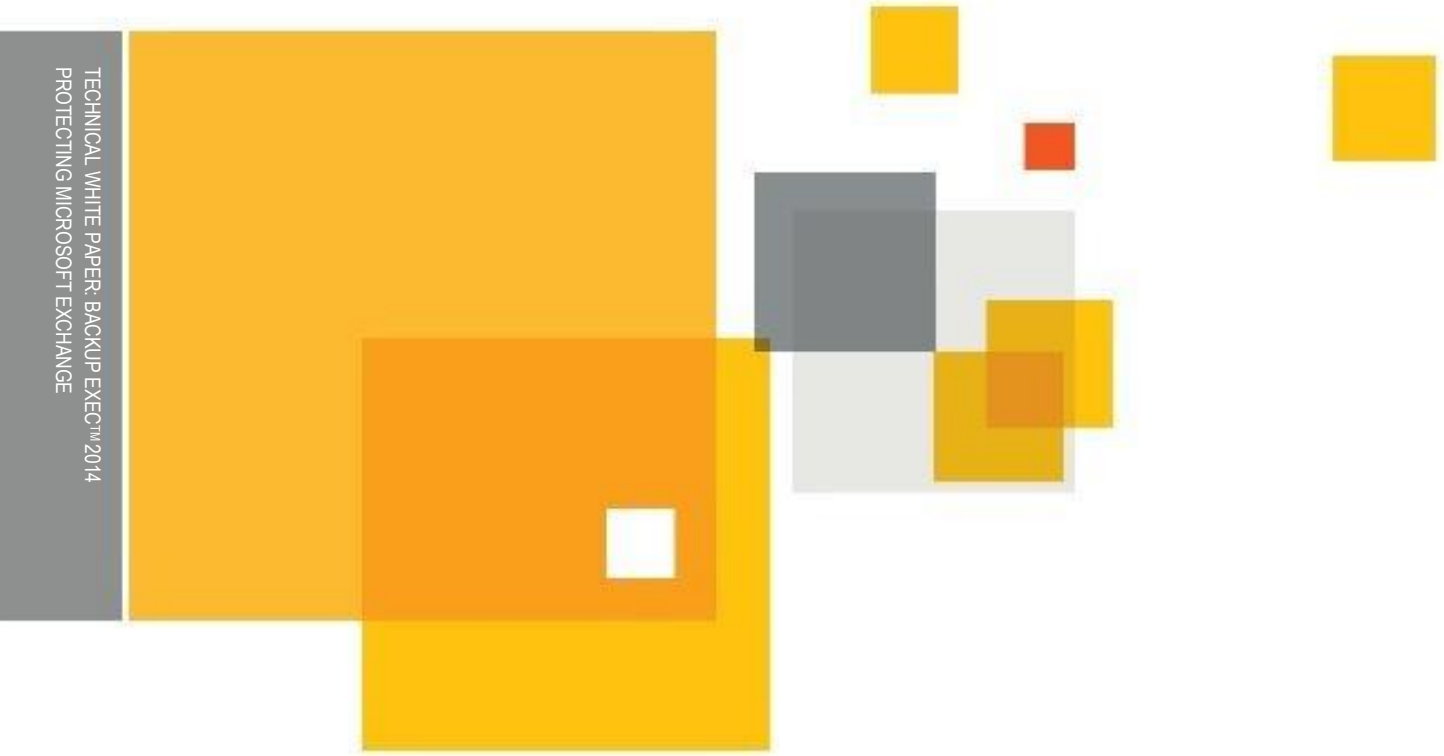


Backup Exec™ 2014 Technical White Paper

Protecting Microsoft Exchange

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.

Confidence in a connected world. Symantec.

Contents

Introduction

This white paper is intended to assist technical personnel as they design and implement Backup Exec 2014 and the Agent for Applications and Databases to protect servers hosting Microsoft Exchange, and make related decisions. The business value of the Agent for Applications and Databases as it applies to Microsoft Exchange environments will be touched upon lightly 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

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

Email is Business Critical

Email has become an indispensable way of communicating and transferring data in the modern electronic age. In the year 2010, it was estimated that almost 300 billion emails were sent each day, and around 90 trillion emails were sent every year. Considering the rate at which data continues to increase year-over-year, the number of emails sent today is likely significantly greater. Email is used for many forms of communication, including business critical communications for companies of all sizes.

Companies rely heavily upon email systems to conduct day-to-day business operations, and any significant period where access to email is lost is considered to be highly intolerable.

Microsoft Exchange

All email solutions used by modern businesses are based upon a server infrastructure hosting an email software system. Whether hosted locally on physical or virtualized servers, hosted by a partner, or hosted in the cloud, these email software systems support the incredible amount of email transmissions that happen every day, and can be implemented in many different sizes and configurations. Perhaps the most common and popular email system used in the industry today is Microsoft Exchange.

Because Microsoft Exchange plays such a critical role in the ability for organizations to conduct day-to-day business, it's equally critical that companies employ protection solutions that enable them to quickly and easily recover their Exchange system should a data loss or disaster event occur. Backup and recovery solutions of the highest value will offer features that enable the following:

- Functionality designed specifically for Microsoft Exchange
- Protection of Exchange while it remains online and functional
- Ability to protect physical Exchange servers as well as virtualized Exchange systems
- Support for highly available Exchange configurations
- Adherence to Microsoft best practices for Exchange backup and recovery
- Optimization of secondary (backup) storage using data deduplication technology
- Support for local as well as offsite storage of backup data
- Multiple levels of recovery from a single-pass backup

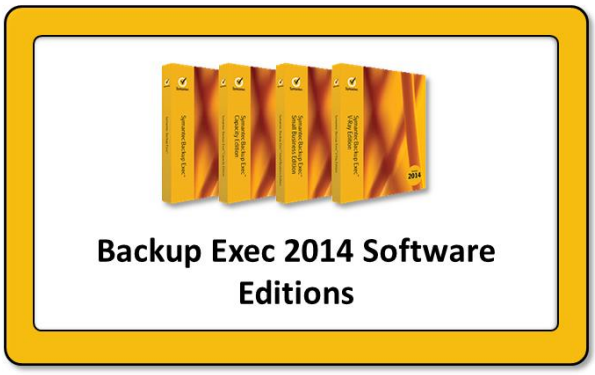
Symantec Backup Exec

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.



Unified Virtual and Physical Protection in a Single Solution

Exchange Protection Methods and Technology

Backup Exec employs modern, highly advanced, and scalable technology to protect and recover Microsoft Exchange systems. While very easy-to-use, these sophisticated technologies ensure that Microsoft Exchange remains properly protected and ready for recovery events, allowing customers and partners to sleep easy at night knowing they are prepared to handle any disaster that may befall their Exchange infrastructure.

Supported Exchange Versions

Backup Exec supports all major versions of Microsoft Exchange, including the following:

Exchange Version	Supported by Backup Exec
Exchange 2007	✓
Exchange 2010	✓
Exchange 2013	✓

Note: For Exchange 2010/2013 systems, the Backup Exec server must be hosted on 64-bit hardware.

Note: For a complete list of supported software platforms and applications, please refer to the Backup Exec Software Compatibility List (SCL) available here: TECH205797.

Components Used to Protect Exchange

The Backup Exec Server

The primary component used to protect and recover Microsoft Exchange is the Backup Exec server. The Backup Exec server interacts with the Exchange system to prepare the system for backup, to capture backup data selections, to store backup sets to the target storage device, and to perform recovery operations.

The Agent for Windows

For physical Exchange servers, the Backup Exec Agent for Windows is installed on the physical Exchange servers to identify, capture, and transmit Exchange backup data to the Backup Exec server for storage. For Exchange 2007 and later, Exchange backup data is captured through VSS snapshots and transmitted by the Agent for Windows to the Backup Exec server over the NDMP protocol, using a secure (TSL/SSL) and trusted connection.

For virtualized Exchange servers on the VMware vSphere or Microsoft Hyper-V platforms, the virtual machines hosting Exchange are protected using image-level backups through snapshot interactions with the virtual host. In these virtualized configurations, the Agent for Windows can be installed on the Exchange virtual machine to enable application discovery and metadata collection, allowing for granular application recovery features for virtualized Exchange servers. Protection of virtualized Exchange servers without the Agent for Windows installed is also supported, but without the Agent for Windows installed on the virtual machine, recovery options are limited to full virtual machine recovery and file/folder recovery.

The Agent for Applications and Databases

When protecting either physical or virtualized Exchange servers with Backup Exec, a license for the Agent for Applications and Database is required before Backup Exec can perform backup and recovery operations of Exchange application data.

