

BackupAssist™

BackupAssist v7

# System Protection for Hyper-V Whitepaper

# Contents

<b>1. Introduction</b>	<b>2</b>
Documentation	2
Licensing	2
Hyper-V requirements	2
Definitions	3
Considerations	3
<b>2. About the BackupAssist Hyper-V solution</b>	<b>4</b>
Advantages	4
Granular technology	4
Backup Types	4
<b>3. Hyper-V in a Shared Clustered Volume</b>	<b>5</b>
Backing up a CSV environment	5
Restoring to a CSV environment	5
<b>4. Backup considerations</b>	<b>6</b>
Exchange VM Detection	6
Windows Server 2012	6
Restore vs. Recovery	6
Data containers	7
Windows SystemState	8
<b>5. BackupAssist settings</b>	<b>9</b>
Backup user identity	9
Email server settings	9
Email address list	9
Network paths	9
Windows Settings	9
<b>6. Creating a Hyper-V backup</b>	<b>10</b>
<b>7. Restoring a Hyper-V backup</b>	<b>15</b>
Hyper-V guest & host files restore	16
Hyper-V granular restore	18
Quick recovery from staging disk	20
<b>8. Hyper-V backup management</b>	<b>21</b>
Manually running a backup job	21
Scheduling	21
Files and applications	21
<b>9. The Hyper-V Config Reporter</b>	<b>22</b>
<b>10. Support and Resources</b>	<b>24</b>

# 1. Introduction

---



## System Protection

For bare metal recovery

Method: Drive Imaging  
Backup to Disk / iSCSI / NAS

BackupAssist protects Hyper-V environments by creating an image backup that can be used to restore individual files from a guest and its host, and to restore the virtual machine itself.

File Archiving, File Protection and System Protection can back up Hyper-V and Hyper-V CSV environments. System Protection backups can also be used to perform granular restores of Hyper-V guests using the Hyper-V Granular Restore Console. For this reason, System Protection is recommended for all Hyper-V backups. This whitepaper explains how to create, modify and restore Hyper-V backups using *System Protection*.

## Documentation

This whitepaper provides a comprehensive guide to using BackupAssist System Protection for Hyper-V environments, and can be used in conjunction with other BackupAssist guides.

- For general advice on Hyper-V protection, see the [Hyper-V backup implementation guide](#)
- To protect Hyper-V environments using File Archiving, see the [File Archiving User Guide](#)
- To protect Hyper-V environments using File Protection, see the [File Protection User Guide](#)
- To protect your data using System Protection, see the [System Protection User guide](#)

## Licensing

To restore Hyper-V guest data at a granular level requires the *Hyper-V Granular Restore Add-on* license, once the initial trial period has expired. Please contact your local BackupAssist reseller or distributor for pricing information, or visit [www.BackupAssist.com](http://www.BackupAssist.com).

For instructions on how to activate / deactivate license keys, visit our [Licensing BackupAssist page](#).

## Hyper-V requirements

### Supported operating systems

- Windows Server 2012/R2, including Server Core and Hyper-V Server versions.
- Windows Server 2008R2, including Server Core and Hyper-V Server versions.
- Windows Server 2008R1

### Pre-requisites

- Windows Backup - it is included with Windows Server but may not be installed.
- In a CSV environment, BackupAssist must be installed and licensed on each host.
- Partition sizes should be less than 2TB.
- Turn on the Backup Integration service for each Hyper-V guest as explained in this [blog post](#).



**Important:** Before implementing a Hyper-V protection solution, please refer to the [Hyper-V implementation guide](#) for advice and useful tips on backing up Hyper-V hosts and guests.

## Definitions

### Virtual Machine (VM)

A software environment that simulates a real computer (including hardware) on a host computer.

### Hyper-V

Hyper-V is Microsoft's implementation of virtual machine (VM) technology. Virtual machines run on a physical host machine and provide dedicated operating system environments (guests) to run applications (e.g. Exchange) or functions (e.g. a print server).

### Volume Shadow Copy Service (VSS)

VSS is a Microsoft Service that creates a shadow copy of an application's data (e.g. Exchange or SQL) so that data can be backed up without interfering with the application. VSS is explained in detail in the backup considerations section of this whitepaper.

### Hyper-V host

The Hyper-V host is the physical server (and operating system) that virtual machines (guests) run on.

### Hyper-V guest

The Hyper-V guest is a virtual machine running on a physical host machine. Examples include: A guest running Exchange on a Windows 2012 Server, a guest running file sharing on a Small Business Server and a Windows Server used to manage printers. Each guest runs using virtualized hardware, within a physical host machine.

### Cluster Share Volume (CSV)

CSV is Microsoft's implementation of server clustering, which is designed for use with Microsoft's Hyper-V. CSV provides a shared disk (volume) that can be used by any guest (virtual machine) in the cluster. This means a guest can be moved within the cluster, and guests can share the same physical disk. This improves flexibility and helps to provide seamless operation in the event of a system or hardware problem.

## Considerations

### Hyper-V backups

BackupAssist is VSS aware so Hyper-V backups can be performed without stopping the guest VM.

### Hyper-V restores

- *BackupAssist's Restore Console* will restore any data inside the host and any guest image (virtual environment) inside the host.
- *BackupAssist's Granular Restore* will restore data from inside the guest.

### VMWare backups

VMWare is a non-Microsoft virtualization technology. When guests are running on a VMWare Server, BackupAssist is currently unable to use VSS to create a live backup. The VMWare guest must be suspended prior to the backup taking place, and then resumed once the backup has completed.

The *Hyper-V Granular Restore Add-on* is currently only able to restore from backups performed on a Windows Hyper-V Server. For more information, see our online [VMWare article](#).

### Cluster Shared Volume backups

BackupAssist creates a System Protection backup of a Hyper-V CSV, by copying the data from the host and the guests to an intermediate staging area. System Protection then creates an image file (VHD) that contains the host data and an image of each guest (virtual environment).

## 2. About the BackupAssist Hyper-V solution

---

### Advantages

The BackupAssist Hyper-V solution eliminates the time consuming procedures and overcomes the reliability issues inherent in Hyper-V backups.

BackupAssist's granular technology simplifies Hyper-V backups by allowing you to use one image backup of the host to retrieve files and documents from any guest machine on that host.

The advantages of this are:

- ✓ You can restore multiple guest files from a single host backup.
- ✓ There is no need for separate backups of the host and guest.
- ✓ You can back up unlimited guest machines in moments – no extra licensing costs!
- ✓ A simple 2-step restore process with easy to follow wizards.
- ✓ Individually select which guest machines to back up.

### Granular technology

Without granular technology, you can only restore folders and files from regular backups created for each guest VM within the host, and it is this that makes back up and restore procedures so complicated. The BackupAssist VM Granular Restore console offers you simple wizards for every restore scenario, that take just minutes to complete.

Granular restore technology makes it possible to restore the individual files and folders that live on a guest VM (virtual machine), from the image backup of the host. The BackupAssist VM Granular Restore console allows you to “dig down” into the image backup, find the restore point, choose your guest VM and then retrieve files from within it.

You can also export a guest VM drive volume to a VHD (Virtual Hard Disk) file so you can easily rebuild a virtual machine in the event of a major disaster scenario.

### Backup Types

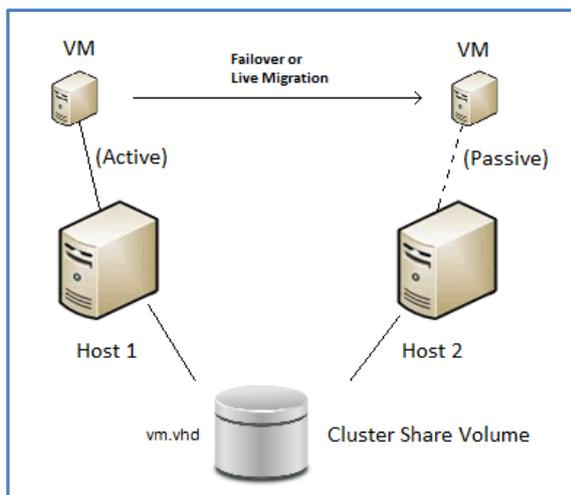
File Archiving and File Protection backups can detect Hyper-V environments, but the recommended method is a System Protection backup. System Protection creates an image backup file (VHD) that can be used in all restore and recovery scenarios, and provides the greatest flexibility.

The advantages of using *System Protection* include:

- It is the fastest way of backing up a Hyper-V environment.
- It can be used for Cluster Shared Volumes.
- It can be used to perform a granular restore.
- The backup can be used for a full system recovery when part of a bare-metal backup.

