

# Protecting Exchange Server 2007 Deployments on the Hitachi Adaptable Modular Storage 2000 Family with Symantec Backup Exec Off-host Backups

Best Practices and Tested Deployment Guide

*By Patricia Brailey*

July 2009

## Summary

E-mail systems are mission-critical applications for most businesses. When e-mail — or, more specifically, Microsoft® Exchange — goes down or performance degrades, businesses suffer. Internal and external communication channels are interrupted, which can affect user productivity, internal processes and, more importantly, revenue. In small to medium sized business, IT administrators often function in more than one role, charged with Exchange, storage and data protection responsibilities.

Exchange Server 2007 environments must be backed up regularly to prevent excessive disk capacity consumption and to capture validated recovery points that can be used to restore from when outages occur. Maintaining acceptable user experience levels, meeting service level agreements and ensuring regulatory compliance are critical objectives for IT administrators, but these are critical success factors for Exchange administrators in many organizations. This means that businesses of all sizes need data protection solutions that are easy to deploy and maintain, provide granular recovery capabilities, are cost effective to implement, and that allow business needs, rather than resource availability, to dictate backup timing.

Hitachi Data Systems offers a data protection solution that meets these needs. Using the Hitachi Adaptable Modular Storage 2000 family, it seamlessly integrates with Symantec Backup Exec, provides an easy-to-use interface, allows IT administrators to “fire and forget” and uses best-in-class replication technologies.

This white paper, which describes best practices for this solution, is intended for organizations that are experiencing difficulties achieving validated backups of Exchange Server 2007 within the allotted backup window on a consistent basis.

## Contributors

The information included in this document represents the expertise, feedback and suggestions of a number of skilled practitioners. The author recognizes and sincerely thanks the following contributors and reviewers of this document:

- Rudy Castillo
- Naoki Hino
- Larry Meese
- Lisa Pampuch
- Manoj Rajagopalan
- Michael Shaler

# Table of Contents

<b>Solution Overview .....</b>	<b>2</b>
Hitachi Adaptable Modular Storage 2000 Family .....	4
Microsoft VSS Overview.....	5
Hitachi ShadowImage In-System Replication Software .....	7
Hitachi VSS Hardware Provider .....	7
Symantec Backup Exec 12.5 .....	8
<b>Tested Deployment .....</b>	<b>9</b>
Scenarios .....	9
Hardware.....	9
Software .....	10
Storage Configuration .....	12
<b>Best Practices.....</b>	<b>13</b>
Exchange .....	13
Deployment .....	14
Backup Exec .....	14
<b>Conclusion.....</b>	<b>15</b>

# Protecting Exchange Server 2007 Deployments on the Hitachi Adaptable Modular Storage 2000 Family with Symantec Backup Exec Off-host Backups

## Best Practices and Tested Deployment Guide

*By Patricia Brailey*

E-mail systems are mission-critical applications for most businesses. When e-mail — or, more specifically, Microsoft® Exchange — goes down or performance degrades, businesses suffer. Internal and external communication channels are interrupted, which can affect user productivity, internal processes and, more importantly, revenue. In small to medium sized business, IT administrators often function in more than one role, charged with Exchange, storage and data protection responsibilities.

Exchange Server 2007 environments must be backed up regularly to prevent excessive disk capacity consumption and to capture validated recovery points when outages occur. Maintaining acceptable user experience levels, meeting service level agreements and ensuring regulatory compliance are critical objectives for IT administrators. This means that businesses of all sizes need data protection solutions that are easy to deploy and maintain, provide granular recovery capabilities, are inexpensive to implement, and that allow business needs, rather than resource availability, to dictate backup timing.

This paper describes Hitachi Data Systems' off-host based, data protection solution that meets these needs. Although the Hitachi Adaptable Modular Storage 2100 was used in the testing, this solution is applicable to any member of the Hitachi Adaptable Modular Storage 2000 family. The Hitachi Adaptable Modular Storage 2000 family provides a reliable, flexible and cost-effective storage platform for demanding applications like Microsoft Exchange Server. This solution seamlessly integrates with Symantec Backup Exec and Microsoft Volume ShadowCopy Services (VSS). It provides an easy-to-use interface, allows IT administrators to "fire and forget" and uses best-in-class replication technologies.

This paper is intended for organizations that are experiencing difficulties achieving validated backups of Exchange Server 2007 consistently within the established backup window, and that need to restore and recover their Exchange Server 2007 environments at the following levels:

- Full server
- Storage group
- User mailbox
- Messages

These levels of recovery needs can result from a number of problems, including hardware failures, virus attacks, database corruptions and more.

This white paper is intended for use by IT administrators at small to medium size companies responsible for Exchange, data protection or storage. It assumes a working knowledge of Exchange Server 2007 and how to perform basic backups.

## Solution Overview

This white paper provides best practices on how to configure a Hitachi Adaptable Modular Storage 2000 family storage system for use in an Exchange 2007 environment that is backed up using the Hitachi VSS Hardware provider and Symantec Backup Exec 12.5 for Windows servers. This is an ideal solution for backing up Exchange 2007 data because it virtually eliminates the need for a backup window, alleviates load from the Exchange server, and provides quick recovery options for a wide range of restore scenarios ranging from an entire Exchange server down to an individual object level such as a mailbox or individual mail message. Included are details regarding the test environment and methods used to validate the protection solution. For information about how to deploy and configure the environment see the [Deploying Symantec Backup Exec Off-host Backups for Exchange Server 2007 on the Hitachi Adaptable Modular Storage 2000 Family Installation and Configuration Guide](#) white paper.

