BackupAssist™ v8

System Protection

Whitepaper

Contents

1. Introduction

System Protection
For bare metal recovery

Method: Drive Imaging
Backup to Disk / iSCSI / NAS

Windows Server Backup uses drive imaging technology for data protection. BackupAssist allows you to take advantage of this backup functionality. The result is a feature-rich, reliable and cost-effective data and disaster protection solution.

This whitepaper explains how to protect your computer using BackupAssist System Protection, including how to create a backup, manage the configurations and restore both data and applications.

Documentation

This whitepaper provides a comprehensive guide to BackupAssist System Protection and can be used in conjunction with other BackupAssist guides.

- To perform a system recovery using an image backup, see the Recover Tab Whitepaper
- To protect Hyper-V environments, see the System Protection for Hyper-V Whitepaper
- For information on the BackupAssist Backup tab, see the BackupAssist Backup Tab Whitepaper.
- For information on the BackupAssist Restore tab, see the BackupAssist Restore Tab Whitepaper.

Licensing

System Protection is a standard feature included with the BackupAssist license, and requires a BackupAssist license once the initial trial period has expired. Please contact your local BackupAssist reseller or distributor for pricing information, or visit www.BackupAssist.com.

For instructions on how to activate / deactivate license keys, visit our Licensing BackupAssist page.

Operating system considerations

System Protection supports image backups on the following operating systems:

- Windows 7
- Windows 8 and 8.1
- Windows Server 2012R1
- Windows Server 2012R2
- Windows Server 2008R1
- Windows Server 2008R2

For a full list of the platforms supported by BackupAssist, see our BackupAssist homepage page.

> **Note**: System Protection cannot incrementally back up data from a ReFS formatted drive (source). This means a full backup of all selections will take place each time the backup job runs.

2. System Protection backup strategies

A good backup strategy is important to protect your company in every recovery scenario. There are five critical points to consider when setting up a backup strategy. Each point is described below.

Last known recovery point

One very important factor to consider is that your backups should provide you with a **last known good point** for recovery. Consider the following story.

> A hacker has found and exploited a security vulnerability in the operating system, modified some system settings and uploaded a back-door for future access. The entire system is now compromised and the system has been infested with malware and Trojans. The actions taken by the hacker are unknown, and there is no easy way to know what changes were made.

Some malware / virus infections may go undetected for several days. If the infection happened 3 days ago, and the only backup available is last night's backup, then the backup is effectively useless. However, if there is a backup from 3 days ago (just before the infection) then the server can be restored to the *last known good point*.

It is not always possible to know when your *last known good point* is – so for this reason it is important to have a variety of backups from different points in time. That means you need more than one backup medium (i.e. more than one disk to store your backups). These disks are then commonly divided into different sets - one set of backup media (in this case, disk) for daily backups, and another set of backup media for weekly backups. BackupAssist also gives you the option of having monthly and yearly backup disks for additional security.

Multiple removable media

When using a backup destination such as USB hard drives or RDX drives, it is recommended that multiple disks/cartridges are used as part of the rotation strategy. Due to the nature of Windows Imaging backups, the number of different points in history that we can restore from is correlated to the number of devices used for the backups.

Backup Device	Recommended Number of Disks/Cartridges
USB Hard-drive	3 to 5 or more
RDX drive	5 or more

Running a test restore

In addition to running backups successfully, the integrity of backups should be checked, on average, once a month to ensure that they are restorable. By frequently running a test restore, you will be able to confirm that the backups can be used in a real restore scenario. Test restores also give you practice in the restoration process so that you are aware of the steps and what is required.

Offsite storage of backup media

In order to protect your company data from physical events like natural disasters or theft of hardware, backups should be taken offsite and kept in a secure location. Although it is important to keep some backups on-site to be able to restore data quickly, is equally important to keep at least one backup a week off-site.

Keeping backups off-site enables users to restore their servers in the event of any such disasters. The convenience of being able to restore data immediately from on-site storage of backups should not deter users from also storing backups off-site.

> A hurricane has gone through the city's business district and destroyed everything its path. Your company has been severely affected - all office equipment such as servers, personal computers, and lap-tops has been destroyed beyond salvage. The IT department implemented a backup strategy earlier in the year covering all the computers on the network. Unfortunately, all the backups were stored in a safe on-site and were also destroyed in the hurricane.

We suggest that you store the daily backups on-site and the weekly backups off-site. (BackupAssist can even help you manage off-site backups using the Internet. For more information, visit our online product page: http://www.backupassist.com/BackupAssist/tour_Rsync.html)

Imaging backup scenarios

Imaging daily

When running a Windows Imaging backup daily to a removable device, a good strategy would be to use 5 disks – for example, 2 for daily backups and 3 for weekly backups. The two *daily* disks can be rotated across the daily backups (i.e. Monday and Wednesday's backup goes to Daily 1 and Tuesday and Thursday's backup goes to Daily 2). The three *weekly* disks can be swapped across the three weeks and the most recent weekly backup can be stored off-site. With multiple disks for the backups, you have a variety of restore points from which to choose. It is possible to alter this strategy – for example, 3 daily backup disks and 2 weekly disks, or 3 daily disks, 1 weekly disk and 1 monthly disk.

Imaging weekly

If there are constraints (excessive amounts of data, limited physical access to the server or procedural constraints) that make it impossible to image your system daily, it is still possible to have an effective backup system in place by running a Windows Imaging backup on a weekly basis.

For example, this scenario will still enable you to recover a system in the event of a disaster:

- Perform the drive imaging backups on a weekly basis (with 3 or more drives to enable media swapping).
- Use a different backup technology, such as a BackupAssist File Protection, to back up your applications and data on a *daily* basis.

In the event of a disaster, you can restore your system to the last image and then "roll forward" your data and applications from your daily backup.

3. Backup considerations

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

Exchange VM Detection

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

Figure 1: Selection screen - for an Exchange Server on a Hyper-V guest

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

Restore vs. Recovery

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

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

System Protection can create the image backup used in the recovery process. It can also create an image backup to protect data and applications so they can be restored onto a functioning computer (as explained in this whitepaper). These two capabilities make System Protection a powerful and versatile backup solution. It is important to understand the difference between restore and recover so that both solutions can be implemented effectively.