### 3. Hyper-V in a Shared Clustered Volume

When stored in a Cluster Share Volume (CSV), a virtual machine's files (virtual disks and configuration files) present as a shared resource between the hosts. As the CSV's files are shared, access to the virtual machine's files must be coordinated so only the one host accesses a virtual machine's files at a time.



This diagram depicts a configuration with a small cluster of two hosts with a single virtual machine, which may fail-over at any time from Host 1 to 2.

This virtual machine will only be active on a single host at any time - referred to as the *active node*. The other node is called the *passive node*.

Other virtual machines added to the cluster may be active on either host at any point in time.

#### Backing up a CSV environment:

Because a backup of a CSV must be coordinated, BackupAssist jobs on each host must have their start times staggered. The scheduled start time of the jobs on each host must be set at least 5 minutes apart. This will allow BackupAssist time to initialize and coordinate its access to the CSV. BackupAssist will automatically delay the second job so that it will not commence until the first job has completed. During a *System Protection* backup, the host and all guests are copied to an intermediate staging disk. The intermediate staging disk must be a local disk and it is overwritten each time a backup is run.

- BackupAssist v7 supports Hyper-V CSV on both Windows Server 2008R2 and 2012 machines.
- When a fail-over or migration occurs, one or more of the virtual machines will no longer be active on the original host. Therefore, BackupAssist must be installed and licensed on each host.
- A backup job must be created on each of the hosts to back up all virtual machines which are active on that host (at the time the backup runs). This can be done by selecting the entire Hyper-V VSS object for each job, which automatically finds active virtual machines at the time the backup runs.

#### Restoring to a CSV environment

When a guest is successfully restored to a Hyper-V cluster (CSV), it will become available on the Hyper-V machine that it was restored to.

- If the restore replaces the existing guest, the CSV settings will be retained and the guest will be added back to the cluster.
- If the restore does not replace the existing guest, the CSV setting will need to be manually configured to add the guest to the cluster.
- This affects Hyper-V CSV implementations on Windows 2008/ 2008R2 / 2012.

**Note:** 1) The Hyper-V Granular Restore Console does not support mounting image backups (VHD files) that were backed up off a CSV. 2) Windows Server 2012R2 does not support CSV environments.

## 4. Backup considerations

---



Before creating a backup job, it is important to understand what backup and restore options are available. This section provides guidance on some key considerations.

### Exchange VM Detection

If your backup job contains a Hyper-V guest with an Exchange Server, the authentication information for that guest should be entered into the **Exchange VM Detection** tab on the **Selection** screen when you create the backup job. With these credentials, BackupAssist can detect what guests have an Exchange Server, and list the EDB file available for each guest when you perform a restore using the Exchange Granular Restore console.

The Exchange VM Detection tab will appear when the Hyper-V role is installed and running on the server. If you are backing up multiple Exchange guests, each one should have the same username and password. The Hyper-V process is automated but the restore requires both the *Exchange Granular Restore Add-on* and the *Hyper-V Granular Restore Add-on* licenses.

### Windows Server 2012

Windows Server 2012 introduces the CSVFS format, which allows a cluster to differentiate CSV storage from other NTFS storage. BackupAssist supports backing up Hyper-V guests located on CSV storage using the CSVFS file system.

- BackupAssist supports SMB 3.0 servers as a CSVFS backup destination.
- Bit Locker drive encryption is not supported.
- BackupAssist does not support backups of files from both CSVFS and NTFS locations in the same snapshot. For example, it is not possible to back up a Hyper-V guest with a source in a CSV along with another guest that is on an NTFS volume.

Hyper-V is Microsoft's implementation of virtual machine (VM) technology. Virtual machines run on a physical host machine and provide dedicated operating system environments.

- Hyper-V Replica enables replication of a virtual machine across the internet. BackupAssist supports Hyper-V Replica and can back up and restore a primary Hyper-V guest using any backup type.

CSV Environments: CSV backups are supported by System Protection, File Protection and File Archiving backup types, but CSVFS and NTFS file systems cannot be mixed (as described above).

### Restore vs. Recovery

A restore is the process of accessing a backup and restoring it to the original (or a new) location, if your data is lost, corrupted or if you want an earlier version of that data. However, if your computer cannot start itself, you may need to perform a recovery.

A recovery is the process by which a computer is recovered after hardware has been replaced or an operating system failure has occurred, and your computer can no longer start itself. To perform a recovery you need a bootable media to start your computer, and an image backup that the bootable media can use to recover your operating system, data and applications.

For more information on data recovery, see the [Recover tab & RecoverAssist Whitepaper](#).

## Data containers

### The backup

BackupAssist *System Protection* creates image backups that can be used to restore and recover your data. These backups can be full or incremental, and the Windows Volume Shadow copy Service (VSS) maintains historical information so that each backup can be restored from.

Key points:

- If you have Windows VSS on the data source, data can be backed up incrementally.
- Incremental backups overwrite the data in the image backup that has changed.
- Windows can create shadow copies (snapshots) of the data that was changed.
- Data that was overwritten by previous backups can be restored using a VSS snapshot.

### The problem

On RDX drives and network destinations (e.g. NAS), shadow copies are not supported so Windows cannot maintain a backup history (snapshots of data that changed). This means restores can only be done from the last backup. A work around has been to put each backup into a different folder but this requires a full back up each time the backup jobs runs, which requires additional disk space.

Key points:

- Windows VSS cannot maintain historical information (snapshots) on a NAS or RDX device.
- Data can only be restored from the last backup.

### The solution

BackupAssist overcomes these Network/RDX destination limitations, by implementing *Data containers*. A Data container is a VHD file that *System Protection* backups can be stored inside of. The Data container is created on the destination media and each time the backup jobs runs, the Data container is mounted and treated as a local disk. Because the container is seen as a local disk, Windows can maintain shadow copies of data that changed (was overwritten), so that it can still be restored from.

When using a Data container for System Protection backups to NAS and RDX destinations:

- Data (in the backup) that has changed can still be restored, because snapshots are maintained.
- Folders are not needed to provide different restore points, saving valuable disk space and time.

### Other advantages

*RDX granular restore:* When Windows detects an RDX drive, it will compress the data that is being backed up. This compression means that individual files cannot be restored. By using a Data container, Windows will see the destination as a local drive and not compress the data. BackupAssist will therefore be able to restore individual files from an image backup stored on an RDX drive.

*Portable backups:* Enable portable backups for RDX, network, external disk and local drive destinations.

On Windows Server 2008R2 and later, you can copy a backup image to another device, but only the last backup can be restored because you cannot copy the shadow copy (snapshot). If the backup is in a Data container, the snapshot can be moved and all backups can be restored from.

### Supported systems

Data containers are supported on Window Server 2008 R1/R2 and SBS 2008/2011 and later operating systems.

- To learn more, see the [Data container resource page](#).

## Windows SystemState

### Overview

In previous versions of BackupAssist, Windows SystemState was called System State and it was available during the creation of a backup job. The Windows SystemState option is now selected by editing a backup job after it has been created. There are exceptions, as shown in the table below.

A Windows SystemState backup contains some of the important files, registry values and settings that are used by the Windows operating system. It does NOT back up the operating system itself. This means a Windows SystemState backup can be used to restore the settings your computer had at an earlier point in time, but it will not allow you to recover your computer. A Windows SystemState backup can be helpful if your computer is encountering errors and you want to restore your settings to an earlier point in time, before the errors occurred.

Because Windows SystemState requires a functioning computer, and can only *restore* Windows settings, we recommend that a bare-metal backup is used. A bare-metal backup can restore Windows SystemState data, and it can ALSO be used to perform a *recovery* of your computer, when used with a Windows recovery environment, like RecoverAssist.

### Selecting Windows SystemState

Windows SystemState can be selected after a backup job has been created, if you have enabled the *Windows settings*. The exceptions, considerations and steps required are explained below:

This table shows what backup jobs can include Windows SystemState.

	NTBackup (Windows 2003)	File Archiving, File Protection and System Protection backup jobs	File Archiving zip-to-tape backup jobs	File Protection Rsync backup jobs
During the creation of a new backup job	YES	NO	NO	NO
By editing an existing backup job	YES	YES, if enabled	YES	NO

#### To enable Windows SystemState:

1. Select the BackupAssist *Settings tab*.
  2. Select *Windows settings*.
  3. Tick *Enable v6 compatible Windows SystemState selection*.
- ❖ Backup jobs created in earlier versions of BackupAssist (that included System State) will have the setting enabled by default in BackupAssist v7.
  - ❖ Zip-to-tape backup jobs will not need to enable this setting, to select Windows SystemState.

