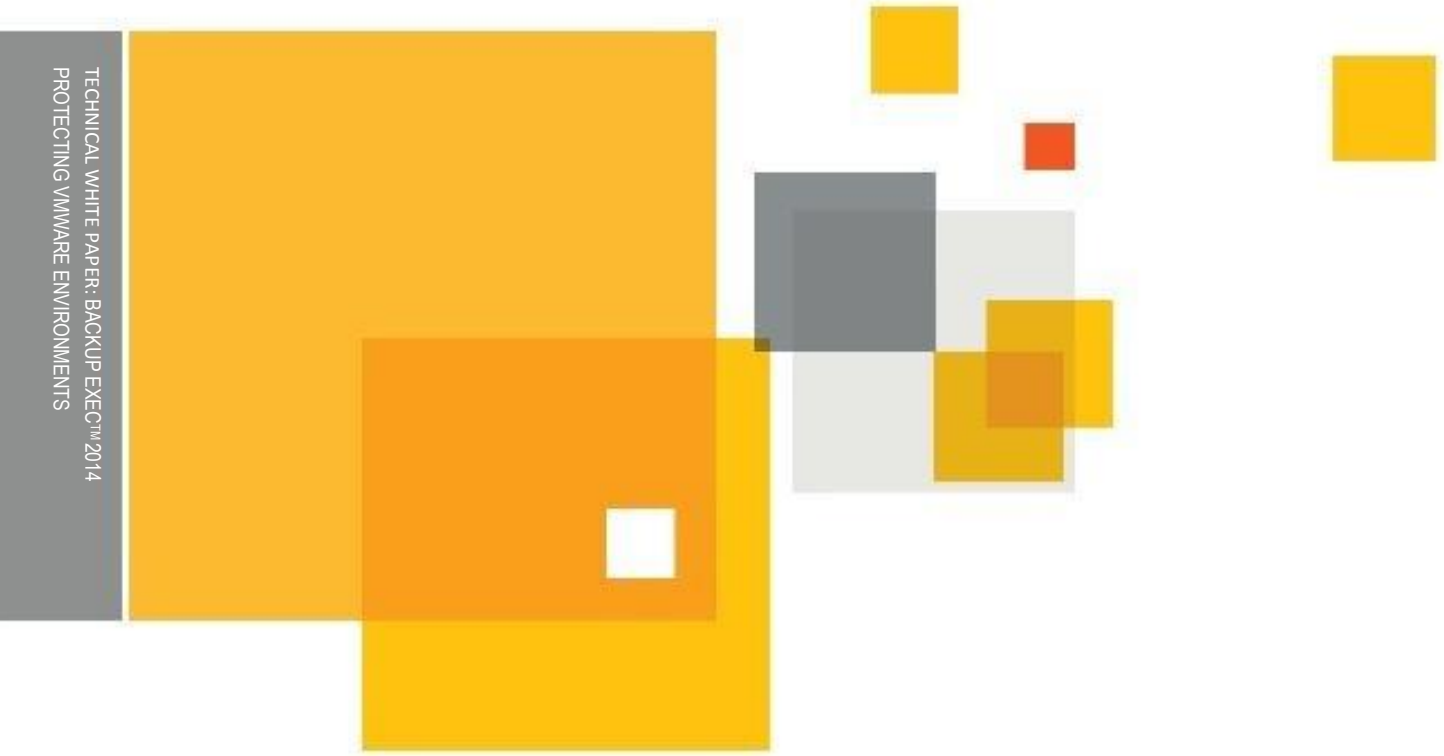

Backup Exec™ 2014 Technical White Paper

Protecting VMware Environments

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 partners and end users as they design and implement Backup Exec 2014 in VMware environments and make related decisions. The business value of Backup Exec 2014 in VMware environments is also covered.

This white paper includes the following topics:

- Business Value
- Underlying Technical Principles
- Virtualized Application Protection
- Virtual Machine Recovery Options
- Improved Usability for Virtual Environments
- Backup Exec Management Plug-in for VMware
- Example VMware Configurations
- Performance Recommendations
- Notes and Best Practices

For step-by-step instructions for installing and managing Backup Exec 2014 and the Agent for VMware and Hyper-V, refer to the *Symantec Backup Exec 2014 Administrator's Guide* available here: TECH205797.

Business Value

Virtualization technology has been widely adopted by organizations of all sizes to optimize critical IT assets, such as data and application servers. As a result of this virtualization trend, companies are looking for efficient and effective ways to back up and recover their virtual servers and the critical applications that many of these virtual machines host, such as Microsoft Exchange®, SQL Server®, SharePoint®, and Active Directory®.

Because virtual host servers are used by many companies to virtualize production servers, the loss of a production virtual host can cost an organization more than losing a standalone physical server, since a single virtual host can be responsible for multiple virtual servers. A lost virtual host can impact productivity for hours or days while the IT administrator struggles to recover or repair the virtualization infrastructure.

Market leaders in virtualization technology include the VMware vSphere platform and the Microsoft Hyper-V platform. Modern backup and recovery solutions designed specifically for VMware and Hyper-V environments are critical to helping organizations quickly recover in the event of a disaster, whether it occurs at the virtual host level, the virtual machine level, the application level, or the file/folder level.

Backup Solutions Designed Specifically for Virtual Environments

Administrators responsible for the backup and recovery of virtualized environments understand the frustration and difficulty associated with backup technologies that are not specifically designed to protect virtual infrastructures. Administrators who rely on legacy, misfit solutions to protect their virtual resources face several challenges, such as the following:

- Performance impacts from agent-based backups inside virtual machines competing for resources
- Downtime resulting from having to shut down virtual machines to protect them completely
- Slow file-by-file backups that repeatedly capture redundant data in each virtual machine
- Lengthy restore processes of an entire virtual machine to recover a single file
- Separate backups for virtualized applications like Microsoft Exchange®, SQL Server®, and SharePoint®
- Lack of ability to leverage different data transport paths depending on the needs of an environment
- Storage management problems from storing backups of large virtual disk files, such as VMDK files

Backup Exec 2014 and key virtual features, such as Backup Exec's integrated V-Ray technology, are designed specifically to protect virtual environments and solve the problems listed above.

Integration with the Latest Virtualization Technology

A significant advantage of Backup Exec 2014 in virtual environments is direct integration with the VMware virtual platform. This integration enables advanced functionality built specifically for the optimized protection of VMware environments.

VMware vSphere Integration

Backup Exec 2014 integrates with VMware's vStorage APIs for Data Protection (VADP) to eliminate important challenges associated with the backup of VMware virtual machines and to provide faster backup performance with less overall storage consumption. This is accomplished through the following:

Support for the Latest VMware vSphere Environments

- vSphere 5.5 (including update 1)
- vSphere 5.1 (including updates 1 and 2)
- vSphere 5.0 (including updates 1, 2, and 3)
- vSphere 4.1 (including updates 1, 2, and 3)

- vSphere 4.0 (including updates 1, 2, 3, and 4)

**For an authoritative list of platforms and applications supported by Backup Exec 2014, please refer to the Backup Exec Software Compatibility List available here: TECH205797*

VMware VADP Integration

- Enables backup of all virtual machines
- Provides backup of VMware virtual machines over SAN infrastructures
- Eliminates the shutting down of virtual machines in order to protect them

VMware Changed Block Tracking Support

- Enables full, differential, and incremental backups of VMware virtual machines
- Full backups: capture full point-in-time backup of the virtual machine
- Differential backups: backup of only what has changed since the last full backup
- Incremental backups: backup of only what has changed since the last backup

VMware Block Optimization Support

- Intelligent skipping of unused blocks within a virtual disk file
- Greatly reducing backup sizes and increasing backup speed

Integrated Granular Recovery Technology

From a single-pass backup of a virtual machine, recover:

