BackupAssist™ v8

Hyper-V Protection

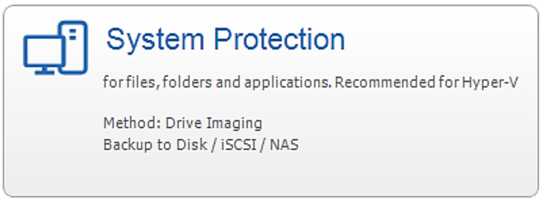
User guide

backupassist.com

Cortex I.T.

Contents

1. Hyper-V overview



System Protection

for files, folders and applications. Recommended for Hyper-V

Method: Drive Imaging
Backup to Disk / iSCSI / NAS

This guide explains how to create Hyper-V backups using System Protection, how to perform Hyper-V guest and host restores, and how to perform granular restores using the Hyper-V Granular Restore Add-on.

File Protection and File Archiving can also be used to back up Hyper-V environments, but System Protection is our recommended backup type for Hyper-V because it supports:

- Customized Hyper-V destination, CSV and Exchange Server detection steps
- Block level backups of a Hyper-V Server
- Incremental image backups, including fast incremental.
- Superior handing of large files.
- Bare-metal recovery

Documentation

The following documentation and articles are available as additional reading.

- For expert Hyper-V backup advice, see the Hyper-V backup implementation guide
- To learn about moving physical servers to virtual servers, see our P2V with Hyper-V article.
- If you're using Exchange Protection as your backup, you should read this Exchange backup article.
- For an overview of the difference between Hyper-V and VMware, see our Hyper-V VMware article.

Licensing

System Protection is a standard feature included with the BackupAssist, and requires a BackupAssist license once the initial trial period has expired. 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.

Hyper-V requirements

BackupAssist supports Hyper-V Servers (including CSV) with the following operating systems:

- Windows Server 2012R1/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 for BackupAssist Hyper-V protection

- Windows Server Backup. If Windows Server Backup is not installed, BackupAssist will provide a prompt to install it when the first backup job is created.
- In a CSV environment, BackupAssist must be installed and licensed on each host.
- For Windows Server 2008, the partition size of the disks being backed up should be less than 2TB.

The following Add-ons **DO support** guests backed up from CSV environments:

- The Exchange Granular Restore Add-on
- The Hyper-V Granular Restore Add-on

2. Hyper-V protection features

Windows 2012 R1/R2 Hyper-V support

Windows Server 2012 introduces the CSVFS format, which allows a cluster to differentiate CSV storage from NTFS storage. BackupAssist's support for these and other feature is listed below:

- BackupAssist can back up Hyper-V guests located on CSV storage using the CSVFS file system.
- BackupAssist supports SMB 3.0 servers as a CSVFS backup destination.
- BackupAssist does not support backups of CSVFS and NTFS locations in the same snapshot. E.g. It's not possible to back up a guest that uses CSV as well as a guest that uses an NTFS volume.
- BackupAssist supports Hyper-V Replica and can back up and restore a primary Hyper-V guest.

Custom Hyper-V backup job steps

When you use BackupAssist System Protection to create a Hyper-V backup job, you will be presented with the following Hyper-V specific, setup screens.

Hyper-V data selection

The data selection screen is focused on the Hyper-V guests, rather than a generic bare-metal backup. This makes it easier to select Hyper-V guests and their host, and create a dedicated Hyper-V backup.

Exchange VM detection

System Protection Hyper-V backup jobs have an Exchange authentication information step. Providing Exchange authentication information allows BackupAssist to detect what guests have an Exchange Server, and list the EDB files available for each guest when you perform an Exchange Granular Restore.

CSV configuration

If you have a CSV environment, a staging configuration step is used to define a staging location. This location is used to put your guests and host into a single image, even if they are on different volumes.

Hyper-V restore options

A System Protection backup can be used to restore Hyper-V data using the following tools.

BackupAssist Restore Console

You can use the console to restore a host and its guests, selected guests or data from inside the host.

Hyper-V Granular Restore console

The Hyper-V Granular Restore console is enabled when you purchase the Hyper-V Granular Restore Add-on. The Add-on allows you to restore individual files from inside of a guest. The backup can contain multiple guests, and the Add-on allows you to mount one and restore specific files.

Exchange Granular Restore console

The Exchange Granular Restore console is enabled when you purchase the Exchange Granular Restore Add-on. The Add-on allows you to restore mail items from an Exchange Server that is installed on a guest. This requires both the Exchange Granular Restore and the Hyper-V Granular Restore Add-ons.

3. Hyper-V best practice backups

Backing Hyper-V virtual machines virtual machines, can become complicated once you factor in host data, volumes, domains, disks, VSS writers, services and the resulting issues that can arise. To keep the backups of your virtual machines as simple and robust as the environments themselves, we've put together a list of 10 tips for best practice Hyper-V backups.

1. Do not install other roles or applications on your Hyper-V host.

Your physical Hyper-V host server should only have one function, to be the Hyper-V host server. It should not double as a file server, a DNS server or, even worse, an application server. Any non-Hyper-V software and data should be on another physical server or one of the Hyper-V guests.

If you don't follow this advice, you can complicate host level backups and affect the stability of the host server itself. Any problem with another role or application on the Hyper-V host can impact the guests. Even something as simple as a patch to an application could require a physical server reboot, and cause an outage for all of your Hyper-V guests (VMs) and the services they provide.

2. Only assign a single role or application to each guest

Each Hyper-V guest (VM) should only have a single role or application. It's easy enough to make another guest, and dedicated environments are what make virtual machines so great.

For backups, having only one role or application per guest makes it easier to:

- Recover guests and services in a managed way.
- Allocate backup agents and licenses
- Perform granular restores of data inside of Hyper-V guests.

3. Focus on guest only Hyper-V backups

The Hyper-V host provides the platform, architecture and processes required to support and maintain your Hyper-V guests (VMs). Although it's good to have a bare-metal backup of the entire physical server, backups of just the Hyper-V guests can also be very useful as they contain all the data you need and use less space. For a recovery, you can just reinstall the Hyper-V Server and use the backup to add the guests back. A mix of weekly full-metal archive backups and daily "guest only" backups can provide a good balance.

4. Enable Hyper-V integration services

Backup software can use a VSS snapshot to maintain a copy of data that has changed during the backup, so that all of the data in the backup reflects the data as it was at a single point in time – this is called crash-consistent. Application-consistent means a VSS-Aware application checks its own files in the VSS snapshot to make sure they are correct. For example, information in memory and uncompleted database transactions are included in the snapshot, making it more accurate and consistent. This is critical, especially for applications like Exchange and SQL.

Without *Hyper-V Integration Services* installed, a Hyper-V guest (VM) will not be aware of the backup job so you will only get a crash-consistent backup. When you install the *Hyper-V Integration Services* on the host, and enable it on the guest, the host and guest VSS writers can work together to create online, application-consistent backups of applications like Exchange and SQL, inside the Hyper-V guest.

5. Run the backup on the Hyper-V host server, not the guest

The easiest way to protect Hyper-V guests is to install your backup software on the Hyper-V host (physical server) and back up the guests from there. This way you can back up multiple guests using the same backup job, and have those guests in a single backup. This will also save money, because you only need one backup license. Some backup solutions may require a backup agent on each guest but BackupAssist only requires a single host license.

As long as you have Hyper-V integration services installed, the Hyper-V VSS writer on the host, where the backup is running, can communicate with an application (Exchange, SQL) VSS writer on the guest, so that you have application-consistent backups of all guests - in a single backup.

To learn more about the VSS process, see our virtual shadow copy article.

6. Do not back up a CSV device directly

If your guests use a cluster shared volume (CSV), do not back up the CSV device directly because the Hyper-V Server's VSS writer will not be involved. Back up the Hyper-V Server so that the Hyper-V VSS writer is used to make application-consistent backups of data on the cluster shared volume.

