



**Redefining Exchange Server
Data Protection with
Symantec Backup Exec™ 11d
for Windows® Servers
Agent for Microsoft®
Exchange Server**

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d *for Windows Servers*

Contents

Executive summary	5
Traditional backups are not enough	6
Database or mailbox protection or both?	6
Redefining Exchange protection and recovery	9
Granular Recovery Technology benefits	9
Continuous Protection of Exchange benefits	10
Product highlights	12
Protecting Exchange Server with Backup Exec 11d	14
Complete Exchange Server protection (required for disaster recovery)	14
New! Eliminate mailbox backup—still recover individual messages, folders, and mailboxes	15
One-pass Exchange backups with GRT	15
GRT-enabled backup of Exchange databases	17
Granular recovery with GRT	18
Continuous Protection	19
System requirements	20
Exchange data protection deployment guidelines	21
Configuring Continuous Protection backup jobs	22
Monitoring Continuous Protection jobs	26
Automated transaction log management	26
Exchange data protection best practices	27
In small office environments	27
In medium to large office environments	27

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d
for Windows Servers

Contents *(cont.)*

Restoring Exchange data from Continuous Protection backups	29
Individual mailbox, message, and folder recovery	29
Full mailbox store database recovery	31
Advantages of Backup Exec GRT over Exchange recovery storage groups	32
Summary	34

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Executive summary

Companies today are facing the ever-increasing challenge of managing the explosive growth of valuable data. As the predominant form of communication for business transactions, email is an application that is mission critical to organizations of all sizes. It generates a huge amount of information that must be immediately available and protected. The loss of a single message may generate hours of unnecessary and frustrating labor for administrators and can lower productivity or even hinder progress within organizations.

Email applications have become key communication tools for businesses of all sizes. Today, email is the most common and vital form of communication, often replacing the phone as the preferred mechanism for exchanging information in the business world. It is a more efficient and cost-effective way of disseminating information of all types (text, image, video, and even voice) to fellow employees and between companies located anywhere in the world. In fact, as companies consider their messaging servers to be mission critical, these are among the first servers to be recovered after a disaster, sometimes even before phone systems.

Various recent reports indicate that:

- 75 percent of a typical company's intellectual property is contained in email
- 79 percent of companies accept email as written confirmation of transactions
- 75 percent of Fortune 500 litigation involves discovery of email communications

While businesses need email data to be protected and available, the amount of such data is growing exponentially. IT is faced with the challenge of backing up this critical Microsoft Exchange data within the existing backup window and recovering it quickly.

The objective of traditional backups is to minimize downtime for the enterprise messaging environment while providing the quickest possible data recovery in the event of a system crash, database corruption, loss of a single mailbox, or other forms of data loss. In order to maintain the availability of Exchange and protect its mission-critical data stores, companies go to great lengths to protect their Exchange environments. Today, this protection is primarily accomplished through online backups of the Exchange databases. If organizations also need to recover individual email messages or mailboxes, separate slow, error-prone, "brick-level" mailbox backups are typically required to recover these individual items without restoring the entire Exchange database.

With its latest release, Symantec™ Backup Exec 11d *for Windows Servers* redefines traditional Exchange protection, eliminating daily Exchange backup windows with continuous data protection. And whether protecting Exchange continuously or not, Backup Exec 11d also eliminates slow, arduous mailbox backups, while still enabling the recovery of individual emails, folders, and mailboxes.

Key Benefits

- Helps safeguard critical Microsoft Exchange 2000 Server and/or Exchange Server 2003 data
- Eliminates daily backup windows for Exchange with Continuous Protection
- Eliminates mailbox backups, with or without Continuous Protection
- Recovers individual email messages, mailboxes, and public and private folders from database backups—without mailbox backups—in seconds

Traditional backups are not enough

Current administrators have two basic ways to back up Exchange Server data—at the database and at the mailbox level.

Database or mailbox protection or both?

Database backup is mandatory, as restoring a database is the only way to retrieve all of the Exchange Server data when a disaster occurs. Almost all backup applications protect Exchange databases in a similar fashion using the Microsoft provided Exchange backup application programming interfaces (APIs).

Individual “brick-level” or mailbox backups have often been considered “optional,” but they are highly advantageous when a fast recovery is needed of specific mailbox or public folder data. Protecting the Exchange Server at the mailbox or message level enables the user to restore Exchange data at a granular level (for example, a single message, calendar item, or note). Mailbox backups are usually performed to restore message data for regulatory, legal, or emergency situations, such as a corporate audit, subpoena, or deletion of critical files. Although they can be a very fast and convenient way to restore data, they incur a higher cost than database backups for the following reasons:

- **Twice the backups:** They require administrators to run two separate backups of essentially the same information. One backup is of the individual mailboxes, and the other is for the Exchange mailbox stores. This leads to the second major drawback.
- **Twice the time—or more:** Individual mailbox backups are not easy or fast. While Exchange Server provides backup vendors with high-performance APIs to protect the database, this is not the case with traditional individual mailbox backups. Backup application vendors have had to rely on an older, slower technology (Microsoft Messaging application programming interface, known as MAPI) that was not designed for backup purposes to perform individual mailbox-level backups. Individual mailbox-level MAPI-based backups typically take two to eight times longer to perform than Exchange mailbox store database backups. In many cases, these backups have a maximum transfer rate of about 80 megabytes per minute and are prone to errors such as corrupt messages, antivirus software contention, or disabled mailboxes, which results in failed backups.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

- **Twice the media/storage:** Mailbox backups duplicate information backed up with Exchange database backups. In addition, because mailbox data can contain many entries, mailbox backups result in larger catalog sizes and greater tape usage. Even if organizations do accept redundant backups of their Exchange data and the performance limitations of individual mailbox-level backups, they must also consider the additional storage cost associated with duplicate backups. This can result in purchasing and managing additional tape media if tape-based backups are performed. If they use disk-based backups, organizations need to acquire and manage sufficient disk.
- **Twice the headache:** All of these limitations lead to increased costs and management headaches for administrators to ensure that they can recover the Exchange data they want, when they need it.

If administrators want to back up Microsoft Exchange databases for complete disaster recovery purposes *and* be able to recover individual email, folders, or mailboxes, they typically have to do separate backups including:

- Full backups of the Exchange mailbox store databases for disaster recovery
- Full backups of the individual mailboxes at least once a week for individual mailbox or message recovery
- Incremental or full backups to back up the changes since the last incremental or full backup.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Figure 1 displays Exchange nightly backups that include both full and incremental backups of the Exchange database and daily full and incremental backups of the individual mailboxes for granular recovery. This traditional Exchange protection strategy requires administrators to do twice the backups of the same Exchange data, taking twice as long (or more), using twice as much storage space to hold the additional backup data—creating twice the headache to protect Exchange.

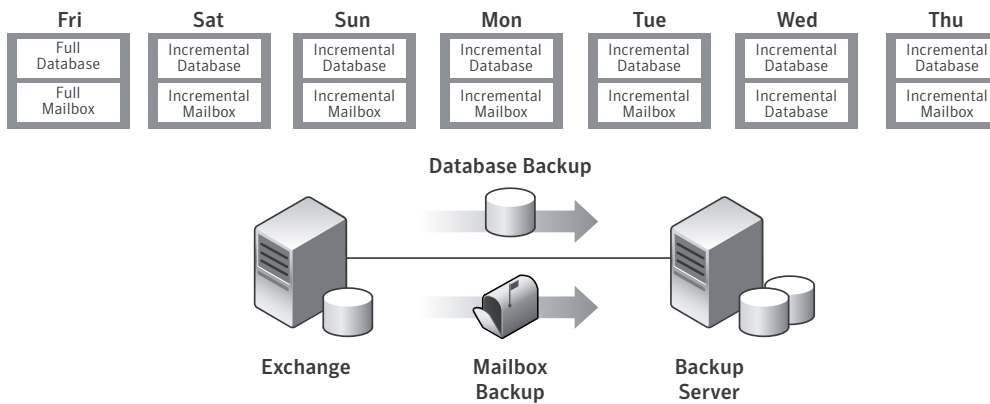


Figure 1. Traditional Exchange mailbox and database backups

If traditional Exchange protection methods are currently in place, administrators need to answer the following questions:

- How much time and space is your Exchange backup costing you?
- What if you could eliminate your daily backup windows for Exchange?
- What if you could eliminate separate, individual, “brick-level” mailbox backup operations?
- How do you recover individual emails, folders, or mailboxes today?
- Are you backing up to tape or disk?

