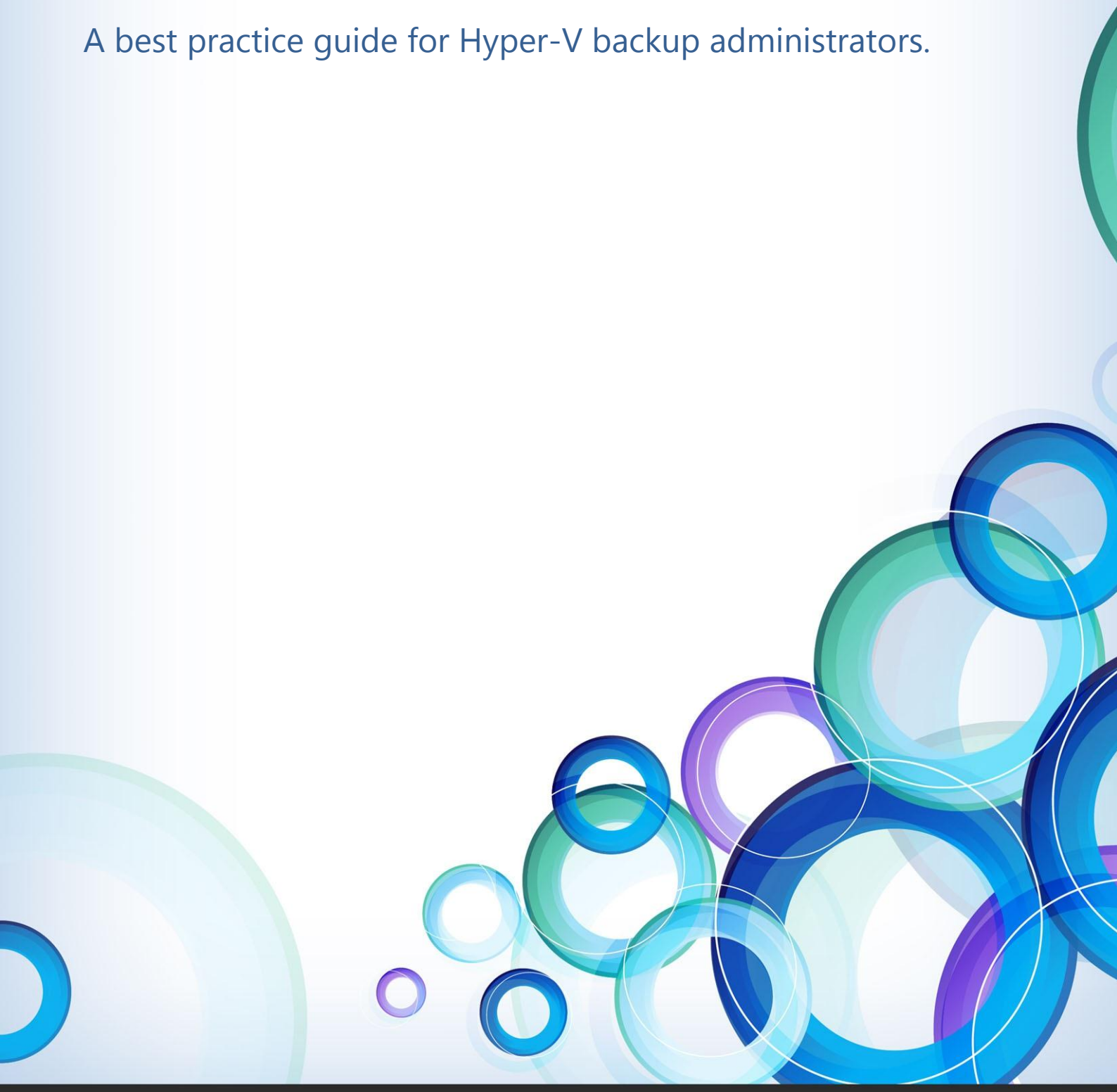
BackupAssist™

Hyper-V backup implementation guide

A best practice guide for Hyper-V backup administrators.



Cortex I.T.

