



Confidence in a connected world.

Windows® Enterprise Data Protection with Symantec Backup Exec™—Best Practices for Implementing a Centralized, SAN-Based Infrastructure

Windows® Enterprise Data Protection with Symantec Backup Exec™

Contents

Executive summary	4
Centralizing remote office data protection: Central Admin Server Option (CASO)	5
Challenges	5
Product highlights	6
How it works	6
<i>Conceptual overview</i>	6
<i>Architecture</i>	7
CASO summary	8
Lowering your total cost of ownership: Backup Exec Infrastructure Manager	9
Challenges	9
Mastering your Backup Exec infrastructure	10
Product highlights	10
How it works	11
Backup Exec Infrastructure Manager summary	12
Meeting today's storage management needs: Backup Exec SAN Shared Storage Option (SSO)	13
SAN topology: SCSI over Fibre Channel	13
Challenges	10
Product highlights	14
How it works	15
<i>Conceptual overview</i>	15
<i>Centralized database, device pooling, and media sharing</i>	16
<i>Device conflict resolution</i>	17
<i>Enhanced centralized management with SAN SSO and CASO</i>	17
SAN SSO summary	17

Contents (cont'd)

Achieving faster backups and restores and reduced backup windows: disk-based data protection	18
Advantages of disk-based backup	19
<i>Reduced backup windows</i>	19
<i>Reduced recovery times</i>	19
<i>Reduced tape cost</i>	19
Strengths and weaknesses of today's backup media	20
<i>Traditional tape-based backups</i>	20
<i>Traditional disk-based backups</i>	20
<i>Continuous disk-based backups</i>	21
Solution highlights	22
Traditional disk-based backup methods	23
<i>Backup-to-Disk folders</i>	23
<i>Duplicate Backup Set template</i>	24
Continuous disk-based data protection	25
<i>Disk as the primary backup target</i>	25
Advanced disk-based backup options	26
<i>Synthetic Backup</i>	26
<i>True Image Restore</i>	26
<i>Off-Host Backup</i>	27
Disk-based data protection summary	27
Summary	28

Executive summary

Today's enterprises face a growing data protection challenge: how to optimize the backup and recovery of a volume of business-critical data that grows larger each day and, in many cases, doubles each year. Most enterprises are finding that their IT footprint and storage resources continue to grow at a rate of 40 to 50 percent per year, which adds considerable complexity to their existing data protection strategies. This challenge becomes yet more difficult as companies migrate from stand-alone Windows® server backups to enterprise site-wide backups that are performed across their local area network (LAN) and storage area network (SAN) environments.

With the data protection landscape becoming more distributed and IT resources growing increasingly constrained, businesses need a centralized data protection strategy that can efficiently manage multiple backup and recovery jobs across the enterprise. In addition, the data protection strategy must be able to support an off-host backup strategy to efficiently minimize the impact on mission-critical applications and interruption to network users, and take advantage of the speed of disk-based data protection.

Symantec Backup Exec™ 12.5 addresses these critical enterprise challenges with the following cutting-edge features: Central Admin Server Option, Backup Exec Infrastructure Manager, SAN Shared Storage Option, and dynamic disk-based data protection. These four features are the subjects of this paper.

Centralizing remote office data protection: Central Admin Server Option (CASO)

Remote offices and distributed networks offer a distinct set of challenges to companies that are unable or unwilling to consolidate their data protection and storage management in a central location. The task of setting up and managing backup jobs is extremely time-consuming when many backup servers are deployed, and this effort is magnified when backup servers are remotely distributed. Proactive monitoring of media server activities and the ability to report on backup, restore, and storage management activities are critical to an administrator's ability to effectively manage a highly distributed storage network. The Symantec Backup Exec 12.5 Central Admin Server Option (CASO) offers simplified centralized management that delivers a robust and highly scalable solution for managing multiple Symantec Backup Exec media servers. The functionality lets today's storage administrator maximize a Backup Exec software investment by providing centrally managed operations, load balancing, fault tolerance, monitoring, and reporting for all Symantec Backup Exec media servers, whether in a Windows data center or distributed throughout the network.

Challenges

With the distributed IT environments of today, administrators are constantly forced to do more with less. Challenges ranging from lack of backup staff at remote locations to better utilization of the backup medium often make data protection operations cumbersome and overwhelming:

- Remote sites often have little to no IT staff, and backup operations are sometimes left to non-IT personnel.
- Administrators often have to manage media servers locally and have no holistic view of their enterprise backup environment.
- Undistributed catalog data often increases recovery time objectives.

Product highlights

CASO creates a one-to-many relationship between a central administration server and managed media servers. This dramatically reduces administration time while increasing the resiliency and visibility of Symantec Backup Exec software in a Windows environment.