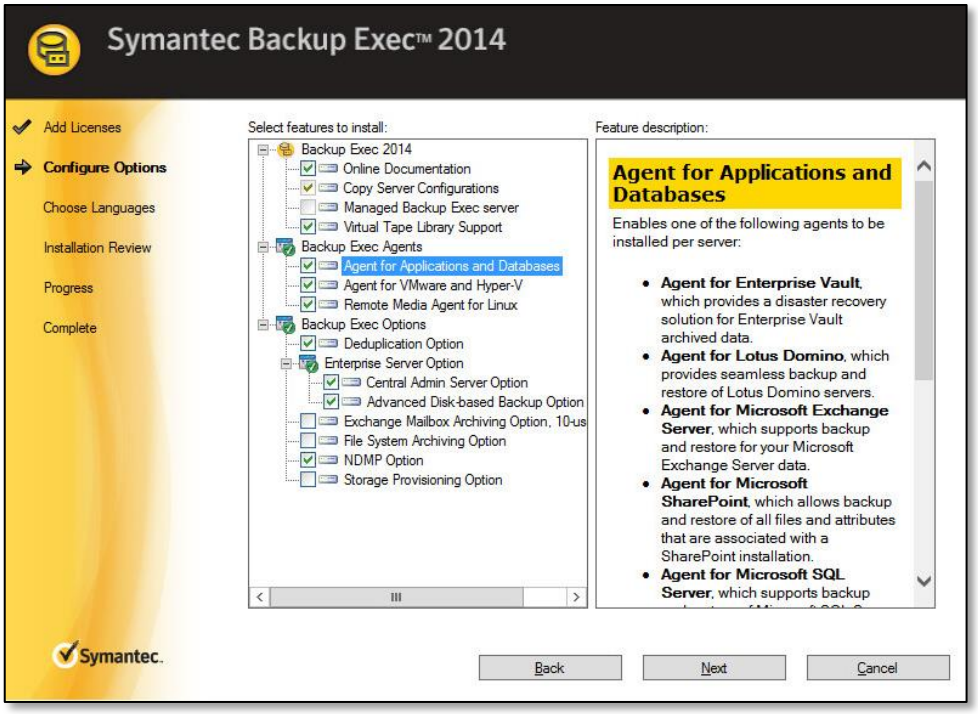


Figure 1: Enabling the Agent for Applications and Databases

Whether the Agent for Applications and Databases license is included or purchased separately depends on the Backup Exec version that is being used. For example, the standard Backup Exec 2014 product allows customers to pick and choose the different agents and options they need to protect their environment, while the Backup Exec 3600 Appliance includes unlimited use of the Agent for Applications and Databases in its core license.

It's important to note that the Agent for Applications and Databases does not represent a true software agent that needs to be pushed or installed on a physical Exchange server in order to protect it; the license simply unlocks the ability for the Backup Exec Agent for Windows to interact with Exchange components and perform advanced operations such as Backup Exec's VFF driver, which is used for advanced granular recovery operations.

Note: For additional information on the different versions and editions of Backup Exec that are available, to the Backup Exec website available here: www.backupexec.com.

Note: For additional information on requirements for protecting Exchange environments using Backup Exec, refer to the Backup Exec Administrator's Guide available here: TECH205797, and the following technotes:

- General Exchange protection requirements: HOWTO24128
- Exchange granular recovery requirements: TECH51740

Uniquely Named Mailbox

To enable key features related to the protection and recovery of Exchange servers, such as granular recovery of Exchange objects, Backup Exec must have access to a uniquely named mailbox within the Exchange infrastructure. Access to this mailbox enables Backup Exec to interact with Exchange and important components within the Exchange Information Store. In order to enable granular recovery of Exchange objects,

you must use the appropriate Exchange Server management utility to assign the user account to the Exchange Organization Administrators role (Exchange 2007) or the Exchange Organization Management role (Exchange 2010/2013). The unique mailbox should be hosted on the same version of Exchange the target mailbox is hosted.

Note: The uniquely named mailbox cannot be hidden in the Exchange Global Address List.

Note: For more information about this mailbox and associated requirements, refer to the Backup Exec Administrator's Guide available here: TECH205797, or the following technote:

- Ensuring Exchange mailbox name is unique: TECH24691

Exchange Management Tools

To protect and recover Exchange environments using Backup Exec, the Exchange Management Tools must be installed on the Backup Exec server. The management tools must be the same version or later as the management tools that are on the Exchange Server. For more information about installing the Exchange Management Tools, refer to your Microsoft Exchange documentation.

Protection of Virtualized Exchange Servers

For virtualized Exchange servers protected using the Agent for VMware and Hyper-V, Backup Exec interacts with the Exchange server through the virtual host, either through software APIs provided by the virtual infrastructure (VMware), or through the Agent for Windows installed on the virtual host (Hyper-V). For virtualized Exchange servers, Backup Exec fully supports what is generally known as "agentless" backup, both for VMware as well as Hyper-V environments.

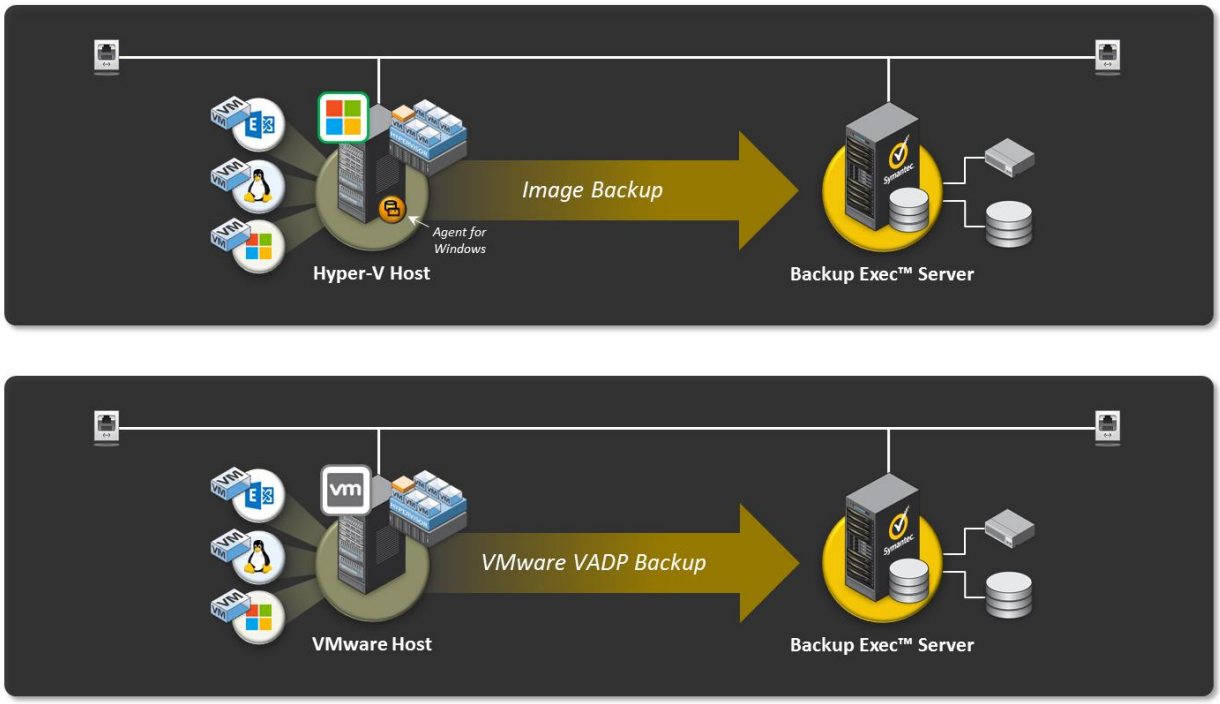


Figure 2: Backup of Virtualized Exchange Servers

Granular Application Recovery of Exchange Virtual Machines

To enhance Backup Exec's virtual machine protection and recovery capabilities, particularly when the virtual machine is hosting Exchange, the Agent for Windows should be installed on the guest virtual machine itself. In this configuration, Backup Exec can still capture snapshot-based, image-level backups of the destination virtual machine, but can then also offer dynamic application discovery capabilities and granular recovery of Exchange application components, all from a single-pass backup. In other words, even with the Agent for Windows installed on the virtual machine, the backup process remains what is known in the industry as an "agentless" backup; the presence of the Agent for Windows within the virtual machine simply allows for application metadata capture and granular recovery of application objects directly back to the original virtual machine.

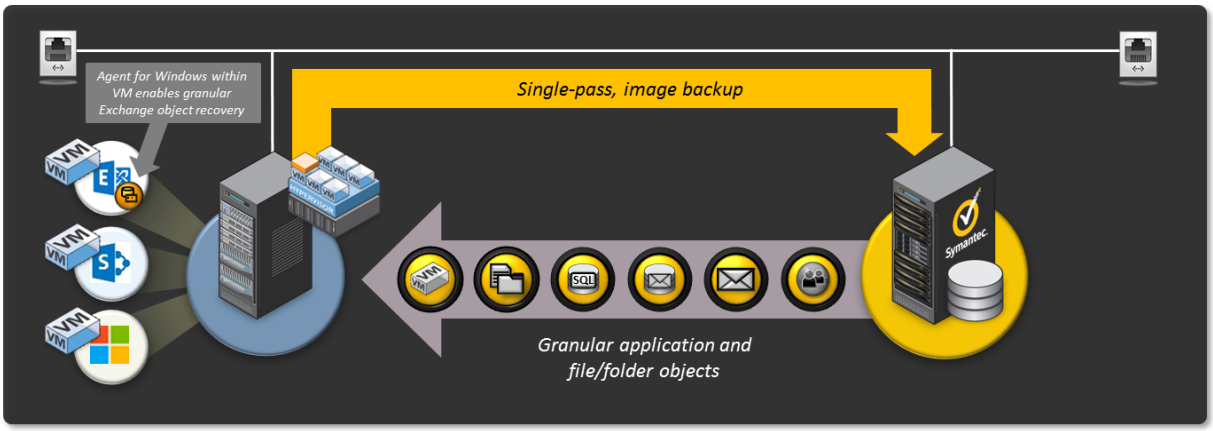


Figure 3: Agent for Windows Enables Granular Recovery of Virtualized Exchange Servers

While Backup Exec fully supports protecting virtualized Exchange servers without installing the Agent for Windows to the virtual machine, recovery options are limited in this configuration. When the Agent for Windows is not present on the Exchange virtual machine, Backup Exec has no direct knowledge of Exchange being present on the virtual machine, and recovery options are limited to full virtual machine recovery and file/folder recovery.