The Recovery using a System Protection backup section of this whitepaper, explains how a System Protection image backup is used in the recovery process. For more information on data recovery, see the Recover tab & RecoverAssist Whitepaper.

Windows SystemState

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

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

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

Selecting Windows SystemState

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

This table shows what backup jobs can include Windows SystemState.

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

To enable Windows SystemState:

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

To select Windows SystemState:

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

4. Data containers

The backup

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

Key points:

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

The problem

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

Key points:

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

The solution

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

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

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

Other advantages

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

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

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

Supported systems

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

To learn more, see the Data container resource page.

5. BackupAssist settings

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

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

Backup user identity

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

A video explaining the creation of a backup user identity can be found on our, Videos Webpage.

Email server settings

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

Email address list

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

Network paths

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

Windows Settings - Enable image tracking

System Protection creates a full backup the first time it runs. Subsequent backups are incremental. To create an incremental backup, BackupAssist scans and compares the data to be backed up and the data in the destination image to see what data changed. The process can take a long time, but when **Enable image tracking** is selected, System Protection backups record the changes to the data using a virtual snapshot. This means the backup job only needs to look at the snapshot to see what data changed. The result is significantly faster backups. *Enable image tracking* is enabled by default under the **Incremental backup tracking for System Protection** section, in the *Windows Setting* screen.

To learn more, visit our article on making faster incremental image backups.

6. Creating a System Protection backup

The following instructions describe how to create a backup job using BackupAssist System Protection.

Launch BackupAssist and follow the steps outlined below:

1. Select the **Backup** tab

2. Select **Create a new backup Job**

3. 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.

4. **Selections:** The selections screen is used to select the data and applications that you would like to back up. Any VSS applications detected here will be displayed as application directories.

   There are two selections to choose from:

   - **Back up the Entire System**. This option will create an image of your system that can be used to perform a full *recovery* of your computer. The Critical Volumes are selected by default and include *bare-metal* recovery data.

   - **Back up selected items only**. This option is used if you only want to create a backup of files, folders and applications. The option will allow you to deselect *Critical Volume's* (bare-metal) and select specific VSS applications and drives.

     You can select specific data within a drive (e.g. C:) if the backup is to a *Removable* disk. To do this, modify the backup job after you save it using the *Manage* menu on the *Backup* tab.
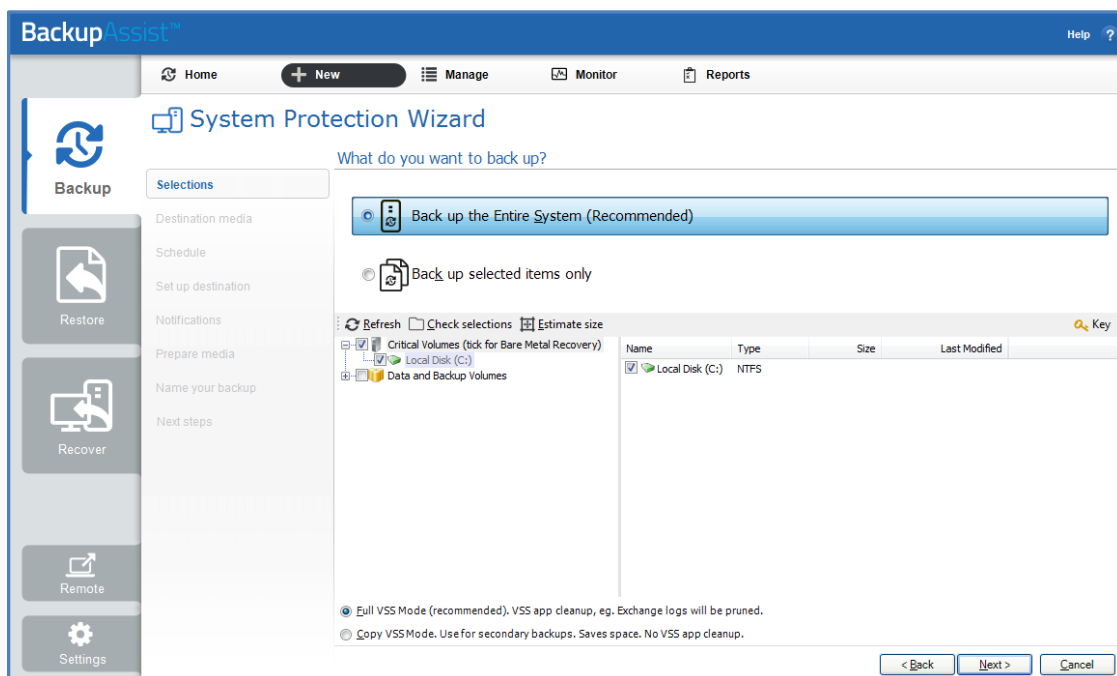

Figure 2: System Protection backup – data selection screen

Critical Volumes is required for a bare-metal backup. The backup can be used with a bootable recovery media to recover your computer, after hardware has been replaced or an operating system failure has occurred and your computer can no longer start itself.

5. **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.

