BackupAssist™ v9

Backup Scenarios

User Guide

backupassist.com

Contents

Backup considerations

This document explains common usage scenarios for BackupAssist. This is designed to enable system administrators to achieve data protection tasks in accordance with best practices.

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

VSS Application backups

The Volume Shadow Copy Service (VSS) is a Microsoft Windows Service that creates a copy of an application's data so the data can be backed up while the application is running. This means the data will not change or be locked while a backup is taking place. VSS also supports live application restores, so you do not need to stop an application before restoring a previous version of it.

BackupAssist is VSS-aware, so File Protection, File Archiving and System Protection backups can detect VSS applications such as Exchange, SQL, Hyper-V and SharePoint. BackupAssist will display a VSS application as an application container during the *Destination* step of the backup job's creation. You can select the container or individual components and BackupAssist will select the files that need to be backed up.

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.

File Protection and File Archiving can be used to back up and restore data, but if you want to recover your computer, the following should be considered when planning your backup strategy:

- **RecoverAssist bootable media**: BackupAssist's *Recover* tab can be used to create a customized, bootable recovery media. This media will start your computer and load a recovery environment that can access an image backup to recover your computer.
- **Bare-metal backup**: A BackupAssist **System Protection** backup can create a bare-metal image of your computer that *RecoverAssist* can use to recover your operating system and data.

  System Protection creates an image backup for Windows Vista, 7, 8, Windows Server 2008/12 and SBS 2008/11 computers. For older operating systems, System Protection will use NTBackup.

1. Disaster recovery

The best way to prepare for a full server recovery is to configure BackupAssist to perform System Protection (imaging) backups. That way your entire server can be restored with just the backup media and a bootable (RecoverAssist) recovery disc. This also allows for the fastest possible restores.

- To learn about BackupAssist Recovery, refer to the System Recovery guide.
- To learn about System Protection backups, refer to the System Protection guide.

Scenario 1: Daily backups with weekly archives and disaster recovery

Daily backups onto removable disk media

Backup type	System Protection	*Effectiveness:*	
		Open format:	Yes (VHD)
Backup Destination	External HDD, RDX	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Daily + Weekly	One step restore:	Yes
		Human intervention required	
Backup Process	Select the drives to backup, including the system drives. We recommend using a scheme that contains multiple disks for redundancy and onsite/offsite swapping, and a mixture of daily and weekly disks to provide a range of restore points.		
Recovery Process	Plug your backup device into a new machine, boot using a RecoverAssist disk (or Windows install disc), and launch the recovery environment, which will automatically partition your new disks and start the restore.		

Scenario 2: Manual disaster recovery backups as part of a preventative maintenance plan

Manual backups to removable disk media

Backup Engine	System Protection	*Effectiveness:*	
		Open format:	Yes (VHD)
Backup Destination	External HDD or RDX.	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Daily scheme, but suspend the job	One step restore:	Yes
		Human intervention required	
Backup Process	Select the drives to backup, including the system drives. Perform manual backups to an external disk device that is taken offsite. We recommend that your data is backed up daily by another backup job.		
Recovery Process	Follow the standard recovery process (as outlined above) to restore your entire system from the image backup. Then restore your data from the latest available data backup.		

Scenario 3: Fully automated daily backups with disaster recovery

Fully automated backups to NAS or local disk

Backup Engine	System Protection	*Effectiveness:*	
		Open format:	Yes (VHD)
Backup Destination	NAS or Local Disk	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Daily	One step restore:	Yes
		No human intervention required	
Backup Process	Select the drives to backup, including the system drives. Backups are performed automatically. Note: The file system of the backup device must be NTFS. Note: We do not recommend this strategy because it does not provide for offsite storage of the backups.		
Recovery Process	Follow the standard recovery process (as outlined above) to restore your entire system from the image backup.		

2. Network file backups on Server 2008

Windows Server 2008's block-level drive imaging features do not allow for backups of files via network shares. You can use the File Protection backups to overcome this limitation.

Scenario 1: Basic network file backup

Backup directly onto removable disk media

Backup Engine	File Protection Engine	*Effectiveness:*	
		Open format:	Yes
Backup Destination	External HDD or RDX	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Your choice, using multiple disks	One step restore:	Yes
		Human intervention required	
Backup Process	Select your network files and directories to back up. (You may of course choose local files as well.) We recommend using multiple disks to provide redundancy and onsite/offsite swapping, and a mixture of daily and weekly (and possibly monthly) disks to provide a range of backup history. In addition, using the Single Instance Store feature (activated by default) will save space and extend the amount of backup history available.		
Recovery Process	Copy the files from your backup media.		