© Cortex I.T. 2001-2014

Contents

© Cortex I.T. 2001-2014

1. Planning a Hyper-V backup

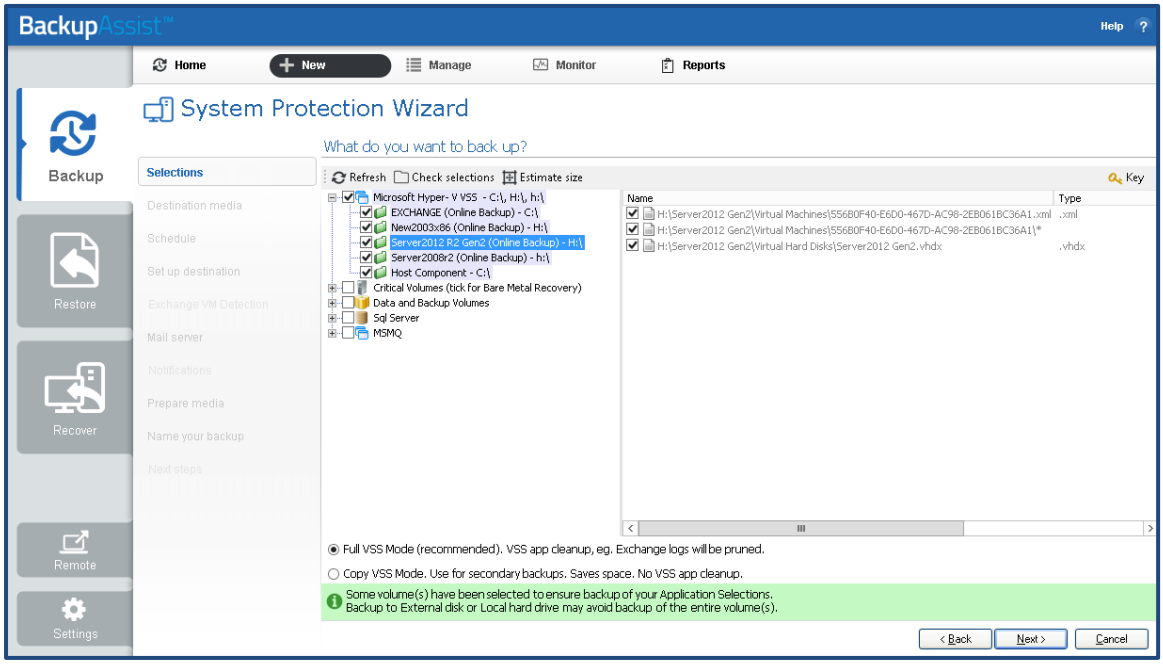
Planning your Hyper-V backup solution is important to ensure that backups and restores of Hyper-V hosts and guests work as intended. This document provides information and helpful hints so that you have a best practice solution that meets your expectations.

Hyper-V backup considerations

When planning a backup, the following points should be considered:

- The most effective usage of space when backing up guest machines
- The backup window available and the limitations of that backup window
- What restore options your backup will allow:
  - The *Hyper-V Granular Restore Console Add-on* can restore files from within a guest.
  - The *BackupAssist Restore console* can restore files located on the host or the complete guest machine.
- Backup redundancy through the use of both local and offsite backups
- Having one base license on each host. BackupAssist can use one license on a host to backup all guest machines and perform a one-pass backup.
- A Hyper-V guest will not be aware of the backup unless you install *Hyper-V Integration Services* on it. Without *Hyper-V Integration Services*, you will only get a crash-consistent backup of the VM, not an application-consistent backup
- Always use the Hyper-V VSS writer otherwise the guests will not be aware of the backup. This is critical, especially for guest applications like Exchange that must be involved in the backup.
- Back up the entire host volume containing the guest VHD files. Volume based backups are faster smaller and more reliable.

The below screenshot illustrates the selection of Hyper-V data using BackupAssist.



© Cortex I.T. 2001-2014

2. Hyper-V best practice

Implementing a Hyper-V backup solution means aligning what you are backing up, how you are backing it up and your backup destination. This section provides best practice suggestions for a Hyper-V backup implementation, using BackupAssist.

Best practice for hosts

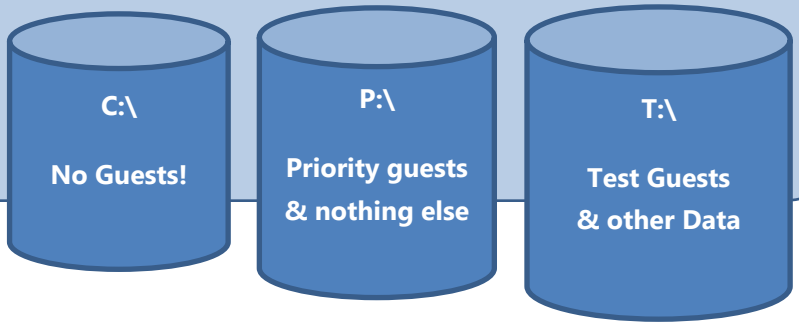
- The host machine shouldn't be located on the same domain as the guest machines.
- Only assign the Hyper-V role to the host server.
- Whatever backup destination you use, we recommend that you use a hardware solution for encryption.

