

BackupAssist™ v9

Hyper-V Protection

User guide

Contents

1. Hyper-V overview	2
Documentation	2
Licensing	2
Hyper-V requirements.....	2
2. Hyper-V protection features.....	3
Windows 2012 / 2012 R2 Hyper-V support.....	3
Custom Hyper-V steps.....	3
Hyper-V restore and recovery options.....	3
Bootable backups.....	3
3. Hyper-V best practice backups.....	4
4. BackupAssist settings	6
Backup user identity.....	6
Email server settings	6
Email address list.....	6
Network paths	6
Windows Settings	6
5. Hyper-V in a CSV environment.....	7
Backing up a CSV environment.....	7
Restoring to a CSV environment.....	7
6. Hyper-V Tab.....	8
Hyper-V tab columns.....	8
Guest details view	9
Hyper-V Tab menu	9
7. Creating a Hyper-V backup.....	10
8. Hyper-V Host Files restore	17
9. Hyper-V Granular restore	21
10. Hyper-V backup management	25
Scheduling	25
Files and applications	25
Imaging options	25
11. The Hyper-V Config Reporter.....	27

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 Advanced 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 handling 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 [implementation](#) and [best practice](#) guides.
- 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 perform a Hyper-V Granular Restore or a Rapid VM Recovery requires the *Hyper-V Advanced 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 2016 - from v9.5 (does not include CSV support)
- Windows Server 2012 / 2012 R2, including Server Core and Hyper-V Server versions.
- Windows Server 2008 R2, including Server Core and Hyper-V Server versions.
- Windows Server 2008

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 2008/2008 R2 the partition size of the disks being backed up should be less than 2TB

The following features support guests backed up from CSV environments:

- The Exchange granular restores
- The Hyper-V granular restores

2. Hyper-V protection features

Windows 2012 / 2012 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 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 Selections screen makes it easier to select Hyper-V guests and guest configuration files for Application consistent guest only backups, as well as full host backups.

A dedicated Exchange VM detection screen allows you to provide Exchange authentication information so that BackupAssist can detect what guests have an Exchange Server, and list the EDB files available for each guest when you perform an Exchange Granular Restore.

A dedicated CSV staging 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 and recovery options

BackupAssist can restore and recover Hyper-V data using these features.

Integrated Restore Console: restore files from a Hyper-V host.

Hyper-V Granular Restore: restore individual files from inside of a guest. Requires the Hyper-V Advanced Add-on.

Exchange Granular Restore: restore mail items from an Exchange Server installed on a guest. Requires the Exchange Granular Add-on and the Hyper-V Advanced Add-on.

Rapid VM Recovery: spin up a single guest from its backup destination to keep critical systems online. Requires the Hyper-V Advanced Add-on.

Full VM Recovery: recovers a guest back to the host.

Bootable backups

If you create a System Protection bare-metal backup on an external USB hard disk, the media can be made into a *Bootable Backup Media*. The backup media can be used to boot into a RecoverAssist recovery environment and recover the server, without a separate boot disk.

The backup media will be made bootable the first time the job runs unless you deselect the **Make media bootable with RecoverAssist** tick box on the *Set up destination* step.

3. Hyper-V best practice backups

Backing Hyper-V 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.

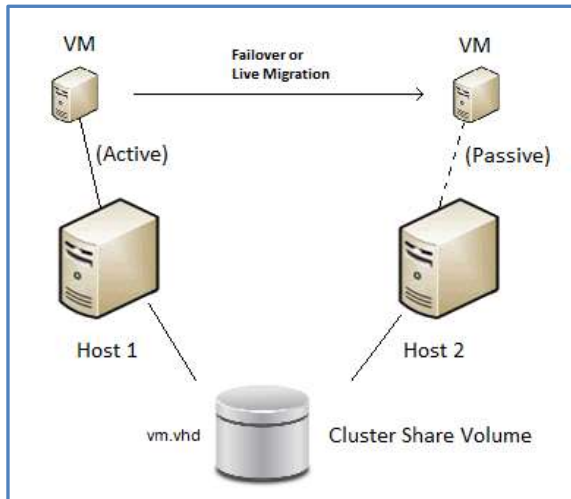
Windows Settings

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 v9 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. Hyper-V Tab

When you install BackupAssist on a server with the Hyper-V role installed, a Hyper-V tab will appear. The tab lists all guests on the server, including those without BackupAssist. At a glance, you can see what guests are active, what guests are being backed up and when the last successful backup ran. You can also begin a granular restore or a guest recovery.

Hyper-V tab columns

The Hyper-V tab lists all of the guests on the Hyper-V host, and uses columns to provide information about the guests. You can sort the guests by selecting a columns' heading.

The **Name** column displays the name of the guest. To the left of the name are two icon columns. One column shows if the guest has an error, alert or warning, the other column, the guest's configuration. The configuration icon will indicate if the guest uses CSV and if it is running an Exchange Server.

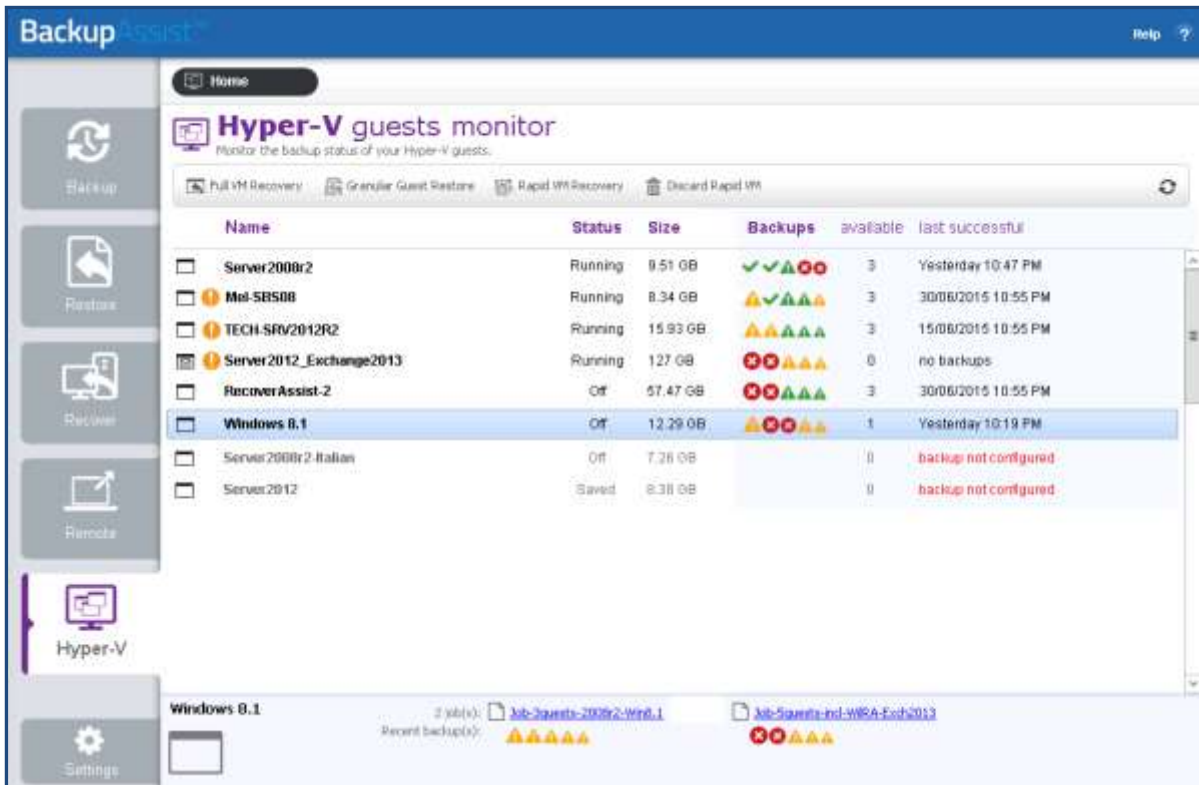
-  Hyper-guest
-  Hyper-guest on a CSV
-  Hyper-guest running Exchange Server

The **Status** column shows if a guest is running, backing up, saved, paused or off. Guests can be started and stopped using the Microsoft Hyper-V Manager.

The **Size** column shows the total size of the guest's virtual disk and configuration files, on the host.

The **Backups** column shows the results of the last 5 backups. The icons indicate if the backup was successful, had a warning or failed. Mouse over an icon to display any warnings, errors or messages.

The **available** column shows how many backups are available for restoring to the guest, and the **last successful** column shows when the last successful backup job ran.