#### To select Windows SystemState:

1. Select the BackupAssist *Backup tab*, and then the *Manage* menu.
2. Select the *backup job* that you want to modify, and then *Edit* from the menu.
3. Select *Files and applications* from the left pane.
4. Select *Windows SystemState* at the top of the data selection pane.

## 5. BackupAssist settings

---



When creating a backup job, there are some global settings that should be configured in BackupAssist. If they are not configured, you will be prompted to complete them during the creation of your first backup. It is recommended that this is done in advance.

BackupAssist's settings can be entered and modified using the selections available in the **Settings** tab. Clicking on the *Settings* tab will display the selections as icons. Four of these are used when creating new a backup job and each one is described below:

### Backup user identity

Backup jobs require an administrator account with read access to the data source, and full read-write access to the backup's destination. It is recommended that a dedicated backup account is created for this purpose. The account's details are entered here and your backup jobs will be launched using these credentials. The account's permissions will be validated both when the backup user identity is entered and when the job is executed. If no account is specified or the account has insufficient permissions, the backup job will fail and note the error in the backup report.

A video explaining the creation of a backup user identity can be found on our, [Videos Webpage](#).

### Email server settings

This menu item is used to enter the details of the SMTP server used by BackupAssist to send email notifications. The SMTP server must be configured if you want to have an email *Notifications* step enabled when you create a backup job.

### Email address list

This menu item is used to define and store the email addresses of potential notification recipients. The list will be used to populate the recipient selection screen when configuring an email notification for a backup job. Any email addresses entered during the creation of a new notification are automatically added to the *Email address list*.

### Network paths

This option allows you to enter access credentials for networks, domains and drives that the default account does not have access to. Enter or browse to the location and add it to the *Path list*. The *Edit* option will allow you to enter an authentication account, specifically for that path. When you create a backup job to a remote location, that location will be automatically added here.

### Windows Settings

System Protection creates a full image backup the first time it runs to a destination, but further backups will usually be incremental. This is achieved by scanning and comparing the data to be backed up and the data in the destination image to see what data changed, and only the data that has changed will be updated. Scanning can take some time, but can be avoided by enabling "incremental reading" using the option under the *Setting* tab > *Windows Settings* > *Enable Incremental Windows Image backups*.

## 6. Creating a Hyper-V backup



The following instructions describe how to back up Hyper-V environments using System Protection.

File Archiving and File Protection backups can also detect and back up Hyper-V environments but they do not support granular restores of guests or full recoveries of Hyper-V servers.

Launch BackupAssist and follow the steps outlined below:

1. Select the **Backup** tab, and click **Create a new backup Job**
2. Select **System Protection**

If this is the first time you have created a backup job, you will be asked to provide a *Backup user identity* if one has not been defined. See the section above, [BackupAssist settings](#), for guidance.

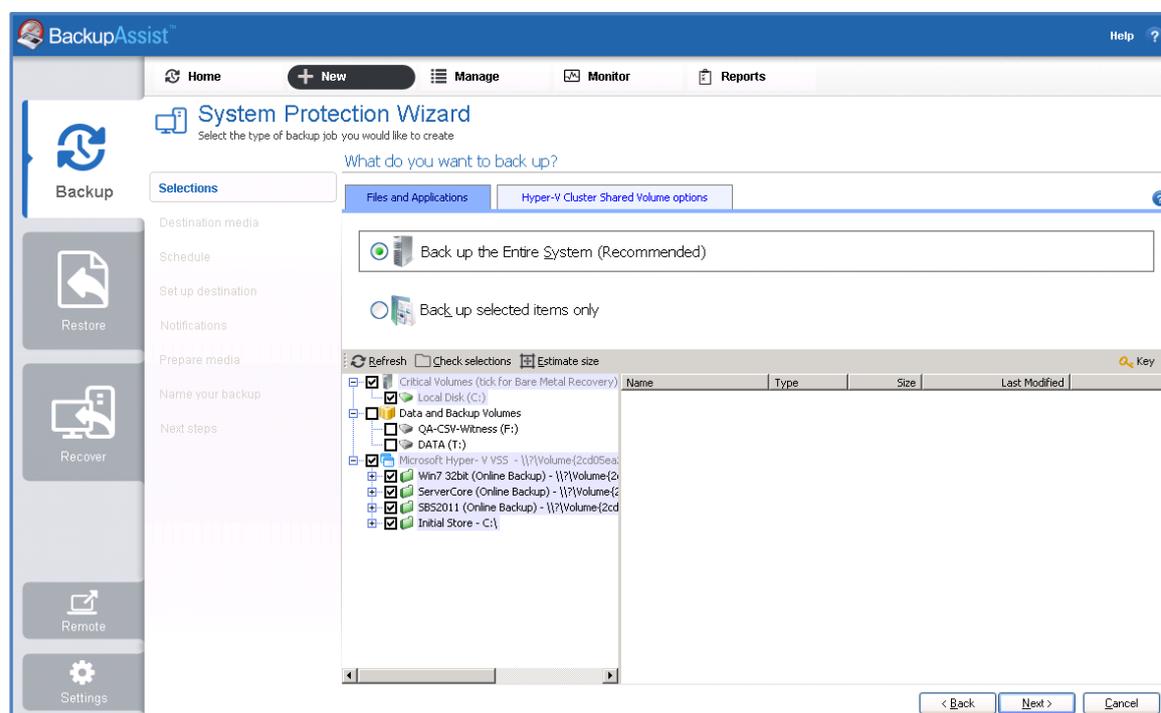
3. **Selections:** The selections screen is used to select the Hyper-V environments to be backed up.

An [Exchange VM Detection](#) tab will be available if you are backing up an Exchange VM guest.

All Hyper-V environments detected will be displayed here. The example below in figure 2 is of a CSV environment, so there is also a CSV tab.

**Files and Applications** tab.

Select the Hyper-V environments to be backed up. You can also select the *Back up Entire System* option to create a backup that can be used for a system recovery.



**Figure 1: BackupAssist Hyper-V backup – Selections screen**

- For a **non-clustered** host: Select **Next** and you will be taken to the *Destination media* step.
- For a **clustered** host: Select **Next** to proceed to the *Hyper-V Cluster Shared Volumes* tab.

## Hyper-V Clustered Shared Volume options tab.

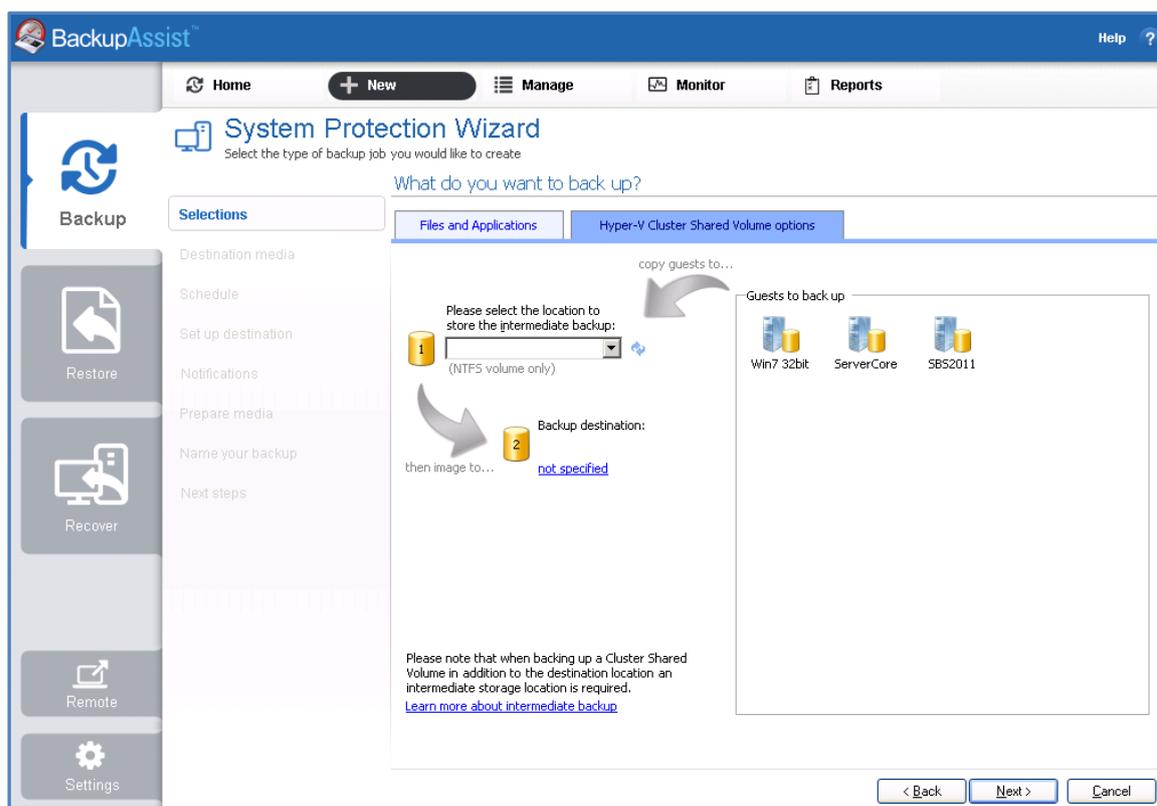
If you are creating a Hyper-V backup job for a shared clustered volume, then this tab will need to be completed. This step only applies to System Protection, Hyper-V backups using CSV. The tab will not appear in non-clustered environments.