7. Don't put the Hyper-V host on the same domain as the guests

This safeguard applies when one of your Hyper-V guests (VMs) has the role of domain controller. If that domain controller guest goes down and the host is on the same domain, you may not be able to log into your Hyper-V Server.

8. Backup the whole volume

When performing a Hyper-V image backup (i.e. BackupAssist System Protection backup), it's best to back up the whole volume. This can improve the performance of incremental image backups, and it makes the backups faster.

If you follow this best practice, and backup the whole volume, you should have your non-production guests (VMs) on a different volume, so that you can exclude them from the backup. If you mix guest categories or guest files across volumes, both backups and restores become more complicated and less efficient.

9. Keep system and guest data on separate volumes.

The volume you install Microsoft Hyper-V Server onto, and the volume used by the physical server's operating system, should not be used to store Hyper-V guest data (VHDs). For example, if your physical server uses C: drive, your Hyper-V guests should not. They should have their own volumes, and those volumes should not contain system files, such as the physical server's swap file. This is important for performance and to remove conflicts. It's also important for backups because you want to be able to make "guest only" backups using complete volumes.

10. Use fixed virtual disks

The types of disks you use can have an impact on your Hyper-V host server's performance and data integrity, both of which are important for backups. For this reason, your Hyper-V host server should use fixed virtual disks. Pass-through disks add complexity and don't allow VM snapshots or Hyper-V replica, and dynamic and differencing disks add a performance and space overhead. Fixed disks enable better performance and data integrity. This means better backups.

4. 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.

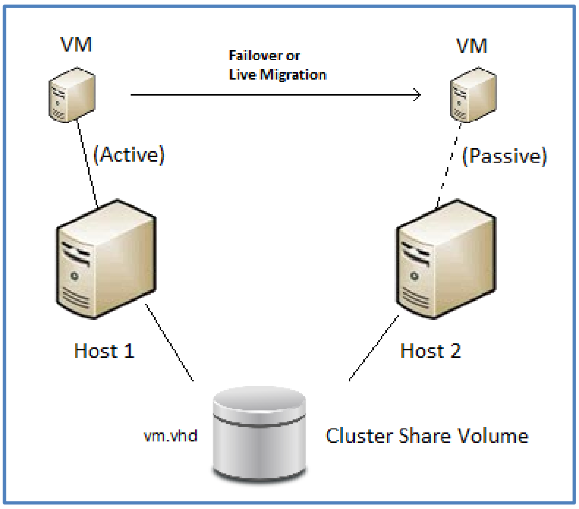
Windows Settings

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.*

5. Hyper-V in a CSV environment

Cluster Share Volume (CSV) is Microsoft's implementation of server clustering, and designed for use with Hyper-V. CSV provides a shared disk that can be used by any guest in the cluster. This means a guest can be moved within the disk cluster, and guests can share the same physical disk.



When stored in a CSV, a guest's files present as a shared resource between the hosts. As the CSV's files are shared, access must be coordinated so that only one host accesses a guests 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 CSV backup 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 allows BackupAssist time to initialize and coordinate its access to the CSV. BackupAssist will delay the second job so that it will not commence until the first job has completed.

CSV backup considerations:

- BackupAssist v8 supports Hyper-V CSV on both Windows Server 2008R2 and 2012R1/R2 machines.
- During the backup process, the guests are copied to an intermediate staging area, from where they are backed up into a single image. The staging disk acts as a cache for the backup job.
- The staging disk must be a local disk and it is overwritten each time a backup is run.
- The staging disk must be able to hold every guest being backed up from all CSVs used to store the guests' files (a copy of every file). The staging disk must be used for this purpose only.
- 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.

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.

6. Creating a Hyper-V backup

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

Launch BackupAssist and follow the steps outlined below:

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

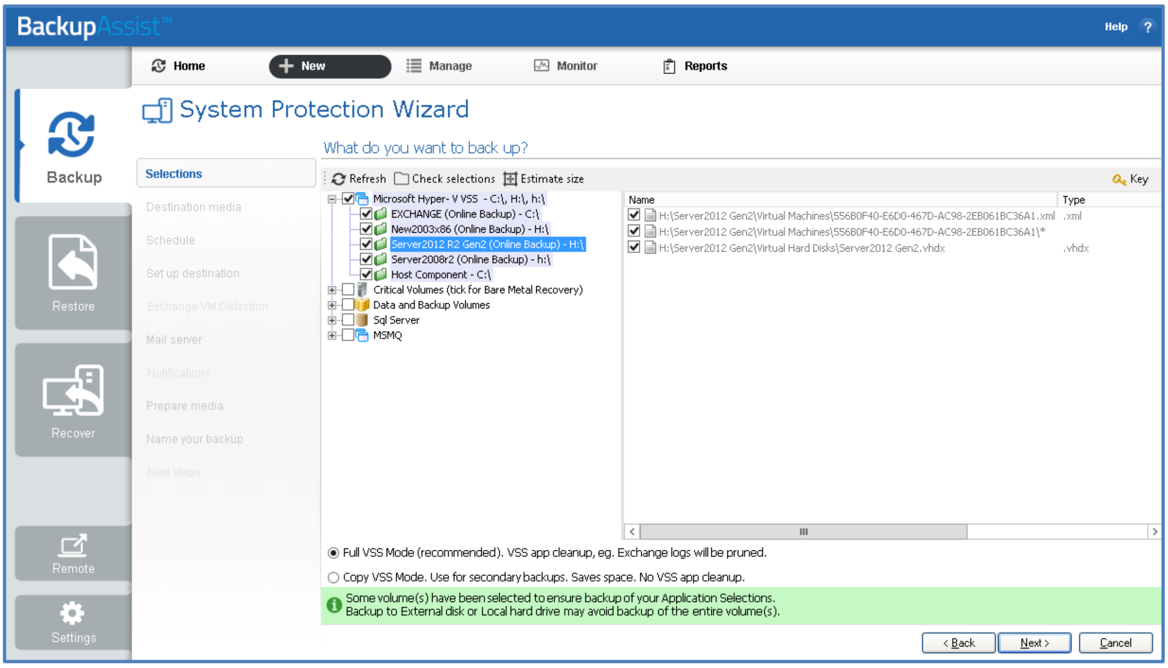
   If this is the first time you have created a backup job, you will be asked to provide a *Backup user identity* if one has not been defined. See the section above, BackupAssist settings, for guidance.

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

   If you want a full Hyper-V Server backup, select *Microsoft Hyper-V VSS* and the required data will be ticked. If this is not selected, failover or migrated guests may not be backed up. The *Microsoft Hyper-V VSS* selection is highly recommended for CSV environments.

   Selecting *Critical Volumes* will create a backup for a full system recovery. If you only have a backup of the guests, you can still restore any of those guests in full, to a rebuilt Hyper-V Server.

   Select the Hyper-V environments that you want to back up.



What do you want to back up?

- ☑ Microsoft Hyper- V VSS - C:\, H:\, h:\
  - ☑ EXCHANGE (Online Backup) - C:\
  - ☑ New2003x86 (Online Backup) - H:\
  - ☑ Server2012 R2 Gen2 (Online Backup) - H:\
  - ☑ Server2008r2 (Online Backup) - h:\
  - ☑ Host Component - C:\
- ☐ Critical Volumes (tick for Bare Metal Recovery)
- ☐ Data and Backup Volumes
- ☐ Sql Server
- ☐ MSMQ

Name	Type
☑ H:\Server2012 Gen2\Virtual Machines\556B0F40-E6D0-467D-AC98-2EB061BC36A1.xml	.xml
☑ H:\Server2012 Gen2\Virtual Machines\556B0F40-E6D0-467D-AC98-2EB061BC36A1\*	
☑ H:\Server2012 Gen2\Virtual Hard Disks\Server2012 Gen2.vhdx	.vhdx

● Full VSS Mode (recommended). VSS app cleanup, eg. Exchange logs will be pruned.

