WHITE PAPER: WINDOWS PROTECTION

Confidence in a connected world.

Efficient Data Protection for Microsoft Applications with Symantec Backup Exec™

White Paper: Windows Protection

Efficient Data Protection for Microsoft Applications with Symantec Backup Exec™

Contents

Introduction to protecting Microsoft® applications

Companies today face the ever-increasing challenge of managing the explosive growth of valuable data. Symantec Backup Exec™ 12 for Windows Servers is the gold standard in Windows® data protection, providing cost-effective, high-performance, disk-to-disk-to-tape backup and recovery. Continuous data protection for Microsoft applications, including Exchange, SQL, Active Directory, and SharePoint, helps ensure that data is continuously backed up as it changes.

Protecting these Microsoft applications within your allotted backup window—and recovering them quickly and reliably—presents a formidable challenge. Symantec Backup Exec 12 simplifies and streamlines the process with centralized administration, continuous protection, patent pending granular recovery, and more.

What's new in Symantec Backup Exec 12

- Improved media management of Granular Recovery Technology (GRT) enabled backups to align with current media management policies, procedures, and data retention guidelines
- Support for off-host backups of Exchange with GRT-enabled backups using the Symantec Backup Exec 12 advanced disk based backup option (ADBO), which enables off-host backup protection
- Support for remote and removable disk locations for GRT-enabled backups
- Support for Windows Server 2008 Active Directory
- Support for integrated consistency checks of Active Directory backups
- Support for Active Directory Lightweight Directory Services (AD LDS)

Redefining Exchange Server data protection

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, because 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 entails discovery of email communications

While businesses need email data to be protected and available, the amount of such data needing protection is growing exponentially—at a rate of 40 to 50 percent per year. 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 fastest possible data recovery in the event of a system crash, database corruption, loss of a single mailbox, or other 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, a separate slow and error-prone "brick-level" mailbox backup is typically required to recover each individual item without restoring the entire Exchange database.

Symantec Backup Exec 12 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 also eliminates the need for slow, arduous mailbox backups while still allowing the recovery of individual email messages, folders, and mailboxes with patent pending Granular Recovery Technology (GRT).

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

Key business benefits

- Helps safeguard critical Microsoft Exchange 2000–2007 Servers with the same agent
- Recovers individual email messages, mailboxes, and public and private folders from single-pass database backups in seconds—without separate "brick-level" individual mailbox backups
- Eliminates daily backup windows for Exchange with Continuous Protection
- Intuitive and easy-to-use interface makes backing up Exchange resources painless

Database protection, mailbox protection—or both?

Database backup is mandatory, because 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 Exchange backup application programming interfaces (APIs) provided by Microsoft.

An additional "brick-level" or mailbox backup job has often been considered optional, but it is highly useful for fast recovery 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**—Exchange mailbox backups require administrators to run two separate backups of essentially the same information: one backup of the individual mailboxes, and another of the Exchange mailbox stores. This leads to the second major drawback.
- **Twice the time and twice as error prone**—Individual Exchange mailbox backups are neither easy nor fast. While the 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 the Microsoft messaging application programming interface (MAPI)—an older, slower technology 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 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, and disabled mailboxes, which result in failed backups.

- **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 or disk 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. For organizations that use tape-based backup, duplicate backups can mean purchasing and managing additional tape media. If disk-based backups are used, that means sufficient disk must be acquired and managed.
- **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 as well, they typically have to perform separate backups, including:

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

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 back up the same Exchange data twice as much, taking twice as long (or more), using twice as much storage space to hold the additional backup data—and making the process of protecting and recovering Exchange twice the headache.