- An entire virtual machine
- Individual files and folders*
- Entire applications*
- Granular application objects*

**For an authoritative list of platforms and applications supported by Backup Exec 2014, please refer to the Backup Exec Software Compatibility List available here: TECH205797*

Advanced Data Deduplication Support

- Support for deduplication of VMware virtual machine backups
- Advanced stream handler enables increased deduplication efficiency of VMDK files and their contents
- Significant reduction of disk backup storage requirements

Integration with Microsoft's VSS API

- Leverages VSS writers within each Windows-based virtual machine
- Enables Microsoft best-practice protection of applications such as Exchange®, SQL Server®, and SharePoint®
- Support for "VSS Full" and "VSS Copy" backup operations
- Application quiescence and log truncation

Complete Virtual and Physical Protection in a Single Solution

Backup Exec 2014 delivers a cost-effective and state-of-the-art solution for the protection of VMware environments. This includes the following:

- Image-level protection of VMware virtual machines
- Comprehensive protection of virtual systems and physical systems in a single backup solution
- Support for disk, tape, and cloud storage targets
- Integration with VMware's vStorage APIs for optimized backup and recovery processes
- Granular file and application object recovery of VMware virtual machine backups
- Storage optimization through advanced data deduplication technology

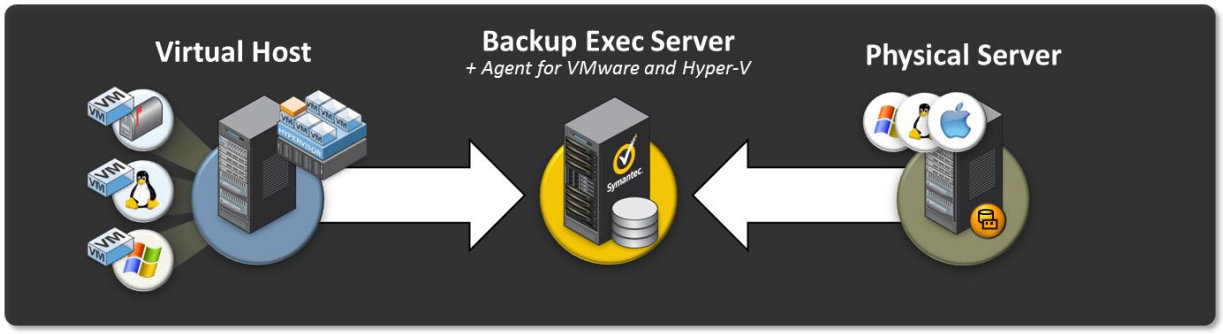

Figure 1: Protection for Physical and Virtual Environments

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.

Backup Exec 2014 Software Editions

Backup Exec 3600 Appliance

Unified Virtual and Physical Protection in a Single Solution

Underlying Technical Principles

VMware Resource Discovery

When configuring Backup Exec 2014 to protect VMware resources using the Agent for VMware and Hyper-V, virtual machines can be added to the backup infrastructure in either of the following ways:

- **vSphere ESX/ESXi servers** – Individual vSphere ESX/ESXi servers can be added by entering the vSphere hostname or IP address into the Backup Exec interface.
- **vCenter servers** – Environments with multiple vSphere ESX/ESXi servers managed by a vCenter server can be added by connecting to the vCenter server that automatically discovers all the virtual machines in the vCenter environment.

Backup Exec 2014 uses VMware Web Services for most communications with vCenter servers, including vSphere ESX/ESXi host and virtual machine discovery operations. The VMware vSphere Web Services SDK was specifically designed to allow management applications to integrate with the vSphere platform.

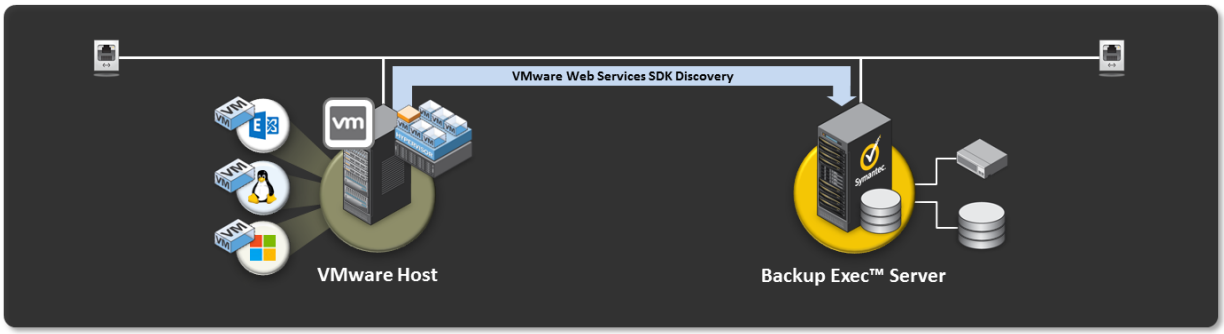

Figure 2: VMware Virtual Machine Discovery Diagram

Dynamic Inclusion

The dynamic inclusion feature of Backup Exec 2014 allows new virtual machines – created or added to the environment after backup jobs for the virtual infrastructure are configured – to be automatically discovered and protected by Backup Exec without the administrator having to manually adjust existing backup jobs to include new virtual machines. New virtual machines are discovered at job run time and are automatically protected.

This dynamic inclusion capability applies to all new virtual machines that are added to a vSphere ESX/ESXi server after one or more Backup Exec jobs have been configured to protect virtual machines on that vSphere ESX/ESXi server.

When Administrators do not want certain new virtual machines to be protected by Backup Exec or by a specific backup job they can exclude those virtual machines by using the Backup Exec console to edit the corresponding backup job.

Virtual Machine Backup Methods

When protecting VMware environments with Backup Exec 2014, partners and customers have the option to protect virtual machines using any of the following methods:

- **Agentless backups** (file server virtual machines) – this method captures image-level, snapshot backups of virtual machines associated with the vSphere ESX/ESXi server without a local Backup Exec agent present within the virtual machine; this method enables full virtual machine recovery and granular file and folder recovery.

- **Agent-assisted backups** (Windows virtual machines hosting Microsoft applications) – This method captures image-level backups of virtual machines and also includes additional application protection and recovery functionality, including full application recovery and granular application recovery.

  Advanced application recovery capabilities are enabled by the Agent for Windows being installed on the virtual machine.

  > **Note:** An agent-assisted backup is not an agent-based backup; backups are still image-level, snapshot backups captured through VMware VADP processes. The presence of the Agent for Windows within the virtual machine is leveraged for discovery of the application and the collection of application metadata required for granular recovery operations.

- **Agent-based backups** (virtual machines with unique attributes) – This method captures backups through a local agent installed on the virtual machine, and essentially treats the virtual machine like a standalone physical server.

  This method is recommended in situations where image-level backups are not optimal, such as when protecting virtual machines configured with Physical Compatibility Mode RDM disks.

Agentless, agent-assisted, and agent-based backups can be mixed and matched to meet the needs of an environment. For example, a partner or customer may choose to protect all Windows virtual machines using agent-assisted backups while protecting Linux-based virtual machines using agent-based backups.

Backup Data Transport Modes

A transport mode is the physical data path used for moving virtual machine backup data to the Backup Exec server.

The following transport modes are supported by Backup Exec:

Transport Mode	Description
SAN	Uses shared storage connections for data transfers to a physical Backup Exec server
HOTADD	Backup Exec server installed on a virtual machine
NBD	Uses the LAN/ethernet for data transfers to a Backup Exec server
NBDSSL	Uses the encrypted LAN/ethernet for data transfers to a Backup Exec server

While capturing backups of VMware virtual machines, Backup Exec 2014 leverages integration with the VMware vStorage APIs for Data Protection (VADP), enabling the utilization of “advanced transport mode”. This means that for each virtual machine that is protected by Backup Exec, VMware will determine all the available ways through which the requested backup data can be transported to the Backup Exec server. After a data request is generated by Backup Exec, VMware returns a list of transport modes (SAN, NBD, HOTADD, etc) that are supported and available. Based on this list and the selections supplied by the user within Backup Exec, a transport mode is selected.