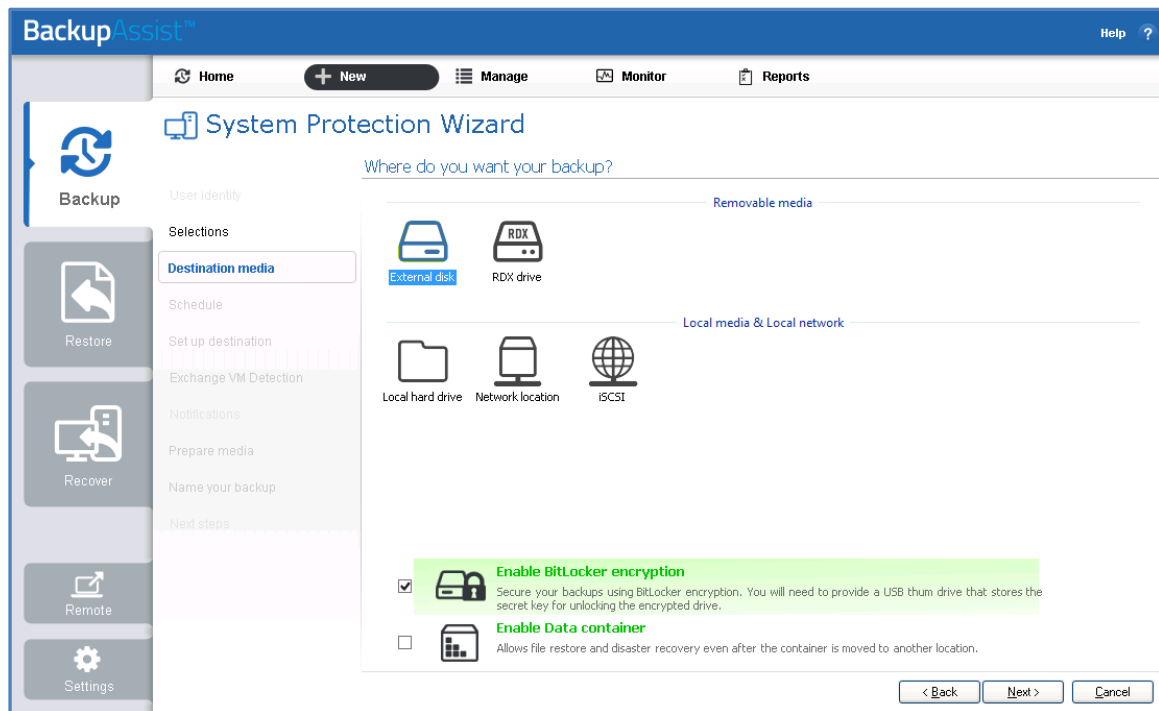   Select a device for your backup destination, and click **Next.**

Figure 3: System Protection – Destination media

Enable BitLocker encryption 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 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, 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.

6. **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.

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

7. **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 Data container destinations, 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.

- The *Use all available space* selection will use all available space, up to 2TB.

For BitLocker encrypted destinations, 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.
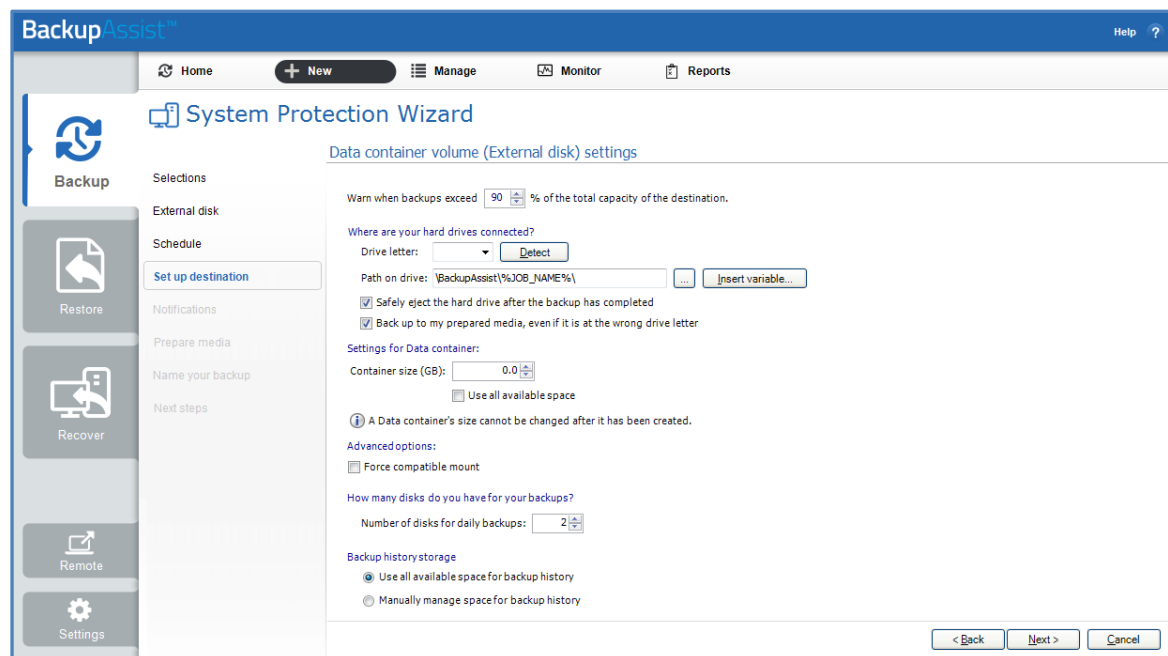

Figure 4: BackupAssist System Protection – Set up destination screen

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

8. **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.

To learn more, see the BackupAssist settings section and the Backup tab user guide.

9. **Prepare media:** If you selected a portable backup destination, a prepare media step will be next. This step allows BackupAssist to write a label onto the media so it can recognise what media has been attached, and determine if the correct media is being used on the correct day.

   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.

   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 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.
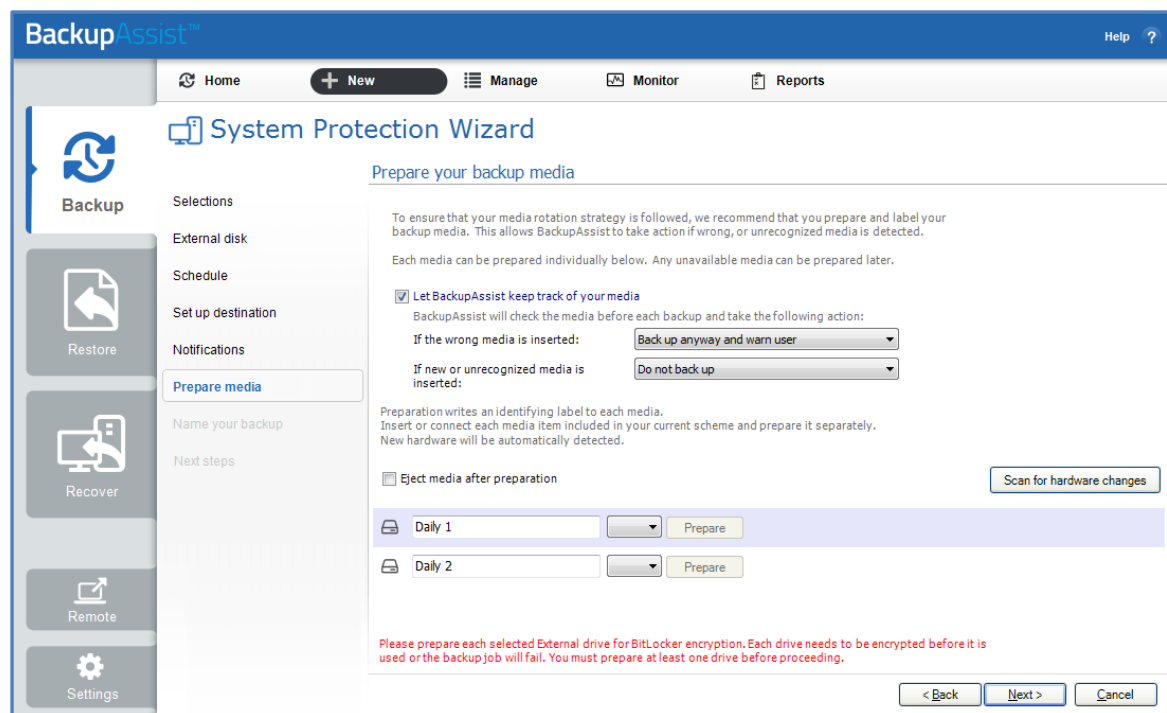