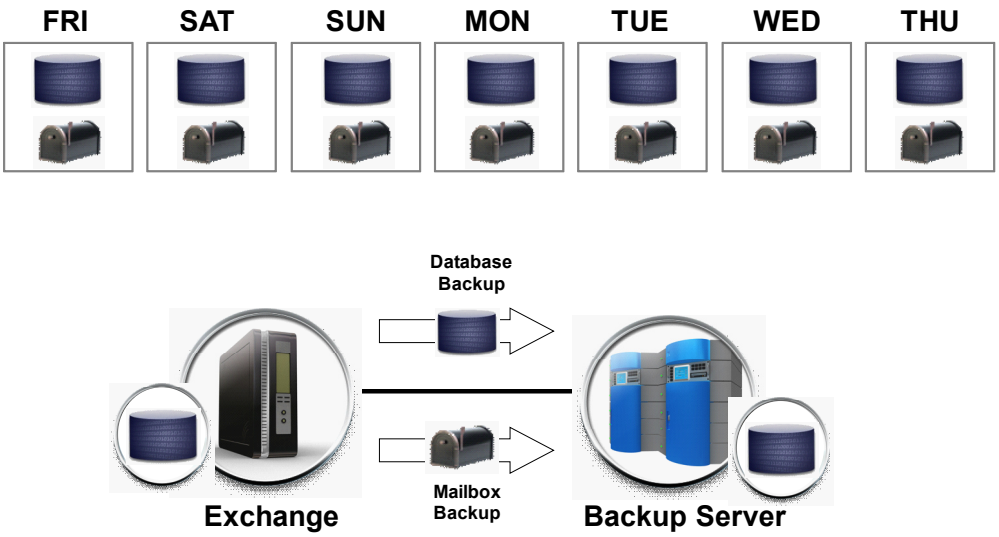

Figure 1. Traditional Exchange mailbox and database backups

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 email, folders, or mailboxes today?
- Are you backing up to tape or to disk?

Redefining Exchange protection and recovery

Symantec Backup Exec has supported Exchange since its introduction by Microsoft in 1996, and the Windows Server operating systems since their introduction in 1992. Symantec Backup Exec delivers established experience and proven reliability in the Exchange Server market. With Backup Exec 12 and the Backup Exec Agent for Microsoft Exchange Server, Symantec delivers two key technologies 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 that these technologies provide the fastest and most flexible way to protect and recover Exchange 2000 Server, Exchange Server 2003, and Exchange Server 2007 data.

Granular Recovery Technology benefits

By using Symantec Backup Exec Granular Recovery Technology (GRT), you can:

- 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
- Configure 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 and the associated IT management time
- Perform granular recovery or complete database recovery of all Exchange data

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

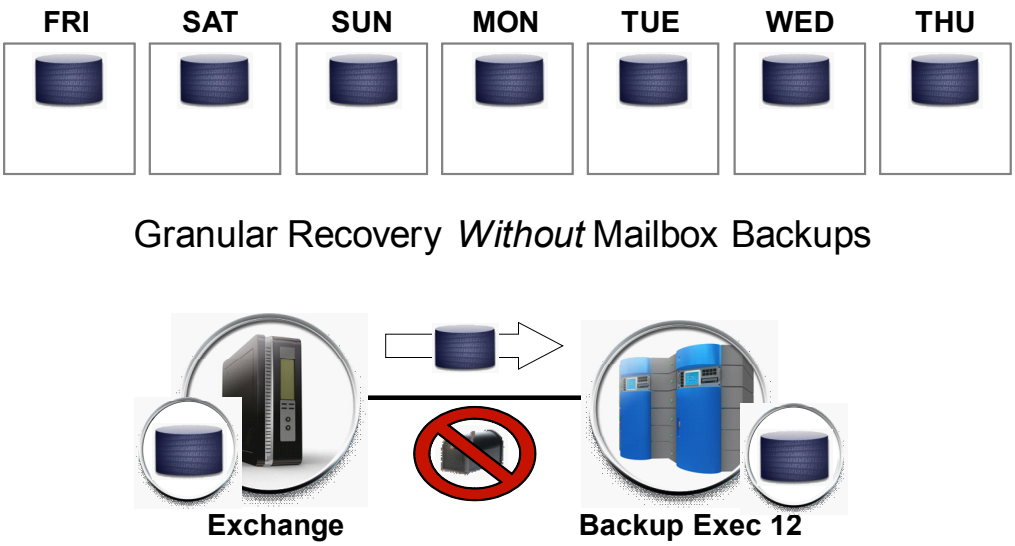

Figure 2. GRT-enabled Exchange mailbox and database combined backups

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

Continuous Data Protection for Exchange benefits

Using Continuous Data Protection for Exchange, you can:

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

Again, 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 Symantec 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 Data Protection for Exchange in Symantec Backup Exec uses the same GRT-enabled technology for full database or granular recovery, but extends it by permitting these backups to occur continuously to help enable Exchange recovery back to just a few minutes before the data loss. Continuous Data Protection enables Backup Exec to create GRT-enabled "recovery points" of Exchange at intervals that you specify in the Backup Exec console.