For SAN environments, it is important to note that if Backup Exec is unable to acess the SAN during a backup operation, it will revert to other available data paths, such as NBD (LAN), in order to complete the job successfully.

Users can select one or more transport modes from a list within the Backup Exec interface and adjust the priority of the modes (move up/move down in screenshot below).

The transport mode options can be found by editing the virtual machine backup job and navigating to the **Virtual Machines** option on the left pane:

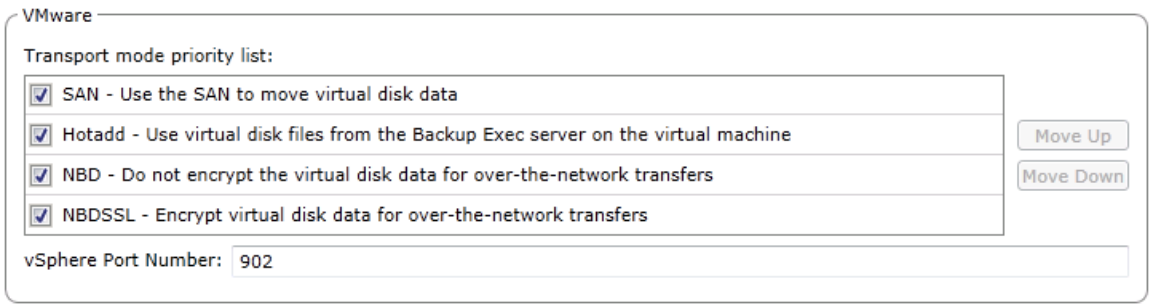

Figure 3: VMware Transport Mode Options

If incorrect or unexpected transport modes are being used for backup operations, as a troubleshooting step, disable all transport modes except the desired transport mode. If the job fails, review the job logs for a better understanding of the root cause.

VMware VADP Integration

Backup Exec 2014 fully integrates with VMware's vStorage APIs for Data Protection (VADP) and provides a number of key capabilities, including the following:

- High overall backup performance, particularly in SAN-based environments
- Changed-block tracking for fast block-level incremental or differential backups
- Block optimization, that ignores unused virtual disk blocks, improves performance and lowers backup storage requirements
- Backup and recovery support of both thin and thick-provisioned virtual disks
- Template virtual machine backup

Backup Exec 2014 supports the protection of the following VMware vSphere environments:

VMware vSphere Version	Notes
vSphere 5.5	Includes update 1
vSphere 5.1	Includes updates 1 and 2
vSphere 5.0	Includes updates 1, 2, and 3
vSphere 4.1	Includes updates 1, 2, and 3
vSphere 4.0	Includes updates 1, 2, 3, and 4

Note: For an authoritative list of platforms and applications supported by Backup Exec 2014, please refer to the Backup Exec Software Compatibility List available here: TECH205797

No Proxy Server Required

The protection of VMware virtual machines using the Agent for VMware and Hyper-V does not require a proxy server. Backup data is moved directly to the Backup Exec server for storage.

The VMware vStorage APIs for Data Protection (VADP) eliminate the need for a proxy server to mediate between a vSphere ESX/ESXi host and the Backup Exec server. Symantec and VMware work closely together to ensure that performance impacts during backup are minimal.

Storage Optimization Features

Backup Exec 2014 includes multiple storage optimization technologies that offer scaled benefits to partners and customers looking to control backup storage costs. These include the following:

- Block optimization
- Differential and incremental backups
- Data deduplication

When used together, these storage optimization features greatly reduce backup data requirements to only a small fraction of what they would be without these optimization technologies.

Block Optimization

Virtual disks, like physical disks, always contain some free space. The amount of free space within a virtual disk can vary; in the case of some virtual machines, a large percentage of the disk may be free or unused.

Backup Exec 2014 includes block optimization technology that enables the intelligent identification of empty space within a virtual disk file and the protection of only used portions of the virtual disk. For example, if a virtual disk file has a total capacity of 40 GB but contains only 15 GB of actual data, Backup Exec captures only 15 GB of data during a full backup job. This accelarates backups and reduces backup storage requirements.

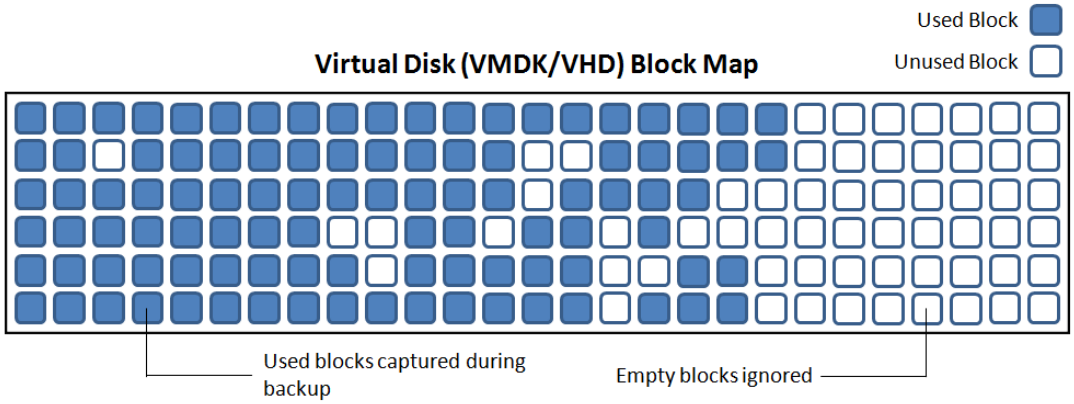

Figure 4: Block Optimization Diagram

Incremental and Differential Backups

Backup Exec 2014 supports changed block tracking (CBT) for VMware environments. This means that Backup Exec can track the changes that have occurred against a virtual machine since the last backup operation at the block level, and capture only the block-level changes since the last backup (incremental) or since the last full backup (differential).

Differential and incremental backups capture significantly less data than full backups. As a result, incremental and differential backups reduce backup windows and reduce the amount of required backup storage when protecting VMware virtual machines.

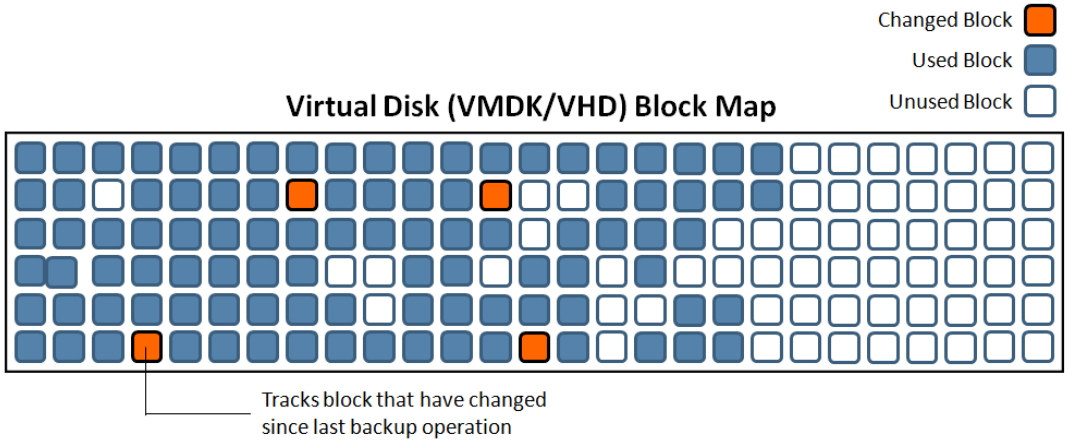

Figure 5: Changed Block Tracking Diagram

Data Deduplication

Backup Exec 2014 also supports the deduplication of VMware virtual machine backups. The Deduplication Option enables block-level deduplication of all backups stored in a Backup Exec deduplication disk storage device, generally resulting in a 9-to-1 or greater reduction in storage consumption for backup data.

