BackupAssist Common Usage Scenarios

WHITEPAPER

BackupAssist Version 5

www.BackupAssist.com

Table of Contents

Introduction

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

In each situation a number of alternative examples are given to show how the task can be achieved. You may use the examples directly or modify to suit the individual requirements and circumstances.

If you have feedback concerning this document, backup topics that you'd like to see covered, or any questions, please contact Linus Chang at linus.chang@backupassist.com.

Disaster recovery for Server 2008, SBS 2008 & EBS 2008

The best way to prepare for a full server recovery is to configure BackupAssist to perform drive imaging backups. That way your entire server can be restored with just the backup media and a recovery disc (such as the Windows installation disc). This also allows for the fastest possible restores. Refer to the "BackupAssist and Server 2008 White Paper" for a step-by-step guide to the restoration process.

Scenario 1: Daily backups with weekly archives and disaster recovery *Daily backups onto removable disk media*			
Backup Engine	Windows Imaging Engine	*Effectiveness:*	
Backup Destination	External HDD, rdx or REV	Open format:	Yes (VHD)
Backup Scheme	Daily + Weekly	Offsite storage:	Yes
		Multiple backup media:	Yes
		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 the Windows install disc (or a specially created recovery disc) and launch the Recovery Wizard, 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	Windows Imaging Engine	*Effectiveness:*	
Backup Destination	External HDD, rdx or REV.	Open format:	Yes (VHD)
Backup Scheme	Daily scheme, but suspend the job	Offsite storage:	Yes
		Multiple backup media:	Yes
		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	Windows Imaging Engine	*Effectiveness:*	
Backup Destination	NAS or Local Disk	Open format:	Yes (VHD)
Backup Scheme	Daily	Offsite storage:	**No**
		Multiple backup media:	**No**
		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.		

Network file backups on Server 2008

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

Scenario 1: Basic network file backup *Backup directly onto removable disk media*			
Backup Engine	File Replication Engine	*Effectiveness:*	
Backup Destination	External HDD, rdx or REV	Open format:	Yes
Backup Scheme	Your choice, using multiple disks	Offsite storage:	Yes
		Multiple backup media:	Yes
		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 Replication Engine	*Effectiveness:*	
Backup Destination	Local Directory	Open format:	Yes
Backup Scheme	Mirror	Offsite storage:	Yes (2nd job)
		Multiple backup media:	Yes (2nd job)
		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.		

Disaster recovery for Server 2003, Server 2000, XP & SBS 2003

The best way to prepare for a full server recovery is to configure BackupAssist to full backups using the NTBackup engine. Using the ASR option in NTBackup full bare metal restores can be achieved with just the backup, the Windows installation disc and a recovery diskette. Refer to the BackupAssist ASR Whitepaper for full details on performing ASR backups. Full backups without ASR can be used to perform a full recovery, but require a manual install of the OS.

Scenario 1: Daily backups with weekly archives and one step disaster recovery *Daily backups onto removable disk media*			
Backup Engine	NTBackup Engine	*Effectiveness:*	
Backup Destination	External HDD, rdx or REV	Open format:	Yes (BKF)
Backup Scheme	Daily + Weekly	Offsite storage:	Yes
		Multiple backup media:	Yes
		One step restore:	Yes
		Human intervention required	
Backup Process	Select the drives to backup, including the system drive. Once the job has been created, edit the Files and Folders section, select the 'Local system selections' tab and ensure the ASR option is checked. A floppy disk should be inserted before each backup, though the files required to create a new floppy will be stored on the backup media as well.		
Recovery Process	Plug in your backup device and insert the recovery diskette and the Windows install disc. Press F2 to start an ASR restore when prompted. This will automatically partition your disk and start the restore. Note that if a new drive is installed it must be at least as large as the original.		

Scenario 2: Daily backups with weekly archives and disaster recovery (no floppy drive) *Daily backups onto removable disk media*			
Backup Engine	NTBackup Engine	*Effectiveness:*	
Backup Destination	External HDD, rdx or REV.	Open format:	Yes (BKF)
Backup Scheme	Daily + Weekly	Offsite storage:	Yes
		Multiple backup media:	Yes
		One step restore:	**No**
		Human intervention required	
Backup Process	Select the drives to backup, including the system drive. Make sure the local system state is also selected for backup.		
Recovery Process	Install Windows from your Windows install disc. Open NTBackup and follow the instructions in the restore wizard to fully recover your server.		

Scenario 3: Fully automated daily backups with disaster recovery *Fully automated backups to NAS or local disk*			
Backup Engine	NTBackup Engine	*Effectiveness:*	
Backup Destination	NAS or Local Disk	Open format:	Yes (BKF)
Backup Scheme	Daily	Offsite storage:	**No**
		Multiple backup media:	**No**
		One step restore:	**No**
		No human intervention required	
Backup Process	Select the drives to backup, including the system drives and the local system state. Backups are performed automatically. Note: We do not recommend this strategy alone because it does not provide for offsite storage of the backups.		
Recovery Process	Follow the recovery procedure outlined in Scenario 2.		