With Continuous Data Protection for Exchange, you perform a full backup once a week or once a month. Exchange transaction logs are continuously protected by Symantec Backup Exec and are automatically consolidated into easily managed recovery points to help ensure that your Exchange databases are protected up to the latest complete transaction log. When your recovery points are 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 the last recovery point created. The Exchange database and transaction logs are completely protected and quickly recoverable in a disaster recovery situation, providing comprehensive, continuous protection for your Exchange environment (see figure 3).

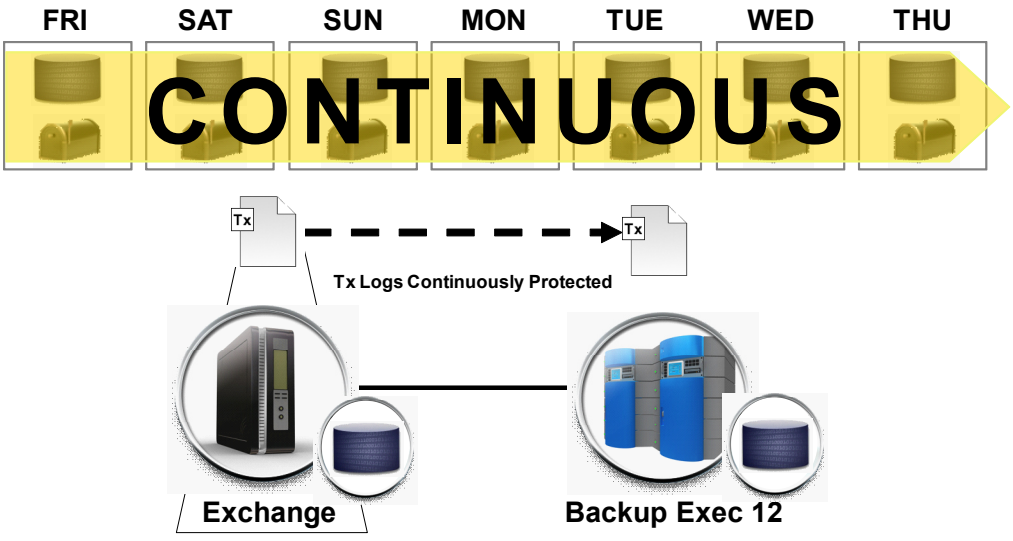

Figure 3. Continuous Data Protection for Exchange

Quick recovery of Microsoft Active Directory with Symantec Backup Exec 12

Microsoft Active Directory has become the cornerstone of organization and management in organizations of all sizes that deploy Windows-based systems. It is the standard directory service for applications dependent on Active Directory, such as Microsoft Exchange and SharePoint Server. Because of its increasingly widespread use, the need has intensified for comprehensive data protection for and quick recovery of Active Directory.

Human error and hardware or software failures are the leading causes of data and system loss. Active Directory has objects that are sometimes modified or deleted by mistake and attributes that can be overwritten by faulty scripts. Also, the Active Directory database can be corrupted as a result of hardware failure. An accidentally deleted user account translates into a loss of user productivity for hours—or even days—during which time the user has no access to company resources. Furthermore, other Microsoft applications dependent on Active Directory, such as Exchange and SharePoint, exacerbate the risks associated with Active Directory downtime. The loss or corruption of Active Directory data can create a ripple effect across the Windows environment, affecting Microsoft Exchange, SQL Server, and SharePoint.

Most Active Directory recoveries involve lost, deleted, corrupted, or overwritten user accounts, objects, and attributes. If not quickly resolved, these “small disasters” can quickly escalate. However, when an individual user account, object, or even attribute is lost or corrupted, recovering the entire Active Directory is not practical in terms of administrative time and effort.