The *Hyper-V Cluster Shared Volume* tab graphically shows the guests selected, and a field to select the intermediate backup location.

The intermediate backup is used to copy the host and guest data to a single location. This is also known as the *staging disk*. An image backup will then be made. The image is of the host, and within that image, is an image of each guest residing on the host.

- The intermediate backup's location must be a local disk.
- The intermediate backup's disk is overwritten each time a backup is run.
- The image backup is taken from the whole disk.

Enter the drive to be used for the intermediate backup, and click **Next**.

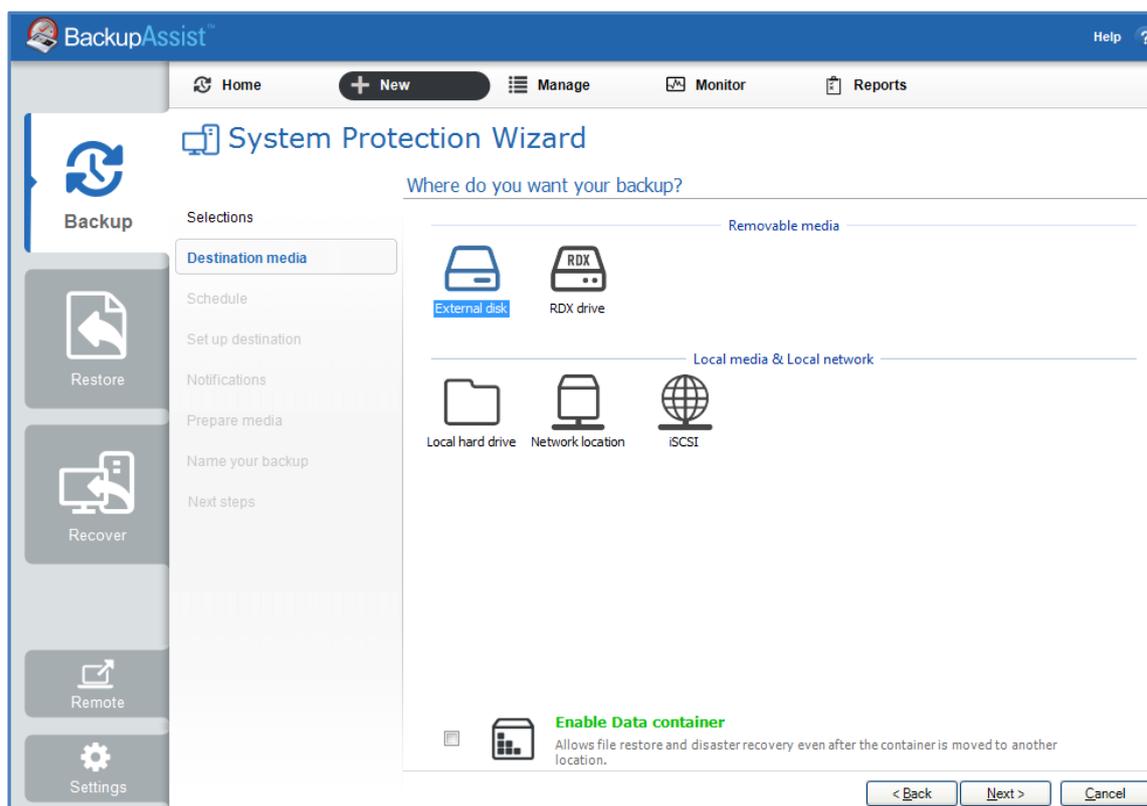


**Figure 2: Hyper-V intermediate (staging) disk selection**

**Note:** The entire contents of the staging disk will imaged to the backup destination each time the backup is run. Check that the disk is both appropriate and prepared for this step.

4. **Destination media:** The destination screen is used to select the type of media that you want to back your data up to. This step's name will change to the media type selected, when you click next.

The **Enable Data container**, option is available for the following destinations: *RDX drive*, *Local hard drive*, *Network location* and *External disk*. A Data container is a file that the backups will be stored inside of. To learn more, see the section about [Data containers](#).



**Figure 3: Destination media selection**

**Note:** System Protection backups on RDX drives cannot be used to restore individual files unless Data containers are used. This applies to Windows Server 2008R2 and later.

Select a device for your backup destination, and click **Next**.

5. **Schedule:** This screen is used to select when and how you would like the backup job to run, and how long you would like the backup to be retained for. A selection of pre-configured schedules, called schemes, will be displayed.
  - The schemes available will depend on the type of destination media selected in step 4.
  - Clicking on a scheme will display information about the schedule used.
  - The schedule can be customized after the backup job has been created.

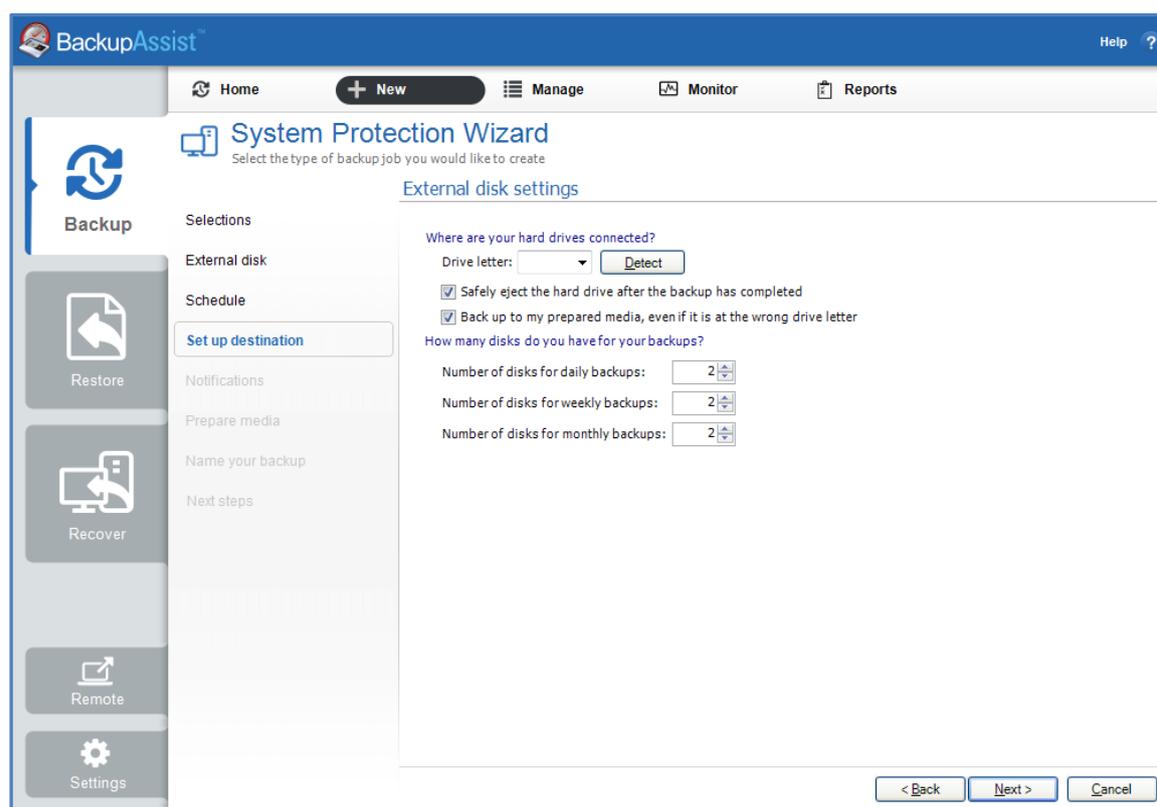
Select an appropriate scheme, and click **Next**.