Figure 5: System Protection – Prepare media selections

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

11. **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 backup job has now been created.**

Important: Once a **backup job** has been created, it should be reviewed and run using the *Manage* menu. See the section, System Protection backup management, for more information.

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 from a System Protection backup

This section provides instructions on how to *restore* data and applications from a System Protection image backup. The next section on page 17 explains how to an image backup is used in a system *recovery*.

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

1. Select the **Restore tab**

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

2. From the **Home page**, select the type of restore you want to perform.

    *   *Files and folders* will display all data backups and all VSS application backups.
    *   *Applications* will display backups that contain VSS applications, and exclude data only backups.
    *   *Exchange*, *SQL* or *Hyper-V*, will display all backups that contain the selected application. Selecting an application type will display application specific restore tools (e.g. Hyper-V Granular Restore and SQL Restore) as well as the Restore Console.

3. Once you have selected the type of restore you want to perform, the *Home page* will display all catalogued backups that match your selection. The backups displayed will be for active backup jobs, and grouped by the source data's location and the restore tool that can be used.

    *   If a backup can be used by two restore tools, it will appear in two groupings.
    *   If a backup contains data from multiple locations, it will appear in a grouping for each location.

    Select the required Restore tool.

    For a *System Protection* backup, the restore tool that will be displayed for both data and VSS applications is the **Restore Console**. How to use the *Restore Console* is explained in the next step.
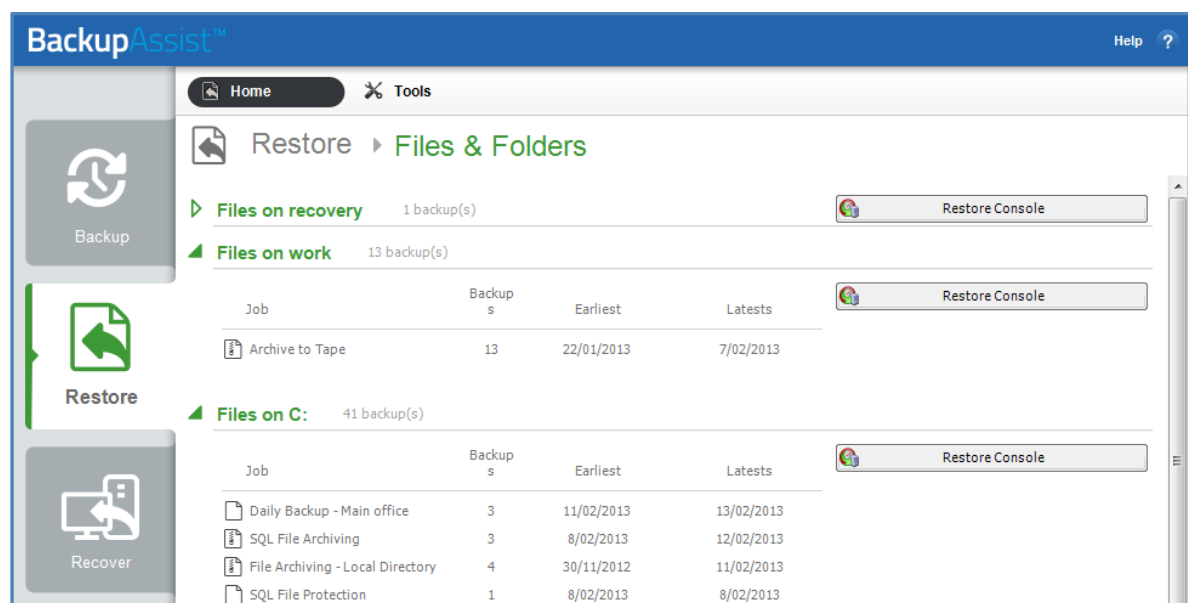

Figure 6: BackupAssist Restore Home page - selection results

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

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

The Restore Console provides two tools to locate your data:

- The **Browse** tab. Select this tab if you know the backup and date you wish to restore from, or if you need to restore an entire backup set.

    a. Use the drop-down menu to choose the backup that you want to restore from.
    b. Use the calendar to select the date you want to restore from.
    c. Use the middle panes to expand the backup set.
    d. Select the data to restore.
    e. Click **Restore to** at the bottom right of the window.

- The **Search** tab. Select this tab to search all of the loaded backups for the data you want to restore. You can display data filtered by name, date, size and type, for all backups. The results can be compared (e.g. the dates of two files) to identify the correct data selection.