Application-specific recovery features are only available when the Agent for Windows is installed on the Exchange virtual machine, which allows Backup Exec to discover the Exchange application and capture the Exchange metadata needed to enable application-specific recovery features for the associated virtual machine backup.

VSS Integration and Virtualized Exchange Servers

When protecting virtualized Exchange servers, Backup Exec utilizes Microsoft's VSS service to prepare the Exchange virtual machine for backup and truncation of Exchange transaction logs.

For VMware environments where the Agent for Windows has been installed on the Exchange virtual machine, these VSS calls are made to the Agent for Windows through interactions with the vStorage API and involve the VSS writer on the virtual machine. The VSS writer will be either the VSS writer included with VMware Tools, or the Backup Exec VSS writer that is installed with the Agent for Windows.

For Hyper-V environments, a similar process happens through interactions with the Hyper-V host via the local Agent for Windows agent installed on the Hyper-V host. The VSS writer that is used to prepare the virtual machine for backup will be either the VSS writer installed on the virtual machine along with Hyper-V Integration Services, or the Backup Exec VSS writer that is installed with the Agent for Windows.

With either VMware or Hyper-V environments, Backup Exec invokes a virtual machine-level VSS full backup, which prepares Exchange for the virtual machine snapshot event and truncates Exchange transaction logs. If

the Agent for Windows is installed on the Exchange virtual machine, the VSS backup method can be changed to a VSS copy, which will not truncate log files.

Note: For more information, refer to the following technote: HOWTO74082

Virtualized Exchange Servers in Distributed Configurations

Backup Exec supports modern image-level protection of VMware and Hyper-V virtual machines, including virtual machines hosting applications such as Exchange. It's important to note that Backup Exec does not currently support image-level backups of virtualized Exchange servers in a distributed configuration. Only standalone virtual machines hosting Exchange are supported for image-level backup and granular recovery.

In order to achieve granular recovery support of virtualized Exchange servers in a distributed configuration, such as an Exchange 2013 Database Availability Group (DAG), the virtual machines must be protected using agent-based backups, which essentially treat each virtual machine as if it were a standalone physical system.

Protection of Physical Exchange Servers

For physical Exchange servers, the Agent for Windows is installed locally to the Exchange server. The Agent for Windows interacts with the physical Exchange server to prepare the Exchange databases for backup and to transmit backup data to the Backup Exec server over the NDMP protocol.

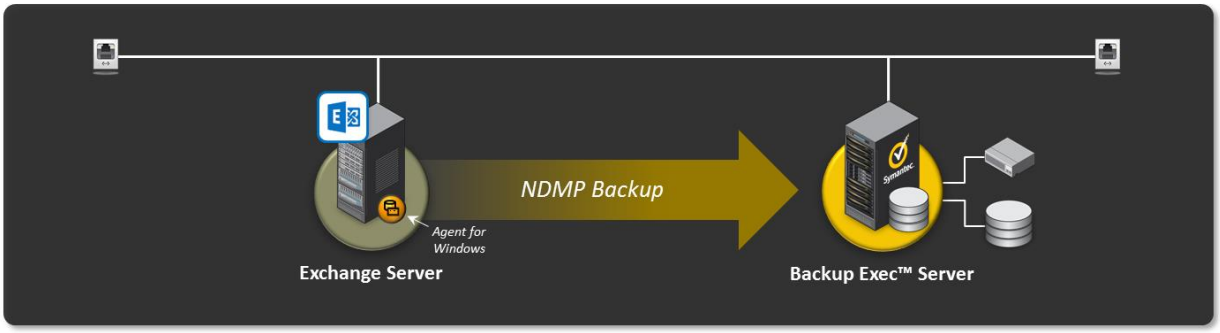


Figure 4: Backup of Physical Exchange Servers

VSS Integration and Physical Exchange Servers

Backups of physical Exchange servers that are captured by the Agent for Windows are snapshot backups performed using Microsoft's VSS Writers. In most cases, Backup Exec uses a VSS full backup, which ensures that Exchange is placed into a consistent state at the time of backup and also truncates transaction logs, a key element of maintaining a healthy database application over time.

The Agent for Windows can only protect components of an Exchange server after the Agent for Applications and Databases has been licensed within Backup Exec.

Granular Application Recovery of Physical Exchange Servers

In addition to preparing physical Exchange servers for backup and transmitting Exchange backup data to the Backup Exec server for storage, the Agent for Windows also plays a key role during Exchange recovery. For example, the presence of the Agent for Windows locally installed on a physical Exchange server enables the Backup Exec server to directly transmit and restore granular Exchange objects back to the production Exchange environment of an organization. Other granular object recovery features are also available, such as the ability to restore granular Exchange objects to a PST file.

Note: When recovering Exchange objects to a PST file certain requirements apply relating to Microsoft Outlook. For

more information on these requirements, refer to the Backup Exec Administrator's Guide available here: TECH205797.

Offhost Backups of Physical Exchange Servers

Backup Exec also supports offhost backups of physical Exchange servers. Offhost backups help alleviate the processing overhead of backup operations from the physical Exchange server by transferring them to the Backup Exec server.

Note: For more information on Backup Exec and configuring offhost backups of physical Exchange servers, refer to the Backup Exec Administrator's Guide available here: TECH205797, and the following technote: HOWTO12231.

Communication Security

Ensuring the security of backup data is just as important as ensuring the security of live data resources within an IT environment. To ensure the protection and security of backup data captured from business critical Exchange servers, all transmissions between the Backup Exec server and the Agent for Windows are encrypted using TSL/SSL encryption technology and require a trust to be established. This applies to the backup and recovery of physical Exchange servers as well as Exchange servers that are virtualized on Hyper-V infrastructures.