6. **Set up destination:** This screen is used to configure the location of the media selected in step 4.
  - The options presented will change with the type of media selected.
  - If your media is removable, you can set the media to eject after the backup job has finished.

If your destination is a Data container, the container size and location is set using this screen.

- You will need to provide the destination path, the location where the container will be created.
- For an RDX or External disk destination, *Use all available space* will be selected by default. It is important to review this setting to ensure it is appropriate.
- For a Local hard drive and Network location, set the size manually by using the field provided, or select the *Use all available space* option.
- The size of a Data container cannot be changed once the backup job has run.
- The *Use all available space* selection will use all available space, up to 2TB.

Configure your backup destination, and click **Next**.



**Figure 4: System Protection for Hyper-V – Set up destination configuration**

- **Mail Server:** If you have not configured an SMTP mail server for BackupAssist, you will be prompted to provide those details after the backup destination step has been completed. See the [BackupAssist settings section](#) for guidance.
- 7. **Notifications:** Once a backup job has completed, BackupAssist can send an email to inform selected recipients of the result. This email notification can be enabled during the creation of a backup job, if the mail server has been configured.

To enable email notifications:

- a. Select, **Add an email report notification**.
- b. Enter recipients into the **Send reports to this email address** field.
- c. Enter recipients into the **Also send reports to this email address** field. You can then select the condition under which the email should be sent, using the drop-down box.

After the backup job has been created, you can modify the notifications by adding and removing recipients, setting additional notification conditions and including print and file notification types.

To learn more about notification options, see the [BackupAssist Backup tab whitepaper](#).

8. **Prepare media:** If you selected a portable media device as your backup destination (such as an RDX drive or an external drive) you will be given the option to prepare the media for BackupAssist. BackupAssist will write a label onto the media so that it can recognise what media has been attached, and determine if it is the correct media for your backup schedule.

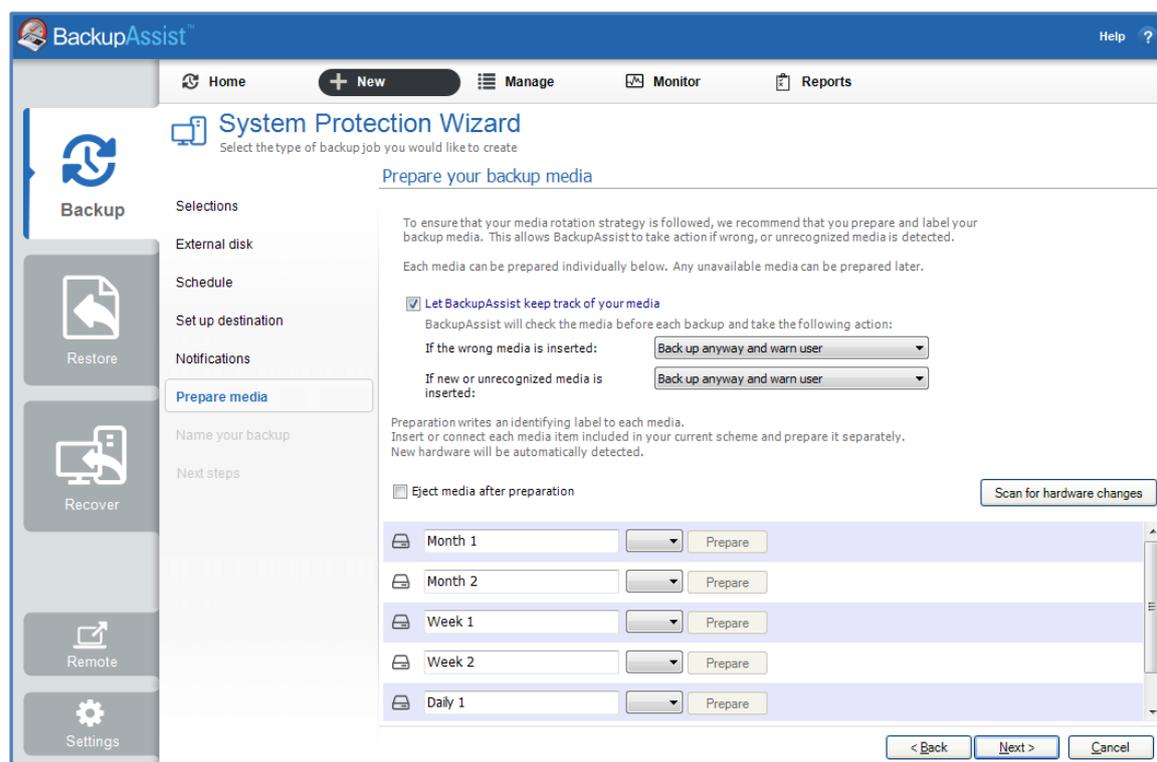
To enable media detection:

- Select, **Let BackupAssist keep track of your media.**
- Select what you would like BackupAssist to do, *if the wrong media is inserted.*
- Select what you would like BackupAssist to do, *if new or unrecognized media is inserted.*

BackupAssist will display all removable media that are currently attached, along with a text field and drive designation drop-down box, which can be used to provide a label for the media.

To prepare your media:

- Enter the name and drive designation to be used for each media device listed.
- Select **Prepare** for each media device listed.



**Figure 5: System Protection for Hyper-V – removable media preparation**

BackupAssist will write the label to the media so that it is able to recognize the media and ensure that the correct media is being used on the correct day.

- Name your backup:** Provide a name for your backup job, and click **Finish**.
- Next Steps:** If you are creating a backup of your entire system for use in a recovery, you can use this option to launch the RecoverAssist builder and create and bootable recovery media.

► **Your System Protection for Hyper-V backup job has now been created.**

**Important:** Once a backup job has been created, it should be reviewed and run using the *Manage* menu. See the section, [Hyper-V backup management](#), for more information.

**Important:** Once a backup job has been run and a backup created, a MANUAL test restore should be performed to ensure the backup is working as intended. See the section, [Restoring a Hyper-V backup](#).

**Important:** Hyper-V Granular Restore does not support mounting image backups that were backed up off a CSV

## 7. Restoring a Hyper-V backup



This section provides instructions on how to restore files from within a guest or host (granular) or an entire guest or host environment using a System Protection backup image.

A System Protection backup image can be used by two different restore tools:

- The **Hyper-V Granular Restore** tool, which can restore files from within a guest (virtual machine).
- The **Restore Console**, which can restore a guest image and files from within a host.

When performing a restore, the steps required to locate the backup are the same for both restore tools. This section explains how to locate the backup and is followed by sections explaining how to use the *Restore console* and how to use the *Hyper-V Granular Restore* tool, to restore from the backup.

To restore Hyper-V data from a **System Protection** backup, start BackupAssist and follow these steps:

1. Select the **Restore tab**

The *Restore tab* has a *Home page* and a *Tools menu*. The *Home page* is the default screen and the recommended starting point for performing a restore.

2. Select **Hyper-V** from the Home page.

3. The **Home page** will now display all backups that contain Hyper-V data.

Hyper-V image backups will be displayed twice for each backup location. First in a group with the prefix *Entire* – associated to the *Restore Console* tool, and then in a group with the prefix, *File* – associated to the *Hyper-V Granular Restore* tool.