○ Copy VSS Mode. Use for secondary backups. Saves space. No VSS app cleanup.

Some volume(s) have been selected to ensure backup of your Application Selections.
Backup to External disk or Local hard drive may avoid backup of the entire volume(s).

Figure 1: BackupAssist Hyper-V backup – Selections screen

Select Full VSS Mode or Copy VSS Mode.

- *Full VSS Mode* is enabled by default and will allow a VSS log cleanup. If you select one guest, Full VSS Mode will back up all guests on the same volume.
- *Copy VSS Mode* can be used to select individual guests and save backup space, but should only be used for a secondary backup.

To learn more about VSS, see our VSS blog article.

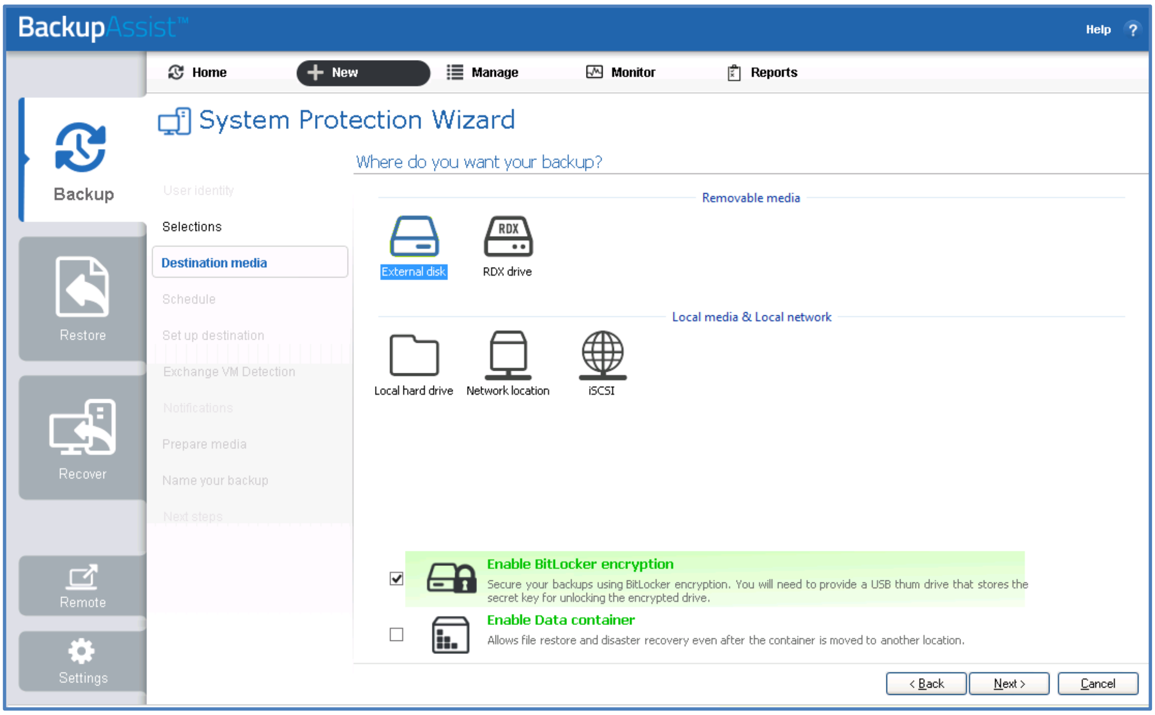
4. **Destination media:** The destination screen is used to select the type of media that you want to back your data up to. This step's name will change to the media type selected, when you click next.

   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. The Data container is created on the destination media and each time the backup jobs runs, the container is mounted and treated as a local disk. On Windows 2008R2 and later - backups on RDX drives cannot be used to restore individual files unless Data containers are used.

   Before using Data containers, it is important to read our Data container resource.

   The **Enable BitLocker encryption** option is available for Windows servers that have BitLocker installed. BitLocker can be used to encrypt *External disk* and *RDX drive* backup destinations. This protects the drives from unauthorized access. When enabled, BitLocker will encrypt and lock each drive, and assign an encryption key which can be used to unlock and access the drive.

   Before using BitLocker, it is important to read our BitLocker resource page



System Protection Wizard

Where do you want your backup?

☑ **Enable BitLocker encryption**
Secure your backups using BitLocker encryption. You will need to provide a USB thum drive that stores the secret key for unlocking the encrypted drive.

☐ **Enable Data container**
Allows file restore and disaster recovery even after the container is moved to another location.

Figure 2: Destination media selection

   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.

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

   To learn more about System Protection schedules, see to the Backup management section below.
   To learn more about scheduling options and customizations, see the Backup tab user guide.

6. **Set up destination:** This screen is used to configure the media selected in step 4.

    - The options presented will change with the type of media selected.
    - For removable media, a *Prepare media* step will be displayed later in the setup process.

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

    - The size of a Data container cannot be changed once the backup job has run.
    - For an *RDX* or *External disk* destination, *Use all available space* will be selected by default.
    - 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 *Use all available space* selection will use all available space, up to 2TB.

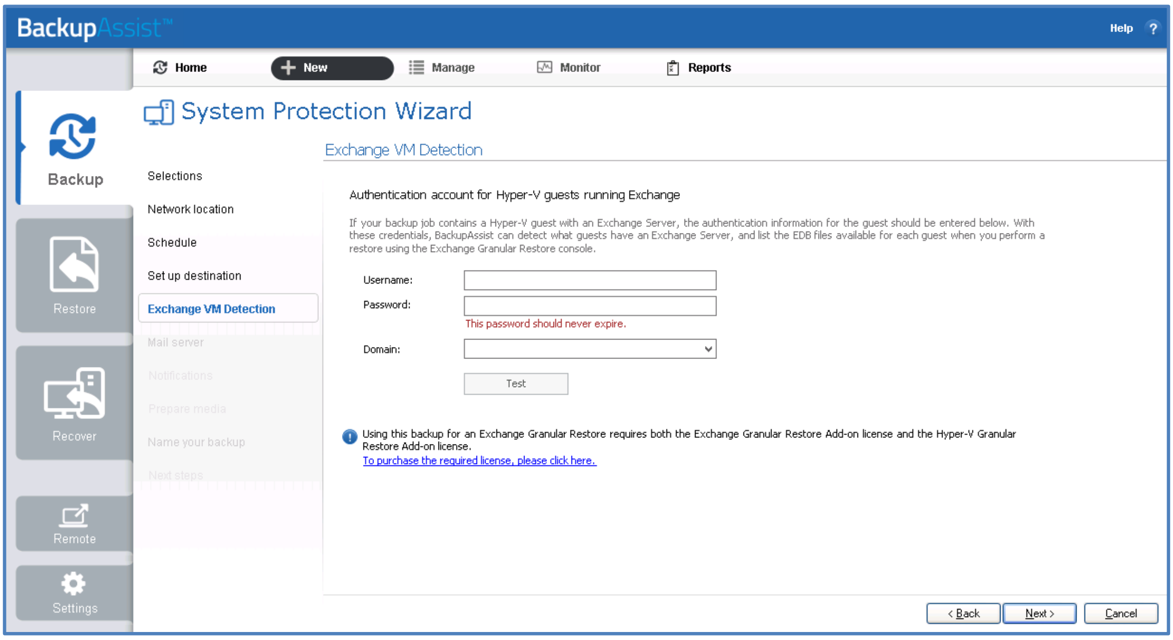
    Configure your backup destination, and click **Next**.

7. **Exchange VM detection**

    If you have a Hyper-V guest with an Exchange Server, use this step to provide authentication information for that guest. With this information, BackupAssist can see what guest contains the Exchange Server, even if it is on a different domain to the host. BackupAssist can then create a backup catalogue of the Exchange Server's EDB files that the Exchange Granular Restore Add-on can use to perform a granular restore.

    If more than one guest has an Exchange Server, then each guest with an Exchange Server should be on the same domain, and accessible using the same account. This account's username, password and domain is entered in the Exchange VM detection screen.