> **Note:** The actual reduction in disk storage requirements as a result of the deduplication of VMware virtual machine backups will vary depending on a number of factors, such as the selected retention period for the backups, the type of data within the VMware virtual machines, and so on.
>
> For an estimate of how well VMware virtual machine backups will deduplicate in a specific environment, the Backup Exec Deduplication Assessment Tool (part of the Backup Exec Partner Toolkit) may be used. This tool is available free of charge, and does not require Backup Exec to be installed or present in the environment being evaluated.
>
> Backup Exec Partner Toolkit

The Deduplication Option includes intelligent stream handlers for VMware virtual disk files (VMDK) enabling further storage savings when using both the Agent for VMware and Hyper-V and the Deduplication Option together. The Deduplication Option and associated virtual disk stream handler technology will be discussed in further detail later in this document.

VMware Storage Distributed Resource Scheduling

The vSphere platform's SDRS capabilities allow virtual administrators to simplify management of datastores through the introduction of datastore clusters, also referred to as storage pods. In addition, depending upon settings defined by the administrator, SDRS has the capability to automatically move virtual machine disk files to different datastores within a cluster to optimize performance, without interrupting virtual machine operations. This feature works synchronously with other VMware technologies, such as vMotion.

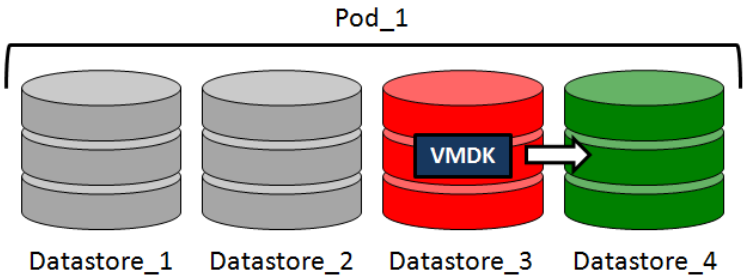

Figure 6: VMware Storage Distributed Resource Scheduling Diagram

Backup Exec 2014 fully supports virtual machines that are located within a datastore cluster and enabled for SDRS.

If a virtual machine is being actively backed up by Backup Exec or is having data restored to it at the time an SDRS event for that virtual machine occurs, Backup Exec places a temporary lock on the virtual machine, delaying the SDRS event until after the operation has completed and the associated virtual machine snapshot has been removed. After the backup is complete, the virtual machine is unlocked and the SDRS event proceeds normally. Backup Exec does not remove SDRS attributes from a virtual machine during backup or restore operations.

In addition, administrators can restore virtual machines to the cluster level or to specific datastores within a cluster.

Virtualized Application Protection

VSS Support

Backup Exec 2014 supports online backups of VMware virtual machines that host Microsoft applications and that utilize Microsoft's VSS framework.

VSS-aware applications such as these are protected as part of a normal image-level backup of the entire virtual machine. This process leverages VSS to capture a consistent snapshot of the virtual machine and the VSS-aware applications that it hosts. This VSS snapshot process also automatically truncates transaction logs for Exchange, Active Directory, and SQL. These virtual machines are not taken offline during this process; normal operations continue.

Backup Exec 2014 supports both "VSS Full" and "VSS Copy" backup operations. By default, "VSS Full" backups are performed. Administrators can adjust this setting in the 'Virtual Machines' backup options section of the Backup Exec 2014 user interface.

Note: For performing online backups of VMware virtual machines, VMware Tools must be installed on the virtual machines that host applications for enhanced VSS provider support.

Note: Without installing the Agent for Windows on the virtual machine hosting the VSS-aware application, the virtual machine is still protected using VSS and the application inside the virtual machine continues to be backed up in a consistent state. However, recovery options are limited to restoring the entire virtual machine or granular files and folders.

Advanced Application Protection and Recovery

Advanced protection and recovery of applications that have been virtualized in a VMware environment can be enabled by combining the Agent for Applications and Databases with the Agent for VMware and Hyper-V. When these agents are combined, advanced protection and recovery capabilities are enabled through agent-assisted backups. This agent-assisted configuration continues to provide single-pass, image-level backup protection of the virtual machines hosting applications in a VMware environment.

This agent-assisted configuration also allows for additional application protection capabilities to be enabled, such as automatic virtualized application discovery and granular application object recovery capabilities. Because of these critical additional features enabled by the Agent for Applications and Databases, Symantec recommends using this agent with the Agent for VMware and Hyper-V when protecting virtualized applications in a VMware environment.

Without the addition of the Agent for Applications and Databases, and without installing the Agent for Windows on each virtual machine hosting an application, backups become standard agentless VMware virtual machine backups. In this configuration, the recovery capabilities are limited to full virtual machine recovery and granular file and folder recovery.

Note: When the Agent for Windows is not installed on a virtual machine, files and folders cannot be restored directly back to that virtual machine. The files and folders being recovered first must be restored to another accessible location and then moved back to the target virtual machine using other methods.

Streamlined SQL Log Truncation

Backup Exec 2014 introduces a simplified approach to the truncation of SQL transaction logs where SQL is running as a virtual machine in a VMware or Hyper-V environment. A new check box option within the Backup

Exec user interface includes an additional process to backup and truncate SQL transaction logs further streamlining this process for administrators.

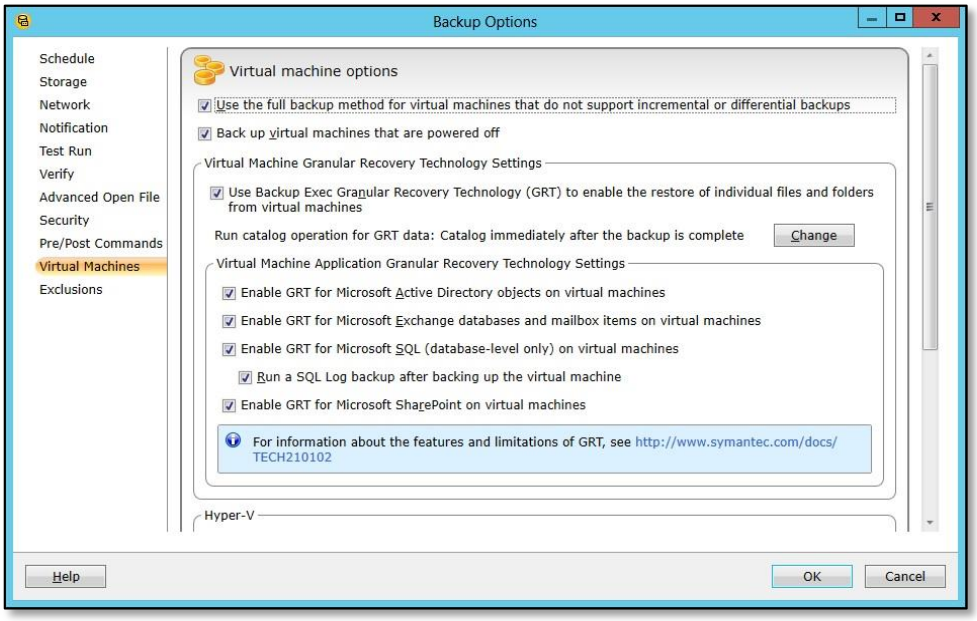

Figure 7: Streamlined SQL Log Truncation Options

Non-VSS Compliant Virtual Machines and Applications

Platforms and applications that are not VSS-compliant (such as many versions of Linux), cannot be effectively protected using VSS processes. If such non-VSS compliant virtual machines are protected using the Agent for VMware and Hyper-V and image-level backups, such backups will be captured without knowledge of any applications that may reside within the virtual machine. The virtual machines remain online and functional during the snapshot and backup process; however, the backups are crash-consistent.