Table 1. Central Admin Server Option (CASO)—features and benefits

Feature	Description	Benefit
Centralized administration	Provides a single console for managing the entire Backup Exec environment, creates and delegates jobs to multiple Backup Exec media servers, defines device and media sets	Provides a single point of administration and control unifying independent Backup Exec media servers, dramatically cuts the time and effort required to make changes, reduces duplication of effort
Operational resiliency	Automatically load-balances jobs across media servers, provides job failover from one Backup Exec server to another, centralizes or replicates catalogs for restores	Increases efficiency and usage of storage resources, removes single point of failure, eliminates manual connection restores
Reporting and monitoring	Monitors all job activity dispatched by the CAS in real time, provides holistic reporting for the entire storage environment, centrally defines notification and alert settings	Improves reaction time and reduces the time to resolve issues, easily identifies trends across the entire Backup Exec environment, helps ensure accurate notification of alerts across the network

How it works

Conceptual overview

The Symantec Backup Exec Central Admin Server Option transforms your stand-alone Backup Exec media server-based environment into a centrally managed data protection solution. In the CASO-enabled environment, the central admin server provides a single point of management and administration for the Backup Exec environment. The central admin server is where you make decisions about what data and servers are to be protected in your environment. Unlike single server-oriented Windows backup solutions, CASO uses a state-of-the-art architecture built on the following architecture highlighted in figure 1.

Architecture

The Symantec Backup Exec Central Admin Server Option unifies multiple, independent Backup Exec servers to provide one central point of administration and control. In a CASO-enabled Backup Exec environment, a group of standard stand-alone Backup Exec media servers are managed and monitored from the Backup Exec media server where the CASO software has been installed. This media server, known as the central admin server, becomes the single point of administration for a CASO-based Backup Exec data protection environment, and it is where all Backup Exec related administration tasks occur (see figure 1).

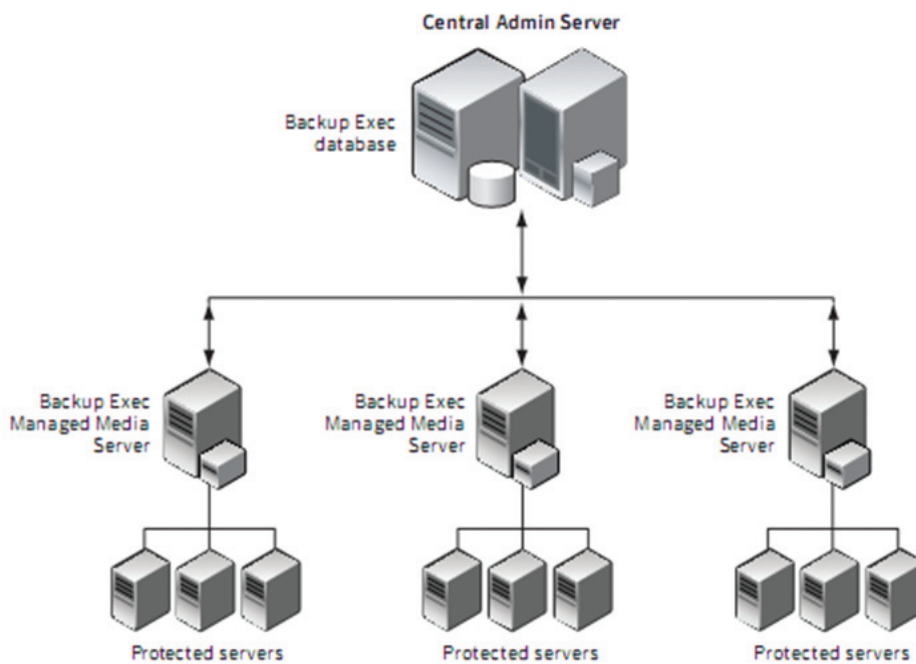


Figure 1. Central Admin Server Option architecture

The Central Admin Server Option includes two components:

- **Central admin server**—a Symantec Backup Exec 12 media server that is used for central administration tasks such as
 - Creating backup jobs by creating policies and selection lists from a centralized location
 - Centralizing job delegation and load balancing
 - Managing notification and alerts
 - Job monitoring and reporting
 - Job history and job logs
 - Centralized restore jobs
- **Managed media servers**—Backup Exec media servers with one or more backup storage devices attached that fall under the management of the central admin server and are responsible for the actual processing of backup and restore jobs. In the event of a loss of communication with the central admin server, managed media servers can operate autonomously.

A central admin server can also be targeted as a managed media server to process jobs.

CASO summary

In an era of continuing data growth, organizations need simple, centralized, scalable management. The Backup Exec 12 for Windows Servers Central Admin Server Option gives Windows based organizations the flexible, powerful solution they need to manage backups and restores across a distributed organization—with multiple servers either in one campus or distributed among remote offices. CASO can help you manage the explosive growth of data and avoid the pitfalls of Windows single server-based backup, all with reduced management requirements.

For larger organizations that require efficient software and patch management for their Backup Exec and Backup Exec System Recovery environment, Symantec has introduced Backup Exec Infrastructure Manager 12.5 (powered by Altiris), which provides centralized Backup Exec software management through one console. The Backup Exec Infrastructure Manager allows companies to easily inventory, discover, and upgrade Backup Exec software or deploy infrastructure patches to existing and new Backup Exec and Backup Exec System Recovery systems across an entire organization, providing simplified reporting and maximum return on investment.

Lowering your total cost of ownership: Backup Exec Infrastructure Manager

Challenges

As Symantec Backup Exec gains wider distribution in an organization's IT infrastructure, the need for ways to automate its deployment, updating, monitoring, upgrading, and licensing grows too. Like many applications, a significant deployment or upgrade of Backup Exec can require careful planning and specialized tools to reduce its total cost of ownership and that of its components.

A backup solution must be scalable and facilitate the deployment, updating, and management of hundreds of remote backup servers from a single console. Many organizations desire “cookie cutter” yet customized installations of Backup Exec at all of their locations. When new installations of Backup Exec must be installed or maintained, how quickly can an administrator do the job?