    a. Enter your search term (The search accepts wild card searches, such as **.log* or **.doc*).
    b. Select a filter/s if required.
    c. Click the *Search* button.
    d. Select the data to restore.
    e. Click **Restore to** at the bottom right of the window.
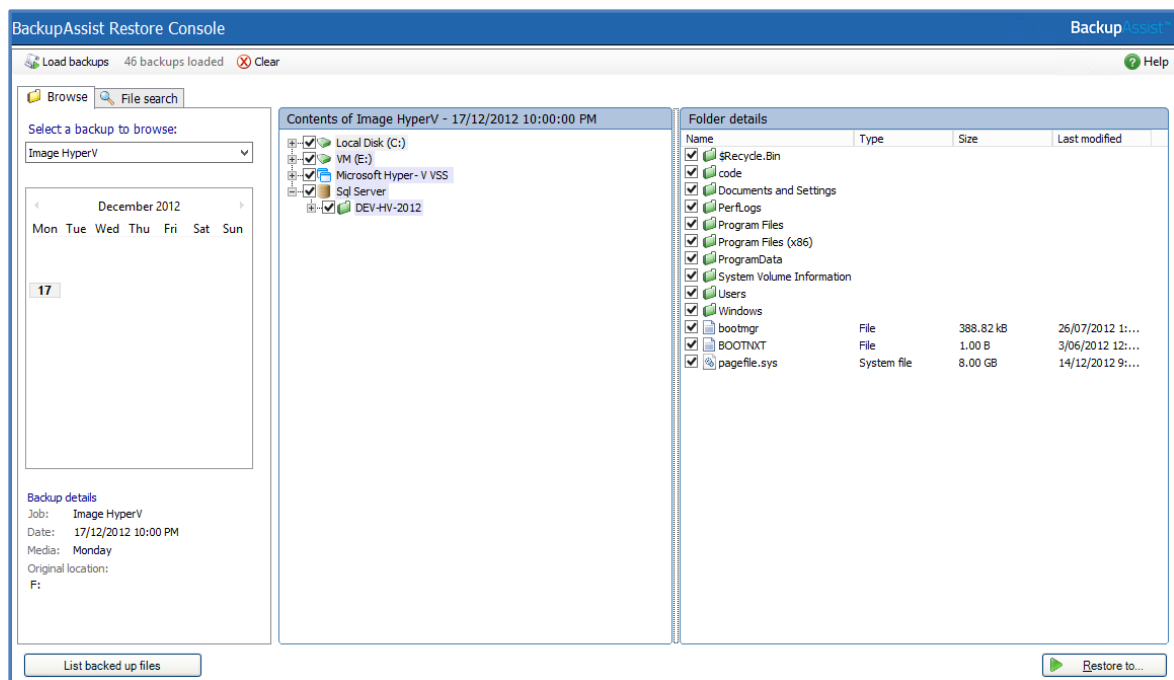

Figure 7: BackupAssist Restore Console – backup and data selection

If 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*.

For more information about data selection, refer to the Restore tab user guide.

5. **Restore Console – restore destination selection**

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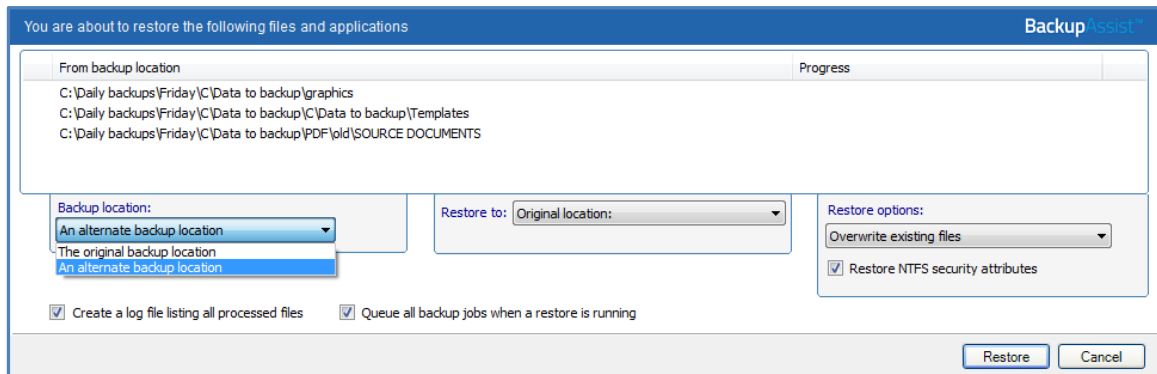

Figure 8: BackupAssist Restore Console – restore destination

a. Review **Backup location:** Change the selection if the backup was moved after it was created.

b. Review **Restore to:** Leave the *Original location* selected or chose an *Alternative path*.

Restoring to an alternate location will use a minimal path. For example, restoring a single file to an alternate location will copy the file to the location without re-creating the original folder structure.

c. Review the **Restore options:**

   - Select one of the following: *Overwrite all existing files*, *Do not overwrite existing files* or *Only overwrite older files*.
   - The option, *Restore NTFS security attributes* will be selected by default.

d. Selecting *Create a log file listing all processed files*, will create a file that lists the success or failure of each file. The log is opened by selecting the log file's link in the backup report.

e. *Queue all backup jobs when a restore is running*, is selected by default.

f. Click the **Restore** button to restore your data.

If BackupAssist cannot access the backup location, you will be prompted to either connect the appropriate media or specify an alternate location where the backup can be found. The restore will run from the destination window. A **Report** link will appear once the restore has finished.

g. Select **Done**.

▶ **Your System Protection restore has now been completed.**

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

Helpful hint: If you backed up a Hyper-V machine using System Protection, and selected *Hyper-V* on the Restore tab's *Home page*, the **Hyper-V Granular Restore tool** will be displayed (as well as the Restore Console) and can be used to restore files from within a Hyper-V guest. For instructions on how to use this tool, see the System Protection for Hyper-V whitepaper.

Helpful hint: BackupAssist automatically mounts Data containers when backups and restores are performed. However, there may be times when you want to do this manually. For example, if you want to check what is inside a Data container or have it available for another task. To manually mount a Data container, please refer to the steps outlined in our blog article.

8. Recovery using a System Protection backup

This section provides an overview of the BackupAssist recovery process. It is important to understand the link between a System Protection backup and RecoverAssist, because both technologies are used together to perform a recovery.

Overview

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

Once the computer has been started, RecoverAssist will create a recovery environment (on your monitor), which can access your System Protection image backup, and recover your operating system, data and any applications that were included in the image backup.

➢ System Protection creates an image backup of your entire system, known as a *bare-metal* backup.
➢ BackupAssist's RecoverAssist feature creates a customized, bootable recovery disk.