Name	Status	Size	Backups	available	last successful
Server2008r2	Running	9.51 GB	✓✓✓✓	3	Yesterday 10:47 PM
Mel-SBS08	Running	8.34 GB	⚠✓✓✓	3	30/06/2015 10:55 PM
TECH-SRV2012R2	Running	15.93 GB	⚠✓✓✓	3	15/08/2015 10:55 PM
Server2012_Exchange2013	Running	127 GB	✗✗✗	0	no backups
RecoverAssist-2	Off	57.47 GB	✗✗✗	3	30/06/2015 10:55 PM
Windows 8.1	Off	12.29 GB	⚠✗✗	1	Yesterday 10:19 PM
Server2008r2-Italian	Off	7.26 GB		0	backup not configured
Server2012	Saved	8.38 GB		0	backup not configured

Guest details view

When you select a guest, a details panel will display guest information at the bottom of the tab. The information provided includes links to the backup jobs configured for that guest, and the results of recent backups. The results are displayed as icons below the relevant backup job.

Selecting the job's result icon will open the backup report for that backup.



Hyper-V Tab menu

The Hyper-V Tab's menu can be used to access BackupAssist's guest restore and guest recovery tools.

Full VM Recovery

This button will take you directly into the *Full VM Recovery* process with the highlighted guest already selected. The Full VM Recovery console will be used to recover the guest to the current host. *Full VM Recovery* can also be accessed from the BackupAssist Recovery tab.

You can perform a Full VM Recovery of both a normal VM and a Rapidly Recovered VM. To learn more about these options, see the BackupAssist [Hyper-V Recovery guide](#)

Full VM Recovery is included in the base BackupAssist license.

Granular Guest Restore

This button starts the guided restore process for the selected guest. This process will use the *Integrated Restore Console* to restore files and folders from inside the guest. Hyper-V Granular Restore can also be accessed from the BackupAssist Restore tab.

Granular Guest Restore is a licensed feature that requires the *Hyper-V Advanced* add-on.

Rapid VM Recovery

This button starts a *Rapid VM Recovery*, which will use the current Hyper-V host to run a guest from its backup. This means if the guest that was backed up becomes unavailable, the backup can be used to resume that guest's functions within seconds, while a recovery of the guest is planned and scheduled.

When you select the *Rapid VM Recovery* button, you will be asked to confirm if you want to proceed with a *Rapid VM Recovery* for the selected guest.

Rapid VM Recovery is a licensed feature that requires the Hyper-V Advanced add-on.

Discard Rapid VM

This will stop a Rapidly Recovered VM, discard any changes made to the guest's data since it was rapidly recovered, and remove the guest instance from the Hyper-V Manager.

To learn more about this option and how to use it, see the **Managing a Rapidly Recovered VM** section of the [Hyper-V Recovery guide](#)

7. 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.

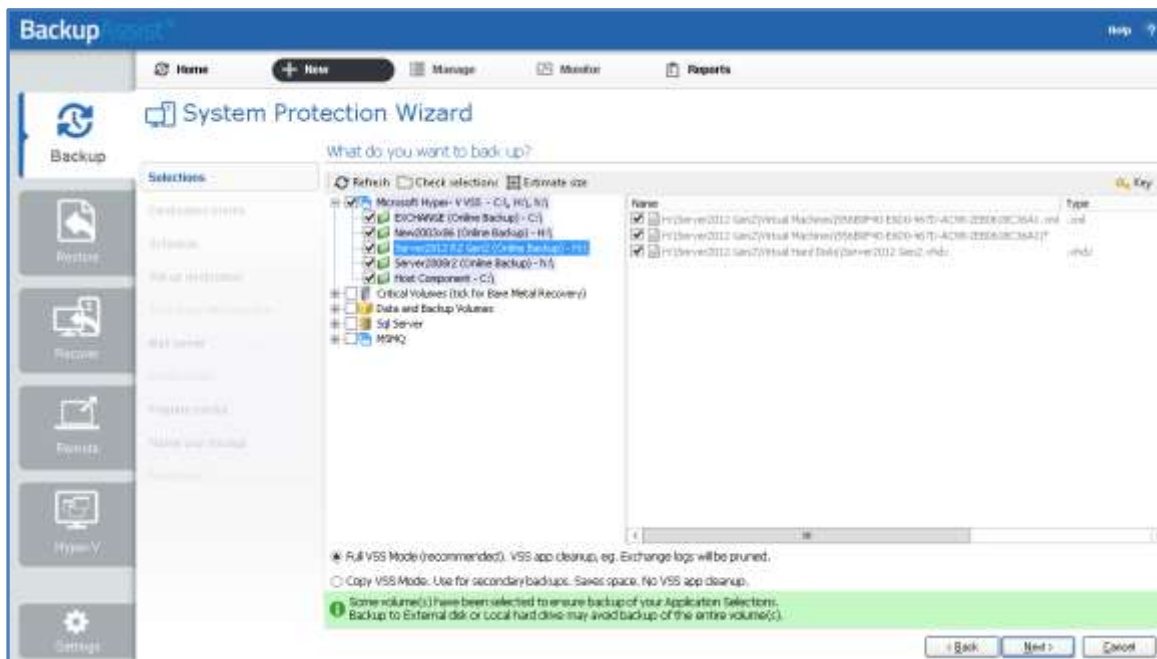


Figure 1: BackupAssist Hyper-V backup – Selections screen

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.

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

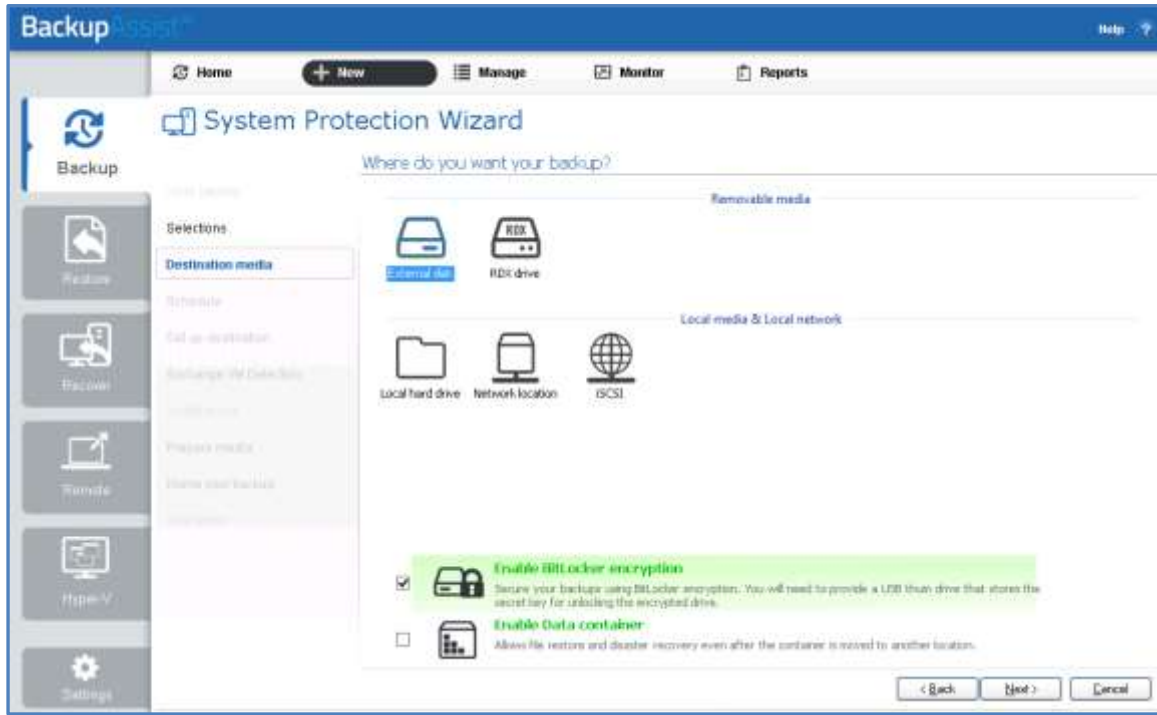


Figure 2: System Protection – Destination media

Enable BitLocker encryption

This 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.

- A USB flash drive containing the encryption key must be connected to the server running BackupAssist, to allow BackupAssist to access the drive when you backup or restore data.
- The encrypted drive will be assigned a password that can be manually entered to unlock an encrypted drive when you want to restore data or perform a recovery using RecoverAssist.

To learn more, including how to install BitLocker, see our [BitLocker resource page](#)

Enable Data container

This 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.

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

5. Schedule

This screen is used to select when you would like a backup job to run and how long you would like the backup to be retained for. A selection of pre-configured 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**.

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.