Your choice of protection technologies for Exchange Server 2007 is expansive, including Microsoft's first generation of in-box continuous replication technologies, local continuous replication (LCR) and clustered continuous replication (CCR). With the addition of these native Exchange 2007 protection options, you must carefully weigh the various risks and benefits that such individual or combined solutions provide. All protection technologies replicate data to allow for recovery at a later time. Table 1 compares the primary purpose of off-host and continuous replication protection technologies.

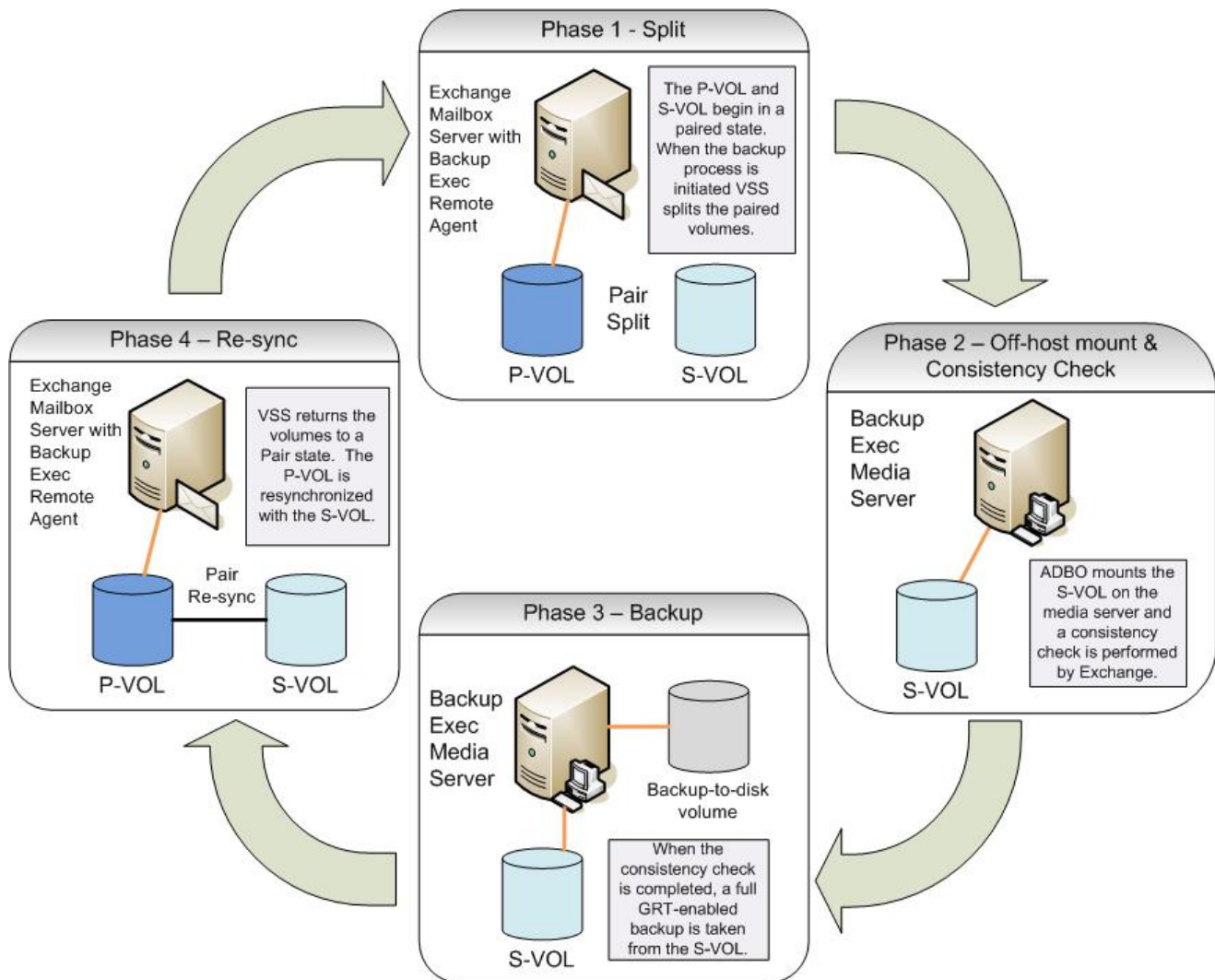
**Table 1. Exchange Protection Technology Comparison**

<i>Protection Technology</i>	<i>Purpose</i>
Off-host backup to disk or tape using Hitachi VSS Hardware Provider	Long-term data retention Quick recovery of individual Exchange items like e-mail messages Disaster recovery Enhanced availability
LCR	Recovery from data corruption or local disk failure Quick recovery of an entire Exchange storage group
CCR	Recovery from server failure Easy system maintenance Enhanced availability Disaster recovery when combined with standby continuous replication

Off-host backup is a well-known and widely adopted method of transferring the resource intensive backup process from a production server to an intermediary system. In this solution, Hitachi ShadowImage® In-System Replication software, Backup Exec and options such as the Advanced Disk Based Option (ADBO), and VSS is used to create an I/O consistent, point-in-time copy, also known as a ShadowImage secondary volume (S-VOL), of the required Exchange 2007 production LUs. In turn, the S-VOL is presented to the Backup Exec Media Server where it is validated for consistency using the Exchange 2007 ESEUTIL utility and backed up to disk or tape using Backup Exec and its agent for Microsoft Exchange Server.

Employing Hitachi ShadowImage In-System Replication and Backup Exec software for off-host backup requires minimal overhead and does not interfere with operations or resources on the production Exchange 2007 systems. This allows administrators to dictate when backups need to occur based on business needs, instead of the backups being controlled by the availability of resources or limited to a specific and ever shrinking backup window. Figure 1 depicts the off-host backup process.