For example, many organizations run a mixed environment that includes many different versions of Backup Exec, complete with different patch levels. When managing a large Backup Exec installation, it may not be clear:

- Which versions of Backup Exec are installed—and on which systems?
- What Backup Exec license keys have been installed, and for which Agents and Options?
- What patch level are the Backup Exec Servers and Agents at?
- Which machines on the network are currently not protected by any Backup Exec software?
- How can multiple Backup Exec installations be quickly updated and upgraded when needed?

When data protection solutions are being compared, many of these questions are overlooked. The ideal backup solution should have capabilities that minimize the administrator's need to perform management tasks at every phase of the backup application's lifecycle in the organization—from installation, to updates, to upgrades, to discovering unprotected new systems and applications.

Mastering your Backup Exec infrastructure

For environments that are large enough to experience these challenges, the new release of Backup Exec Infrastructure Manager introduces the specialized management tools needed for multiple Backup Exec installations across large organizations and multiple sites. Leveraging the award-winning Altiris Notification Server's Configuration Management Database (CMDB) technology, Backup Exec Infrastructure Manager delivers a highly scalable solution for complete Backup Exec lifecycle management that complements a Central Admin Server Option (CASO) deployment.

The benefits of Altiris are helping many of today's Backup Exec customers who already use Altiris to manage thousands of systems and their applications worldwide. Additional information on Altiris CMDB technology is available at the following link:

<http://www.altiris.com/Products/AssetCMDB.aspx>

Product highlights

Backup Exec Infrastructure Manager allows administration from a centralized console. After configuration of a Backup Exec Infrastructure Manager server, almost all Backup Exec operations can be managed at the CASO server, including the following:

- Centralized discovery and inventory of all Backup Exec Servers, Agents, and Options
- Centralized creation of custom Backup Exec installations
- Centralized view of protected vs. unprotected systems
- Centralized creation of Backup Exec 9.1–12.5 version upgrades
- Centralized creation of Backup Exec patch deployments
- Centralized Backup Exec license management
- Centralized Backup Exec disk consumption monitoring for catalog and disk-based backup data
- Centralized command-line script management and diagnostic log gathering

Backup Exec Infrastructure Manager was created to help organizations reduce the total cost of ownership of Backup Exec. It was designed to reduce the time involved in deploying, patching, upgrading, troubleshooting, and monitoring the various components of Backup Exec in large organizations. Backup Exec Infrastructure Manager works with the Central Administration Option (CASO), which provides active management of Backup Exec operations across multiple

Backup Exec servers, while Backup Exec Infrastructure Manager delivers a new level of centralized standardization for deploying, upgrading, and patching Backup Exec installations. This combination of CASO and Backup Exec Infrastructure Manager is ideal for remote branch offices where network connectivity may be intermittent, but standardization is needed.

How it works

Backup Exec Infrastructure Manager utilizes the Altiris Notification Server and Microsoft SQL database to store data about your Backup Exec configuration from systems it has discovered and inventoried using the Altiris Notification Server (NS) Agent. It can then deploy updates or upgrades to your existing Backup Exec Servers and Agents or deploy new customized installations of Backup Exec (see figure 2).

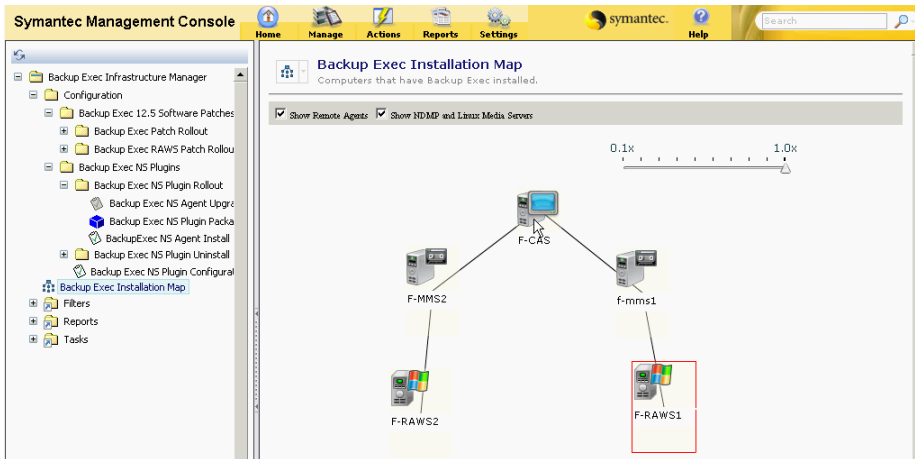


Figure 2. The Backup Exec Infrastructure Manager console view of a Backup Exec server environment

Table 2. Backup Exec infrastructure Manager—features and benefits

Feature	Benefit
Discovery and inventory	<ul style="list-style-type: none"> • Discover Backup Exec 9.1–12.5 components across the enterprise • Inventory all Backup Exec components and license keys • Display an Installation Map of Backup Exec Servers, Agents, and Options
Standardize Backup Exec deployments	<ul style="list-style-type: none"> • Deploy new customized Backup Exec installations based on a standardized configuration • Deploy upgrades to existing Backup Exec installations from 9.1–12.5 • Deploy new Backup Exec updates and patches to Backup Exec 12.5 Servers and Agents
Proactive Insight (reporting and monitoring)	<ul style="list-style-type: none"> • Monitors Backup Exec disk consumption for catalog and backup data written to disk locations • Provides holistic reporting for the entire storage environment • Centrally defines Backup Exec custom scripts and tasks through a built-in CLI editor
View system protection status	<ul style="list-style-type: none"> • Get protected vs. unprotected view of systems that are being protected with Backup Exec software • See which system are “at risk” due to an incomplete backup • Determine status of last backup from Backup Exec Job History data