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Redefining Exchange protection and recovery

Backup Exec has supported Exchange since its introduction by Microsoft in 1996 and Windows Server operating systems since their introduction in 1992. Backup Exec delivers established experience and proven reliability in the Exchange Server market.

With Backup Exec 11d and the Backup Exec Agent for Microsoft Exchange Server, Symantec is introducing two key new technologies for Exchange to address the problems with traditional Exchange backups:

- Granular Recovery Technology (GRT)
- Continuous Data Protection for Exchange

Together, these technologies eliminate not only separate individual mailbox backups but also daily backups, along with Exchange protection management headaches. Symantec believes these technologies provide the fastest and most flexible way to protect and recover Exchange 2000 Server and Exchange Server 2003 data.

Granular Recovery Technology benefits

The main benefits of Backup Exec's Granular Recovery Technology (GRT) include:

- Eliminate separate, slow individual mailbox backups completely
- Perform fast single-pass backups of Exchange databases and still recover individual mailboxes, individual messages, and private and public folders
- Works with or without the need for recovery storage groups (RSGs)
- Cut backup time and storage in half by performing fast, single-pass Exchange database backups
- Reduce storage/media costs
- Enable granular recovery or complete database recovery of all Exchange data

With Backup Exec 11d GRT-enabled backups, Exchange mail messages, mailboxes, and folders are restored individually without having to restore the entire Exchange database—and without mailbox backups. All that is required is a single-pass full or incremental backup of Exchange, so this feature dramatically decreases the time required to back up mailboxes while also reducing the storage requirement. You can now recover critical Exchange data in seconds, including individual emails, individual mailboxes, public folders, calendars, and contacts from a fast, single-pass Exchange database backup (see Figure 2).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

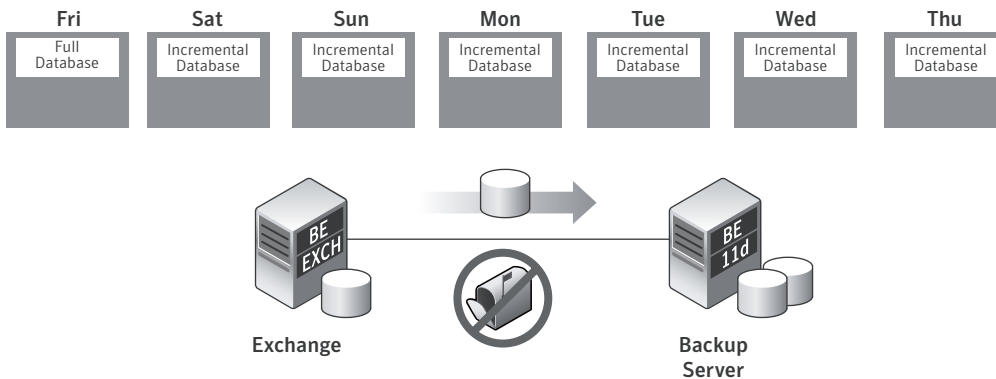


Figure 2. GRT-enabled Exchange mailbox and database combined backups

Unlike other Exchange protection solutions in the marketplace today, Symantec Backup Exec 11d Agent for Microsoft Exchange Server completely eliminates traditional separate, individual, brick-level MAPI-based mailbox backups.

Continuous Protection of Exchange benefits

The main benefits of Continuous Protection include:

- Eliminate daily backups—Exchange is protected continuously
- Recover emails, folders, and mailboxes in seconds using GRT
- Automatically truncate Exchange transaction logs for automated log growth control
- Provide complete disaster recovery of Exchange databases up to the latest transaction log

As previously mentioned, GRT-enabled backups provide administrators the best of both worlds by protecting Exchange at the storage group and mailbox store database level while also providing granular recovery of individual mailboxes, messages, and folders from a single-pass backup. Most organizations today run these traditional full or incremental backups of Exchange databases nightly using Backup Exec.

However, as Exchange has become mission critical to most organizations, the need for more frequent recoveries of Exchange data beyond daily backups has increased. It is no longer acceptable to be able to recover only Exchange mailboxes, messages, folders, and databases from the previous night's backups. The Continuous Protection of Exchange technology in Backup Exec 11d uses the same GRT-enabled technology for full database or granular recovery but extends it

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

by enabling these backups to occur more often to help ensure Exchange recoveries are always possible. Continuous Protection enables Backup Exec to create GRT-enabled “recovery points” of Exchange at intervals that you specify in the Backup Exec console.

With Continuous Protection for Exchange, you perform a full backup once a week or once a month. Exchange transaction logs are continuously protected by Backup Exec and are consolidated into easily managed recovery points automatically to help ensure your Exchange databases are protected up to the latest complete transaction log. When you enable recovery points to run at intervals between the weekly or monthly full backups, you can restore individual mailboxes, messages, and private and public folders of all Exchange Server components, including embedded objects and attributes, to a time when the recovery point was created. The Exchange database and transaction logs are completely protected and quickly recoverable in a disaster recovery situation to provide comprehensive protection for your Exchange environment (see Figure 3).