Best practice for guests

- Do not use pass-through disks.
- Use basic disks because VSS does not support dynamic disks.
- Use a fixed VHD format for guests.
- Do not run Hyper-V snapshots on guests. The backup will run a VSS snapshot which is all that is required for a consistent back up of the guest machine - and hyper-v snapshots complicate restores.
- Only assign a single role to each guest e.g. An Exchange Server on one guest and a File Server on a separate guest.
- Enable the backup integration services.

Best practices for storing host data

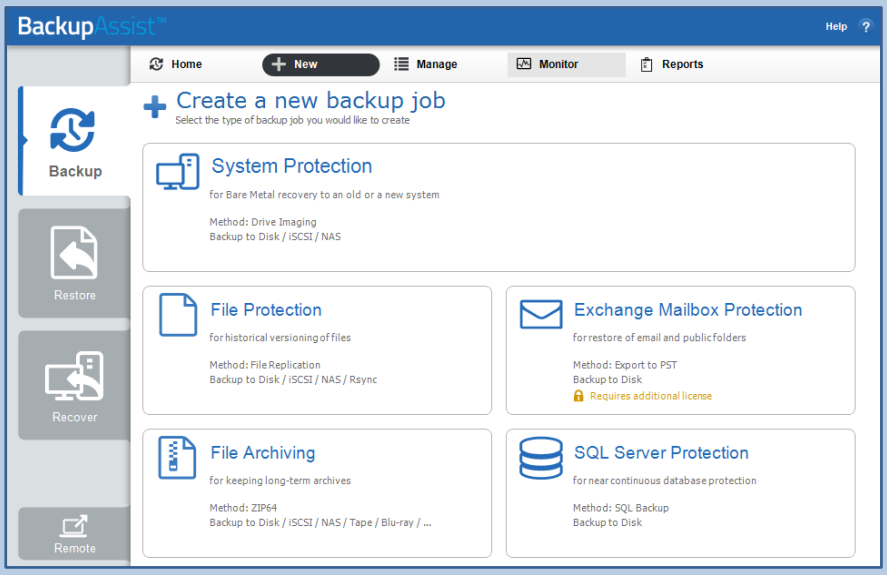
- Keep Hyper-V data on separate volumes (away from system volumes).
- Avoid storing "*other data*" on Hyper-V volumes.
- Keep non-critical guests and other data away from priority guests.
- Keep guest files such as XML, VHDs and snapshots together on the same volume.
- If you mix guest categories or guest files across volumes, both backups and restores become more complicated and less efficient. See the section "Backing up individual guest machines using System Protection" for more information.



© Cortex I.T. 2001-2014

Selecting the best backup type

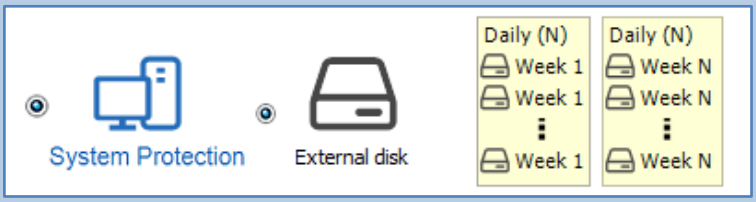
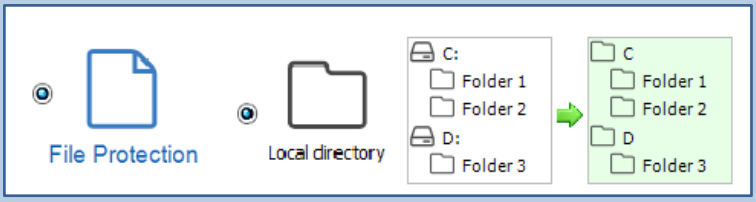
The three backup types included with BackupAssist can all back up Hyper-V and CSV environments, but it is important to select the one that best meets your requirements. The following table provides information to assist in selecting the right type of backup.