Communication Security in VMware Environments

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

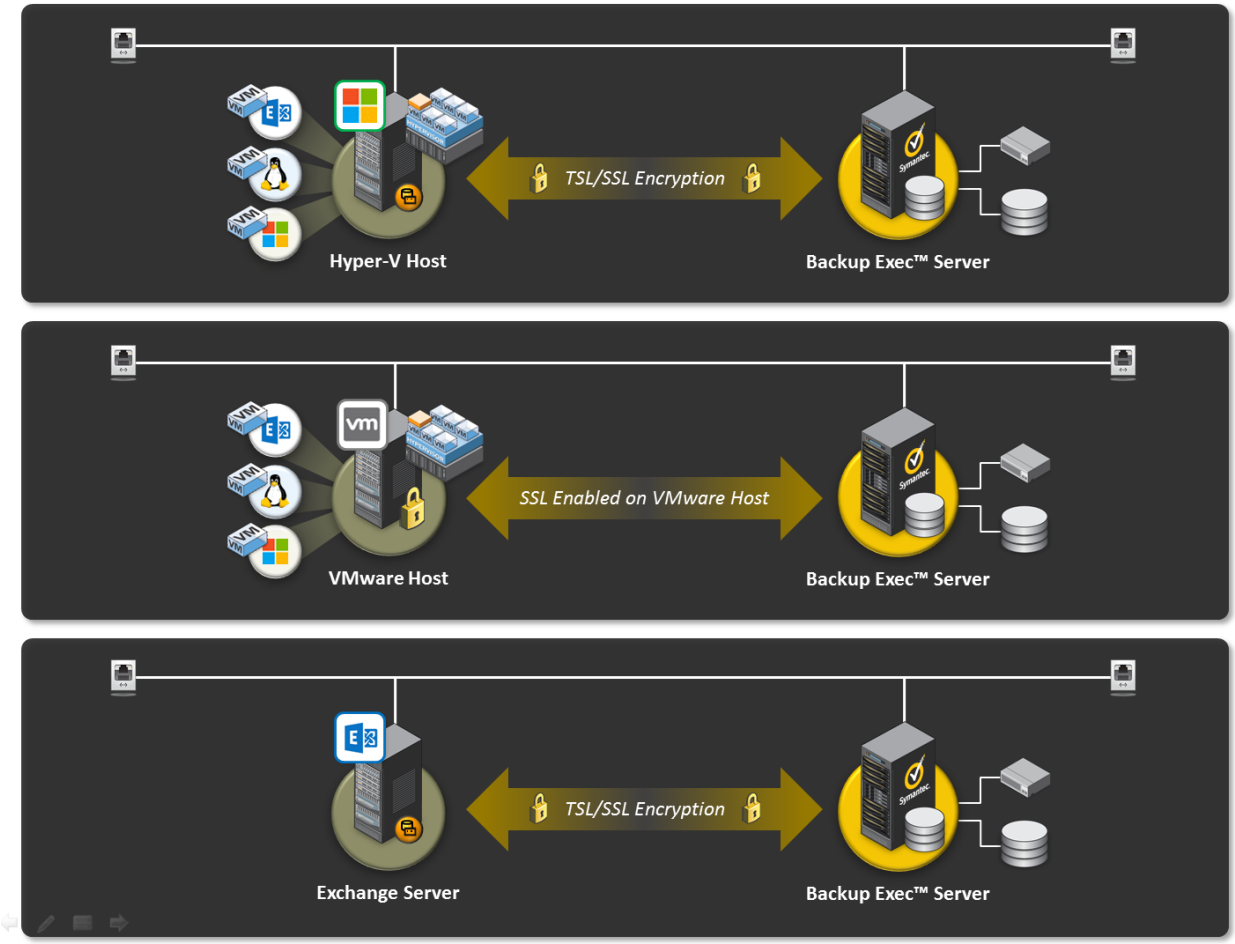


Figure 5: Communication Security when Protecting Exchange with Backup Exec

The Exchange Information Store

Mailbox Servers and the Exchange Information Store

The primary storage component of Microsoft Exchange is commonly referred to as the Information Store. The Exchange Information Store is associated with Exchange mailbox servers, and each mailbox server can contain one or more mailbox databases. The Information Store can be implemented in highly available configurations, such as Exchange 2010/2013 Database Availability Group (DAG) configurations. The Information Store represents the primary storage component of any Exchange infrastructure.

Mailbox Databases

Each mailbox server in an Exchange environment will contain one or more mailbox databases. Each mailbox database contains one or more user-specific mailboxes and related components, such as mailbox folders, emails, email attachments, and calendar items.

For Exchange 2007, mailbox databases are contained within Storage Groups. Storage Groups are associated with a set of Exchange transaction logs, which are used to manage and track database write operations. Exchange 2010/2013 does not include Storage Groups, and associates transaction logs with individual databases.

In Exchange 2007/2010, public folders are hosted in 'public folder' databases. Backup Exec 2014 can restore the contents of public folders but does not support recreating the public folder mailbox directly. In Exchange 2013, public folders are hosted across one or more public folder mailboxes in a mailbox database.

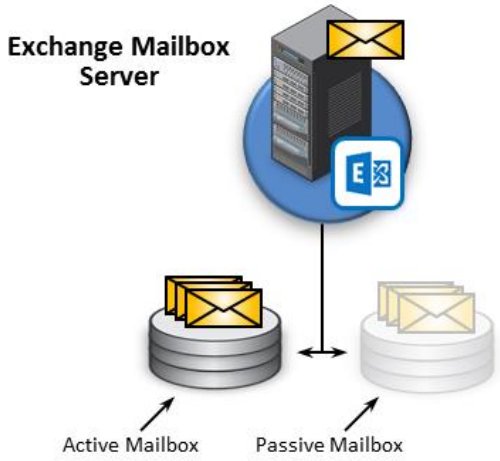


Figure 6: Exchange Mailbox Server and Mailbox Databases

Mailbox Servers and Distributed Exchange Configurations

In distributed Exchange configurations, only servers with the Mailbox role (mailbox server) will contain Information Store data, and as such mailbox servers are the focus of any Exchange backup strategy. When browsing the contents of servers from the Backup Exec interface, Information Store selections will only appear under mailbox servers. All other Exchange server roles in the distributed Exchange environment should be treated like standard servers (file and system state backup selections apply).

Full, Incremental, and Differential Backups of Exchange

Backup Exec supports multiple methods for protecting Exchange servers, including full, copy, incremental, and differential backups. Different backup methods can be used to protect the same Exchange server. For example, an administrator may decide to protect his Exchange infrastructure with weekly full backups and daily incremental backups.

- Full backup – Backs up everything selected for protection in the backup job.
- Differential backup – Backs up everything selected for protection that has changed since the last full backup event.
- Incremental backup – Backs up everything selected for protection that has changed since the last full or incremental backup event.

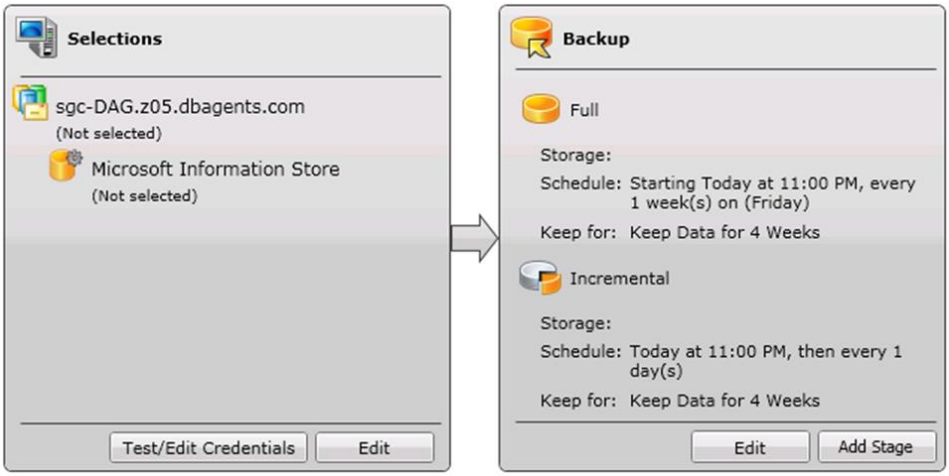


Figure 7: Exchange Backup Methods

Note: For more information about these backup methods, refer to the Backup Exec Administrator's Guide, available here: TECH205797.

Data Deduplication and Exchange Backups

Backup Exec includes advanced, block-level data deduplication technology that allows administrators to greatly optimize backup disk storage resources that are managed by a Backup Exec server. Exchange backup data is fully supported for data deduplication. Administrators leveraging Backup Exec's data deduplication technology when protecting Exchange environments will benefit from significant backup disk storage savings when compared to standard (non-deduplicated) disk backup devices. Data deduplication will offer the most storage optimization benefits against full backups of Exchange data.

Backup Exec Partner Toolkit

Overview

To assist partners and end users as they implement Backup Exec 2014 and the Backup Exec 3600 Appliance, Symantec has released the Backup Exec Partner Toolkit. The Backup Exec Partner Toolkit demonstrates the power of the Backup Exec data protection portfolio by qualifying the hardware configuration of potential backup servers to ensure they will perform to expectations, by calculating front-end capacity amounts to streamline the Backup Exec licensing process, and by demonstrating the storage optimization benefits of Backup Exec's deduplication technology.

Note: The Backup Exec Partner Toolkit is available to Symantec partners and end users at no charge and can be downloaded from the Symantec Connect portal here: Backup Exec Partner Toolkit.

Business Value

The Backup Exec Partner Toolkit includes three tools designed to help partners and end users perform environmental assessments either before or after installing a Backup Exec solution. These are as follows:

- **Performance Analyzer** - The Performance Analyzer Tool will assess the readiness of one or more server systems to act as a Backup Exec server. Each server's hardware and software configuration is analyzed for performance inhibitors, including any disk and tape backup devices attached to that server.

- **Deduplication Assessment Tool** - The Deduplication Assessment Tool will directly demonstrate the value of Backup Exec's deduplication technology to partners and end users by scanning one or more servers in an environment and offering deduplication ratio and backup storage savings estimates.
- **Front-end Capacity Analyzer** - The Front-end Capacity Analysis Tool will easily and quickly identify the amount of front-end data in an environment and greatly streamlines the process of selling the Backup Exec Capacity Edition, which is licensed against the amount of front-end data in an environment.

Ease of Use

By design, the Backup Exec Partner Toolkit offers a wizard-driven experience that is very easy to use. Simply select the tool to run, identify the servers and associated volumes and application resources to scan, provide associated credentials, and run the selected operation. Upon completion, a results screen is displayed in the form of a report which can be saved to a number of common file formats.

Platform and Application Support

The Backup Exec Partner Toolkit supports Windows 2003, Windows 2008, and Windows 2012 x86 and x64 platforms, including both physical and virtual systems. Front-end capacity analysis is supported for Windows volumes. Deduplication analysis is supported for Windows volumes, Exchange application data, and SQL application data. Performance analysis is supported for any server running Windows 2003, Windows 2008, or Windows 2012 (x86 or x64).

Exchange Backup Consistency

In many cases, Exchange transactional database systems can remain in a near constant state of receiving, logging, and committing operations to its databases. If a snapshot of an Exchange system is taken for backup purposes without properly preparing the Exchange application for backup, the data that is captured could represent an inconsistent view of the Exchange application, and recovery from that inconsistent backup would likely be problematic and subject to potential recovery failure.

In accordance with Microsoft best practices, Backup Exec interacts with Exchange through the VSS service to ensure that Exchange is momentarily placed into a quiet or consistent state at the time of backup. This ensures that the backup data that is captured represents a consistent view of the Exchange application, ensuring successful recovery if needed.

Exchange Transaction Log Truncation

Transaction logs are a key element of any Exchange infrastructure. Exchange transaction logs are used to track database write operations (such as a user creating an email object) both before and after they are committed to the associated Exchange database. The transaction log process within Microsoft Exchange helps maintain the integrity of Exchange databases over time.