Backup Exec Infrastructure Manager summary

Backup Exec Infrastructure Manager helps larger organizations optimize their Backup Exec environment and helps to ensure that their entire system is efficiently backed up with the latest data protection technology. It also makes it easier for administrators to keep their entire server system up to date with the latest software patches, protecting the organization from the latest viruses and threats. From license discovery and inventory to automated Backup Exec upgrades to ongoing system risk reports, Backup Exec Infrastructure Manager is a perfect complement for every Backup Exec enterprise.

Meeting today's storage management needs: Backup Exec SAN Shared Storage Option (SSO)

The storage industry is at a turning point in the evolution of storage management. Data is growing at an unprecedented rate, stressing the limits of current technology. The emergence of storage area networks (SANs) offers significant advantages over the traditional approaches used for backup today. The SAN storage paradigm combines the benefits of high performance with the ease of centralized management. Data movement during backup processes occurs off the LAN, freeing network resources and reducing the impact on users while improving business productivity.

Furthermore, SAN topologies let multiple distributed backup servers share common, centralized storage devices that are connected over a Fibre Channel SAN for greater efficiency and fault tolerance. By sharing, backup servers can load-balance activity across all available storage devices, thereby increasing performance and backup speeds, centralizing management tasks, and lowering the total cost of ownership.

The emergence of SANs based on Fibre Channel (FC) has redefined server backup. A SAN interconnects storage devices and servers in a many-to-many configuration, making it possible for servers to share the same storage devices. Data movement does not occur over the LAN, but over a separate network attached to the back end of the server. In essence, the SAN acts like a more sophisticated SCSI bus that lets several distributed servers attach directly to a centralized storage repository over a high-speed connection.

SAN topology: SCSI over Fibre Channel

A SAN replaces the SCSI bus that normally connects a server to a local storage device. Most SANs are constructed using advanced Fibre Channel technology rather than the conventional Ethernet technology used in most LANs. Current SAN architectures use a switched-fabric topology. The use of Fibre Channel technology offers several benefits that enhance the flexibility and scalability of a SAN when compared to tethered devices connected to servers over a SCSI bus:

- **Capacity**—A switched-fabric network could include millions of nodes.
- **Performance**—Communications transfer speeds of as fast as 4 Gbps are possible over Fibre Channel networks.
- **Distance**—Connections can be as long as 10 km with single-mode fibre, and even longer if a repeater is used.

Challenges

Despite the benefits that make LAN-free backup so appealing, there are some challenges to deploying a SAN, and directly attaching multiple servers has several consequences. In most cases, IT administrators look to the storage software solution to resolve the following issues and deliver the benefits of SAN-enabled backup:

- Multiple servers may request services from the storage device simultaneously, leading to device contention.
- Servers may accidentally overwrite recent backup tapes created by other servers.
- Industry standards are just now maturing, and hardware and software manufacturers are only now providing interoperable solutions.

Product highlights

The Symantec Backup Exec for Windows Servers SAN Shared Storage Option (SSO) is a powerful, LAN-free backup solution that lets multiple distributed backup servers centralize the use of storage devices (tape libraries, virtual tape libraries, or backup-to-disk folders connected over a switched-fabric SAN) for greater performance, efficiency, and fault tolerance. SSO improves storage manageability and performance for large-scale, high-end storage environments.

Table 3. SAN Shared Storage Option—features and benefits

Feature	Description	Benefit
Backup device sharing	Allows multiple Backup Exec servers to share backup devices directly across a SAN	Decreases LAN traffic and improving backup-and-restore performance
Device control through the SAN	Dynamically controls any tape drive(s) in a library by independently issuing commands to the robotic arm	Expensive tape libraries do not need to be dedicated to individual machines better leveraging your hardware investments
Central hardware resource tracking	Centrally tracks device and media usage	Provides the ability to generate accurate, reportable statistics on devices and their media
Combines easily with the Symantec Backup Exec Central Admin Server Option (CASO)	Three-tier centralized monitoring, management, alerting, and reporting for multiple Backup Exec servers in SAN, LAN, and WAN environments	One point of control for all backup needs

