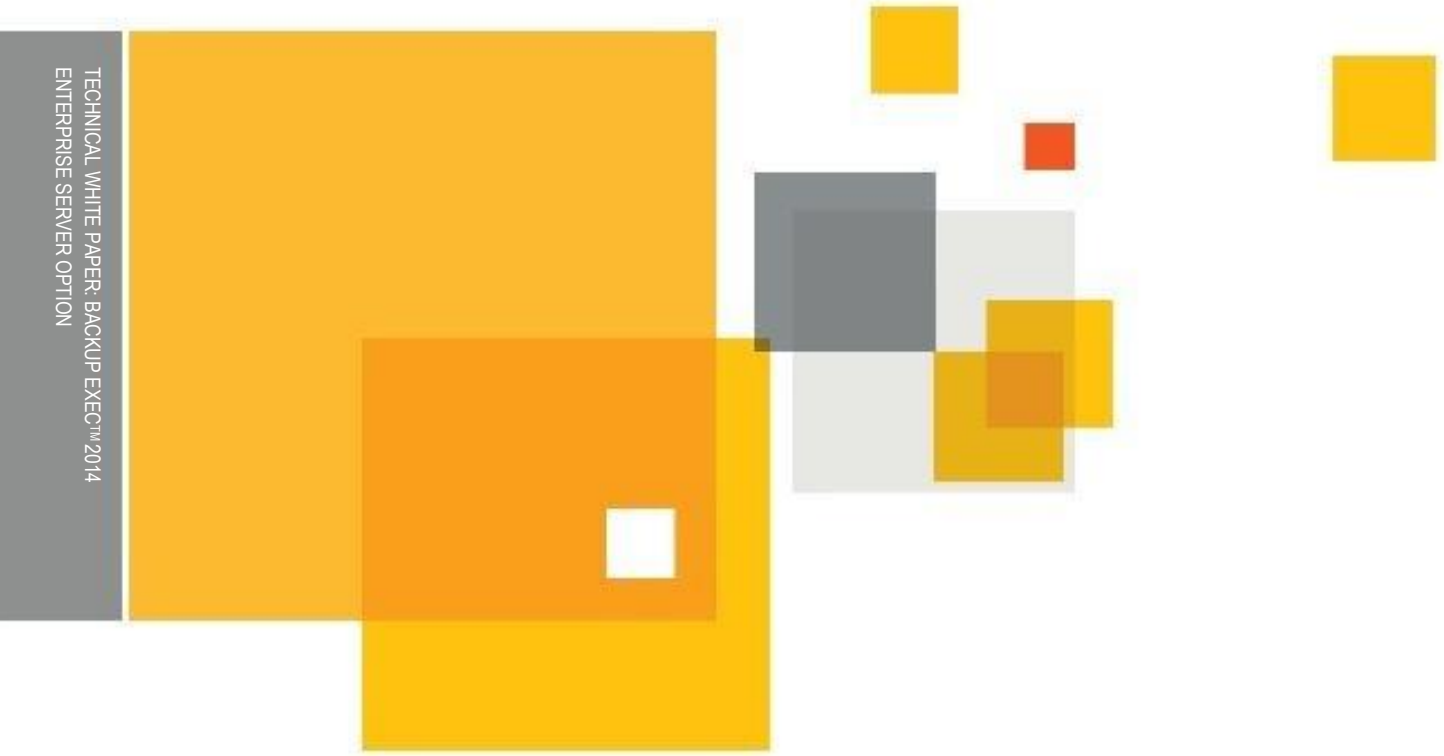

Backup Exec™ 2014 Technical White Paper

Enterprise Server Option

Who should read this paper

Technical White Papers are designed to introduce Symantec partners and end users to key technologies and technical concepts that are associated with the Symantec Backup and Recovery product family. The information within a Technical White Paper will assist partners and end users as they design and implement data protection solutions based on Symantec Backup and Recovery products.

Technical White Papers are authored and maintained by the Symantec Backup and Recovery Technical Services group.

Contents

Introduction

This white paper is intended to assist technical personnel as they design and implement Backup Exec™ 2014 and the Enterprise Server Option and make related decisions. The business value of the Enterprise Server Option will also be discussed in this white paper.

This white paper includes the following topics:

- Business Value
- Exchange Protection Methods and Technology
- Backup Exec and Exchange High Availability Configurations
- Exchange Recovery Methods and Technology
- Managing Backup Exec Rights and Permissions in Exchange Environments
- Example Backup Exec Configurations for Protecting Exchange
- Exchange Protection Notes and Best Practices
- Additional Resources

Note: For step-by-step instructions on installing, configuring, and managing the Agent for Applications and Databases, refer to the Backup Exec™ 2014 Administrator's Guide available here: TECH205797.

Business Value

Managing Backup Operations in Large or Distributed Environments

As a result of the natural growth process companies experience over time, IT environments may experience changes that can increase the difficulty of achieving a successful data protection strategy. Some of these changes may include the following:

↑	Increase in the number of critical data and application servers that need to be protected
↑	Increase in the amount of data in the environment
↑	Increase in the number and complexity of backup servers and associated storage devices
↑	Additional company sites or locations

Without the proper backup solution and associated management tools, these issues can quickly cause an increase in difficulty for administrators when it comes to ensuring critical business data is properly protected against disaster.

The Backup Exec™ 2014 Enterprise Server Option is designed to help IT administrators and Managed Service Providers meet the backup protection needs of growing companies. The Enterprise Server Option includes tools to scale a backup infrastructure and associated management capabilities to meet the needs of a growing environment. The Enterprise Server Option includes two components, which are as follows:

1. Central Admin Server Option (CASO)
2. Advanced Disk-based Backup Option (ADBO)

CASO and ADBO are optional components that can be leveraged to expand and scale the capabilities of a Backup Exec™ 2014 environment.

Central Administration Server Option

The first component of the Backup Exec™ 2014 Enterprise Server Option is the Central Admin Server Option (CASO). CASO can help address a number of key problems associated with large or growing environments, including centralized management and monitoring of backup servers, load balancing of backup operations, centralization of backup data, and offsite disaster recovery.

Centralized Management and Monitoring

One of the most important capabilities that CASO enables for administrators is the ability to centrally manage and monitor backup and recovery operations across multiple Backup Exec servers in an environment. This includes protection policy configuration and deployment, backup server management, storage device management, reporting, as well as the ability to monitor the status of protected servers and associated active alerts.

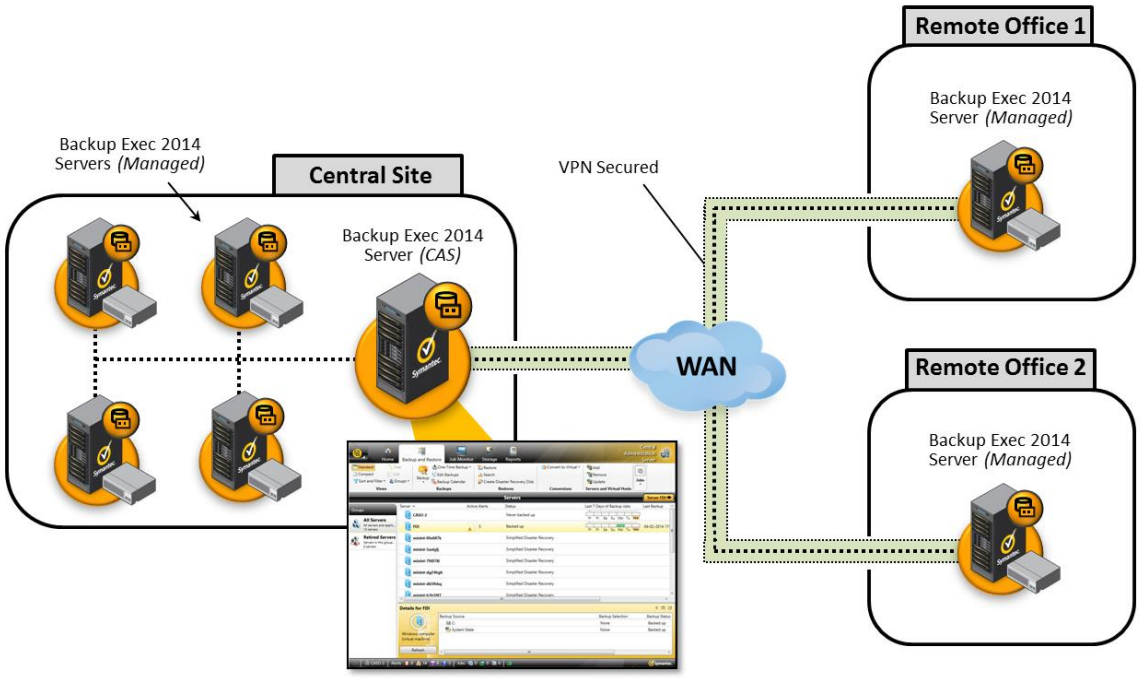

Figure 1: Centrally Managed Backup Exec™ 2014 Environment Diagram

By enabling centralized management and monitoring of multiple Backup Exec™ 2014 servers in a large or distributed environment, CASO allows administrators to centralize operations across an infrastructure, simplifying management and monitoring operations and lowering TCO.

Load Balancing of Backup Operations

CASO also allows administrators to eliminate backup task processing bottlenecks in an environment through the use of backup server pools and storage device pools. If one backup server or storage device is unavailable, the backup task can be processed by another server or storage device in the defined pool.

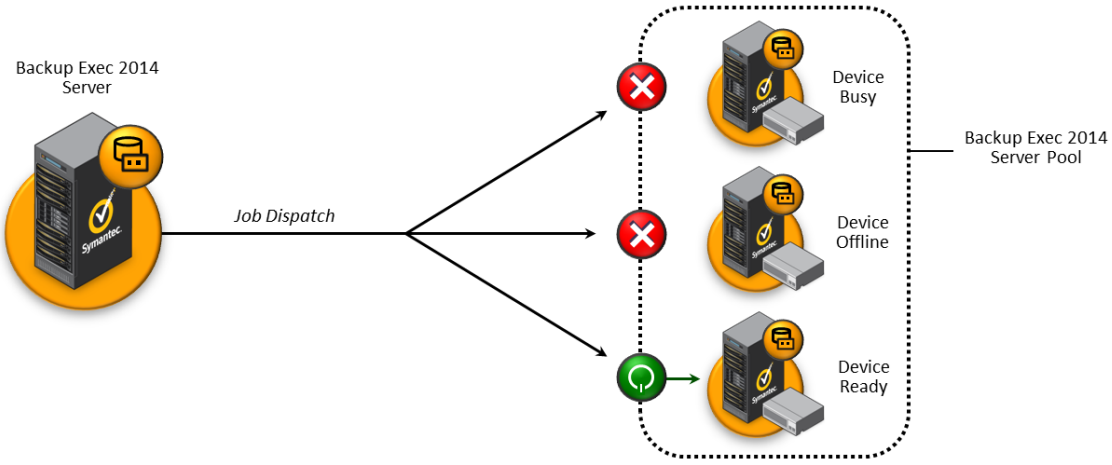

Figure 2: Load Balancing Diagram

The load balancing capabilities offered by CASO enable administrators to meet their assigned backup windows through the bypassing of bottlenecks in the environment.