To prevent transaction logs from eventually saturating available disk storage resources, periodic truncation of Exchange transaction logs is needed. Truncation of transaction logs refers to the process by which Exchange transaction logs that can be safely removed are identified and deleted. Backup Exec, through the Microsoft VSS service integration, initiates transaction log truncation as a part of backup operations. This is true for backups of physical Exchange servers as well as virtualized Exchange servers on VMware or Hyper-V platforms.

Backup Exec and Exchange High Availability Configurations

Backup Exec fully supports protecting Exchange infrastructures that have been implemented in highly available configurations. Exchange high availability options and technologies have evolved over time, and the high availability options available are dependent upon the version of Microsoft Exchange being used in the environment.

Exchange 2007 High Availability Configurations

Backup Exec supports Exchange 2007 environments that are implemented in high availability configurations. This includes the following:

- Single Copy Cluster (SCC)
- Clustered Continuous Replication (CCR)
- Local Continuous Replication (LCR)

The following is a basic diagram of a Standby Continuous Replication (SCR) environment:

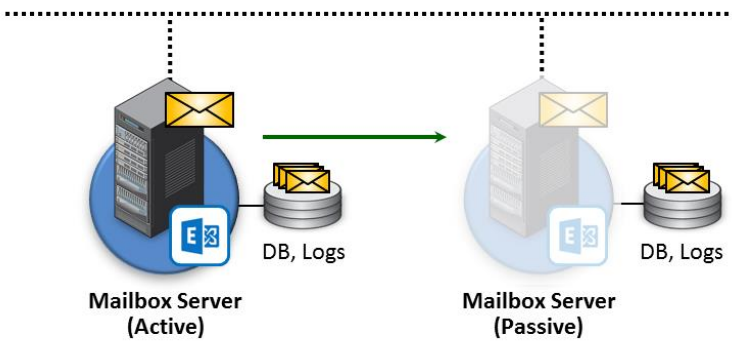


Figure 9: Basic Exchange 2007 SCR Diagram

Exchange 2010 and 2013 Database Availability Groups

Backup Exec supports Exchange 2010/2013 environments that are implemented in a Database Availability Group (DAG) configuration. To back up the databases within a DAG, you must install the Agent for Windows on all the servers in the DAG.

For Exchange 2010, Exchange recovery operations are performed via Exchange Web Services. Recovery operations are directed to a Mailbox Server.

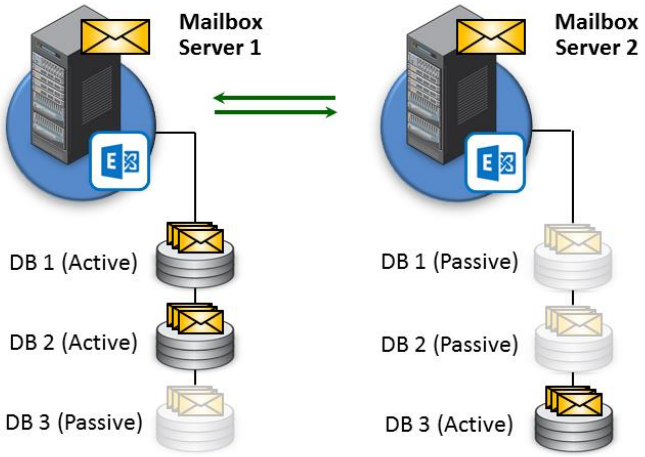


Figure 10: Basic Exchange 2010 or 2013 DAG Diagram

Best Practices for Exchange High Availability Configurations

It is recommended that Backup Exec be used to protect standby or secondary mailbox servers and Information Stores whenever possible in Exchange environments that are configured for high availability. This allows Backup Exec to successfully protect Exchange data without burdening the active or primary Exchange servers with backup processes and associated overhead.

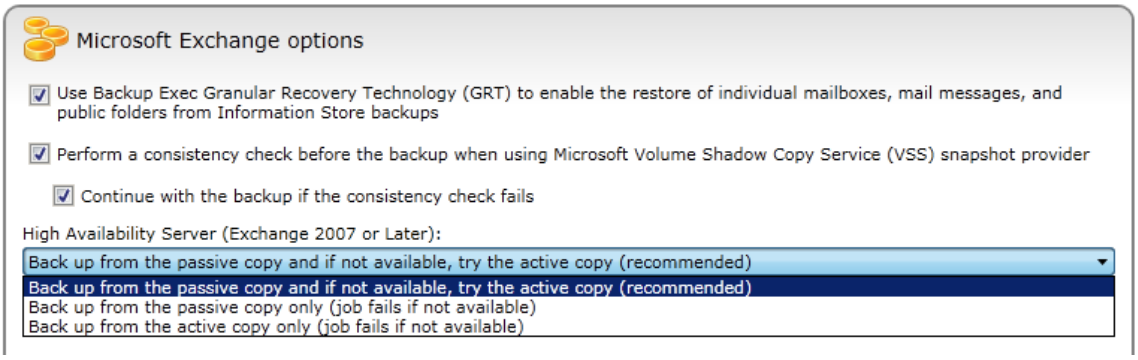


Figure 11: High Availability Server Options

It's important to plan a Backup Exec implementation that aligns properly with the topological view of the destination Exchange environment. For example, in environments where Exchange has been configured to replicate or failover across WAN connections, ensure that Backup Exec servers are located at the same site as the Exchange servers they are protecting, and use the Preferred Server Configuration features of Backup Exec to ensure the correct Exchange servers are selected for backup operations. This will prevent Backup Exec from pulling large amounts of data over WAN connections that may have limited available bandwidth.

Utilizing disk storage as the initial location for storage of Exchange backups can help increase backup performance. For environments where placing Exchange backups on tape media is a requirement, adopting a disk-to-disk-to-tape (D2D2T) strategy is recommended for optimal performance.

Note: For information on Preferred Server Configurations, refer to the Backup Exec Administrator's Guide available here: TECH205797.

Exchange Recovery Methods and Technology

Backup Exec remains a pioneer in application recovery technology, and Microsoft Exchange is no exception. From a single-pass backup of an Exchange server – whether that Exchange server is on physical hardware or has been virtualized – Backup Exec offers a wide variety of powerful and flexible recovery options.

Virtualized Exchange Server Recovery Options

Exchange servers that have been virtualized on the VMware vSphere or Microsoft Hyper-V platforms and protected by Backup Exec can be restored using any of the following methods:

- Full virtual machine recovery
- Exchange application recovery, such as recovery of the Exchange Information Store
- Granular Exchange recovery, such as mailboxes, mailbox folders, emails, and attachments
- Redirected recovery of Exchange data

These flexible and powerful recovery options offer partners and customers the tools they need to quickly and easily recover their Exchange environment, whether they need to quickly recover the entire Exchange virtual machine, restore only a single email, or anything in between.

Full Virtual Machine Recovery

When protecting virtualized Exchange servers using Backup Exec and the Agent for VMware and Hyper-V, the entire virtual machine can be recovered to the original virtual host, or to an alternate virtual host. This recovery operation restores the virtual machine in its entirety, and can be immediately powered on after the restore process is complete.

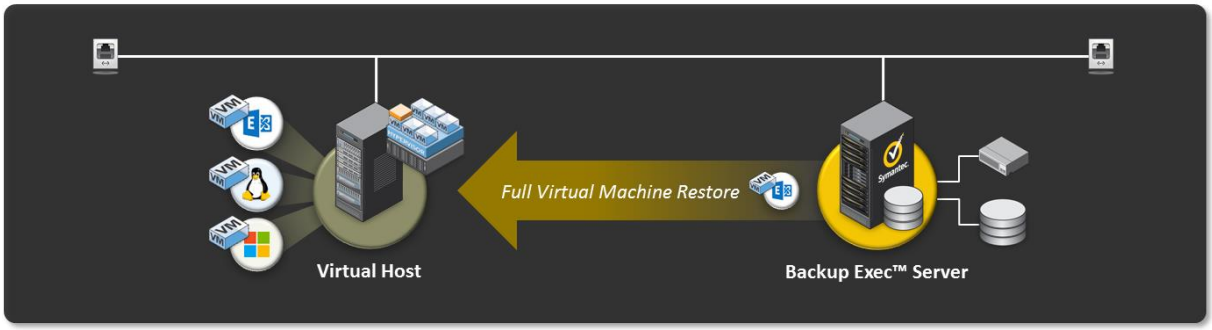


Figure 12: Full Exchange Virtual Machine Recovery

Note: In order to restore an Exchange virtual machine to an alternate virtual host, the alternate virtual host must be licensed for the Agent for VMware and Hyper-V.

Exchange Application Recovery

Full recovery of an Exchange application instance in virtualized environments is also supported by Backup Exec. This includes the recovery of all selected Exchange application components back to the original Exchange virtual machine.

The recovery of an Exchange application instance is performed by creating a restore job in the Backup Exec interface for the selected Exchange server. Backup Exec intelligently identifies Exchange servers and streamlines the recovery experience by showing the administrator those recovery options and data choices that are specific to the server selected for recovery.

It's important to note that application-level recovery is only supported for Exchange virtual machines when the Agent for Windows has been installed on the Exchange virtual machine. This allows Backup Exec to detect the Exchange application within the virtual machine at the time of backup and collect the necessary metadata in order to support application recovery operations. The Agent for Windows is also required to be installed on the virtual machine in order to restore data directly back to the virtual machine.