Administrators using Backup Exec 2014 to protect virtual machines that are not VSS-compliant should consider using agent-based backups, leveraging the Agent for Windows or the Agent for Linux. Using the Agent for Windows or the Agent for Linux to protect non-VSS-compliant virtual machines helps to ensure that the virtual machines, as well as the applications they contain, are backed up effectively.

Virtual Machine Recovery Options

Backup Exec 2014 supports a wide range of recovery options for VMware virtual machines. Each of these recovery options is possible from a single-pass, image-level backup operation. No additional or separate backup pass is required to achieve additional levels of granular restore.

Note: For virtualized applications, granular application recovery can only be enabled by combining the Agent for VMware and Hyper-V with the Agent for Applications and Databases, and by installing the Agent for Windows to the virtual machines hosting applications in the VMware environment.

Full Virtual Machine Recovery

Backup Exec 2014 supports full recovery of VMware virtual machines. This includes all elements of a virtual machine, such as the virtual disk files and any other virtual machine-related files. During a full virtual machine recovery operation, virtual disk files are completely recovered, including the operating system, applications, and data. Integration with the Microsoft VSS service ensures that VSS-aware applications, such as Exchange and SQL, hosted on VSS-aware platforms, such as Windows 2008/R2 and Windows 2012/R2, are completely recovered.

A virtual machine can be recovered to the original VMware host or can be redirected to an alternate host.

Note: To redirect a virtual machine to an alternate VMware host during recovery, the alternate host must also be licensed for the Agent for VMware and Hyper-V.

Virtual Disk Configurations and Support

Backup Exec 2014 supports the protection of VMware virtual machines configured with either thick or thin virtual disks. On recovery, the administrator can recover a VMware virtual machine with either a thick or thin virtual disk, and can therefore change the virtual disk type during a recovery operation (e.g. thick to thin or thin to thick).

Application Recovery

For virtual machines hosting Exchange, SQL, SharePoint, and Active Directory, full recovery at the application level is also supported by Backup Exec 2014, but only when the Agent for VMware and Hyper-V is combined with the Agent for Applications and Databases and the Agent for Windows is installed on the virtual machine hosting the application. This allows administrators to recover a full application instance if a full virtual machine recovery is not necessary or is not intended.

Exchange, SQL, SharePoint, and Active Directory backups are fully VSS-compliant in accordance with Microsoft best practices, ensuring that the applications operate and function correctly after recovery.

Note: Application-level recovery is not supported for virtualized applications in a distributed configuration when protecting the virtual machines using image-level VADP backups through the Agent for VMware and Hyper-V.

Granular Application Recovery

Backup Exec 2014 enables administrators to recover granular application objects from single-pass backups of VMware virtual machines when the Agent for VMware and Hyper-V is combined with the Agent for Applications and Databases and the Agent for Windows is installed on the virtual machine hosting the application. For example, the granular application objects that can be recovered in this configuration include Exchange mailboxes, emails, attachments, and calendar items, Active Directory objects such as user and computer objects, SharePoint documents, SQL databases, and more.

Important: A separate database-level or object-level backup is not required for granular application recovery; the same single-pass, image-level backup is harvested for granular application object recovery operations.

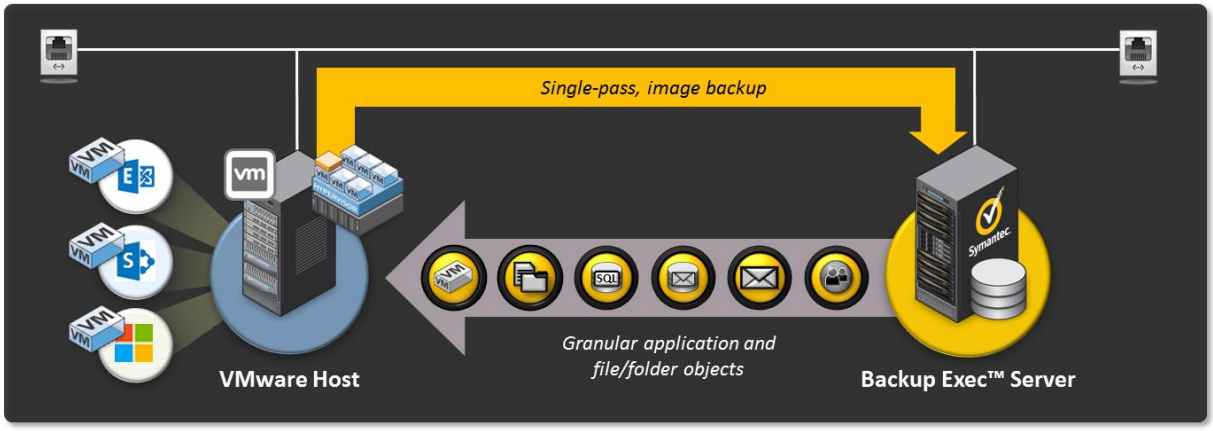

Figure 8: Granular Recovery for Virtualized Applications

Note: Granular application recovery is not supported for virtualized applications in a distributed configuration when protecting the virtual machines using image-level VADP backups through the Agent for VMware and Hyper-V.

Granular File and Folder Recovery

Backup Exec 2014 also supports granular file and folder recovery from VMware virtual machine backups captured using the Agent for VMware and Hyper-V. The recovery is performed from the same single-pass, image-level backups used for other recovery options.

It is not necessary to have the Agent for Windows installed on a VMware virtual machine to enable granular file and folder recovery. However, having the Agent for Windows installed on the virtual machine is required in order to recover files and folders directly to the source virtual machine.

Optionally, if the Agent for Windows is not installed on the original machine from which backups were captured, files and folders can be recovered to a local directory on the Backup Exec server and moved back to the original virtual machine using other methods.

Improved Usability for Virtual Environments

New Lower Pane Feature

In Backup Exec 2014, a new feature was implemented to increase the usability experience for administrators protecting virtual environments. This new feature – commonly referred to as the 'lower pane' view – enables administrators to view additional details about a virtual host in the **Backup and Restore** tab of the Backup Exec 2014 user interface.

Interactive View

This new view area associated with virtual hosts represents a current view of the target virtual host and the folders and virtual machines it contains, and can be refreshed as required. From this new view area, recovery operations can be directly initiated for those virtual machines that have been backed up at least once by Backup Exec.