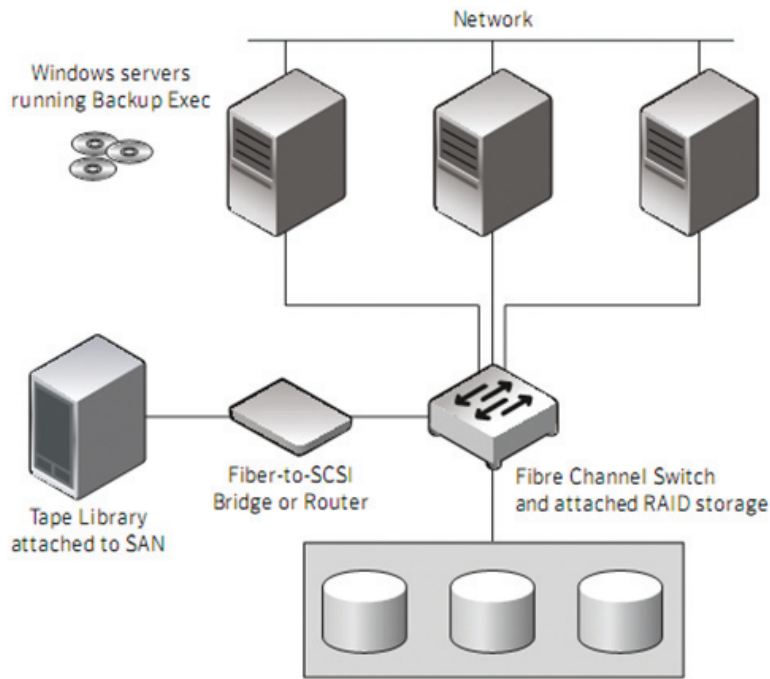


Figure 3. Backup Exec SAN Shared Storage Option architecture

How it works

Conceptual overview

Three Symantec Backup Exec components are needed in a SAN deployment:

- Symantec Backup Exec for Windows Servers
- Symantec Backup Exec SAN Shared Storage Option (SSO)
- Symantec Backup Exec Library Expansion Option (LEO)

The Symantec Backup Exec software is the workhorse, performing the actual backup activity, while the SAN SSO centralizes and arbitrates the scheduled activities to the storage devices. The LEO allows the SAN SSO to be licensed to use multiple drives in the storage device simultaneously in order to take advantage of multiple drive libraries. Each Symantec Backup Exec media server performs a local backup directly over the SAN, minimizing the impact time of the backup operation.

Centralized database, device pooling, and media sharing

Centralized management and control of the backup media server's activities is provided by the SAN SSO, which manages a centralized database of all server activities. The SAN SSO is designed around the Symantec Backup Exec Advanced Device and Media Management (ADAMM) database, which provides a single, unified view of all backup devices and media within the SAN. Instead of each backup server having its own dedicated ADAMM database, all Backup Exec servers are configured to use the central ADAMM database, which allows all device and media information to be shared with all Backup Exec servers on the SAN.

All Symantec Backup Exec servers on the SAN share the same device configuration, including information about which devices belong to which pools. As with the standard edition of Backup Exec software, backup devices can be pooled together as a unit to offer the benefits of fault tolerance (if a device is unavailable) while job activity is load-balanced across all available devices within a pool. Device pools are highly recommended to optimize the system's overall performance and fault tolerance.

All Symantec Backup Exec servers on the SAN share the same media configuration, including the various media sets and corresponding defined overwrite protection periods. Media created and used by one Backup Exec server will be recognized by all other Backup Exec servers on the SAN and will not be overwritten before the protection period has expired. Once the protection period has expired, any Backup Exec server can reuse the media.

All historical information for device and media usage is tracked in the central ADAMM database. Reports may be generated to show read/write statistics and error counts. Furthermore, all reports can be created from a single location, since there is a common database for all Backup Exec servers.

Device conflict resolution

The SAN SSO lets any Symantec Backup Exec server dynamically control any tape drive(s) available in the library, and it also lets each Backup Exec server issue commands independently to the robotic arm. All device activity is controlled through software.

Device conflicts are managed by issuing SCSI reserve and release commands to devices during use. The reserve and release mechanism is defined in the SCSI specification and permits device-sharing in multi-initiator configurations. Thus, the sharing intelligence built into the SCSI devices provides arbitration of potential device contention, instead of leaving the servers to try to arbitrate.

Enhanced centralized management with SAN SSO and CASO

The Central Admin Server Option (CASO) is optional but highly recommended in order for SAN SSO environments to monitor and manage the multiple Backup Exec servers, including SAN SSO enabled Symantec Backup Exec servers.

The Symantec Backup Exec Central Admin Server Option (CASO) transforms your stand-alone Backup Exec media server-based environment into a centrally managed data-protection solution. In the CASO-enabled SAN SSO environment, the central admin server extends a single point of management and administration for the Backup Exec environment beyond just centralized management and sharing of backup devices. It is where users can decide which data and servers are to be protected in their environments.

A Symantec Backup Exec 12 SAN SSO primary media server can also be configured as a central admin server and used for additional central administration tasks such as:

- Creating backup jobs by creating policies and selection lists from a centralized location
- Centralizing job delegation and load balancing
- Managing notification and alerts
- Monitoring jobs and reporting
- Monitoring job history and job logs
- Managing centralized restore jobs

SAN SSO summary

Storage area networks are changing the way IT organizations serve their customers, providing higher availability and more centralized management of storage resources. Symantec Backup

Exec SAN SSO software reduces LAN traffic and improves backup performance with a LAN-free backup solution, reduces redundant backup hardware, and decreases the cost of maintenance and service.

In addition, by combining the Backup Exec SAN SSO software with the Backup Exec CASO, Symantec Backup Exec 12 delivers simplified centralized management that delivers a robust and scalable solution for managing multiple Backup Exec media servers in a SAN, LAN, or WAN environment. The functionality lets today's storage administrator maximize a Backup Exec software investment by providing centrally managed operations, load-balancing, fault tolerance, monitoring, and reporting for many Backup Exec media servers, whether in a Windows based data center or distributed throughout the network.