Backup type	Guidance
File Archiving	File Archiving is not recommended for the following reasons: • The compression of the VHD is slow and time consuming • Encrypting the backup is time consuming and complicates the backup and restore
File Protection	This type of backup has the following advantages: • The backup VHD is an exact copy of the guest • File can be recovered quickly • Redundancy - it provides an additional level of security NOTE: File Protection to an *Rsync* destination is NOT recommended for any Hyper-V backup. VHD files are very large and Rsync will run checksums on the entire VHD file which will consume both time and resources.
System Protection	System Protection is highly recommended for the following reasons: • It can be used by the Hyper-V Granular Restore add-on • It can be used for a disaster recovery External hard drives provide ideal backup destinations for System Protection because they support all of the following: • Bare metal backups • Block level changes • Backup history, therefore multiple restore options
Backup type selection	Backup types are selected using the, *Create a new backup job* screen. 

© Cortex I.T. 2001-2014

Best practice backup scenarios

The table below provides examples of ideal backups for daily and archive (historical) backup jobs.

Backup type	Backup scenario
System Protection	A daily backup A System Protection bare-metal backup (*Critical Volumes* selected) of the host and priority guests to external hard drive pool #1. The external hard drives are rotated on a daily basis. Priority guests include guests that are running applications such as Exchange and SQL, and guests running and storing critical data (such as financial applications and business data). Note: Windows 2008R2 or Windows 2012 allow individual file selection. This means you can store the priority guests on one volume and non-priority guests on a separate volume – a recommended best practice. 
System Protection	A weekly backup A System Protection bare-metal backup (*Critical Volumes* selected) of the host and ALL guests to external hard drive pool #2. This backup achieves: • Redundancy with both local and offsite backups • Multiple restores options. Local backups allow for easy access to the guest machine VHDs.
File Protection	A recommended implementation of this backup type is to back up priority guests to a local drive using the '*Mirror*' backup scheme. 

© Cortex I.T. 2001-2014

3. System Protection backups

System Protection backups are recommended for most Hyper-V servers because they can use the Hyper-V Granular Restore tool and Data containers, and they can be used in a recovery. Below are some important considerations when using System Protection to back up a Hyper-V environment.

Destination considerations

The backup destination needs to be at least twice the size of the source data.
E.g. 1TB of guest data requires a 2TB drive.

The destination needs to be NTFS formatted and support VSS.
E.g. Local directory, External hard drives, data container or iSCSI destinations.

There is a 2TB limit on the size of source volumes to be backed up, on operating systems prior to Windows Server 2012.

Advanced format drives (usually over 2TB in size) will have a sector size of 4KB (4096B.) This is not supported by System Protection backups in operating systems earlier than Windows Server 2012.

Backing up individual guest machines using System Protection

We recommend that you back up entire volumes only using System Protection, and back up individual guests using file protection. In cases where you only want to back up specific guests using System Protection, the following requirements and recommendations should be considered:

It is only possible back up specific guests (using System Protection) on Windows Server 2008R2 and Windows Server 2012.

Back up to an NTFS formatted destination that supports VSS

E.g. Local drive, External hard drive, data container or iSCSI destinations.

Check that you have selected *Copy* under *VSS backup mode*. Go to the Backup tab's *Manage* menu, select the backup job, and then select *Edit* > *Imaging options*.

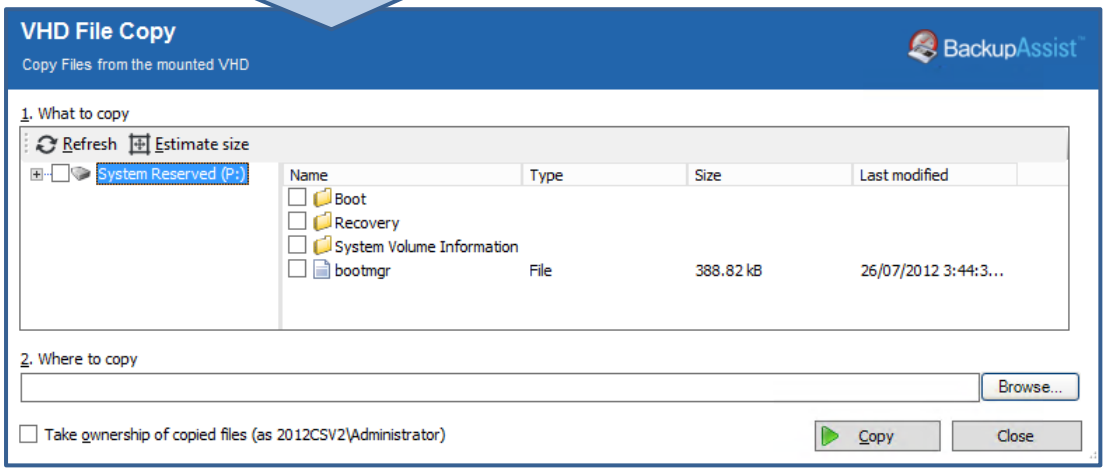
© Cortex I.T. 2001-2014

4. Hyper-V Granular Restore tips

The Hyper-V Granular Restore console allows the recovery of files from individual guests. Below are a set of quick tips for when performing a Hyper-V granular restore.