**Figure 1. Off-host Backup Process**



This solution delivers a broad range of the restore and recovery options as outlined earlier, each of which is pragmatic and straightforward at a time when an inadvertent mouse click, a typo or a missed step could elongate an outage and add to the costs an organization must absorb. Administrators can perform common restore operations, such as single object/item restores, full server restores and in-between scenarios quickly and easily. The Exchange 2007 continuous replication offerings are built upon log shipping technology and cannot address the backup or restore scenarios that an off-host backup solution can as they primarily protect against hardware failures and are intended to enhance availability. This off-host backup solution can be integrated with Exchange 2007 CCR or it can be extended using Hitachi TrueCopy® Remote Replication software or the Hitachi Storage Cluster solution to provide stringent levels of protection and availability regardless of data center locations.

For more information about Microsoft's continuous replication technologies and how they integrate with 2000 family storage systems, see the [Protecting Hitachi Adaptable Modular Storage 2000 Family and Exchange 2007 Environments with Continuous Replication](#) white paper from Hitachi Data Systems.

For more information about Hitachi TrueCopy Remote Replication software, see the [Hitachi Data Systems Web site](#).

A review of each technology's purpose reveals that they cannot be directly substituted for one another. For more information about the tradeoffs involved with protection technologies, see the MExchange.org article by Dr. Vas Srinivasan and Bilal Ahmed, [High Availability and Disaster Recovery for Exchange Servers - A Comparative Analysis](#).

Instead of deploying either off-host backup or replication, consider deploying a combination of technologies to achieve these goals:

- Maximum protection coverage
- Multiple recovery capabilities
- Higher availability
- Enhanced disaster recovery
- Long-term preservation of key Exchange data

## Hitachi Adaptable Modular Storage 2000 Family

The Hitachi Adaptable Modular Storage 2000 family provides a reliable, flexible, scalable and cost effective modular storage system for the Microsoft Exchange and Symantec Backup Exec protection solution described in this white paper. The 2000 family is ideal for demanding application requirements and delivers enterprise class performance, capacity and functionality at a midrange price.

The 2000 family is the only midrange storage product with symmetric active-active controllers that provide integrated, automated hardware-based, front-to-back-end I/O load balancing. This ensures I/O traffic to back-end disk devices is dynamically managed, balanced and shared equally across both controllers, even if the I/O load to specific logical units (LUs) is skewed. Storage administrators are no longer required to manually define specific affinities between LUs and controllers, simplifying overall administration. In addition, this new controller design is fully integrated with standard host-based multipathing, thereby eliminating mandatory requirements to implement proprietary multipathing software. Because the 2000 family provides native support for Windows Server 2008 MPIO, organizations that deploy it can potentially eliminate the additional acquisition costs and reduce management overhead associated with third-party multipathing offerings.

However, deploying the 2000 family with Hitachi Dynamic Link Manager Advanced software creates a comprehensive multipathing solution that provides robust path failover, load balancing capabilities and integrated path management. It improves access to and availability of storage by distributing loads across multiple paths and from one path to another in the event of a path failure. Hitachi Dynamic Link Manager Advanced software provides centralized multipath storage connection management and reporting capabilities that drastically increase administrator efficiency and minimize configuration errors. These integrated path management capabilities improve system reliability and reduce downtime with automated path health checks, reporting alerts and error information from each host to assist with rapid problem troubleshooting.

No other midrange storage product that scales beyond 100TB has a serial attached SCSI (SAS) drive interface. The point-to-point back-end design virtually eliminates I/O transfer delays and contention associated with Fibre Channel arbitration and provides significantly higher bandwidth and I/O concurrency. It also isolates any component failures that might occur on back-end I/O paths.

### *Hitachi Adaptable Modular Storage 2100*

Three models make up the Hitachi Adaptable Modular Storage 2000 family: the 2100, 2300 and the 2500. Although the Hitachi Adaptable Modular Storage 2100 was used in the testing of this solution, the information in this paper is relevant and applicable to the other 2000 family members. The 2100 is an easy-to-use, scalable, cost effective storage system for mission-critical business applications like Exchange Server 2007. It is also a top choice for tiered and standalone storage, consolidation, business continuity, data replication, backup and archiving. The 2100 offers a rich set of features in a model that scales to 120 disk drives. Table 2 lists some of the 2100's specifications.

**Table 2. Hitachi Adaptable Modular Storage 2100 Specifications**

<b>Raw capacity</b>	118TB SATA 52TB SAS
<b>Internal disk drives (SAS unless otherwise noted)</b>	146GB (15K RPM) 300GB (15K RPM) 400GB (10K RPM) 450GB (15K RPM) 500GB SATA II (7200 RPM) 1TB SATA II (7200 RPM)
<b>Disk drive interfaces</b>	SAS and SATA
<b>Host interfaces</b>	Fibre Channel: 1, 2 or 4Gb/sec iSCSI: GigE
<b>Maximum host connections</b>	4 Fibre Channel or 4 iSCSI
<b>Maximum attached hosts through virtual ports</b>	512
<b>SAS links</b>	16
<b>Maximum number of LUs</b>	2048
<b>Maximum LU size</b>	60TB
<b>Controller cache (per system)</b>	4GB to 8GB

## Microsoft VSS Overview

Volume Shadow Copy Service (VSS) is part of Microsoft File and Storage services framework and provides the backup infrastructure for the Windows operating system. VSS in the context of storage hardware provides the ability to perform point-in-time backups using storage assisted technologies like Hitachi ShadowImage software. Requestors, writers and providers communicate in the VSS framework to create and restore volume shadow copies. A shadow copy of a volume is a point-in-time replica of all contents residing on the original volume. Microsoft's VSS was introduced in Windows Server 2003, and Windows Server 2008 contains an enhanced version of the framework. The Volume Shadow Copy Service has three main components. Table 3 provides the definitions of these components.