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

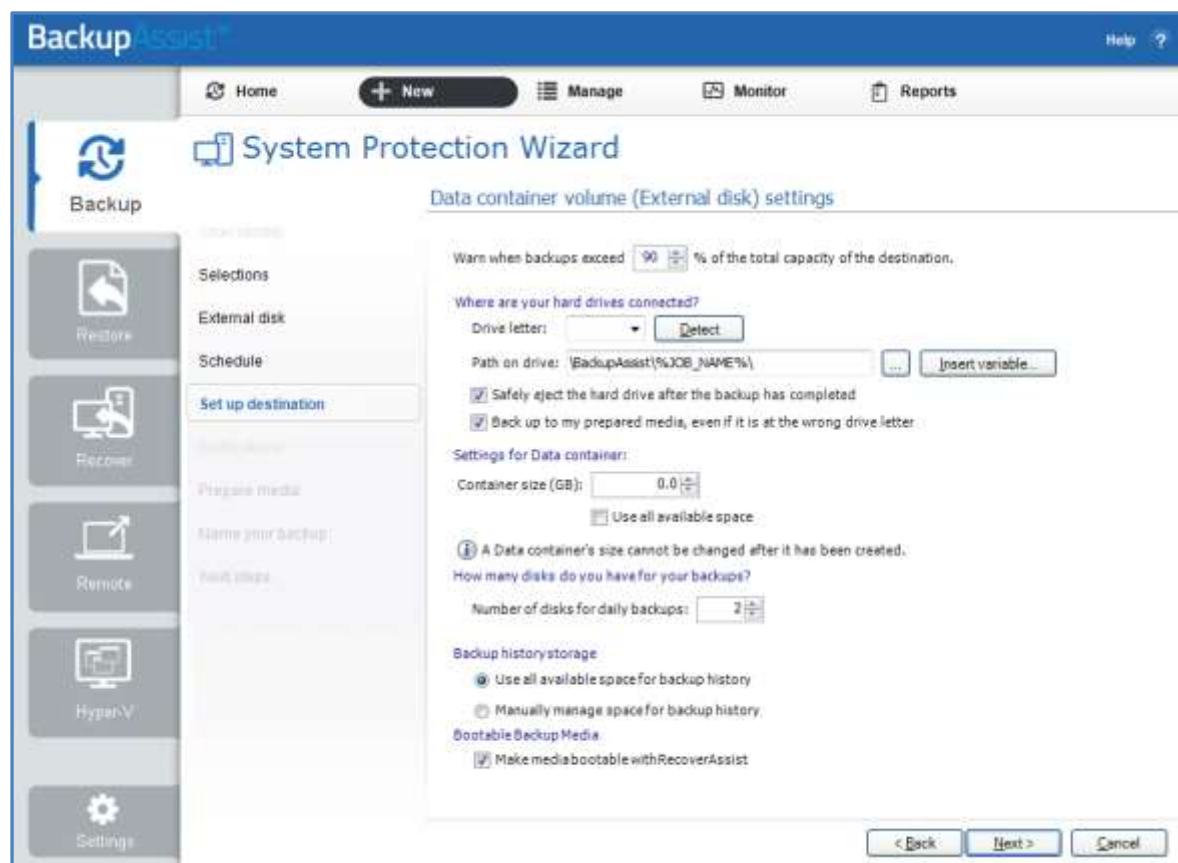


Figure 3: BackupAssist System Protection – Set up destination screen

BitLocker encryption

To encryption the backup destination, you will need to provide:

- A drive letter of the USB drive used to store the encryption key. An encryption key is saved for each encrypted drive, and is used to unlock the drive when you backup and restore data.
- A password that will allow you to manually access any drive encrypted by this job when you perform a restore or a recovery. This password is saved in the backup job.

Data containers

The container size and location is set using this screen.

- 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.
- Selecting *Use all available space* will allow the Data container to grow into the available space.

Bare Metal Bootable Backups

If you are doing a bare-metal backup to an external hard disk, a *Bootable Backup Media* option will be displayed and selected by default. This feature allows your backup media to boot into a RecoverAssist recovery environment and recover the server, without a separate boot disk.

Destination check report

If you are using a *Local media & Local network* destination, a *Check destination* button will be available to check your backup destination for possible problems. After the checks have been completed, the results can be viewed by selecting the *Report* link. If you are using *Removable media* destinations, these checks are performed when you select *Prepare* on the *Prepare Media* step.

7. Exchange VM detection

If a Hyper-V guest runs 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.

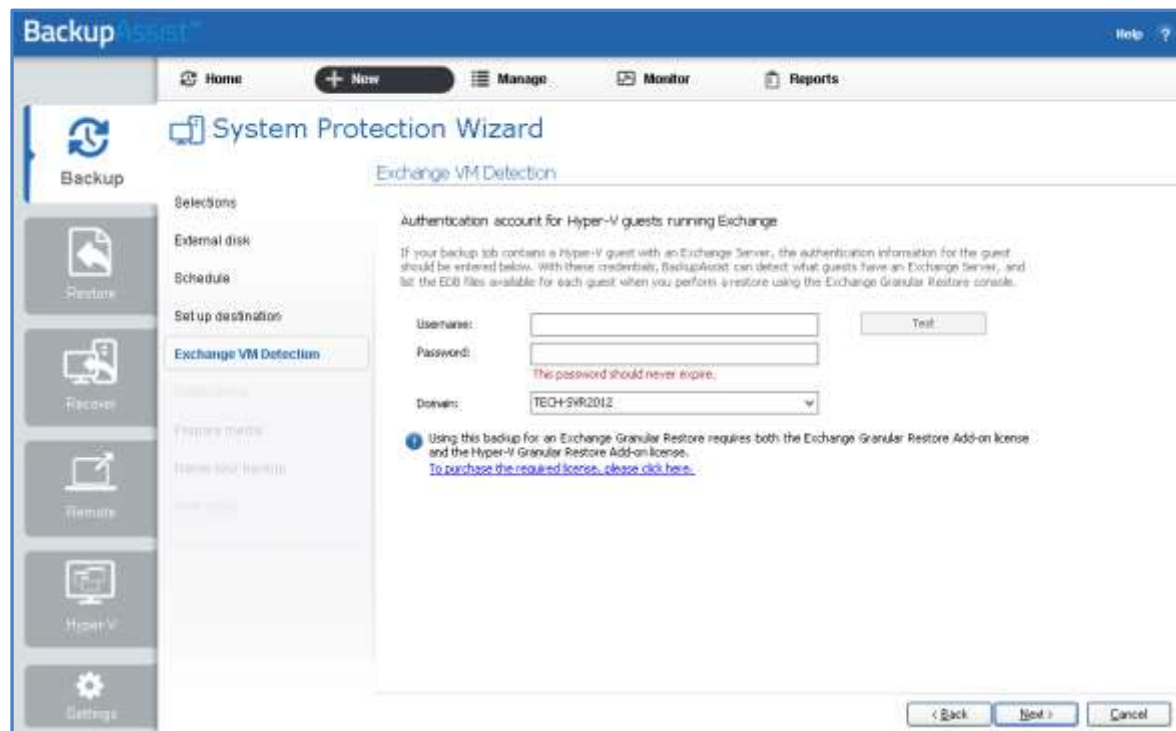


Figure 4: Hyper-V - Exchange VM detection

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.

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.

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.

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.