> A granular restore of Exchange data from a Hyper-V guest, requires both *Hyper-V Granular Restore Add-on* (which will run automatically as part of the restore) and the *Exchange Granular Restore Add-on* licenses.



System Protection Wizard

Exchange VM Detection

Authentication account for Hyper-V guests running Exchange

If your backup job contains a Hyper-V guest with an Exchange Server, the authentication information for the guest should be entered below. With these credentials, BackupAssist can detect what guests have an Exchange Server, and list the EDB files available for each guest when you perform a restore using the Exchange Granular Restore console.

Username:

Password:

This password should never expire.

Domain:

Test

Using this backup for an Exchange Granular Restore requires both the Exchange Granular Restore Add-on license and the Hyper-V Granular Restore Add-on license.

To purchase the required license, please click here.

Figure 3: Hyper-V - Exchange VM detection

Enter the following Exchange VM Detection authentication information, and select **Next**.

- The **Username** and **Password** of an account that has access to the guest/s running Exchange.
- The **Domain** of the guest/s running Exchange.

8. **Hyper-V CSV options**

The *Hyper-V CSV options* step is used to configure an intermediate backup location, called a staging disk. System Protection uses the staging disk to put the Hyper-V host and its guests into a single image backup (VHD file), even if they are on different volumes.

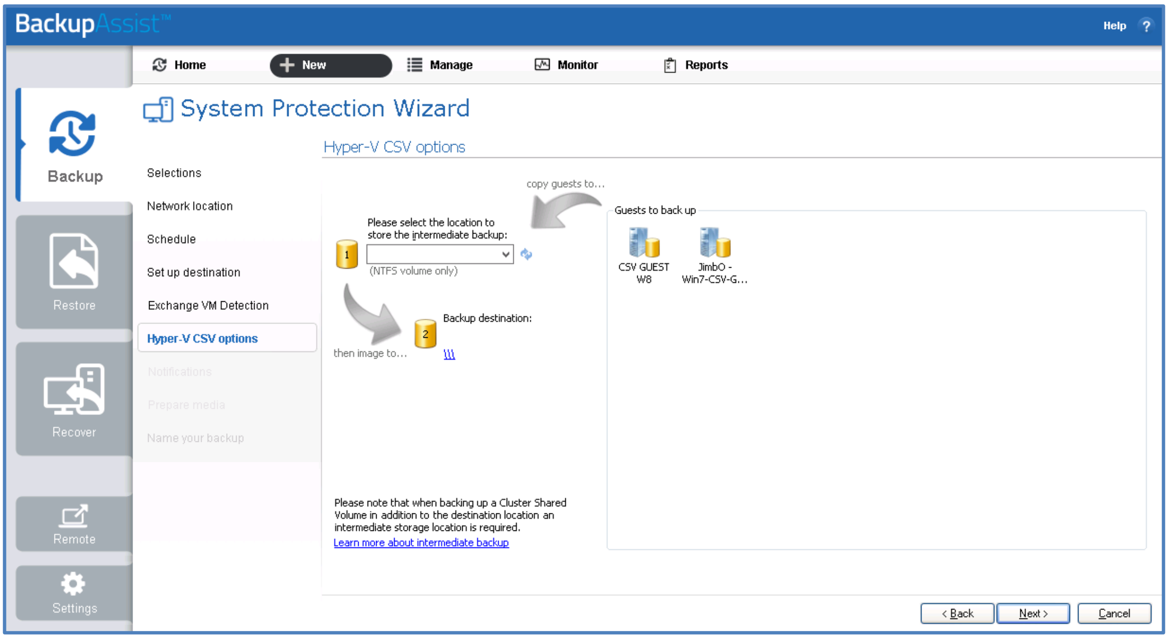
This step will only appear if you have Cluster Shared Volumes (CSV) environments.

The staging drives available and the *Backup destination* shown are based on the selections made during the *Set up* destination step.

Hyper-V CSV staging disk considerations:

- 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 staging disk.

Enter the drive to be used for the intermediate backup (staging disk), and click **Next**.



System Protection Wizard

Hyper-V CSV options

Please select the location to store the intermediate backup:

(NTFS volume only)

Backup destination:

\\\

Guests to back up

Please note that when backing up a Cluster Shared Volume in addition to the destination location an intermediate storage location is required.

Learn more about intermediate backup

Figure 4: Hyper-V intermediate (staging) disk selection

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. For more information, refer to the Backing up a CSV environment section of this user guide.

9. **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.

10. **Prepare media:** If you selected a removable media as your backup destination, you will be given the *Prepare media* option. 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:

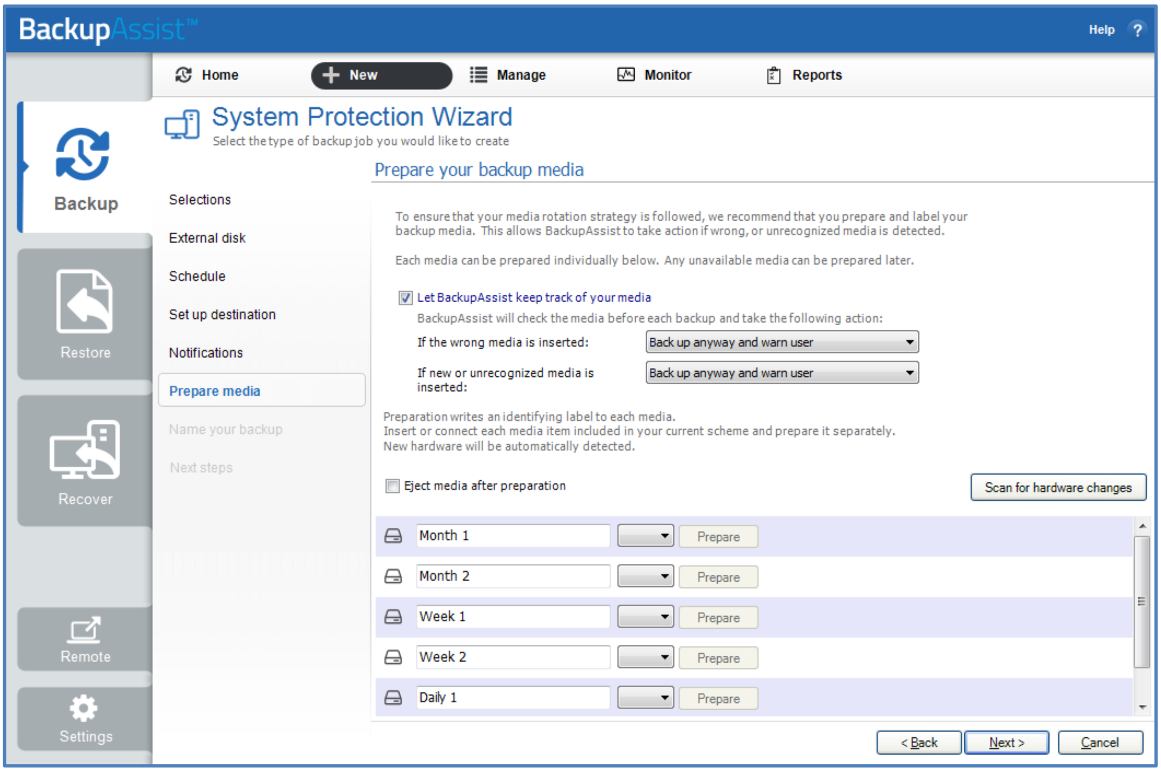
    a. Select, **Let BackupAssist keep track of your media.**
    b. Select what you would like BackupAssist to do, *if the wrong media is inserted*.
    c. Select what you would like BackupAssist to do, *if new or unrecognized media is inserted*.

    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:

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

    If you have selected **BitLocker encryption,** use the **prepare** media button to indicate what drives are to be encrypted. The encryption process will be initiated by the final backup job creation step.