Scenario 2: Local mirror of a network drive with additional archive backups

Mirror onto a central server, then back up the central server as part of a different backup job

Backup Engine	File Protection Engine	*Effectiveness:*	
		Open format:	Yes
Backup Destination	Local Directory	Offsite storage:	Yes (2nd job)
		Multiple backup media:	Yes (2nd job)
Backup Scheme	Mirror	One step restore:	Yes
		Human intervention required	
Backup Process	Select your network files and directories to back up. Using the Mirror scheme, every time the backup runs, a copy of the network files and directories will be taken and placed in your destination directory on a central server. Then set up a second job to back up this directory – for example, back this up as part of your server image, to provide version history and offsite storage.		
Recovery Process	Copy the files from your server's mirror, or if a past version is required, restore from your server's backup job.		

3. Maximizing backup history (Archives & version history)

There are situations in which you may need to restore an older version of a file than the one in your last backup. This might be necessary if a user has changed or deleted important information some time ago or if a malware infection began corrupting data weeks ago but has only just been discovered.

Use BackupAssist File Protection to make a copy of your data. Using the Single Instance Store feature will allow a large backup history to be stored with almost zero overhead for the data that is unchanged from day to day.

Scenario 1: Maximum version history with offsite backups

Backup onto removable disk media

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	External HDD or RDX	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Your choice, using multiple disks	One step restore:	Yes
		Human intervention required	
Backup Process	Select files and directories to back up. (You may choose local and network files.) We recommend using multiple disks to provide redundancy and onsite/offsite swapping, and a mixture of daily and weekly (and possibly monthly) disks to provide a range of backup history. Choose Backup mode with the Single Instance Store feature (activated by default) to provide archival backups with backup history.		
Recovery Process	Copy the files from your backup media.		

Scenario 2: Fully automated backups with maximum history

Fully automated backups to NAS or local directory

Backup Engine	File Protection Engine	*Effectiveness:*	
		Open format:	Yes
Backup Destination	NAS or Local Directory	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Mirror	One step restore:	Yes
		No human intervention required	
Backup Process	Select files and directories to back up. (You may choose local and network files.) Choose a backup scheme that allows for backup history, and activate the Single Instance Store feature to save space on the backup device and extend the backup history available. Note: This strategy does not store your data offsite. We recommend that you have another backup job that allows for offsite storage.		
Recovery Process	Copy the files from the backup.		

4. Backing up massive data sets

Backing up large datasets can been difficult. The main problem is that although only a small proportion of the data changes from day to day, it takes a long time to backup the full data set. Administrators use a mixture of full plus incremental backups, however this still takes a long time, and the restore process is more error prone due to a reliance on multiple backups for a single restore.

The File Protection backups overcome these problems because the daily backups are performed with the speed of differentials, but each backup looks like a full backup so the restore is a one step process. Additionally, the ever increasing size of hard drives means it is often possible to fit the entire data set on one disk or to use an external mass storage device to fit it onto one device. The initial backup to each device will be slow because a full transfer of all the data is required. However, subsequent backups will be fast because only changed and new files will need to be replicated.

Scenario 1: Basic backup with history for large data sets

Backup onto removable disk media

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	External HDD or RDX	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Your choice, using multiple disks	One step restore:	Yes
		Human intervention is required	
Backup Process	Select your files and directories to back up. (You may choose local and network files.) We recommend using multiple disks to provide redundancy and onsite/offsite swapping, and a mixture of daily and weekly (and possibly monthly) disks to provide a range of backup history. Choose Backup mode with the Single Instance Store feature to provide archival backups with backup history.		
Recovery Process	Copy the files from your backup media.		

Scenario 2: Fully automated backups with history for large data sets

Fully automated backups to NAS or local directory

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	Local Directory	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	A scheme with backup history	One step restore:	Yes
		No human intervention required	
Backup Process	Select your files and directories to back up. (You may choose local and network files.) Choose a backup scheme that allows for backup history, and activate the Single Instance Store feature to save space on the backup device and extend the backup history available. Note: This strategy does not store your data offsite. We recommend that you have another backup job that allows for offsite storage.		
Recovery Process	Copy the files from the backup.		

5. Overcoming slow backup media issues

In situations where the desired backup method is slow, the amount of data to be backed up is huge or the backup window is very short, a disk-to-disk-to-X strategy can be a good solution. Most commonly this is done by backing up one or more servers to a dedicated backup server using a fast differential or incremental backup method (such as File Protection or System Protection) and then copying the backup to the slow medium. This effectively extends the backup window of the second backup to the start of the next backup, or in the case of daily backups, close to 24 hours.

Use the File Protection feature to back up files to a backup server or to mass storage, and then use a different backup job to back up the backup.

Scenario 1: Single local backup with archives stored on slower removable media

File backup to backup server or mass storage

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	NAS or Local Directory	Offsite storage:	Yes (2nd job)
		Multiple backup media:	Yes (2nd job)
Backup Scheme	Mirror	One step restore:	Yes
		Human intervention required	
Backup Process	Select your files and directories to back up. Back up to a NAS or local directory using the mirror mode. Set up a second backup job to then back up the backup to slower media. This job should allow for backup history and offsite storage.		
Recovery Process	Simply copy the files from your either of your backups.		

