

Replay 4 Hyper-V

Technical Overview

This guide contains an overview of Replay for Hyper-V, a new feature in Replay 4.

Copyright 2009 by AppAssure, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means — graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage and retrieval systems — without the written permission of the publisher.

For permission to use material from this publication, contact

AppAssure Software, Inc.
1925 Isaac Newton Square, Suite 440
Reston, VA 20910
+1 703-547-8686
info@appassure.com

Contents

Introduction	4
Host Based Image Backups	4
Guest Image Backups	5
Host Image Backups vs. Guest Image Backups	5
Windows Server Backup	5
Replay for Hyper-V	6
Features	6
Protecting and Restoring a Hyper-V Server	7
Restoring Files	8
Restoring a Volume	8
Restoring a Virtual Machine	8
Installation and Configuration	9
Replay 4 Components	9
VHD Naming Recommendation	9

TECHNICAL OVERVIEW

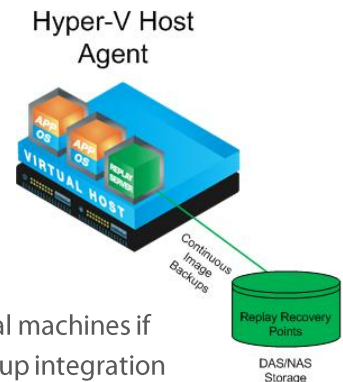
Introduction

One of the challenges of managing a Hyper-V environment is creating and implementing a disaster recovery plan. While creating virtual machine snapshots is a valuable facility for protecting your virtual machines during risky procedures they are not a substitute for host-based backups. The biggest limitation of virtual machine snapshots is that they do not offer the same level of protection as host based image backups, and they can really hurt virtual machine performance.

There are two choices to protect a Hyper-V environment, host based backups or running backups within the guest virtual machine. Depending on the type of workloads, each approach has its advantages and disadvantages.

Host Based Image Backups

The easiest approach to backing up a Hyper-V host is to run a host based backup. One of the cool features of Hyper-V is its integration with VSS. The Hyper-V VSS writer safely snapshots each guest virtual machine from a single host based VSS backup. To use this facility, there are several technical considerations that you should understand.

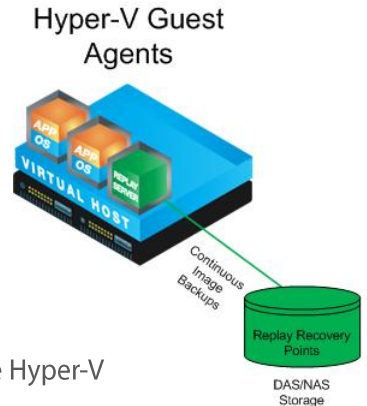


1. Integration Services – You can perform a backup of running guest virtual machines if each virtual machine has the integration services installed and the Backup integration service enabled. This approach will not support non Windows guest virtual machines or Windows versions that are not compatible with the integration services.
2. The guest virtual machines use volumes formatted as NTFS or FAT and are configured to use basic disks. Dynamic disks are not supported within a VHD, Hyper-V virtual hard disk however they are supported by host volumes that store the guest virtual machines (VHD).
3. VSS must be enabled for all volumes that contain virtual machine components and each volume must be configured to store its own shadow copy data. Make sure each volume has the appropriate amount of free space to accommodate shadow copy data.
4. If the above are not met, the backup will place each guest virtual machine in a paused state during the snapshot, disconnecting users and pausing applications until the snapshot is complete. This can take many minutes to complete.

Guest Image Backups

Guest Image backups install an agent on each guest virtual machine and perform that backup from within the guest. While this approach requires additional installation and setup time, it is recommended for particular types of application workloads such as Exchange. To use this approach, there are several technical considerations that you should understand.

1. The backups occur at the virtual machine level not the host level.
2. VSS is leveraged from within the virtual machine, no need to install the Hyper-V integration services.
3. Supports dynamic and basic disks.
4. The Backup does not impact the performance of the other virtual machines on the host.