Centralization of Backup Data

Successful and automated backup and recovery operations at remote sites can be a difficult goal for administrators to achieve. Administrators need the ability to protect critical IT resources at remote office locations and store copies of backup data offsite, but often lack sufficient manpower at remote offices to handle the management of removable media storage devices commonly used for backup, such as tape.

CASO allows administrators to leverage a technology known as optimized duplication to both back up critical IT resources at remote office locations and transfer copies of backup data to a central location, all without the need of staffing media management personnel at the remote office. Optimized duplication allows backup data to be copied from one backup server to another in deduplicated form, greatly reducing the amount of data copied from one site to another. Optimized duplication works by only sending deduplicated data blocks that are not already contained at the destination server.

Note: In order to leverage optimized duplication, deduplication disk storage devices must be present on the Backup Exec server located at the remote office as well as the Backup Exec server located at the central site.

After backup data has been transferred from Backup Exec servers at remote office locations to a centralized Backup Exec server using optimized duplication, administrators have the option to also copy the backup data to a tape storage device located at the central site, enabling advanced disk-to-disk-to-tape (D2D2T) scenarios.

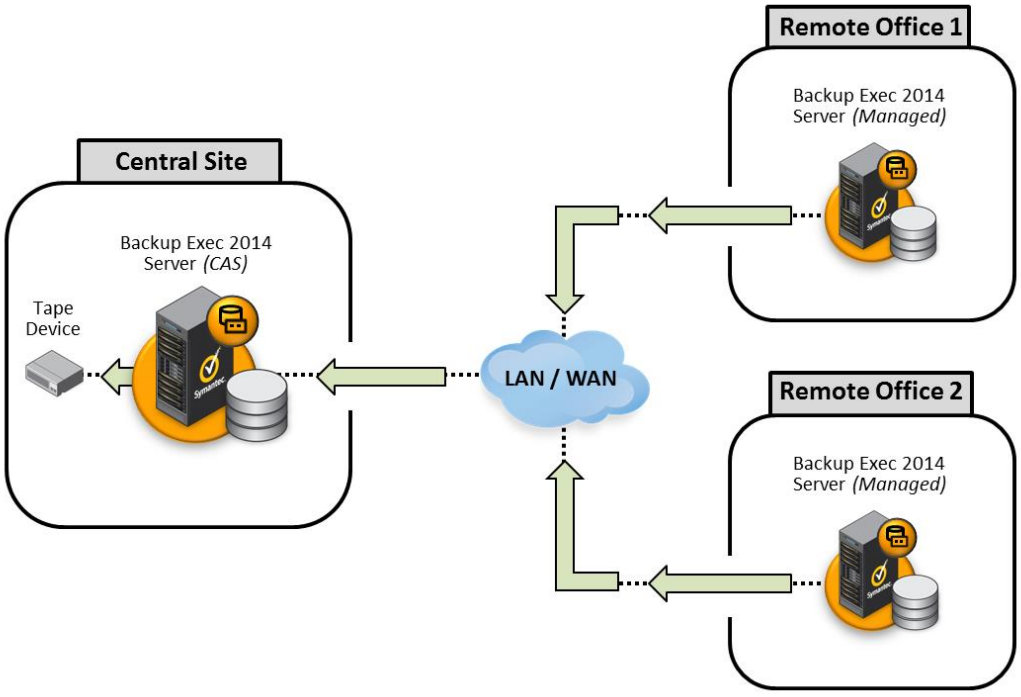

Figure 3: Centralizing Backup Data to a Central Data Center Diagram

The data transfer process is optimized by data deduplication, which transfers only unique blocks from one server to another. This greatly reduces the time and bandwidth required to perform the transfer.

A new feature known as Private Cloud Services is designed specifically for Managed Service Providers and administrators of distributed networks who want to use Backup Exec servers in remote offices for local backups, and then copy the backup sets to a Backup Exec server that is located in a remote data center.

Offsite Disaster Recovery

Additionally, CASO enables IT administrators to implement offsite disaster recovery protection for their environment. Also, through the use of optimized duplication, administrators can efficiently replicate backup data to a sister site or DR site, allowing them to protect against site-level disasters.

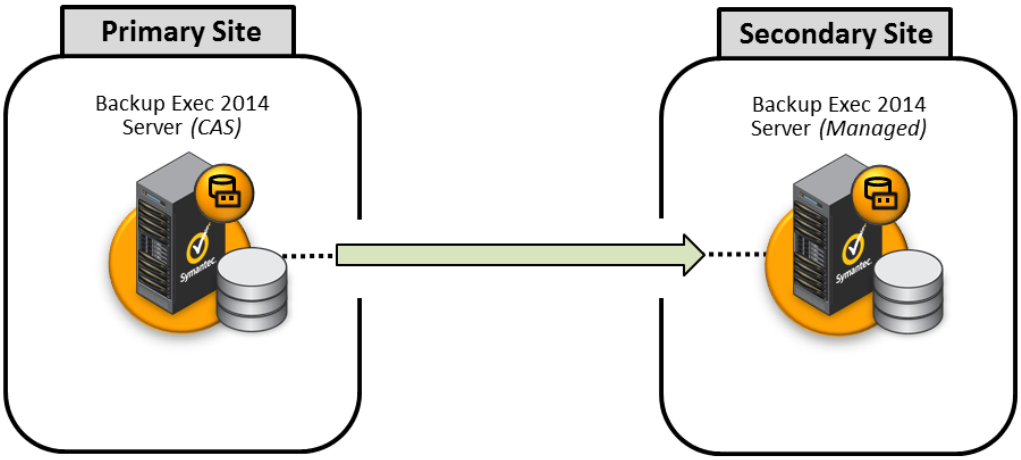

Figure 4: Basic Optimized Duplication Diagram

The data transfer process is optimized by copying only deduplicated, or unique, blocks from one server to another, greatly reducing the time and bandwidth required to perform the transfer.

Key features in Backup Exec™ 2014 enhance the offsite disaster recovery capabilities of Managed Service Providers and IT administrators for standalone physical servers. These features include:

- **Bare Metal and Dissimilar Hardware Recovery** – Easily and quickly recover backups to bare metal, either to similar or dissimilar hardware configurations.
- **Automated and Ad Hoc Virtual Conversions** – Leverage VMware or Hyper-V resources to create virtual replicas of standalone physical servers, on an automated or ad hoc basis.

When these capabilities are combined with the optimized duplication scenarios described above, Managed Service Providers and IT administrators can add additional disaster recovery services for protected standalone physical servers either at remote sites or at a central data center, such as the ability to periodically perform test recoveries of protected physical servers to dissimilar hardware or virtual machine replicas, or perform actual recovery processes if protected physical servers experience a disaster.

Advanced Disk-based Backup Option

The second component of the Backup Exec™ 2014 Enterprise Server Option is the Advanced Disk-based Backup Option (ADBO). ADBO enables advanced backup processes associated with using disk storage devices, including the following:

- **Synthetic Backups** – A Synthetic Backup is a full backup manufactured by the Backup Exec server and assembled on disk storage without performing an actual full backup operation of the original protected

resource. The synthetic full backup is "synthesized" using previous full and incremental backups that were already captured.

- **True Image Restore** – A True Image Restore operation recovers the latest and correct versions of files and directories precisely as they existed at a certain point in time.
- **Off-host Backups** – The Off-host Backup feature allows the bulk of the processing resources required to perform a backup operation to be spent at the Backup Server, alleviating the burden from the server that is being protected.

ADBO is an optional component of Backup Exec that expands the capabilities of Backup Exec™ 2014 in a specific infrastructure.

Symantec Backup Exec

Symantec Backup Exec™ delivers powerful, flexible, and easy-to-use backup and recovery to protect your entire infrastructure, whether built upon virtual, physical, or a combination of both. Using modern technology, Backup Exec backs up local or remote data to virtually any storage device including tape, disk and cloud. Recovery is fast and efficient. With a few simple clicks, you can quickly search and restore granular file or application objects, applications, VMs, and servers directly from backup storage. Additionally, easily protect more data while reducing storage costs through integrated deduplication and archiving technology.

- **Powerful**: Super charge the performance of your backup with Backup Exec. Get fast and reliable backups that are up to 100% faster than prior releases, comprehensive and innovative virtualization capabilities, and powerful built-in data deduplication and archiving. Avoid lengthy downtime and missing a critical backup window with Backup Exec.
- **Flexible**: Not all backup solutions have the flexibility to protect your environment while also supporting agile recovery. You should be able to recover what you need, when you need it - quickly and easily. Whether you want to recover a single, critical file or an entire server, Backup Exec can quickly search and restore without mounting or staging multiple backup jobs. Backup Exec protects hybrid architectures with a single solution that backs up to virtually any storage device and achieves fast, efficient, versatile recovery.
- **Easy to use**: Traditional, complex and point backup and recovery solutions can be inefficient, time consuming, and expensive to manage. Through intuitive wizards and insightful dashboards, Backup Exec is easy to implement, use and manage, whether you're upgrading from a previous version or switching from an alternative solution.

Central Admin Server Option

The Central Admin Server Option (CASO) is an optional expansion component of Backup Exec™ 2014. CASO enables a Backup Exec™ 2014 server to be promoted to the role of central administration server, enabling it to monitor and manage backup operations across multiple Backup Exec servers in an environment. This includes the following capabilities:

Central Admin Server Option Features	
Central monitoring and management of multiple Backup Exec servers	✓
Storage device management	✓
Storage device sharing	✓
Duplication of data from one backup server to another	✓
Centralized protection policy management	✓
Backup load balancing	✓
Reports	✓

Central Administration Server

A central administration server is a Backup Exec server to which CASO has been installed. The central administration server includes additional management features and capabilities that are not found on a standard Backup Exec server. A central administration server can bring existing Backup Exec™ 2014 servers under management or deploy new managed Backup Exec servers.

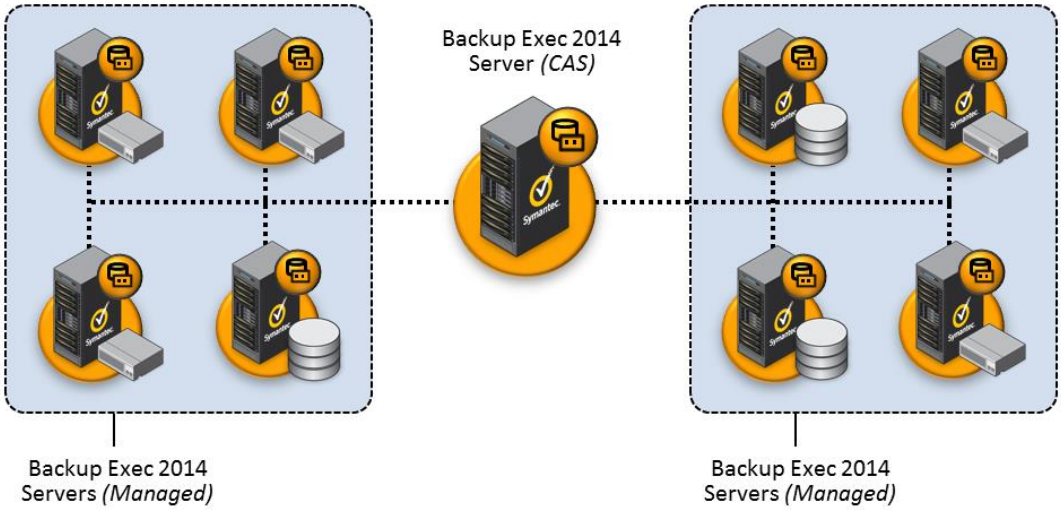

Figure 5: Central Administration Server Diagram

After a Backup Exec server is managed by a central administration server, whether by adoption or deployment, it becomes known as a managed Backup Exec server.

