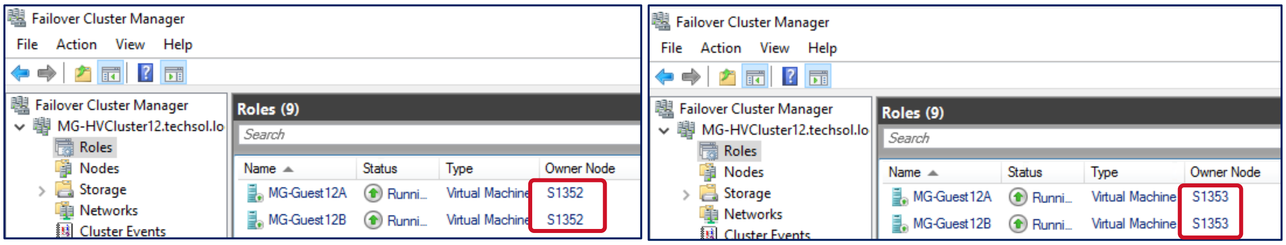
Host / Virtual Machine	Label
S1352	10.0.14393.0
☑ MG-Guest12A	OK
☑ MG-Guest12B	OK
□ MG-Guest12C	OK
□ MG-Guest12D	OK
□ MG-Guest12E	OK
□ MG-Guest12F	OK
□ MG-Guest12G	OK

Backup Set / Restore Point
Hyper-V Backups [MG-Guest12A;...
Successful restore point

Component	Serial Number	Label	Pro
C:\ClusterStorage\CSV01\		CSV01	
COMPELNT Compellent Vol	0001034f-0000091b		Com

Figure 9	Use the Hyper-V Guests backup extension to protect a group of guest VMs

In Figure 10, the two protected guests can be owned by either node of this two-node cluster and the Replay Manager job will complete successfully.

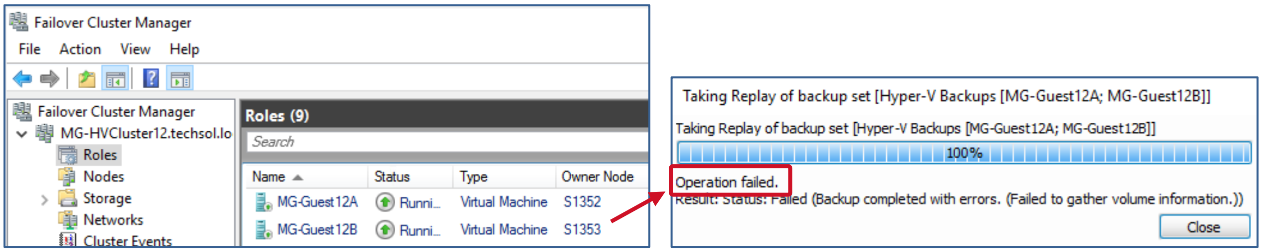


Name	Status	Type	Owner Node
MG-Guest12A	Runni...	Virtual Machine	S1352
MG-Guest12B	Runni...	Virtual Machine	S1352

Name	Status	Type	Owner Node
MG-Guest12A	Runni...	Virtual Machine	S1353
MG-Guest12B	Runni...	Virtual Machine	S1353

Figure 10	Guest VMs grouped on a common Hyper-V node

If the guest VMs become separated to dissimilar nodes as shown in in Figure 11, the Replay Manager job will fail.



Name	Status	Type	Owner Node
MG-Guest12A	Runni...	Virtual Machine	S1352
MG-Guest12B	Runni...	Virtual Machine	S1353

Taking Replay of backup set [Hyper-V Backups [MG-Guest12A; MG-Guest12B]]

Taking Replay of backup set [Hyper-V Backups [MG-Guest12A; MG-Guest12B]]

100%

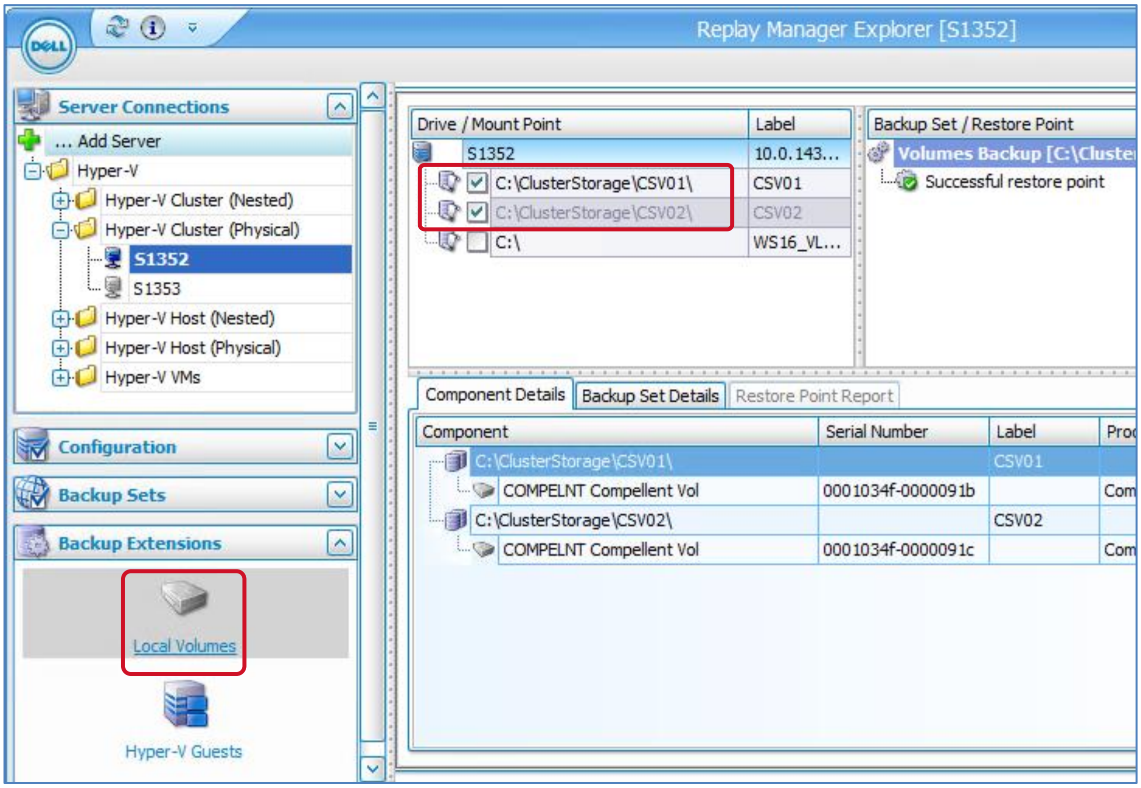
Operation failed.

Result: Status: Failed (Backup completed with errors. (Failed to gather volume information.))

Figure 11 Separated guest VMs result in a backup failure if they are part of the same backup set

Option 3: Use of the Replay Manager **Local Volumes** backup extension to protect CSVs, while possible, is usually not necessary or recommended, unless the CSV is hosting shared virtual hard disks. In Hyper-V environments, this backup option is intended primarily for cases where the Replay Manager agent is installed directly on a guest VM that has data on direct-attached iSCSI or pass-through disks as local disks. See section 3.1.4 for more information on protecting guest VMs with direct-attached or pass-through disks.

CSVs usually contain more than one guest VM. Recovery of a CSV that is protected by a Local Volumes backup does not allow any granularity to recover a specific guest VM (although this could be done manually by using Replay Manager Expose).



Drive / Mount Point	Label
S1352	10.0.143...
☑ C:\ClusterStorage\CSV01\	CSV01
☑ C:\ClusterStorage\CSV02\	CSV02
□ C:\	WS16_VL...

Component	Serial Number	Label	Pro
C:\ClusterStorage\CSV01\		CSV01	
COMPELNT Compellent Vol	0001034f-0000091b		Com
C:\ClusterStorage\CSV02\		CSV02	
COMPELNT Compellent Vol	0001034f-0000091c		Com

Figure 12 Use Local Volumes option to protect CSVs with Replay Manager

The preferred method to protect a CSV is to use the **Hyper-V Guests** backup extension to back up individual guest VMs or a group of VMs. The CSV should also have an SC Series snapshot profile assigned as an additional (although crash-consistent) means of recovery. This also helps to ensure the existence of at least one unexpired snapshot so that that the CSV is eligible for daily Data Progression and data reduction operations.

If a guest VM spans more than one CSV, a **Local Volumes** backup of a CSV may result in an incomplete backup of the guest VM. For example, if the boot virtual hard disk for a guest VM resides on CSV1, and a data virtual hard disk for the same guest VM resides on CSV2, then a **Local Volumes** backup of just CSV1 would not capture the data on CSV2. Use of the **Hyper-V Guests** backup extension ensures that all the guest VM resources are included in the restore point even if those resources span several CSVs.

3.1.4 Guest VMs with direct-attached iSCSI, virtual Fibre Channel, or pass-through disks

As a Hyper-V best practice, guest VMs are configured to use virtual hard disks that reside on cluster shared volumes. However, there are some use cases where pass-through (not recommended), direct-attached iSCSI (preferred), or direct-attached virtual Fibre Channel (not officially supported) disks are required in order for Replay Manager to obtain granular backups.