Existing recovery solutions for Active Directory typically fall into two categories:

- Standalone utilities requiring Active Directory backups that are managed separately from existing backups
- Command-line utilities included free with the Windows operating system

Symantec Backup Exec provides an agent for Microsoft Active Directory that dramatically reduces the time needed to recover from small disasters, helping to improve employee productivity, reduce the potential for greater issues, and alleviate the aggravation associated with traditional Active Directory protection and recovery.

Key business benefits

- Online, granular recovery of individual Active Directory (AD) objects
- Restore objects without rebooting AD Domain Controllers
- Single Pass Backups for complete AD or object level recovery from single backup
- Point and Click restores
- Centralized System State and Active Directory protection

Traditional Active Directory recovery process

Any administrator who has ever had to restore Active Directory data (such as deleted user accounts and lost attributes) using standard tools (such as Microsoft Ntdsutil) understands the time and frustration that are hallmarks of the current recovery process. Administrators and companies recovering Active Directory data using current Active Directory recovery tools face several limitations:

- Active Directory authoritative restores require the use of command-line system tools such as Ntdsutil.
- A full restore of the system state must be performed, which increases downtime.
- The domain controller must be disconnected from the network for authoritative restores, which prevents user access to network resources during recovery.
- The domain controller must be rebooted at least twice, causing additional downtime and risk.
- After full recovery, Active Directory installations that have redundancy through replication must wait for large portions of the directory to replicate inbound and outbound, leading to additional downtime.

Traditional recovery for an Active Directory authoritative restore in case of corruption or deletion usually requires multiple time-consuming reboots and the use of complex command-line utilities on a critical domain controller. This process is as follows:

- Reboot in Active Directory recovery mode (F8).
- Restore system state.
- Pull network cable.
- Reboot.
- Use command-line utility Ntdsutil to elevate objects to recover.
- Attach to network.
- Wait for outbound and inbound replication to occur.

Improving Active Directory backup and recovery

The Symantec Backup Exec Agent for Active Directory is licensed as a separate, add-on component on a per-domain-controller basis. It also includes a Remote Agent for Windows Servers license for protecting non–Active Directory data on the domain controller.

The Backup Exec Agent for Active Directory allows you to recover from inadvertent deletions or changes to Active Directory data in as little as seconds or minutes.

Using this new agent, you can restore Active Directory or Active Directory Application Mode (ADAM) objects and attributes without performing an authoritative or non-authoritative full restore—and without rebooting.

Simply perform normal System State full backups of your Windows 2000, 2003, and 2008 Active Directory domain controllers locally or across the network. The Active Directory Agent's online, granular restore capability then allows you to recover selected objects—including users, organizational units, and printers, among others—down to the individual attribute level inside of those objects, specific sections of the directory, or the entire Active Directory without taking any Active Directory domain controllers offline.

This Active Directory backup and recovery process is much simpler than the traditional process shown earlier:

- Select System State components on your Active Directory domain controller(s) for backup.
- Ensure the checkbox to enable granular restore is selected (enabled by default).
- Initiate the backup.
- Browse Symantec Backup Exec created backups of your Active Directory domain controller.
- Select objects or attributes to recover.
- Initiate the restore.

Symantec Backup Exec Agent for Active Directory differentiators

Unlike other solutions, the Symantec Backup Exec Agent for Active Directory works with your backups of the Windows system state (where Active Directory is installed) and ADAM. When you back up the Windows system state, Active Directory is included as a component.