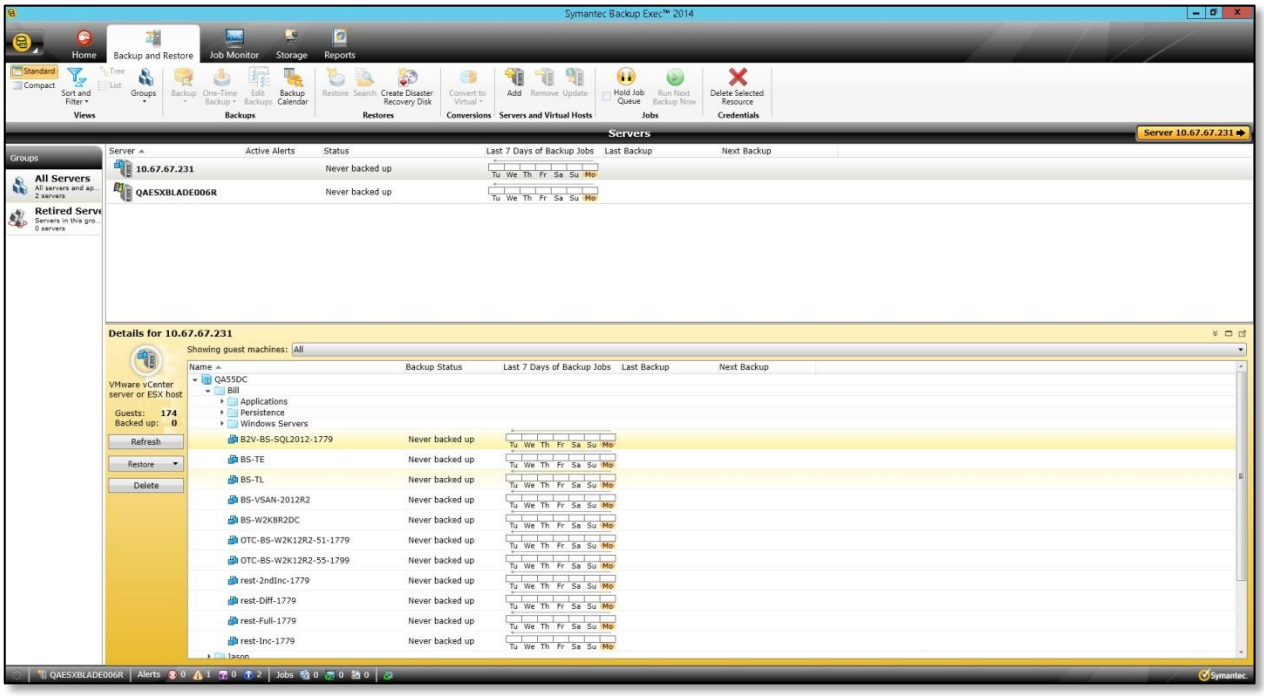

Figure 9: New 'Lower Pane' View for Virtual Hosts

This new feature further streamlines the overall experience for Backup Exec 2014 administrators protecting critical virtual infrastructures.

Backup Exec Management Plug-in for VMware

Overview

The Backup Exec Management Plug-in for VMware allows administrators of VMware virtual environments that are protected by Backup Exec 2014 to utilize the vSphere client application to perform status monitoring and virtual machine validation tasks without having to visit the Backup Exec server console. The Backup Exec Management Plug-in for VMware provides the administrator with the following capabilities:

- Monitor backup status of VMware virtual machines protected by Backup Exec.
- View resource-centric backup status of protected virtual machines.
- Perform virtual machine validation tasks.

The information that is displayed in the vSphere client interface is retrieved from the Backup Exec server that controls the backup jobs protecting VMware virtual machines.

The Backup Exec Management Plug-in for VMware is installed on a system that also runs the VMware vSphere client, and supports both vCenter server environments and standalone vSphere ESX/ESXi hosts. The Backup Exec management information is displayed within the context of the vSphere client application on a separate **Symantec Backup Exec** tab.

The Backup Exec Management Plug-in for VMware requires VMware vSphere 4.0 or later components.

> **Note:** For more information on the versions of Backup Exec and VMware vSphere that are supported by this management plug-in, please refer to the Backup Exec Software Compatibility list, available here: TECH205797

Login

Users of the Backup Exec Management Plug-in for VMware will be required to log in to the associated Backup Exec server. This can be done by specifying the server's hostname or IP address. The credentials must represent a user who is a member of the Backup Exec Operators group.

Monitoring

In the plug-in display, the administrator can view all the Backup Exec backup jobs that protect virtual machines in the VMware environment. For environments with multiple Backup Exec servers running jobs that protect VMware virtual machines, the administrator can connect to one Backup Exec server at a time to monitor the status of VMware backup jobs processed by that server.

Additional views are also offered, such as a view that displays unprotected virtual machines or a view that displays virtual machines that are protected by a different Backup Exec server.

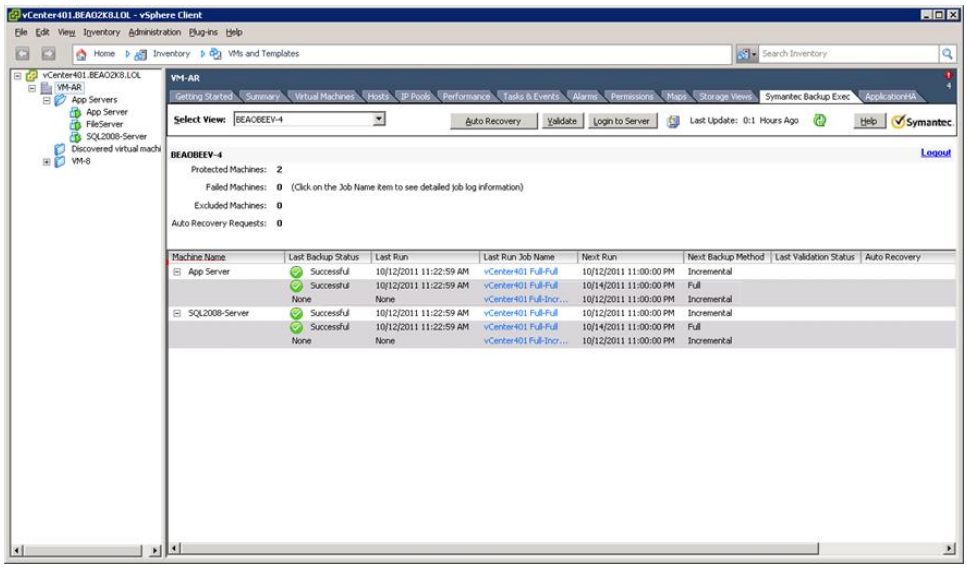

Figure 10: Backup Exec Management Plug-in for VMware

Virtual Machine Validator

A key feature of the Backup Exec Management Plug-in for VMware is the Virtual Machine Validator. This feature enables administrators to validate the integrity of VMware virtual machine backups captured using Backup Exec 2014. The Virtual Machine Validator functionality is available through the VMware vSphere client application. Like the Management Plug-in for VMware, the Virtual Machine Validator feature is available to Backup Exec customers at no additional charge.

The Virtual Machine Validator operates by leveraging VMware Workstation to mount a backup of a virtual machine from backup storage and launch it. After the virtual machine boots, the Virtual Machine Validator connects to the local VMware Tools application inside of the virtual machine to ensure that the backup of the virtual machine booted correctly and to verify that it is valid. Custom scripts can also be executed within the virtual machine for further validation.

Validation events are initiated from the vSphere client interface, using the Backup Exec Management Plug-in for VMware. When the plug-in has been installed, a **Symantec Backup Exec** tab will appear in the vSphere client interface. The administrator can perform validation tasks using the options available on this tab.

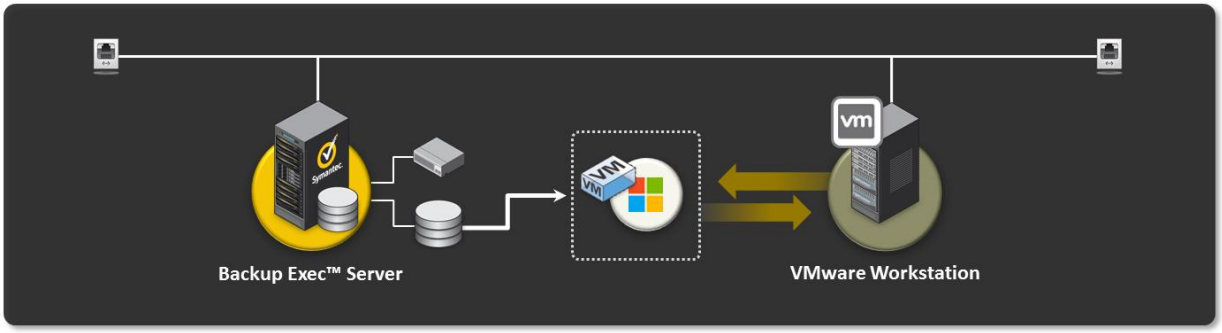

Figure 11: VMware Virtual Machine Validator Diagram

Results from virtual machine validation tests are published back to the Management Plug-in for VMware and displayed in the **Last Validation Status** column of the **Symantec Backup Exec** tab in the vSphere client.