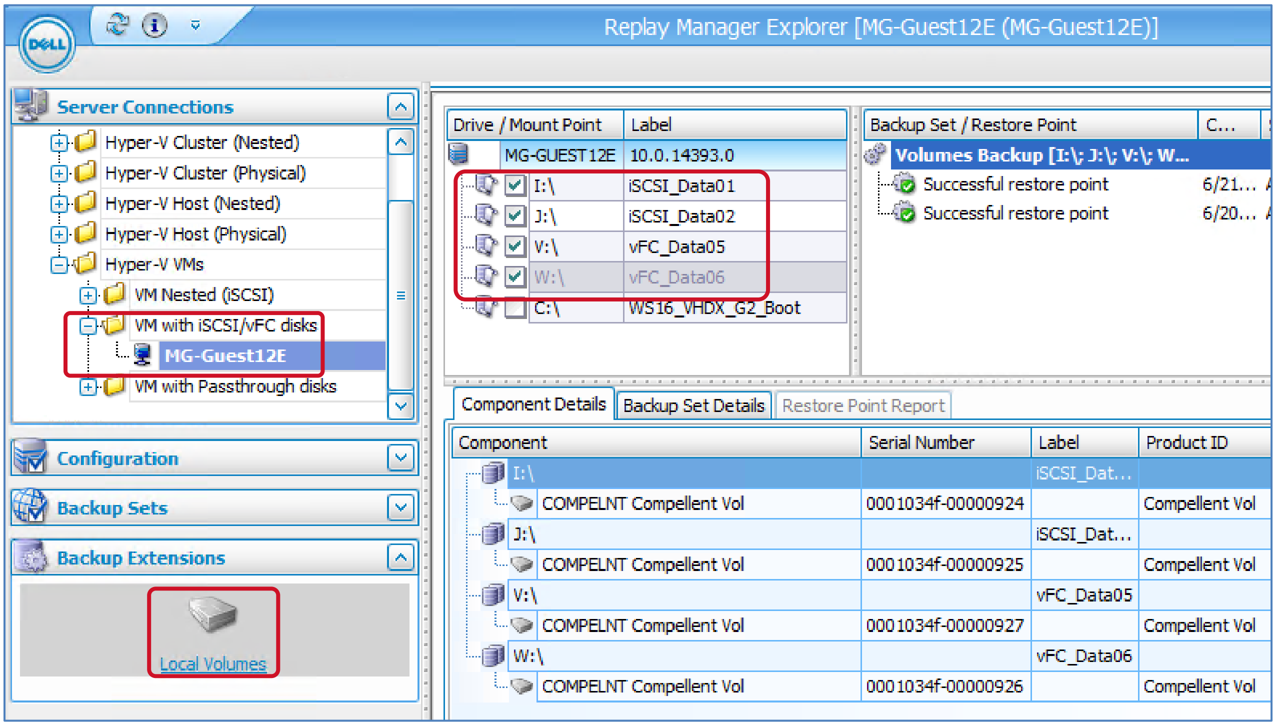
Note: Use of pass-through disks is not recommended by Dell EMC or Microsoft. Use of in-guest iSCSI disks is recommended if direct-attached storage is required.

Note: Replay Manager 7.8 does not officially support protecting virtual Fibre Channel (vFC) disks. vFC was introduced with Windows Server 2012 Hyper-V and requires SCOS 6.3.1 or newer. vFC is supported by Windows Server 2008 R2 or newer guest VMs, assuming the latest guest VM integration services (virtual drivers provided by Microsoft) are applied to the VM. Protecting vFC volumes with Replay Manager should be limited to non-production use cases.

Note: Use of vFC is discouraged because of the complicated setup. Problems can be difficult to troubleshoot, and guest VM clusters that use vFC do not support cluster server objects with SC Series storage.

The need for direct-attached or pass-through storage applies specifically to protecting guest VMs workloads such as Microsoft SQL Server or Microsoft Exchange. In order for Replay Manager to perform granular backup and recovery of SQL Server or Microsoft Exchange database components, the following requirements must be met:

- SQL and Exchange data must reside on a physical volume that is a pass-through (not recommended) or direct-attached iSCSI disk (recommended). vFC is not officially supported with Replay Manager 7.8 and should not be used to protect vFC volumes in production.
- The Replay Manager server agent must be installed directly on the guest VM so that it can be managed from the Replay Manager Explorer GUI as shown in Figure 13.
- If a guest VM is configured to use a pass-through disk, the guest VM must also be configured to support iSCSI. Replay Manager requires iSCSI in order to map SC Series recovery volumes directly to a guest VM to do granular (individual databases) restores of Microsoft SQL Server or Exchange Server.

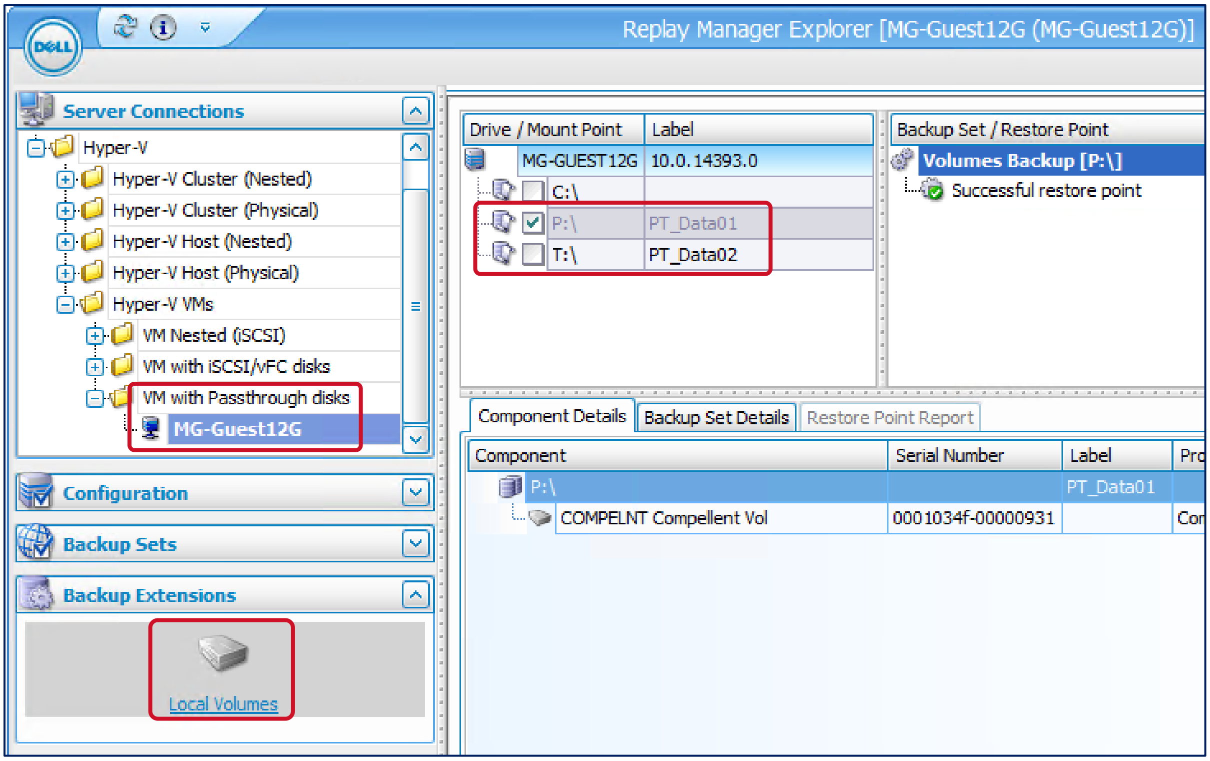


Drive / Mount Point	Label
MG-GUEST12E	10.0.14393.0
☑ I:\	iSCSI_Data01
☑ J:\	iSCSI_Data02
☑ V:\	vFC_Data05
☑ W:\	vFC_Data06
□ C:\	WS16_VHDX_G2_Boot

Backup Set / Restore Point	C...
Volumes Backup [I:\; J:\; V:\; W...	
Successful restore point	6/21...
Successful restore point	6/20...

Component	Serial Number	Label	Product ID
I:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000924		Compellent Vol
J:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000925		Compellent Vol
V:\		vFC_Data05	
COMPELNT Compellent Vol	0001034f-00000927		Compellent Vol
W:\		vFC_Data06	
COMPELNT Compellent Vol	0001034f-00000926		Compellent Vol

Figure 13 Guest VM with direct-attached iSCSI and virtual Fibre Channel disks protected with Replay Manager using the Local Volumes backup extension

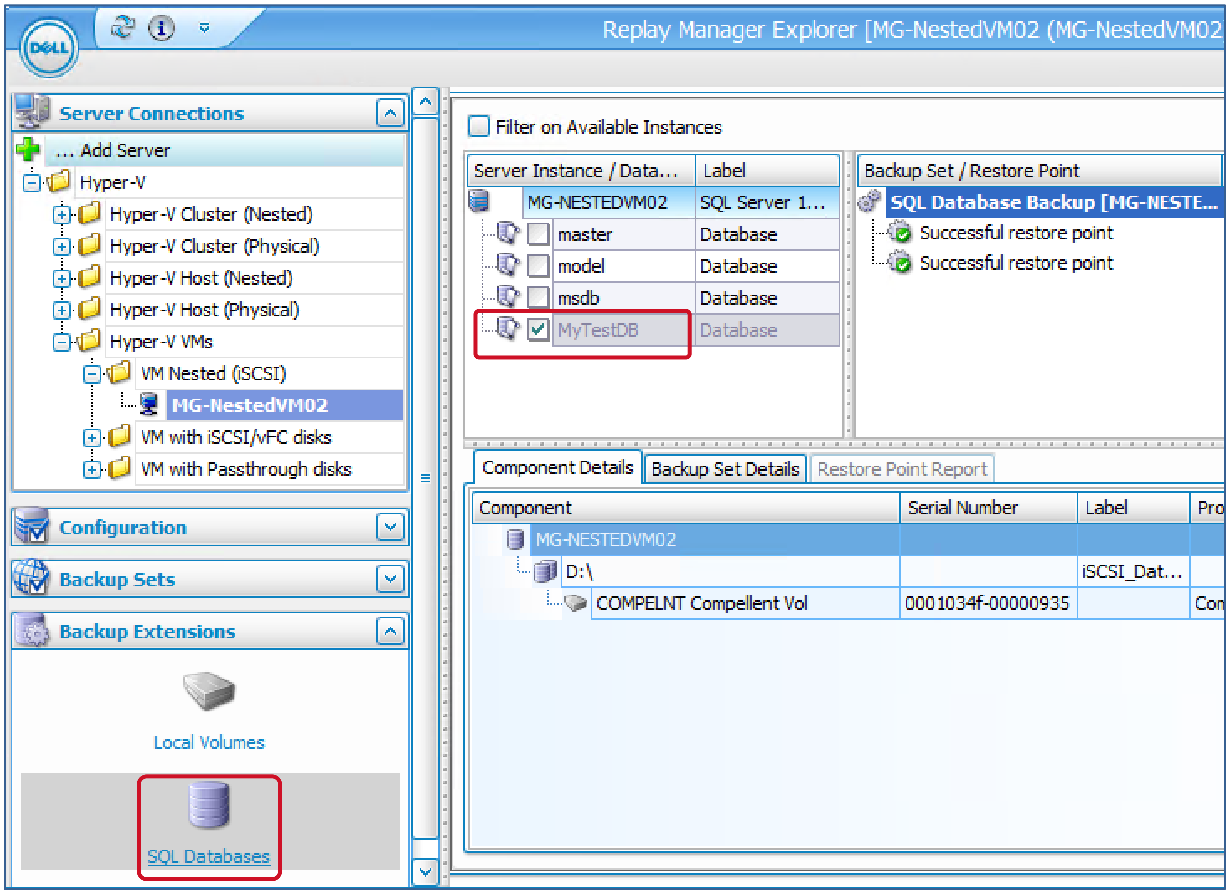


Drive / Mount Point	Label
MG-GUEST12G	10.0.14393.0
□ C:\	
☑ P:\	PT_Data01
□ T:\	PT_Data02