System Protection Wizard

Select the type of backup job you would like to create

Prepare your backup media

To ensure that your media rotation strategy is followed, we recommend that you prepare and label your backup media. This allows BackupAssist to take action if wrong, or unrecognized media is detected.

Each media can be prepared individually below. Any unavailable media can be prepared later.

☑ Let BackupAssist keep track of your media

BackupAssist will check the media before each backup and take the following action:

If the wrong media is inserted: Back up anyway and warn user

If new or unrecognized media is inserted: Back up anyway and warn user

Preparation writes an identifying label to each media.
Insert or connect each media item included in your current scheme and prepare it separately.
New hardware will be automatically detected.

☐ Eject media after preparation

Month 1
Month 2
Week 1
Week 2
Daily 1

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.

11. **Name your backup:** Provide a name for your backup job, and click **Finish**.
12. **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.

- If you selected *BitLocker encryption*, the encryption can process will begin. When you select finish, the BitLocker encryption tool will open and encrypt the prepared drives. If an unencrypted drive is used for a BitLocker backup job, the job will fail.

To learn about the BitLocker encryption tool, see our BitLocker resource page

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

Important: Once the *backup* has been created, it should be checked. You can check the backup by performing a manual test restore, or using the Backup Verification feature. A manual restore is the only way to fully test a backup, and regular manual restores should be part of your backup solution.

7. Restoring a Hyper-V backup

This section provides instructions on how to restore a Hyper-V guest, files from within a guest and files from within a host.

A Hyper-V backup can be restored using the following 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 and files from within a host.
- The **Exchange Granular Restore Console** can restore mail items from an Exchange Server that is installed on a guest. This restore process also uses the Hyper-V Granular Restore Add-on.

When performing a restore, the steps required to locate the backup are the same. 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 perform the restore.

To restore from a Hyper-V 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.

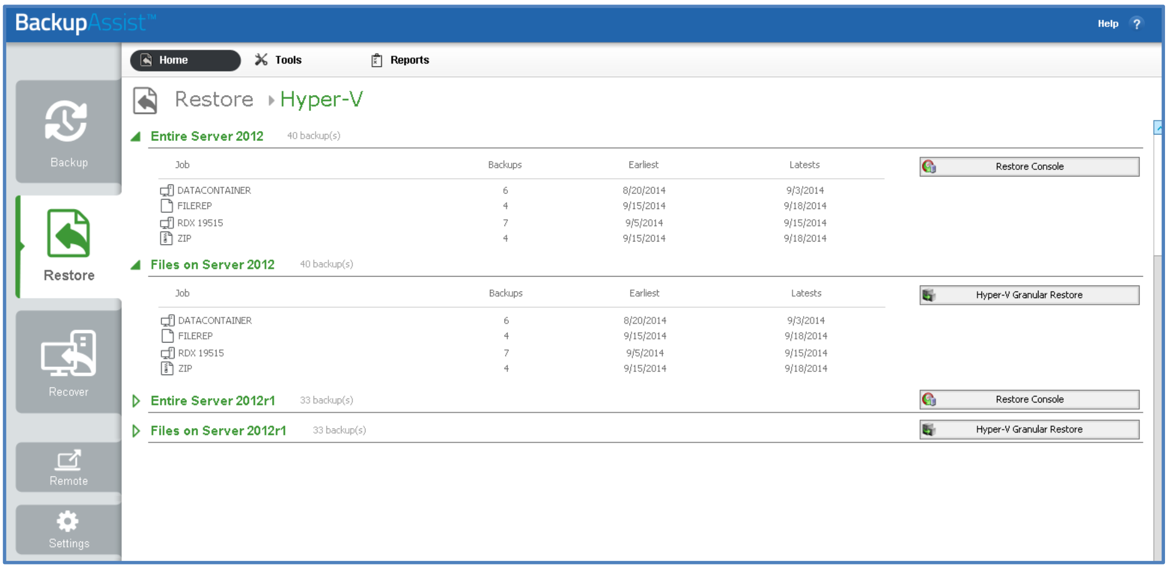
   The Home page will display all backups for active backup jobs that contain Hyper-V data.

3. Select the **Restore console** or **Hyper-V Granular Restore**

   Hyper-V image backups will be displayed twice. 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.

   If you selected **Restore console** go to the section below, BackupAssist Restore Console

   If you select **Hyper-V Granular Restore** go to the section below, Hyper-V Granular Restore



Entire Server 2012 40 backup(s)

Job	Backups	Earliest	Latests
DATACONTAINER	6	8/20/2014	9/3/2014
FILEREP	4	9/15/2014	9/18/2014
RDX 19515	7	9/5/2014	9/15/2014
ZIP	4	9/15/2014	9/18/2014

Files on Server 2012 40 backup(s)

Job	Backups	Earliest	Latests
DATACONTAINER	6	8/20/2014	9/3/2014
FILEREP	4	9/15/2014	9/18/2014
RDX 19515	7	9/5/2014	9/15/2014
ZIP	4	9/15/2014	9/18/2014

Entire Server 2012r1 33 backup(s)

Files on Server 2012r1 33 backup(s)

Figure 6: BackupAssist Restore screen - restore tool selection

BackupAssist Restore Console

Files & Folders

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.

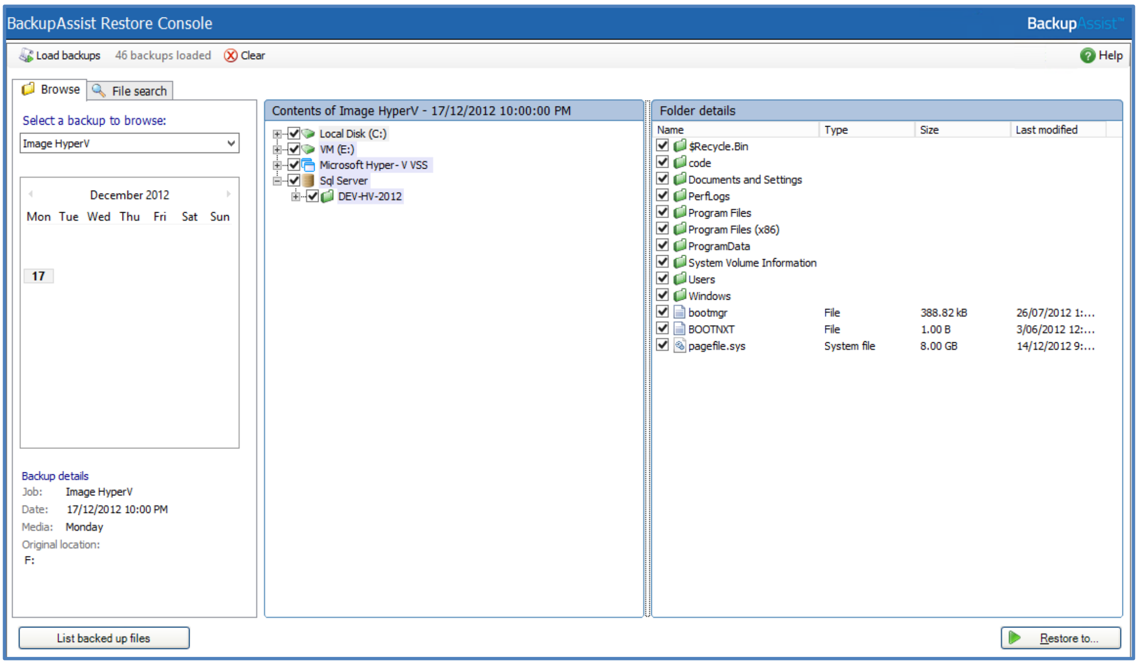


Image HyperV

Contents of Image HyperV - 17/12/2012 10:00:00 PM

- ☑ Local Disk (C:)
- ☑ VM (E:)
- ☑ Microsoft Hyper- V VSS
- ☑ Sql Server
  - ☑ DEV-HV-2012

Folder details

Name	Type	Size	Last modified
☑ $Recycle.Bin			
☑ code			
☑ Documents and Settings			
☑ PerfLogs			
☑ Program Files			
☑ Program Files (x86)			
☑ ProgramData			
☑ System Volume Information			
☑ Users			
☑ Windows			
☑ bootmgr	File	388.82 kB	26/07/2012 1:...
☑ BOOTNXT	File	1.00 B	3/06/2012 12:...
☑ pagefile.sys	System file	8.00 GB	14/12/2012 9:...