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

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

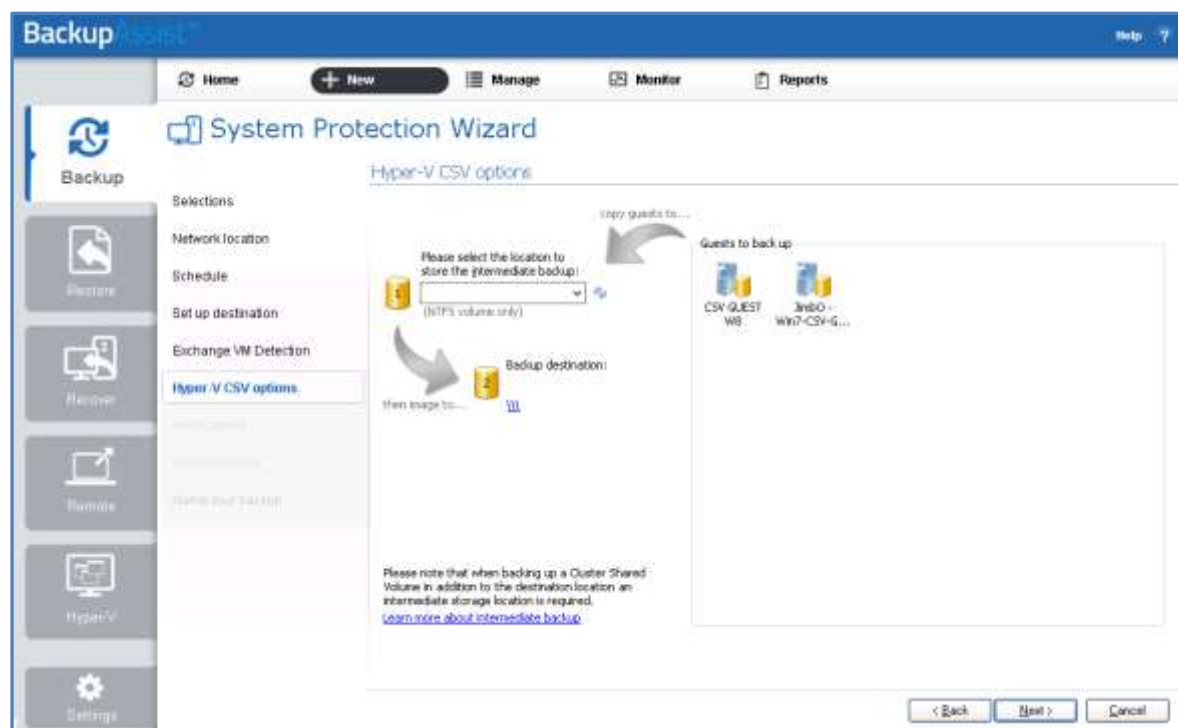


Figure 5: Hyper-V intermediate (staging) disk selection

The entire contents of the staging disk will be 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:

- Select, **Add an email report notification**.
- Enter recipients into the **Send reports to this email address** field.
- 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.

To learn more, see the [Backup tab user guide](#).

10. Prepare media

If you selected a portable media device as your backup destination, you will be given the option to prepare and label the media. The label allows BackupAssist to recognize the media and ensure that the correct media is being used on the correct day.

For example, if you put an RDX drive in on Tuesday but it was labelled Wednesday, BackupAssist will warn you that the incorrect media has been detected.

BackupAssist will display a list of media based on the backup schedule you selected, and the *Number of disks for daily backups*, selected on the *Set up destination* screen.

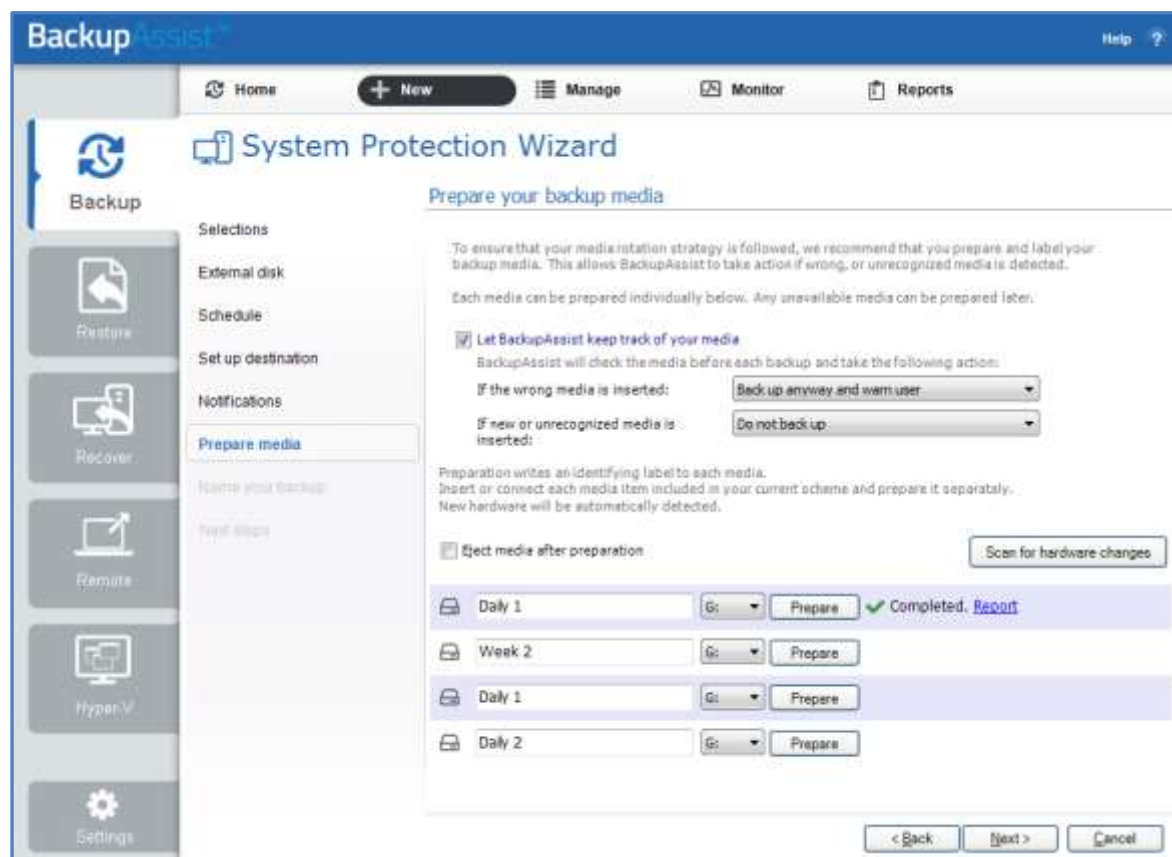


Figure 6: System Protection – Prepare media selections

To prepare the media and enable media tracking:

- a. Select, *Let BackupAssist keep track of your media*.
- b. Select what you want BackupAssist to do if an incorrect or unrecognized media is inserted.
- d. Enter the label you want added to each media in the text field provided. Default label names are provided, based on your backup schedule.
- e. Select *Prepare* for each media device. Prepare will be selectable when the media is attached.

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

Destination Check Report

Selecting *Prepare* will generate a *Destination Check Report*. The report will advise if any problems were detected with the media. If *Make media bootable with RecoverAssist* was selected in the *Set up destination* screen, the report will also advise if the media can or cannot be made bootable.

11. Name your backup

Provide a name for your backup job, and click **Finish**.

12. Next Steps:

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 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](#).

Backup verification is an automated process for testing backups. A manual restore is the only way to fully test a backup, and regular manual restores should be part of any backup solution

8. Hyper-V Host Files restore



BackupAssist's Restore tab displays two restore options for Hyper-V: **Hyper-V Host Files** and **Hyper-V Granular Restore**. This section explains how to perform an *Hyper-V Host Files* restore using a *System Protection*, *File Protection* or *File Archiving* backup.

The **Hyper-V Host Files** restore option allows you to restore files and folders from the Hyper-V host to their original location or a new location. **Hyper-V Host Files** comes with the BackupAssist base license.

If you want to recover a full Hyper-V guest, see the [Hyper-V Recovery guide](#).

To restore Hyper-V host files, follow the steps below:

1. Select the Restore tab

The *Restore tab* has a *Home page* and a *Tools page*. The *Home page* is the default page and the recommended starting point for performing a restore. The *Tools page* should only be used by experienced administrators or users being assisted by technical support.

2. Select Local and Network Files

This will display the volumes backed up by this installation of BackupAssist. It can also show backups from other machines added using the *Discover Backups* button, which is explained below.

Expand a volume to display all of the backups available for that volume. The tabs above each volume's list of backups can be used to help locate the required backup.

- The *Last 7 days* and *Last 30 days* tabs display the backups within those ranges.
- The *Custom* tab allows you to select a specific date range and display backups for that period.