Achieving faster backups and restores and reduced backup windows: disk-based data protection

Today's Windows based organizations are facing the challenge of how to efficiently back up and protect data volumes—which are growing at 40 to 50 percent each year—as well as how to ensure instant, on-demand data recovery. While traditional tape backup has proven effective over the years, today's business climate demands a faster, more efficient approach to backup and recovery. For this reason, many companies are starting to implement disk-based backup methods, which can help solve several major challenges:

- Backup to traditional tape is often slower than backup to disk, requiring longer backup windows.
- Restore from traditional tape is slower due to longer seek times, which extends recovery times.
- Backup windows are often strained and not easily defined in today's world where 24x7x365 uptime is a reality.
- It takes additional time, disk, and server resources to perform a traditional restore of an entire resource in order to obtain an individual file or object.
- Traditional backup of application servers places a heavy burden on the server that is hosting the application.
- Making a duplicate copy of a backup set is often a manual operation and requires more of the administrator's valuable time.

Advantages of disk-based backup

Disk-based backup can reduce backup windows, restore time, and expensive tape consumption as well as allow the use of enhanced Symantec Backup Exec 12 features such as Granular Recovery Technology.

Reduced backup windows

Often disk is faster than tape in raw throughput and because of the random access nature of disk technology. Also, with either backup-to-disk or Continuous Protection Server, backups can take advantage of multi-streaming—so more than one backup job can transfer data at the same time.

Reduced recovery times

Administrators can enable the Granular Recovery Technology feature with disk-based backups. Granular Recovery Technology makes data recovery as easy as searching for the file, email message, or object and starting the restore. For Exchange, Granular Recovery Technology eliminates brick-level backups and improves recovery times because individual email messages are extracted from a full or incremental backup. Disk-based backups help to ensure that administrators need no longer look in various media cabinets to find a tape or file—no more searching for the tape and no more swapping tapes in and out of the drive. Continuous Protection Server also allows end users to restore their own file server files using a simple Web browser.

Reduced tape cost

Disk-based backups reduce tape expenditure because fewer tapes are needed for daily, weekly, and monthly backups. With either backup-to-disk or Continuous Protection Server in use, the disk drive acts as a staging area. Backups to tape can be reduced from once a day to once a week—or even once a month—which greatly decreases the cost of tape in the environment.

Strengths and weaknesses of today's backup media

To select the right data protection strategy for your organization, it is important to understand the differences between traditional tape-based, traditional disk-based, and continuous disk-based data protection offerings.

Traditional tape-based backups

Over the years, tape backups have proven to be an effective data protection and recovery method. Tape is an inexpensive medium on which to store data. It is also a format that can be easily moved offsite, which is a familiar solution for IT administrators. However, tape presents some significant challenges. The first is reliability: Industry reports note that tape can fail 17 to 40 percent of the time. The second is complexity: Tape lacks the flexibility and simplicity that many organizations require in a data protection solution. Finally, there is speed: As data volumes increase, tape backups take longer—and the recovery process can also be time-consuming, delaying file delivery and requiring trained administrators to recover data.

Traditional disk-based backups

Disk-based backups provide several key benefits over tape-based backups. Disk-based backups are typically faster and more efficient and demonstrate dramatic recovery time improvement. Disk also provides a more reliable format for initial data protection and improves overall performance for simultaneous backup jobs (or multi-streaming). The drawbacks of disk-based backups include the potential impact on production servers and complexity in managing backup jobs. Also, data is backed up in a format that requires IT intervention for restores. Overall, the benefit of disk-based backup is that data is much faster to restore and the data recovery process is more reliable. There is no need to find the tape, load it, and then reload the data. In addition, disk-based data can still be backed up to tape for long-term archival and off-site storage.

Continuous protection with the Backup Exec Continuous Protection Server

The Backup Exec Continuous Protection Server helps ensure that business-critical data is always protected and always available. It combines proven replication technology and disk-based data protection to provide fast and reliable data backup and retrieval. The Continuous Protection Server lets administrators restore data at a granular level from points in time throughout the day. Administrators can also perform simultaneous backups of multiple servers. While the Continuous Protection Server is a separate application, there is integration between the Continuous Protection Server and Backup Exec for Windows Servers to enable complete protection and recovery of the Continuous Protection Server environment.

Continuous data protection offers the core benefits of disk-based data protection (faster backups, near-instant restore) while removing some of the key weaknesses. The Continuous Protection Server offers many benefits, including these:

- Data is always protected.
- Only the changed portions of files (block-level changes) are captured.
- Multiple file servers can be backed up simultaneously.
- Data can be recovered to many points in time rather than once per day, which is typical with traditional backup
- There is no impact on business servers (no backup windows).
- Files are in native format, enabling end-user recovery.
- End users can perform their own file recoveries through the Backup Exec Retrieve Web console, without contacting IT.

The Continuous Protection Server has one major caveat—it is a separate installation and administration console than the remainder of Backup Exec. However, this concern may be offset by robust backup and recovery capabilities and instant granular recovery, which can help reduce IT administration while improving service levels and end-user productivity.

Solution highlights

To protect mission-critical resources in a timely fashion, many administrators are turning to disk-based backup methods in order to meet the demands of their data protection policies. Through maximized disk-based data protection methodologies, Symantec Backup Exec 12 for Windows Servers offers multiple ways to improve backup and restore operation times and shorten or eliminate backup windows.