Granular Exchange Recovery

Backup Exec remains an industry leader in the granular recovery of Microsoft Exchange. Administrators can easily recover individual mailbox databases, mailbox folders, emails, email attachments, and many other granular Exchange application objects and recover them back to the original Exchange server, or save them as .PST files.

Granular recovery of Exchange application data is supported for both physical Exchange servers as well as virtualized Exchange servers. Granular recovery of Exchange is supported from a single-pass backup of the virtualized Exchange server; additional backups of the Exchange infrastructure are not necessary.

It's important to note that granular recovery of Exchange objects is only supported for Exchange virtual machines when the Agent for Windows has been installed on the Exchange virtual machine. This allows Backup Exec to detect the Exchange application within the virtual machine at the time of backup and collect the necessary metadata in order to support granular object recovery operations. The Agent for Windows is also required to be installed on the virtual machine in order to restore data directly back to the virtual machine.

Also, the Client Access Server role needs to be installed on the Exchange virtual machine in order for granular object recovery tasks to be successful.

Note: For more information about the granular Exchange recovery capabilities in Backup Exec, please refer to the Backup Exec Administrator's Guide available here: TECH205797.

Redirected Recovery of Exchange Data

Backup Exec supports redirected recovery of Exchange virtual machines as well as Exchange application data. In order to restore a full Exchange virtual machine to an alternate host, the destination virtual host must be licensed with the Agent for Applications and Databases.

The redirected recovery of Exchange application data for virtualized Exchange servers is very similar to the process for physical servers. In order to redirect the recovery of Exchange data, such as storage groups and mailbox databases, the target Exchange server must be licensed for the Agent for Applications and Databases and the Agent for Windows must be installed on the Exchange server.

Physical Exchange Server Recovery Options

Exchange servers that are installed on standalone physical hardware configurations and protected by Backup Exec can be restored using any of the following methods:

- Full server recovery, including bare metal and dissimilar hardware recovery
- Conversion of Exchange servers to virtual
- Exchange application recovery, such as recovery of the Exchange Information Store
- Granular Exchange recovery, such as mailboxes, mailbox folders, emails, and attachments
- Redirected recovery of Exchange data

Full Server Recovery

Backup Exec includes fully integrated and streamlined support for performing full server recovery operations, including bare metal and dissimilar hardware recovery of physical Exchange servers.

To enable support for full server recovery, at least one full Simplified Disaster Recovery (SDR) backup of the physical Exchange server must exist. SDR backups include the necessary system-level information required to reconstruct a physical server from bare metal.

Should a physical Exchange server suffer a fatal crash or disaster, the Symantec Recovery Disk (included with Backup Exec) can be used to locate the SDR backup and recover the server through a single, automated process. The server can be recovered back to the original hardware configuration or to a new or dissimilar hardware configuration. The Symantec Recovery Disk uses information within the SDR backup to reconstruct the server without the need for the administrator to partition or format disk storage, install the operating system, or any similar step associated with manual, legacy recovery processes. The administrator simply boots the destination physical server with the recovery disk, connects to the Backup Exec server hosting the SDR backup, and performs the recovery; everything else is automated.

Recovery processes are secured using the same TSL/SSL encryption methods used during backup operations. After booting the target physical server with the Symantec Recovery Disk and identifying the Backup Exec server hosting the SDR backup, the administrator must authenticate to the Backup Exec server which results in a secure, trusted connection between the server being recovered and the Backup Exec server. SDR backup data is transmitted to the server being restored through this secure connection over the NDMP protocol.

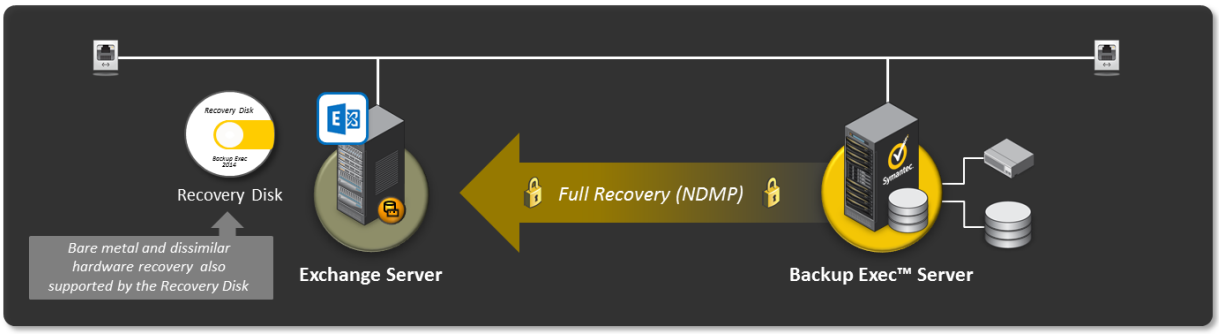


Figure 13: Full Recovery of a Physical Exchange Server

During full recovery operations for a physical Exchange server, either to the original configuration or to a dissimilar hardware configuration, only the disk and volume structure, operating system components, and file/folder contents of the server are recovered. After the core Exchange server system has been recovered, either to the original hardware configuration or to a new or dissimilar hardware configuration, the Exchange application components can be restored to the physical Exchange server from the Backup Exec administration console.

For virtualized Exchange servers, full virtual machine recovery is also supported. Full virtual machine recovery can target either the original virtual host or an alternate virtual host. This support extends to both VMware and Hyper-V environments. Full recovery of Exchange virtual machines is a single step operation.

Note: For more information about SDR recovery capabilities of Backup Exec, refer to the Backup Exec Administrator's Guide available here: TECH205797, or the corresponding white paper on the subject.

Converting Exchange Servers to Virtual

Backup Exec also supports recovering or converting SDR backups of a physical Exchange server to a VMware or Hyper-V virtual machine. These conversion operations can run in parallel to SDR backups, after SDR backups,

on a different schedule, or on an ad hoc basis. These virtual conversion capabilities are also based on SDR technology. SDR backups include the necessary system-level information required to construct a virtual machine replica of a physical server.

After performing a virtual conversion of a physical Exchange server, should the original physical Exchange server experience a fatal crash or other disaster event, the virtual machine replica can be used to quickly recover the Exchange server in virtual mode.

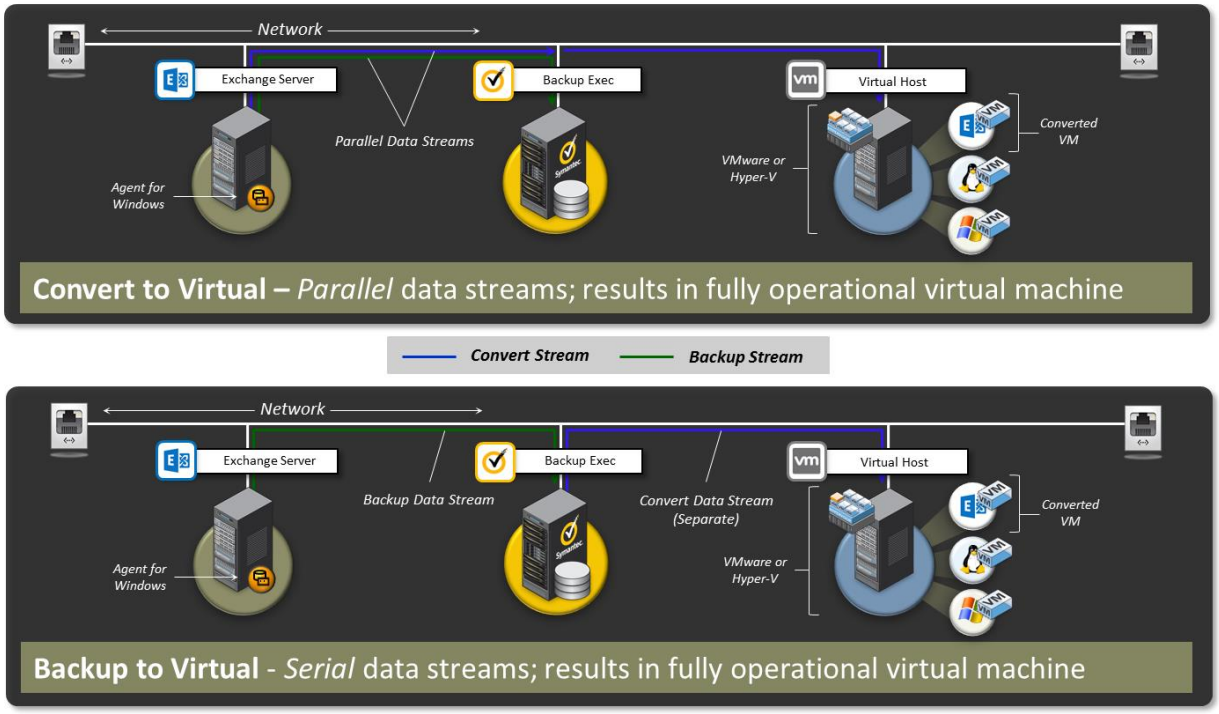


Figure 14: Virtual Conversion of Physical Exchange Server

Virtual conversions can also be used for other purposes, such as permanent conversion of an Exchange server to a virtual infrastructure, or for testing purposes.