Monitoring and Management of Backup Exec Servers

Centralization of Information

One of the most important capabilities offered by a central administration server is the centralization of information. This allows administrators to monitor the status of managed Backup Exec servers in their

environment, as well as the servers they are protecting, from the central administration server console. This allows administrators to ensure that the servers themselves and the storage devices they control are online and operational, and that the servers being backed up are properly protected.

Active Alerts

The active alert system enables administrators to quickly identify and drill down to any problems that may exist in the Backup Exec environment they are managing, allowing them to focus their time on high-priority tasks and resolve problems in an environment quickly.

The central administration server also allows an administrator to monitor the protection status of the critical file and application servers being backed up by all of the managed Backup Exec servers that are controlled by the central administration server. This includes information about the type of server being protected (virtual, physical, Windows, Linux, etc) and its protection status, as well as the ability for administrators to drill-down to the protected server itself to view information or resolve problems.

Server Grouping

Another key feature of the central administration server is the ability for administrators to logically group servers in a central administration server environment. This allows administrators of large Backup Exec environments to quickly view specific groups of servers by any attribute they desire, such as server type, server role, server location, etc.

Backup Exec™ 2014 also supports the ability to sort the servers shown in the interface by any of the available columns, further enhancing the administrator's ability to easily identify and view the servers they are looking for.

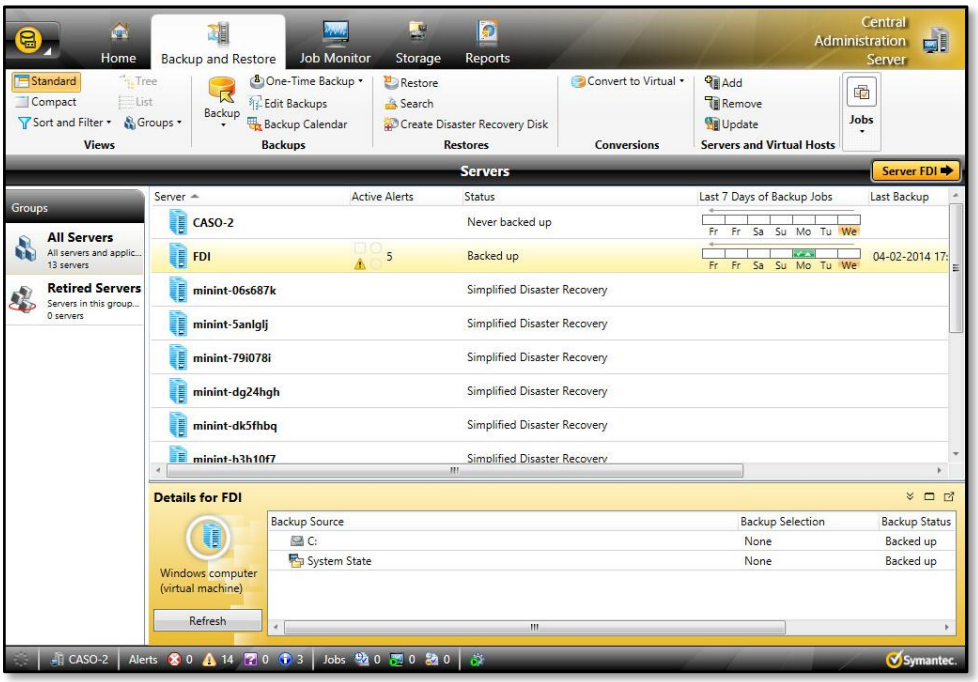

Figure 6: Central Administration Server User Interface

Compliance and Auditing

Administrators can also centrally view backup history information from the central administration server console, which can greatly assist with the problem of meeting compliance and audit requirements associated with data protection and recovery.

Managed Backup Exec Servers

When a Backup Exec server is centrally managed by a central administration server, it becomes a managed Backup Exec server.

A managed Backup Exec server will have access to one or more storage devices that are attached to the managed Backup Exec server locally, accessible by the managed Backup Exec server through the network or SAN infrastructure, or available as a shared storage device from another managed Backup Exec server or central administration server. A managed Backup Exec server can exist in a number of flexible configurations to meet the specific needs of an environment, such as whether to host device and media information locally or to allow device and media information to be centrally managed at the central administration server level.

Depending on its configuration, a managed Backup Exec server will process backup and restore tasks that have been dispatched to it by a central administration server. From the central administration server console, managed Backup Exec servers can be configured in server pools for load balancing and bottleneck avoidance purposes.

Environment Security

Communication Security and Encryption

In Backup Exec™ 2014, all communication between servers is encrypted using TSL/SSL encryption technology, and requires a trust relationships to be established. This includes communication between the central administration server and managed Backup Exec servers, communication between the central administration server and protected servers, as well as communication between managed Backup Exec servers and protected servers.

Encrypted communications in a central administration server environment ensure that backup data and related information remain secure and protected from unauthorized access.

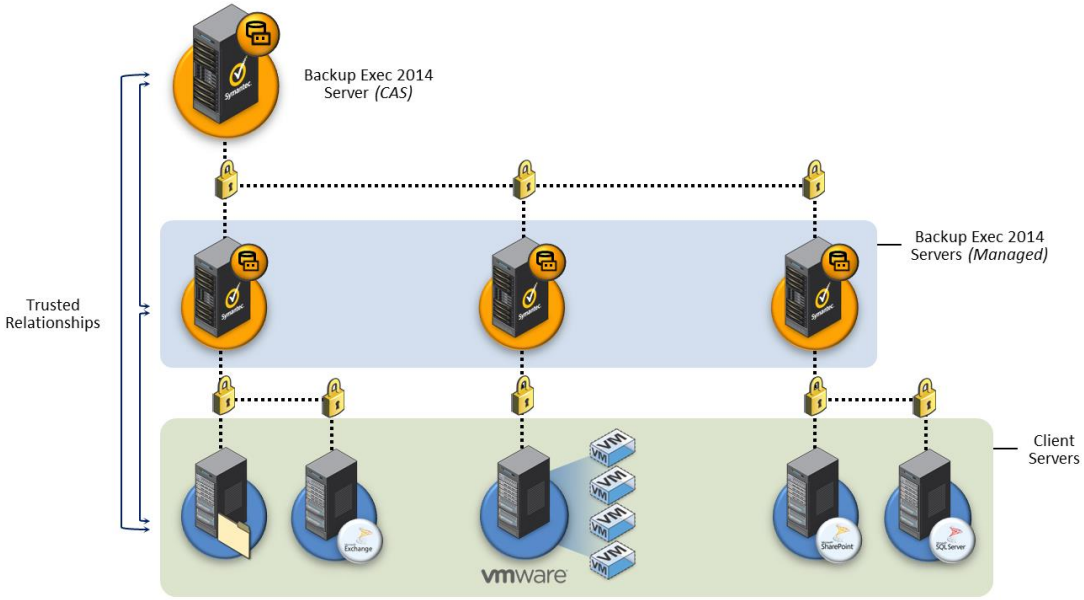

Figure 7: Communication Security Diagram

Hyper-V Host Considerations

Backup Exec interacts with Hyper-V hosts through the Agent for Windows, which is installed to the Hyper-V host itself. The same trust relationships exist between the Agent for Windows on the Hyper-V host and the Backup Exec servers with which it is associated (managed Backup Exec server/central administration server).

VMware Host Considerations

Backup Exec interacts with VMware hosts through VMware APIs designed specifically to enable backup and recovery of a VMware environment. To ensure that communications between Backup Exec servers and VMware hosts remain secure, it is recommended that SSL be enabled on the VMware hosts.

Configuring Device and Media Information

An important and configurable element of managed Backup Exec servers in a central administration server environment is whether device and media information will be managed locally by the managed Backup Exec server or managed centrally by the central administration server.

Device and media information relates to the management of storage devices owned by a managed Backup Exec server. The decision on whether device and media information will be managed locally by the managed Backup Exec server or centrally by the central administration server will impact several important factors, such as how much bandwidth will be required between the central administration server and the managed Backup Exec server, whether the network connection between the central administration server and the managed Backup Exec server needs to be persistent and have low latency, and whether backup and restore tasks can be centrally dispatched to the managed Backup Exec server from the central administration server.

Device and Media Information Locally Managed by the Managed Backup Exec Server

Having a managed Backup Exec server manage device and media information locally is optimal for configurations where the connection between the central administration server and the managed Backup Exec server is not optimal. This could include low bandwidth, high latency, or non-persistent connections. Although backup and restore tasks cannot be dispatched centrally from the central administration server to a managed Backup Exec server that is managing device and media information locally, the central administration server can still monitor the managed Backup Exec server for status and task results, and perform some tasks such as executing backup tasks. In this configuration, some backup operations for the managed Backup Exec server must be managed by a local administrator at the remote site.

Device and Media Local to the Managed Backup Exec Server	
Persistent network connection required	-
Low latency connection required	-
Storage devices centrally managed by the central administration server	-
Managed Backup Exec server can be centrally monitored from the central administration server	✓
Backup tasks can be dispatched centrally from the central administration server	-
Backup tasks can be configured locally on the managed Backup Exec server	✓

Device and Media Information Centrally Managed by the Central Administration Server

Centralizing device and media information on the central administration server is optimal for managed Backup Exec servers located close to the central administration server, such as the same site. This ensures that a constant, low latency network connection will always be available and connection problems will not be an issue.

It's important to note that centralizing device and media information on the central administration server is required in order to enable optimized duplication between Backup Exec servers and appliances. Centralized device and media information – sometimes referred to as centralized ADAMM – is required to enable storage device sharing, which in turn is required for optimized duplication.

Having device and media information managed centrally by the central administration server allows the central administration server to centrally create and dispatch tasks to the managed Backup Exec server, but requires a persistent, low latency connection.

Device and Media Centralized on the Central Administration Server	
Persistent network connection required	✓
Low latency connection required	✓
Storage devices centrally managed by the central administration server	✓
Managed Backup Exec server can be centrally monitored from the central administration server	✓
Backup tasks can be dispatched centrally from the central administration server	✓
Backup tasks can be configured locally on the managed Backup Exec server	✓

Device and Media Configuration Flexibility

Different device and media configurations can be used with different managed Backup Exec servers in the same central administration server environment. For example, a central administration server is managing a mixed topological environment that includes:

- Several Backup Exec servers in a central data center that would benefit most from centralized device and media management.
- Several managed Backup Exec servers at remote sites that would benefit most from local device and media management.

In this example, the administrator could use both device and media management configurations. A single central administration server could centrally manage device and media information for the managed Backup Exec servers in the central data center, while allowing device and media information to be managed locally by the managed Backup Exec servers at the remote sites.

Load Balancing

The load balancing capabilities of the central administration server help administrators avoid storage device and server bottlenecks that could prevent backup processes from finishing within targeted backup windows. These load balancing capabilities include the creation and management of pools, such as backup server pools and storage device pools.