Backup Set / Restore Point
Volumes Backup [P:\]
Successful restore point

Component	Serial Number	Label	Pro
P:\		PT_Data01	
COMPELNT Compellent Vol	0001034f-00000931		Co

Figure 14 Guest VM with pass-through disks protected with Replay Manager using the Local Volumes backup extension



□ Filter on Available Instances

Server Instance / Data...	Label
MG-NESTEDVM02	SQL Server 1...
□ master	Database
□ model	Database
□ msdb	Database
☑ MyTestDB	Database

Backup Set / Restore Point
- SQL Database Backup [MG-NESTE...
  - Successful restore point
  - Successful restore point

Component	Serial Number	Label	Pro
MG-NESTEDVM02			
D:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000935		Con

Figure 15 SQL Databases backup extension used for granular protection of databases on direct-attached disks (on a nested guest VM in this example)

If granular backups and restores of SQL or Exchange are not needed, use virtual hard disks and protect the guest VM with the **Hyper-V Guests** backup extension. This will back up the entire guest VM to an application-consistent state, but will not allow individual SQL or Exchange database objects to be backed up or restored in Replay Manager.

Note: If the **Local Volumes** backup extension is used to back up SQL or Exchange data, then individual SQL or Exchange objects may still be recovered manually after performing a Replay Manager Expose operation. In this case, granular recovery of SQL or Exchange data may require additional steps and tools provided by the customer.

For more information on protecting SQL Server and Microsoft Exchange with Replay Manager, see the *Replay Manager Administrator's Guide* and the resources listed in appendix A.

3.1.5 Protect guest VMs with multiple drive types

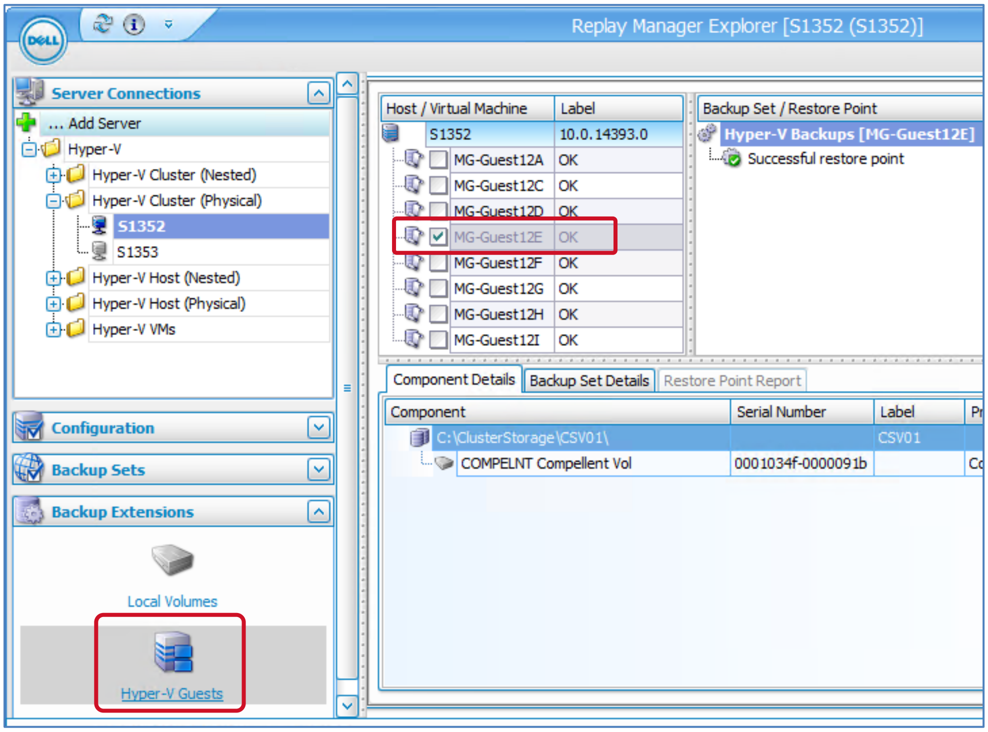
Where possible, it is a best practice to keep the design as simple as possible and configure a guest VM to use virtual hard disks only. This allows a single Replay Manager backup job (with the **Hyper-V Guests** backup extension) to protect the entire guest VM.

If a guest VM is configured to use other types of drives besides virtual hard disks, additional Replay Manager backup sets may be required for the same guest VM in order to protect all the guest VM data.

In the following example, the guest VM named **MG-Guest12E** can be configured to use one, several, or all of the backup sets (as required) to protect the guest VM data. Mix and match different backup sets for the same guest VM if necessary in order to protect the desired data. If more than one backup set is created for the guest VM or group of VMs, it may be necessary to stagger the job start times to avoid VSS conflicts.

Note: These options assume that a basic SC Series snapshot profile is already applied to each SAN volume to ensure there is always at least one unexpired snapshot per volume so Data Progression and data reduction operations include that volume. This also ensures there is a secondary means of recovery (crash-consistent) in case recovery from Replay Manager is not possible.

Option 1: Use the **Hyper-V Guests** backup extension on the Hyper-V host to protect a guest VM configuration along with its virtual hard disks (see Figure 16). This type of backup set ignores guest VM data that is in pass-through disks, direct-attached disks, or shared virtual hard disks.



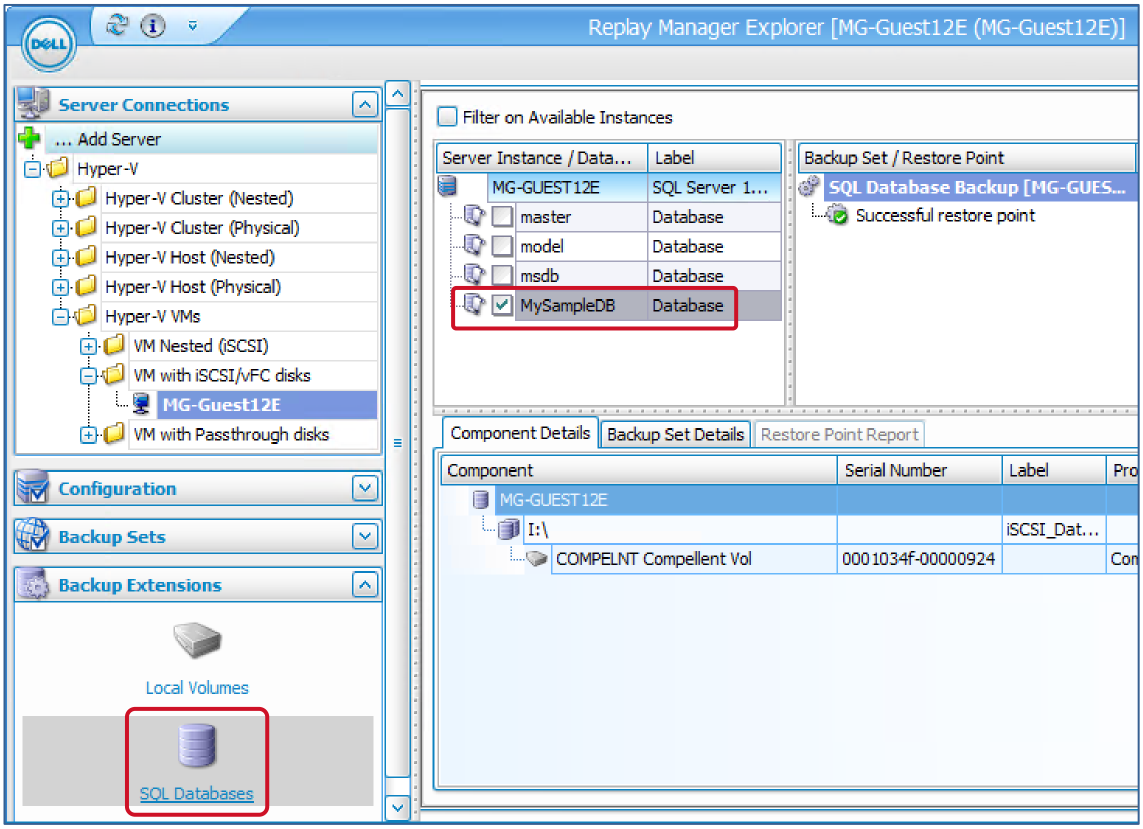
Host / Virtual Machine	Label
S1352	10.0.14393.0
☐ MG-Guest12A	OK
☐ MG-Guest12C	OK
☐ MG-Guest12D	OK
☑ MG-Guest12E	OK
☐ MG-Guest12F	OK
☐ MG-Guest12G	OK
☐ MG-Guest12H	OK
☐ MG-Guest12I	OK

Backup Set / Restore Point
Hyper-V Backups [MG-Guest12E]
Successful restore point

Component	Serial Number	Label	Pr
C:\ClusterStorage\CSV01\		CSV01	
COMPELNT Compellent Vol	0001034f-0000091b		Co

Figure 16 Protect guest VM virtual hard disks with the Hyper-V Guests backup extension

Option 2: Use the **SQL Databases** or **Exchange** backup extension when the Replay Manager server agent is installed directly on the guest VM (see Figure 17). This provides for granular protection of specific database components. In this example, the guest VM is running Microsoft SQL.