RecoverAssist

RecoverAssist is accessed through the BackupAssist Recover tab. It will use a wizard to create a customized, recovery disk using the local machine or a Windows installation disk.
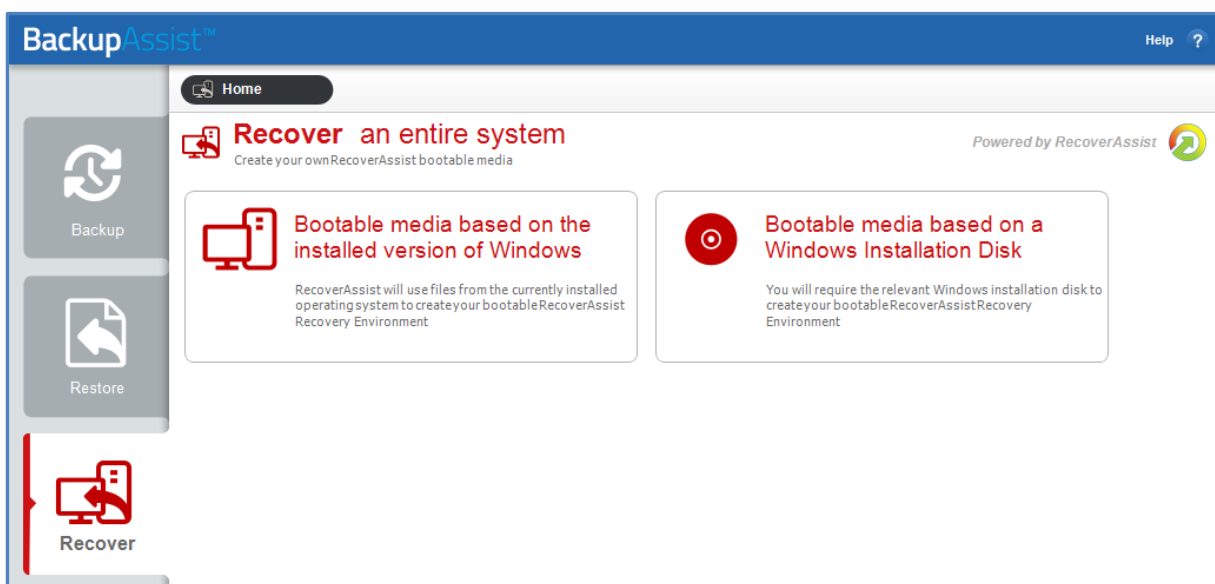

Figure 9: RecoverAssist media selection screen

For instructions on how to create a bootable *RecoverAssist* media, and how to use it with a *System Protection* backup, refer to the whitepaper, Recovery tab - RecoverAssist whitepaper.

The RecoverAssist whitepaper contains instruction on

- Bare-Metal backups and recoveries.
- How to create a bootable, Recovery media.
- How to recover a Windows Server using RecoverAssist and a System Protection image backup.

9. System Protection 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.

Destination

Backup storage options

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.
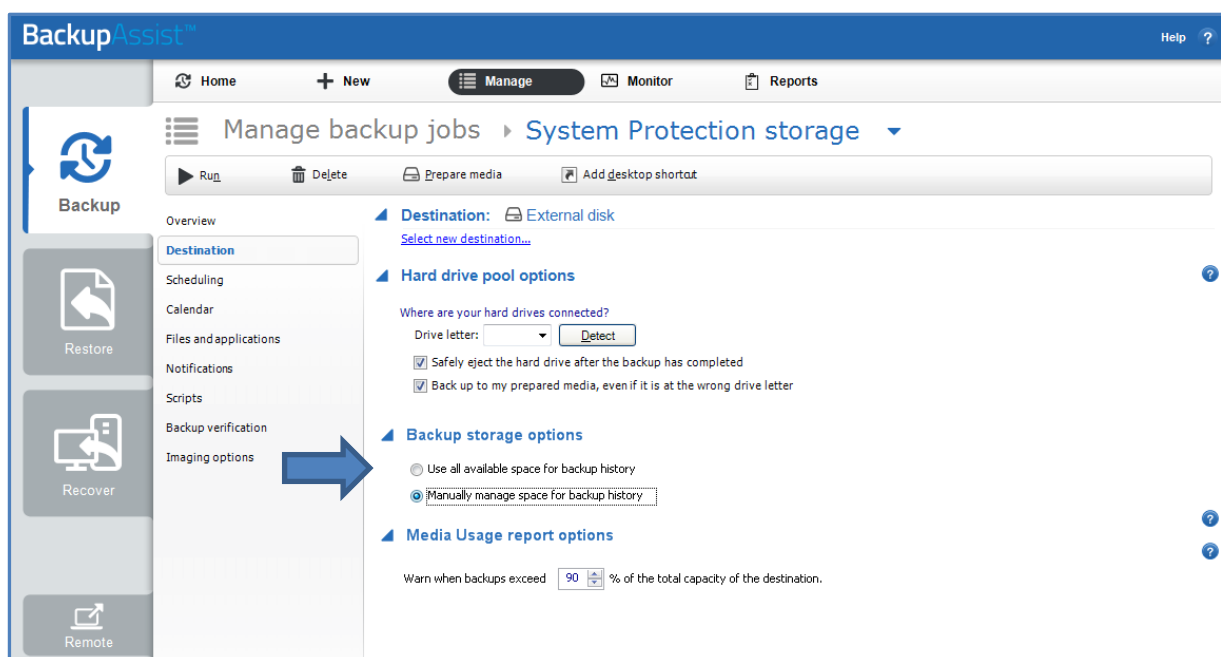

Figure 10: Imaging options - NEW Backup storage options

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 the *Shadow Copies* tab and access the *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.

Data container options

You can modify the size settings of a Data container, if the container does not exist. For example, if the backup job has not been run or if the container has been manually deleted.

To modify the size select **Destination** and go down to **Data container options***:*

- *Container size (GB):* Use the up and down arrows to set the size of the Data container.
- *Use all available space*: Tick this box and all available space on the destination device will be used by the Data container, up to 2TB.

Files and applications

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

The Volume Shadow Copy Service (VSS) is a Microsoft Service that creates a copy of an application's data (e.g. Exchange and SQL) so the data can be backed up without interfering with the application. BackupAssist will automatically detect *locally* running VSS applications and list them for selection during the **Destination** step of the backup job creation.

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

The Hyper-V process is automated but the restore requires both the *Exchange Granular Restore Add-on and the Hyper-V Granular Restore Add-on* licenses.

Scheduling

Selecting **Scheduling** will display the **Scheduling options.** You can use this screen to change the following settings for your scheme's daily backups: the time the backups run, how many times a day the backups run and the days of the week each backup runs on.