Backup Server Pools

A key load balancing feature of CASO is the ability to group one or more managed Backup Exec servers into backup server pools. Managed Backup Exec servers can be a part of more than one backup server pool. When managed Backup Exec servers are configured into logical backup server pools, all of the devices and device pools on those managed Backup Exec servers become available for task delegation when a task is dispatched to the associated backup server pool. The central administration server itself can participate in backup server pools.

Backup server pools can only be used in managed environments where a central administration server is present.

Backup server pools can prevent task processing bottlenecks resulting from backup tasks waiting for a specific managed Backup Exec server to become available before they are processed. If a managed Backup Exec server is unavailable or unreachable, the backup task can be processed by other managed Backup Exec servers in the same backup server pool, allowing task processing to continue and preventing operational bottlenecks.

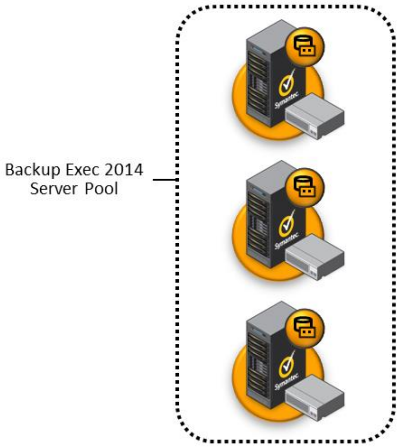

Figure 8: Server Pool Diagram

Storage Device Pools

CASO also allows administrators to group storage devices into pools. In Backup Exec™ 2014, storage devices can only participate in a pool if they are of the same storage device type. For example, disk storage devices can be pooled together and tape storage devices can be pooled together, but a pool cannot consist of both disk and tape storage devices.

Storage device pools can be configured in standalone (unmanaged) Backup Exec server configurations or in configurations where managed Backup Exec servers are managed by a central administration server. Storage device pools can consist of multiple storage devices attached to the same server or can consist of storage devices attached to different servers.

Storage device pools can prevent task processing bottlenecks resulting from backup tasks waiting for a specific storage device to become available. If a specific storage device is unavailable or offline, the backup task can be processed by another storage device in the same pool, allowing task processing to continue and preventing operational bottlenecks.

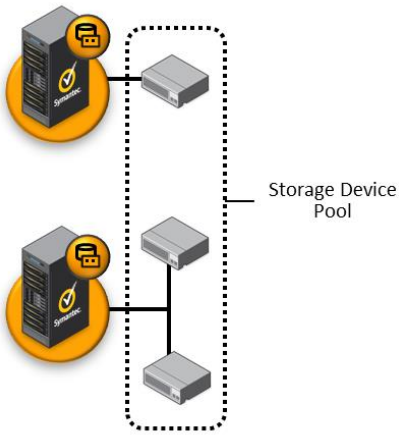

Figure 9: Storage Device Pool Diagram

Task Delegation

The central administration server enables administrators to delegate tasks to specific managed Backup Exec servers and specific storage devices, or to back up server pools and storage device pools. This capability to leverage backup server pools and storage device pools enables administrators to load balance an environment and avoid backup process bottlenecks.

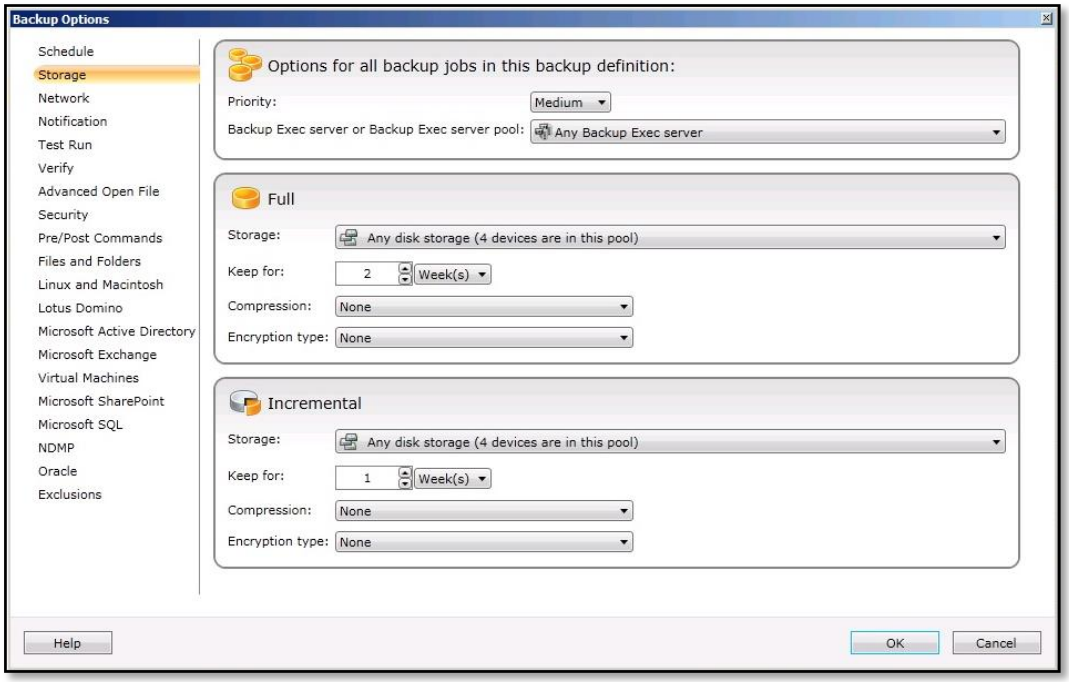

Figure 10: Protection Policy Backup Storage Options

When a central administration server is used to delegate a backup task to a backup server pool, the task – depending on priority – is assigned to a managed Backup Exec server and storage device in the backup server pool. In configurations where server pools are utilized, backup tasks are not assigned to managed Backup Exec servers in any particular order; rather, they are assigned based on a load balancing algorithm in the central administration server. If the managed Backup Exec server does not have an available storage device, or if the managed Backup Exec server is offline or unavailable, the task does not enter a paused or stalled state;

instead, other managed Backup Exec servers in the pool are considered until an available managed Backup Exec server with an available storage device is found. When an available managed Backup Exec server with an available storage device is found, the task is delegated to that managed Backup Exec server for processing.

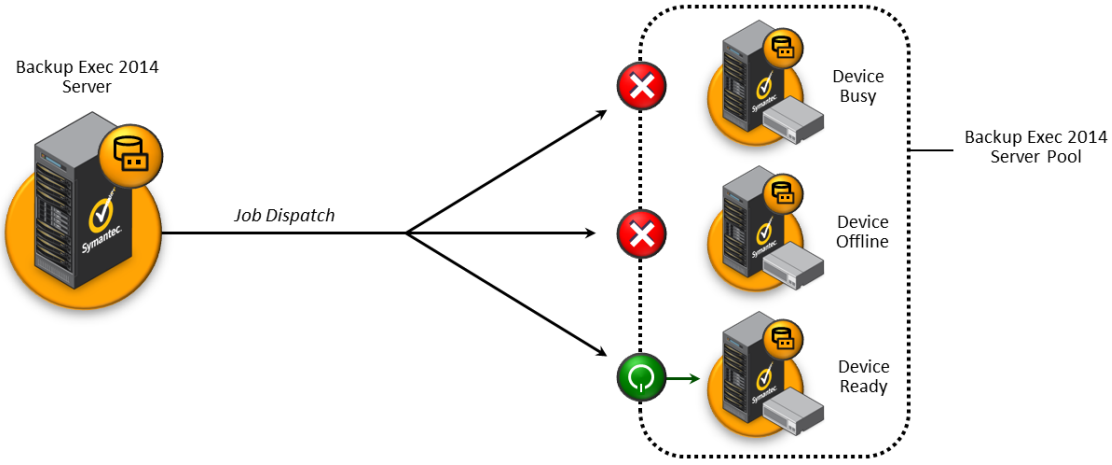

Figure 11: Load Balancing Diagram

An environment with multiple backup servers located in a central data center is an example of where the load balancing capabilities of CASO would benefit an administrator.

Remote Site Considerations

Remote sites with smaller backup infrastructures, such as a single backup server with a single storage device, may be better served by other remote management strategies, such as the following:

- **Direct Targeting of a Remote Managed Backup Exec Server** - Assigning backup tasks for the remote site directly to the backup server and associated storage device located at that site (prevents transmission of large amounts of backup data from servers at the remote site to storage devices located at the central site).
- **Device and Media Information Managed by a Remote Managed Backup Exec Server** - Configuring device and media information to be managed locally by the backup server at the remote site and having a local administrator manage backup operations using the local backup server console (preferred configuration for low bandwidth connections or unstable connections between remote managed Backup Exec servers and the central administration server).

Regardless of the configuration and backup strategy, it is possible to enable the central administration server to monitor and report against backup operations in the environment, and to perform some task management operations, such as pausing or cancelling a backup task.

Sharing Storage Devices in a Central Administration Server Environment

Storage devices can be shared between Backup Exec servers. The central administration server can manage SAN storage devices, devices that are attached to the central administration server, and devices that are attached to managed Backup Exec servers. Depending upon the device and media configuration for the different managed Backup Exec servers managed by the central administration server, the central administration server may be able to see and manage all storage devices in the environment.

Sharing storage devices in a central administration server environment allows multiple Backup Exec servers to utilize the same storage device resource without allowing one backup process to overwrite the data stored by

another backup process. In order to share a storage device, the managed Backup Exec server must be configured to use shared device and media management.

Sharing Disk Storage Devices

Disk storage devices are general disk storage devices that can be defined on any local or network-accessible disk storage device. Disk storage devices do not employ data deduplication, but backups stored to a disk storage device can be compressed using the software compression capabilities of Backup Exec™ 2014.

When sharing a disk storage device owned by one managed Backup Exec server to other managed Backup Exec servers, the other managed Backup Exec servers to which the disk storage device has been shared access the disk storage device through the network interface using the folder's UNC path. When configuring a shared disk storage device, the administrator must provide the folder's UNC path.