Scenario 2: Single local backup with disaster recovery, and archives stored on slower media

Drive image backup to a backup server

Backup Engine	System Protection	*Effectiveness:*	
		Open format:	Yes (VHD)
Backup Destination	NAS	Offsite storage:	Yes (2nd job)
		Multiple backup media:	Yes (2nd job)
Backup Scheme	Daily	One step restore:	**Yes***
		Human intervention required	
Backup Process	Perform a full System Protection image backup to your backup server. Then set up another job on your backup server to back up this image to achieve backup history and offsite storage.		
Recovery Process	Recover your server as normal from the backup server. * In the case that your backup server is unavailable, then recover the backup server firstly, then your server. This becomes a two-step restore process.		

6. Backing up Hyper-V guests from the host

It is possible to backup Hyper-V guest machines while they are running. The VSS writer for Hyper-V means that the backups will be consistent, with no need to shut down the guest.

Use File Protection to copy the directories of the Hyper-V guests to your backup media. If you employ Scenario 1 using removable eSata drives, there will be zero downtime when you need to recover!

Scenario 1: Daily backups with weekly archives for Hyper-V

Backup onto removable disk media

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	External HDD or RDX (eSata recommended)	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Daily + Weekly	One step restore:	Yes
		Human intervention required	
Backup Process	Set up your job to back up the folders of your Hyper-V VMs (including configuration files and VHD files). We recommend using a scheme that contains multiple disks for redundancy and onsite/offsite swapping, and a mixture of daily and weekly disks to provide a range of restore points.		
Recovery Process	If your host computer's hardware fails, set up a new Hyper-V host and connect your backup device. If using eSata, you can run your host directly from the backup device at normal Sata speeds. Otherwise, copy your VMs from the backup onto the hard drive of the new host and run them from there.		

Scenario 2: Fully automated daily backups for Hyper-V

Fully automated backups to NAS or local directory

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	Local Directory or NAS	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Mirror to keep the last backup only, or any scheme with backup history	One step restore:	Yes
		No human intervention required	
Backup Process	Set up your job to back up the folders of your Hyper-V VMs (including configuration files and VHD files). Note: this strategy will not automatically give you offsite backups. We recommend backing up this backup in another job, such as an overall server backup to external HDD or tape.		
Recovery Process	If your host computer's hardware fails, set up a new Hyper-V host and copy the guest VMs files from the backup onto your new host. Run the VMs on the new host.		

7. Backing up VMware guests from the host

It is possible to backup VMware guest machines from the host, but it is necessary to suspend each machine, back it up, and then resume it. Therefore there will be a period of downtime. Use File Protection to copy the directories of the VMware guests to your backup media, and scripts before and after the backup job to suspend and resume the machines. If you employ Scenario 1 using a removable eSata disks, there will be zero downtime when you need to recover!

Scenario 1: Daily backups with weekly archives for VMware

Backup onto removable disk media

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	External HDD or RDX. (eSata recommended)	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Daily + Weekly	One step restore:	Yes
		Human intervention required	
Backup Process	Set up your job to back up the folders of your VMware VMs (including configuration files and VDMK files). We recommend using a scheme that contains multiple disks for redundancy and onsite/offsite swapping, and a mixture of daily and weekly disks to provide a range of restore points. In the Scripting section of your job, set up the pre-backup and post-backup scripts as explained below to suspend the VMs before, and resume the VMs after the backup.		
Recovery Process	If your host computer's hardware fails, set up a new VMware host and connect your backup device. If using eSata, you can run your host directly from the backup device (at normal Sata speeds). Otherwise, copy your VMs from the backup onto the hard drive of the new host and run them from there.		

Scenario 2: Fully automated daily backups for VMware

Fully automated backups

Backup Engine	File Protection	*Effectiveness:*	
		Open format:	Yes
Backup Destination	Local Directory or NAS	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Mirror to keep the last backup only, or any scheme with backup history	One step restore:	Yes
		No human intervention required	
Backup Process	Set up your job to back up the folders of your VMware VMs (including configuration files and VDMK files). In the Scripting section of your job, set up the pre-backup and post-backup scripts as explained below to suspend the VMs before, and resume the VMs after the backup. Note: this strategy will not automatically give you offsite backups. We recommend backing up this backup in another job, such as an overall server backup to external HDD or tape.		
Recovery Process	If your host computer's hardware fails, set up a new VMware host and copy the guest VMs files from the backup onto your new host. Run the VMs on the new host.		

Example scripts to suspend and resume VMware Guest VMs

These instructions apply to VMware Server 1.0.7 and modifications may need to be made for different versions.