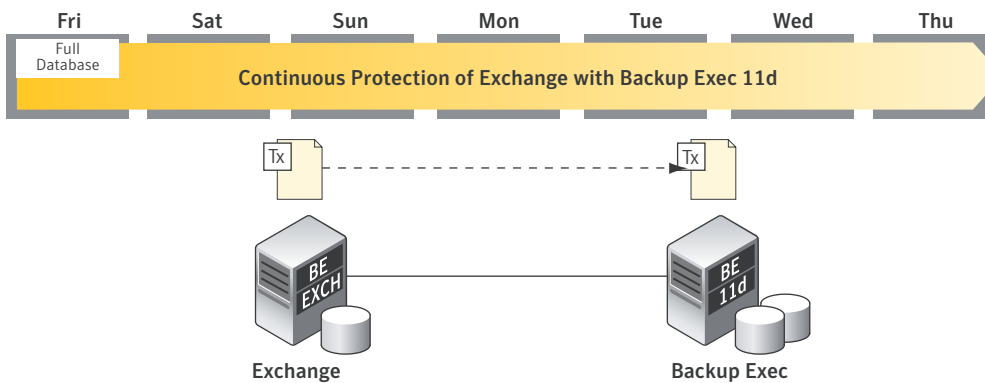


Figure 3. Continuous Protection

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Product highlights

Feature	Description	Benefit
Continuous Protection¹	<ul style="list-style-type: none"> Eliminates backup windows and enables email continuity Recovers to a specific time, even just 15 minutes ago Recovers critical individual Exchange documents such as emails, folders, or mailboxes in just seconds through the use of GRT 	<ul style="list-style-type: none"> Eliminate daily backup window for Exchange (including mailbox backup) Recover Exchange to a specific point in time Recover the Exchange data you want, when you want, where you want
Granular Recovery Technology	<ul style="list-style-type: none"> Restores individual Exchange objects including individual mailboxes, private folders, public folders, and even individual email messages, contacts, and calendars 	<ul style="list-style-type: none"> Eliminate mailbox backups forever Reduce recovery time of individual objects versus entire Exchange database Restore only the emails, mailboxes, or folders you want, when you want, for increased ability to quickly recover your most critical Exchange data
Full Disaster Recovery Support	<ul style="list-style-type: none"> Supports complete backups of all Exchange components including storage groups and mailbox databases 	<ul style="list-style-type: none"> Provide full disaster recovery support of Exchange from an easy to use point-and-click interface
Backup and Restore Performance	<ul style="list-style-type: none"> No separate jobs for database and granular recovery of individual emails, mailboxes, or folders Uses the native Exchange Server backup APIs and messaging APIs for reliable Exchange protection 	<ul style="list-style-type: none"> Cut backup times by half or more by eliminating mailbox backups Obtain the benefits of individual mailbox, folder, and message-level recovery from your normal high-performance backups of the Exchange databases GRT-enabled backups support both the Microsoft Exchange (ESE) backup and restore APIs and use of the VSS snapshot backups¹
Complete Exchange Server Protection	<ul style="list-style-type: none"> Includes an Agent for Windows systems (Remote Agent for Windows Servers along with the Continuous Protection Agent) to ensure that all of the necessary data outside of Exchange on an Exchange Server can be just as easily protected Key management service database and site replication service databases can be easily protected if deployed 	<ul style="list-style-type: none"> Includes everything you need for complete peace of mind for your Exchange Servers, including all Exchange and non-Exchange Server data protected in an integrated fashion If these services databases have been deployed, they can be easily included in the traditional Exchange Server backups²
Ease of Management	<ul style="list-style-type: none"> Provides an easy-to-use, intuitive interface designed to look similar to Outlook and Exchange for data protection Clearly displays all Exchange Server data and allows easy integration of Exchange data into the backup scheme of your entire environment 	<ul style="list-style-type: none"> Reduced training and administrative costs

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Feature	Description	Benefit
Online Recovery (No Reboots Required)	<ul style="list-style-type: none"> Recovers important Exchange information while Exchange is online 	<ul style="list-style-type: none"> No rebooting of critical Exchange Servers to restore lost or damaged Exchange objects
Redirected Restore	<ul style="list-style-type: none"> Provides redirected database, mailbox, message, and folder restore 	<ul style="list-style-type: none"> Recover your Exchange data quickly to wherever you need it
Single Point of Administration (Centralized Management)	<ul style="list-style-type: none"> Provides centralized Exchange backup and recovery operations Enables use of a single console for managing backups for the entire Exchange environment Integrates Exchange protection and individual object recovery with your overall backup strategy, including Microsoft Exchange, SharePoint, and SQL 	<ul style="list-style-type: none"> All restore operations can be performed from one central location without requiring the administrator to go to the domain controller A single point of administration and control for local and remote backups of Exchange Servers Schedule and manage all of your Exchange and non-Exchange backups from a single product instead of several different utilities
Media Independence	<ul style="list-style-type: none"> Supports backups to disk or tape³ Supports automatic disk-to-disk-to-tape (D2D2T) staging³ 	<ul style="list-style-type: none"> Almost any backup device can be used for protecting Exchange data Exchange backups can be staged to disk initially for quick recovery and then to tape for offsite disaster recovery protection
Built-In Encryption	<ul style="list-style-type: none"> Secures your company's sensitive Exchange data with industrial-strength 128-/256-bit AES encryption included in the Backup Exec 11d core license at no additional charge 	<ul style="list-style-type: none"> Ensure Exchange backup information is stored securely both onsite and offsite⁴
Single Instance Storage (SIS) Support	<ul style="list-style-type: none"> Maintains Exchange's native single-instance storage of attachments during database backups 	<ul style="list-style-type: none"> Eliminate the backup of redundant copies of files sent to large numbers of users Reduce the time and media required to protect the Exchange environment
Cluster Support²	<ul style="list-style-type: none"> Supports cluster failover in a Microsoft Cluster Server or Veritas™ Cluster Server environment, providing improved fault tolerance 	<ul style="list-style-type: none"> Provide seamless protection for Exchange Servers installed in high-availability environments
SAN SSO Support	<ul style="list-style-type: none"> Provides LAN-free Exchange Server backup—supports storage area networks (SANs) with the SAN Shared Storage Option 	<ul style="list-style-type: none"> Increase backup and recovery performance over a Fibre Channel or iSCSI network to a shared storage device
Recovery Storage Group (RSG) Support	<ul style="list-style-type: none"> Works with or without recovery storage groups to enable granular recovery of individual Exchange databases, mailboxes, messages, and private and public folders 	<ul style="list-style-type: none"> Allow flexible recovery methods for Exchange data

¹ The Continuous Protection feature does not support the Microsoft Volume Shadow Copy Service (VSS) snapshot provider.

² Snapshot backups (leveraging VSS) do not support site replication service databases, individual Exchange databases, mailbox backup, or network attached storage (NAS) devices. Site replication databases are dynamically re-created when full Exchange databases are restored.

³ If you restore individual items from a GRT-enabled backup to a tape device, then Backup Exec must temporarily stage the entire database to a path on the Backup Exec server to extract individual items.

⁴ Backups enabled for encryption and sent to a disk-based backup target with the new Backup Exec 11d Granular Recovery Technology are not stored in an encrypted format. GRT allows individual object-level recovery for Microsoft Exchange, SharePoint, and Active Directory objects. GRT-enabled backups targeted to backup-to-disk (B2D) devices are encrypted at the source server during the network transit but are stored in an unencrypted format on the final backup-to-disk target location. These backups can be reencrypted when moved to tape, if desired. Tape-based GRT-enabled backups are stored on tape in an encrypted format and do not have this limitation. Exchange backups using Continuous Protection cannot be encrypted to disk, but once on disk, protected data can be encrypted when moved off to tape.

Protecting Exchange Server with Backup Exec 11d

With most database applications like Exchange Server, data protection and recovery can be divided into three main objectives:

- **Complete Exchange Server protection (required for disaster recovery):** Complete disaster recovery where both system and data (Windows operating system, Exchange Server application, and its database) are destroyed
- **Database protection (required for disaster recovery):** Provide quick recovery in case of loss or corruption of an entire mailbox store(s) or storage group that requires restoration of the entire mailbox store or storage group
- **Mailbox protection:** Provide quick recovery in case of loss of individual Exchange data such as individual emails, mailboxes, and private folders, including contacts, calendars, tasks, and public folders

Data protection for Microsoft Exchange traditionally is divided into three major categories, which support the objectives outlined above. Backup Exec 11d GRT and Continuous Protection technologies now allow administrators to concern themselves only with Exchange Server and database protection.

Complete Exchange Server protection (required for disaster recovery)

Since Exchange Server runs on Windows 2000 or Windows 2003, protecting the underlying Windows operating system and Exchange Server's files and settings are very important for a timely disaster recovery. This includes backing up all files on the volumes where Windows and Exchange are installed and backing up the Windows system state, which contains critical Exchange Server configuration information.

The backup schedules for this data should coincide with the backups of Exchange Server data (outlined below), creating a consistent set of data for an easier disaster recovery. The Symantec Backup Exec Agent for Microsoft Exchange Server includes a Backup Exec Agent for Windows Systems to ensure that all of the necessary data outside of Exchange on an Exchange Server can be just as easily protected.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Backup Exec easily protects Windows files, Windows system state, Exchange Server files, and GRT-enabled Exchange storage group/mailbox store database backups within a single schedulable job. Or you can break up these tasks into multiple jobs as your environment, performance needs, schedule, or data retention periods demand. When you select System State on a Windows 2000 Server or Shadow Copy Components (which include system state) on a Windows Server 2003 within the Windows Server's backup selections, Backup Exec backs up all critical Windows operating system data, including Exchange, cluster DB, registry, boot, and system files. If disaster strikes your Exchange Server, the Backup Exec Intelligent Disaster Recovery (IDR) Option or Backup Exec System Recovery product can help you quickly restore the Windows system in preparation for performing a disaster recovery of Exchange.

The Exchange recovery points described previously run at the specified intervals after the recurring full backup has started. Recovery points do not run if the full backup is active. The recovery points start running again at the specified interval when the full backup is completed. Replication of the transaction logs is continuous, even when the full backup is active.