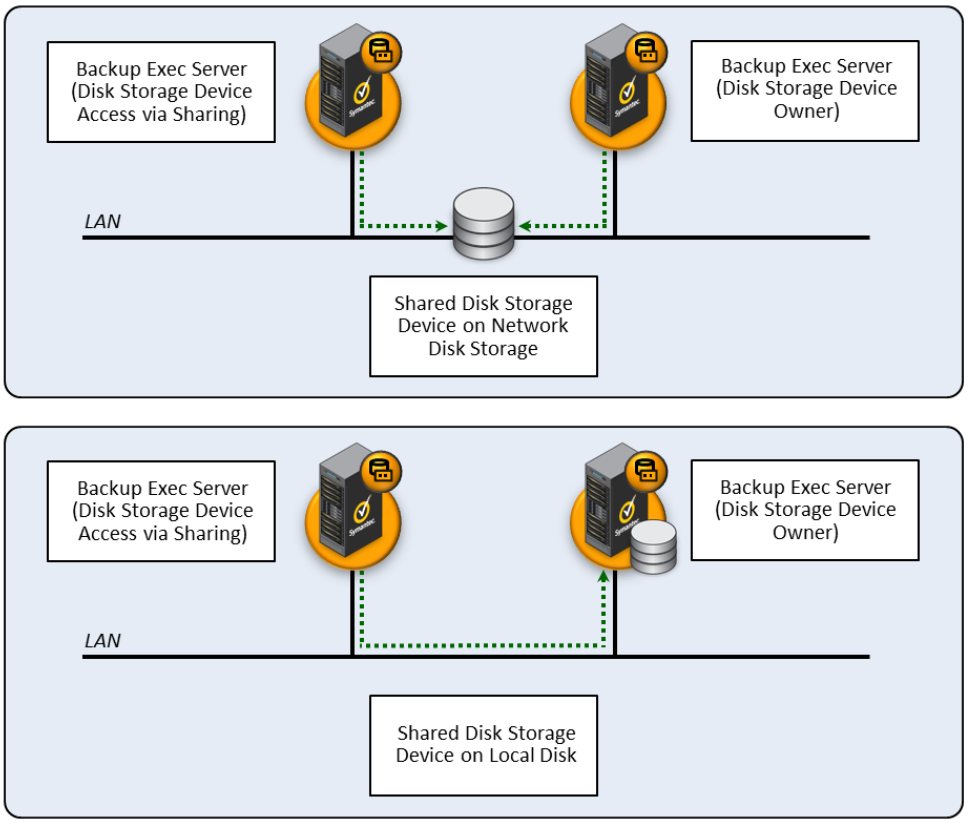

Figure 12: Sharing Disk Storage Devices in a LAN Diagram

Catalog data for backup sets stored to a shared disk storage device will be saved either to the managed Backup Exec server storing the backup set to the disk storage device, the central administration server, or both. Where catalog data is stored depends on the catalog configuration for the central administration server-administered environment.

Sharing Deduplication Disk Storage

Deduplication disk storage devices are disk storage devices that are enabled for deduplication. Deduplication disk storage can only reside on disk storage devices that appear local to the Backup Exec server, such as local disk volumes or SAN LUNs presented to the Backup Exec server. A Backup Exec server can own only a single deduplication disk storage device.

Deduplication disk storage devices can be shared between managed Backup Exec servers in a central administration server environment. Unlike disk storage devices, deduplication disk storage devices are considered to be OpenStorage (OST) devices, and as such they are accessed by Backup Exec servers through the OST protocol.

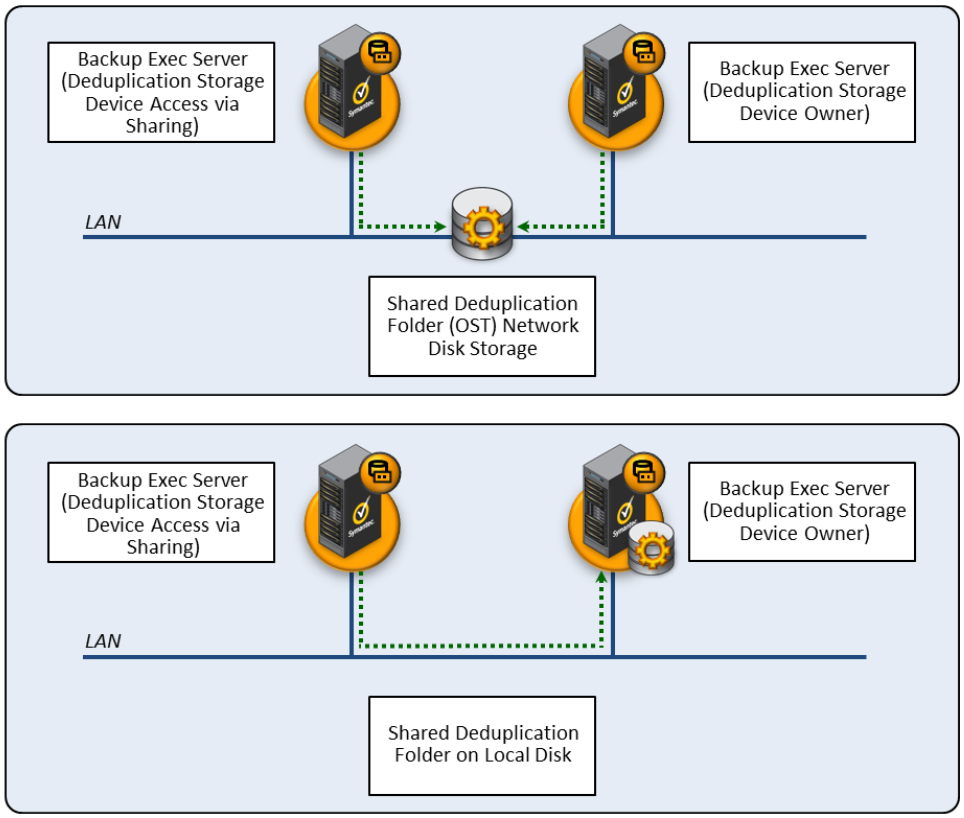

Figure 13: Sharing Deduplication Disk Storage in a LAN

Catalog data for backup sets stored to a shared disk storage device will be saved to the managed Backup Exec server storing the backup set to the disk storage device, the central administration server, or both. Where catalog data is stored depends on the catalog configuration for the central administration server-administered environment.

Sharing Storage Devices in a SAN

Sharing Disk Storage Devices on SAN Disk Storage

It is possible to share a disk storage device that is owned by one managed Backup Exec server and located on SAN disk storage with other managed Backup Exec servers in a central administration server environment.

In such a configuration, the SAN-connected managed Backup Exec server that owns the disk storage device will be able to store backup sets to that disk storage device over the SAN data path. However, because shared disk storage devices are accessed by other managed Backup Exec servers through the folder's UNC path, other managed Backup Exec servers will store data to that shared disk storage device through the network interface.

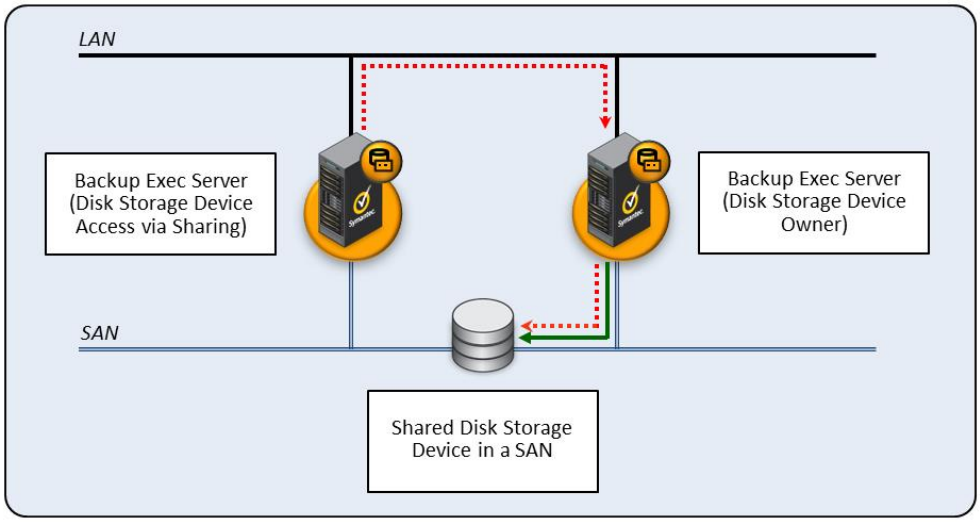

Figure 14: Sharing Disk Storage Devices in a SAN Diagram

Managed Backup Exec servers accessing a disk storage device on SAN storage that has been shared to them from another managed Backup Exec server will send data to that disk storage device over the network interface (LAN) using the folder's UNC path.

Catalog data for backup sets stored to a shared disk storage device will be saved to the managed Backup Exec server that owns the disk storage device, the managed Backup Exec server storing the backup set to the disk storage device, the central administration server, or some combination of these. Where catalog data is stored depends on the catalog configuration for the central administration server-administered environment.

Sharing Deduplication Disk Storage on SAN Disk Storage

It is possible to share a deduplication disk storage device, owned by one managed Backup Exec server and located on SAN disk storage, with other managed Backup Exec servers in a central administration server environment.

In such a configuration, the SAN-connected managed Backup Exec server that owns the deduplication disk storage device will store backup sets to the deduplication disk storage device through the OST interface and also over the SAN data path. Other managed Backup Exec servers to which the deduplication disk storage device is shared will also transmit data to the deduplication disk storage device through the OST interface; however, the data will flow over the LAN and not the SAN. Because of client-side deduplication and optimized duplication, the access is optimal – only segments that the deduplication disk storage device does not already contain will be transferred.

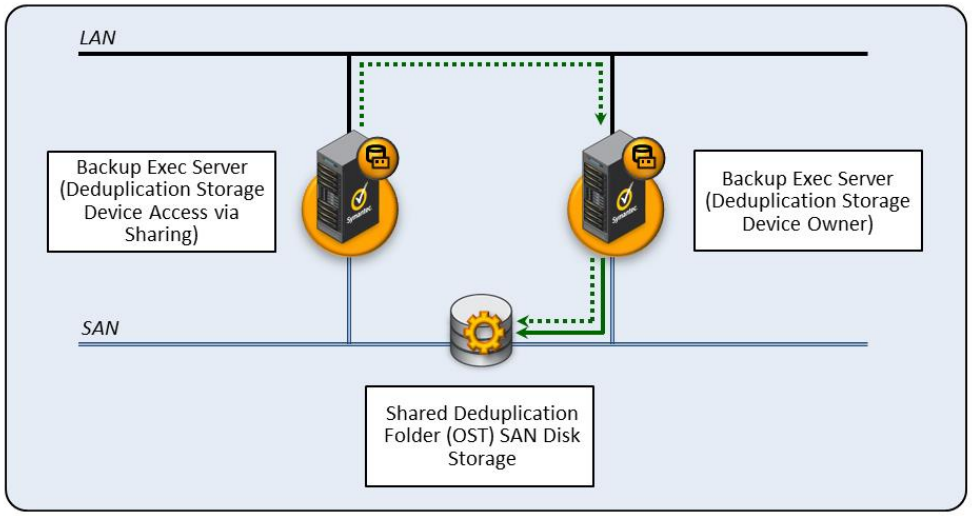

Figure 15: Sharing Deduplication Disk Storage in a SAN Diagram

The necessary OST plug-in for writing data to deduplication disk storage devices is built into the Backup Exec™ 2014 product.

Catalog data for backup sets stored to a shared disk storage device will be saved to the managed Backup Exec server storing the backup set to the disk storage device, the central administration server, or both. Where catalog data is stored depends on the catalog configuration for the central administration server-administered environment.

Sharing Robotic Tape Libraries in a SAN

SAN-connected robotic tape libraries can be shared between multiple managed Backup Exec servers. In this configuration, each managed Backup Exec server that requires access to the SAN-connected robotic tape library will also need to be connected to the SAN.

Optimized Duplication

Backup Exec supports optimized duplication, which enables deduplicated data to be copied directly from one OpenStorage (OST) device to another OpenStorage device from the same vendor, such as from one Backup Exec deduplication disk storage device to another Backup Exec deduplication disk storage device. Because the data is deduplicated, only unique data is copied between the devices. The optimized duplication feature can be used to copy data between Backup Exec servers or between Backup Exec and NetBackup PureDisk servers and OST-enabled Appliances.