Note: For more information about the virtual conversion capabilities of Backup Exec, refer to the Backup Exec Administrator's Guide available here: TECH205797, or the corresponding white paper on that subject.

Application Recovery

Full recovery of an Exchange application instance is also supported by Backup Exec. This includes the recovery of all selected Exchange application components back to the original Exchange server in single-server Exchange environments, or the recovery of the Exchange Information Store and other Exchange components to associated mailbox servers and other Exchange servers in distributed Exchange configurations.

The recovery of an Exchange application instance is performed by creating a restore job in the Backup Exec interface for each of the servers involved in the Exchange environment. Backup Exec intelligently identifies Exchange servers and streamlines the recovery experience by showing the administrator those recovery options and data choices that are specific to the Exchange server that is selected for recovery.

When considering a protection strategy for an Exchange environment, it's important to consider the role of Active Directory. Exchange modifies the Active Directory database with additional fields, such as the mailbox

name for each Exchange user, and Exchange stores important configuration data in Active Directory database. The Active Directory database is also leveraged to control other important Exchange data elements, including administrative groups, storage groups, and stores. It is very important that the Active Directory infrastructure be protected alongside Exchange, to ensure a successful application recovery can be completed in the event of a disaster.

Application-level recovery processes are secured using the same TSL/SSL encryption methods used during backup operations, and leverage the established trust relationship between the Backup Exec server and the Exchange server.

Granular Application Recovery

Backup Exec remains an industry leader in the granular recovery of Microsoft Exchange. Administrators can easily recover individual mailbox databases, mailbox folders, emails, email attachments, and many other granular Exchange application objects and recover them back to the live Exchange infrastructure, or save them to .PST files.

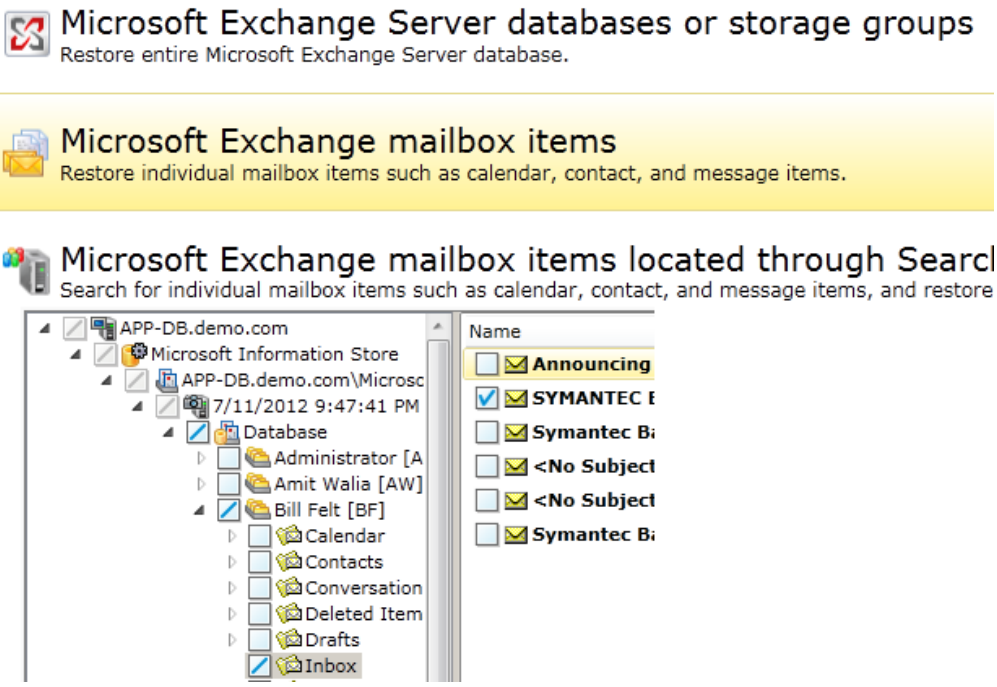


Figure 15: Granular Recovery of Exchange Application Data

Granular recovery of Exchange application data is supported for both physical Exchange servers as well as virtualized Exchange servers. Granular recovery of Exchange is supported from a single-pass backup of the Exchange server; additional backup events or “touches” of the Exchange infrastructure are not necessary.

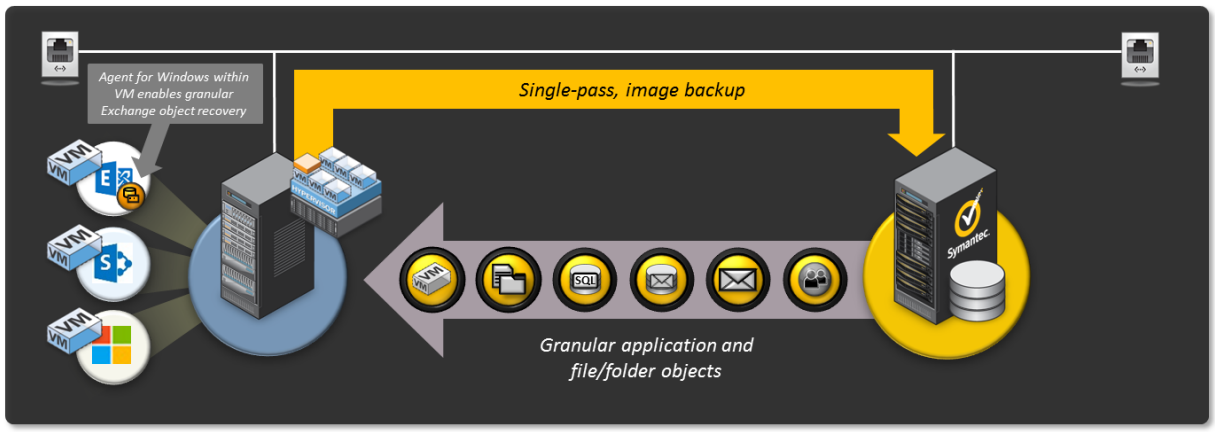


Figure 16: Granular Recovery of Exchange Servers

Note: For more information about the granular Exchange recovery capabilities in Backup Exec, please refer to the Backup Exec Administrator's Guide available here: TECH205797.

Redirected Recovery of Exchange Data

Backup Exec supports the recovery of Exchange data, such as storage groups and mailbox databases, to an Exchange server that is different from the original Exchange server that was backed up. Important use scenarios for this feature include disaster recovery to an alternate host, and seeding secondary copies of Exchange databases in high availbility configurations, such as DAG configurations.

To redirect Exchange data, the destination Exchange server must be the same Exchange version and service pack as the original, must have the Agent for Windows installed, and must have an Agent for Applications and Databases license.

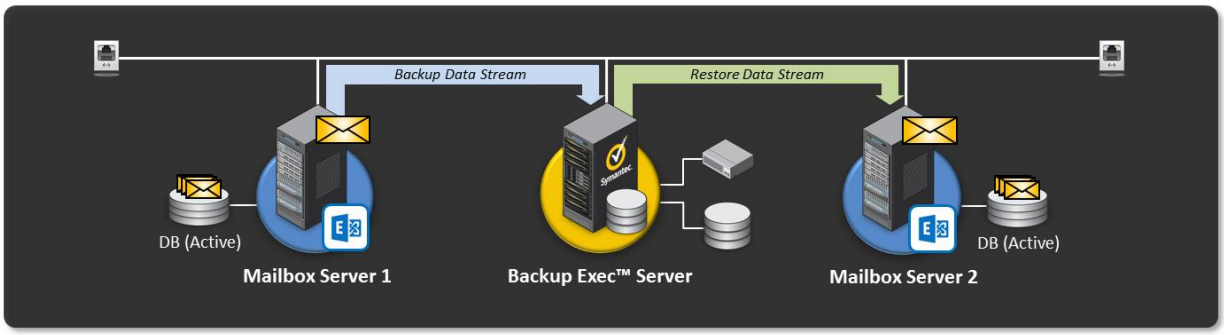


Figure 17: Redirected Recovery of Exchange Data

Note: For additional information on redicted recovery of Exchange data, refer to the Backup Exec Administrator's Guide available here: TECH205797, and the following technote: HOWTO24078.

Managing Backup Exec Rights and Permissions in an Exchange Environment

It is very important to ensure that the different user accounts that Backup Exec uses to protect Microsoft Exchange are granted the necessary privileges in order for Backup Exec to function properly. This section offers important guidance for each of the key accounts leveraged by Backup Exec to perform Exchange backup and recovery operations.

Agent for Windows

For the protection of physical Exchange servers, Backup Exec requires the Agent for Windows to be installed on the Exchange server.

For Exchange 2010/2013 Database Availability Group (DAG) configurations, the Agent for Windows should be installed on each mailbox server participating in the DAG.

The Agent for Windows should be installed on the Exchange server and must be running under the 'Local System' account on both the Exchange server as well as the Backup Exec server. The file versions of the Agent for Windows on the Backup Exec server and on the Exchange server should match.

Backup Exec Logon Account

To enable key features related to the protection and recovery of Exchange servers, such as granular recovery of Exchange objects, Backup Exec must have access to a uniquely named mailbox within the Exchange infrastructure. This mailbox is accessed by the Backup Exec logon account to enable Backup Exec to interact with Exchange and important components within the Exchange Information Store. The unique mailbox should be hosted on the same version of Exchange the target mailbox is hosted.