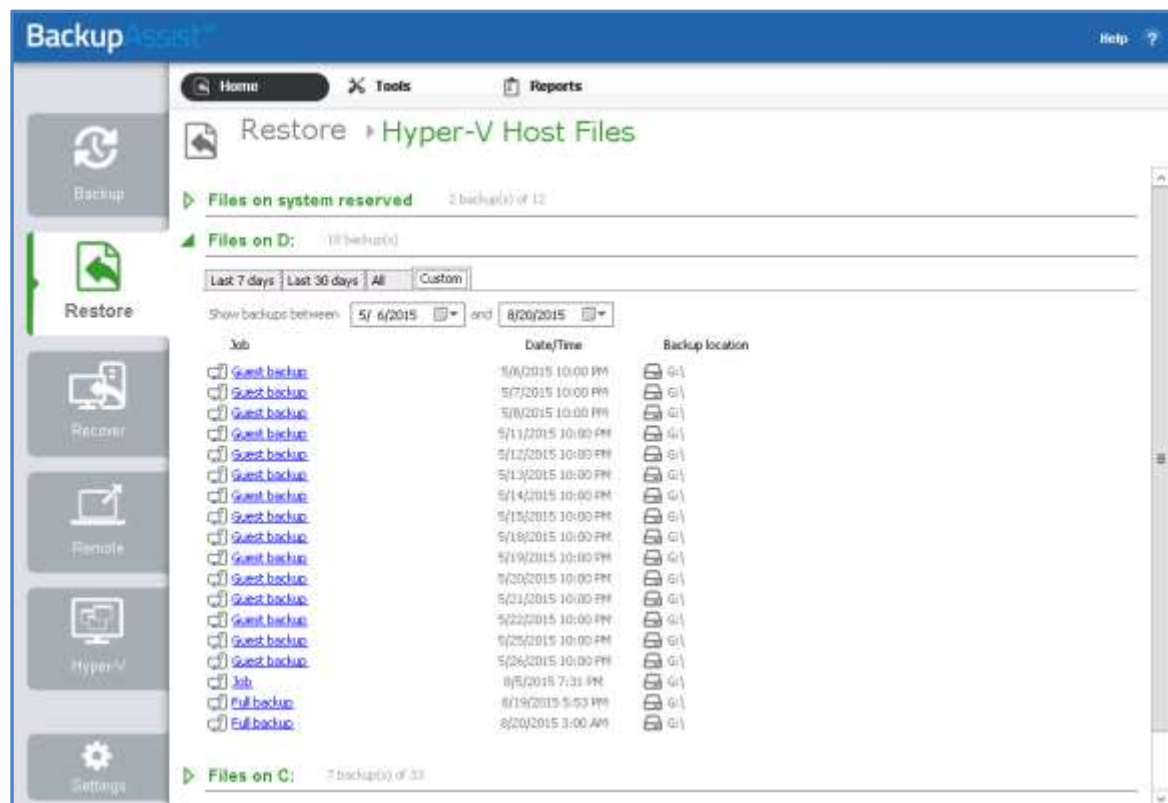


Figure 7: Restore tab – backup selection

The **Search** button allows you to locate files to restore across multiple backups. When you select Search, the Restore console will display the Search page.

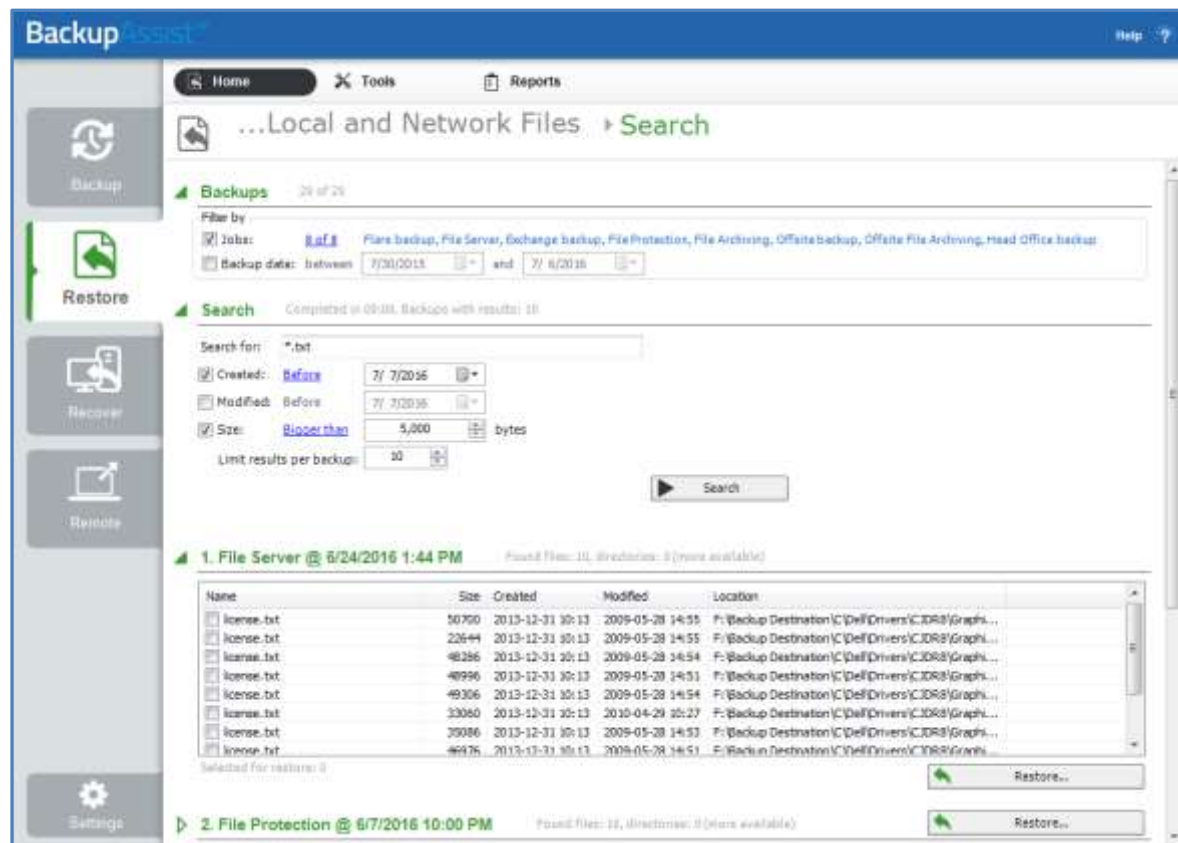


Figure 8: Restore Tab – Search page

- a) The *Backups* section allows you to use the *Jobs* Filter, to limit the search to specific backup jobs. You can also use the *Backup Date* filter search within a specified date range.
- b) The *Search* section is used to enter a search term associated with the name of the file you want to find. The *Search for* field will take the string provided and search for occurrences of that string within a file or directory name. The results of the search are displayed by backup.

To refine the search, use the *Created*, *Modified* and *Size* options. Ticking any of these options will activate a drop down list of variables to select from. For *Created* and *Modified*, you can select a date using the Calendar selection fields. For *Size*, you can select the file size in bytes.

Discover Backups allows you to browse for backup catalogs created by deleted jobs and other servers. Selecting those backups will add them to the list of available backups.

3. Select the backup that you want to restore from

Clicking on a backup's name will open the *Integrated Restore Console (IRC)*. The *Integrated Restore Console* is used to select the data to be restored, where to restore it to and the restore conditions.

4. Select the Hyper-V Host files that you want to restore

Use the left pane to locate and select the data.

The right pane will display the contents of the folder selected in the left pane.

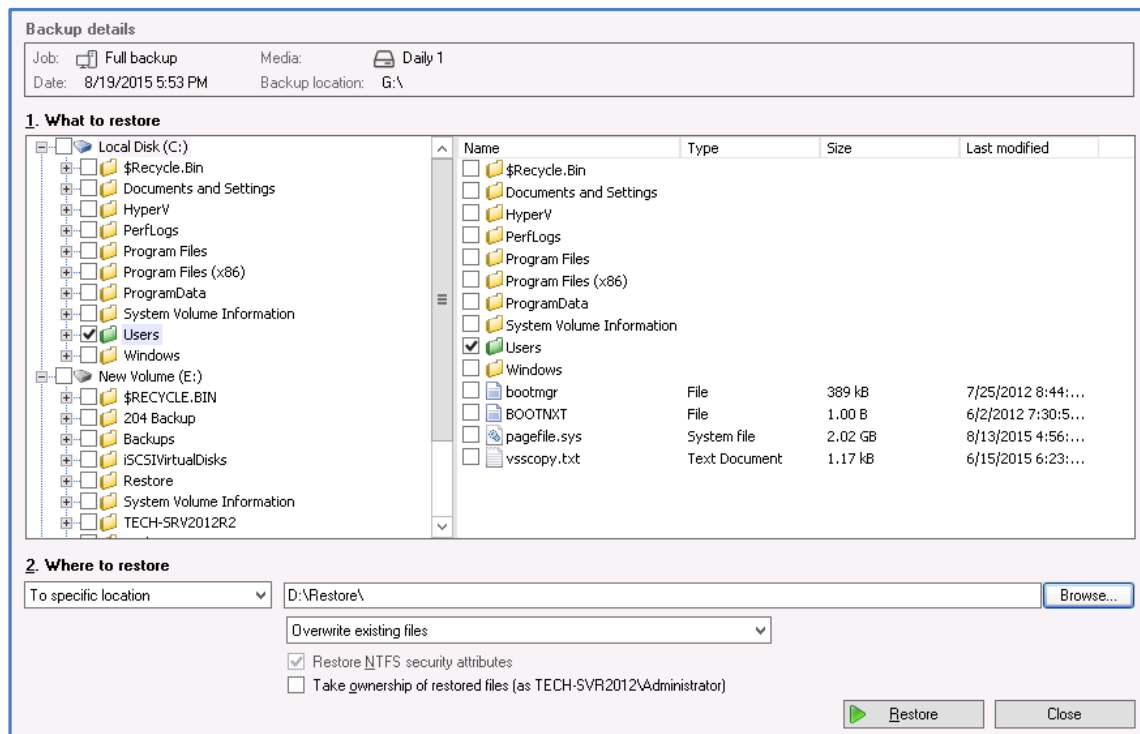


Figure 9: Integrated Restore Console

5. Select Where to restore the data to

Follow these steps to select the restore destination for the host files and the restore options:

- Under *Where to restore* select *To original location* or *To Specific location*.
- Use the *Browse* button to locate and select the restore destination.
- Use the drop down box to set the overwrite rules. The overwrite rules will apply if the files being restored encounter files with the same name in the restore destination.