☐ Filter on Available Instances

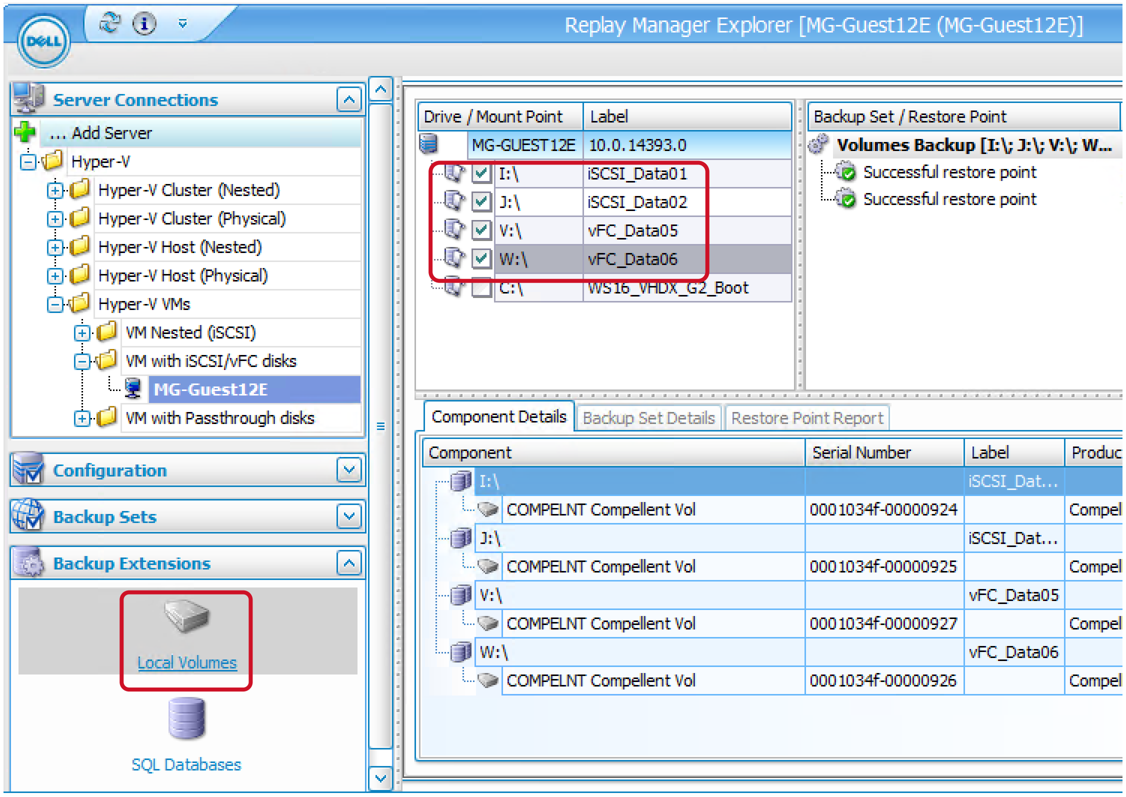
Server Instance / Data...	Label
MG-GUEST12E	SQL Server 1...
☐ master	Database
☐ model	Database
☐ msdb	Database
☑ MySampleDB	Database

Backup Set / Restore Point
SQL Database Backup [MG-GUES...
Successful restore point

Component	Serial Number	Label	Pro
MG-GUEST12E			
I:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000924		Con

Figure 17 Protect SQL Server data with the SQL Databases backup extension

Option 3: Use the **Local Volumes** backup extension on the guest VM (with the Replay Manager server agent installed on the guest VM) to protect direct-attached or pass-through disks (see Figure 18). This method does not provide for granular backup or recovery of SQL or Exchange databases. As a suggestion, use intuitive volume naming so that the **Label** column in Replay Manager indicates the type of disk. With this type of backup set, do not include drives that are virtual hard disks (the **C:\** drive in this example) because this will cause the job to fail.



Drive / Mount Point	Label
MG-GUEST12E	10.0.14393.0
☑ I:\	iSCSI_Data01
☑ J:\	iSCSI_Data02
☑ V:\	vFC_Data05
☑ W:\	vFC_Data06
□ C:\	WS16_VHDX_G2_Boot

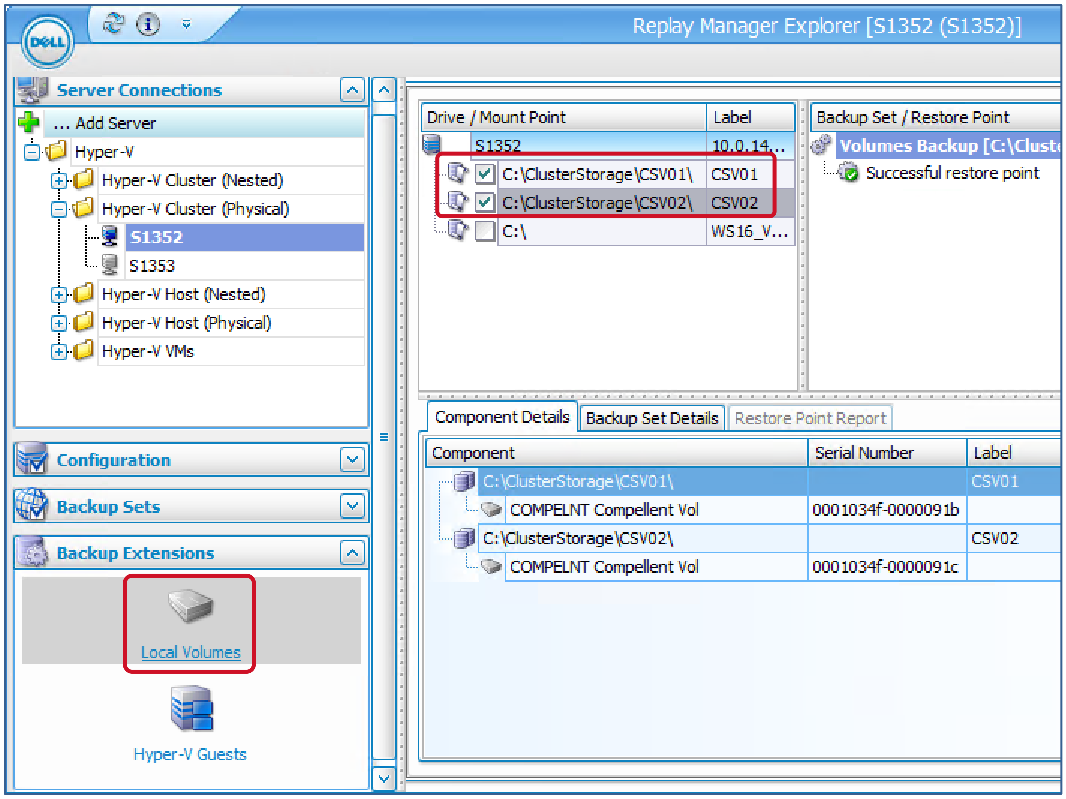
Backup Set / Restore Point

- **Volumes Backup [I:\; J:\; V:\; W...**
  - Successful restore point
  - Successful restore point

Component	Serial Number	Label	Produc
I:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000924		Compel
J:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000925		Compel
V:\		vFC_Data05	
COMPELNT Compellent Vol	0001034f-00000927		Compel
W:\		vFC_Data06	
COMPELNT Compellent Vol	0001034f-00000926		Compel

Figure 18 Protect direct-attached disks with Local Volumes backup extension on the guest VM

Option 4: Use the **Local Volumes** backup extension with the Replay Manager server agent installed on the Hyper-V host to protect CSVs (see Figure 19). Use intuitive volume names to make it easier to select the right volumes when creating backup sets. This is currently the only means with Replay Manager to protect data in shared virtual hard disks that reside on a CSV. If the shared virtual hard disk contains transactional data, and application consistency is essential when obtaining a snapshot or Replay, then take steps to do so (outside of Replay Manager) on the guest VM cluster. For example, temporarily pause or stop the application or service that generates transactional I/O.



Drive / Mount Point	Label
S1352	10.0.14...
☑ C:\ClusterStorage\CSV01\	CSV01
☑ C:\ClusterStorage\CSV02\	CSV02
□ C:\	WS16_V...

Backup Set / Restore Point
Volumes Backup [C:\Clust
Successful restore point

Component	Serial Number	Label
C:\ClusterStorage\CSV01\		CSV01
COMPELNT Compellent Vol	0001034f-0000091b	
C:\ClusterStorage\CSV02\		CSV02
COMPELNT Compellent Vol	0001034f-0000091c	

Figure 19 Protect shared virtual hard disks on CSVs with the Local Volumes backup extension on the Hyper-V host

3.2 Achieve application consistency with SC Series snapshots

Where possible, use Replay Manager to ensure that Hyper-V workloads (guest VMs) are put into an application-consistent state when backed up. Where this is not possible, there are alternative ways to achieve application consistency with standard SC Series snapshots. Although these methods may not always be practical in a production environment, two common methods include:

- Temporarily power off the host or guest VM to halt I/O. This is a common strategy when a snapshot of a server is obtained that will serve as a gold image for provisioning new servers.
- Temporarily stop key applications or services that generate transactional data before taking a snapshot. This is a common strategy with backup processes that run after hours. When possible, the process can be automated with tools such as PowerShell so the job can run unattended.

Note: If a database spans more than one volume, create a consistent snapshot profile to snap two or more volumes at the same time to create a consistency group.

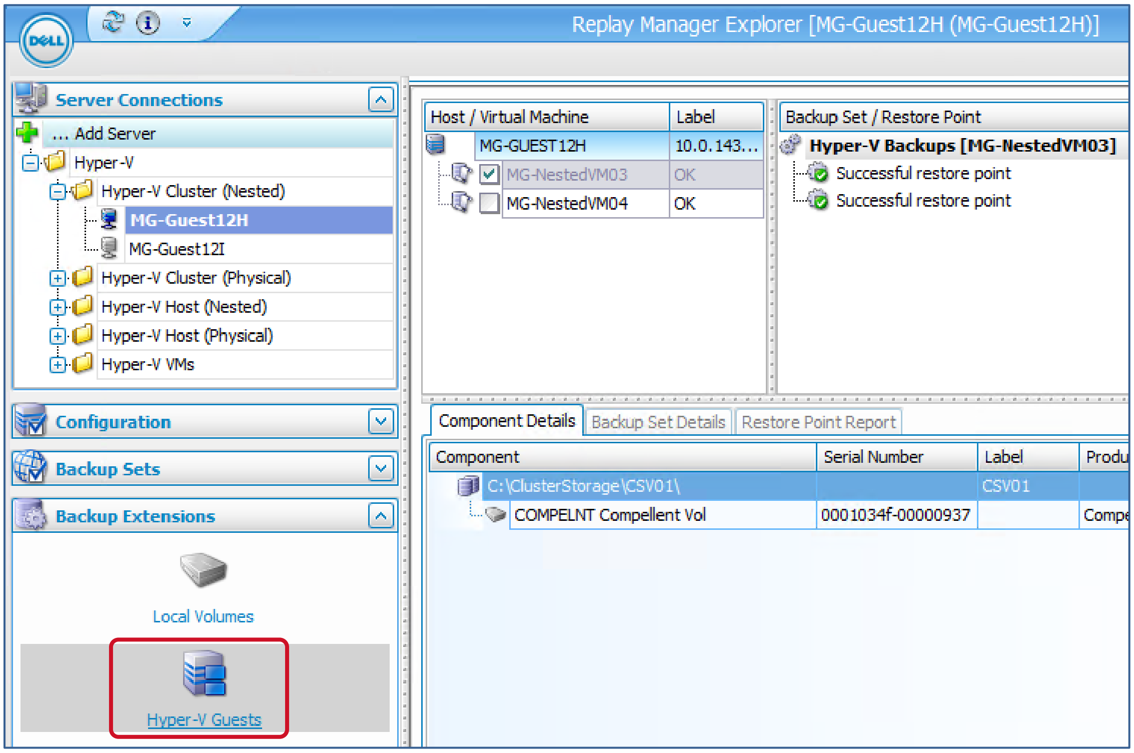
3.2.1 Protect nested Hyper-V resources with Replay Manager

With the release of Windows Server 2016, the Hyper-V role can now be installed on guest VMs to create nested Hyper-V hosts, nested Hyper-V clusters, and nested guest VMs. With nesting, administrators now have more options for creating tailored virtualized environments with less physical hardware.