New! Eliminate mailbox backup—still recover individual messages, folders, and mailboxes

With Backup Exec 11d GRT-enabled backups, Exchange mailboxes, messages, and folders are always backed up with the Exchange mailbox store databases. You no longer have to back up Exchange mailboxes separately from the databases to restore an individual mailbox, email message, public folder, private folder, contact, or calendar. If you select to enable the restore of individual items, you can restore individual mail messages and folders from the Exchange mailbox store database backups without having to restore the entire database. When you select to enable the restore of individual items, then Backup Exec collects additional information for the catalog. This information enables you to restore single mail messages or folders from information store backups.

One-pass Exchange backups with GRT

Backups are performed by simply selecting the “big items” such as Exchange storage group(s) or mailbox store(s) to back up. Since all user data is contained in the Exchange Server databases, protecting that data is the main objective. Exchange Server provides several methods to back up and restore data, but consider the pros and cons of each to achieve your data protection goals.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

You can simply browse to the Exchange 2000 Server or Exchange Server 2003 you want to protect and select which mailbox stores or storage groups to protect. Symantec recommends that you select individual storage groups for backup rather than individual databases in storage groups. Although you can select individual databases in a storage group for backup, the transaction logs for the entire storage group are backed up for each database selected.

For example, if you select four databases in a storage group for backup, the entire collection of transaction logs for the storage group is also backed up four times. The transaction logs are not deleted until a full backup is run on every database in the storage group. You can still restore an individual database from a storage group backup. Again, unlike other backup solutions there is no need to select individual mailboxes for protection (see Figure 4).

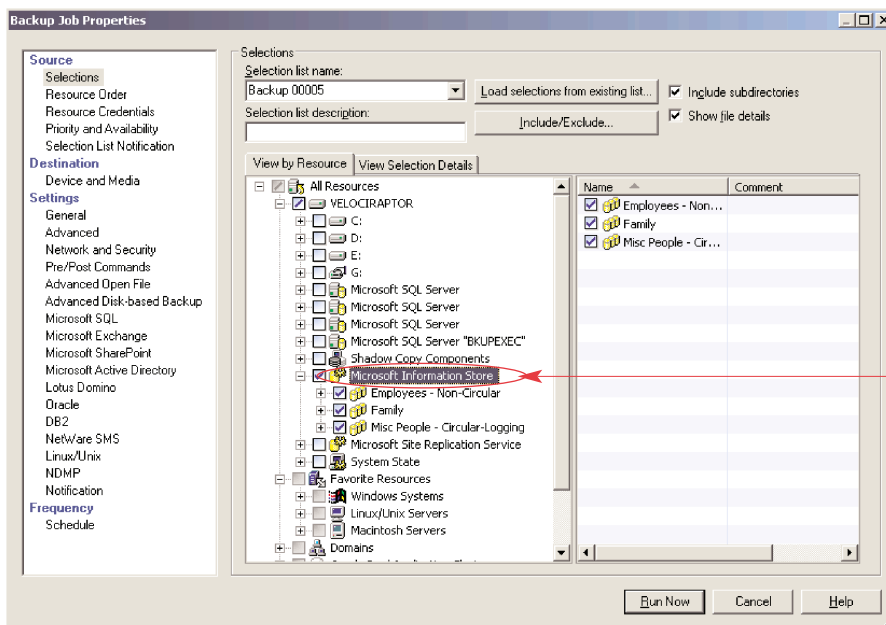


Figure 4. Selecting Exchange data for GRT-enabled backup

Enabling GRT technology for single-pass backups of Exchange in Backup Exec is as simple as selecting a checkbox (see Figure 5).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

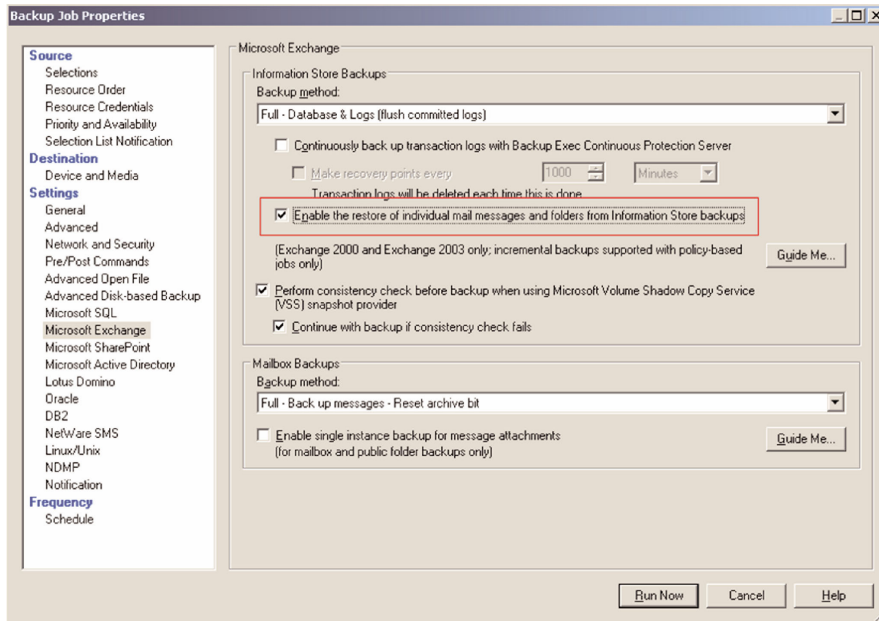


Figure 5. Enabling restore of individual mail messages and folders

GRT-enabled backup of Exchange databases

As Exchange is now often viewed as mission critical, it is important that it always be available. To meet this need, the Backup Exec Exchange Agent offers a method of performing an online or hot backup of Exchange databases. This allows several backup methods for use with GRT technology including:

- **Full backup:** Backs up the selected database and the associated transaction logs and then deletes the logs after backup. Full backups are the foundation backup type on which complex and scalable backup schemes can be based. If given a choice of only one method of backup, choose full.
- **Incremental backup:** Backs up the transaction logs for the associated database and deletes them after backup. The advantage of the incremental method is that it backs up the least amount of data and therefore has the least impact on the Exchange Server. Another advantage is that it helps conserve log file space. The disadvantage is that all incremental backups must

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

be restored consecutively after restoring a full backup. For example, if full backups are performed Sunday and incremental backups during weekdays, then five (one full plus four incremental) sets of data would be needed to recover from a disaster on Friday.

- Exchange Server 2003 VSS writer support can be leveraged to take snapshot-based backups for the GRT-enabled full backup but cannot be used with Continuous Protection of Exchange backups.
- VSS-based incremental backup types require Exchange Server 2003 SP1.
- GRT-enabled backups can be done to tape or disk; however, it is recommended that they be done to disk. GRT-enabled backups to tape require a two-step staging process for individual mailbox, message, and folder restores.
- GRT-enabled backups require the use a Backup Exec policy to control both the full and incremental backup schedules.
- Incremental GRT-enabled backups must be done to disk only.