**Table 3. Volume Shadow Copy Service Components**

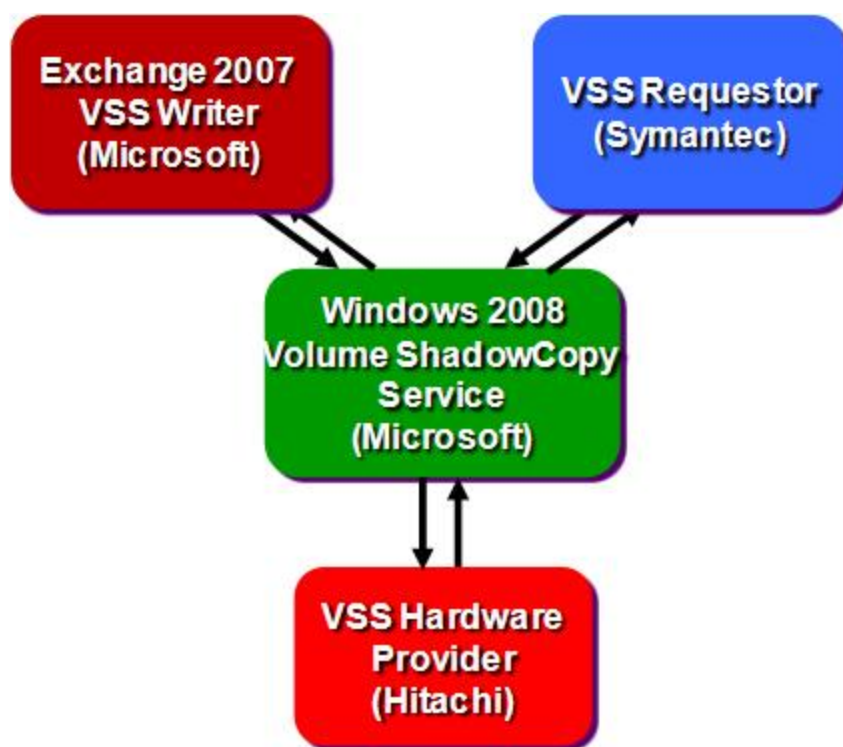
<b>Component</b>	<b>Description</b>
Requestor	Application, such as Backup Exec, that requests that a volume shadow copy be taken.
Writer	Software that is included in applications, such as Exchange 2007, that coordinates I/O operations with VSS shadow copy and shadow copy related operations (such as backups and restores) so that the data contained on the shadow copied volume is in a consistent state.
Provider	Component that creates and maintains shadow copies. A VSS hardware provider is a storage vendor supplied component used during a VSS backup process.

A requestor controls the backup process within the VSS framework. When a Backup request is initiated by the requestor, the VSS service instructs the writer to prepare a dataset for backup. When everything is ready, a command is sent to the provider to create a shadow copy. The Exchange VSS Writer is automatically installed with Exchange Server 2007 and the service is a default service with Windows Server 2008.

The Microsoft VSS framework facilitates taking I/O consistent snapshots of Exchange 2007 storage groups by freezing write I/O temporarily, advancing the checkpoint file and flushing cache buffers prior to obtaining the actual snapshot (shadow copy volume) via the Hitachi VSS Hardware Provider. The Shadow copy volume is then imported on the Backup Exec media server where an Exchange 2007 ESEUTIL integrity check is performed on the shadow copy volumes and they are subsequently backed up to disk or tape in an off-host scenario.

Figure 2 illustrates each component and the technology owner of the VSS framework deployed for the off-host solution.

**Figure 2. VSS Framework**



For more information about requestors, writers and providers, see the Microsoft Developer Network article [Basic VSS Concepts](#).

The VSS provider is responsible for managing and maintaining the shadow copy volumes. It is a critical component because it is the engine that performs the data replication or copy processes and related activities. The following list outlines and describes the types of providers supported by the Microsoft VSS framework.

- The system provider is made available through an installation of Windows Server 2008 and its current implementation is a specific instance of a software provider. Windows Server 2008 uses a copy-on-write technique on the production host to capture and maintain a point-in-time view of the LUs or volumes that comprise a shadow copy.
- As the name implies, software-based providers create and maintain shadow copies using software that runs on the production host, typically in the form of a kernel mode storage filter driver. This design is necessary to accurately and consistently capture and process application-specific I/O requests so that changes can be tracked and applied against the shadow copy recreate the LUs or volumes when necessary. In addition to

supporting workloads and activities on a production system, resources on the production hosts are used by a software (system) provider to perform its tasks.

- Hardware-based providers capture changes and replicate the corresponding data at the storage hardware or controller level by using block-based or similar copy-on-write, storage-based software or firmware. Hardware providers replicate at the LU level and maintain a bit-for-bit, block-for-block copy of disks that comprise a LU. Because the replication occurs at the LU level with hardware providers, VSS maintains the required volume and disk mappings from the host perspective. Hardware providers are installed and run on the production host, but the computation and processing related to the replication process is performed by resources on the storage hardware.

Host-based replication leverages software providers, while storage-based replication solutions utilize hardware providers in the protection solutions that are developed around VSS. Storage-based replication removes processing overhead on the production required to manage and maintain shadow copies and provides extremely fast operations by leveraging storage hardware resources and taking advantage of its advanced technologies and intelligence.