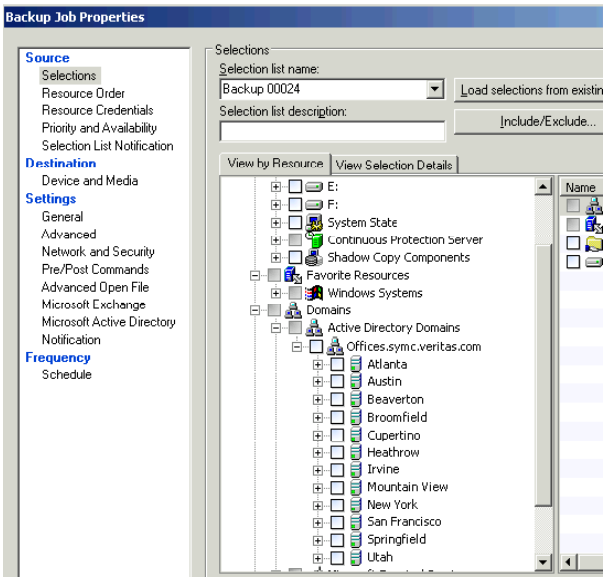

Figure 4. Single-pass backup of system state

To restore individual Active Directory objects and attributes, select them from the View by Resource tab in the Restore Job Properties view. You can also restore individual ADAM objects and attributes by selecting individual ADAM objects and attributes. If multiple ADAM instances are backed up, each instance appears under the ADAM node. To perform a full single-pass backup of Active Directory:

- Select System State components on your Active Directory domain controller(s) for backup.
- Verify that the checkbox to enable granular restore is selected (enabled by default).
- Initiate the backup.

Protecting Microsoft SharePoint

Collaboration—the hosting and exchange of information within an organization or between a business and its customers—has become a business-critical need for organizations of all sizes. Microsoft's SharePoint products are designed to make organizational collaboration more effective, enabling comprehensive content management and search capabilities, business process sharing, and information sharing across boundaries for better business insight.

Ensuring that the content within SharePoint is safely protected is paramount to a company's success. Even momentary loss of this data causes delays in effective communications both internally and externally, leading to losses in productivity and revenues. Today's information and technology administrators need reliable, easy-to-use, and efficient backup and recovery solutions to protect their intellectual property.

With Granular Recovery Technology (GRT) in Symantec Backup Exec 12, you can recover the entire Microsoft SharePoint Server or Services databases or individual SharePoint documents in seconds from a single database backup using the enhanced Agent for Microsoft SharePoint. SharePoint offers a document management, project collaboration, and intranet site management tool with improved scalability and flexibility for Windows servers. It facilitates easy organization, sharing, retrieval, and publishing of information over corporate intranets and seamlessly integrates with Microsoft Office and Web development tools.

SharePoint is fast becoming an industry platform for information distribution and content management. Its importance in the corporate environment is approaching mission-critical status as it becomes a vital link for internal communications. The loss of SharePoint Server data stores could potentially cause a large disruption should any one of the SharePoint components become corrupted or lost.

Many utilities and tools are available for backing up the various SharePoint components, but the complexity of coordinating them to ensure proper recovery of the SharePoint Server makes the process time-consuming—and they do not permit recovery of individual documents from the backup sets.

Key business benefits

- Protects and recovers business-critical Microsoft SharePoint Server 2003, SharePoint Server 2007, and server farms
- Using Granular Recovery Technology, enables the individual document restore from SharePoint Server and Windows SharePoint Services 2.0 and 3.0
- Simplifies and helps to ensure that the necessary components of SharePoint Server 2003 and 2007 are comprehensively protected and available for restoration and complete disaster recovery

The releases of SharePoint Server 2003, SharePoint Server 2007, and Windows SharePoint Services have dramatically changed the SharePoint architecture, requiring new methods of presenting data to the user and backing up this data. Not only is this format different from the previous version of SharePoint, but it also introduces many complexities in supporting data that is passed freely between servers. The exchange of information between servers in the farm will not only change how an administrator backs up this data, but also how the user goes about selecting backup and restore methods without having to know the configuration details of the servers or server farms.

Product highlights

The Symantec Backup Exec Agent for Microsoft SharePoint Server automates the many steps required to comprehensively protect a SharePoint Server environment. Protecting SharePoint Server 2003 or 2007 requires the use of the Backup Exec media server and the Agent for SharePoint, including the necessary remote agent for a single server or small server-farm configuration.