The benefits of GRT-enabled backups include:

- Back up big items but restore small items
- Single checkbox—set and forget
- Easy Restore view In Backup Exec

Granular recovery with GRT

Prior to Backup Exec 11d, organizations backed up individual Exchange mailboxes separately from the information store so they could restore individual mailboxes. This resulted in additional time and media-consuming backups. With Backup Exec 11d, you can enable the option to restore individual mail messages and folders from information store backups. If you checked “Enable the restore of individual mail messages and folders from Information Store backups” on the backup job properties for the information store backups, then you can restore individual messages and folders from that backup (see Figure 6).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

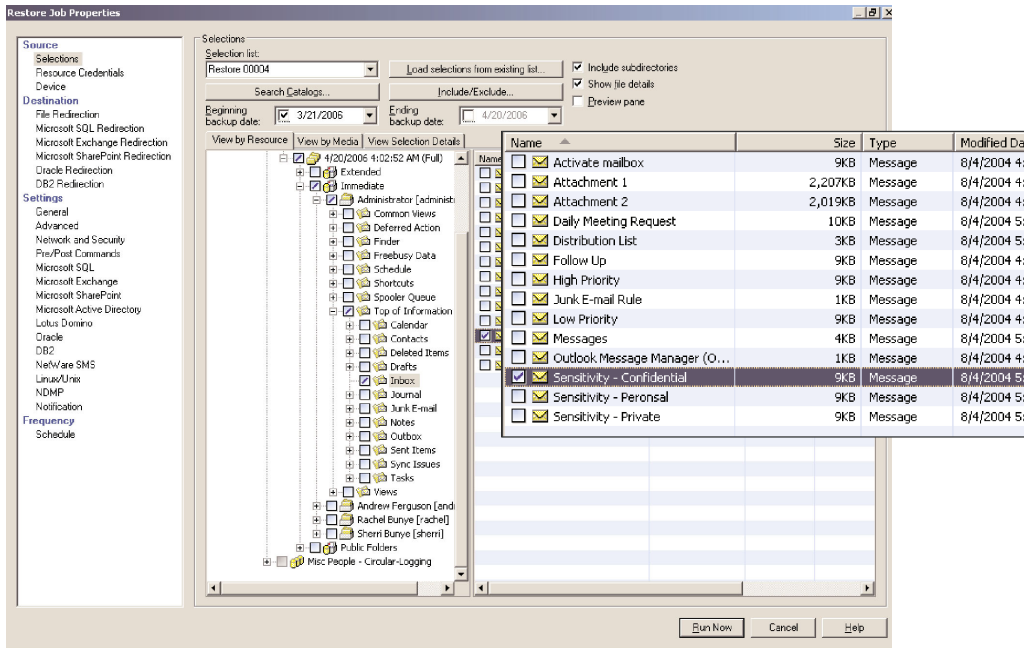


Figure 6. GRT-based restores
Restores are just like browsing Microsoft Outlook

Continuous Protection

The Symantec Backup Exec Continuous Protection Server (CPS) combines data protection with continuous protection (or replication) technology and disk-based data protection. When CPS components are installed on the Backup Exec 11d media server and the Backup Exec 11d Agents on the Exchange Server, you can enable GRT technology and continuously protect Exchange data.

To deploy Backup Exec 11d for use with Continuous Protection of Exchange please note the following (see Figure 7):

- The CPS components must be installed on the Backup Exec 11d media server.
- The Backup Exec 11d Agent for Microsoft Exchange Server license must be installed on the Backup Exec 11d media server. The Backup Exec 11d Agent for Microsoft Exchange Server license includes a license for the Backup Exec 11d Agent for Windows Systems (Remote Agent for Windows Servers along with Continuous Protection Agent). This license key is entered into the Backup Exec media server during installation or through Tools/Serial Numbers in the Backup Exec console after installation.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

- The Backup Exec 11d Agent for Windows Systems, which consists of the Backup Exec 11d Remote Agent for Windows Servers (RAWS Agent) and Backup Exec 11d Continuous Protection Agent (CPA), must be installed on the Exchange 2000 Server or Exchange Server 2003. Both of these agents can be installed together from the Continuous Protection Server CD.

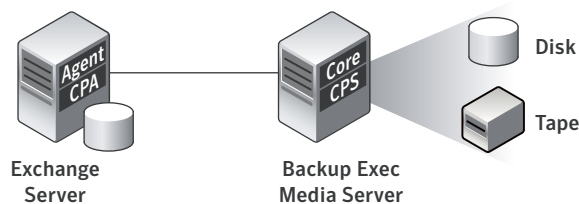


Figure 7. Deploying Backup Exec 11d Continuous Protection of Exchange components

Please note that the requirement of having the CPS components installed on the Backup Exec 11d media server only applies for Exchange Continuous Protection. For normal file server protection with the Backup Exec 11d Agent for Windows Systems, the CPS can be installed on a separate server from Backup Exec 11d.

Also, in order to support the use of GRT-enabled backups or Continuous Protection of Exchange, Backup Exec 11d cannot be installed on an x64 Windows 2003 Server. It must be installed on a 32-bit version of Windows to perform GRT-enabled or continuous backups of Exchange 2000 Server or Exchange Server 2003 data. Please see the “System requirements” section of this document for specific operating system, Exchange, Backup Exec, and service pack version requirements.

System requirements

To support the restore of GRT individual mail messages and folders from information store backups, the Backup Exec server must be installed on a Windows operating system that supports mini-filter drivers including:

- Microsoft Windows 2000 Server (with Service Pack 4 and Update Rollup 1 for Service Pack 4)
- Microsoft Windows Server 2003 (with at least Service Pack 1)
- Microsoft Windows Server 2003 R2 Editions

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

To support Backup Exec Continuous Protection of Exchange, the following requirements must be met:

- CPS must be installed on the Backup Exec 11d media server.
- Exchange must be installed on a system remote to the Backup Exec 11 media server. They cannot be installed on the same system.
- Both the Backup Exec 11d Remote Agent for Windows Servers and the CPA must be installed on the Exchange 2000 Server or Exchange Server 2003.
- Both CPS agents must use the Backup Exec service account. The service account must have domain and local administrator rights.

Important note: In order to support the use of GRT-enabled backups or Continuous Protection of Exchange, Backup Exec 11d cannot be installed on an x64 Windows Server 2003. Backup Exec 11d must be installed on a 32-bit version of Windows to perform GRT-enabled or continuous backups of Exchange 2000 Server or Exchange Server 2003 data.

Exchange data protection deployment guidelines

- Avoid making the Exchange Server a domain controller. For disaster recovery purposes, it is much easier to restore Exchange if you don't have to first restore the Exchange Server or primary domain controller.
- Do not install Exchange into a domain that does not have at least two domain controllers. Database replication is not possible with only one domain controller in a domain. If the domain controller fails and corrupts the Exchange Server, some transactions may not be recoverable if they were not included with the last backup. With at least two domain controllers in a domain, databases on the failed domain controller can be updated using replication to fill in missing transactions after the database backups have been restored.
- Disable Write Cache on the SCSI controller. Windows does not use buffers, so when Exchange (or other applications) receives a write complete notice from Windows, the write to disk has been completed. If Write Cache is enabled, Windows responds as though a write to disk has been completed, and it will provide this information to Exchange (or other applications) incorrectly. The result could be data corruption if there is a system crash before the operation is written to disk.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

- Locate transaction log files on a separate physical disk from the database. This is the single most important configuration affecting the performance of Exchange. This configuration also has recovery implications, since transaction logs provide an additional recovery resource.
- Continuous Protection of Exchange does not support the delegation of Exchange Continuous Protection jobs to Backup Exec Central Admin Server Option (CASO) managed media servers. Continuous Protection of Exchange jobs must be created and managed on the Backup Exec media servers.
- Disable circular logging. Circular logging minimizes the risk that the hard disk will be filled with transaction log files. But, if a solid backup strategy is in place, transaction log files are purged during the backup, thus freeing disk space. If circular logging is enabled, transaction log histories are overwritten, incremental and differential backups of storage groups and databases are disabled, and recovery is only possible up to the point of the last full or copy backup.

Configuring Continuous Protection backup jobs

As described previously, GRT-enabled backups can be enabled as part of normal Exchange full or incremental backups by selecting a checkbox. Continuous Protection of Exchange uses the same GRT and principles.

All interaction between Backup Exec and the Continuous Protection technology occurs on the Backup Exec 11d server. The Exchange Continuous Protection job is created, deleted, stopped, and started by Backup Exec. The Exchange transaction logs available on the Backup Exec server can be used for a complete restore of the Exchange databases or for GRT-enabled granular restore of individual mailboxes, messages, and folders.