## Hitachi ShadowImage In-System Replication Software

Hitachi's ShadowImage In-System Replication software uses local mirroring technology to create full-volume copies or clones within the 2000 family. Although ShadowImage software is the underlying technology that replicates the volumes necessary to perform an off-host backup, it cannot be used to achieve consistent, point-in-time backups of Exchange 2007 without integrating into the Microsoft VSS framework. This integration occurs through the Hitachi VSS Hardware Provider, which is addressed in an upcoming section.

A volume pair is created when you take the following actions:

1. Select a volume that you want to replicate.
2. Identify another volume that will contain the copy.
3. Associate the primary and secondary volumes.
4. Copy all primary volume data to the secondary volume.

When the initial copy is made, all data on the primary volume (P-VOL) is asynchronously copied to the secondary volume (S-VOL) at the block level. The P-VOL remains available for read and write I/O during the pair operation and, due to its asynchronous nature, the P-VOL is not affected by the replication process. Write operations or changes performed against the P-VOL are marked in cache-based bitmaps and replicated to the S-VOL.

The P-VOL and S-VOL remain synchronized until they are split. When the S-VOL is split from the P-VOL, it contains a mirror image of the P-VOL at that point in time, a process also known as establishing a clone. After the pair is split, the secondary volume can be used for offline testing, analytical purposes or, in this solution's case, the Exchange 2007 ESETUIL consistency check and Backup Exec backup process. Because no dependencies exist between the primary and secondary volumes, each can be written to and read from by separate hosts. Changes to both volumes are tracked via the bitmaps so they can be re-synchronized. The bitmaps reside in and are protected and preserved by non-volatile, battery-backed cache and a dedicated differential management LU (DMLU) to ensure the integrity of the replication process.

For more information about ShadowImage software, see the ShadowImage In-System Replication User's Guide that accompanies the software.

## Hitachi VSS Hardware Provider

The Hitachi VSS Hardware Provider works with Microsoft's Volume Shadow Copy Service (VSS) to generate consistent point-in-time copies of data known as shadow copies. Through the Hitachi VSS Hardware Provider, ShadowImage pairs for the Exchange 2007 storage group and log LUs are created; the provider splits the pair during the backup operation so an off-host backup can take place. This is an extremely fast process that comfortably occurs within the allotted ten second window as defined by Microsoft in the VSS framework. Ten

seconds is the maximum amount of time that can lapse during the commit phase when the write I/O to the Exchange 2007 storage group and log LUs are being queued or frozen by the Exchange 2007 VSS Writer.

The result effectively reduces the backup window to a matter of a few seconds, as the S-VOL — not the Exchange 2007 production LUs — are used as the source LUs to perform the integrity check and off-host backup processes. In addition, the Hitachi VSS Hardware Provider permits secondary volume to also be used as the source for additional backups, using VSS aware Backup Applications like BUE as is the case in this solution.

For Exchange 2007 backups to occur on a Hitachi Adaptable Modular Storage 2000 family storage system in this solution, the Hitachi VSS Hardware provider must be installed on both the Exchange mailbox server and Backup Exec media server. Download Hitachi VSS Hardware Provider from the [Symantec solutions page](#) on Hitachi Data Systems Web site. Click the link in the Download section on the right side of the Web page.

## Symantec Backup Exec 12.5

Symantec Backup Exec for Windows Servers is data management software that provides fast, reliable backup and restore capabilities for servers and workstations across networks. Backup Exec is ideal for small to medium environments that are mostly composed of Windows servers. Table 4 lists Backup Exec components needed for this solution.

**Table 4. Required Backup Exec Components**

<i>Backup Exec Component</i>	<i>Description</i>
Agent for Microsoft Exchange Server	To backup the Exchange databases you must install the Backup Exec Exchange Agent. The Exchange agent allows you to select storage groups for backup and restore jobs, or to select one or more databases within the storage group for backup and restore jobs. Installing the Exchange agent also gives you the ability to restore individual databases or storage groups from snapshot backups.
Advanced Open File Option	To use snapshot technologies, such as ShadowImage with the Hitachi VSS Provider, you must install the Advanced Open File Option (AOFO). AOFO uses open file and copy technologies to alleviate issues that are sometimes encountered during backup operations, such as protecting open files and managing shortened backup windows. For Exchange 2007, Backup Exec automatically performs snapshot backups, so you do not need to select options for the AOFO when creating backup jobs.
Advanced Disk-based Backup Option	The Advanced Disk-based Backup Option (ADBO) provides several features including off-host backup. Off-host backup moves the backup operation away from the Exchange mailbox server to the Backup Exec media server. When the backup is moved to the media server, the Exchange mailbox server is free for other operations. Off-host backup for Exchange Server backups that have the GRT option enabled are also supported.
Granular Recovery Technology	Backup Exec's agent for Microsoft Exchange takes advantage of GRT functionality that allows you to restore individual items from an information store backup without having to restore the whole backup. This functionality does not require a separate install as it is part of the Agent for Microsoft Exchange.

## Tested Deployment

The following sections describe the configuration used for building and validating the backup and restore scenarios documented in this white paper.