This agent supports backup and restore of SQL databases, document libraries, index databases, and some additional metadata. The Backup Exec Agent for SharePoint Server enables administrators to scale their backup and recovery activities from a single-server SharePoint environment to large, distributed server-farm environments. The use of server farms lets an administrator break out the various components of SharePoint Server configuration to many servers in an enterprise. (Each server is a component of a server farm.) The Agent for SharePoint also lets administrators browse the farm apart from the rest of the servers in the enterprise in order to customize their data protection strategy.

Comprehensive online Microsoft SQL Server data protection

Microsoft SQL database backup and recovery is an inherently challenging process that becomes more difficult as databases grow and as demands on their availability increase, limiting the time available for backup and recovery operations. Many organizations use manual backups to protect their SQL data. However, these methods do not provide the reliability required by corporate environments or improve the availability of critical systems.

Eliminating backup overhead on production databases is a requirement for many of today's critical online business applications. As use of SQL continues to grow in today's enterprise, so does the demand for backup administrators to protect the database in an online state while reducing the risk of data loss for the database and the applications that rely on it. Accordingly, the slightest performance impact or downtime can result in significant business loss. A backup and recovery solution must eliminate downtime and provide the efficiency and speed required by SQL environments.

SQL database protection challenges include:

- Protecting the database in an online state while minimizing impact during backup windows
- Restoring the database to a point in time that exists between backup sets
- Maintaining rigid service-level agreements for both backup and recovery operations

Symantec Backup Exec 12 Agent for Microsoft SQL Server protects business-critical online transaction processing (OLTP), online analytical processing (OLAP), and e-business data in case of application- or hardware-based corruption or loss. Designed for flexibility and ease of use, this agent gives SQL Server 7.0, 2000, and 2005 users comprehensive and customizable protection—down to the individual file group.

Is your backup window too small for a full backup? This agent can perform differential as well as transaction log backups with automatic truncation. Restoring to another SQL Server machine is easy, because Backup Exec Agent for Microsoft SQL Server can redirect a restore. The agent supports rollback and single-pass restores, so administrators can restore databases based on a point in time instead of on a specific backup job. Backup Exec leverages Microsoft's Virtual Device Interface (VDI) to give users the easiest and fastest way to protect the SQL database. To resolve backup window issues, consider using off-host backup or continuous protection for SQL.

Key business benefits

- Non-disruptive SQL server backup and quick restoration
- Support for both 32- and 64-bit SQL Server installations
- Integrity of vital SQL Server data is maintained during backup and recovery operations
- Increases the chance of data recovery and minimizes data loss without inhibiting daily database activity
- Point-in-time database recovery allows for quick database restore

Why protect Microsoft SQL Server?

Microsoft SQL Server is a general-purpose relational database server that can scale from hosting simple databases to supporting clustered, mission-critical business applications such as SAP. In fact, with over 51 percent market share, SQL Server is the most popular relational database on Microsoft Windows. Simply put, the more a business depends on SQL Server, the more important it is to protect it.

To maintain Microsoft SQL Server's availability and protect its databases, a business needs a working and thoroughly tested data protection and recovery plan, as well as reliable data protection software. Together, they can help ensure recovery of the SQL Server environment and its databases. The key objectives are to minimize downtime for your database environment and to provide the fastest possible data recovery in the event of a system crash, database corruption, or other data loss.

Key benefits

- Enables non-disruptive SQL Server backup and quick restoration
- Supports both 32-bit and 64-bit SQL Server installations
- Helps maintain the integrity of vital SQL Server data
- Increases the chance of data recovery and minimizes data loss without inhibiting daily database activity
- Recovers the database to a point in time or last commit point, allowing for quick and reliable data restore

Key features

- Database snapshot—This backup method, a new feature in SQL Server 2005, is fully supported and used to quickly restore SQL Server databases. Grooming and pruning are automatically maintained in the Backup Exec catalog and job history; a fast and reliable snapshot has very little impact to SQL Server operations.
- Copy-only backup (also known as out-of-band backup)—This backup method operates as a full backup but does not disrupt future full or differential backup rotations.