Exchange storage groups are initially selected for backup the same way as they are in a traditional Exchange backup. Symantec recommends that you select individual storage groups for backup rather than individual databases in storage groups. Although you can select individual databases in a storage group for backup, the transaction logs for the entire storage group are backed up for each database selected (see Figure 8).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

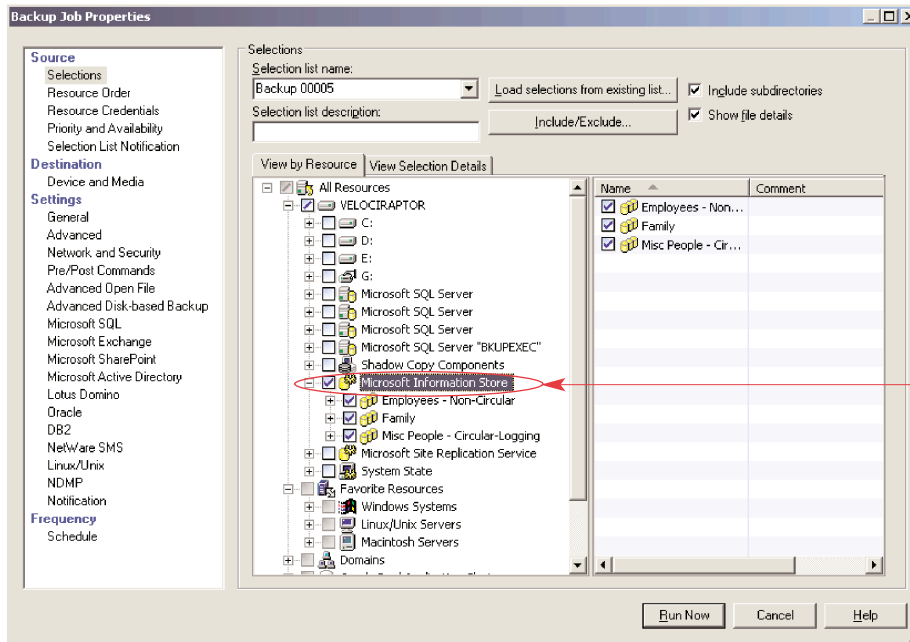


Figure 8. Selecting Exchange database for continuous backup

Continuous Protection produces the same GRT-enabled backups that you can use to recover from, just more frequently. These frequent GRT-enabled backups are known as recovery points. Recovery points can only be created as part of the Continuous Protection strategy. If you choose not to use recovery points, individual mail messages and folders can only be recovered from the last full backup.

As part of the Continuous Protection of Exchange, you can enable Backup Exec to make recovery points at intervals that you specify. Recovery points create backup sets that you can browse from the Restore view. You can recover individual messages or folders from a point in time when either a full backup or recovery point was run (see Figure 9).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

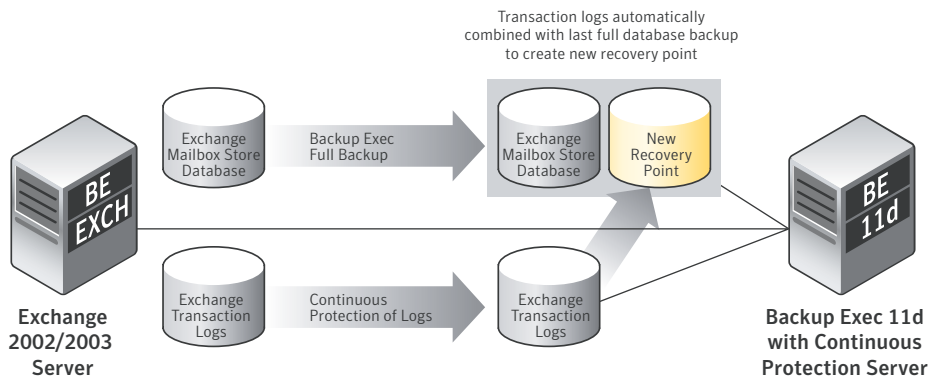


Figure 9. Recovery point creation

To configure continuous backups of Exchange, administrators only need to select a single checkbox and choose their recovery point creation interval from within the Backup Exec Job Properties screen (see Figure 10).

Note: If this option is selected, also select a backup-to-disk folder on a local NTFS volume as the destination device.

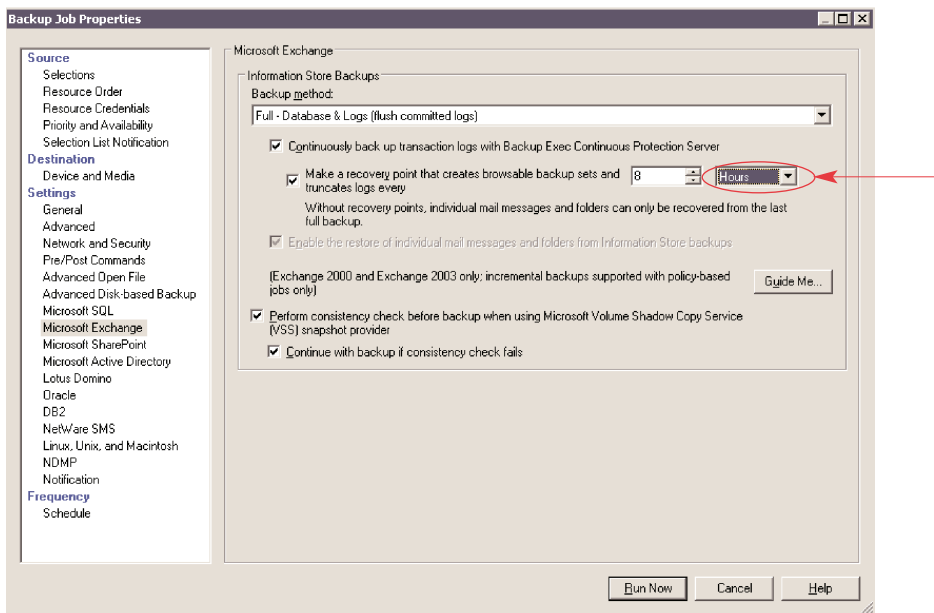


Figure 10. Configuring continuous backups

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Recovery points start to run at the specified intervals after the recurring full backup has started. If you enabled recovery points to run at intervals between the full backups, you can restore individual messages or folders at a point in time when the recovery point was created.

Recovery points do not run if the full backup is active. The recovery points start running again at the specified interval when the full backup has been completed. Replication of the transaction logs is continuous, even when the full backup is active.

If you change the specified interval for the recovery points, the new interval applies after the next full backup or recovery point runs. The recovery point only affects Exchange resources in the backup selection list. Resources that are not related to Exchange but are in the same backup selection list are not affected by recovery points.

If recovery points are set to occur *less frequently* than the default rate of every eight hours, transaction logs are also deleted less frequently and therefore use more disk space.

If recovery points are set to occur *more frequently* than the default rate of every eight hours, some additional ramifications must be considered:

- The Job Monitor view and the restore selections list may become crowded and difficult to read.
- The performance of the Exchange Server may be slower than when the recovery points are set to occur at the default rate.

Each time a recovery point is made, it also truncates the transaction logs so that log growth is controlled. This is discussed further in the following section.

These recovery points are also designed to be “virtualized” and space saving to help ensure you are not creating new complete backups of Exchange that require additional disk space each time a new recovery point is created. The actual disk space consumed by an individual recovery point is only the size of the transaction logs that have been continuously protected combined with the associated last full backup.

Monitoring Continuous Protection jobs

All backup operations that are related to the Continuous Protection of the Exchange Server are handled as a single job from within the Backup Exec console. This job is displayed in the Current Jobs view on the Backup Exec Job Monitor screen. The status of the job changes according to the operation that is running, as indicated in the following table.