Note: As of the date of this paper, Microsoft does not recommend running production workloads on nested Hyper-V hosts, clusters, or guest VMs. Microsoft may provide future support for production workloads on nested resources as the technology matures.

Replay Manager can be used to protect workloads on nested Hyper-V hosts, clusters, or guest VMs as long as the data being protected resides on direct-attached iSCSI disks. Simply install the Replay Manager server agent on nested Hyper-V hosts, cluster nodes, or guest VMs.

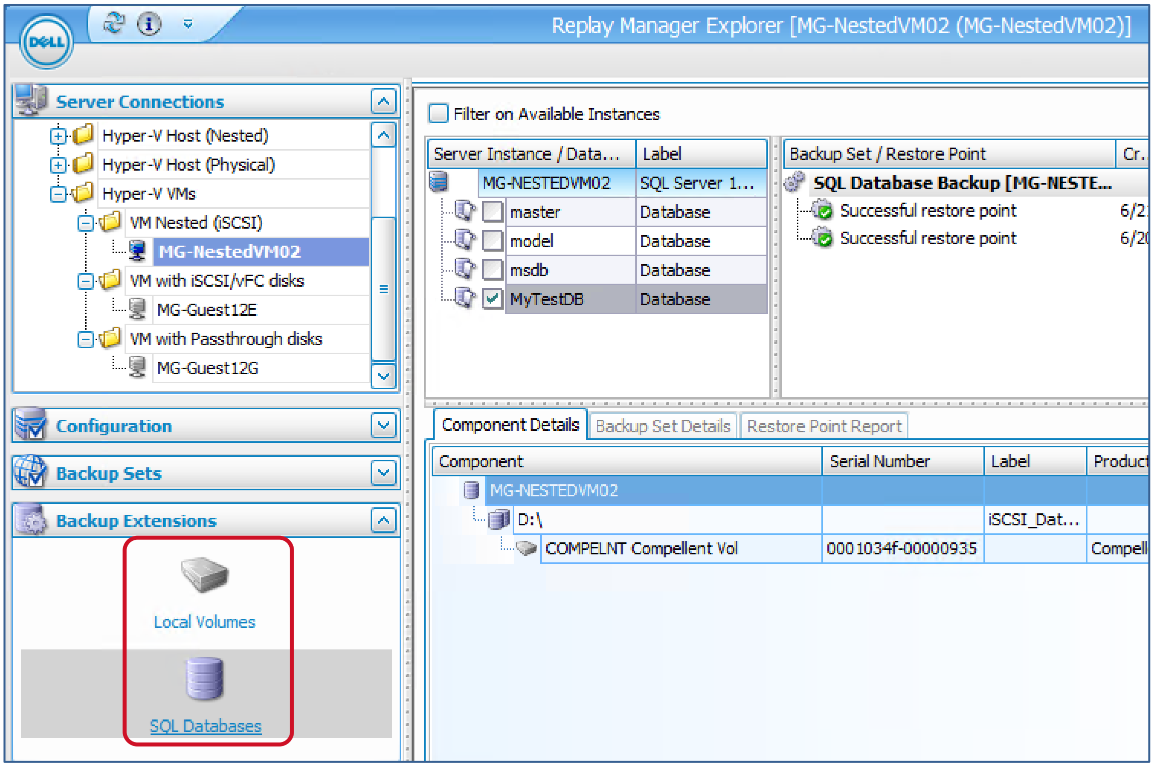
As a suggestion, create folders and subfolders in Replay Manager Explorer to logically group similar Hyper-V resources to make navigation easier.



Host / Virtual Machine	Label
MG-GUEST12H	10.0.143...
☑ MG-NestedVM03	OK
□ MG-NestedVM04	OK

Component	Serial Number	Label	Produ
C:\ClusterStorage\CSV01\		CSV01	
COMPELNT Compellent Vol	0001034f-00000937		Compe

Figure 20 Use the Hyper-V Guests backup extension on a nested Hyper-V cluster to protect a nested guest VM



☐ Filter on Available Instances

Server Instance / Data...	Label
MG-NESTEDVM02	SQL Server 1...
☐ master	Database
☐ model	Database
☐ msdb	Database
☑ MyTestDB	Database

Backup Set / Restore Point	Cr.
SQL Database Backup [MG-NESTE...	
Successful restore point	6/2
Successful restore point	6/2

Component	Serial Number	Label	Product
MG-NESTEDVM02			
D:\		iSCSI_Dat...	
COMPELNT Compellent Vol	0001034f-00000935		Compell

Figure 21 Use the Local Volumes or SQL Databases extension on a nested guest VM with Microsoft SQL to protect SQL data

4 Back up guest VMs with Replay Manager

4.1 Determine backup schedule and retention policies

Many factors affect backup strategy:

- An organization’s overall backup policy
- The nature and sensitivity of the data
- The rate of change of the data (which determines how much additional SAN space is needed for restore points and Replays)
- Applicable industry-specific regulations
- The recovery point objective (RPO), which is the acceptable amount of data loss
- The recovery time objective (RTO), which is maximum time a system can be offline

In many cases, a daily backup of a guest VM performed during off-peak hours will provide an acceptable RPO. However, for mission-critical servers, a tighter RPO might require a more frequent backup schedule. Determining how long to keep restore points generated by a Replay Manager backup is also a function of the same factors listed previously.

The best backup strategy will typically achieve a good balance between media demand (overhead for SAN space in this example), replication bandwidth (if the data is being replicated to another SC Series array), and appropriate frequency in order to satisfy RPO objectives.

Table 2 depicts an example backup strategy for a critical Hyper-V guest VM that has a four-hour RPO during the business day. Three Replay Manager backup sets are scheduled as shown. This results in a total retention of no more than 18 restore points for this guest VM after one month. This backup strategy provides a good balance that satisfies the four-hour RPO requirement in the near term, and purges old restore points for better SAN utilization in the long term.

Table 2 Example backup strategy for a Hyper-V guest VM

Job	Schedule	Retention	Restore points
Hourly	Every 4 hours between 6 a.m. and 7 p.m.	2 days	8 restore points (4 per day)
Daily	Monday–Saturday at 11:30 p.m.	1 week	6 restore points
Weekly	Sunday at 11:30 p.m.	4 weeks	4 restore points
Total			18 restore points

As a comparison, if just the hourly backup set was configured with a retention policy of 30 days, while it would fulfill the requirement to restore the guest VM back 30 days, it would also result in an unnecessary accumulation of restore points (120 instead of 18) which would consume SAN resources needlessly.

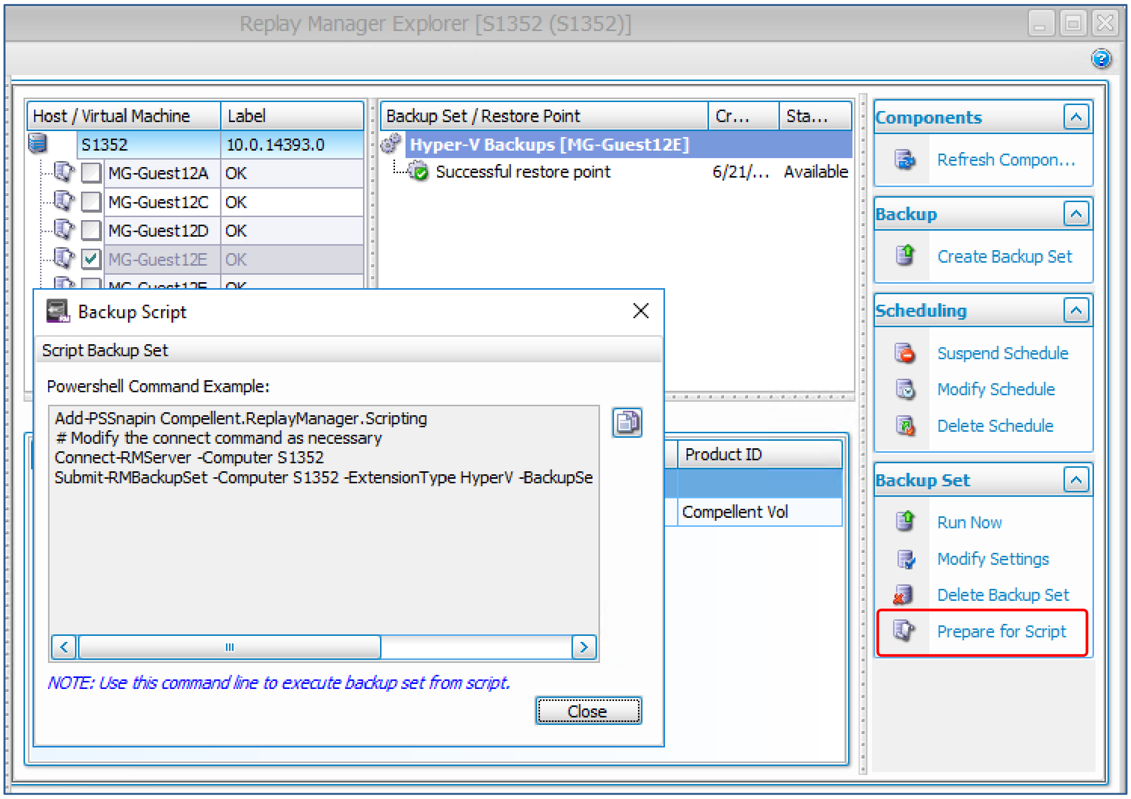
4.2 Create a Replay Manager backup set for a Hyper-V guest VM

Once the Replay Manager service is installed and configured on all Hyper-V host servers (standalone and clustered) — along with any guest VMs with direct-attached iSCSI or pass-through disks — and these servers have been added to Replay Manager Explorer, create backup sets to back up the guest VM data. The following steps demonstrate how to create and schedule a Replay Manager backup set for a Hyper-V guest VM using the **Hyper-V Guests** backup extension.