Host Image Backups vs. Guest Image Backups

	Pros	Cons
Host Image Backups	<ul style="list-style-type: none"> ▪ Backs up the entire host, operating system, virtual machine configuration, snapshot data and each virtual machine. ▪ Application-aware backups support Exchange and SQL workloads ▪ Protects against host failures ▪ One agent on host only 	<ul style="list-style-type: none"> ▪ Can't restore application level objects ▪ No application backup validation and log truncation ▪ Limits on individual file-level restores ▪ Backups can impact host performance
Guest Image Backups	<ul style="list-style-type: none"> ▪ Granular restores ▪ Can protect each virtual machine uniquely ▪ Application log truncation and backup validation ▪ Backup overhead is limited to the virtual machine 	<ul style="list-style-type: none"> ▪ Agent must be installed on each guest virtual machine

Windows Server Backup

Performing a host level backup of a Hyper-V server requires the use of the Hyper-V VSS Writer. This means that the backup application must be integrated with the Hyper-V Writer.

Windows Server Backup is available with Windows 2008 but it not designed to work with the Hyper-V VSS writer but can be configured to support Hyper-V by registering the Hyper-V VSS writer in the registry. Registration can be accomplished by hand using REGEDIT or in an automated fashion by importing a .REG file.

Using the .REG file is the recommended approach to configuring Hyper-V VSS writer support to eliminate errors and automate the process. <http://technet.microsoft.com/enus/windowsserver/dd775213.aspx>

Replay for Hyper-V

Replay for Hyper-V is an enterprise-class backup & disaster recovery solution designed for Windows Server 2008 Hyper-V environments. It supports both host and guest backup methodologies while delivering backup and recovery, advanced disaster recovery and replication capabilities in one solution.

Features

Replay 4		Hyper-V
Backup & Recovery Features		
	Host based agents supports an unlimited number of guest virtual machines	✓
	Continuous application protection – online point-in-time imaging for Hyper-V hosts and guest virtual machines	✓
	Application support for Exchange, SQL and SharePoint	✓
	Compression and Dedupe of recovery points	✓
	Flexible storage options, recovery points can be stored on a remote or removable disk drive, DAS NAS or SAN storage	✓
	Centralized monitoring and management of backups	✓
	Snapshot Granularity	Minutes
	File level and application object level recoveries	✓
Disaster Recovery Features		
	Bare-metal server recoveries Restore to Dissimilar Hardware is an available option	✓
	Rescue images enabling 1 click server restores	✓

	P2V, V2V, Export to virtual machines for migrations and testing (VMware and Hyper-V Supported)	✓
	Off-host processing eliminates backup windows – fast Backups (RPO)	✓
	Live Replay – fast Restores (RTO)	✓
	Centralized recovery points for efficient storage management	✓
High Availability Features		
	Virtual Standby – Automatic creation and continuous updates of virtual standby environments. Supports VMware and Hyper-V P2V,V2V,P2P	✓
	Push button failover with High Availability features	✓
Replication Features		
	Off-site backups to Cloud Offering or Client DR Site	✓
	Off-site recovery of virtual machines and servers to Cloud or DR Site	✓
	Off-Site retention policies	✓

Protecting and Restoring a Hyper-V Server

Follow the steps below to protect a Hyper-V host:

1. Protect the Hyper-V host machine by installing the Replay Agent on the host.
2. Take a base image of the hyper-v host from the Replay Admin Console.
3. Make a rescue image export for the hyper-v host and export it to a network drive.
4. Make an RRC CD for the domain (this will allow you to restore the system drive.)

Follow the steps below to restore a Hyper-V host:

1. Boot from the RRC boot CD.
2. Map network drive to the location of the rescue image and restore all the drives. The host will be restored back to the point in time when the rescue image was last exported.
3. Reboot when complete.

Note: The virtual network settings are restored when the Hyper-V host is restored.

Restoring Files

Individual files within virtual machines can be restored. Replay's recovery points are mountable as drive letters or mount points.

Replay offers a free Explorer utility that mounts VHD's as drive letters so you can access the files.