Continuous Protection Operation	Status in Backup Exec Job Monitor
When the recurring full backup for the information store is running	Active: CPS backup job running
When transaction logs are being replicated	Scheduled: CPS backup job running Note: To view the Continuous Protection job for transaction log replication, or to view related errors, go to the Continuous Protection Administration Console. If the Continuous Protection Server Administration Console component is installed on the media server, you can view the CPS console.
When an Exchange recovery point is being created	Running Note: The job name is displayed with the Exchange recovery point appended to it.
When the recovery point is complete	Completed Note: When the recovery point is complete, on the Job Monitor in the Job History view, the recovery point is displayed with Exchange recovery point appended to the name of the full job.

Automated transaction log management

Exchange uses shared transaction logs for each database within a storage group, allowing the protection of Exchange in a highly granular manner via Continuous Protection of the logs of the individual mailbox store databases. Exchange Server can generate large numbers of transaction logs very quickly if the Exchange Server is busy. To control log growth, frequent incremental or full backups are required since Exchange Server deletes or truncates the committed log files after these types of backups. To help manage log file growth on the Exchange Server, each time a recovery point is made, Backup Exec truncates the transaction logs on the Exchange Server so that log growth is controlled automatically (see Figure 11).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

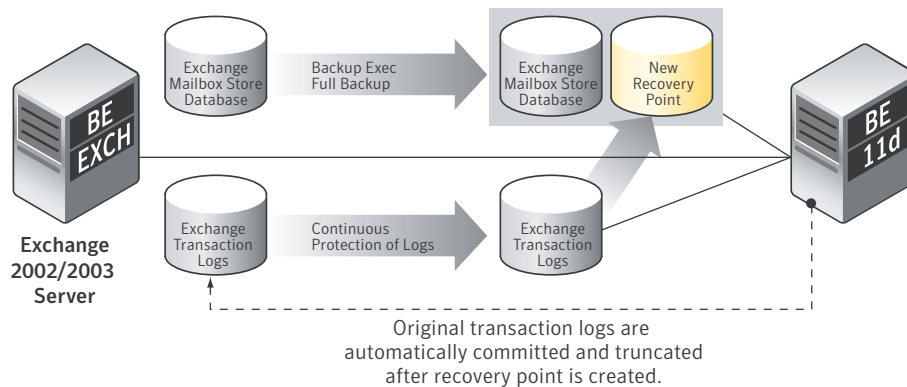


Figure 11. Log file truncation after recovery point creation

Keep in mind that Backup Exec automatically handles the truncation of the Exchange transaction log files. This affects other Backup Exec jobs for the Exchange Server, if you are running them outside of the Continuous Protection jobs, or other backups that are created by third-party applications outside of Backup Exec.

Exchange data protection best practices

The Exchange Server backup scheme that will work best for each organization is based on the size of the environment, the number of transactions processed each day, and the service level agreement with users when a recovery is required. To decide which backup methods to use, consider the following.

In small office environments

With relatively small numbers of messages passing through the system, a daily full backup at night will provide sufficient data protection and the quickest recovery.

If log file growth becomes an issue, use incremental backups at midday to provide an added recovery point and manage the log file growth automatically.

In medium to large office environments

Many organizations run full backups on the weekend and incremental backups during the week or intraday. If you have sufficient disk space for a week's worth of log files, then consider implementing differential backups during the week. Mix the backup types interday or interweek, but keep the scheme as simple as possible to make disaster recovery manageable.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

- To restore a consistent snapshot of backup data during disaster recovery, a good strategy is to coordinate the full backups of the Windows operating system files, Exchange Server application files, and the Windows system state with the full backups of the Exchange Server database. Follow this strategy for differential or incremental backups of files and database backups too. If this cannot be accomplished, at least back up the Windows system state with each Exchange database backup since this will not add much time to your backup and will provide a higher degree of protection for a disaster recovery.
- For Exchange Servers running Exchange (AD), following the guidelines stated previously to back up the Exchange host server would automatically back up the AD database with the system state backup. If the Exchange Server is not running AD, then select to back up the system state on a server running AD. Attempt to schedule the AD backups as close to the backups of Exchange Server data as possible to create a consistent data set around the most recent server and operating system settings.

Important note: Backup Exec 11d also introduces a specific Backup Exec for Microsoft Active Directory. Just like the Agent for Exchange, the Backup Exec Agent for Active Directory also includes the Granular Recovery Technology, enabling object level recovery of Active Directory from a single-pass backup. For more information, please see the white paper on the new Backup Exec 11d Agent for Active Directory.

- Intermix traditional Exchange Agent backups (differential, incremental, or copy backups) with Exchange Writer backups in an Exchange Server 2003 protection scheme on Windows Server 2003 is neither recommended nor supported.
- If the services databases have been deployed, then include them (each is normally very small) into the traditional Exchange Server backups. Both will be protected using the same backup method that you selected for the Exchange database.
- Back up Exchange data to disk if possible. If Exchange data such as mailboxes, folders, and even individual messages are the main restore cases for your environment, consider backing up Exchange data to disk through GRT-enabled backups. This allows for very quick restores of individual Exchange items without staging the entire Exchange database backup to disk first to do the restore.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Note: The following items when using Continuous Protection as part of your backup strategy:

- Symantec recommends that you back up only one Exchange Server for each continuous backup job. Create a separate selection list for each Exchange Server resource.
- If you must copy backup sets to tape for offsite storage or vaulting, create a job to duplicate backup sets. You can configure the job to copy the backup sets to tape after each occurrence of the full backup job.
- If the job template is in a policy, create a duplicate backup sets template to copy the backup sets after the last incremental backup before the full backup to tape.
- If necessary, consider creating a copy job to run before the full backup to copy all of the transaction logs as well as the full backup sets to tape.
- Consider creating a custom filter to limit the display of recovery points in the Job History view.

Restoring Exchange data from Continuous Protection backups

Just as with traditional GRT-enabled backups, Continuous Protection backups offer several different recovery types.

- Individual mailbox, message, and folder recovery
- Full mailbox store database recovery

Individual mailbox, message, and folder recovery

Recovery points create virtual backup sets that represent points in time of your Exchange database. Simply browse through them to select data to restore from the Restore view of Backup Exec just like any other GRT-enabled backup of Exchange (see Figure 12).

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

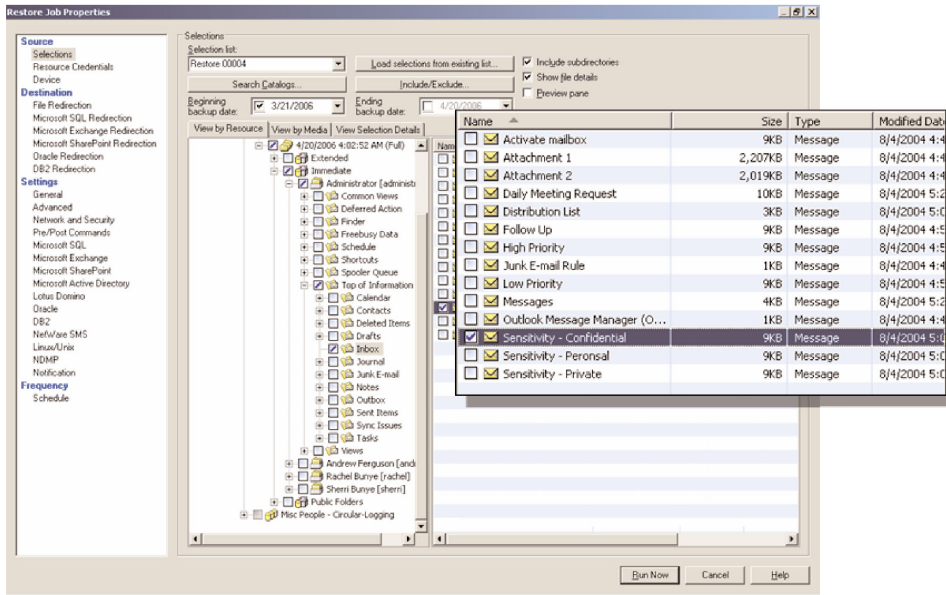


Figure 12. Browsing recovery points to restore
Restores are just like browsing Microsoft Outlook

You can recover individual messages or folders from a point in time when either a full backup or recovery point was run. Even without recovery points, you can restore individual messages or folders from any full backup.