The Virtual Machine Validator feature of the Backup Exec Management Plug-in for VMware supports different network configuration settings, allowing administrators to validate individual virtual machines or validate multiple virtual machines in a private network environment.

Virtual Machine Validator Notes

- Validation tasks can only be run for full, GRT-enabled VMware backups
- Validation tasks can only be run for VMware backups stored to disk or deduplication disk storage devices
- Validation tasks cannot be run for backup sets that have been transferred to remote Backup Exec servers through optimized duplication
- Symantec recommends installing VMware Workstation on a standalone system and not the same system where the Backup Exec server is installed

Note: For additional information on supported platforms and other requirements for the Virtual Machine Validator, please refer to the Backup Exec Software Compatibility List available here: TECH205797

Note: The Virtual Machine Validator component of the Backup Exec Management Plug-in for VMware does not support the validation of virtual machines using hardware version 10.

Note: The Virtual Machine Auto Recovery component of the Backup Exec Management Plug-in for VMware does not support the automatic recovery of vSphere 5.5 virtual machines. This is because the current release of ApplicationHA does not yet support the vSphere 5.5 platform.

Example VMware Configurations

Configurations of Backup Exec 2014 in virtual environments vary depending on the size, configuration, and complexity of the virtual environment that is being protected. In this section, we will review some basic configuration examples for VMware environments.

Basic VMware Environment with a Single vSphere ESX/ESXi Server

In this example, Backup Exec 2014 is protecting a single vSphere ESX/ESXi server with a small number of virtual machines. Backup Exec is installed on a separate physical server, because this usually offers the best performance. Optionally, Backup Exec could be installed as another guest virtual machine on the vSphere ESX/ESXi host.

This example also shows the virtual machines being protected as residing on a shared SAN storage array. When a vSphere configuration utilizes shared SAN storage, and the Backup Exec server is connected to the SAN infrastructure, VMware virtual machine backup data can be transported to the backup destination over the SAN, which can offer significant performance benefits.

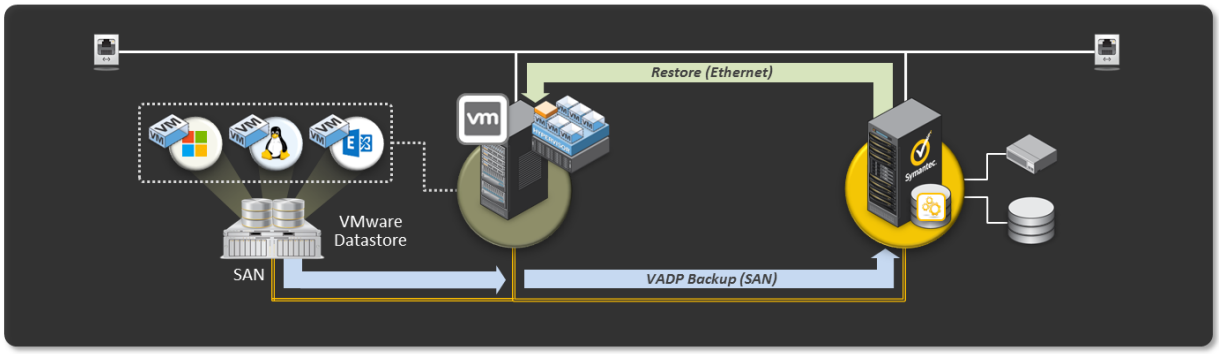

Figure 12: Basic VMware Environment with a Single vSphere ESX/ESXi Server

Advanced VMware vCenter Environment (Multiple vSphere ESX/ESXi Hosts)

In this example, Backup Exec 2014 is protecting a more complex VMware vSphere environment that includes multiple vSphere ESX/ESXi servers and a vCenter server. In configurations such as these, Backup Exec can protect virtual machines through the vCenter server itself and it is not necessary to perform operations at the vSphere ESX/ESXi server level.

This example also shows the virtual machines being protected as residing on a shared SAN storage array. When a vSphere configuration utilizes shared SAN storage, and the Backup Exec server is connected to the SAN infrastructure, backup data can be transported over the SAN, that can offer significant performance benefits.

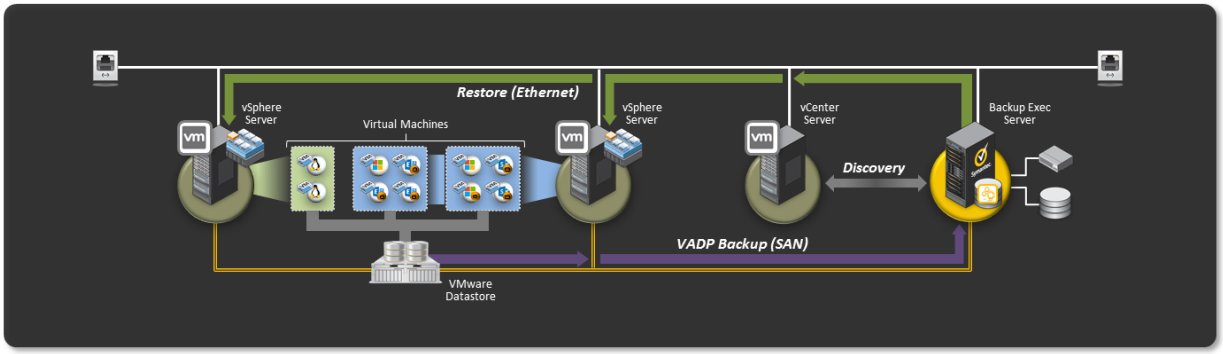

Figure 13: Advanced VMware vCenter Environment

Performance Recommendations

Tape Backup Devices

In most – but not all – environments, larger block and buffer sizes will yield better performance.

The host bus adapter (HBA) and HBA driver being used in a backup environment govern what block and buffer sizes are available for optimization. The screenshot below highlights the area of the Backup Exec 2014 user interface where block and buffer values can be customized for a specific tape drive.