If you selected a scheme with archive backups (e.g. weekly, monthly), you can also specify when each archive backup will run. The current scheme is shown, along with two pop-up menus: *Select a new schedule* and *Customize schedule*.
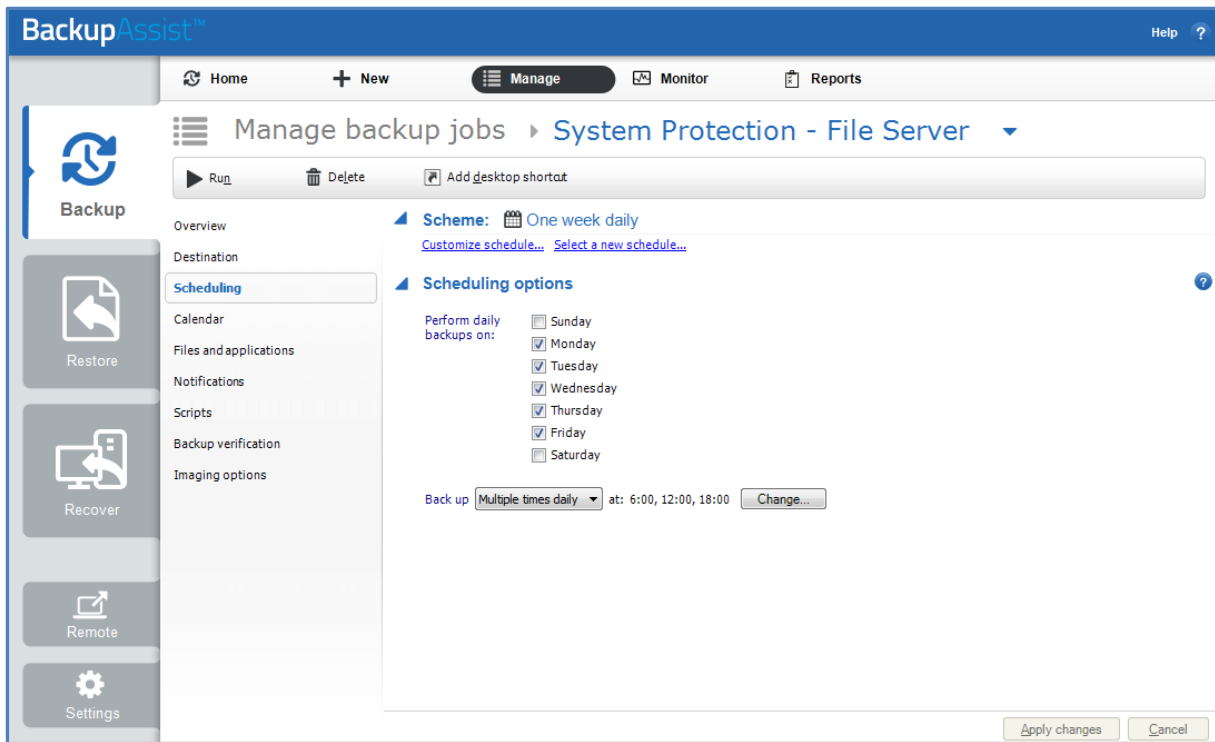

Figure 11: Manage Scheduling

Select a new Schedule: This will display the pre-configured backup schemes that you chose from during the creation of your backup job. The selections available will depend on the type of destination media you have selected. You can select a different scheme using this option.

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

The *Method* selection can only be *Automatic*. This is because when a System Protection backup job runs, it scans the data, identifies what has changed and updates the backup image (VHD file) with the data changes. This means you have a full image backup that is updated incrementally. In some circumstances (a new destination or a change to the backup job) a full backup will still be performed.

Selecting the *Incremental Windows Image Backups* option on the *Settings* tab (under *Windows settings*) makes Windows flag any data that changes, so that when the System Protection job is run, it does not need to scan the data selection to know what has changed. This makes the backup a lot quicker, but there is a performance overhead between backups due to Windows keeping track of the changed data. In some circumstances (a change the job's settings or destination) a full scan may be required.

Imaging options

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

VSS backup mode

The VSS Full / Copy options allow you to set how VSS views the backup. A full backup is recommended as it allows VSS to prune logs that would otherwise grow and consume disk space.

Shadow Copy Protection Mode (SPM) is a solution for backup jobs that are losing backup history.

In rare instances, VSS can delete backup history when the backup job is having trouble writing to the backup destination. This can occur in backups that use low performance (iSCSI / NAS with Data container) destinations. SPM allows a failed write by the backup job to be retried. If the retry does not work, the backup job will stop and report a failed backup job. No backup history will be lost.

Shadow Copy Protection Mode should only be used if you are experiencing backup history loss.

* If you are unsure if you have lost history, try a test restore from your oldest available backup.
* If you are using iSCSI / NAS with a Data container, try to resolve the problem by improving the performance of your network or backup destination, and use SPM if the problem persists.

There are two space management options with Shadow Copy Protection Mode:

* The GB selection is used to reserve space for SPM for storage management purposes.
* The storage space percentage bar, allows you to specify the amount of space reserved for historical backups. As the full backup grows, historical backups are deleted to make room. However, you can specify a % of protected space within which the historical backups cannot be deleted. These will be the most recent historical backups, and the backup job will report that the destination is full, rather than write over them.

  The full backup can use the reserved space, if the space is not being used by historical backups. For example, if 12.5 % is reserved on a 1TB drive, then 125GM will be reserved for historical backups. If the historical backups are only using 100GB, then the full backup can use 25GB of that reserved space.

BackupAssist manages the space at the backup destination for System Protection backups.

* If you are using Shadow Copy Protection Mode, you can set the percentage of protected storage space for the backup history.
* If you are not using Shadow Copy Protection Mode, the percentage of protected storage space is not managed by SPM so the bar will be set to BackupAssist's default of 12.5%

Quick Catalogue

Selecting this option means the cataloging phase is done without mounting the VHD file. That means the catalogue does not contain details of the files and folders that were backed up, it only contains the other metadata associated with the backup, such as backup destination, VSS metadata and VSS snapshot ID. Because the quick catalogue does not contain an index of files and folders, you cannot search for a specific file or folder in the restore console. The restore console does allow you to browse the files and folders in the backup, however it does this by mounting the backup VHD rather than using the data in the catalogue. This means that the backup must be available.