Maximizing backup history for archival backup & version access

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 the File Replication Engine to copy data files. 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 Replication Engine	*Effectiveness:* Open format: Yes
Backup Destination	External HDD, rdx or REV	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 Replication 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.	

Backing up massive data sets

Some organizations have data sets that are terabytes in size. Traditionally, backing up this amount of data has 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.

The traditional approaches include performing full backups using tape autoloaders or manually spanning tapes. However, each backup may take many hours or even days to complete. Alternatively, some administrators use a mixture of full plus incremental backups. However this is also problematic – the full backup still takes too long, and the restore process is more error prone due to a reliance on multiple backups for a single restore.

The File Replication Engine is a superb tool for overcoming these problems because 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 (usually based on a striped RAID arrangement) to fit it onto one device. (At the time of writing, USB connected storage devices 2TB in size are readily available and retail for under $500).

Use the File Replication Engine to backup data files. 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 Replication Engine	*Effectiveness:* Open format: Yes Offsite storage: Yes Multiple backup media: Yes One step restore: Yes Human intervention is required
Backup Destination	External HDD, rdx or REV	
Backup Scheme	Your choice, using multiple disks	
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 (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 history for large data sets *Fully automated backups to NAS or local directory*		
Backup Engine	File Replication Engine	*Effectiveness:* Open format: Yes Offsite storage: **No** Multiple backup media: **No** One step restore: Yes **No** human intervention required
Backup Destination	Local Directory	
Backup Scheme	A scheme with backup history	
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.	

Overcoming problems with slow backup media: Disk-to-disk-to-X

In situations where the desired backup method is slow (e.g. Internet based backups), 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 the File Replication Engine or Windows Imaging Engine) 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 Replication Engine 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 Replication Engine	*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	Windows Imaging Engine	*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 drive 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.		

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 the File Replication Engine 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 Replication Engine	*Effectiveness:* Open format: Yes
Backup Destination	External HDD, rdx or REV. (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 Replication Engine	*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.	

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 the File Replication Engine 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 Replication Engine	*Effectiveness:* Open format: Yes Offsite storage: Yes Multiple backup media: Yes One step restore: Yes Human intervention required
Backup Destination	External HDD, rdx or REV. (eSata recommended)	
Backup Scheme	Daily + Weekly	
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 Replication Engine	*Effectiveness:* Open format: Yes Offsite storage: **No** Multiple backup media: **No** One step restore: Yes **No** human intervention required
Backup Destination	Local Directory or NAS	
Backup Scheme	Mirror to keep the last backup only, or any scheme with backup history	
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.

Backing up SQL servers

BackupAssist supports online SQL server backups for local and remote SQL 7, SQL 2003 and SQL 2008 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 Engine	*Effectiveness:* Open format: Yes (BAK) Offsite storage: **No** Multiple backup media: **No** One step restore: **No** Human intervention required
Backup Destination	Local Directory	
Backup Scheme	Basic	
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 restore. 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 Engine	*Effectiveness:* Open format: Yes (BAK) Offsite storage: **No** Multiple backup media: **No** One step restore: **No** **No** human intervention required
Backup Destination	Local Directory	
Backup Scheme	Transactional	
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 restore. Follow the instructions to restore a local or remote server completely, or to a specific point in time.	

Backing up Exchange servers

BackupAssist supports online Exchange server backup for local and remote Exchange 2000 and 2005 servers. It also supports online remote backups for Exchange 2007. BackupAssist will backup mailboxes in the PST format. Using the NTBackup Engine it is also possible to back up at the storage group level.

Scenario 1: Daily online Exchange storage group backups *Fully automated backups*		
Backup Engine	NTBackup Engine	*Effectiveness:* Open format: Yes (BKF) Offsite storage: Yes Multiple backup media: Yes One step restore: Yes Human intervention required
Backup Destination	External HDD, rdx or REV	
Backup Scheme	Daily + Weekly	
Backup Process	After completing the new job wizard, edit the job and add all required Exchange servers to the Exchange tab. 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 restore using NTBackup. Find and catalog the backup and select restore. Note that the detail side of the NTBackup restore screen will always be blank when a storage group has been selected. This is normal and does not mean that the backup is empty. Also note that 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 Engine	*Effectiveness:* Open format: Yes (PST) Offsite storage: **No** Multiple backup media: **No** One step restore: **No** **No** human intervention required
Backup Destination	Local Directory	
Backup Scheme	Basic	
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.	