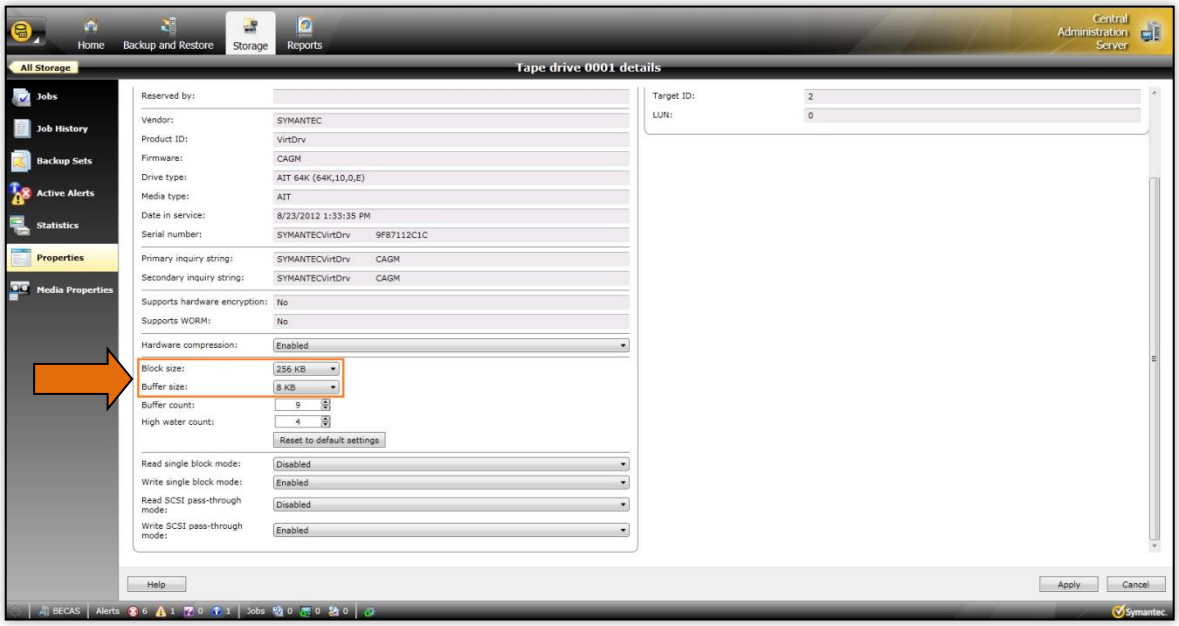

Figure 14: Block and Buffer Settings

Note: To avoid issues when using older tape devices or tape devices from different hardware manufacturers, please review the following tech note: TECH64105

Disk Backup Devices

In most – but not all – environments, larger block and buffer sizes will yield better performance.

Deduplication Disk Storage Devices

For deduplication disk storage devices hosted on NTFS volumes local to the Backup Exec server, the NTFS cluster size can impact performance. For optimal performance, consider placing the deduplication disk storage device on an NTFS volume formatted with a cluster size of 64 KB.

VADP Buffer Settings

Buffer settings associated with VADP (VMware) backups captured by Backup Exec can be adjusted by modifying the values of several registry keys on the Backup Exec server. Modifying the values of these registry keys may result in improved performance for VMware backups using SAN transport mode or NDB mode.

Please review the following tech note for more information: TECH185691

Note: The tech note above was originally written for Backup Exec 2010, but the information it contains also applies to Backup Exec 2014.

GRT Catalog Operation Scheduling

Backup Exec 2014 now allows administrators to configure schedules for when GRT cataloging operations must be performed. Managing the GRT catalog operation schedule improves backup performance by allowing these operations to occur at a later time, separate from the backup jobs with which they are associated.

SAN-based Backup Guidance

Configuring SAN-based VMware backups with Backup Exec 2014 and the Agent for VMware and Hyper-V is simple with the following guidelines:

- Zone the LUNs that contain the VMFS data store such that the Backup Exec server can see and access them.
- On the Backup Exec server, ensure that the `automount disable` and `automount scrub` commands have been run to disable automatic drive letter assignment.
- As a result of the `automount disable` and `automount scrub` commands having been run, the VMFS datastore LUNs will appear in Windows Disk Administrator (on the Backup Exec server) as "unknown"; do not attempt to mount, partition, or format these disks.

Backup performance will be largely determined by the slowest component of the entire backup data path from the vSphere ESX/ESXi Server to the Backup Exec storage location (i.e. Tape or Disk). These components are:

- vSphere ESX/ESXi server system resources: CPU (GHz)
- vSphere ESX/ESXi system disk I/O capabilities (Gbps)
- Network type (Fiber Channel 1/2/4/8GB, iSCSI, 1/10GB Ethernet, and so on)
- Backup Exec server system resources

General VMware Performance Guidelines and Expectations

Here are some basic guidelines that should be followed when designing a VMware environment to be protected by Backup Exec and configured for optimal performance:

- For SAN-based backups, consider installing Backup Exec on a standalone physical server.
- The internal bus of the Backup Exec server should be fast enough to support the I/O devices that are connected to it.

  If multiple I/O ports are used, a system with multiple internal buses should be considered to support the additional I/O.
- Backup Exec server I/O performance is generally more important than CPU performance.

  For example, a 2 GB Fiber connection should be able to transfer backup data at a nominal transfer rate of 140 MB/second.

  Backups over Gigabit Ethernet will likely be much slower, while 4/8 GB Fiber Channel connections and newer iSCSI configurations should be significantly faster.

Note: For more information, see the following tech note: TECH125455

Recommended Number of Virtual Machines to Protect with a Single Backup Exec Server

There is no programmatic limit to the number of virtual machines that a single Backup Exec server can protect. This is highly dependent on the size of the VMDK files for each virtual machine and the physical backup

infrastructure. In large environments, multiple Backup Exec servers can be used to optimize performance across the infrastructure.

Backup Strategy Recommendations

Symantec recommends using a seven-day rotation to protect VMware virtual machines with incremental or differential backups, where a full backup is run on the seventh day to avoid long incremental/differential backup chains.

Symantec also recommends using the Backup Exec 2014 Deduplication Option with the Agent for VMware and Hyper-V. This will significantly reduce backup storage requirements associated with virtual machine backups.

Notes and Best Practices

Virtual Machines Configured with RDM Physical Compatibility Mode Disks

Backup Exec 2014 and the Agent for VMware and Hyper-V cannot protect Raw Device Mapping (RDM) Physical Compatibility Mode disks using image-level backups.

Physical Compatibility Mode RDM disks bypass the vSphere storage infrastructure and the VMFS file system, and cannot have a snapshot taken through vStorage API processes. Physical Compatibility Mode RDM disks in this configuration are skipped automatically during backup job processing. Associated backup jobs are displayed as successful with exceptions.

To fully protect virtual machines configured with Physical Compatibility Mode RDM disks, the Backup Exec Agent for Windows or Agent for Linux must be installed on the virtual machines to protect them using agent-based backups.

vSphere 5.5 Environments and Virtual Disks with a Capacity Greater than 2 Terabytes

Backup Exec 2014 does not currently support using the Agent for VMware and Hyper-V with GRT-enabled backup jobs for vSphere 5.5 virtual machines that contain virtual disks with a capacity greater than 2 Terabytes. Non-GRT jobs are supported.

For the protection of virtual machines configured with virtual disks with a capacity over 2 Terabytes including GRT, install the Backup Exec Agent for Windows on the virtual machine and protect it using agent-based backups.

Virtual Machines Configured with Fault Tolerance

Backup Exec 2014 does not support using the Backup Exec Agent for VMware and Hyper-V to protect vSphere Fault Tolerant virtual machines.

Virtual machines enabled for Fault Tolerance, snapshots are not supported. The Backup Exec Agent for VMware and Hyper-V uses snap-based backups via the vStorage APIs for Data Protection (VADP) to protect VMware virtual machines, and therefore cannot protect virtual machines with Fault Tolerance enabled. The only way to back up a virtual machine that is enabled with Fault Tolerance using the Backup Exec Agent for VMware and Hyper-V is to break the Fault Tolerance, run the backup, then re-enable Fault Tolerance.

The workaround for protecting Fault Tolerant virtual machines without breaking the Fault Tolerance is to install the Agent for Windows on that virtual machine and protect it like a standalone physical machine using agent-based backups.

Windows 2012/R2 Running as a VMware Virtual Machine

Backup Exec 2014 can protect and recover Windows 2012/R2 virtual machines running in a VMware environment. This includes support for agent-less, agent-assisted, and agent-based backup methods.

For agent-based backups:

- The Backup Exec server must be installed on a Windows 2012/R2 server
- Data deduplication volume data is backed up and recovered in fully hydrated or un-optimized form.
- Data captured from ReFS volumes can only be restored to ReFS volumes.
- WinRE volumes must be mounted (e.g. drive letter assignment) to be protected.

For More Information

Link	Description
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	**Backup Exec White Papers**
www.symantec.com/business/products/datasheets.jsp?pcid=2244&pvid=57_1	**Datasheets, Solution Briefs**
TECH205797	**Backup Exec Compatibility Docs**
www.backupexec.com/configurator	**Backup Exec Product Configurator**
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.