It's important to ensure that the mailbox is uniquely named and activated. To activate the mailbox, create a new profile within Microsoft Outlook for that user and logon to the mailbox using Outlook.

> **Note:** For information on how to confirm that an Exchange mailbox name is unique within the Exchange organization, refer to the following technote: TECH24691.

Ensure that the logon account meets the following requirements:

- For Exchange 2007, the Backup Exec Logon Account should be a member of the 'Organization Administrator' group.
- For Exchange 2010 and 2013, the Backup Exec Logon Account needs to have the 'Organization Administrator' role and be configured with 'Exchange Organization Management' rights.
- The Backup Exec Logon Account must be member of the local computer's Administration group on the Exchange servers.

Example Backup Exec Configurations for Protecting Exchange

This section contains a few example diagrams of Microsoft Exchange 2010/2013 environments protected by Backup Exec. Important components of both the Exchange infrastructure as well as the Backup Exec data protection solution are depicted.

The first diagram below depicts a distributed Exchange 2010/2013 environment with two mailbox servers configured in a DAG. In this example, all servers are being protected by Backup Exec, and as such the Agent for Windows is present on each server, including the Active Directory Domain Controller.

In this configuration, presuming the Agent for Applications and Databases has been licensed on the Backup Exec server, all levels of recovery would be available for the Exchange servers in this example, including granular recovery of Exchange 2010 mailbox objects.

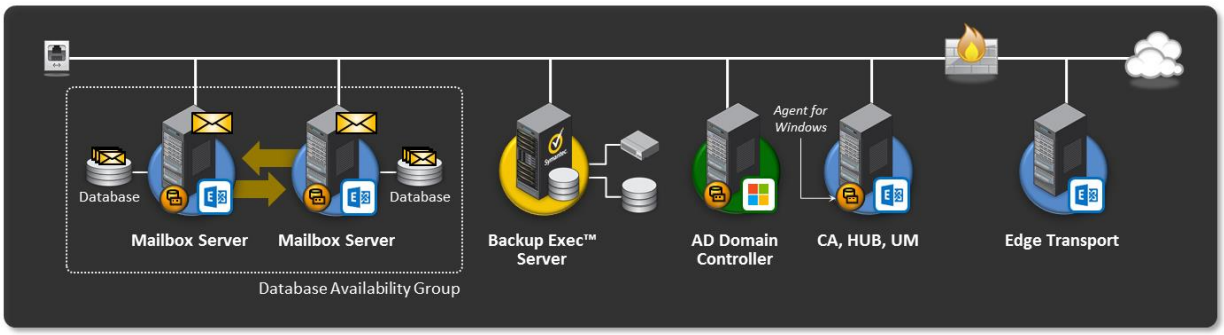


Figure 18: Backup Exec Protecting Physical Exchange 2013 DAG Environment

The second diagram below depicts two very basic virtual environments where Exchange is present. In the first example, a single Exchange virtual machine is being hosted on a Hyper-V server, and Backup Exec captures image-level backups of the Exchange virtual machine by interacting with the Hyper-V host through the local Agent for Windows installed on the Hyper-V host. In the second example, a single Exchange virtual machine is being hosted on a VMware server, and Backup Exec captures image-level backups of the Exchange virtual machine by interacting with the VMware host through the vStorage APIs for Data Protection (VDAP).

Since the Agent for Windows has not been installed on the Exchange virtual machine in either diagram, recovery will be limited to full virtual machine recovery and file/folder recovery; Exchange application recovery or granular Exchange mailbox object recovery would not be available.

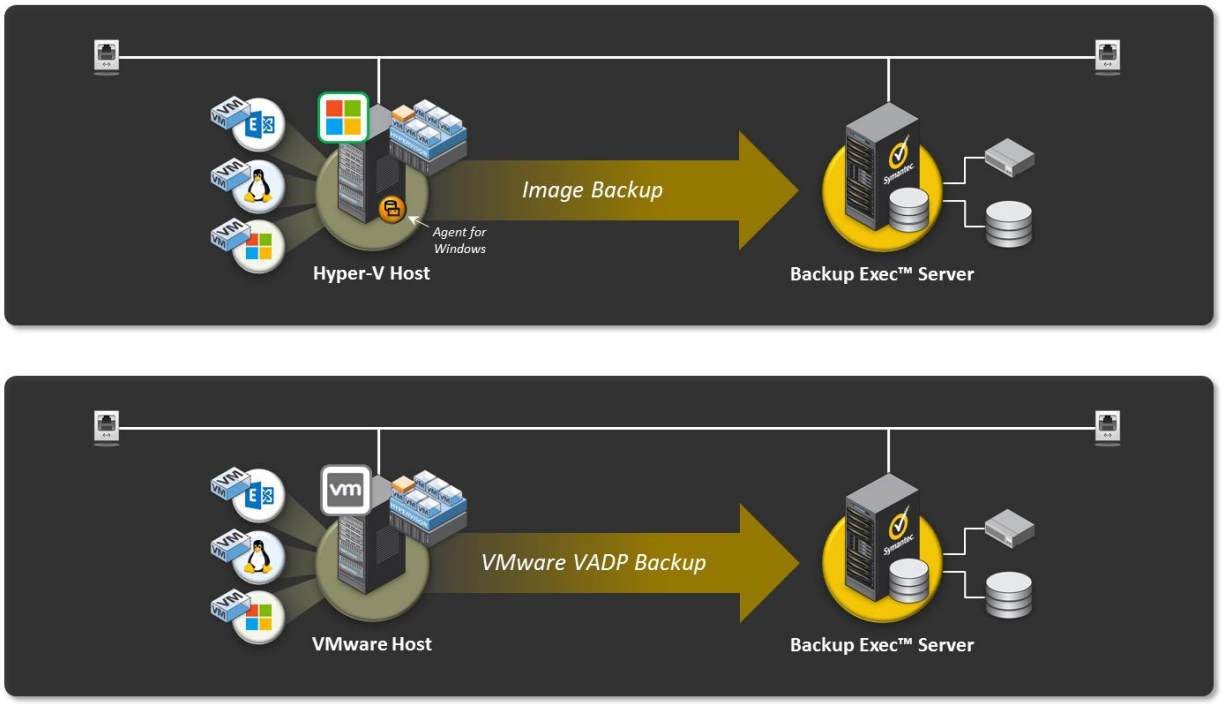


Figure 19: Backup Exec Protecting Virtualized Exchange Servers on Hyper-V and VMware

Exchange Protection Notes and Best Practices

General Exchange Best Practices

- Backup Exec 2014 supports Exchange 2013 CU3; earlier versions of Exchange 2013 are not supported.
- Avoid making the Exchange server a domain controller. This simplifies recovery procedures since Active Directory won't need to be recovered before Exchange.

  Note: In a disaster recovery scenario, if Active Directory and Exchange both need to be recovered, Symantec recommends they should be restored from a similar point in time of backup.

- Install the Exchange Server into a domain that has at least two domain controllers. With two domain controllers in a domain, databases on a failed domain controller can be updated with replication.
- For Exchange 2010/2013, use a Database Availability Group (DAG) with at least one passive database copy for each database to protect against data loss. If you can make more than one passive copy, the second passive copy should use a log replay delay of 24 hours.
- When protecting Exchange 2010/2013 environments, a Windows 2008 SP2 (x64), Windows 2008 R2 (x64), Windows 2012 (x64), or Windows 2012 R2 (x64) Backup Exec server is required. Exchange 2010 or 2013 Management tools must be installed on the Backup Exec server.

Protecting the Exchange Information Store

- When you run full backups, enable the option for Granular Recovery Technology (GRT). The GRT option lets you restore individual mail messages and folders from a database backup without the need for a separate mailbox backup.
- If you run GRT-enabled backup jobs, you should change the default staging location on the Backup Exec server to a volume that is not the system volume for faster performance. This volume should possess the same disk sector size as the volume used for Exchange transaction log storage on the Exchange server.
- Ensure that the scheduled maintenance for the Information Store does not run at the same time as the database backup.
- Run Exchange backup jobs separately from other backup jobs.
- Back up the Active Directory on a regular basis.
- Run a backup after you make any changes to system settings or application settings.
- For Exchange 2007, select individual storage groups for backup rather than individual databases in storage groups.
- For all versions of Exchange, to perform incremental and differential backups of storage groups, ensure that circular logging is not enabled on the storage group.

Note: A more comprehensive list of best practices for using Backup Exec to protect Exchange can be found here: HOWTO21796

Additional Resources

Link	Description
http://www.symantec.com/docs/HOWTO74428	**Exchange Protection Best Practices**
http://www.symantec.com/docs/TECH125261	**Exchange Management Tools**
http://www.symantec.com/docs/TECH158850	**Protecting Exchange Using PowerShell**
http://www.symantec.com/connect/blogs/new-backup-exec-partner-toolkit-v10	**Backup Exec Partner Toolkit**
http://www.symantec.com/business/support/index?page=content&id=TECH178479	**Backup Exec Licensing Guide**
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, Feature Briefs**
TECH205797	**Compatibility Documentation**
www.backupexec.com/skugenerator	**SKU Generator and BEST Tool**

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.

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. Other names may be trademarks of their respective owners. 8/2014