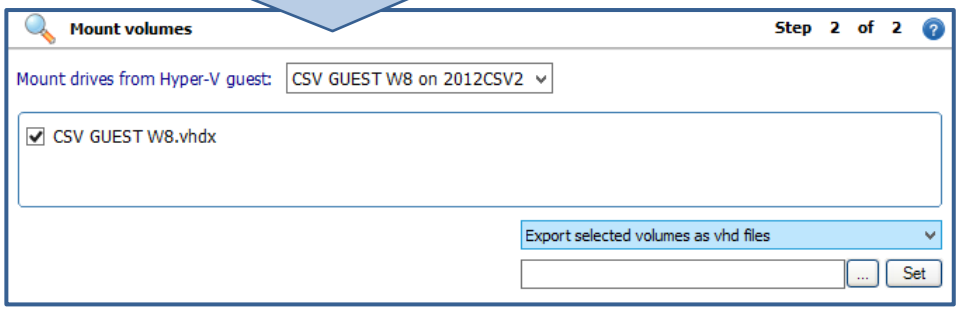
Tip 1: Taking ownership of copied files

- When you mount a disk from a guest computer on a domain, you might not have the permissions required to open or copy the file from Windows explorer.
- The *VHD File Copy* feature includes the option *Take ownership of the copied files*. This allows full access to the copied VHD file instead of manually changing permissions via file properties.



Tip 2: Export option - allows you to export selected volumes instead of mounting:

- This option creates and exports a copy of the VHD (of the guest).
- If a VHD is copied manually, it can contain AVHDS, VHDS and other configuration files which will need to be manually merged in order to get a valid VHD file.
- The advantage of the *Export* tool is that it merges AVHDS and VHDS into a single parent VHD.



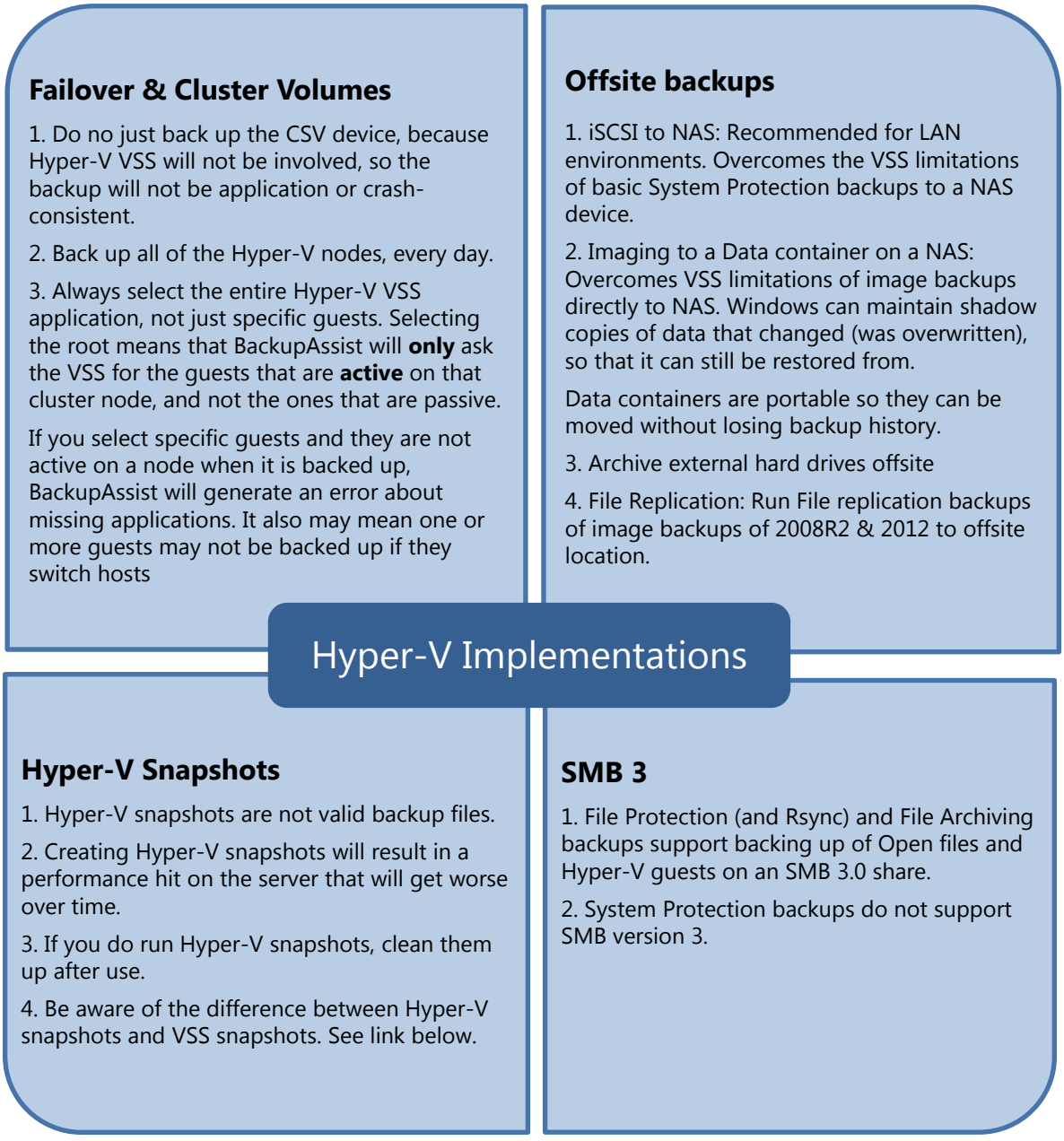
Tip 3: Add command-line options to the Granular Restore console