You can select:

- **Overwrite existing files** - The restored files will overwrite files in the restore destination.
 - **Do not overwrite existing files** – The restored files will not overwrite files in the restore destination. This means the files will not be restored.
 - **Only overwrite older files** - If a source file has changed since the backup was made it will not be overwritten.
- Review the **Restore NTFS security attributes** option

If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the *Security* tab on the file's *Properties*

- Review the **Take ownership of restored files** option

Selecting the *Take ownership of restored files* tick box will give the current user ownership of the restored files. The user is shown to the right of the text box description.

6. Select Restore

When you select the *Restore* button, the restore process will begin. The *Integrated Restore Console* will display information about the restore job and provide status updates as the job runs.

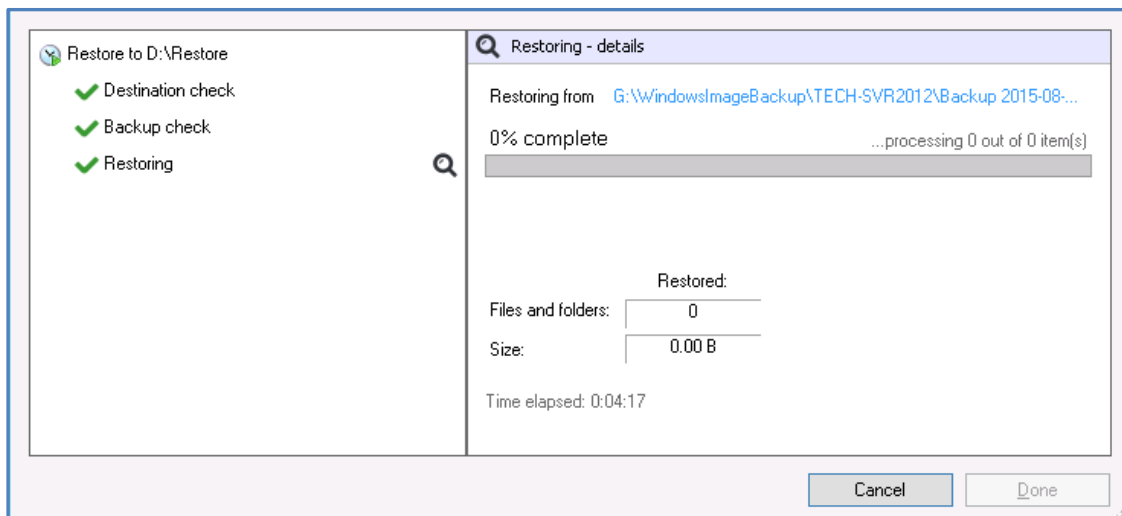


Figure 10: Integrated Restore console – restore monitor

Selecting *List all processed files and folders ...* will open notepad and display a list of the files restored, including their full path.

Encrypted backups

If your backup is encrypted, you'll be prompted for the encryption password when the restore job tries to access the backup. It is important that you keep a copy of your password in a safe place, as we cannot assist you with opening password encrypted files if your password is lost or forgotten.

If you encrypted the backup using BitLocker, you can use the password or encryption key to unlock the drive by connecting the flash drive. BackupAssist will use the key to unlock the drive that you are restoring from. You will not be prompted to do anything other than the normal restore steps.

7. Select Done

Once the restore has finished, selecting *Done* will return you to the main UI.

▶ **Your Hyper-V Host Files restore has now been completed.**

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

9. Hyper-V Granular restore



The BackupAssist Restore tab displays two restore options for Hyper-V: **Hyper-V Host Files** and **Hyper-V Granular Restore**. This section explains how to perform an *Hyper-V Granular Restore* using a *System Protection*, *File Protection* or *File Archiving* backup.

Hyper-V Granular Restore allows you to restore individual files from a guest using a Hyper-V backup of one or more guests. **Hyper-V Granular Restore** requires the Hyper-V Advanced add-on license.

If you want to recover a full Hyper-V guest, see the [Hyper-V Recovery guide](#).

To perform a Hyper-V Granular Restore, follow the steps below:

1. Select the Restore tab

The *Restore tab* has a *Home page* and a *Tools page*. The *Home page* is the default page and the recommended starting point for performing a restore. The *Tools page* should only be used by experienced administrators or users being assisted by technical support.

2. Select Files inside Hyper-V Guests (Hyper-V Granular Restore)

This will display the guests backed up by this installation of BackupAssist. It can also display backups from other machines added using the *Discover Backups* button.

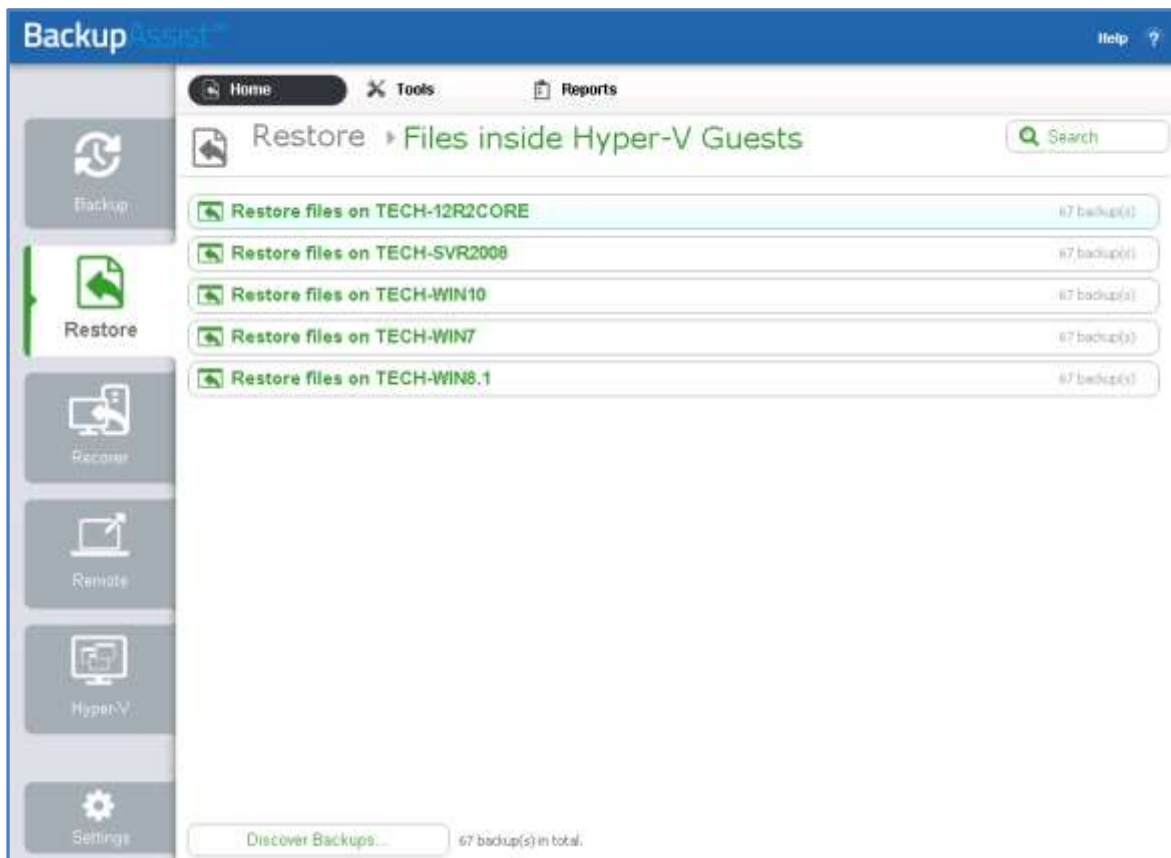


Figure 11: Restore tab – backup selection

Discover Backups allows you to browse for backup catalogs created by deleted jobs and other servers. Selecting those backups will add them to the list of available backups.