### Scenarios

The following backup and restore scenarios were tested for the solution described in this white paper:

- Full off-host backup of an Exchange 2007 information store
- Full off-host backup with GRT enabled of an Exchange 2007 information store
- Full backup of an Exchange 2007 information store
- Restore a storage group to the same location
- Restore a storage group to a recovery storage group and recover a single mailbox
- Restore a single e-mail message or other Exchange objects from a GRT backup

### Hardware

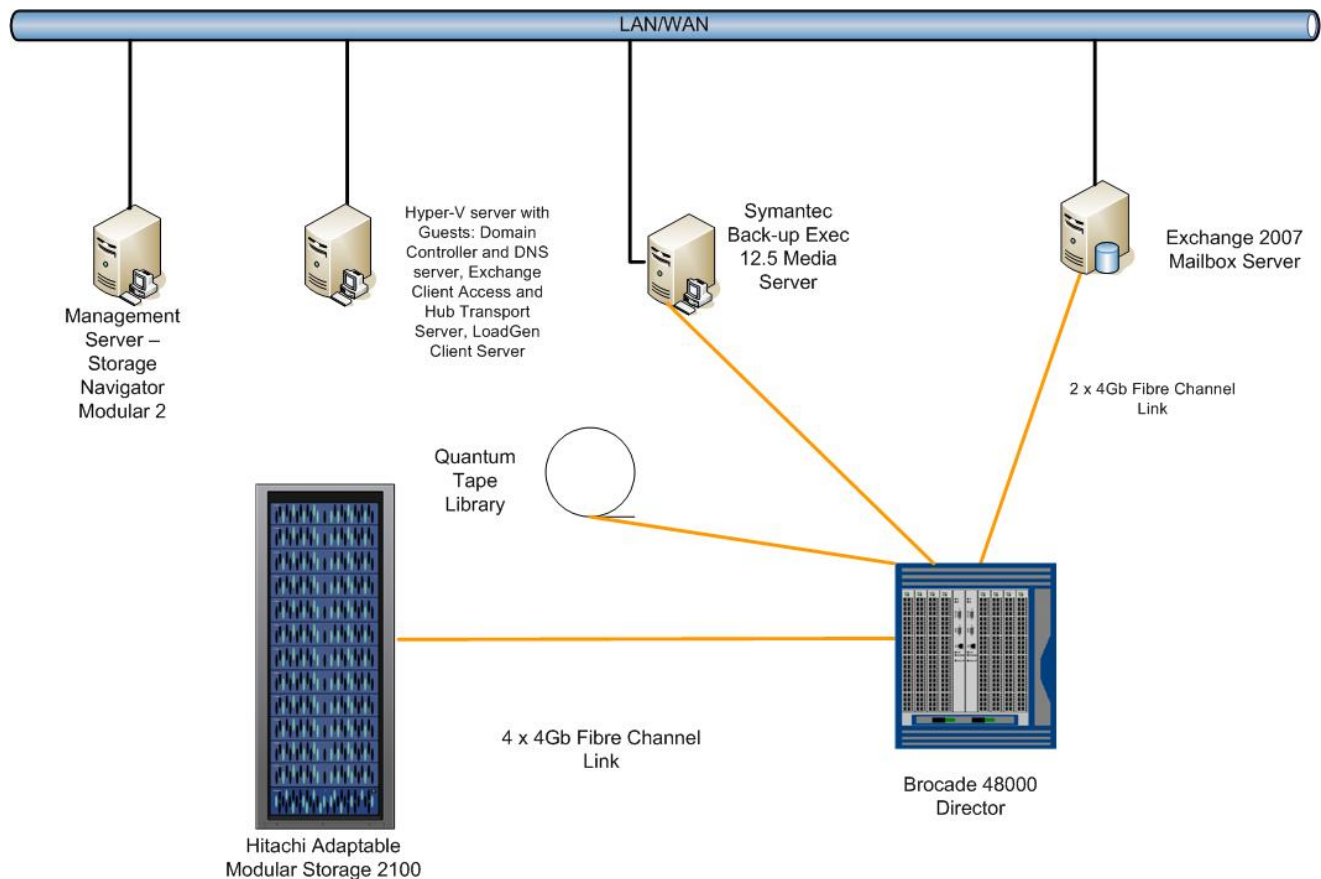
To support the backup and restore scenarios, a Hitachi Adaptable Modular Storage 2100 storage system was used. A Brocade 48000 director was used as the storage area network (SAN) backbone. Two Emulex LightPulse LPe111-H host bus adapters (HBAs) were used in the server housing the Exchange Mailbox role, and four of these HBAs were used in the Backup Exec media server. Table 5 lists server specifications.

**Table 5. Server Specifications for Backup and Restore Testing**

<i>Number of Servers</i>	<i>Server Make and Model</i>	<i>Role</i>	<i>Memory and Processor</i>
1	HP DL385	Mailbox server	16GB memory, 2 x dual-core AMD processors
1	HP DL385	Back-up Exec 12.5 media server	16GB memory, 2x dual-core AMD processors
1	Dell R905	Windows 2008 Hyper-V with three guests: <ul style="list-style-type: none"><li>• Domain Controller and DNS</li><li>• Exchange Client Access and Hub Transport</li><li>• LoadGen Client Server</li></ul>	128GB memory, 4 x quad-core AMD processors
1	Dell PowerEdge 750	Management server – Hitachi Storage Navigator Modular 2	2GB memory, 2 x Intel Xeon processors

Figure 3 illustrates the test environment topology.

Figure 3. Test Environment Topology



## Software

The following software was used in the test environment:

- Microsoft Windows Server 2008 SP1
- Microsoft Exchange Server 2007 SP1
- Symantec Backup Exec 12.5 for Windows Servers with Service Pack 2
- Hitachi ShadowImage In-System Replication Software
- Hitachi VSS Hardware Provider v3.2
- Microsoft Exchange Load Generator v08.02.0045.000
- Hitachi Storage Navigator Modular 2 v5.02

The level of Hitachi Adaptable Modular Storage firmware that was used in this test was 0860/A-M.

### *Service Packs and Hotfixes*

The Symantec Live Update feature was used to install the latest service pack on the media server and the remote servers. For this solution, Service Pack 2 is required. In addition, the following hotfixes are required:

- Backup Exec 12.5 for Windows Servers revision 2213 hotfix 322898, Device Driver Installer, 64-bit download
- Backup Exec 12.5 for Windows Servers revision 2213 hotfix 324011, 64-bit download

LoadGen was used to simulate an active Exchange 2007 environment. Table 6 lists the parameters used to set up the LoadGen simulation for all backup and restore scenarios.