- Select **the Restore console** - to restore a guest (virtual machine) or files from within the host – and go to the section below, [Hyper-V Guest & Host files restore](#).
- Select **the Hyper-V tool** – to restore individual files from a guest (virtual machine) – and go to the section below, [Hyper-V granular restore](#)

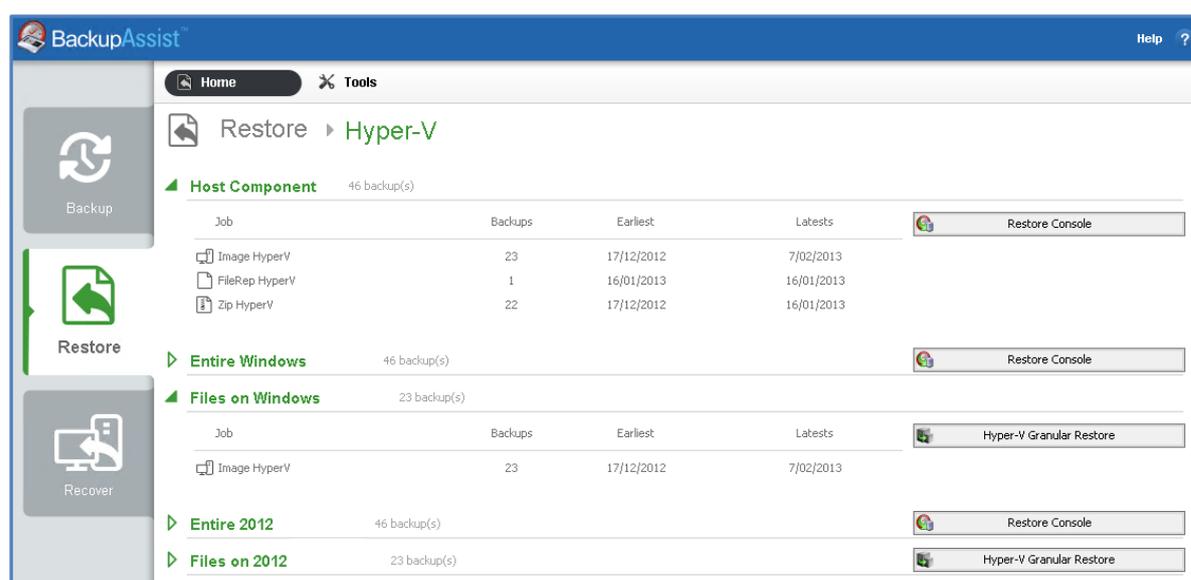


Figure 6: BackupAssist Restore screen - restore tool selection

## Hyper-V guest & host files restore



The following section explains how to use the BackupAssist *Restore Console*, to restore a *guest* (virtual machine) or files from within a Hyper-V *host* using a System Protection image backup.

### 4. Restore Console – backup and data selection

The *Restore Console* will open and load all of the backups that were listed on the *Home page*. The next step is to locate the data you want to restore, from the loaded backups.

The Restore Console provides two tools to locate your data:

- The **Browse** tab. Select this tab if you know the backup and date you wish to restore from, or if you need to restore an entire backup set.
  - a. Use the drop-down menu to choose the backup that you want to restore from.
  - b. Use the calendar to select the date you want to restore from.
  - c. Use the middle panes to expand the backup set.
  - d. Select the data to restore.
  - e. Click **Restore to** at the bottom right of the window.
- The **Search** tab. Select this tab to search all of the loaded backups for the data you want to restore. You can display data filtered by name, date, size and type, for all backups. The results can be compared (e.g. the dates of two files) to identify the correct data selection.
  - a. Enter your search term (The search accepts wild card searches, such as *\*.log* or *\*.doc*).
  - b. Select a filter/s if required.
  - c. Click the *Search* button.
  - d. Select the data to restore.
  - e. Click **Restore to** at the bottom right of the window.

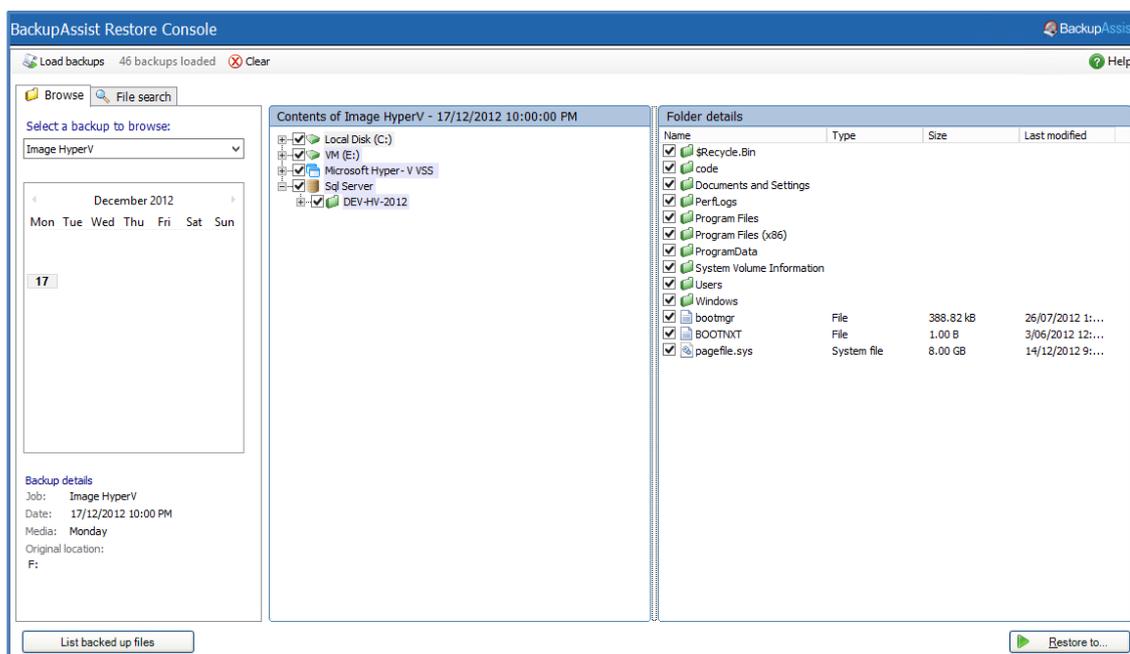
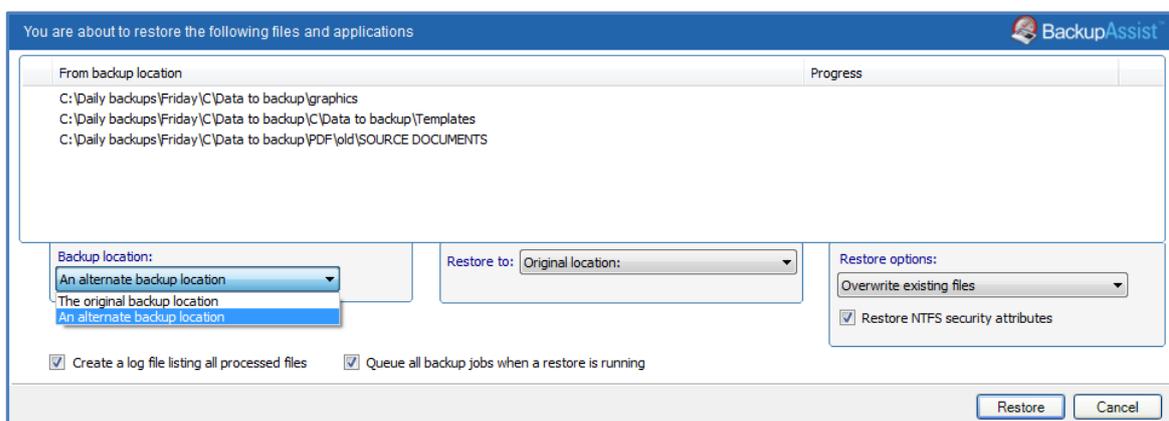


Figure 7: BackupAssist Restore Console – backup and data selection

If the backup is not present, or if you wish to load additional backups, select the **Load backups** option. Click **Load all known backups** to load all backup catalogues.

## 5. Restore Console – restore destination selection

When you select *Restore to*, a window will open showing the *Backup location*, the *Restore to* destination and the *Restore options*.



**Figure 8: BackupAssist Restore Console – restore destination**

- a. Review **Backup location:** Change the selection if the backup was moved after it was created.
- b. Review **Restore to:** Leave the *Original location* selected or chose an *Alternative path*.  
Restoring to an alternate location will use a minimal path. For example, restoring a single file to an alternate location will copy the file to the location without re-creating the original folder structure.
- c. Review the **Restore options:**
  - Select one of the following: *Overwrite all existing files*, *Do not overwrite existing files* or *Only overwrite older files*.
  - The option, *Restore NTFS security attributes* will be selected by default.
- d. Selecting *Create a log file listing all processed files*, will create a file that lists the success or failure of each file. The log is opened by selecting the log file's link in the backup report.
- e. *Queue all backup jobs when a restore is running*, is selected by default.
- f. Click the **Restore** button to restore your data.  
If BackupAssist cannot access the backup location you will be prompted to either connect the appropriate media or specify an alternate location where the backup can be found.  
The restore will run from the destination window and a **Report** link will appear once the restore has finished.
- g. Select **Done**.

► **Your Hyper-V restore has now been completed.**

**Important:** Only backups made with BackupAssist v5.3 or later will show up in the Restore Console.

**Important:** Refer to the [Restoring to a CSV environment](#) section, if you are restoring a guest to a CSV

## Hyper-V granular restore



The following section explains how to use the *Hyper-V Granular Restore* tool, to restore individual files from within a guest (virtual machine) using an image backup.