There are **Search** buttons on both the guests' screen and the files inside of a guest screen. The Search feature allows you to locate files to restore across multiple guests. When you select Search, the Restore console will display the Search page.

To be able to use the Search feature on a Hyper-V guest, the backup must be cataloged. A Cataloging the Hyper-V guest is enabled by Editing the backup job in the Manage menu as follows:

- For a File Protection backup, select *Catalogue Hyper-V Guests* under *Replication Options*.
- For a System Protection backup, select *Catalogue Hyper-V Guests* under *Imaging Options*.

A backup will only be cataloged if it is created by a backup job that has this option enabled.

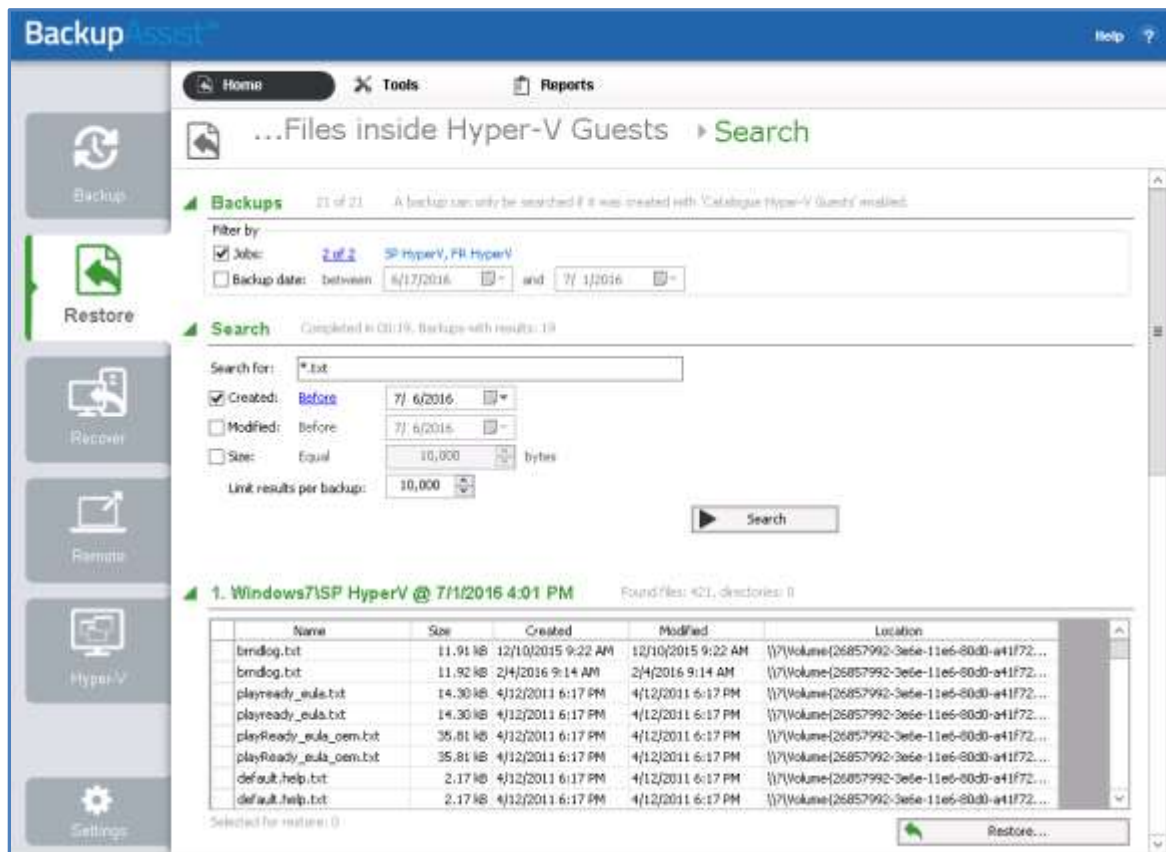


Figure 12: Restore Tab – Search page

- The *Backups* section allows you to use the *Jobs* Filter, to limit the search to specific backup jobs. You can also use the *Backup Date* filter to search within a specified date range.
- The *Search* section is used to enter a search term associated with the name of the file you want to find. The *Search for* field will take the string provided and search for occurrences of that string within a file or directory name. The results of the search are displayed by backup.

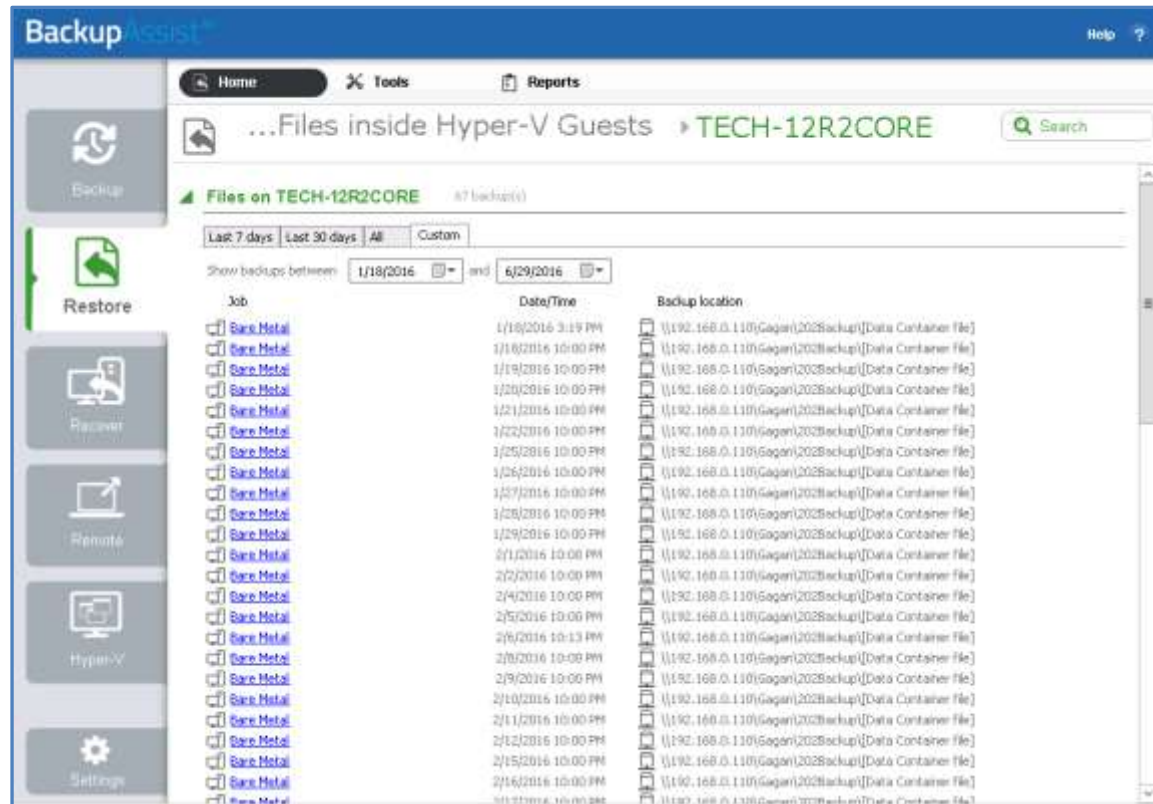
You can refine your search using the Search section's Created, Modified and Size options. Ticking any of these options will activate a drop down list of variables to select from. For Created and Modified, you can select a date using the Calendar selection fields. For Size, you can select the file size in bytes.

- To perform a restore, select the file/s that you want to restore and select the *Restore* button.

3. Select the guest that you want to restore files from.

The screen will reload and display all available backups for that guest. The tabs above the list of backups can be used to help locate the required backup.

- The *Last 7 days* and *Last 30 days* tabs display the backups within those ranges.
- The *Custom* tab allows you to select a specific date range and display backups for that period.



4. Select the backup that you want to restore from

Clicking on a backup's name will open the *Integrated Restore Console*. The *Integrated Restore Console* is used to select the data to be restored, where to restore it to and the restore conditions.