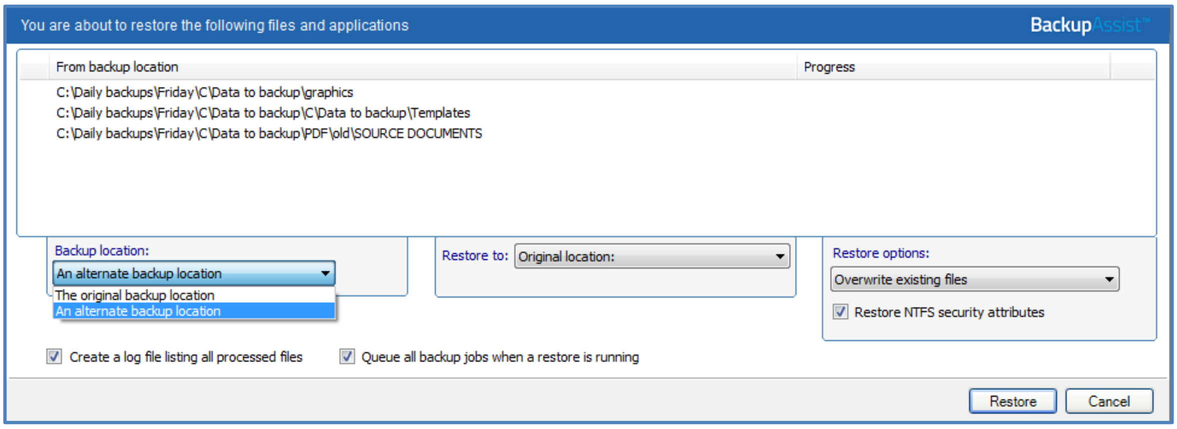
Backup details
Job: Image HyperV
Date: 17/12/2012 10:00 PM
Media: Monday
Original location:
F:

Figure 7: BackupAssist Restore Console – backup and data selection

If you wish to load backups for deleted backup jobs and for other backup groupings on the Home page, select *Load backups* and then *Load all known backups*.

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*.



You are about to restore the following files and applications

From backup location	Progress
C:\Daily backups\Friday\C\Data to backup\graphics	
C:\Daily backups\Friday\C\Data to backup\C\Data to backup\Templates	
C:\Daily backups\Friday\C\Data to backup\PDF\old\SOURCE DOCUMENTS	

Backup location: An alternate backup location ▾
- The original backup location
- An alternate backup location

Restore to: Original location: ▾

Restore options: Overwrite existing files ▾

☑ Restore NTFS security attributes

☑ Create a log file listing all processed files

☑ Queue all backup jobs when a restore is running

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 console

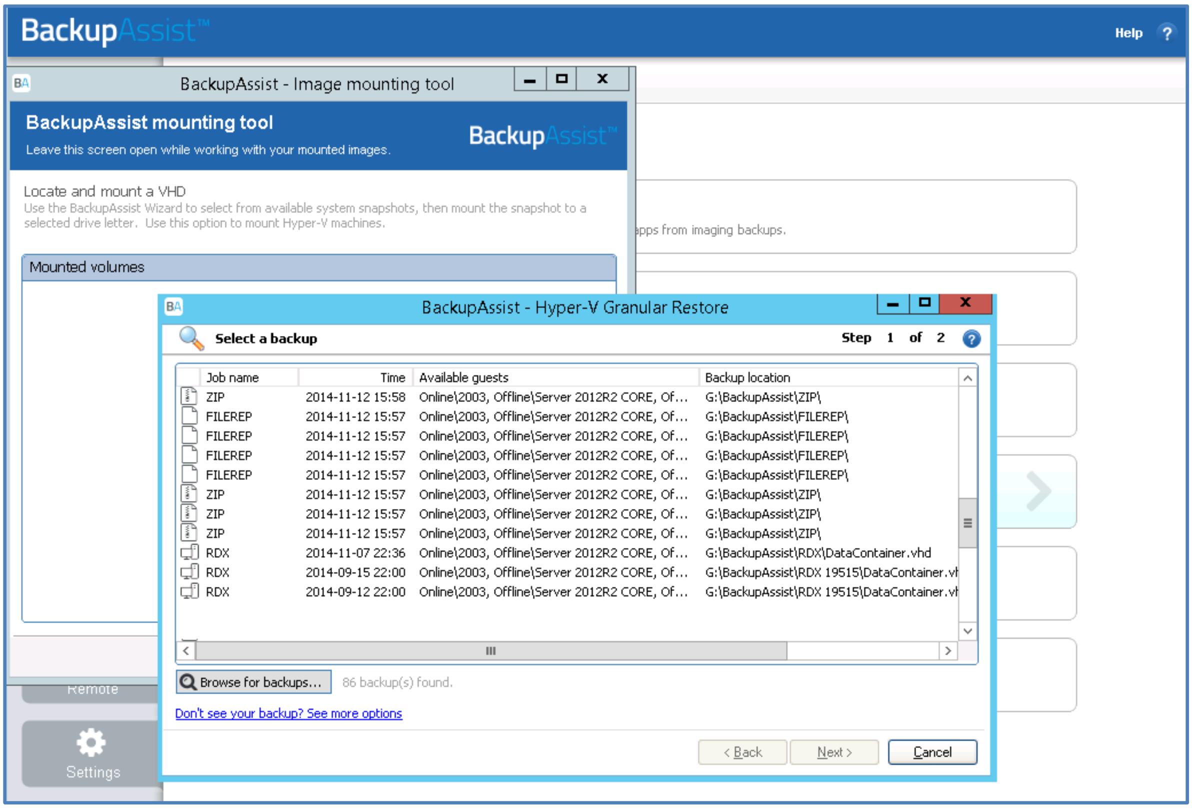
The following section explains how to use the *Hyper-V Granular Restore* tool, to restore individual files from within a guest (virtual machine) using a System Protection, File Protection or File Archiving backup.

The BackupAssist *Hyper-V Granular Restore* tool will run on 64-bit Window 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.

4. Select **Hyper-V Granular Restore**

   This will launch the *BackupAssist Image mounting tool*, which opens the *Hyper-V Granular Restore* console. The console will display your Hyper-V backups.

   - The *Time* column can be used to help determine what backup to select.
   - The *Available guests* column displays the guests that are inside the backup.
   - The *Don't see your backup*, option allows you to manually search for a connected backup.
   - You can use the *Browse for backups* button to locate other backup catalogues. This allows you to restore from backups that are not available on the local system. This feature applies to backups created with BackupAssist v8.2.1 and later.


BackupAssist™
Help ?
BackupAssist - Image mounting tool
BackupAssist mounting tool
Leave this screen open while working with your mounted images.
BackupAssist™
Locate and mount a VHD
Use the BackupAssist Wizard to select from available system snapshots, then mount the snapshot to a selected drive letter. Use this option to mount Hyper-V machines.
Mounted volumes
apps from imaging backups.
Remote
Settings
BackupAssist - Hyper-V Granular Restore
Select a backup
Step 1 of 2

Job name	Time	Available guests	Backup location
ZIP	2014-11-12 15:58	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\ZIP\
FILEREP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\FILEREP\
FILEREP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\FILEREP\
FILEREP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\FILEREP\
FILEREP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\FILEREP\
ZIP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\ZIP\
ZIP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\ZIP\
ZIP	2014-11-12 15:57	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\ZIP\
RDX	2014-11-07 22:36	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\RDX\DataContainer.vhd
RDX	2014-09-15 22:00	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\RDX 19515\DataContainer.vh
RDX	2014-09-12 22:00	Online\2003, Offline\Server 2012R2 CORE, Of…	G:\BackupAssist\RDX 19515\DataContainer.vh

86 backup(s) found.