Table 4. Disk-based backup—features and benefits

Feature	Description	Benefit
Backup-to-disk folders	<ul style="list-style-type: none"> • Use existing NTFS storage for backup and restore. • Create a virtual tape library that can emulate up to 16 tape drives for concurrent operation. • Enable multi-streaming from a number of different sources locally, over the network, or over the SAN. 	<ul style="list-style-type: none"> • Use nearly any NTFS device as a backup target—SAN, NAS, direct attached storage. • Use existing infrastructure to store backups. • Eliminate purchase of expensive virtual tape library hardware. • Drastically cut backup and restore times.
Granular Recovery technology	<ul style="list-style-type: none"> • Restore individual email messages and mailboxes without brick-level backups. • Restore individual Active Directory objects. • Restore individual SharePoint documents. 	<ul style="list-style-type: none"> • Restore only the Exchange/email data you want without having to perform brick-level backups. • Quickly recover the most critical email messages, Active Directory objects, or SharePoint documents. • Store easily to a remote or removable disk drive or off a Fibre Channel or iSCSI SAN environment for fast recovery.
Continuous protection for Exchange	<ul style="list-style-type: none"> • Back up Exchange transaction logs in near real time for up-to-the-minute protection. • Back up files as they change for up-to-the-minute protection. • Back up Exchange data to disk. 	<ul style="list-style-type: none"> • Get up-to-the-minute recovery of Exchange databases. • Eliminate mailbox or brick-level backup. • Reduce storage costs by leveraging disk as a staging area.

Table 4. Disk-based backup features and benefits, <i>cont'd</i>		
Continuous protection server	<ul style="list-style-type: none"> • Reliably and effectively back up remote offices. • Reduce the backup window. Web-based restore method called Backup Exec Retrieve allows end users to restore their own files from a file server backup. • Continuously protect Exchange and SQL application servers. 	<ul style="list-style-type: none"> • Centralize data from remote offices, eliminating or reducing tape drive, media, and administrative overhead at that remote office. • Spread backup overhead throughout the day. Backups occur as files change, which can be more efficient than backing up everything at the same time. • Reduce administration and training costs.
Backup window reduction	<ul style="list-style-type: none"> • Back up critical data to fast disk devices, and then offload to tape. 	<ul style="list-style-type: none"> • Back up data to disk at night, and then transfer to tape during the day—outside of the backup window.
Fast restores	<ul style="list-style-type: none"> • Enjoy an easy-to-use, intuitive interface designed for Windows data protection. • Enable end users to restore their own files from a file server backup with Continuous Protection Server. 	<ul style="list-style-type: none"> • Reduce training and administrative costs.
Tape utilization reduction	<ul style="list-style-type: none"> • Copy less data to tape using disk-based backup methods. • Use reliable and redundant modern disks. 	<ul style="list-style-type: none"> • Reduce costs by decreasing the number of tapes used. • Keep important data on disk longer, reducing the amount of data transferred to tape.

Traditional disk-based backup methods

Backup-to-Disk folders

Backup-to-Disk folders are directories on a disk drive or disk drive array that store backup data. They are the Symantec Backup Exec version of a virtual tape library. Backups are stored on disk in the same way that a backup would be stored on a tape drive. Backup-to-Disk folders allow you to use familiar Backup Exec concepts such as backup sets, media sets, and policies to manage your backups. Using a Backup-to-Disk folder also enables an administrator to use Granular Recovery technology—an innovative disk-based protection method that allows granular restoration of file server data, Microsoft® Exchange data, Active Directory objects, and SharePoint Server documents.

Duplicate Backup Set template

Administrators can use the Duplicate Backup Set template to back up their data to disk and then copy it to tape later on—effectively implementing a multi-stage backup strategy. The template does not replace the existing Duplicate Backup Sets Option; instead, it provides an automated alternative for duplicating backup sets, allowing multiple levels of data to be duplicated either within or outside of the backup window.

Duplicate backups are useful in the following situations:

- **Staging data**—For example, data can be backed up to disk with a 28-day retention (stage 1), copied to another disk for three-month retention for longer-term storage (stage 2), and then moved to tape for offsite storage (stage 3). A policy for this staging would include a backup template to back up the data to disk for 28 days, a Duplicate Backup Set template to copy the data from the original disk to the second disk, and another Duplicate Backup Set template to copy the data from the second disk to the tape. Each of these stages may have a different media set to define the data retention period.
- **Reducing the backup window**—For example, a policy can be created containing a backup job template that uses the Backup-to-Disk option to back up data to disk during the backup window. A duplicate template can be created to copy the backed-up data from disk to tape, and the duplication job can be scheduled to occur outside of the backup window.
- **Creating a duplicate set of backup tapes to store off-site**—For example, a backup template could be created to back up data to either disk or tape, and then a duplicate template could be created that either sets the duplication job to run immediately after the first backup job is completed or schedules it to run at a specific time. If data must be restored from a duplicate backup, it can be restored from the source backup or from any of the duplicate backups.

Continuous disk-based data protection

While traditional tape- and disk-based backups have proven effective over the years, today's business climate is changing the rules. As a result, IT administrators find it increasingly difficult to back up mission-critical data within available backup windows. Continuous data protection can eliminate these backup windows.