One important problem that optimized duplication can help solve is the problem of disaster recovery (DR). Copying backup sets from one Backup Exec server to another using optimized duplication makes the same backup data available for recovery at multiple locations, such as secondary/DR sites, thereby offering a convenient disaster recovery solution.

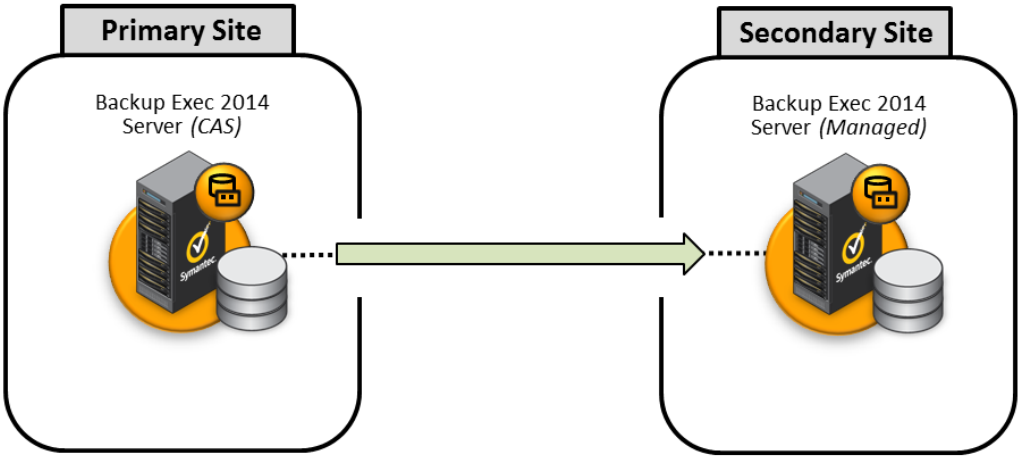

Figure 16: Basic Optimized Duplication Diagram

Catalog Management

When Backup Exec captures backup data and saves it to a storage device, catalog files that correspond to the backup set are also created and stored. These catalog files contain information used by a Backup Exec server to recover or restore the associated data when processing a restore task. Because catalog data is required in order to successfully process an associated restore task, managing and protecting catalog data is an important consideration for administrators of Backup Exec environments.

There are several configurations that can be leveraged to manage where catalog data is maintained in a central administration server-administered environment. These configurations include:

- Centralized
- Distributed
- Replicated
- Unrestricted access

Each of these catalog configuration options, along with their advantages and disadvantages, is discussed in greater detail below.

Centralized Catalog (Central Administration Server)

When using the centralized catalog configuration, all catalog data is stored centrally on the central administration server. The primary benefit of using the centralized catalog configuration is that it makes it relatively easy to back up the catalog data. However, this configuration places an increased demand on the network connection between the central administration server and managed Backup Exec servers as catalog data will be transferred between the two in order to centralize it at the central administration server location. In a centralized catalog configuration the managed Backup Exec server can only "see" its own catalogs.

A persistent connection between the central administration server and the managed Backup Exec server is required for the centralized catalog configuration.

Distributed Catalog (Managed Backup Exec Server)

When using the distributed catalog configuration, most catalog data is maintained on the local managed Backup Exec server. Some minor catalog information is still transferred to the central administration server. This configuration is optimal for distributed environments where managed Backup Exec servers have a low

bandwidth or unstable connection to the central administration server. However, protecting catalog files becomes more complex, since each managed Backup Exec server will need to have its local catalog files protected separately.

A persistent connection between the central administration server and the managed Backup Exec server is not required for the distributed catalog configuration.

Note: When device and media information is configured to be stored locally on the managed Backup Exec server, then the only catalog configuration that can be used is the distributed mode.

Replicated Catalog (Central Administration Server and Managed Backup Exec Server)

When using the replicated catalog configuration, an administrator gains both the advantages as well as the disadvantages of the centralized and distributed catalog configurations, as catalog files are maintained at the local managed Backup Exec server and are replicated to the central administration server.

The replicated catalog configuration enables centralized backup of catalog files, but is not optimal for environments where the central administration server and managed Backup Exec servers are separated by low bandwidth or unstable network connections. A persistent connection between the central administration server and the managed Backup Exec server is required for the replicated catalog configuration.

Unrestricted Access Catalog

A new and additional catalog configuration available in Backup Exec™ 2014 is the unrestricted access catalog configuration. This configuration is similar to the centralized catalog configuration in that catalog files are stored at the managed Backup Exec server and are also replicated to the central administration server.

A persistent network connection is required between the central administration server and the managed Backup Exec server in unrestricted access catalog mode. The catalogs are centralized and are stored on the central administration server. Note that this combination of options may not be suitable if you have a low-bandwidth network connection to the central administration server. This managed Backup Exec server can access and restore backup sets for all storage devices that it shares with other Backup Exec servers. The backup tasks that are created on the central administration server can be load-balanced and delegated to this managed Backup Exec server. A rolling upgrade cannot be performed with this configuration. This managed Backup Exec server must be upgraded at the same time as the central administration server.

Domain Considerations

Domain Environment Required

CASO can only be used in environments where a Windows domain is present due to its integration with the Windows Active Directory infrastructure.

Multi-domain Environments

It is possible to use CASO in network environments where more than one Windows domain is present. In such an environment, a trust relationship must exist between the two domains allowing the central administration server to interact with managed Backup Exec servers and protected servers in either domain. If this trusted configuration is not desirable, then a separate CASO environment must be configured for each domain, acting independently from one another.

Private Cloud Services

Purpose and Design

Backup Exec Private Cloud Services is a new capability of Backup Exec and CASO designed specifically for Backup Exec partners who are interested in offering managed backup services to their customers. Backup Exec Private Cloud Services works within the partner's datacenter as a "private cloud" configuration. Managed Service Providers (MSPs) can provide backups over the Internet to a private cloud as an alternative to using tape at local customer sites.

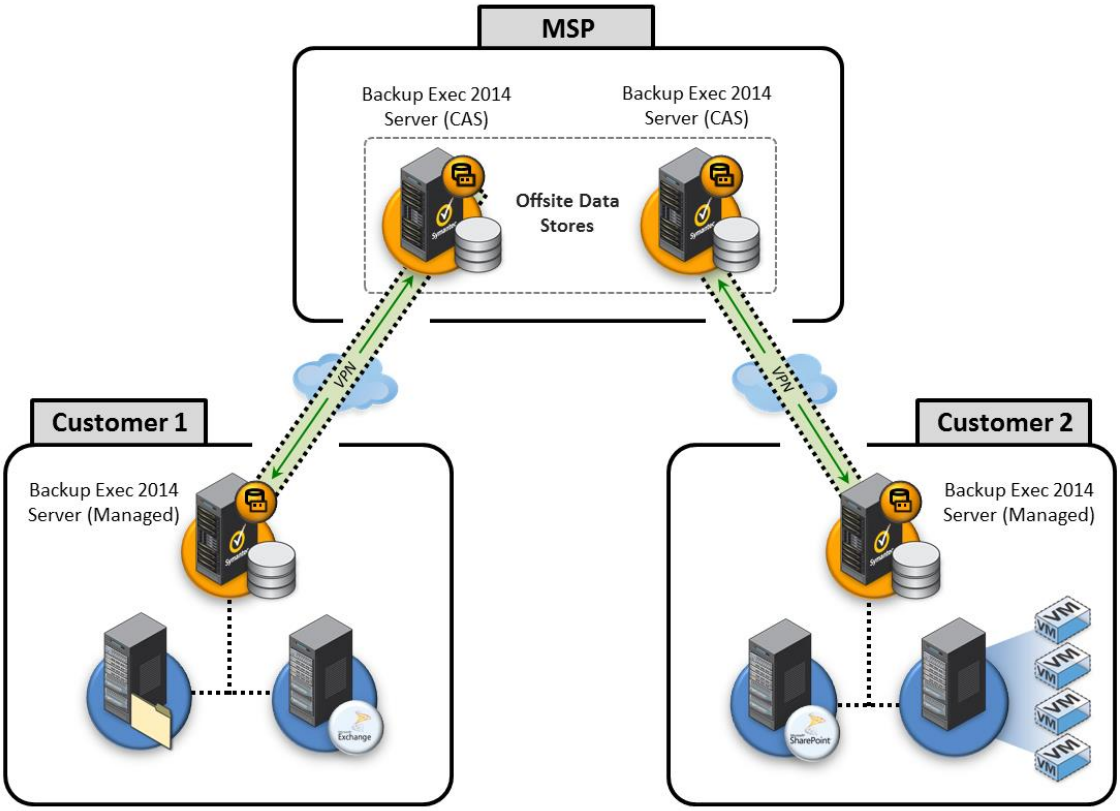

Figure 17: Private Cloud Services Diagram

Backup Exec Private Cloud Services can also be used by customers with widely distributed environments who are interested in storing backup copies from remote sites to disk and tape storage resources located within a central data center location.

Backup Data Security

Backups transmitted over the Internet in this manner are kept confidential and safe from unauthorized access. Security of backup information travelling between remote sites and a central cloud data center in a Private Cloud Services configuration is ensured using the following:

- **VPN Tunnel** – Communications between the central cloud data center and remote sites travel over a VPN tunnel. This remains true whether a managed Backup Exec server exists at the remote site or whether backup data is travelling directly from protected servers to the central cloud data center.
- **TSL/SSL Encryption** – All communications between Backup Exec components, such as central administration servers, managed Backup Exec servers, and protected servers containing a remote agent, are encrypted using TSL/SSL encryption technology and a trust relationship is established. This is also true for Hyper-V backups, as a Backup Exec agent resides on the Hyper-V host and participates in the trusted relationship process.

For environments protecting VMware virtual machines using VDAP-enabled backups, it is recommended that SSL be enabled on the VMware host.

Note: Other recommended security measures for some Private Cloud Services configurations can be found in the Private Cloud Services Planning and Deployment Guide, available here: TECH172464.

Data Transfer Optimization

Backup data transmitted over the Internet to a private cloud in this manner is optimized through deduplication, such that only unique data blocks are transferred to the central cloud data center. This reduces backup windows and optimizes storage utilization at the data center.

Variable Configuration Support

Backup Exec Private Cloud Services supports different configurations to meet the unique and varied needs of MSPs and their customers. This includes configurations that allow for a local backup server at customer sites for fast, local recovery purposes in addition to sending copies of deduplicated data to an MSP-hosted cloud data center, or configurations where backups are sent directly to the cloud, including the capability to restore full or granular information directly from the cloud.

VPN Considerations

Static VPN connections are required from the MSP-hosted cloud data center to remote customer sites in order to leverage Private Cloud Services. Most third-party VPN solutions can be used.

Multitenant Configuration Support

The Backup Exec Private Cloud Services feature allows MSPs to store backup data from multiple customer sites to a centralized, deduplication-enabled Backup Exec server located at the MSP data center, while ensuring each customer's data is protected from unauthorized access. This provides multitenant separation of customer data while maintaining the storage optimization benefits of deduplication for the cloud data center.

Note: For information about how to implement this configuration, along with security recommendations and other best practices, please refer to the Private Cloud Services Planning and Deployment Guide available here: TECH172464.