The BackupAssist *Hyper-V Granular Restore* tool will only run on 64-bit Windows 2008 / 2012 Servers or a standalone Hyper-V Server. The machine must also have the Hyper-V role, which can be added to most Windows 2008 / 2012 Servers, and is the default for a Hyper-V Server.

**!** Hyper-V Granular Restore does not support mounting image (VHD) backups that were backed up off a CSV

### 1. Select, Hyper-V Granular Restore

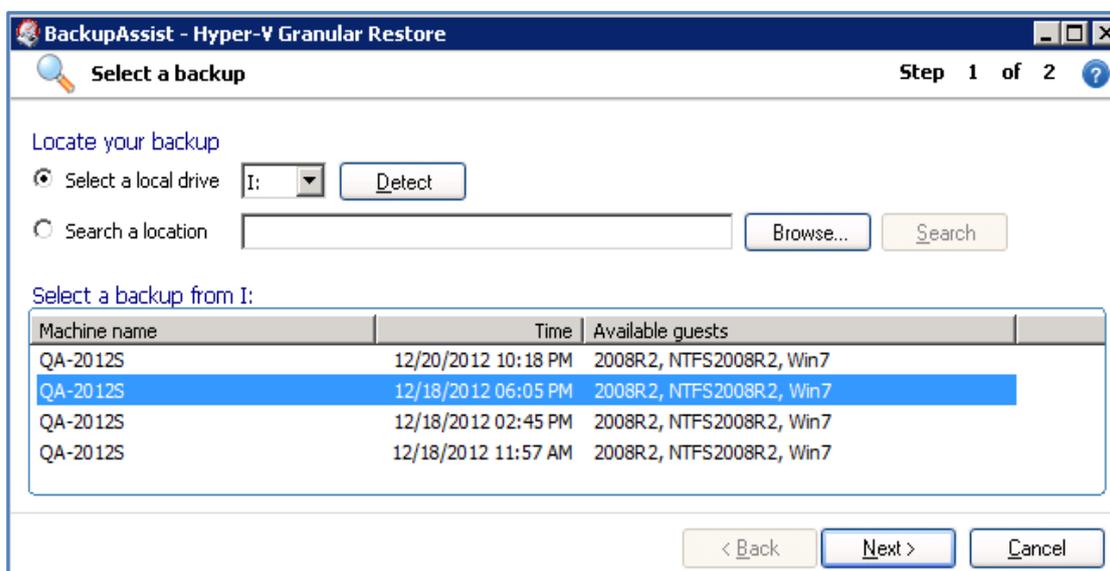
The tool will launch the *BackupAssist Image mounting tool*, which will open the *Hyper-V Granular Restore* console. The console is used to locate the image backup.

### 2. Locate your backup

Select a local drive that contains your System Protection VHD backup (Press *Detect* if the image does not display), or select *Search a location* and use the *Browse* or *Search* functions to locate your VHD backups.

Once the backups have been located, a list of VHD files will be displayed:

- The *Time* column can be used to help determine what backup to select.
- The *Available guests* column can be used to see what guests are inside the image backup.



**Figure 9: BackupAssist disk mounting tool - detected Hyper-V backups**

### 3. Select the host image to restore from, and click **Next**.

You will be presented with the **Mount volumes** screen, as shown in *Figure 11* below. The Mount Volumes screen is used to select the guest, within the VHD backup, that you want to restore data from.

### 4. Select the guest image, using the drop down list. The guest will appear as a selected item.

5. **Select the drive letter** to mount the guest image as.

6. Select the appropriate action from the drop down list.
  - Option 1 –**Mount selected volumes to drive letter.**
  - Option 2 –**Export volumes as VHD files.**

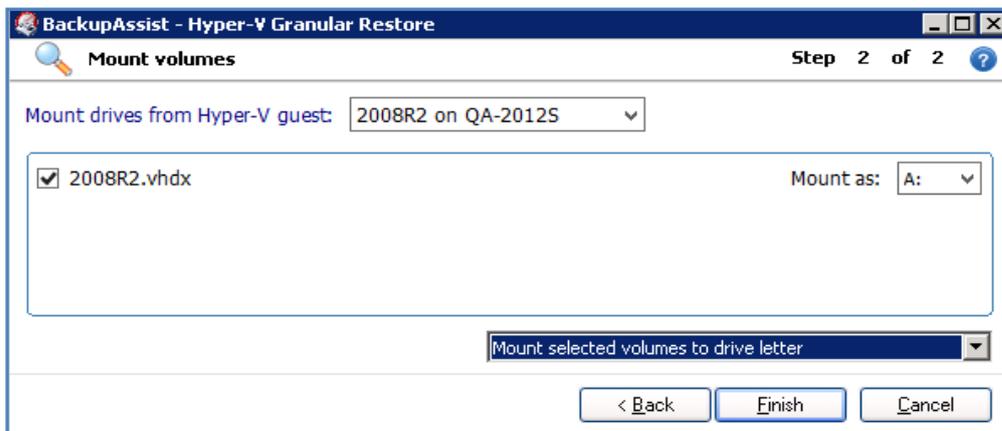


Figure 10: Selecting guest image to mount

7. **Option 1 –Mount selected volumes to drive letter.**

- The Mounting Disk progress bar will be displayed until the image is mounted.
- If there are two partitions, you will be asked to select which one.

Once the *guest* VHD is mounted, a new drive will appear on your computer with the drive letter specified on the guest selection screen.

- a. Open Windows Explorer to view the contents of the image.
- b. Copy the files and folders you want to restore (from the mounted VHD file) to a network location that the guest machine can access.
- c. Once you have finished copying data to a network location, you can then copy it back to the original guest machine.
- d. Once your data restoration is complete, click **Unmount** in the Hyper-V Granular Restore Console, and click **Done**.

**Option 2 –Export volumes as VHD files.**

Use this option if you would like to mount the image on another machine.

- a. Set the location that you would like to export the VHD files to in the field located at the bottom right corner.
- b. Click **Finish** to export the selected guest image.

A new drive will appear on the selected machine using the letter specified. Open Windows Explorer to view the contents of the image and follow the steps in option 1.

## Quick recovery from staging disk

When a backup of a Hyper-V in a CSV environment is created, an intermediate staging disc is used to create the image backup. If the guest VM needs to be recovered (or its image backup is rendered unusable) the intermediate staging disc can be used to recover the guest. Configure a new guest using the staging disk and the virtual machine will be operational again with minimal data loss. When you are ready to perform a migration back to the server, the differencing VHD stored on the staging disk along with the last back up from the staging disk can be merged together and installed on the server.

## 8. Hyper-V backup management

---



Once you have created a backup job, you can modify the settings and access advanced configuration options using the *Manage* menu.

To access the backup management screen:

1. Select the BackupAssist, **Backup tab**.
2. Select **Manage** from the top menu. A list of all backup jobs will be displayed.
3. Select the backup job you want to modify, and select **Edit**.
4. Select the required configuration item on the left. Key configurations are described below.

To learn more about the backup management options, see the [Backup tab whitepaper](#).

### Manually running a backup job

All new and modified backup jobs should be manually run to ensure they work as intended.

1. Select the backup job, and select **Run**.
2. You will be prompted to *Rerun a past backup* or to *Run a future backup now*.
3. When the backup job starts, the screen will change to the *Monitor* view.
4. Once the backup has been completed, select the *Report* button and review the results.

### Scheduling

Selecting *Scheduling* will display the **Scheduling options**. You can use this screen to change the default time and days of your scheme's daily backups. If you selected a scheme with archive backups (e.g. weekly, monthly), you can specify when each archive backup will run. Some backup types will have additional configuration options. The current scheme is shown, along with two pop-up menus: *Select a new schedule* and *Customize schedule*.

**Select a new Schedule:** This will display the pre-configured backup schemes that you chose from during the creation of your backup job. You can select a different scheme using this option.

**Customize schedule:** This selection can be used to modify each backup within your current schedule. The customizations available will depend on the type of backup and the type of backup media used.

For additional information on *Scheduling*, please refer to the whitepaper for the type of backup you are using (e.g. System Protection), and the [Backup tab whitepaper](#).

### Files and applications

**File and applications tab:** A new *System Protection* backup job will back up an entire disk or application. However, under the *Files and applications* menu item, you can modify your backup job by selecting specific files and folders, or individual components within a VSS application.