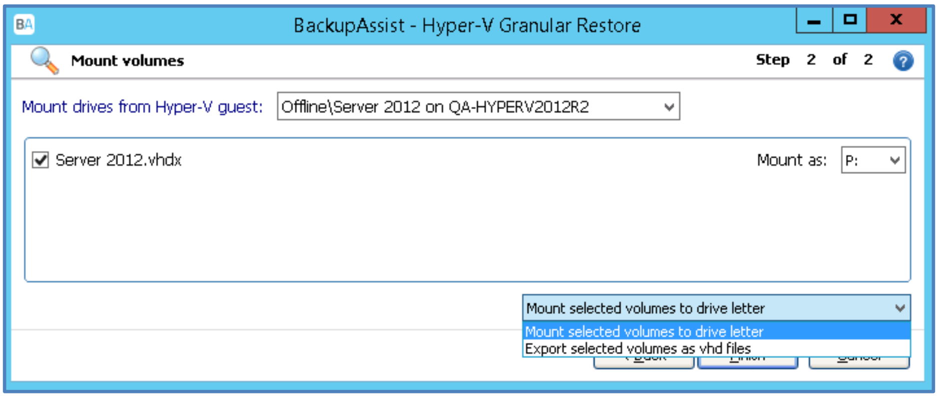
Don't see your backup? See more options

Figure 9: Hyper-V Granular Restore console - backup selection

5. Select the **host backup** to restore from.

6. Click **next** to proceed to the **Mount volumes** screen.

The Mount Volumes screen is used to select the guest within the backup that you want to restore data from, and to determine how the data will be restored.



BackupAssist - Hyper-V Granular Restore

Mount volumes

Step 2 of 2

Mount drives from Hyper-V guest: Offline\Server 2012 on QA-HYPERV2012R2

☑ Server 2012.vhdx

Mount as: P:

Mount selected volumes to drive letter

Mount selected volumes to drive letter
Export selected volumes as vhd files

Figure 10: Hyper-V Granular Restore console - mount volumes

7. Use the **Mount Drives from the Hyper-V guest** drop down list, to **select the guest.**

   This is the guest on the Hyper-V host backup that you want to restore data from. When the section is made, that guest will appear in the window.

8. **Tick the guest image** that you want to restore from.

9. **Select a drive letter** to mount the guest image as.

10. **Select the appropriate restore function from the drop down list**.

    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.

    a. Set the location that you would like to export the VHD files to.
    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.

    A backup of a guest disk may include checkpoints that have not been applied to the VHD. An Export merges the checkpoints with the VHD, to create a version of the VHD as it was when it was backed up. You cannot get a VHD in this state by copying it out of the backup. Exported VHDs are transportable and can be used to manually recover a guest or migrate it to another Hyper-V host.

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.

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.

To learn more about Scheduling, refer to the Backup tab whitepaper and our scheduling blog articles.

To learn about full, differential and incremental backups, see our Backup Methods, blog article.

Files and applications

The Files and applications tab can be used to modify your Hyper-V and data selections. This screen also displays a **Hyper-V CSV options** tab and an **Exchange VM Detection** tab, to change the information provided when the backup job was created.

Imaging options

Imaging options provides configurations that can be applied to an existing System Protection backup.

Backup history storage

This option is used to determine how space is allocated for shadow storage on a removable backup destination. Shadow storage is used by VSS to store historical backup data from previous backup jobs.

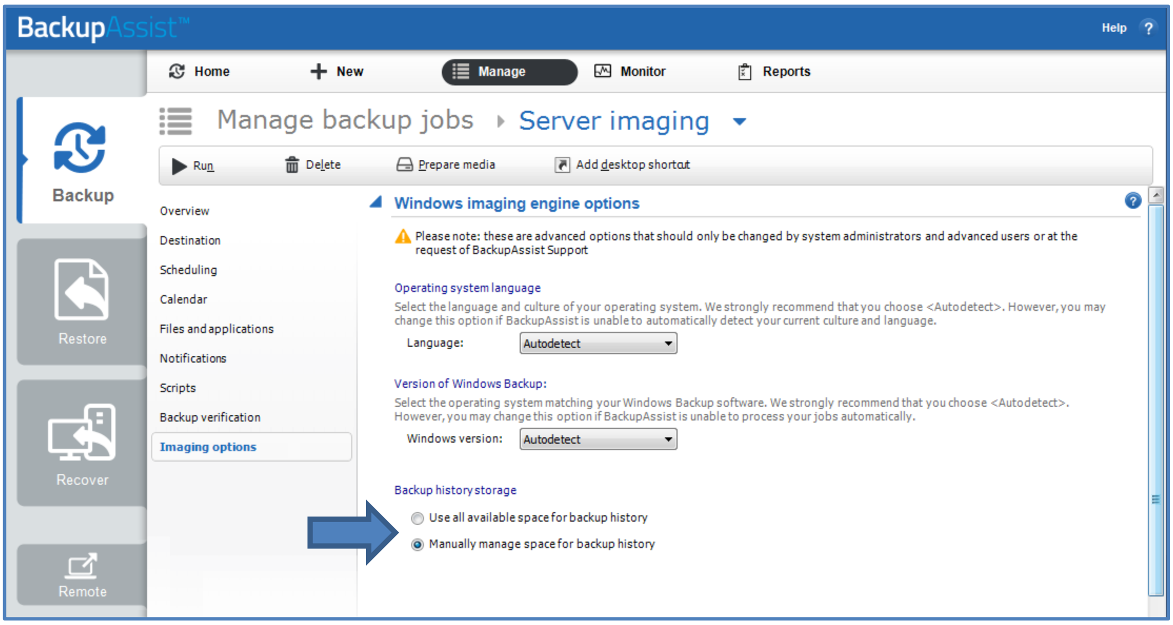
There are two options available:

- **Use all available space for backup history**

  With this option, BackupAssist makes all free space on the backup destination available for storing historical backups. The exact amount of the space used changes with time, depending on the amount of space used by the latest backup and other data.

- **Manually manage space for backup history**

  With this option, Windows is used to determine the shadow storage size. You can allow Windows to automatically determine the size, or manually manage the size yourself using either the Windows Server settings or the vssadmin tool.



Windows imaging engine options

⚠ Please note: these are advanced options that should only be changed by system administrators and advanced users or at the request of BackupAssist Support

Operating system language

Select the language and culture of your operating system. We strongly recommend that you choose <Autodetect>. However, you may change this option if BackupAssist is unable to automatically detect your current culture and language.

Language: Autodetect

Version of Windows Backup:

Select the operating system matching your Windows Backup software. We strongly recommend that you choose <Autodetect>. However, you may change this option if BackupAssist is unable to process your jobs automatically.

Windows version: Autodetect

Backup history storage

○ Use all available space for backup history

● Manually manage space for backup history

Figure 11: Imaging options - Backup history storage

To set the size using the Windows Server settings:

- For Windows Server 2008, right click the drive and select Configure Shadow Copies
- For Windows Server 2012, open the drive's properties, select *Shadow Copies* tab, access Settings.

To set the size using the vssadmin tool:

- You can view the amount of space reserved for the shadow copy storage by running the command ***vssadmin list shadowstorage*** at an elevated command prompt.
- You can change the amount of disk space allocated to the shadow copy storage in GB or as a percentage of the disk, using the following commands.

> *vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=XX%*
>
> *vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=XXGB*
>
> This will resize the limit to ***XX*** size for drive ***X:***
>
> **The use all available space for backup history** option is equivalent to "*vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=UNBOUNDED*".

To see more VSS admin commands, please refer to this Microsoft VSS admin resource.