Additional Resources for Private Cloud Services

Listed below are links to additional resources to assist MSPs as they plan and implement the Backup Exec Private Cloud Services capability. These resources include a calculator that can be used to determine time requirements for backing up to a central cloud data center, as well as the Private Cloud Services Planning and Deployment Guide, which includes additional information about Private Cloud Services, alternate configurations, and step-by-step installation and configuration instructions:

- Cloud backup time calculator: TECH172473
- Planning and Deployment Guide: TECH172464

Central Administration Server Scalability

CASO can be used to centrally manage large to very large environments protected by Backup Exec™ 2014. If necessary, multiple central administration servers can be used to overcome significant or unique scalability challenges. When planning for a CASO implementation for a large or very large environment, please note the following scalability considerations:

Maximum Number of Managed Backup Exec Servers per Central Administration Server (SQL Server)

Using a full instance of SQL as the Backup Exec database on the central administration server, a single central administration server can manage up to 180 managed Backup Exec servers. Please note that this is the maximum number of managed Backup Exec servers supported by a single central administration server, not the maximum number of servers that can be backed up in such an environment (this number would be much higher). Also note that these values do not necessarily apply to optimized duplication configurations.

It's also important to note that the maximum number of managed Backup Exec servers that a single central administration server can manage will vary depending on the number of storage devices being managed by each managed Backup Exec server, the catalog configuration being used (centralized vs. distributed), and whether the managed Backup Exec servers are enabled for deduplication.

Maximum Number of Managed Backup Exec Servers per Central Administration Server (SQL Express)

Using SQL Express as the Backup Exec database on the central administration server, a single central administration server can manage up to 50 managed Backup Exec servers. Please note that this is the maximum number of managed Backup Exec servers supported by a single central administration server, not the maximum number of servers that can be backed up in such an environment (this number would be much higher).

It's also important to note that the maximum number of managed Backup Exec servers that a single central administration server can manage will vary depending on the number of storage devices being managed by each managed Backup Exec server, the catalog configuration being used (centralized vs. distributed), and whether the managed Backup Exec servers being managed are enabled for deduplication.

Maximum Number of Storage Devices per Managed Backup Exec Server

The following technical article describes the maximum number of storage devices that can be utilized by a single Backup Exec server: TECH164967.

Maximum Managed Backup Exec Servers Sharing Same Deduplication Disk Storage Device

The following technical article describes the maximum number of Backup Exec servers that can share a single deduplication disk storage device: TECH164967.

Central Administration Server to Managed Backup Exec Server Network Link Considerations

When storage devices that are attached to managed Backup Exec servers are centrally managed by a central administration server, also known as centralizing device and media information, a direct SQL connection must be maintained between the central administration server and the managed Backup Exec servers. If this connection is lost, then all backup operations for the managed Backup Exec servers will cease until the connection has been restored.

It is recommended that a "round trip" latency of no higher than 250ms be achieved between the central administration server and managed Backup Exec servers when centralizing device and media information.

When remotely managing managed Backup Exec servers over WAN connections where a "round trip" latency of 250ms or less cannot be achieved, consider alternate configurations for the managed Backup Exec server, such as locally managing device and media information and a distributed catalog configuration.

General Central Administration Server Scalability Notes

As any given customer environment may not exactly match the tables and 'upper maximum' values offered in this section, and as such some extrapolation may be required to estimate how a central administration server will scale in a particular environment. The information provided here is offered for general guidance purposes to assist in making such estimates.

Note: Additional tech notes that deal with CASO scalability can be found here: HOWTO74432, TECH60559

Central Administration Server and Backup Exec Product Editions

The following table lists the different products and editions in the Backup Exec product family and whether or not each edition can be centrally managed from a central administration server.

Backup Exec Edition	Manageable from Central Administration Server
Backup Exec 2014	✓
Backup Exec 2014 V-Ray Edition	✓
Backup Exec 2014 Capacity Edition	✓
Backup Exec 2014 Small Business Edition	-
Backup Exec 3600 Appliance	✓
Backup Exec QuickStart Edition	-

Advanced Disk-based Backup Option

The Advanced Disk-based Backup Option (ADBO) offers additional backup and recovery features that leverage disk-based storage devices. These features include synthetic backups, true image restore, and off-host backups, each of which will be explored in greater detail below.

Synthetic Backups

When the synthetic backup option is used in a protection policy, it essentially removes the need for recurring full backups to be captured from a protected server over time. Instead, only an initial full backup is captured from the protected resource, and from that point, only incremental backups are captured from the protected resource. At defined intervals, the backup server combines data from incremental backups and the previous full backup -- which could be the original full backup that was captured from the protected resource or a previous synthetic full backup – to create a synthetic full backup.

Synthetic Backup Advantages

There are several key advantages enabled through the use of synthetic backups. The advantages of leveraging synthetic full backups as part of a backup strategy are as follows:

- The burden of full backups are offloaded from the protected server to the backup server.
- Synthetic full backup scheduling flexibility – can be scheduled outside of normal backup windows.
- Lower network bandwidth consumption – only incremental backups are transmitted from the protected resource to the backup server.

Synthetic Backup Limitations

For synthetic full backups, only file system assets can be protected; no application or database resources are supported

Note: For additional information on creating and managing protection policies that leverage synthetic full backups, please refer to the Backup Exec™ 2014 Administrator's Guide available here: DOC5211.

True Image Restore

When administrators select the "Using catalog" method in the file and folder section of backup options, Backup Exec™ 2014 enables an administrator to recover a file or directory structure to the exact state in which it existed at the time of backup. This is also referred to as True image Restore. Using this technology, only the latest version of a directory structure is restored as it existed at the time of backup, and deleted files are not recovered.

True Image Restore Limitations

True Image Restore is supported for agent-based backups, or backups that are captured via a local install of the Agent for Windows. As such, True Image Restore is not supported for backups captured using the Agent for VMware and Hyper-V, which leverages host-level integration to capture image-level backups of virtual machines.

For additional information on creating and managing protection policies that leverage True Image Restore, please refer to the Backup Exec™ 2014 Administrator's Guide.

Off-host Backups

The primary benefit of using off-host backups is removing the bulk of the backup 'burden' from the server being protected and moving it to the backup server. This is done through the use of snapshot technology. Snapshots are created from volumes that are being backed up, and these snapshots are imported to the

backup server, enabling the backup server to perform the backup operation. Once the backup completes, the snapshot is released.

A number of requirements need to be in place before off-host backups can be realized. Some of these are as follows (taken from the Backup Exec™ 2014 Administrator's Guide):

Requirement Type	Requirement Description
Backup Server	• Backup Exec • Backup Exec Advanced Disk-based Backup Option
Protected Server	• Agent for Windows
Backup Server and Protected Server	• Microsoft Windows Server 2003 with Service Pack 2 or Windows Server 2008. • Most recent Volume Shadow Copy Services (VSS) patches. • The Microsoft VSS hardware or software snapshot provider that you want to use; otherwise, the snapshots of the volumes cannot be deported to the Backup Exec server. • Ability to access the disks that are shared between the Backup Exec server and the remote computer.
GRT-enabled Off-host Backup of Exchange Server Resources	Either of the following must be installed on the Exchange Server: • Microsoft Exchange Server 2003 (Service Pack 2) or Exchange Server 2007 (Service Pack 3) instances that run on Windows Server 2003 must be installed on the Exchange Server. • Microsoft Exchange Server 2010 (Service Pack 1) instances that run on 64-bit Windows Server 2008/2008 R2.
Central Admin Server Option	• If the Central Admin Server Option (CASO) is installed, do not let the central administration server delegate the job. It can delegate the job to a managed Backup Exec server that does not have off-host capability. You must manually select the storage device for the CASO jobs that use the off-host backup method.
Other	• Additional requirements are outlined in the Backup Exec™ 2014 Administrator's Guide.

A link to the list of storage devices that are compatible with the Backup Exec off-host backup feature along with some best practices are included in the Notes and Best Practices section of this document.

Note: For additional details on configuring the offhost backup feature of Backup Exec, please refer to the Backup Exec™ 2014 Administrator's Guide available here: DOC5211.

Example CASO Configurations

Environments come in all shapes and sizes, so central administration server and managed Backup Exec server configurations will vary from customer to customer. This section offers some basic configuration examples that can be used as a basic reference when designing central administration server and managed Backup Exec server configurations for specific customers.

Centralized Data Center

Leveraging CASO to manage Backup Exec operations in a central data center configuration is a very common use case. In configurations such as these, using a centralized or unrestricted access catalog configuration and having the central administration server manage all device and media information for an environment is recommended.

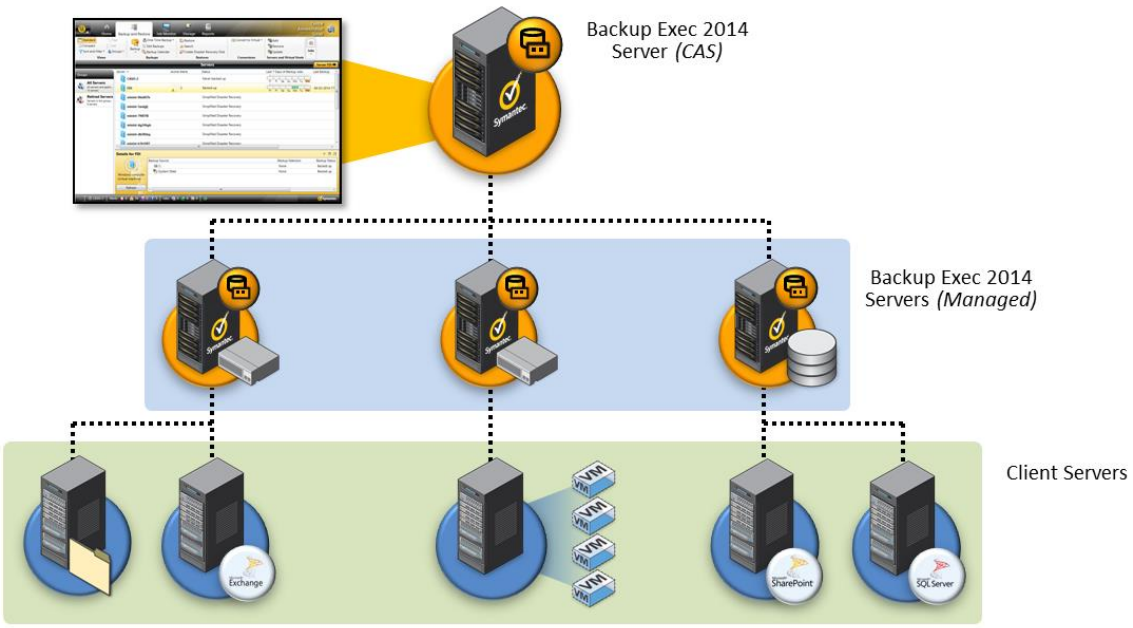

Figure 18: Centralized Data Center Diagram

Centralized Data Center with Remote Sites

Another common configuration for CASO is larger customers with both a centralized site/data center along with one or more remote sites. In configurations such as these, using a distributed catalog mode is recommended. For managed Backup Exec servers located at the central office, device and media information can be centralized at the central administration server. For managed Backup Exec servers at remote sites, unless a persistent, low-latency connection is present with high bandwidth, it is recommended that the remote managed Backup Exec servers host their own device and media information.