**Hyper-V Shared cluster volume options tab:** Changes the intermediate 4 backup location.

**Exclusions tab:** This is an additional tab where certain file types can be excluded from the backup. The exclusions can be applied to selected locations within the backup job. Use the *add* button to enter a *file type* and the *location* to apply the exclusion to. Pre-defined exclusions can also be added.

## 9. The Hyper-V Config Reporter

Best practice backup standards require you to document the configurations of every important server so you can recreate or reconfigure it in the event of a major disaster. With Hyper-V, if you need to migrate a guest machine from one host to another, or restore a guest to a new host, you need the configuration settings of the relevant guest(s) so you can manually create new guest machines that match the original configuration.

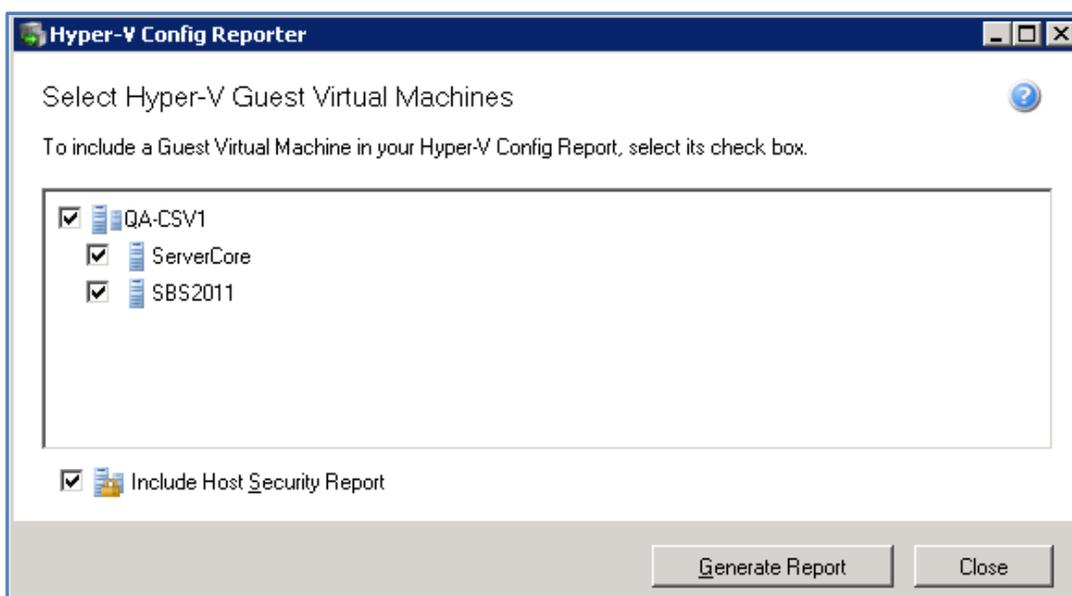
To fully document the setup of a Hyper-V Server, you need to include the setup of each guest machine and the configuration of the host. The BackupAssist Hyper-V Config Reporter (included with the *Hyper-V Granular Restore Add-on*) simplifies and automates this task by creating an HTML report of the configuration settings for each Hyper-V guest VM, and the Hyper-V host settings. The report contains everything needed to recreate the host, migrate a guest from one host to another, or restore a guest to a new host.

System Protection backup reports contain a **Recovery Options section**, which explains the BIOS, EFI and Hyper-V guest recovery options available for each System Protection backup.

To generate a report using the Hyper-V Config Reporter:

1. Run the Hyper-V Config Reporter from the Windows Start Menu on the Hyper-V host machine.

The Hyper-V Config Reporter will display a list of guests configured on the Hyper-V host.



**Figure 11: Hyper-V Config Reporter – guest selection**

2. To generate a report of your guest VM settings, select the individual guest from the list that you want, and click **Generate Report**.

Check **Include Host Security Report** if you want the report to include security and access settings that have been configured on the actual Hyper-V host.

3. A HTML report will then be created and displayed in a new window.

You can use the buttons at the top of the Hyper-V Config Reporter window to either print a copy of the report, save the report to a HTML file that can be opened with a web browser, or close the report window.

At the top of the report, as shown below, is a list of all the guest VMs selected during the previous step. If you click the Virtual Machine Name link of any guest in the list you will be directed to a list of settings for the latest running configuration for that guest VM.

 **Hyper-V VM Configuration Report**

Wednesday, December 19, 2012 4:48:54 PM

**HOST: QA-CSV1**

Virtual Machine Name	Operating System	Snapshots
 <a href="#">ServerCore</a>	Windows Server 2008 R2 Standard	0
 <a href="#">SBS2011</a>	Windows Small Business Server 2011 Standard	0

**ServerCore**

[▶ Latest running configuration](#)

**SBS2011**

[▶ Latest running configuration](#)

Under the list are details of each VM and its associated snapshots. You can click the link for any available snapshot to view the specific settings associated with that snapshot. Each VM included in the report will contain a full description of the VM settings for the latest running configuration at the top, and then a list of any further snapshots available underneath that, in date order.

**SBS2011 - Latest running configuration** ↑

Hardware	
Memory:	2048
BIOS settings	
Numlock:	false
Boot order:	1. CD 2. IDE 3. Legacy Network adapter 4. Floppy
Processor settings	
Number of logical processors:	1

The Host Security Report will be located at the very bottom of the overall report.

## Host Security Configuration - InitialStore.xml ↑

---

### Hyper-V Services

#### Role Definitions

Role Definition - Administrator	
General Settings	
Name	Administrator
Description	
Operation Definitions	
	Read Service Configuration-Authorizes reading configuration of the Virtual Machine Management Service
	Reconfigure Service-Authorizes reconfiguration of Virtual Machine Management Service

## 10. Support and Resources

### Contacting Technical Support

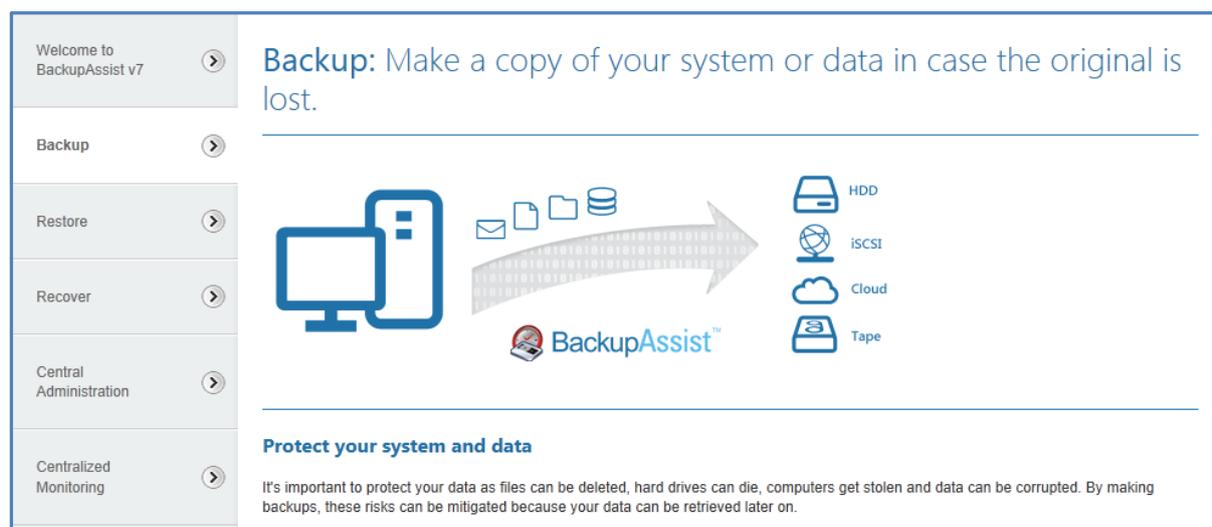
Should you have any questions regarding either BackupAssist or System Protection for Hyper-V, please email [support@backupassist.com](mailto:support@backupassist.com) and we will respond to you as soon as possible.

Similarly, if you have any suggestions for additional functionality in BackupAssist, or new products or add-ons, please also forward your feedback to [support@backupassist.com](mailto:support@backupassist.com)

### Learn more – The Welcome Screen

Each tab in BackupAssist includes a “Learn More” link on the tab’s **Home** page.

For example, selecting the **Learn more about Backup** link will open the **Welcome Screen** with the Backup introduction selected. This screen provides an overview of the tab’s functions and features, and links to documentation and resources.



**Figure 12: Backup tab –Welcome Screen**