- 'ImageBackup': This command returns a top level view of host volumes that were backed up.
- 'SingleVHD': This command allows you to browse for and mount any VHD. This is useful when you do not have disk management options to help mount the VHD.

© Cortex I.T. 2001-2014

5. Advanced topics and technologies

This graphic includes considerations and advice for specific technologies and implementations.



Related links

Snapshots: Difference between Hyper-V snapshots and VSS snapshots:
www.backupassist.com/blog/support/hyper-v-snapshots-vss-snapshots-the-differences/

Offsite backups: VSS limitations of basic System Protection backups to a NAS device:
www.backupassist.com/education/articles/pros-and-cons-backing-up-windows-server-2008-NAS.html

© Cortex I.T. 2001-2014

6. Troubleshooting Hyper-V backups

The following troubleshooting steps are for specific Hyper-V problems. For additional troubleshooting information and resources, please refer to the resource links at the bottom of this page.

❖ **Saved state**

If guests go into 'Saved state' during a backup, or if the guest turns off during the backup, this means that an offline backup was performed. To troubleshoot this:

- Enable 'Backup' integration services
- Ensure that all guest files are on the same host volume
- Use basic disks for your guests
- Use NTFS for all guest volumes
- Hyper-V cannot perform online backups of Unix or Mac machines

❖ **VSS timeout**

VSS snapshots can sometimes take a long time to complete. The default timeout for the VSS snapshot is 10 minutes. This can be extended to 20 minutes to ensure ample time for the VSS snapshot to complete. This is addressed by 'Known issue 2' in the following help article: http://kb.backupassist.com/articles.php?aid=3039

❖ **Exchange**

Be aware of the following when backing up and restoring mail data:

- Restoring mail items from within an Exchange backup on a guest using EGR involves two steps: First mount guest VHD using the Hyper-V Granular restore console, then launch Exchange Granular Restore and browse to the EDB file on the mounted guest VHD.
- Mailbox backups of multiple Exchange guests can be run from the host.

  If you are faced with authorization issues:

  - Create a Domain user with required Exchange privileges.
  - Install a trial copy of BackupAssist on the Exchange guest machine, set the new user as the backup user identity, and run the mailbox backup from the virtual machine.
  - If the backup succeeds on the Exchange guest, create a matching user on the host with the same username and password and use this as your BUI, and then run the back up from the host.

Additional Resources

For detailed instructions on how to create backups and perform restores of Hyper-V environments, **please refer to the Hyper-V whitepaper.**

Exchange backups from a Hyper-V host:
www.backupassist.com/education/articles/mailbox-backups-from-hyper-v-host.html

Configuring Hyper-V permissions for Exchange mailbox backups:
www.backupassist.com/education/articles/setting-up-a-user-for-exchange-mailbox-backups.html

© Cortex I.T. 2001-2014