For guidance on what the size should be, see our article on Image backup destinations.

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.

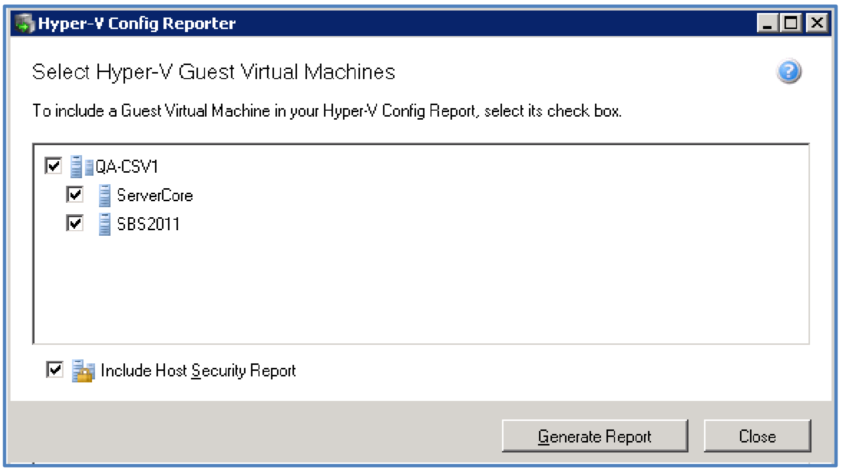
To fully document the setup of a Hyper-V Server, you need to include the setup of each guest machine and the configuration of the host. The BackupAssist Hyper-V Config Reporter (included with the *Hyper-V Granular Restore Add-on*) simplifies and automates this task by creating an HTML report of the configuration 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.



Select Hyper-V Guest Virtual Machines

To include a Guest Virtual Machine in your Hyper-V Config Report, select its check box.

☑ QA-CSV1
  ☑ ServerCore
  ☑ SBS2011

☑ Include Host Security Report

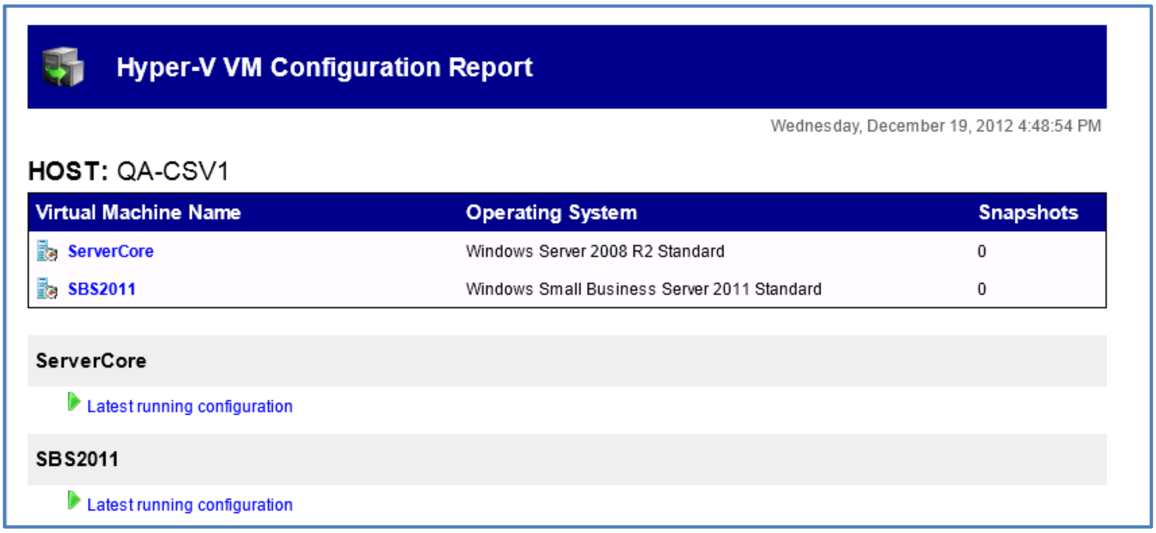
Figure 12: Hyper-V Config Reporter – guest selection

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
ServerCore	Windows Server 2008 R2 Standard	0
SBS2011	Windows Small Business Server 2011 Standard	0

ServerCore

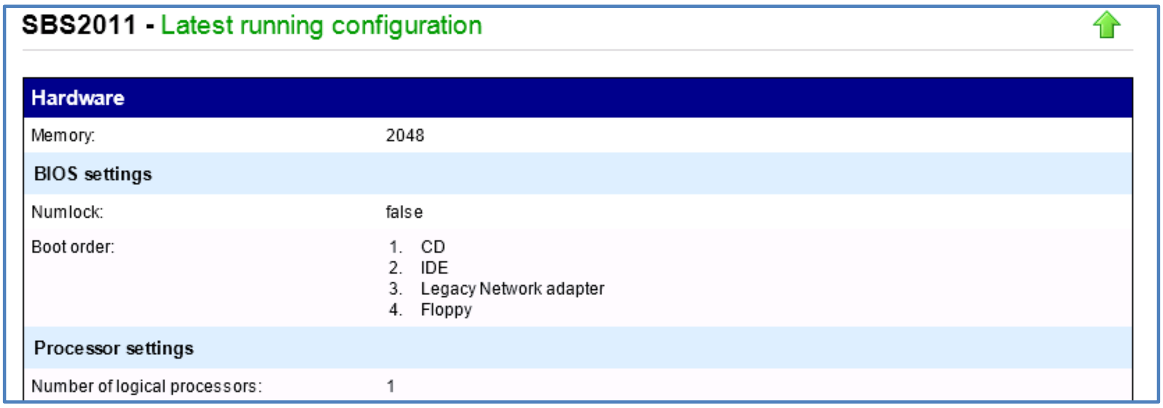
Latest running configuration

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.

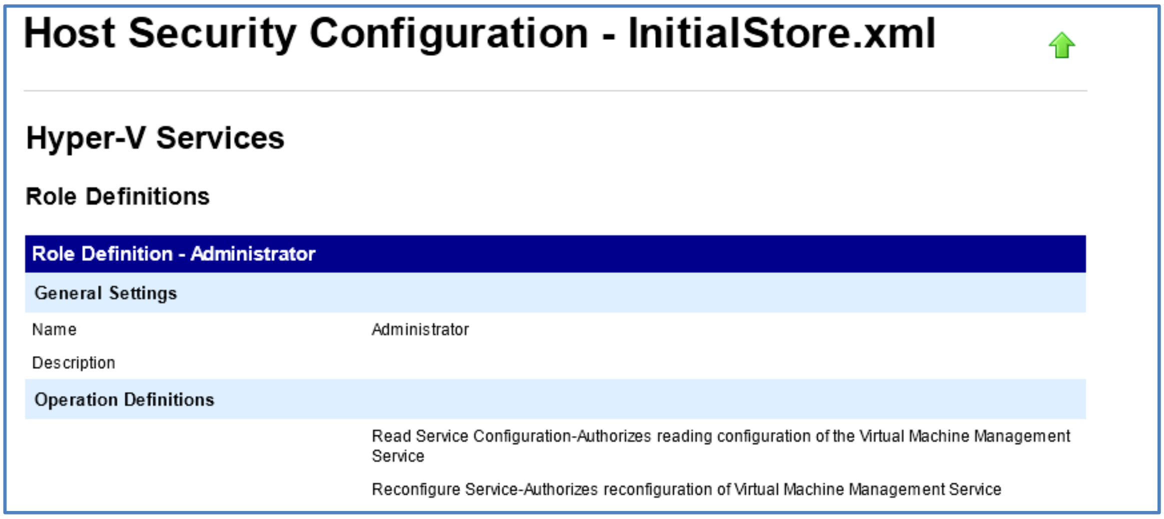
Each VM included in the report will contain a full description of the VM settings for the latest running configuration at the top, and then a list of any further snapshots available underneath that, in date order.



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