1. Launch Replay Manager Explorer.
2. In the navigation pane under **Server Connections**, click the Hyper-V host server or node containing the guest VM to be protected.
3. In the navigation pane under **Backup Extensions**, click **Hyper-V Guests**.
4. In the explorer pane under **Host/Virtual Machine**, a list of guest VMs display that are currently owned by this particular Hyper-V server. Select the desired guest VM(s) by selecting the box in front of each one.
5. In the action pane under **Backup**, click **Create Backup Set**.
6. In the **Create Backup Set** dialog box:
   a. Provide a name for the new backup set (or choose the default name).
   b. Set an expiration policy under **Options** (by number of days or number of restore points).
   c. Under **Backup Type**, select the desired action. Typically, **Scheduled for later** is selected.
   d. If **Scheduled for later** is selected, click **Modify**.
7. In the **Backup Schedule** dialog box:
   a. Change the **Schedule Type** to **Recurring**.
   b. Set the desired backup frequency, such as daily or weekly, along with the time of day.
   c. Enable **Retry after Failure** if desired (recommended).
   d. Click **OK** to return to the **Create Backup Set** dialog box.
8. Click **Submit**.
9. The new backup set will be listed in the explorer window. No restore points are associated with the new backup set because it is newly created.
10. The backup set will run and create a new restore point per the schedule. To create a restore point manually, click the backup set and then in the action pane under **Backup Set**, click **Run Now.**

Note: To avoid a job failure, use Replay Manager to connect to the Hyper-V server that currently owns the guest VM before running a backup set manually.

11. If desired, click **Prepare for Script** to display the PowerShell commands necessary to run the backup set outside of Replay Manager.



Host / Virtual Machine	Label
S1352	10.0.14393.0
□ MG-Guest12A	OK
□ MG-Guest12C	OK
□ MG-Guest12D	OK
☑ MG-Guest12E	OK
□ MG-Guest12F	OK

Backup Set / Restore Point	Cr…	Sta…
Hyper-V Backups [MG-Guest12E]		
Successful restore point	6/21/…	Available

Powershell Command Example:

```
Add-PSSnapin Compellent.ReplayManager.Scripting
# Modify the connect command as necessary
Connect-RMServer -Computer S1352
Submit-RMBackupSet -Computer S1352 -ExtensionType HyperV -BackupSe
```

NOTE: Use this command line to execute backup set from script.

Figure 22 The Prepare for Script option displays the matching PowerShell commands

Note: To make it easier to differentiate between clusters, cluster nodes, standalone Hyper-V hosts, and guest VMs, create folders in the Replay Manager navigation pane under **Server Connections** to logically group Hyper-V and guest VM servers.

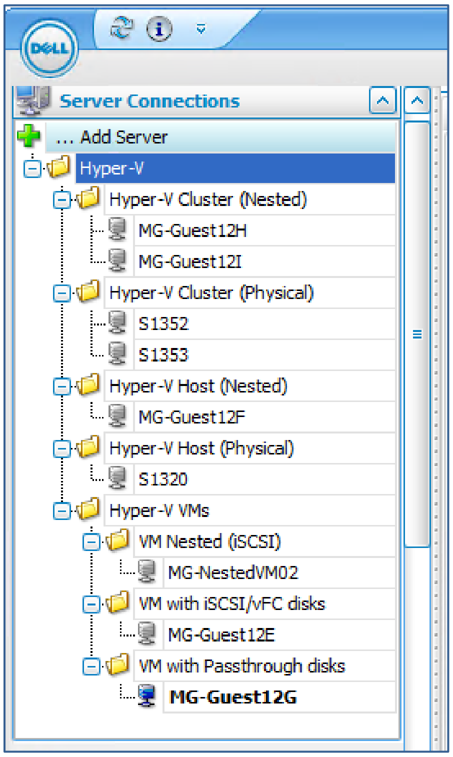


Figure 23 Create folders and subfolders in Replay Manager to organize servers and clusters

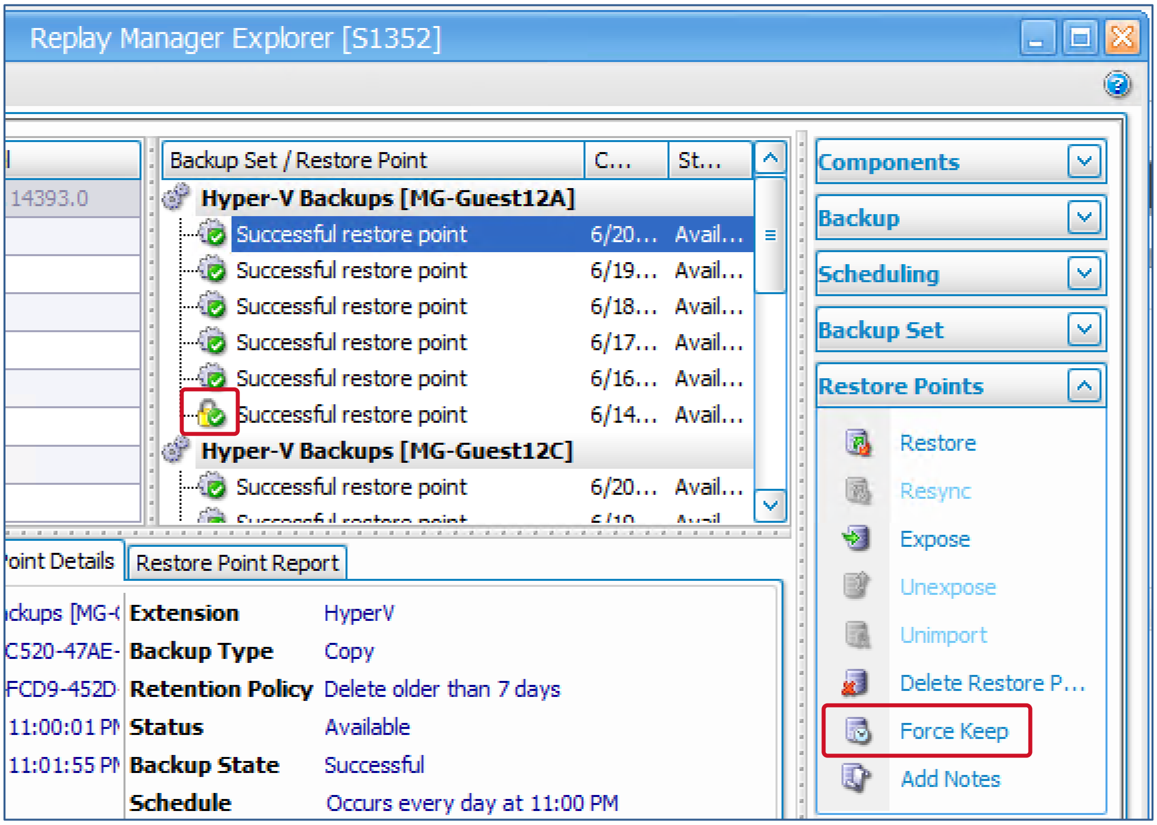
4.3 Manage Hyper-V guest VM restore points

Any scheduled Hyper-V guest VM backup set can be run manually outside of its scheduled window. To do so, select it and click **Run Now** under **Backup Set** in the action pane. Reasons to run a backup set manually include:

- Create an initial restore point to protect a new guest VM instead of waiting for the first scheduled occurrence of the backup set to run.
- Test a new backup set to make sure it works correctly.
- Obtain a restore point right before applying a patch or performing maintenance.

Note: Before clicking **Run Now**, make sure to connect to the Hyper-V host or node that currently owns the guest VM to avoid a job failure.

If choosing to retain a restore point indefinitely, click **Force Keep** to exclude it from retention policy settings. The restore point icon will change to a lock.



Backup Set / Restore Point	C...	St...
Hyper-V Backups [MG-Guest12A]		
Successful restore point	6/20...	Avail...
Successful restore point	6/19...	Avail...
Successful restore point	6/18...	Avail...
Successful restore point	6/17...	Avail...
Successful restore point	6/16...	Avail...
Successful restore point	6/14...	Avail...
Hyper-V Backups [MG-Guest12C]		
Successful restore point	6/20...	Avail...

Extension	HyperV
Backup Type	Copy
Retention Policy	Delete older than 7 days
Status	Available
Backup State	Successful
Schedule	Occurs every day at 11:00 PM

Figure 24 Use Force Keep to retain a restore point indefinitely

- It is a best practice to lock the most recent restore point before performing maintenance or upgrades. Keep it locked for a period of time to allow quick recovery to a known-good, application-consistent state if problems with the maintenance or upgrades are encountered.
- When **Force Keep** is no longer needed for a restore point, click **Allow Auto-deletion** in the action pane to remove the lock and allow it to be purged according to the retention policy.

When a restore point expires, the associated Replays and View Volumes on the SC Series array are also purged and the space is recovered and returned to the SAN to be used elsewhere.

Individual restore points can also be manually expired (deleted), either one at a time or as a group. Select the desired restore point and click **Delete Restore Point** in the action pane. This purges them immediately.

To delete an entire backup set and all associated restore points, select the backup set and click **Delete Backup Set** in the action pane.

5 Restore Hyper-V guest VM data

This section covers the recovery options available with Replay Manager 7 for Hyper-V guest VMs on a clustered or standalone Hyper-V host. These options include:

Restore an entire Hyper-V guest VM from a restore point created with the **Hyper-V Guests** backup extension.