**Table 6. LoadGen Test Parameters**

<b>Number of Storage Groups</b>	1
<b>Number of Databases per Storage Group</b>	1
<b>Number of Users per Database</b>	200
<b>Outlook Profile</b>	Outlook 2007 Cached
<b>User Profile</b>	Very Heavy

### *Backup Exec Configuration*

Table 7 lists the Backup Exec configurations needed for each Exchange backup and restore scenario. All scenarios use a backup-to-disk folder as the Device Destination.

**Table 7. Backup Exec Configurations**

<b>Scenario</b>	<b>Selection</b>	<b>Information Store Backup Method</b>	<b>ADBO</b>	<b>Exchange Options</b>
Full off-host backup of an Exchange 2007 Information Store	Storage group	Full – Database & Logs (flush committed logs)	Use off-host backup to move backup processing from remote computer to media server. Snapshot provider: Hardware	Perform consistency check before backup when using Microsoft VSS snapshot provider.
Full off-host Backup using the GRT option of an Exchange 2007 Information Store	Storage group	Full – Database & Logs (flush committed logs)	Use off-host backup to move backup processing from remote computer to media server. Snapshot provider: Hardware	Perform consistency check before backup when using Microsoft VSS snapshot provider. Use Backup Exec GRT option.
Full backup of an Exchange 2007 Information Store	Storage group	Full – Database & Logs (flush committed logs)	No options checked.	Perform consistency check before backup when using Microsoft VSS snapshot provider.
Restore a Storage Group to the same location	Storage group	N/A	N/A	When restoring individual mail messages and folders, restore over existing messages and folders. Restore desired transaction logs.

<i>Scenario</i>	<i>Selection</i>	<i>Information Store Backup Method</i>	<i>ADBO</i>	<i>Exchange Options</i>
Restore a single mailbox from a GRT backup	E-mail message	N/A	N/A	No Exchange options modified.

## Storage Configuration

This test deployment uses a Hitachi Adaptable Modular Storage 2100 with two trays of 300GB 15K SAS drives. In addition to the LUs needed for the Exchange database and log volumes, a few other configurations need to be made:

- **RAID groups for S-VOLs** — RAID groups for the S-VOLs must be identified and configured before ShadowImage pairs can be created in the Hitachi VSS Provider GUI. Although RAID-1+0 groups made up of high-performing SAS drives are recommended — and in some cases required — for the production LUs or P-VOLs, the RAID groups used for the S-VOLs can be deployed in other configurations, such as RAID-5 or RAID-6 and consist of lower-performing SAS or SATA drives in many environments. In addition, RAID groups do not need to maintain the same number of drives as the P-VOLs, which, when combined with the previously mentioned options, provides configuration flexibility and allows storage configurations to be tailored to meet a variety of business requirements or cost constraints.
- **Command devices** — A command device is a dedicated logical volume that is used by management software, such as Hitachi VSS Provider, to interface with the storage system. Create the command devices from a RAID-5 group as a best practice.
- **Differential management logical units (DMLUs)** — A DMLU is a volume used by ShadowImage to store information about the ShadowImage pairs. Best practice is to create two DMLUs and place them on separate RAID-5 groups.
- **Backup-to-disk LU** — An LU needs to be carved out and presented to the Backup Exec media server to serve as the backup-to-disk folder.

Table 8 lists RAID group and LU configuration details for the Exchange database and log volumes, the S-VOLs, the command devices, and the DMLUs used in the tested deployment.

**Table 8. RAID Group and LU Configuration Details**

<i>RAID Group</i>	<i>LUN</i>	<i>Size (GB)</i>	<i>RAID Level</i>	<i>RAID Type</i>	<i>Disk Spec</i>	<i>Description</i>
0	0	300	RAID-1+0	2D+2D	300GB 15K SAS	Database volume for Exchange storage group 1
1	1	100	RAID-1	1D+1D	300GB 15K SAS	Log volume for Exchange storage group 1
2	2	300	RAID-1+0	2D+2D	300GB 15K SAS	S-VOL for database volume for Exchange storage group 1
3	3	100	RAID-1	1D+1D	300GB 15K SAS	S-VOL for log volume for Exchange storage group 1
4	10	1	RAID-5	4D+1P	300GB 15K SAS	Command device
4	11	1	RAID-5	4D+1P	300GB 15K SAS	Command device
4	20	10	RAID-5	4D+1P	300GB 15K SAS	DMLU
4	21	10	RAID-5	4D+1P	300GB 15K SAS	DMLU
5	30	1000	RAID-5	4D+1P	300GB 15K SAS	Backup to disk

## Best Practices

Hitachi Data Systems' testing of the backup and restore scenarios resulted in the following best practice recommendations for the design of the Exchange environment, the deployment of the solution and configuration of Backup Exec.

### Exchange

To ensure successful backup and restore operations, several general principles apply to Exchange 2007 deployments that must be followed to ensure successful backup and restore. Examples include implementing only one Exchange database per storage group, disabling circular logging, and allowing sufficient space for maintenance and recovery procedures. For performing off-host backups using the Hitachi VSS Hardware Provider with Backup Exec, follow these best practices:

- **Backup storage groups rather than individual databases** — Backups of individual databases are not supported when using snapshot technology such as VSS, and a backup of Exchange 2007 automatically uses VSS.
- **Separate databases from transaction logs** — Keep Exchange databases and transaction logs on separate LUs that reside on separate RAID groups. This ensures that if a problem with the databases' physical disks occurs, you can recover using logs.
- **Use drive letters** — When creating the NTFS volumes in Windows for the Exchange databases and logs, use drive letters instead of mount points. The Backup Exec Exchange Agent does not support mixing snapshot backups and non-snapshot backups. If databases and logs are set up as mount points on a volume that is not prepared for snapshot, the backup job fails.