- Simplified point-in-time restores—Simply select a database and time to recover; Backup Exec assembles the necessary full, differential, and log sequenced backups and identifies any user selection or redirection conflicts—or any even later date to which the database could be restored.
- Full text catalog support—The text catalog is seamlessly protected and recovered as part of any backup/recovery job.
- x64 and i386 concurrent instance protection—Protect x64 and i386 instances running at the same time on the same server.
- Continuous data protection for SQL Server—Continuously back up and recover SQL Server databases and file groups to any point in time.

Product highlights

- Support for SQL Server 7 through 2005
- Data recovery to named transaction log marks within the transaction log, so administrators can restore data up to the point at which the data was last committed to the database
- Modeling of SQL database backups that can be targeted to fit the individual needs of the business by performing full or differential backups and restores of the file group
- Expanded data protection parameters that include multiple and named SQL Server 2000/2005 database instances running concurrently on the same server
- Improved performance of database consistency checks (DBCC) with the ability to perform a physical-only DBCC on SQL Server 2000/2005 databases, which greatly enhances backup speeds without sacrificing backup accuracy
- Support for SQL Server database mirror data protection

Usability

- Transparent integration online or with hot SQL Server backups within regularly scheduled network protection routines
- Individual file group backup and restore
- Support for SQL Server rollback restores to a specific point in time, rather than a specific backup job
- Flexible backup launch options for SQL Server, so backup jobs can be launched immediately or on a schedule
- On-disk copy, allowing administrators to direct a copy of data streams to disk media for quicker recovery
- Restore with errors, enabling administrators to force a restore of the database without failing the job to a suspended state and to allow error correction prior to installation

Reliability

- A Microsoft Certified solution for the protection and recovery of SQL Server 7.0, 2000, and 2005
- Use of native SQL Server APIs for backups, snapshots, and restores, helping to ensure reliable and consistent SQL Server protection
- Verify-only restore, a safety feature that automatically validates SQL Server restore selections and job options prior to executing the restore—a process that detects restoration selection errors and offers to fix them
- Integration with the Symantec Backup Exec Intelligent Disaster Recovery Option, a rapid, bare-metal system disaster recovery to the last full, incremental, or differential backup, complete with identical configuration of the operating system, user profiles, updates, and other applications
- Restore improvements that lead to faster and more reliable SQL Server recovery, including verify-only restore and continue restore on error

Why do you need the Symantec Backup Exec Agent for Microsoft SQL Server?

Protecting a database server such as Microsoft SQL Server requires careful thought and planning to meet the availability needs of your company and its budget. The most common method of formalizing these needs is through service-level agreements (SLAs). An SLA is a contract between the users and the provider (such as the IT department) that outlines such factors as expected services, acceptable downtime, and response time for problem resolution. It is critical that you understand these factors during the design phase of your SQL Server deployment, as they can heavily influence the resources that you will need to support the SLA.

IT must consider its recovery point objective (the point to which data must be restored) and well as its recovery time objective (the amount of time it takes to come back online) when determining an overall data protection and disaster recovery strategy.

The basic rule of thumb regarding data protection is that the higher the requirement for availability, the higher the cost of achieving it will be. Various technology stops along the way to higher availability include file by file, backup, snapshots, continuous protection, and various forms of server/database replication. Data protection is the cornerstone of any availability solution—and choosing a reliable backup product should be paramount, because it may be your last line of defense against data loss.

Symantec Backup Exec, together with the Agent for SQL Server, easily meets the criteria for fast, flexible, and reliable SQL Server data protection. In fact, Backup Exec has supported Microsoft SQL as well as Windows NT and Windows 2000 since its introduction in 1995, giving Symantec significant experience in this market.

Conclusion

Microsoft Exchange, SQL, Active Directory, and SharePoint have quickly risen to mission-critical status in many companies. Therefore, keeping these applications highly available and protecting the associated data is not an option, but a mission-critical responsibility. Symantec Backup Exec 12 reduces the complexity and challenge of protecting these Microsoft applications. With Granular Recovery Technology for Exchange, Active Directory, and SharePoint Servers and Continuous Data Protection for Exchange, Symantec Backup Exec 12 now has the reliable protection and efficient recovery technologies an organization needs to succeed with these Microsoft applications.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage 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

02/08 13803400