Expose a restore point that contains the guest VM virtual hard disk(s) for manual recovery of the guest VM or a subset of data.

Transport a restore point that contains a guest VM to another Hyper-V host server for manual recovery of the guest VM, or a subset of data.

5.1 Restore a Hyper-V guest VM from a restore point

It may be necessary to restore an entire guest VM when a major event occurs, such as:

- Malware infection
- Guest VM operating system (or application) upgrade failure
- Significant data corruption or loss
- Other events that would result in significant down time for manual recovery
- Recover a guest VM used for training or testing to pristine state

Note: Before restoring a guest VM, temporarily suspend any backup sets that include the guest VM to avoid causing job failures.

Follow these steps to restore a Hyper-V guest VM from a restore point:

1. In the navigation pane under **Server Connections**, connect to the Hyper-V server that hosts the guest VM to be restored.
2. Under **Server Extensions**, click **Hyper-V Guests**. A list of Hyper-V guest VMs that are running on this Hyper-V host will display in the explorer pane.
3. Check the box in front of the guest VM to be restored. This acts as a filter so that only the applicable backup sets and restore points are displayed.
4. Click the desired restore point to select it.
5. In the action pane under **Restore Points**, click **Restore**.
6. In the **Restore Snapshot** dialog box, make sure only the desired guest VM is selected. Deselect all other guest VMs.
7. Click **Restore** to start the job.
8. A progress bar will display the status of the operation. Optionally, click **Hide** and click **Queued Items** under **Backup Sets** in the navigation pane to monitor the status of the restore operation as it runs in the background.
9. The restore process will cause a brief service outage for the Hyper-V guest VM if it is online. In the background, the restore operation does the following:

    a. The Hyper-V guest VM is temporarily powered down and removed from Hyper-V Manager, and (if part of a cluster) the guest VM is placed offline in Failover Cluster Manager.

b. Replay Manager maps the appropriate VSS View Volume to the physical Hyper-V host server as a read-only volume.
c. Replay Manager restores the guest VM from the View Volume (configuration and virtual hard disks).
d. If the Hyper-V guest VM was running previous to the restore, it is powered on and will be listed again in Hyper-V Manager, and (if part of a cluster) will return to online status in Failover Cluster Manager.

10. Once the restore is complete, the progress bar reports a status of **Restore completed successfully**. If the progress bar window was closed by clicking **Hide**, the status of the restore job can be verified by clicking **Reports** in the navigation pane and viewing the job results under the **Details** tab. Once the restore job has finished, the log should report **Completion status: success**.
11. Complete any steps required to verify the health of the guest VM after the restore.
12. If any backup set schedules were suspended prior to restoring the Hyper-V guest VM, click **Resume Schedule** to return them to active status again.
13. For convenience, after performing a restore of a guest VM to a host server, Replay Manager will leave the VSS View Volume attached (imported) to the host server in case the administrator wishes to perform additional manual file copy operations. By clicking **Expose**, an administrator can assign the VSS View Volume a drive letter or mount point and perform additional steps if necessary as part of the restore process. This is typically not necessary.
14. If no additional steps are required, under the action pane in Replay Manager Explorer, highlight the imported restore point and click **Unimport** to remove the VSS View Volume mapping from the Hyper-V host server.
15. After clicking **Unimport**, the restore point will show as available again.
16. The guest VM restore is now complete.

5.2 Use Replay Manager Expose to recover guest VM data

With Replay Manager, a backup administrator may choose to expose a VSS View Volume of a restore point as a side-by-side (read-only or writable) volume on the physical Hyper-V server host. This allows for the manual recovery of a Hyper-V guest VM or a subset of its data. A Replay Manager Expose operation is helpful if an administrator wishes to:

- Create a duplicate copy of the guest VM in an isolated environment for testing or troubleshooting.
- Manually restore specific data files to a guest VM without having to restore the entire guest.
- Recover data from a restore point that has been transported from another server. For more information on transporting restore points, see section 6.

Follow these steps to recover guest VM data using the Replay Manager Expose operation:

1. Log in to the Replay Manager Explorer GUI.
2. In the navigation pane under **Server Connections**, click the physical Hyper-V host server that contains the desired Hyper-V guest VM.
3. In the navigation pane under **Backup Extensions**, click **Hyper-V Guests**.
4. In the explorer pane, click the desired Hyper-V guest VM for the restore. Selecting the desired Hyper-V guest VM acts a filter that displays only the backup sets and restore points applicable to this guest VM.
5. Click the desired restore point to select it.

6. In the action pane under **Restore Points**, click **Expose**.
7. In the **Hyper-V Expose** dialog box, click the **Expose Path** drop-down menu.
8. Select a free drive letter to assign to the exposed volume (or specify a mount point) and click the **Submit** button.
9. Click **Expose**.

Note: If **Make exposed volumes writable** is checked, this restore point is removed from the list in Replay Manager because VSS is unable to continue managing a restore point once it is write enabled. In most cases, exposed restore points should be left read-only (the default) so Replay Manager can continue to manage them. For more information about accessing and managing a restore point that has been made writable (no longer listed in Replay Manager), refer to section 7.

10. Once the expose operation has completed, the volume associated with the VSS View Volume is accessible on the host server by the assigned drive letter or mount point.

At this point, there are several manual recovery options:

Option 1: Use Disk Management to mount the virtual hard disk file as a local disk using a drive letter or mount point, and then recover specific files from the virtual hard disk (see section 5.2.1).

Option 2: Use Hyper-V Manager to attach the virtual hard disk to the same guest VM (see section 5.2.2).

Option 3: Manually recover the guest VM to the original location.

Option 4: Create a duplicate copy of the original guest VM, typically in an isolated environment. With this option, care must be taken to avoid causing server name or IP address conflicts.

5.2.1 Attach a virtual hard disk to a physical host and assign a drive letter

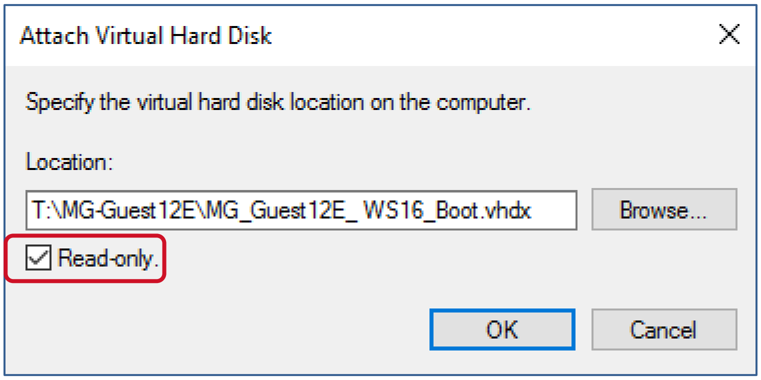
The ability to attach a virtual hard disk as a local disk on a physical Hyper-V host server was introduced with Windows Server 2008 R2. Windows Server 2008 R2 or newer is required to attach a VHD virtual hard disk as a local disk. Windows Server 2012 or newer is required to attach a VHDX virtual hard disk as a local disk.

This makes the recovery of specific files from a virtual hard disk simple and easy. This is especially useful in cases where an administrator does not need to recover the entire guest VM.

1. On the physical host server, launch **Disk Management** and click the **Action** drop-down list. Select **Attach VHD**.

2. In the **Attach Virtual Hard Disk** dialog box, click **Browse,** select the desired virtual hard disk file, and click **Open**. Select the box for **Read-only** unless the volume was exposed as writeable.

Note: If the VSS View Volume was exposed as read-only (the default), make sure the **Read-only** option is selected in step 2.



Attach Virtual Hard Disk

Specify the virtual hard disk location on the computer.

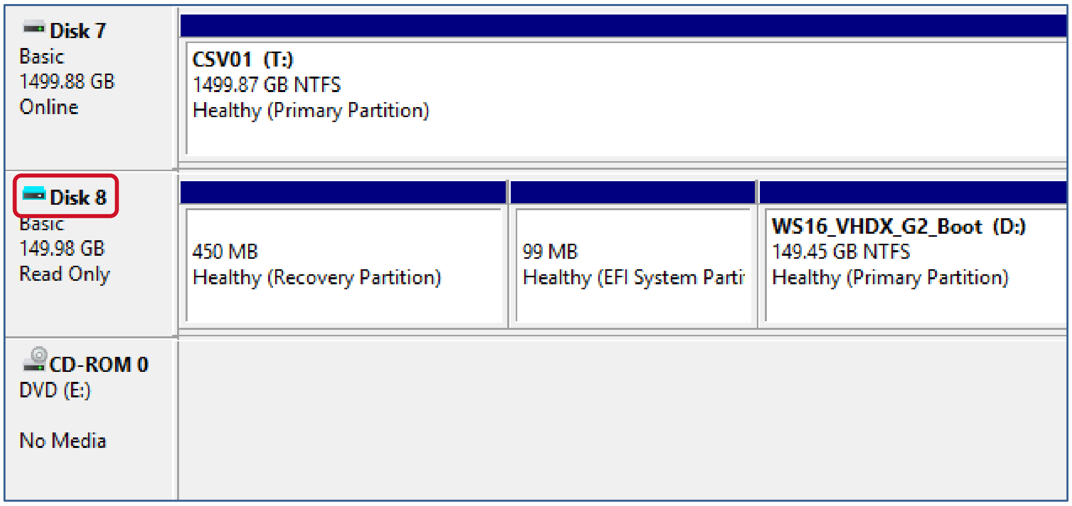
Location:

T:\MG-Guest12E\MG_Guest12E_ WS16_Boot.vhdx

☑ Read-only

Figure 25 Attach a virtual hard disk as read-only

3. Click **OK**.
4. Disk Management mounts the virtual hard disk as a new disk on the host, and assigns drive letters to disk partitions on the virtual hard disk file. On the physical host, the disk icon for an attached virtual hard disk is displayed with a light blue color to aid with identification.



Disk 7
Basic
1499.88 GB
Online

CSV01 (T:)
1499.87 GB NTFS
Healthy (Primary Partition)

Disk 8
Basic
149.98 GB
Read Only

450 MB
Healthy (Recovery Partition)

99 MB
Healthy (EFI System Parti

WS16_VHDX_G2_Boot (D:)
149.45 GB NTFS
Healthy (Primary Partition)

CD-ROM 0
DVD (E:)

No Media

Figure 26 Attached virtual hard disk (read only) with drive letters assigned to the partitions

5. Using Windows Explorer, locate the desired files on the attached virtual hard disk and recover them.

Note: If all servers involved are members of the same Active Directory domain and the recovered files and folders do not have any explicitly assigned security permissions, the recovered files should retain the correct permissions. Regardless, the backup administrator should verify that any manually recovered files and folders have the correct security settings and permissions.