## Deployment

Follow these best practices for deploying the solution:

- **Use current version of HBA drivers** — Use the latest driver and firmware for the HBAs installed on the Exchange and Backup Exec servers. Check the HBA vendor's Web site and the Hitachi support matrix (available from the Interoperability section of the Hitachi Data Systems Web site's [Adaptable Modular Storage 2000 page](#)) for the latest compatibility information.
- **Use current version of Hitachi VSS Hardware Provider** — Install the latest version of the Hitachi VSS Hardware Provider and any patches or registry updates. Check the companion guide that comes with the Hitachi VSS Hardware Provider for the latest information.
- **Use the latest version of the Symantec Device Driver Installer** — The latest version ensures compatibility with the Hitachi VSS Hardware Provider. For this tested deployment, the latest DDI was installed with Symantec hotfix 322898.
- **Create ShadowImage Pairs with Hitachi VSS Hardware Provider** — Use the Hitachi VSS Hardware Provider GUI or CLI to create ShadowImage pairs. RAID groups for the ShadowImage S-VOLs must be created using Storage Navigator prior to the pair creation. Do not use Storage Navigator to create the pairs. The Hitachi VSS provider will not recognize them.
- **Use round robin multipathing algorithm** — If using multipathing software such as Hitachi Dynamic Link Manager or MPIO, select the round robin algorithm for the Exchange LUs.
- **Provide two unique multipathing paths** — To obtain maximum availability when using multipathing software, design and implement your host-storage connections so that at least two unique paths exist from the Exchange host to the storage system.
- **Follow Hitachi Data Systems multipathing recommendations** — Hitachi Data Systems recommends the use of dual SAN fabrics, multiple HBAs and host-based multipathing software when deploying Exchange Server.

## Backup Exec

Hitachi Data Systems recommends using an off-host backup with the GRT option to backup Exchange 2007 using the Hitachi VSS Hardware Provider and Backup Exec. Follow these best practices when setting up Backup Exec:

- **Use ADBO** — The Advanced Disk-based Option includes the off-host backup functionality that is required for this protected Exchange solution.
- **Separate source volumes and snapped volumes** — When using ADBO for off-host backups, keep source volumes and snapped volumes from sharing the same physical disks. This is also a ShadowImage requirement.
- **Use AOFO** — The Advanced Open File option must be installed on both the Exchange server and the Backup Exec media server to perform VSS snapshot backups. Backup Exec automatically performs snapshot backups for Exchange 2007, so you do not need to select any options for the AOFO when creating backup jobs.
- **Use the Backup Exec Exchange Agent with the AOFO to backup Exchange** — If you do not, databases and logs are skipped. Backup Exec cannot handle the Exchange database without the agent.
- **Use a backup-to-disk folder for GRT-enabled backups and place that backup-to-disk folder on a volume that does not have file size limitations** — An example of a volume without file size limitations is an NTFS drive. Backup Exec uses a staging location to restore GRT-enabled data from tape and for backup-to-disk folders located on volumes that have file size limitations. In the case of tape, Backup Exec restores the entire backup set to the staging area then deletes it when the restore job is complete. Using a backup-to-disk folder on a volume that does not have file size limitations eliminates this process.

## Conclusion

The white paper provides best practices for protecting environments that use the Hitachi Adaptable Modular Storage 2000 family, Hitachi VSS Hardware Provider, Exchange Server 2007 and Symantec Backup Exec. This solution leverages best-in-class Hitachi storage software and hardware that integrates seamlessly into environments that rely on Exchange Server 2007 and Backup Exec software.

Off-host backup is a solid solution for organizations that need to backup large amounts of data while meeting the demanding availability needs of their Exchange 2007 users in an efficient, user-friendly manner. It provides an easy to use, cost effective data protection solution that allows IT administrators to use disk capacity efficiently, maintain acceptable user experience levels, meet service level agreements and ensure regulatory compliance.

For more information on Hitachi products and solutions, see the Hitachi Data Systems [Web site](#), your sales representative or a channel partner.



---

**Corporate Headquarters** 750 Central Expressway, Santa Clara, California 95050-2627 USA  
Contact Information: + 1 408 970 1000 [www.hds.com](http://www.hds.com) / [info@hds.com](mailto:info@hds.com)

**Asia Pacific and Americas** 750 Central Expressway, Santa Clara, California 95050-2627 USA □  
Contact Information: + 1 408 970 1000 [www.hds.com](http://www.hds.com) / [info@hds.com](mailto:info@hds.com)

**Europe Headquarters** Sefton Park, Stoke Poges, Buckinghamshire SL2 4HD United Kingdom  
Contact Information: + 44 (0) 1753 618000 [www.hds.com](http://www.hds.com) / [info.uk@hds.com](mailto:info.uk@hds.com)

Hitachi is a registered trademark of Hitachi, Ltd. in the United States and others countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd. in the United States and other countries. All other trademarks, service marks and company names mentioned in this document are properties of their respective owners.

Notice: This document is for information purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems. This document describes some capabilities that are conditioned on a maintenance contract with Hitachi Data Systems being in effect, and that may be configuration dependent, and features that may not be currently available. Contact your local Hitachi Data Systems sales office for information on feature and product availability.

© Hitachi Data Systems Corporation 2009. All Rights Reserved.

AS-010-00 July 2009