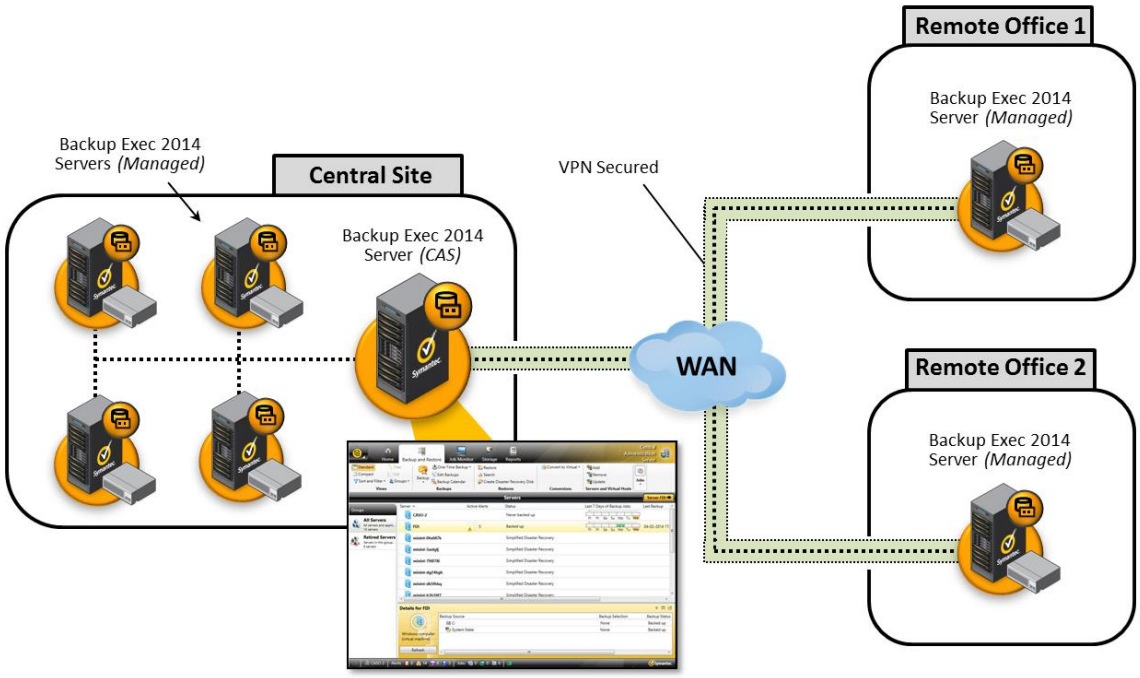

Figure 19: Data Center with Remote Sites Diagram

Private Cloud Services

The Private Cloud Services configuration is optimal for MSPs who are looking to offfer managed backup services to their customers as well as administrators of distributed environments who would like to centralize backups to a central data center and remove tape from remote office locations.

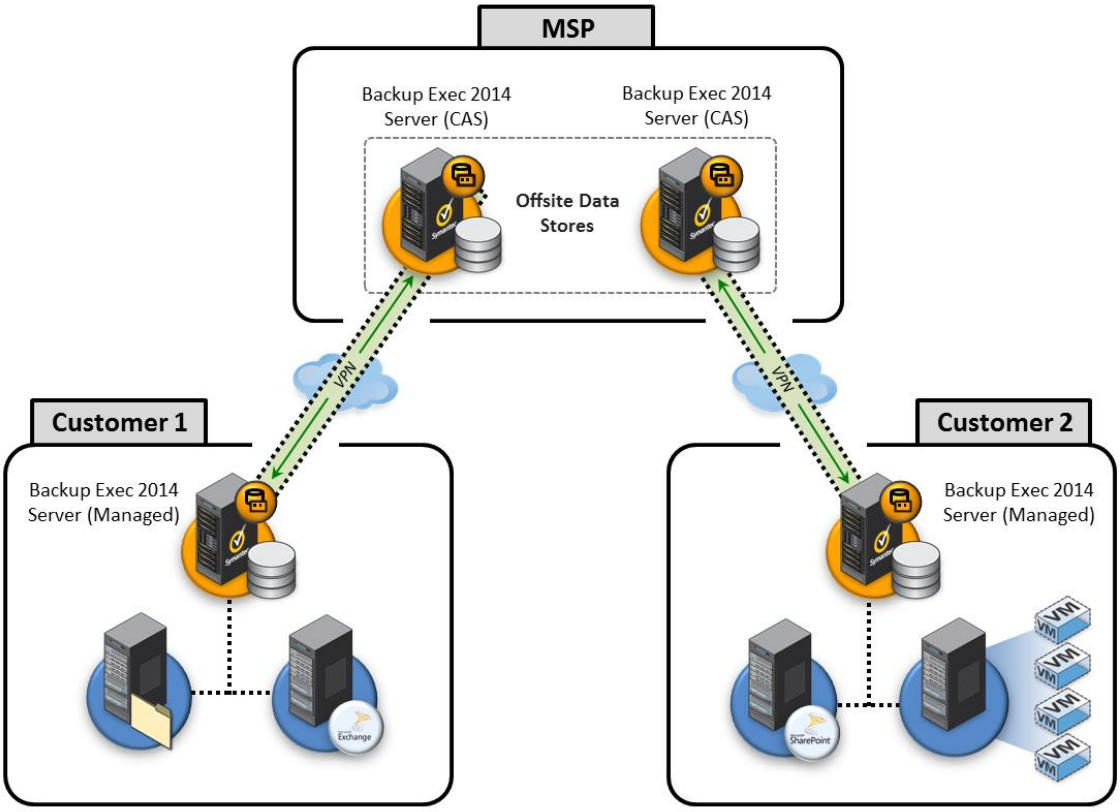

Figure 20: Private Cloud Services Diagram

Notes and Best Practices

CASO Notes and Best Practices

Managing Remote Sites

When using a central administration server to manage Backup Exec servers at remote sites, consider using the distributed catalog mode. Unless a persistent, low-latency connection is present with high bandwidth, it is also recommended that the remote managed Backup Exec servers host their own device and media information.

When following these recommendations, backup tasks cannot be centrally dispatched to the remote managed Backup Exec servers from the central administration server, nor can storage device sharing be used. However, the managed Backup Exec server, its storage devices, and locally managed backup and restore tasks can still be centrally monitored from the central administration server.

Optimized Duplication

Centralized management of managed Backup Exec servers using a central administration server is required in order to enable optimized duplication. In many configurations where optimized duplication is used, a persistent, high-bandwidth connection is required between the central administration server and the managed Backup Exec servers participating in optimized duplication operations.

To perform optimized duplication between a central administration server and a managed Backup Exec server, the following WAN requirements must be met:

- Less than one percent packet loss during transmissions
- Less than 250 milliseconds network latency

Note: For more information on optimized duplication, please refer to the white paper and technical feature brief documents available here: TECH211993.

Network Performance (Latency) Considerations

Whenever a central administration server centrally manages device and media information associated with managed Backup Exec servers, a persistent, high-bandwidth connection is required between the central administration server and the managed Backup Exec servers in question. A destination “round trip” latency of 250ms or better is recommended.

Additional Best Practice Resources

- HOWTO21788
- TECH60559

Note: Additional Backup Exec best practice documents and tech notes can be obtained through the online Symantec support portal located here: Symantec Technical Support Portal.

Central Administration Server Performance Considerations

64-bit Hardware

For best performance, a central administration server should be hosted on a server with a 64-bit hardware and software configuration. The minimum system requirements for a Backup Exec Server or a central administration server can be found in the Backup Exec™ 2014 Administrator’s Guide.

Note: For some features and capabilities, such as the Deduplication Option, a 64-bit hardware configuration and a 64-

bit Microsoft Windows operating system are required.

Regular Database Maintenance

Perform regular database maintenance to ensure your central administration server runs at optimal performance. Database maintenance is a built-in feature of the Backup Exec™ 2014 product, and instructions for running database maintenance can be found in the Backup Exec™ 2014 Administrator's Guide.

SQL Recommendations

For large and distributed Backup Exec environments, SQL Server should be used as the back-end database infrastructure on the central administration server. For optimal performance, consider hosting SQL Server on a separate 'box' or system from the central administration server. If possible, place the database and log files on separate disk subsystems (spindles).

Static IP Addresses for Central Administration Server and Managed Backup Exec Servers

Though Backup Exec will function in an environment utilizing DHCP-assigned IP addresses, it is recommended that any server functioning as a Backup Exec central administration server or managed Backup Exec server have a static IP address to minimize advertising problems which may arise due to DNS propagation issues when an IP address lease may expire.

ADBO Notes and Best Practices

Synthetic Backups

- Synthetic backup is not supported for a remote resource that is in a different time zone than the Backup Exec server.
- Do not select the option Use the Microsoft Change Journal if available if a volume contains hard links, or if you enable Single Instance Storage.
- Ensure that a disk storage device is the destination storage device for the incremental backup jobs when using synthetic backups.
- To automatically back up data to disk and then copy it to tape, use the 'add stage' feature of Backup Exec.

Note: Additional Backup Exec best practice documents and tech notes can be obtained here: Symantec Support Portal.

Off-host Backups

- Do not allow source volumes and snapped volumes to share the same physical disks. If this is not maintained, then any attempt to split the snapshot volume from the original volume fails.
- Most hardware and software providers have some limitation about the types of volumes that are transportable. Symantec recommends that you use off-host backup jobs only for backing up data for which all dependent volumes, or mounted volumes, can be imported and deported.
- Using off-host backup to back up Veritas Storage Foundation for Windows (VSFW) volumes requires that snapshot volumes in shared storage be transferred from host to host. Make sure that VSFW volumes that are backed up with off-host backup reside in VSFW disk groups that have either the "private protection" or "cluster disk group" disk group property.
- The off-host backup will fail if any one volume that you select for backup is only supported by a Microsoft Volume Shadow Copy Services (VSS) provider and cannot be imported or deported, or if the required VSS hardware provider is not on a Symantec-approved compatibility list. You can choose to continue the backup if the off-host backup fails.

List of compatible storage devices: TECH175582

- If the Central Admin Server Option (CASO) is installed, for jobs that use off-host backup, you must manually select the destination storage device that will run the job rather than allowing the job to be delegated by the central administration server. Otherwise, the job could be delegated to a Backup Exec server that does not have off-host capability. See the topic How to use media server pools in CASO here: HOWTO23391.
- Backup Exec™ 2014 does not support offhost backup of Windows 2012 servers.

Note: Additional Backup Exec best practice documents and tech notes can be obtained here: Symantec Support Portal.

For More Information

Link	Description
http://www.symantec.com/business/support/index?page=home	**Enterprise Support Portal**
www.symantec.com/business/backup-exec-for-windows-servers	**Backup Exec Family Landing Page**
www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_business_cont&pvid=57_1	**White Papers, Datasheets, Solution Briefs**
www.backupexec.com/compatibility	**Compatibility Documentation**
www.backupexec.com/skugenerator	**SKU Generator and BEST Tool**
http://www.symantec.com/docs/TECH172473	**Private Cloud Services Calculator**
http://www.symantec.com/docs/TECH172464	**Private Cloud Services Documentation**
https://partnernet.symantec.com/Partnercontent/Login.jsp	**Symantec PartnerNet Portal**

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with data backup and recovery software.