6. Once the files have been recovered from the attached virtual hard disk, detach it using Disk Management. To do this, right-click the disk and select **Detach VHD.** Click **OK**.
7. In Replay Manager, the restore point shows a status of **Imported and Exposed**. To return the restore point to **Available** status:
   a. Click the restore point to select it.
   b. Click **Unexpose** and click **Yes**. Allow the job to finish.
   c. Click **Unimport** and click **Yes**. Allow the job to finish.
   d. Verify that the restore point status shows as **Available** again.

5.2.2 Attach a virtual hard disk as an additional hard disk on the same host

In some cases, it may be desirable to attach the recovery virtual hard disk from an exposed VSS View Volume to the same Hyper-V guest VM. This may make it easier to copy or compare files within the Hyper-V guest VM.

However, attempting to attach an exposed copy of a virtual hard disk as additional disk on the same Hyper-V guest VM generates a Windows error. This is default Windows behavior because the live virtual hard disk and the exposed copy have the same disk signature.

Note: Renaming a virtual hard disk does not change the disk signature, even if it is made writeable when it is exposed.

To assign a new disk signature to the virtual hard disk on the exposed VSS View Volume, do the following:

1. Make a copy of the virtual hard disk.
   - If the VSS View Volume was exposed as read only, copy the virtual hard disk to another volume that is writable on that same host server.
   - If the VSS View Volume was exposed as writable, make a copy of the virtual hard disk on the same volume (if there is room to do so).

Note: Copying a large virtual hard disk file may not be practical if it is extremely large. If necessary, map a temporary SAN volume to the host, or expand an existing volume to provide the space needed.

2. As part of the copy process, Windows will detect the duplicate disk signature and assign a new signature to the copy automatically. In order for this to work correctly, the source and destination must be on the same Hyper-V host.
3. Once the virtual hard disk file has been copied, to avoid any confusion, rename the copy. Choose a name that will make it easy to identify its purpose.
4. Present the virtual hard disk with the new disk signature to the guest VM as an additional disk using the desired management tool such as Hyper-V Manager.

5. Once the recovery is complete, detach the additional virtual hard disk and complete any other desired cleanup steps.
6. If applicable, return the restore point to **Available** status in Replay Manager by performing an **Unexpose** and **Unimport**. This only works if the VSS View Volume containing virtual hard disk was exposed as read-only. If it was exposed as writable, it will no longer be visible in Replay Manager.

6 Transport a Hyper-V guest VM restore point

Transporting a guest VM restore point to another Hyper-V host or cluster allows an identical copy of that server to be brought online in another location, such as when a copy of a production guest VM is needed to test an upgrade or troubleshoot a problem.

Before transporting a restore point for a Hyper-V guest VM, make sure that the destination environment will provide isolation to avoid server name and IP address conflicts.

To transport a restore point for a Hyper-V guest VM to another Hyper-V host server, complete the following steps:

1. Install the Replay Manager server agent on the target Hyper-V server.
2. Add the server to Replay Manager Explorer so it is listed in the navigation pane under **Server Connections**.
3. In Replay Manager, click the source Hyper-V server.
4. In the navigation pane under **Backup Extensions**, click **Hyper-V Guests**. This displays a list of guest VMs running on the source Hyper-V server in the explorer pane.
5. In the explorer pane, select the source Hyper-V guest VM. This filters the list of backup sets and restore points to those that are applicable to the guest VM.
6. Click the desired restore point to select it.
7. In the action pane under Transfer Restore Points, click Transport to Server.
8. In the **Choose Target Server** dialog box, click the desired target Hyper-V host server to select it.
9. Click **OK** to transfer the restore point to that server.

Note: Replay Manager does not permit a transport-to-server operation when the target server is a member of the same cluster as the source server. The target server must be a member of a different cluster or a standalone host.

---

10. Once the transfer job is complete, locate the transported restore point by doing the following:

    a. In Replay Manager, click the destination server under **Server Connections**.
    b. Under **Backup Extensions**, click **Local Volumes**.
    c. The transported restore point is listed in the explorer pane under **Backup Sets**. Click the restore point to highlight it.
    d. The available options are listed in the action pane. Because this is a transported restore point, the options available are limited to delete, expose, force keep, and transport to server.

11. Guest VM recovery (or recovery of a subset of data) can be now performed manually after running an expose operation (see section 5.2).

Note: If this restore point needs to be retained indefinitely, click **Force Keep** in the action pane.

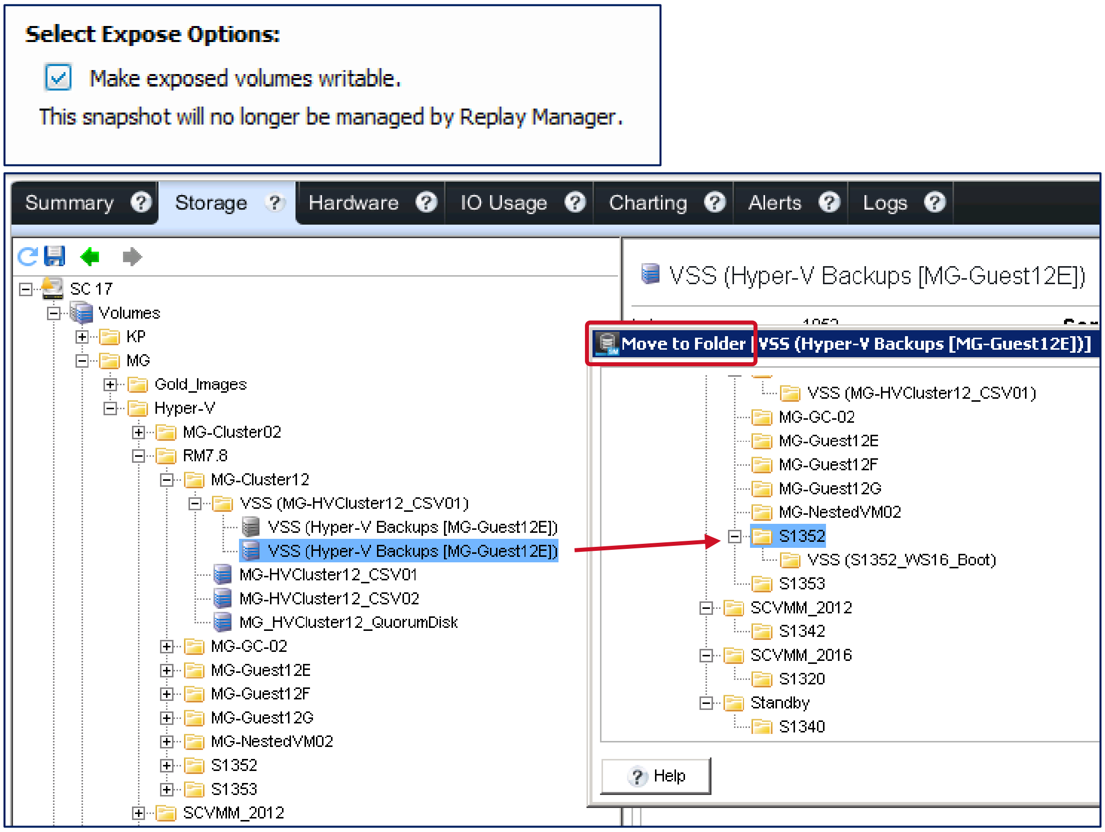
---

7 Manage writeable restore points

In most cases, a restore point is exposed as read only (the default option). If a restore point must be made writable, select **Make exposed volume writable** when performing an expose operation. This causes the restore point to drop from the list in Replay Manager by design, because VSS is unable to manage a restore point once it is made writable. The VSS View volumes that were associated with the restore point can now be managed by using the Dell Storage Manager (DSM) client.

To locate and manage writable VSS View Volume(s) that were formerly associated with a Replay Manager restore point, complete the following steps:

1. Access the DSM client and connect to the desired SC Series array.
2. Under **Storage**, expand the folder tree to the appropriate VSS folder.
3. The View Volume that is now writable is mapped to the target host it was exposed to. Volume icons are blue in color when they are mapped to a host. This aids with identifying the right volume.
4. Use DSM to manage the writable VSS View Volume going forward. As a best practice, it should be renamed and moved to another volume folder to avoid confusing it with the read-only VSS View Volumes still located under the VSS folder.



Select Expose Options:

☑ Make exposed volumes writable.

This snapshot will no longer be managed by Replay Manager.

Figure 27 Identify and move VSS View Volumes that are exposed as writable

Note: Do not use DSM to modify, move, or delete VSS View Volumes in the VSS folder that are read-only. These read-only volumes belong to restore points that are managed by Replay Manager backup sets and their respective retention policies.

A Additional resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware, and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC storage platforms.

Referenced or recommended Dell EMC publications:

- Dell EMC SC Series Storage
- Configuring Microsoft Hyper-V Hosts to Access Dell SCv2000 and SC4020 Arrays with SAS Front-end HBAs
- Dell EMC SC Series Storage: Microsoft Multipath I/O Best Practices
- Dell Compellent Storage Center Virtual Fibre Channel for Hyper-V Demo Video
- Dell EMC SC Series Replay Manager 7 and Hyper-V Demo Video
- Dell EMC SC Series Storage: Windows Server 2016 and Nano Server Best Practices
- Windows Server 2012 R2 Best Practices Guide for Dell EMC SC Series Storage
- Dell Storage Center OS 7.0 Data Reduction with Deduplication and Compression Solution Guide
- Dell SC Series Storage: Synchronous Replication and Live Volume
- Live Volume with Auto Failover Support for Microsoft Demo Video
- Dell Compellent Storage Center Enterprise Manager DR Plan for Hyper-V Demo Video
- Dell Storage PowerShell SDK Cookbook
- Dell EMC SC Series and SMI-S Integration with Microsoft SCVMM Best Practices Guide
- Dell Compellent Storage Center Microsoft System Center VMM 2012 SP1 Rapid Provisioning Demo Video

Referenced or recommended Microsoft publications:

- Microsoft TechNet Library
- Microsoft PowerShell Developer Network (MSDN)