For example, if you have 3 virtual machine guests, stored in C:\PathToVM1, C:\PathToVM2 and C:\PathToVM3. Locate the vmx (Virtual machine config files) in each path, and modify the example scripts below to suit.

Before each backup:

```
@echo off

echo Suspending VM 1

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM1\VMConfig1.vmx" suspend

echo Suspending VM 2

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM2\VMConfig2.vmx" suspend

echo Suspending VM 3

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM3\VMConfig3.vmx" suspend
```

After each backup:

```
@echo off

echo Resuming VM 1

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM1\VMConfig1.vmx" start

echo Resuming VM 2

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM2\VMConfig2.vmx" start

echo Resuming VM 3

call "c:\Program Files\VMware\VMware Server\vmware-cmd" "c:\PathToVM3\VMConfig3.vmx" start
```

Important: we recommend that you try running your batch files manually before running them from within BackupAssist. In some circumstances your VMs will not start because manual intervention is required – such as connecting virtual devices that are locked or nonexistent (e.g. a DVD drive that mounts an .ISO file that has been deleted). Running the batch files manually helps you make sure that your VM configuration will allow your VMs to start automatically.

Note: If you do not use the “call” command in your batch files, only the first command will be executed.

8. Backing up SQL servers

BackupAssist supports online SQL Server backups for local and remote SQL 2005, 2008, 2012 and 2014 Servers. BackupAssist also provides a convenient restore facility for disaster recovery and point in time restores.

It is also possible to configure BackupAssist to perform transactional backups as frequently as every five minutes.

Scenario 1: Daily online SQL backups with disaster recovery

Fully automated backups

Backup Engine	SQL Server Protection	*Effectiveness:*	
		Open format:	Yes (BAK)
Backup Destination	Local Directory	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Basic	One step restore:	**No**
		Human intervention required	
Backup Process	Add all required SQL Servers to the SQL job and set it to run overnight. Note that this strategy will not give you offsite backups. We recommend including the results of this backup in your normal system backup.		
Recovery Process	Open the BackupAssist console, click on the Restore tab and select SQL. Follow the instructions to restore a local or remote server.		

Scenario 2: Frequent SQL backups to minimize data loss with disaster recovery

Fully automated backups

Backup Engine	SQL Server Protection	*Effectiveness:*	
		Open format:	Yes (BAK)
Backup Destination	Local Directory	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Transactional	One step restore:	**No**
		No human intervention required	
Backup Process	Add all required local and remote SQL servers to the job and set the job to run as frequently as desired. BackupAssist will perform a full backup each morning and transactional backups during the day. Note that this strategy will not give you offsite backups. We recommend including the results of this backup in your normal system backup.		
Recovery Process	Open the BackupAssist console, click on the Restore tab and select SQL. Follow the instructions to restore a local or remote server completely, or to a specific point in time.		

9. Backing up Exchange servers

BackupAssist 8 and later can back up Exchange Server 2007, 2010 and 2013 using System Protection, File Protection and File archiving backups, and restore the full server of individual mail items using the Exchange Granular Restore Add-on.

Scenario 1: Daily online Exchange storage group backups			
Fully automated backups			
Backup Engine	System Protection	*Effectiveness:*	
		Open format:	Yes (BKF)
Backup Destination	External HDD or RDX	Offsite storage:	Yes
		Multiple backup media:	Yes
Backup Scheme	Daily + Weekly	One step restore:	Yes
		Human intervention required	
Backup Process	After completing the new job wizard, edit the job and add all required Exchange Servers. Select all storage groups for backup. An Information Store backup will back up the entire information store, including public folders and user mailboxes.		
Recovery Process	Open the BackupAssist console, click on the Restore tab and select Exchange. The restore process will only allow you to restore the entire information store – not just individual mailboxes or public folders. This is an “all or nothing” approach. For this reason, we recommend performing additional mailbox backups as described in Scenario 2.		

Scenario 2: Exchange mailbox backups			
Fully automated backups			
Backup Engine	Exchange Mailbox Protection	*Effectiveness:*	
		Open format:	Yes (PST)
Backup Destination	Local Directory	Offsite storage:	**No**
		Multiple backup media:	**No**
Backup Scheme	Basic	One step restore:	**No**
		No human intervention required	
Backup Process	Add all required local and remote Exchange Servers to the job. Note that this strategy will not give you offsite backups. We recommend including the results of this backup in your normal system backup. Also note that Exchange mailbox backups do not completely back up and protect your Exchange Server. We recommend combining mailbox backups with Information Store backups as described in Scenario 1 for complete protection.		
Recovery Process	The PST files can be loaded with Outlook. Individual emails can then be copied from the file. The PST files may also be imported directly into the Exchange Server by using Microsoft ExMerge.		