5. Select the data that you want to restore

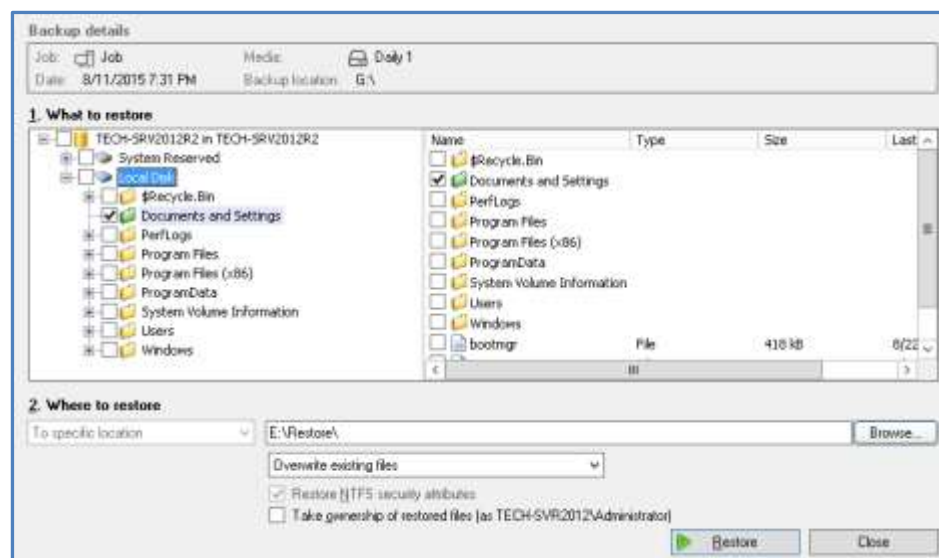


Figure 13: Integrated Restore Console

6. Select Where to restore the data to

Follow these steps to select the restore destination for the guest data and the restore options:

- f) Under *Where to restore* select *To original location* or *To Specific location*.
- g) Use the *Browse* button to locate and select the restore destination.
- h) Use the drop down box to set the overwrite rules. The overwrite rules will apply if the files being restored encounter files with the same name in the restore destination.

You can select:

- **Overwrite existing files** - The restored files will overwrite files in the restore destination.
- **Do not overwrite existing files** – The restored files will not overwrite files in the restore destination. This means the files will not be restored.
- **Only overwrite older files** - If a source file has changed since the backup was made it will not be overwritten.

- i) Review the **Restore NTFS security attributes** option

If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the *Security* tab on the file's *Properties*

- j) Review the **Take ownership of restored files** option

Selecting the *Take ownership of restored files* tick box will give the current user ownership of the restored files. The user is shown to the right of the text box description.

7. Select Restore

When you select the *Restore* button, the restore process will begin. The *Integrated Restore Console* will display information about the restore job and provide status updates as the job runs.

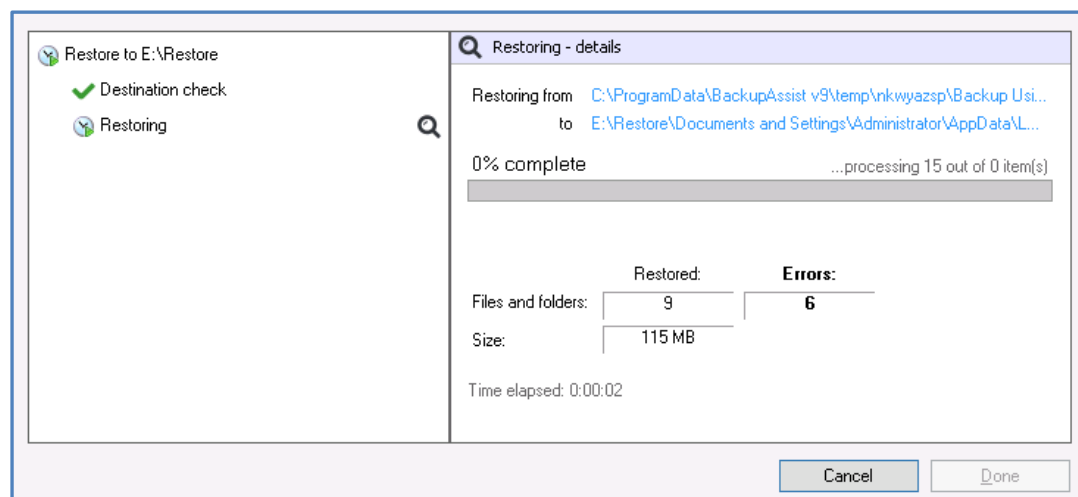


Figure 14: Integrated Restore console – restore monitor

Selecting *List all processed files and folders ...* will open notepad and display a list of the files restored, including their full path.

8. Select Done

- ▶ **Your Hyper-V Granular Restore has now been completed.**

10. 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 guide](#).

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 guide](#) 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.

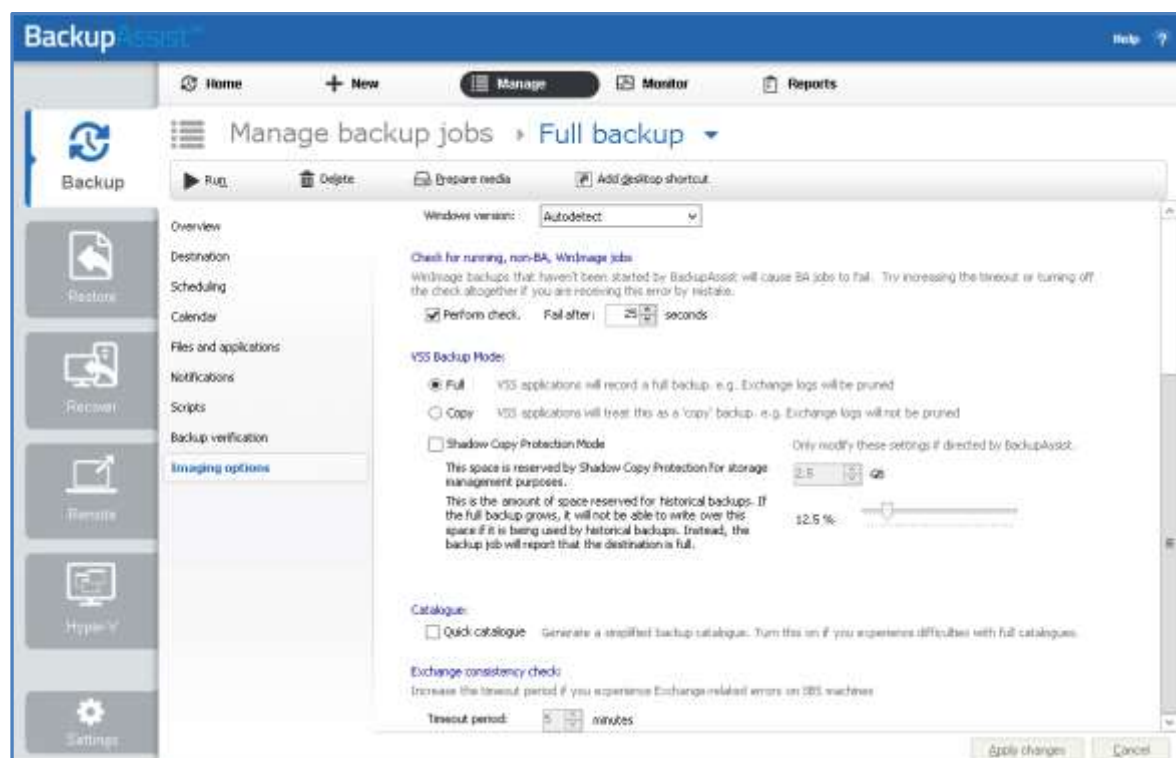


Figure 15: Imaging options - Backup history storage

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 and later, 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](#).

11. 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.

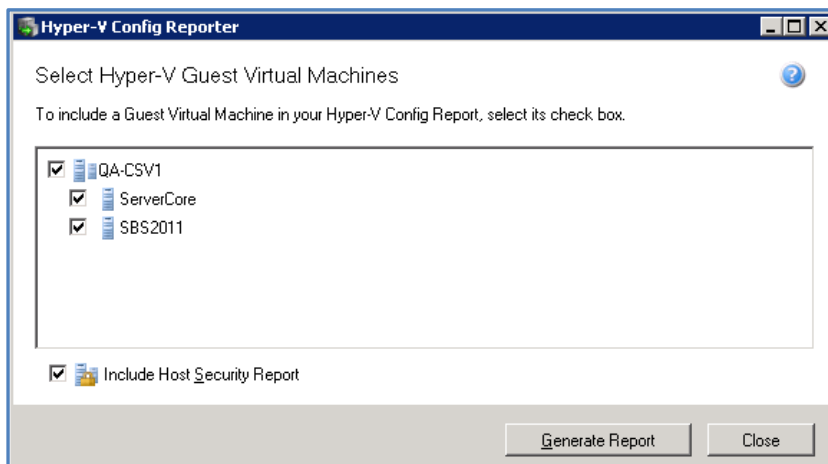


Figure 16: Hyper-V Config Reporter – guest selection

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