10. System Protection backup report

The reporting capabilities of BackupAssist greatly enhance the reliability and accuracy of backup jobs.

Below are some key sections of the backup report:

Errors / Warnings Summary

Shows the status of the backup, plus a list of any warnings or errors. This is displayed at the top of the report so you can see any important messages quickly.

Destination Check

Shows any problems encountered with the backup's destination, such as incorrect backup media being detected (due to human error in the media rotation process) or if no media is detected at all.

Recovery Options

This section explains the BIOS, EFI and Hyper-V guest recovery options available for each System Protection backup.

Backups (Restore points)

This new section will list all of the backups you have on the backup destination. This will make it easy to see what restore options are available, and how far back you can restore from.
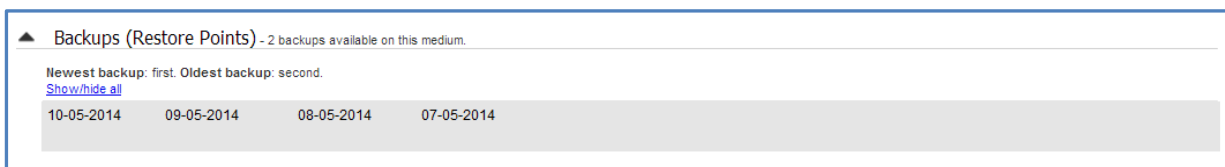

Figure 12: System Protection report - NEW Backup (Restore points)

Media usage

This section breaks down the space available at the backup destination for both the disk space and shadow storage. Shadow storage is used by VSS to store historical backup data from previous backup jobs. The example below shows the media usage report section for a Data container.
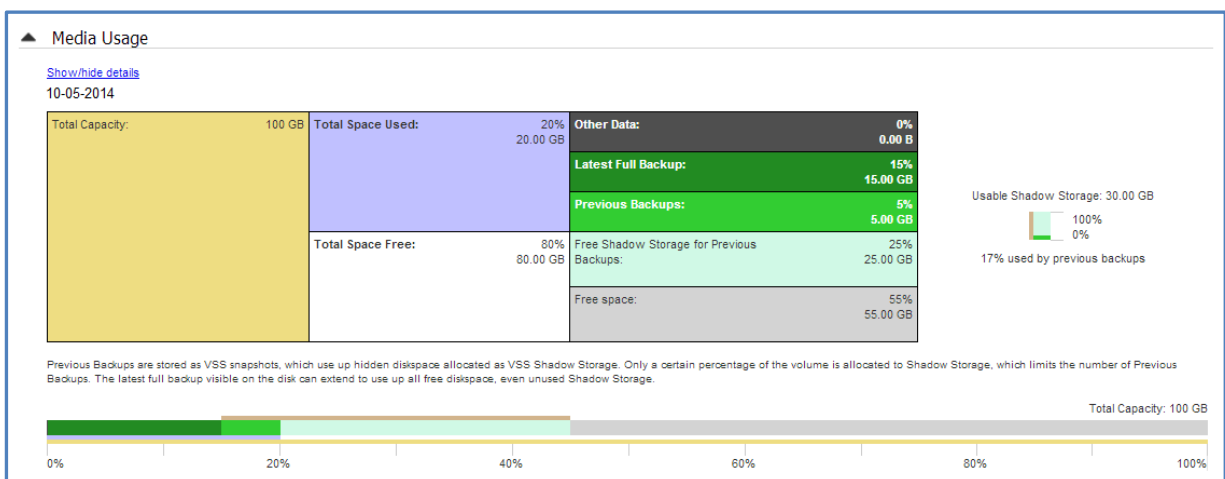

Figure 13: System Protection report – NEW Media usage section

Total Capacity of the backup destination is shown on the left. The usage graph breaks this amount down into **Used** and **Free** space, and then into more detailed allocations, such as shadow storage.

11. Support and Resources

Contacting Technical Support

Should you have any questions regarding either BackupAssist or System Protection, please email support@backupassist.com and we will respond to you as soon as possible.

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

Learn more – The Welcome Screen

Each tab in BackupAssist includes a "Learn More" link on the tab's **Home** page.

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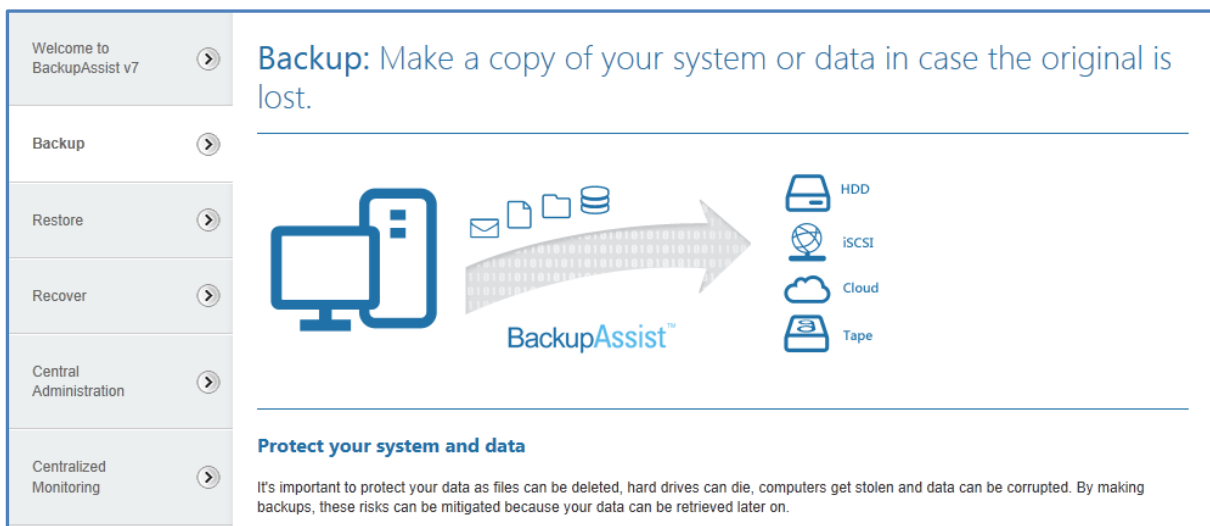

Figure 14: Backup tab - Welcome Screen