If you restore individual items from a GRT-enabled backup on tape device, then Backup Exec must temporarily stage the entire database to a path on the Backup Exec server to extract individual items. Because of the potentially large Exchange database file sizes that are created in the staging location path, system volumes should not be used as a staging location.

To enter the path, on the Restore Job Properties pane, under Settings, click Advanced, and then enter a path in “Path on media server for staging temporary restore data when restoring individual items from tape.” For more information about this path, see “Advanced options for restore jobs” in the *Backup Exec 11d Administrators Guide*.

Full mailbox store database recovery

Backup Exec 11d's Continuous Protection technology is designed to take advantage of GRT technology to enable individual mailbox, message, and folder-level recovery when needed. However, in disaster recovery situations where an entire Exchange mailbox store database(s) is damaged or corrupted, a complete recovery is only a couple of clicks away with Backup Exec. Exchange transaction logs are files containing a running log of changes to the Exchange mailbox store database. Backup Exec 11d's Continuous Protection automatically combines full database backups and the continuously replicated Exchange transaction logs to provide a complete restore to any point in time of the Exchange mailbox store databases, including up to the latest complete transaction log.

To recover a database from error or corruption, Backup Exec can direct Exchange to "replay" these logs back into the database. Backup Exec 11d provides complete control during recovery of Exchange over how the transaction logs should be used during recovery with three different methods (see Figure 13).

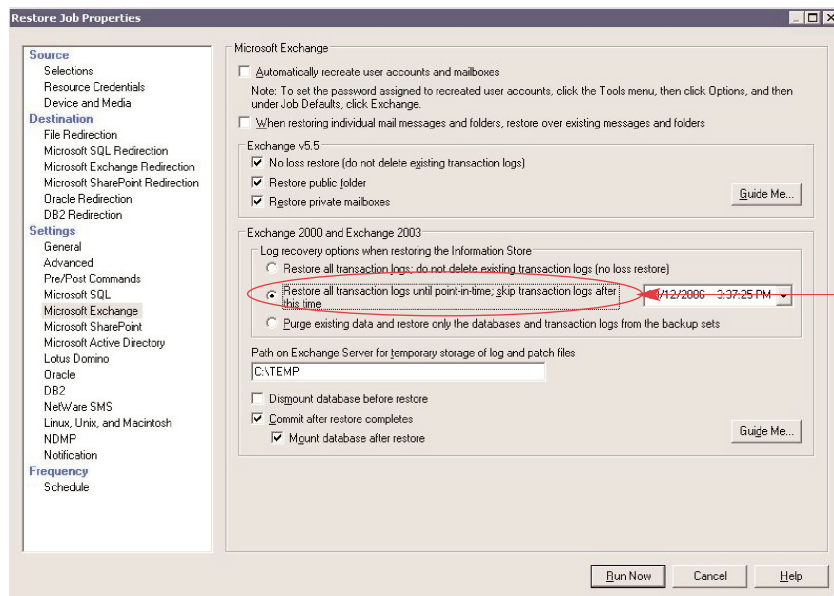


Figure 13. Log recovery options

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

To restore an entire Exchange mailbox store database to the time of a full backup or recovery point:

1. Select backup sets from the full backup or the recovery point that contains the point in time that you want to restore to.
2. On the Microsoft Exchange Restore Job Properties dialog box, select “Purge existing data and restore only the databases and transaction logs from the backup sets.”

To restore up to the latest full transaction log:

1. Select backup sets from the last full backup or recovery point.
2. On the Microsoft Exchange Restore Job Properties dialog box, select “Restore all transaction logs; do not delete existing transaction logs (no loss restore).”

To restore to a point in time between full backups or recovery points:

1. Select backup sets from any full backup or recovery point and specify the point in time.
2. On the Microsoft Exchange Restore Job Properties dialog box, select “Restore all transaction logs until point-in-time; skip transaction logs after this time.”
3. Specify the point in time.

Note: After a restore of a storage group or mailbox store that is being protected by a CPS job has been completed, you must rerun the CPS backup job to restart the replication and recovery points.

Advantages of Backup Exec GRT over Exchange recovery storage groups

The recovery storage group (RSG) feature in Exchange Server 2003 allows you to mount a second copy of an Exchange mailbox store on any Exchange Server in the same Exchange Administrative Group as the original while the original store is still running and serving clients. This allows you to recover data from an older backup copy of the store without disturbing client access to current data.

Backup Exec 11d’s new GRT technology provides all of the advantages of RSGs but overcomes several of the major limitations associated with traditional RSG-based recoveries. Backup Exec 11d still supports the use of RSGs, if desired, but the use of RSGs for mailbox recovery is no longer required. The following chart illustrates some of the key advantages of GRT over traditional RSG recoveries.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d for Windows Servers

Considerations	Backup Exec 11d with GRT	RSG
Ease of Restore Process	Single-step process	Multistep process
Integrated Solution	Yes All needed components are included and integrated with Backup Exec 11d Agent for Microsoft Exchange Server.	No Requires use of separate utility (EXMerge) in Exchange Server 2003 to extract mailbox data from the stores into .PST files and optionally to merge the extracted data back into the online stores.*
One-Pass Fast Individual Object Recovery	Yes GRT allows for direct individual, mailbox, message, and private and public folder restore without restoring entire Exchange database first.**	No Entire Exchange database must be recovered first to RSG to recover an individual mailbox.
VSS Snapshot Support	Yes GRT supports database, individual mailbox, message, and folder recovery from VSS snapshot backups.	No Data cannot be restored from VSS snapshot backups.
Public Folder Restore	Yes Public folders can be restored directly by Backup Exec 11d GRT-enabled backups to original or redirected locations.	No Public folder stores are not supported for restore using the RSG.
Individual Message Restore	Yes	No Not supported.
Multi-Mailbox Restore	Yes Multiple mailboxes can be recovered at a time.	No Mailboxes can only be recovered one at a time from the RSG.
Multi-Database Restore	Yes Multiple databases can be recovered from different storage groups.	No If multiple stores are selected for restore, mailbox stores in the RSG must come from the same storage group. You cannot add mailbox stores from different storage groups to the RSG at the same time.
Entire Exchange Server Restore	Yes Entire Exchange Server can be recovered from Backup Exec 11d backups.	No Not supported.

*Exchange 2003 SP1 adds a Recover Mailbox Data feature to Exchange System Manager.

**If you restore individual items from a GRT-enabled backup to a tape device, then Backup Exec must temporarily stage the entire database to a path on the Backup Exec server to extract individual items.

Redefining Exchange Server Data Protection with Symantec Backup Exec 11d *for Windows Servers*

Summary

Microsoft Exchange Server has quickly risen to mission-critical status in many companies; therefore, keeping it highly available and protecting its data is not an option, but a business requirement. Like many enterprise database solutions, there are several methods of backing up the Exchange Server data, which can make administration of the backup process complex, time consuming, and challenging. Backup Exec 11d alleviates the complexities of protecting Exchange and eliminates the traditional tradeoffs of database versus individual mailbox backups with its revolutionary Granular Recovery Technology (GRT). In addition to GRT, the Continuous Protection of Exchange features of Backup Exec 11d allow for more opportunities to recover your critical Exchange data, including mailboxes, folders, messages, or the entire database, while eliminating the traditional daily Exchange backup window. Continuous Protection eliminates any daily Exchange backups and helps ensure you can recover the Exchange data you want, when you want it. Together, GRT and Continuous Protection offer your environment the Exchange protection and recovery technologies your organization needs to succeed with Microsoft Exchange.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, BindView, Enterprise Security Manager, Sygate, Veritas, Enterprise Vault, NetBackup and LiveState are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
11/06 10753255