A continuous disk-based data protection solution records file changes and makes sure that changes are captured and protected. Because it captures only granular or block-level changes, not the whole file, impact on network performance is substantially reduced. In addition, not only is the most recent data protected, but multiple versions of files are captured and thus made available for recovery. And, because disk is used as the primary medium for Windows protection and recovery, organizations can still leverage traditional tape backups to provide secondary Windows protection for longer-term retention and offsite storage.

Symantec Backup Exec now provides continuous data protection not only for Windows file servers but also for Microsoft applications such as Exchange and SQL Server. Microsoft Exchange is often the mission-critical application running in organizations today—especially Windows based organizations. IT administrators can now recover individual mailboxes and mail messages with a simple browse-and-check recovery process. In the past, a separate, time-consuming, brick-level backup job had to be run to achieve granular recovery.

The Continuous Protection Server uses a Windows feature called Volume Shadow Copy Services (VSS) to take snapshots of data at scheduled intervals. Symantec Backup Exec can back up these snapshots and the data they represent for off-site storage. Also, end users or administrators can restore file server files using a unique Web-based restore feature called Backup Exec Retrieve. Such a solution means no more complex full, incremental, or differential backups of business-critical data.

Disk as the primary backup target

Disk can be significantly cheaper and less complex than equivalent tape drives or libraries. And with the arrival of fast SATA disk drives and disk arrays as well as iSCSI and Serial Attach SCSI (SAS) interfaces, disk is now a viable alternative for cost-effective short-term and midterm data storage. Using disk as the primary backup target has many advantages. The random access nature of disk allows multiple jobs to run at the same time. The Backup Exec Backup-to-Disk feature allows you to create a virtual tape library that enables up to 16 concurrent backup or restore jobs

to run simultaneously. And with Continuous Protection Server, as many as 40 source servers can back up data at the same time. Having several backups running at the same time to the same device—also called multi-streaming—allows you to use existing hardware or share disk space with existing applications. This use of disk can lead to faster backups and restores and can even exceed the data transfer rate of some of the most expensive tape drives.

Advanced disk-based backup options

Symantec Backup Exec provides several advanced features for file servers that are used with disk-based backups (with or without Continuous Protection Server)—including Synthetic Backup, True Image Restore, and Off-Host Backup.

Synthetic Backup

Synthetic Backup uses a policy to enable a full backup to be assembled or synthesized from a baseline, and then subsequent incremental backups are made that are also contained in a policy.

The benefits of using Synthetic Backup include the following:

- The solution requires a smaller backup window, because the backup can be scheduled outside the time-critical backup window.
- Network traffic is reduced, because the backup does not need access to the network (catalog-driven, clientless backup that doesn't access the agent file system).
- Fewer problems occur when performing a restore—select the latest incremental backup job for restore, and Backup Exec does the rest.

True Image Restore

True Image Restore enables Symantec Backup Exec to restore the contents of directories to their state at the time of any full or incremental backup. Restore selections are made from a view of the directories as they existed at the time of the particular backup. Files that were deleted before the time of the backup are not restored. With True Image Restore, only the correct versions of files are restored from the appropriate full or incremental backups that contain them. Previous versions are not unnecessarily restored and then overwritten.

With True Image Restore:

- Backup sets are processed one by one, backwards, starting from the selected set. When all objects of this backup set are restored, the next prior backup set is processed, and so on, until the prior full backup is reached.
- True image information in catalogs is used to determine the files and directories to restore, and where their backup copies reside.
- Catalogs of prior backups up to the prior full backup must be present.
- Only the latest version of every file or directory is restored.
- Deleted files are not restored.
- Renamed and moved files are restored at their new locations.
- The selected volume or directories are restored so that they contain files that were present at the time of the selected backup.

Off-Host Backup

Off-Host Backup enables the backup operation to be processed on a Symantec Backup Exec media server instead of on the remote or host computer. Moving the backup from the remote computer to a media server enables better backup performance and frees up the remote computer.

Companies that use storage area networks (SANs) can benefit from using this feature in the following ways:

- The burden of running the backup process on target servers is eased.
- LAN traffic is eliminated, as the backup operation is performed over the SAN.

Disk-based data protection summary

Disk-based data protection with Symantec Backup Exec 12 enables faster backups and reliable granular recovery of critical business data. Whether a company is running continuous or traditional disk-based backups, Symantec Backup Exec 12 provides innovative, cost-efficient data protection for today's disk-based Windows business.

In addition, Symantec Backup Exec software's innovative technology provides the flexibility to grow and protect small offices to enterprise Windows environments, including departmental workgroups, remote office environments, and critical data on desktops and laptops. Symantec Backup Exec 12 is the gold standard in Windows data protection—providing a reliable, easy-to-manage data protection and recovery solution for companies running tape, disk, or continuous protection backups.

Summary

Symantec Backup Exec 12 for Windows Servers gives Windows based organizations a flexible, powerful solution they need to efficiently manage backups and restores across a distributed organization—across multiple servers in one office or distributed among remote offices. Now you can confidently manage the explosive data growth and avoid the pitfalls of Windows single server-based backup, all with reduced management requirements. Whether your enterprise requires centralized backup and recovery, license inventory and discovery, easy-to-configure SAN support, or efficient disk-to-disk-to-tape data protection, Symantec Backup Exec 12 provides market-leading Windows data protection and recovery to support your growing enterprise.

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

Copyright © 2007, 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds. Mac is a registered trademark of Apple, Inc. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A
09/08 10138589-2