Restoring a Volume

If a disk fails, Replay can restore a volume on the Hyper-V host. Be careful to restore all dependent volumes during the restore process.

Restore non-system drive:

Turn off all VMs that are on the drive. DO NOT SAVE. They must be turned off. The drive cannot be accessed during a restore. Any VM that is not tuned off when the restore starts will have to be recovered.

Restore non-system drive:

The system disk can be restored by Replay using 1 of 2 options. Option 1 is to create a rescue image by enabling the feature in the console. The rescue image is a set of files that can be restore directly from our Replay Recovery Console. Option 2, is available if you have deployed a Replay Core on another machine. If so, you can perform a bare-metal recovery to existing or new hardware.

Follow the steps below to restore a server using a Rescue Image:

1. Boot into the Replay Recovery Console (RRC).
2. Launch the image restore console and point to the location of the rescue image. You can use NET USE to map a drive over the network.
3. Recover the volumes.
4. After the restore is complete remove the RRC disk and reboot.

Restoring a Virtual Machine

Follow the steps below to restore an individual virtual machine:

1. Mount the recover point from the Replay Admin Console.
2. Locate the VHDs of the VM that you want to recover with Explorer.
3. Copy the file to a share that is on the Hyper-V host.
4. Move the VHD off the share and to the new destination location.
5. Make a new VM in the Hyper-V manager point to the VHD's that were copied from the recovery point.
6. Finish the settings for that VM. (Network Cards, Hard Drives, CPU, Memory Settings, etc.)
7. Start the new, recovered VM.

Installation and Configuration

The installation of Replay for Hyper-V requires Windows Server 2008 R2 or Windows Server 2008. Optionally, you can separate the Replay Core from the host to off-load the backups from the Hyper-V host.

Replay 4 Components

Replay Cores – Cores process backups, validates application integrity, compresses and deduplicates snapshots and replicates them over the WAN to a remote disaster recovery site. Cores can be local to the server being protected or distributed throughout the network enabling a flexible and scalable backup and disaster recovery configuration.

Replay Agents – Agents are installed on each the protected server or on Hyper-V hosts. It's responsible for capturing block-level changes on the server and sending them a Relay Core. A core can manage 1 to many agents. It also handles restores and server rollbacks.

Replay Admin Console – An enterprise console that centrally manages the Replay 4 environment.

VHD Naming Recommendation

Before the install it is recommended that you name all of your VHDs as the VM computer name – drive letter as they are mapped in the VM. For example, for the VM guest that has 3 VHD's, the name recommendation is **guestbox-C.vhd guestbox-d.vhd**.

For single server configurations, the Replay Core can be installed as a worker VM within the HyperV host.

1. Install the Replay Agent on the host; turn off all running VMs, then reboot.
2. Set up the Replay Core worker virtual machine on the C drive of the Hyper-V host. This will allow a full restore to other drives if needed. The operating system that the Replay Core runs under should be Windows 2008 with the Hyper-V guest tools installed. If the VM tools are not installed then when the VSS snapshot occurs that VM will save and then stop until the snap is completed.
3. Add the second VHD to use as the Replay repository disk. This should be place on a separate volume that will not be snapped.
4. Setup the virtual network so that the Replay server virtual machine connects with the Hyper-V host.
5. Install Replay Core in the worker Virtual Machine.
6. Test the connections by pinging from Replay core virtual machine to host and vice versa.
7. Launch the Replay Admin Console from the Replay Core virtual machine and add the Hyper-V host, by name or IP address to the console. Make sure and select the option, "Advanced, protect the volume individually" on page two of the Add Server wizard.
8. Select the volume to protect, excluding the volume that contains the Replay repository VHD.
9. A base image will begin automatically.

For distributed configurations, the Replay Core should be installed on a separate machine outside of the Hyper-V host.

1. Install the Replay Agent on the host; turn off all running VMs, then reboot.
2. Install the Replay Core on a virtual machine running outside of the protected Hyper-V host or on another physical server.
3. From the Replay Admin Console, add the Hyper-V host as a protected server.